Éléments explicites en théorie algébrique des nombres

Stéphane Vinatier

UNIVERSITÉ DE LIMOGES

École doctorale
Sciences et Ingénierie pour l'Information, Mathématiques
FACULTÉ DES SCIENCES ET TECHNIQUES

Habilitation à diriger des recherches

Discipline : Mathématiques et interactions

présentée et soutenue par

Stéphane VINATIER

le 9 décembre 2013

Éléments explicites en théorie algébrique des nombres

JURY :

Prof. Philippe Cassou-Noguès	Université de Bordeaux	Président, Rapporteur
Prof. Cornelius Greither	Universität der Bundeswehr München	Rapporteur
Prof. François Laubie	Université de Limoges	
Prof. Stéphane Louboutin	Aix-Marseille Université	Rapporteur
Prof. Christian Maire	Université de Franche-Comté	
Prof. Alain Salinier	Université de Limoges	Chargé du suivi

Éléments explicites
en théorie algébrique des nombres

Stéphane Vinatier

à ma fille Rosanne,
arrivée au milieu de tout cela

à mes collaborateurs Bill, Erik, François *et* Luca

N'est-il pas curieux, pour un animal aussi formidable de dimensions et de force que la baleine, que ce soit par un œil aussi menu qu'il voie le monde, et que ce soit par une oreille plus minuscule que celle d'un lièvre qu'il entende le tonnerre ? Et pourtant, s'il avait les yeux aussi grands que la grosse lentille du télescope de Herschel, et si ses oreilles se déployaient avec l'ampleur des porches de cathédrales, en aurait-il la vue meilleure ou l'oreille plus fine ? Point du tout. Aussi, pourquoi tant vouloir vous « élargir » l'esprit ? Subtilisez-le.

Herman Melville, *Moby Dick*, LXXIV *La tête du cachalot ; vue contrastée*
trad. Armel Guerne, Éd. Phébus, Paris, 2005.

Heaven,
Heaven is a place,
place where nothing,
nothing ever happens

D. Byrne and J. Harrison, *Heaven*,
in *Fear of Music* (Talking Heads),
Warner/Chappell Music, 1979.

Remerciements

Philippe Cassou-Noguès a été l'un de mes deux directeurs de thèse, à ce titre il a essayé avec beaucoup de patience de me transmettre une partie de ses connaissances en théorie algébrique des nombres et plus particulièrement de son expérience des modules galoisiens. Sans jamais paraître découragé par la lenteur de mes progrès, il a continué à suivre mon travail après la fin de ma thèse, m'indiquant des pistes fructueuses, relisant très attentivement mes écrits et m'aidant le cas échéant à y corriger les erreurs qu'il y débusquait. Enfin il m'a encouragé à soutenir mon habilitation à diriger des recherches, a accepté d'être rapporteur du mémoire et de faire partie du jury. Grand merci Philippe.

Cornelius Greither a apporté des contributions essentielles à la théorie des modules galoisiens et à la théorie algébrique des nombres en général : théorie d'Iwasawa, nombres de Tamagawa, classes réalisables… pour ne citer que quelques uns des thèmes qu'il a abordés. Cette stature imposante ne l'empêche pas de faire preuve d'une grande bienveillance et d'être toujours accessible et ouvert à la discussion. Grand merci Cornelius de m'avoir fait l'honneur et le plaisir d'être rapporteur et juré pour mon habilitation à diriger des recherches.

Stéphane Louboutin a énormément produit dans diverses branches de la théorie des nombres, notamment les unités fondamentales (thème sur lesquel j'ai le souvenir de l'avoir entendu donner un très bel exposé), les groupes de classes, les fonctions L ou de Dedekind… Il a accepté de rapporter sur mon mémoire et de faire partie du jury de la soutenance avec la bonne humeur et la décontraction qui le caractérisent. Grand merci Stéphane.

Christian Maire est une connaissance de longue date puisque nous sommes arrivés en même temps dans l'équipe de théorie des nombres de Bordeaux, lui comme maître de conférences, moi comme thésard. Son écoute, sa sympathie, sa détermination et sa droiture m'ont marqué. Ses travaux sur les discriminants dans des tours d'extensions ont donné avec éclat la mesure de ses talents scientifiques, qu'il a exercés de front avec des responsabilités administratives toujours plus importantes. Grand merci Christian d'avoir accepté de faire partie du jury, en plus de toutes ces occupations.

François Laubie et Alain Salinier sont mes collègues thématiquement les plus proches dans l'équipe de théorie des nombres de Limoges. Grand merci à eux deux d'avoir accepté de faire partie du jury de la soutenance, avec une mention spéciale pour Alain qui s'est chargé en amont du suivi de mon habilitation et m'a à ce titre encouragé et aidé à la mener à bien.

Même s'il n'a pu participer au jury de la soutenance, je tiens à remercier aussi Boas Erez, mon autre directeur de thèse, pour m'avoir offert de travailler sur le sujet sur lequel il avait lui-même commencé sa carrière et pour être resté toujours disponible pour discuter de modules galoisiens, voire de bien d'autres choses.

Grand merci enfin à mes quatre collaborateurs : Bill Allombert, Erik Pickett, François Arnault et Luca Caputo, ce fut un plaisir de travailler ensemble !

Table des matières

Chapitre 1

Introduction

Ce mémoire fait la synthèse de mes travaux de ces dernières années, seul ou, pour la plupart, en collaboration avec d'autres auteurs. Bien sûr il leur doit beaucoup, tant j'ai trouvé stimulant et enrichissant le travail à plusieurs, en particulier au moment de la recherche proprement dite : définir un problème à attaquer ensemble, évoquer ses idées et rebondir sur celles des autres, être confrontés à des obstacles imprévus et les dépasser grâce à la persévérance de l'un ou de l'autre, partager sa joie lorsqu'on voit enfin apparaître la solution… La phase de rédaction, qui est pour moi aussi importante et motivante que la précédente, est plus difficile à apprécier à plusieurs : mon besoin quasi-obsessionnel d'explications très détaillées peut paraître fastidieux. Quelques déconvenues antérieures l'ont forgé en m'apprenant qu'en mathématiques, encore plus qu'ailleurs peut-être, *le diable se cache dans les détails*.

Mais pas seulement lui ! De bonnes surprises y attendent parfois l'observateur attentif. Les *éléments explicites* du titre de ce mémoire en sont souvent issus. Ainsi, sans vouloir anticiper sur la présentation des résultats, c'est en réglant des choix assez subtils qu'on arrive dans [PV13] [1] à obtenir l'*égalité* d'une somme de Gauss galoisienne et d'une norme-résolvante ; c'est aussi parce que l'on dispose d'une formule explicite pour certains éléments que l'on parvient à vérifier qu'ils possèdent les propriétés attendues. Il y a donc un double intérêt à rendre plus explicites les objets qui nous concernent : mieux les identifier et les manipuler plus facilement, chacun de ces aspects nourrissant évidemment l'autre. Dans [CV13], une analyse très poussée des modules de torsion considérés fait apparaître, via le théorème de Stickelberger, des unités avec une signification arithmétique très forte et des propriétés qui nous permettent d'arriver à nos fins (notamment le théorème de Hasse-Davenport). Dans [Vin05], l'action du groupe de Galois sur une expression faisant intervenir les conjugués d'un éléments permet de la factoriser explicitement et d'en déduire, via un critère sur sa valuation, la trivialité d'une certaine classe.

Dans [AV12], on construit des extensions à groupe de Galois non abélien de degré 27 et d'exposant 9 par un procédé arithmétique très explicite, ce qui permet d'une part d'accéder à certaines de leurs propriétés et d'autre part de procéder à des calculs numériques assez poussés. Dans [APV12], les bases normales auto-duales explicites construites auparavant par Pickett dans [Pic10] sont utilisées pour mener des calculs de complexité. Dans [Vin13] c'est la base normale auto-duale pour les corps cyclotomiques décrite par Erez dans [Ere88] qui sert de point de départ. Enfin, l'étude de la combinatoire de résolvantes développée dans [Vin09] permet de comprendre pourquoi les calculs de valuation 3-adique explicites menés dans [Vin05] ne peuvent s'étendre à d'autres valuations.

Au-delà de ces exemples, on voit que même dans une théorie mathématique bien établie comme la théorie algébrique des nombres « classique », des progrès restent possibles dans

1. Les références bibliographiques du texte en français se trouvent tout à la fin du mémoire ; celles des textes en anglais à la fin de chacun d'eux.

la description et la compréhension d'objets pourtant définis de longue date. C'est parfois en regardant ces objets très en détail, comme à la loupe, et dans certaines situations particulières que l'on réussit à mieux les appréhender. Il va de soi que cette démarche ne permet pas de répondre à toutes les questions. Chacun des résultats qui sera présenté a ses limitations, que l'explicitation des objets n'a pas permis de faire disparaître ; chacun utilise, de plus, de grands théorèmes obtenus en observant les choses de beaucoup plus loin. Les deux approches, micro et macroscopique, a-t-on envie de dire, sont de fait complémentaires et il serait certainement aussi vain de vouloir se passer de l'une que de l'autre : qui peut dire qu'une grande vérité ne sortira pas *in fine* d'une question d'abord considérée comme secondaire ?

Les travaux cités ci-dessus auxquels j'ai participé sont reproduits dans ce mémoire. Deux d'entre eux sont encore en préparation et donc difficilement accessibles par ailleurs ([CV13], en voie de soumission, et [Vin13], inachevé) ; l'un est soumis à une revue internationale avec comité de lecture sous une forme légèrement différente ([AV12]) ; les quatre autres sont publiés et accessibles ([PV13], [Vin05], [APV12] et [Vin09]), ils figurent tout de même dans ce mémoire car ils permettent d'évoquer des parties importantes de mon travail. Un autre travail effectué depuis la fin de ma thèse n'est pas reproduit et ne sera guère évoqué ([PV12]) parce qu'il emmènerait dans une direction très différente et plus prisée par mon co-auteur d'alors.

Entrons maintenant un peu plus dans la description des travaux présentés dans ce mémoire. Mon thème de recherche principal est l'étude de **modules galoisiens** dans des extensions de corps de nombres, sous certaines hypothèses concernant en particulier la ramification. Il sera développé dans le chapitre 2 de ce mémoire. Étant donnée une extension galoisienne N/F de corps de nombres, de groupe de Galois G, le module le plus étudié est l'anneau d'entiers $\mathcal{O}_N$ de N comme module sur l'algèbre de groupe $\mathbb{Z}[G]$, où $\mathbb{Z}$ est l'anneau des entiers du corps $\mathbb{Q}$ des rationnels. Son étude a commencé avec Hilbert et a culminé avec la preuve de la conjecture de Fröhlich par M.J. Taylor en 1981 ([Tay81]). D'autres modules ont aussi été étudiés, notamment la codifférente de l'extension et, lorsque cet idéal fractionnaire est un carré, sa racine carrée, dont l'étude a été initiée par Erez dans les années 80 ([Ere88], [Ere91]). Plusieurs auteurs, dont Chase, ont étudié des modules de torsion obtenus notamment en faisant des quotients des précédents ([Cha84]).

Mon apport essentiel concerne l'idéal racine carrée de la codifférente $\mathcal{A}$ lorsque l'extension de corps de nombres est faiblement ramifiée (*i.e.* les seconds groupes de ramification sont triviaux en toute place). Cette hypothèse sur la ramification est la condition nécessaire et suffisante, énoncée par Erez, pour que $\mathcal{A}$ soit un module galoisien localement libre. Résultat qui découle, comme le rappelle Erez [Ere91, §2], des travaux antérieurs d'Ullom sur les idéaux ambiges [Ull69], [Ull70] [2]. Plaçons-nous d'abord dans le cas le plus étudié où l'extension est faiblement ramifiée de degré impair (ce qui assure l'existence de l'idéal $\mathcal{A}$ grâce à la formule de valuation de la différente de Hilbert). On pense alors que $\mathcal{A}$ est un $\mathbb{Z}[G]$-module libre, du fait que l'obstruction à ce que l'anneau d'entiers soit libre lorsqu'il est localement libre n'existe pas en degré impair. Erez a obtenu que $\mathcal{A}$ est $\mathbb{Z}[G]$-libre lorsque l'extension est abélienne absolue ([Ere88]) ou modérée ([Ere91]), en utilisant dans le second cas les puissantes techniques développées par Fröhlich pour décrire le groupe des classes de $\mathbb{Z}[G]$-modules localement libres en termes d'homomorphismes équivariants sur le groupe des caractères virtuels de G ([Frö83]). J'ai étendu ces deux résultats d'Erez : sous l'hypothèse que les groupes de décomposition aux places sauvages sont abéliens, j'ai montré dans ma thèse que $\mathcal{A}$ est $\mathbb{Z}[G]$-libre lorsque l'extension est absolue (*i.e.* le corps de base est le corps des rationnels, [Vin01]) puis, avec E. J. Pickett, lorsque les groupes de ramification sont cycliques et le corps de base est non ramifié sur le corps des rationnels en-dessous des places sauvages ([PV13]).

2. Voir aussi l'introduction du très bel article de Johnston [Joh15]

On peut dans certaines conditions se départir de l'hypothèse d'imparité du degré de l'extension, en supposant seulement l'existence de la racine carrée de la codifférente $\mathcal{A}$: dans un travail en voie de soumission avec Luca Caputo ([CV13]), nous développons une nouvelle méthode passant par l'étude d'un module de torsion *à la Chase* pour traiter le cas des extensions relatives modérées localement abéliennes (ce qui revient à dire que les groupes de décomposition aux places ramifiées sont abéliens), sans restriction sur le degré. Nous montrons que la racine carrée de la codifférente et l'anneau d'entiers ont la même classe dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres (G désigne toujours le groupe de Galois de l'extension) et, grâce au théorème de Taylor pour l'anneau d'entiers évoqué plus haut, nous exhibons un exemple d'extension du corps des rationnels de degré pair pour laquelle la racine carrée de la codifférente existe et n'est pas libre en tant que $\mathbb{Z}[G]$-module.

Le résultat principal de [Vin05] est un peu à part, en ce qu'on ne s'y intéresse pas à la classe de la racine carrée de la codifférente mais à son cube, dont on montre qu'il est trivial si l'extension considérée est une 3-extension faiblement ramifiée de $\mathbb{Q}$. De plus on ne suppose pas ici les groupes de décomposition abéliens ; par contre les hypothèses obligent le groupe de ramification à être abélien 3-élémentaire. Enfin l'approche suivie ne se généralise pas au cas des p-extensions faiblement ramifiées de $\mathbb{Q}$ pour $p > 3$, comme le montrera l'étude combinatoire du chapitre 5.

Le point commun des approches menant à ces nouveaux résultats est qu'elles fournissent des expressions bien plus explicites qu'auparavant des objets à étudier. Ce qui permet notamment, dans [PV13], de montrer qu'avec les bons choix de constantes, les normes-résolvantes et les sommes de Gauss galoisiennes que l'on doit comparer sont en fait égales (alors même qu'on a seulement besoin de prouver que leur rapport est le déterminant de certaines unités) ; dans [CV13], on exhibe les unités correspondant aux différents modules de torsion qu'on étudie, et on constate qu'elles sont des unités cyclotomiques, des sommes de Gauss ou de Jacobi, c'est-à-dire avec une forte signification arithmétique (en particulier elles appartiennent à l'idéal de Stickelberger d'une extension cyclotomique qui apparaît naturellement dans notre étude).

Par ailleurs, ces travaux ont permis de dégager de nouvelles pistes de recherche. Le résultat de la thèse d'Erik Pickett que nous avons utilisé pour notre travail en commun ([Pic09]) faisait intervenir l'exponentielle de Dwork d'une extension non ramifiée d'un corps p-adique. Cette exponentielle, qui intervenait dans la résolvante que nous devions étudier, avait les propriétés adéquates pour mener à bien nos calculs ; cependant elle nous obligeait à faire les hypothèses techniques qui demeurent dans notre résultat principal (groupes de ramification cycliques et corps de base non ramifié aux places sauvages). Ces limitations nous ont poussé à considérer des exponentielles généralisant celle de Dwork, en suivant les techniques développées par Pulita ([Pul07]), et à nous intéresser aux modules différentiels qui leur sont attachés. Nous espérions trouver par ce biais un lien direct entre modules galoisiens et modules différentiels, ce qui n'a finalement pas été le cas. Ce travail a cependant donné lieu à un article actuellement soumis pour publication ([PV12]).

La formalisation du travail avec Luca Caputo a fait apparaître des modules galoisiens qui nous semblent plein d'intérêt. Ils pourraient être reliés à des modules introduits par Burns et Chinburg dans [BC96]. Nous avons l'intention de poursuivre leur étude aussitôt que possible.

Je présente maintenant brièvement les autres thèmes de recherche qui m'ont intéressé et qui sont tous, d'une façon ou d'une autre, en lien avec les précédents.

Construction d'extensions. L'étude de la structure galoisienne de l'idéal racine carrée de la codifférente se fait naturellement dans des extensions galoisiennes de corps de nombres de degré impair faiblement ramifiées (*i.e.* à seconds groupes de ramification triviaux). Il semblait intéressant de disposer d'exemples explicites de telles extensions, au moins sur le corps des rationnels, en demandant de plus qu'elles soient non abéliennes. J'ai exhibé une famille infinie

d'extensions répondant à ces critères dans [Vin02] ; avec Bill Allombert, nous avons construit et étudié une autre telle famille dans notre article soumis pour publication [AV12]. Le caractère très explicite des extensions de cette famille permet de déterminer certaines propriétés de leurs groupes de classes. Les calculs numériques indiquent que des propriétés plus fortes sont satisfaites, nous gardons espoir d'arriver à le démontrer. Ce thème fait l'objet du chapitre 3.

Dans [Vin03], je présentais des calculs numériques de structure galoisienne effectués notamment dans les extensions de la première de ces familles, avec l'aide des logiciels MAGMA et PARI/GP. Ils fournissent des résultats intéressants, en particulier on trouve des extensions pour lesquelles l'idéal racine carrée de la codifférente est $\mathbb{Z}[G]$-libre mais n'admet pas de base normale auto-duale (pour la forme trace).

Corps finis. L'exponentielle de Dwork utilisée par Erik Pickett pour construire une base normale de l'idéal racine carrée de la codifférente dans le cas local produit en fait des bases normales auto-duales. Dans [Pic10], il construit aussi des bases normales auto-duales pour les extensions de corps finis. Celles-ci semblaient pouvoir être utilisées pour optimiser la multiplication dans certains corps finis. En collaboration avec François Arnault, nous avons étudié cette question en développant un algorithme permettant, à partir d'une base construite par la méthode d'Erik, de les calculer toutes et de tester leur efficacité ([APV12]).

Parmi les bases ayant une bonne efficacité, une famille est apparue qui semble provenir de bases de l'idéal racine carrée de la codifférente d'extensions cyclotomiques, décrites et utilisées par Erez dans [Ere88]. Le calcul de la complexité globale des bases de cette famille est un travail en cours, dont nous présentons l'état actuel. Ces questions sont présentées dans le chapitre 4.

Combinatoire. Enfin, mon article [Vin05] faisait intervenir une « combinatoire de puissances de résolvantes » qui marchait bien en degré 3, mais s'est avérée impossible à généraliser en degré (premier) supérieur. De fait la combinatoire en question devient bien plus complexe en degré au moins 5. Cependant son étude a donné lieu à [Vin09], voir le chapitre 5. Le résultat principal de cet article a été généralisé en 2010 par quatre combinatoristes hongrois (Gács, Héger, Nagy, Pálvölgyi), qui ont réinterprété le problème en divers termes, le rattachant à plusieurs questions de combinatoire ([GHNP10]). J'avais moi-même commencé à travailler sur l'interprétation de mon résultat en termes d'hyperplans sur les corps finis, et j'espère toujours tirer quelque chose de ce travail.

Chapitre 2

Éléments explicites en théorie des modules galoisiens

Comme écrit plus haut, on peut faire remonter la théorie des modules galoisiens au moins à David Hilbert, avec un théorème de base normale pour l'anneau d'entiers d'une extension abélienne de $\mathbb{Q}$ de discriminant premier au degré. La situation se complique lorsqu'on essaye de généraliser ce résultat à l'anneau d'entiers $\mathcal{O}_N$ d'une extension N/E de corps de nombres, galoisienne de groupe G, considéré comme $\mathbb{Z}[G]$-module. Une première restriction est établie par Emmy Nœther, qui montre qu'il est localement libre (c'est-à-dire que $\mathcal{O}_N \otimes_{\mathbb{Z}} \mathbb{Z}_p$ est $\mathbb{Z}_p[G]$-libre pour tout nombre premier p) si et seulement si l'extension est modérée. Sous cette condition, nécessaire à l'existence d'une base normale, on peut alors considérer la classe $(\mathcal{O}_N)$ de l'anneau d'entiers dans le groupe des classes (de Grothendieck) de $\mathbb{Z}[G]$-modules localement libres, noté $\mathrm{Cl}(\mathbb{Z}[G])$. Cependant, si la classe d'un module libre est nécessairement triviale, la réciproque n'est pas vraie en général, sauf sous certaines conditions de simplification (absence de caractères symplectiques, par exemple en degré impair).

Pendant la première moitié du XX$^{\text{e}}$ siècle, des résultats probants continuent à être obtenus pour l'anneau d'entiers lui-même, tant qu'on reste dans un cadre où on peut expliciter suffisamment les objets en jeu, notamment celui des extensions abéliennes de $\mathbb{Q}$ pour lesquelles la théorie de Kronecker-Weber fournit une description très pratique. Le critère de Nœther oblige cependant à se limiter aux extensions modérées (théorème de Hilbert-Speiser pour les extensions abéliennes de $\mathbb{Q}$ de conducteur sans facteur carré) ou à considérer la structure de l'anneau d'entiers sur un ordre de $\mathbb{Q}[G]$ plus gros que $\mathbb{Z}[G]$ (théorème de Leopoldt pour les extensions abéliennes de $\mathbb{Q}$).

C'est dans les années 60 que le sujet se transforme et s'étoffe, dans le cas modéré, avec en particulier les travaux d'Albrecht Fröhlich. À partir de calculs sur des extensions quaternioniennes, menés par différents auteurs, Jean-Pierre Serre forge son « idée folle » selon laquelle l'anneau d'entiers d'une extension quaternionienne modérée de $\mathbb{Q}$ n'a pas de base normale exactement quand son nombre d'Artin (*i.e.* la constante de l'équation fonctionnelle de la fonction L de l'extension, étendue aux places infinies) prend la valeur -1 sur le caractère symplectique irréductible du groupe de Galois. Ce lien inattendu et mystérieux est établi peu après par Fröhlich. D'autres résultats et conjectures le poussent à développer une théorie générale susceptible d'en faire la synthèse. Il introduit la Hom-description du groupe des classes, isomorphisme explicite associant à chaque classe une fonction équivariante (sous l'action du groupe de Galois absolu du corps des rationnels) sur les caractères virtuels du groupe de Galois de l'extension, à valeurs dans un groupe d'idèles. Cette description bénéficie de très bonnes propriétés fonctorielles (on en verra des exemples dans les articles reproduits dans ce chapitre), ce qui incite à traiter les extensions modérées de corps de nombres en général, sans se restreindre

au cas absolu.

Dans ce nouveau cadre, c'est la classe de l'anneau d'entiers d'une extension galoisienne modérée de corps de nombres, qu'on tente de rattacher aux valeurs du nombre d'Artin en les caractères symplectiques irréductibles. Philippe Cassou-Noguès associe à celles-ci un invariant dans le groupe des classes et Fröhlich conjecture qu'il est égal à la classe de l'anneau d'entiers. Martin Taylor prouve cette conjecture dans [Tay81].

L'histoire ne s'arrête pas là. Ted Chinburg introduit dans [Chi85] de nouveaux invariants, plus délicats à manier. Il prouve que son invariant Ω_2 est égal à la classe de l'anneau d'entiers dans $\mathrm{Cl}(\mathbb{Z}[G])$ dans le cas modéré ; conjecture que l'invariant Ω_3 est égal à celui de Cassou-Noguès–Fröhlich (la définition de l'invariant de Cassou-Noguès a été étendue par Fröhlich au cas des extensions sauvagement ramifiées) en général ; se demande s'il en va de même pour Ω_2. Ces invariants très riches rendent compte à la fois de la structure additive et de la structure multiplicative de l'anneau d'entiers. Il a cependant semblé utile de les réinterpréter dans un cadre plus vaste, englobant aussi les conjectures de Stark et du « lifted root number », celui de la conjecture équivariante des nombres de Tamagawa ([BF01]). Des résultats ont été obtenus dans ce cadre très général, notamment [BG03].

D'autres modules sont introduits et étudiés, notamment par Stephen Chase (voir Section 2.2) et par Boas Erez, qui travaille sur l'idéal (fractionnaire) racine carrée de la codifférente, en degré impair (cette condition assure son existence par la formule de valuation de la différente de Hilbert). Il prouve un critère analogue à celui de Nœther pour l'anneau d'entiers : la racine carrée de la codifférente d'une extension galoisienne de corps de nombres est localement libre si et seulement si l'extension est faiblement ramifiée, c'est-à-dire si ses deuxièmes groupes de ramification sont triviaux en toute place. Dans la mesure où une extension galoisienne est modérément ramifiée si et seulement si ses premiers groupes de ramification sont triviaux en toute place, on voit que la situation est très similaire à celle de l'anneau d'entiers, même si l'introduction d'« un peu » de ramification sauvage complique les choses. Erez prouve aussi, notamment, que la racine carrée de la codifférente d'une extension galoisienne modérée de degré impair, de groupe de Galois G, est $\mathbb{Z}[G]$-libre.

En parallèle à ces travaux et à la suite de Leon Mc Culloh [McC87], se pose la question des classes réalisables : un corps de nombres E et un groupe fini G étant fixés, quels sont les éléments du groupe $\mathrm{Cl}(\mathcal{O}_E[G])$ des classes de $\mathcal{O}_E[G]$-modules localement libres qui peuvent être réalisés par l'anneau d'entiers d'une extension galoisienne modérée de E de groupe de Galois isomorphe à G ? L'ensemble de ces classes forme-t-il un sous-groupe ? Lorsque $E = \mathbb{Q}$, l'étude évoquée ci-dessus de la $\mathbb{Z}[G]$-structure de l'anneau d'entiers permet de donner une réponse assez complète. Pour $E \neq \mathbb{Q}$ et G abélien, Mc Culloh caractérise les classes réalisables et en déduit que leur ensemble est un sous-groupe de $\mathrm{Cl}(\mathcal{O}_E[G])$. Des résultats similaires concernant différents groupes non abéliens ont été obtenus depuis, notamment [BGS06] qui traite une infinité de produits semi-directs d'un certain type (en remplaçant $\mathcal{O}_E[G]$ par un ordre maximal cependant). Dans [Bur95], David Burns étudie un problème similaire, consistant à comparer l'ensemble des classes réalisées par les anneaux d'entiers d'extensions galoisiennes modérées de E de groupe de Galois isomorphe à G et par les idéaux ambiges de telles extensions. Son résultat principal suppose que E soit absolument non ramifiée aux diviseurs premiers de l'ordre de G.

Les articles présentés dans ce chapitre, écrits en collaboration avec Erik Pickett pour le premier, Luca Caputo pour le second, seul pour le troisième (dans l'ordre de présentation), s'intéressent tous à la structure galoisienne de la racine carrée de la codifférente, dans des cadres et avec des techniques assez différents. Si l'incontournable Hom-description du groupe des classes de Fröhlich est utilisée dans tous les cas, elle ne l'est pas tout à fait de la même manière. Pour préciser les choses, rappelons que cet isomorphisme de groupes est livré avec une

« recette » permettant d'associer à chaque classe, de façon non canonique, une fonction équivariante sur les caractères virtuels du groupe de Galois de l'extension, sous forme de rapport entre des normes-résolvantes (semi-)locales et une norme-résolvante globale. Cette dernière est souvent avantageusement remplacée par une somme de Gauss galoisienne (dans [Tay81], [Ere91],...), c'est aussi le cas dans le premier article présenté ci-dessous, dont l'originalité est plutôt dans l'explicitation de tous les objets à étudier, et dans le troisième où elle disparaît du fait que l'on y étudie une puissance adéquate de la classe de la racine carrée de la codifférente. Dans le second article présenté, par contre, on suit scrupuleusement la recette *de base* de Fröhlich, sans faire la substitution par la somme de Gauss galoisienne ; en poussant l'analyse des représentants obtenus, on voit alors apparaître, selon les cas, des unités cyclotomiques ou, via le théorème de Stickelberger, des sommes de Gauss ou de Jacobi classiques (non galoisiennes). Les propriétés de ces éléments permettent alors de conclure. Pour ce qui est du cadre, les deux premiers articles présentés considèrent des extensions localement abéliennes, faiblement ramifiées pour le premier, modérément pour le second, tandis que le troisième se place dans le cas de 3-extensions faiblement ramifiés absolues.

Dans les trois sections suivantes, une présentation succinte de chaque article précède sa reproduction. On retrouvera une allusion à l'invariant de Chinburg en Section 2.2, ainsi qu'un lien avec le problème des classes réalisables.

2.1 Bases normales auto-duales et structure galoisienne

Le titre de cette section est la traduction en français de l'article *Self-dual integral normal bases and Galois module structure*, écrit en collaboration avec Erik Pickett et publié dans le journal Compositio Mathematica (volume **149**, année 2013, numéro 7, pages 1175-1202). Il reflète l'idée de base de notre travail, suggérée par Philippe Cassou-Noguès, qui était de mettre en commun les résultats principaux de nos deux thèses. Pour Erik, il s'agissait de la construction de bases normales auto-duales de la racine carrée de la codifférente d'une extension abélienne faiblement ramifiée d'un corps p-adique non ramifié sur $\mathbb{Q}_p$ (étant donné un premier impair p), voir [Pic09]. De mon côté j'avais pu établir que, dans les extensions galoisiennes faiblement ramifiées de $\mathbb{Q}$ qui sont abéliennes aux places sauvages, la racine carrée de la codifférente est libre en tant que module galoisien, voir [Vin01].

Via la Hom-description de Fröhlich, cette question globale peut être traitée localement et se ramène à étudier la racine carrée de la codifférente d'extensions faiblement ramifiées abéliennes de $\mathbb{Q}_p$, où p est un premier impair. Ces extensions sont faciles à décrire en utilisant la théorie de Kronecker-Weber, et leur racine carrée de la codifférente possède un générateur de base normale très explicite, connu depuis les premiers travaux d'Erez sur le sujet [Ere88]. *A priori*, il devait être possible de généraliser ce résultat aux extensions relatives de corps de nombres (faiblement ramifiées et abéliennes aux places sauvages) en remplaçant la théorie de Kronecker-Weber par celle de Lubin-Tate (déjà à l'œuvre dans la thèse d'Erik) et le générateur de base normale d'Erez par celui d'Erik. L'idée était alléchante et c'est ce que nous avons essayé de faire... et réussi plus ou moins après beaucoup d'efforts !

Dans la pratique, les difficultés liées au passage au cas relatif ont été très nombreuses. L'une d'elles, mais pas la pire, était que je ne m'étais familiarisé avec la Hom-description que dans le cas absolu, et n'avais pas tout à fait mesuré l'étendue des changements qu'apportait le cas relatif ; même si cela a causé quelque retard dans la parution de l'article, il a été possible de résoudre ce problème d'une façon assez satisfaisante (notamment en introduisant la modification aux places faiblement ramifiées des sommes de Gauss galoisiennes, voir la Section 3.2 de l'article ci-dessous). Une autre difficulté, plus sérieuse, est que la construction de bases normales auto-duales d'Erik, à l'aide de l'exponentielle de Dwork, ne marchait que pour une extension

faiblement ramifiée de degré p (donc cyclique) d'un corps p-adique non ramifié sur $\mathbb{Q}_p$. Ce qui explique que notre résultat global ([PV13, Theorem 1]) comporte certaines restrictions techniques, malgré nos nombreux efforts (tous vains jusqu'à présent) pour les éliminer.

Nous avons en particulier longuement essayé de construire une base normale pour la racine carrée de la codifférente de l'extension faiblement ramifiée abélienne maximale de notre corps de base contenue dans une tour de Lubin-Tate fixée (c'est une extension de degré p^f si f est le degré du corps de base sur $\mathbb{Q}_p$; c'est aussi la p-sous-extension de l'extension « de niveau 2 » de la tour de Lubin-Tate, celle « de niveau 1 » étant modérée). Il semble d'après une prépublication d'Erik et de Lara Thomas ([PT13]) que cela soit possible en faisant intervenir des « exponentielles de groupes formels » qui, malheureusement, risquent d'être difficiles à manipuler pour les calculs de normes ou de résolvantes… Une possibilité qui n'a pas été complètement explorée serait de mieux utiliser la structure combinatoire de l'extension faiblement ramifiée abélienne maximale évoquée ci-dessus : son groupe de Galois est isomorphe au produit direct de $\mathbb{Z}/p\mathbb{Z}$, f fois avec lui-même, elle est donc égale au compositum de ses sous-extensions de degré p (pour lesquelles le résultat est acquis). Pour l'instant on ne sait pas utiliser cette propriété.

Nos efforts ont tout de même payé puisque nous avons finalement obtenu le résultat souhaité, malgré quelques restrictions techniques, et même mieux : l'étude locale que nous avons menée nous a permis de prouver l'égalité de la norme-résolvante et de la somme de Gauss galoisienne que nous devions comparer. Il nous suffisait de montrer que leur rapport s'exprimait en fonction d'unités de certaines algèbres de groupes et nous avons pu établir qu'il valait 1, sous réserve que l'on fasse les bons choix dans les définitions assez souples de ces objets. Ce résultat pourrait paraître anecdotique, si l'on oublie que la comparaison d'une résolvante et d'une somme de Gauss est au cœur de la théorie des modules galoisiens, au moins depuis l'introduction de la Hom-description de Fröhlich, en tout cas dans la preuve par Taylor de la conjecture de celui-ci ([Tay81]). On présente souvent cette comparaison comme la confrontation de deux mondes mathématiques, la résolvante étant de nature algébrique tandis que la somme de Gauss galoisienne, qui provient de l'équation fonctionnelle de la fonction L d'Artin, est de nature analytique. Dans ce contexte il est intéressant de noter que nous ne sommes parvenus à l'égalité de ces représentants de deux mondes, dans notre cadre, que grâce à l'expression à l'aide de l'exponentielle de Dwork d'un générateur de base normale de la racine carrée de la codifférente (générateur sur lequel est bâtie la résolvante), c'est-à-dire en rendant analytique celui des deux qui était jusqu'alors entièrement algébrique. En passant on peut se demander si le lien ainsi établi entre l'exponentielle de Dwork et la fonction L d'Artin a d'autres conséquences…

Self-Dual Integral Normal Bases and Galois Module Structure

Erik Jarl Pickett and Stéphane Vinatier

Abstract

Let N/F be an odd degree Galois extension of number fields with Galois group G and rings of integers $\mathfrak{O}_N$ and $\mathfrak{O}_F = \mathfrak{O}$ respectively. Let $\mathcal{A}$ be the unique fractional $\mathfrak{O}_N$-ideal with square equal to the inverse different of N/F. Erez has shown that $\mathcal{A}$ is a locally free $\mathfrak{O}[G]$-module if and only if N/F is a so called weakly ramified extension. There have been a number of results regarding the freeness of $\mathcal{A}$ as a $\mathbb{Z}[G]$-module, however this question remains open. In this paper we prove that $\mathcal{A}$ is free as a $\mathbb{Z}[G]$-module assuming that N/F is weakly ramified and under the hypothesis that for every prime $\wp$ of $\mathfrak{O}$ which ramifies wildly in N/F, the decomposition group is abelian, the ramification group is cyclic and $\wp$ is unramified in $F/\mathbb{Q}$.

We make crucial use of a construction due to the first named author which uses Dwork's exponential power series to describe self-dual integral normal bases in Lubin-Tate extensions of local fields. This yields a new and striking relationship between the local norm-resolvent and Galois Gauss sum involved. Our results generalise work of the second named author concerning the case of base field $\mathbb{Q}$.

1. Introduction

Let N/F denote an odd degree Galois extension of number fields. By Hilbert's formula for the valuation of the different $\mathfrak{D}$ of N/F, there exists a fractional ideal $\mathcal{A}$ $(= \mathcal{A}_{N/F})$ of the ring of integers $\mathfrak{O}$ $(= \mathfrak{O}_F)$ of F such that:

$$\mathcal{A}^2 = \mathfrak{D}^{-1} \ .$$

This ideal is known as the *square root of the inverse different*. It is an ambiguous ideal, namely it is stable under the action of the Galois group G of N/F and hence an $\mathfrak{O}[G]$-module. Erez has shown $\mathcal{A}$ to be locally free if and only if N/F is weakly ramified, *i.e.*, if the second ramification group of any prime ideal $\mathfrak{p}$ of $\mathfrak{O}_N$ is trivial. The study of $\mathcal{A}$ as an $\mathfrak{O}[G]$-module has too many obstructions to be dealt with (in particular $\mathfrak{O}$ may not be principal), so after Fröhlich, Taylor, *et al.* (for the Galois module structure of the ring of integers in a tame extension), we consider the structure of $\mathcal{A}$ as a $\mathbb{Z}[G]$-module.

In [Ere91] Erez proves that when N/F is tamely ramified, then $\mathcal{A}$ is always free over $\mathbb{Z}[G]$. The question of whether $\mathcal{A}$ is free as a $\mathbb{Z}[G]$-module when N/F is wildly but weakly ramified is still open. In this paper we prove the following global result.

Theorem 1. *Let N/F denote an odd degree weakly ramified Galois extension of number fields and suppose that, for any wildly ramified prime $\mathfrak{p}$ of $\mathfrak{O}_N$, the decomposition group is abelian, the ramification group is*

2000 Mathematics Subject Classification 11R04, 11R33, 11S31 (primary), 11R20, 11R29, 11R32, 11S15, 11S20, 11S80 (secondary).
Keywords: Galois module, square-root of the inverse different, weakly ramified extensions, Dwork's power series, self-dual integral normal basis, Galois Gauss sum

cyclic and the localised extension $F_\wp/\mathbb{Q}_p$ is unramified — where $\wp = \mathfrak{p} \cap F$ and $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. Then $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module.

This result generalises [Vin01, théorème 1.2], which is the natural analogue in the absolute case $F = \mathbb{Q}$. In that case, ramification groups at wildly ramified places are always cyclic of prime order. In the relative case, we will see that the abelian decomposition group assumption yields that the ramification group is p-elementary abelian at a wildly ramified place above a rational prime p. Therefore, our hypothesis about ramification groups at wildly ramified places really mimics the situation in the absolute case.

As in Taylor's celebrated theorem for rings of integers in tame extensions of number fields [Tay81, Theorem 1], our result indicates a deep connection between two kinds of invariants of the extension N/F: the Galois Gauss sum, of analytic nature, that emerges in the constant of the functional equation of the Artin L-function of F; and the norm-resolvents attached to semi-local normal basis generators of $\mathcal{A}$, that are entirely of algebraic nature *a priori*.

Generalising the link between these objects to the relative situation has been made possible by the exhibition by the first named author in [Pic09] of explicit normal basis generators for cyclic weakly ramified extensions of an unramified extension of $\mathbb{Q}_p$. These generators are constructed using values of Dwork's p-adic exponential power series at certain units and have very nice properties — in particular they are self-dual with respect to the trace form. Of course, the norm-resolvents we attach to them can no longer be thought of as completely algebraic in nature.

Dwork originally introduced his power series in the context of p-adic differential operators, when considering the zeta function of a hypersurface [Dwo64]. In this paper we demonstrate that Dwork's power series is extremely useful when considering Galois module structure in extensions of both local and number fields. We hope that this work will lead to the further investigation of the connections between these two subject areas.

The core of this paper is Section 4, where we use the rich properties of Pickett's basis generators to compute the product of a norm-resolvent with a modified twisted Galois Gauss sum in local cyclic wildly and weakly ramified extensions. We obtain the following local result (the objects will be defined below).

THEOREM 2. *Let $p \neq 2$ be a rational prime, K an unramified finite extension of $\mathbb{Q}_p$, M a cyclic wildly and weakly ramified extension of K such that p belongs to the norm group of M/K. There exist a normal basis generator α_M of the square root of the inverse different of M/K and choices in the definitions of the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid .)$ and of the modified Galois Gauss sum $\tau_K^\star$ such that, for any character χ of* $\mathrm{Gal}(M/K)$*:*

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi)\tau_K^\star(\chi - \psi_2(\chi)) = 1 \ ,$$

where ψ_2 is the second Adams operator.

Before proving this result in Section 4, we introduce the technical tools for our study in Section 2. Then in Section 3 we give some preliminary results and explain how to reduce the proof of Theorem 1 to that of Theorem 2.

We hope to deal with the general relative abelian case in a future publication, but we have no explicit description of a normal basis generator which lends itself so well to calculations of the type used in this paper — see [Pic09, Remark 13(2)] and [Pic10, Introduction]. We are therefore not able to generalise the explicit computations of Section 4 at this stage.

Throughout this paper, N/F is an odd degree weakly ramified extension of number fields with Galois group G.

Aknowledgments. The authors would like to express their deep gratitude to Philippe Cassou-Noguès and Martin J. Taylor, for many useful comments and suggestions; specifically Philippe Cassou-Noguès pointed out an embarrassing misuse of Fröhlich's Hom-description in the first version of this paper, and helped solve the problem. They also thank Régis Blache for an enlightening discussion about p-adic analysis, and the anonymous referee for his very careful reading of the manuscript.

2. Strategy

In this section, we first explain briefly how Fröhlich's Hom-description translates the problem of showing that $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module into the study of an equivariant morphism on the group of virtual characters of G, with idelic values. For each rational prime p, the local components above p of this morphism decompose as a product of factors indexed by the prime ideals of $\mathfrak{O}$. We recall from the literature the properties we need about these factors, except for the $\wp$-factors of the p-component when $\wp \mid p$ is wildly ramified in N/F; this will be dealt with in Sections 3 and 4.

We first fix some notations for the paper.

NOTATION 2.1. *We let $\mathbb{Q}^c$ denote the algebraic closure in the field of complex numbers of the field $\mathbb{Q}$ of rational numbers; for any rational prime p we fix an algebraic closure $\mathbb{Q}_p^c$ of the field of p-adic numbers $\mathbb{Q}_p$. Any number field (resp. finite extension of $\mathbb{Q}_p$) L we consider is assumed to be contained in $\mathbb{Q}^c$ (resp. $\mathbb{Q}_p^c$), and we set $\Omega_L = \mathrm{Gal}(\mathbb{Q}^c/L)$ (resp. $\Omega_L = \mathrm{Gal}(\mathbb{Q}_p^c/L)$); we let L^{ab} be the maximal abelian extension of L in $\mathbb{Q}^c$ (resp. $\mathbb{Q}_p^c$) and denote $\mathrm{Gal}(L^{ab}/L)$ as Ω_L^{ab}.*

When L is a number field, we denote by $\mathfrak{O}_L$ its ring of integers and, if $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_L$, by $L_\mathfrak{p}$ the completion (also called the "localisation") of L at $\mathfrak{p}$. When L is a finite extension of $\mathbb{Q}_p$, we denote by $\mathfrak{O}_L$ the valuation ring of L and by θ_L the Artin reciprocity map $L^\times \to \Omega_L^{ab}$.

2.1 The class group

To prove Theorem 1 we use the classic strategy developed by Fröhlich. We associate to the $\mathbb{Z}[G]$-module $\mathcal{A}$, its class $(\mathcal{A})$ in the class group of locally free $\mathbb{Z}[G]$-modules $\mathrm{Cl}(\mathbb{Z}[G])$. Since the order of G is odd, the triviality of the class $(\mathcal{A})$ is equivalent to $\mathcal{A}$ being free as a $\mathbb{Z}[G]$-module, which is our goal. Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$ reads:

$$\mathrm{Cl}(\mathbb{Z}[G]) \cong \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)\,\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))} \quad .$$

Here R_G is the additive group of virtual characters of G with values in $\mathbb{Q}^c$, E is a "big enough" number field (in particular E is Galois over $\mathbb{Q}$, contains N and the values of the elements of R_G) and $J(E)$ is its idèle group. The homomorphisms in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$ are those which commute with the natural actions of $\Omega_\mathbb{Q}$ on R_G and $J(E)$. The group $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)$ embeds in the former one through the diagonal embedding of $E^\times$ in $J(E)$, and $\mathcal{U}(\mathbb{Z}[G]) = \mathbb{R}[G]^\times \times \prod_l \mathbb{Z}_l[G]^\times$, with l running over all rational primes. We now briefly define the Det morphism, as well as local and semi-local resolvents and norm-resolvents. For a more complete account of Fröhlich's Hom-description, see [Frö83].

2.2 Determinants and resolvents

Let B/A be a finite Galois extension of number fields, let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_B$ and set $\wp = \mathfrak{p} \cap A$. In the following, the symbols K, L, H, $\mathbb{Q}_*$ and R may have two different meanings corresponding

respectively to the semi-local and local situations:

K	L	H	$\mathbb{Q}_*$	R
A	$B \otimes_A A_\wp$	$\mathrm{Gal}(B/A)$	$\mathbb{Q}$	R_H
$A_\wp$	$B_\mathfrak{p}$	$\mathrm{Gal}(B_\mathfrak{p}/A_\wp)$	$\mathbb{Q}_p$	$R_{H,p}$

In the table, we have denoted by $R_{H,p}$ the group of virtual characters of H with values in $\mathbb{Q}_p^c$. Let χ be the character of an irreducible matrix representation Θ of H and $x = \sum_{h\in H} x_h h \in L[H]$, then

$$\mathrm{Det}_\chi(x) = det\Big(\sum_{h\in H} x_h \Theta(h)\Big) \ ,$$

where det stands for the matrix determinant. Extending this formula by linearity to any $\chi \in R$ yields the morphism

$$\mathrm{Det} : L[H]^\times \longrightarrow \mathrm{Hom}\left(R, (\mathbb{Q}_*^c)^\times\right) \ .$$

The restriction of Det_χ to H yields an abelian character of H that we denote by $\det_\chi$. It can be extended to Ω_K by letting $\det_\chi(\omega) = \det_\chi(\omega|_L)$ for any $\omega \in \Omega_K$.

In order to find a representative character function of the image of $(\mathcal{A})$ under the Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$, one needs to consider resolvents and norm-resolvents.

Definition 2.2. *Let $\alpha \in L$ and $\chi \in R$. The resolvent, and respectively the norm-resolvent, of α at χ with respect to L/K are defined as*

$$(\alpha \,|\, \chi) = (\alpha \,|\, \chi)_H = \mathrm{Det}_\chi\left(\sum_{h\in H} \alpha^h h^{-1}\right) \ , \quad \mathcal{N}_{K/\mathbb{Q}_*}(\alpha \,|\, \chi) = \prod_{\omega\in\Omega} (\alpha \,|\, \chi^{\omega^{-1}})^\omega$$

where the product is over a (right) transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_*}$.

Notice that the norm-resolvent depends on the choice of the right transversal Ω. In view of [Frö83, Prop. I.4.4(ii)], changing Ω multiplies the norm-resolvent by $\det_\chi(h)$ for some $h \in H$, namely by an element in the denominator of the Hom-description. It follows that when using norm-resolvents to describe a representative function for $(\mathcal{A})$, we may choose Ω freely. When $K/\mathbb{Q}_p$ is Galois (in the local context), restriction of $\mathbb{Q}_p$-automorphisms to K maps any such Ω onto $\mathrm{Gal}(K/\mathbb{Q}_p)$. When H is abelian, the formulas simplify to:

$$(\alpha \,|\, \chi) = \sum_{h\in H} \alpha^h \chi(h^{-1}) \ , \quad \mathcal{N}_{K/\mathbb{Q}_*}(\alpha \,|\, \chi) = \prod_{\omega\in\Omega} \left(\sum_{h\in H} \alpha^{h\omega} \chi(h^{-1})\right) \ .$$

2.3 A representative for $(\mathcal{A})$

We now describe a representative f of $(\mathcal{A})$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$. Such a representative is not unique since it can be modified by multiplication by any element in the denominator of the Hom-description. Indeed we construct f by slightly modifying Erez's representative $v_{N/F}$ [Ere91, Theorem 3.6], in order to enable more precise computations at wildly ramified places — the goal being to show that f itself lies in the denominator of the Hom-description.

We define the representative morphism f of $(\mathcal{A})$ by giving, for each rational prime p, its semi-local component f_p taking values in $J_p(E) = \prod_{\mathcal{P}|p} E_\mathcal{P}^\times$, where the product is over the prime ideals of $\mathfrak{O}_E$ above p. This group embeds in $J(E)$ as the subgroup consisting of the idèles $(y_\mathcal{P})_\mathcal{P} \in J(E)$ such that $y_\mathcal{P} = 1$ if $\mathcal{P}$ is a prime ideal of $\mathfrak{O}_E$ that does not divide p. It decomposes into the cartesian product $J_p(E) = \prod_{\wp|p} J_\wp(E)$, where the product is over the prime ideals $\wp$ of $\mathfrak{O}$ above p, and

$J_\wp(E) = \prod_{\mathcal{P}|\wp} E_\mathcal{P}^\times$. Note that, with similar definitions at a lower level, $J_\wp(F) = F_\wp^\times$ diagonally embeds into $J_\wp(E)$ and $J_\wp(N)$ embeds into $J_\wp(E)$ by the map $(x_\mathfrak{p})_{\mathfrak{p}|\wp} \mapsto (y_\mathcal{P})_{\mathcal{P}|\wp}$, such that $y_\mathcal{P} = x_\mathfrak{p}$ if $\mathcal{P}|\mathfrak{p}$.

Furthermore $J_\wp(E)$ is isomorphic to $(E \otimes_F F_\wp)^\times$ via the isomorphism

$$\mathcal{I}_\wp = \prod_\iota (\iota \otimes 1) : (E \otimes_F F_\wp)^\times \xrightarrow{\sim} J_\wp(E) \ ,$$

built on the various embeddings ι of E in $\mathbb{Q}_p^c$ that fix $\wp$. These embeddings are in one-to-one correspondence with the prime ideals of $\mathfrak{O}_E$ above $\wp$. We may not always distinguish between $J_\wp(E)$ and $(E \otimes_F F_\wp)^\times$ in the following.

First consider the case where p is a rational prime that does not divide the order of G. Under this assumption, $\mathbb{Z}_p[G]$ is a maximal order in $\mathbb{Q}_p[G]$, which by [Frö83, Prop. I.2.2] implies

$$\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, \mathcal{U}_p(E)) = \mathrm{Det}(\mathbb{Z}_p[G]^\times) \ ,$$

where $\mathcal{U}_p(E) = \prod_{\mathcal{P}|p} \mathfrak{O}_{E_\mathcal{P}}^\times$. On the other hand, Erez has shown that his representative $v_{N/F}$ takes values in $\mathcal{U}(E) = \prod_\mathcal{P} \mathfrak{O}_{E_\mathcal{P}}^\times$ [Ere91, Theorem 2′]. It follows that $(v_{N/F})_p$ belongs to the p-component of the denominator of the Hom-description, hence we may set $f_p = 1$. Similar arguments show that we may also set $f_\infty = 1$, where ∞ stands for the archimedean place of $\mathbb{Q}$.

From now on we suppose p is a rational prime dividing the order of G. The p-component f_p of our representative f is essentially made of two ingredients: the global Galois Gauss sum of F and norm-resolvents associated to semi-local generators of $\mathcal{A}$.

2.3.1 *Norm-resolvents.* We begin with the latter ingredient. Since N/F is weakly ramified, we know by Erez's criterion [Ere91, Theorem 1] that the square root of the inverse different $\mathcal{A}$ is locally free. Specifically, for each prime ideal $\wp$ of $\mathfrak{O}$ above p, there exists $\beta_\wp \in N \otimes_F F_\wp$ such that $\mathcal{A} \otimes_\mathfrak{O} \mathfrak{O}_{F_\wp} = \mathfrak{O}_{F_\wp}[G]\beta_\wp$. The semi-local resolvent $(\beta_\wp \,|\, \chi)$, for $\chi \in R_G$, takes values in $(E \otimes_F F_\wp)^\times$, identified with $J_\wp(E)$ through isomorphism $\mathcal{I}_\wp$, then embedded in $J(E)$. The norm-resolvent is then obtained as

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi) = \prod_{\omega \in \Omega} (\beta_\wp \,|\, \chi^{\omega^{-1}})^\omega \ ,$$

where the product is over a (right) transversal Ω of Ω_F in $\Omega_\mathbb{Q}$. The action of Ω on $J(E)$ permutes the semi-local subgroups $J_\wp(E)$ corresponding to prime ideals $\wp$ of $\mathfrak{O}$ above p, hence the norm-resolvent $\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)$ takes values in $J_p(E)$; if $\mathcal{Q}$ denotes any prime ideal of $\mathfrak{O}_E$ above p, we denote by $\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)_\mathcal{Q}$ its component in $E_\mathcal{Q}^\times$. Accordingly, we denote by β_p the idèle in $J_p(N)$ whose components in the subgroups $J_\wp(N)$, where $\wp$ is above p, are the $\beta_\wp$ introduced above. The norm-resolvent $\mathcal{N}_{F/\mathbb{Q}}(\beta_p \,|\, \chi)$ belongs to $J_p(E) = \prod_{\mathcal{Q}|p} E_\mathcal{Q}^\times$, with $\mathcal{Q}$-component:

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_p \,|\, \chi)_\mathcal{Q} = \prod_{\wp|p} \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)_\mathcal{Q} \ .$$

2.3.2 *Galois Gauss sums.* We now turn to the global Galois Gauss sum, which is a product of local ones. For each prime ideal ℓ of $\mathfrak{O}$, we fix a prime ideal $\mathcal{L}$ of E above ℓ and we set $\mathfrak{l} = \mathcal{L} \cap N$, $l\mathbb{Z} = \mathcal{L} \cap \mathbb{Q}$. Recall the one-to-one correspondence between prime ideals of $\mathfrak{O}_E$ above ℓ and embeddings of E into $\mathbb{Q}_l^c$ that fix ℓ, and let $\iota_{\mathcal{L}/\ell}$ denote the embedding associated to $\mathcal{L}$. It induces an isomorphism between the Galois group of the local extension $N_\mathfrak{l}/F_\ell$ and the decomposition group $G(\ell)$ of $\mathcal{L}/\ell$, sending $\gamma \in$

$\mathrm{Gal}(N_\mathfrak{l}/F_\ell)$ to $\iota_{\mathcal{L}/\ell}\,\gamma\,\iota_{\mathcal{L}/\ell}^{-1} \in \mathrm{Gal}(N/F)$ (the action on elements is written exponentially, thus to the right, see [Frö83, III (2.7)]). We may thus identify $G(\ell)$ and $\mathrm{Gal}(N_\mathfrak{l}/F_\ell)$ in the following.

In Subsection 3.2 we define the local Galois Gauss sum $\tau_{F_\ell}(\chi)$ when $\chi \in R_{G(\ell)}$ is abelian and at most weakly ramified — for a general definition of the Galois Gauss sum see for instance [Frö83, I.5]. We also recall how this Galois Gauss sum is modified at (at most) tamely ramified places, and present an analogous modification at wildly and weakly ramified places. We denote in both cases[1] the resulting character function by $\tau^\star_{F_\ell}$. Following Erez [Ere91, §3], we finally twist our modified Galois Gauss sum using the action of the second Adams operator ψ_2 and get:

$$T^\star_\ell(\chi) = \tau^\star_{F_\ell}\big(\chi - \psi_2(\chi)\big) \ .$$

Set $\widetilde{T}^\star_\ell = \mathrm{Ind}_{G(\ell)}^G T^\star_\ell$, namely, by definition of induction on character functions:

$$\widetilde{T}^\star_\ell(\chi) = T^\star_\ell(\chi_\ell) = \tau^\star_{F_\ell}\big(\chi_\ell - \psi_2(\chi_\ell)\big) \ ,$$

where for $\chi \in R_G$, we let χ_ℓ denote the restriction of χ to $G(\ell)$.

We now have for each prime ideal ℓ of $\mathfrak{O}$ a function $\widetilde{T}^\star_\ell$ on virtual characters of G. We shall see in Subsection 3.2.3 that it is in fact almost always trivial: Equation (7) shows that $\widetilde{T}^\star_\ell = 1$ whenever ℓ is unramified in N/F. Let S_T and S_W be the sets of prime ideals of $\mathfrak{O}$ that are respectively tamely and wildly ramified in N/F; their union S contains all the prime ideals ℓ of $\mathfrak{O}$ such that $\widetilde{T}^\star_\ell$ is non trivial, and we define the global twisted modified Galois Gauss sum associated to F as:

$$T^\star = \prod_{\ell\in S} \widetilde{T}^\star_\ell \quad \in \mathrm{Hom}(R_G, E^\times) \ .$$

It takes values in $E^\times$, which diagonally embeds into $J(E)$, henceforth into each $J_p(E)$.

2.3.3 *All together.* We will prove the following result in Subsection 3.2.3.

Proposition 2.3. *For any rational prime p and for $\chi \in R_G$ set:*

$$f_p(\chi) = T^\star(\chi)\mathcal{N}_{F/\mathbb{Q}}(\beta_p \,|\, \chi) = T^\star(\chi)\prod_{\wp|p}\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)$$

if p divides the order of G, $f_p(\chi) = 1$ otherwise; furthermore set $f_\infty = 1$. Then $f = (f_p)_p$ is a representative of $(\mathcal{A})$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$.

2.4 Localising and cutting into pieces

We fix a rational prime p dividing the order of G. The $\Omega_\mathbb{Q}$-equivariant component f_p of our representative takes semi-local values. We first transform it into a character function with local values, that we then cut into factors that will be dealt with separately.

We use the localisation procedure described in [Frö83, II.2 & III.2]. Let $\mathcal{Q}$ be a prime ideal of $\mathfrak{O}_E$ above p. The associated embedding $\iota = \iota_{\mathcal{Q}/p}$ embeds E into $E_\mathcal{Q} \subset \mathbb{Q}_p^c$. It gives rise to a homomorphism $E\otimes_\mathbb{Q}\mathbb{Q}_p \to E_\mathcal{Q}$, again denoted by ι, and to an isomorphism $\chi \mapsto \chi^\iota$, of R_G onto $R_{G,p}$, the ring of virtual characters of G with values in $\mathbb{Q}_p^c$. We know by [Frö83, Lemma II.2.1] that it yields an isomorphism:

$$\iota^* : \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J_p(E)) \xrightarrow{\sim} \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_\mathcal{Q}^\times) \ , \tag{1}$$

defined by $\iota^*(v)(\theta) = v(\theta^{\iota^{-1}})^\iota$, and such that

$$\iota^*\big(\mathrm{Det}(\mathbb{Z}_p[G]^\times)\big) = \mathrm{Det}(\mathbb{Z}_p[G]^\times) \ , \tag{2}$$

[1] When dealing with a tamely ramified place, we also use the standard notation $\tau^*_{F_\ell}$ (note the different star in exponent).

where the left hand side Det group takes semi-local values (on characters with values in $\mathbb{Q}^c$) whereas the right hand side takes local values (on characters with values in $\mathbb{Q}_p^c$). However the ambiguity of the notation should not be a problem thanks to this isomorphism.

We now compute $\iota^*(f_p)$. Let $\theta \in R_{G,p}$ and set $\chi = \theta^{\iota^{-1}}$, then

$$\iota^*(f_p)(\theta) = \prod_{\ell \in S} T_\ell^\star(\chi_\ell)^\iota \prod_{\wp \mid p} \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)^\iota \ .$$

For each $\ell \in S$ we let $\mathcal{T}_\ell^\star \in \mathrm{Hom}(R_{G(\ell),p}, E_\mathcal{Q}^\times)$ be such that, for $\phi \in R_{G(\ell),p}$:

$$\mathcal{T}_\ell^\star(\phi) = T_\ell^\star\big(\phi^{\iota^{-1}}\big)^\iota \ ,$$

then $T_\ell^\star(\chi_\ell)^\iota = \mathcal{T}_\ell^\star(\theta_\ell)$, since $\iota : R_G \hookrightarrow R_{G,p}$ commutes with restriction of characters to $G(\ell)$.

Recall from Subsection 2.3.2 that we have fixed a prime ideal $\mathcal{P}$ of $\mathfrak{O}_E$ above each prime ideal $\wp$ of $\mathfrak{O}$, and set $\mathfrak{p} = \mathcal{P} \cap N$. We have not specified the semi-local generator $\beta_\wp$ yet, but in view of [Ere91, Theorem 1] and [Frö83, Prop. III.2.1] — that Erez has already checked to apply to our situation — we may choose a local generator $\alpha_\wp \in N_\mathfrak{p}^\times$ such that $\mathcal{A}_{N_\mathfrak{p}/F_\wp} = \mathfrak{O}_{F_\wp}[G(\wp)]\alpha_\wp$, and set:

$$(\beta_\wp)_\mathfrak{p} = \alpha_\wp \ , \quad (\beta_\wp)_{\mathfrak{p}'} = 0 \ ,$$

for any prime ideal $\mathfrak{p}'$ of $\mathfrak{O}_N$ above $\wp$ and distinct from $\mathfrak{p}$. It then follows from [Frö83, Theorem 19] (see also [Ere91, Prop. 5.1]) that, for $\chi \in R_G$:

$$\mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)_\mathcal{Q} = \mathcal{N}_{F_\wp/\mathbb{Q}_p}(\alpha_\wp \,|\, \chi_\wp^\iota)\ \mathrm{det}_{\chi^\iota}(\gamma_\mathcal{Q}) \ ,$$

for some $\gamma_\mathcal{Q} \in G$ independent of χ. Note that the $\mathcal{Q}$-component $B_\mathcal{Q}$ of our semi-local norm-resolvent $B = \mathcal{N}_{F/\mathbb{Q}}(\beta_\wp \,|\, \chi)$ equals B^ι (strictly speaking we should write $B^{\mathcal{I}_\wp \iota}$ but we have identified $J_\wp(E)$ with $E \otimes_F F_\wp$, hence omitted $\mathcal{I}_\wp$). Define $\mathcal{R}_\wp \in \mathrm{Hom}(R_{G(\wp),p}, E_\mathcal{Q}^\times)$ by

$$\mathcal{R}_\wp(\phi) = \mathcal{N}_{F_\wp/\mathbb{Q}_p}(\alpha_\wp \,|\, \phi)$$

for $\phi \in R_{G(\wp),p}$. Reordering the factors in $\iota^*(f_p)$ we get:

$$\iota^*(f_p)(\theta) = \prod_{\wp' \nmid p} \mathrm{Ind}_{G(\wp')}^G\left(\mathcal{T}_{\wp'}^\star\right)(\theta) \prod_{\wp \mid p} \Big(\mathrm{Ind}_{G(\wp)}^G\left(\mathcal{R}_\wp \mathcal{T}_\wp^\star\right)(\theta)\ \mathrm{det}_\theta(\gamma_\mathcal{Q})\Big) \ .$$

Most of the factors of $\iota^*(f_p)$ can be dealt with using former results, already gathered in [Vin01, §4.2] in the absolute situation.

Lemma 2.4. *Let $E_\mathcal{Q}^0$ and $E_\mathcal{Q}^1$ denote the maximal subextensions of $E_\mathcal{Q}$ over $\mathbb{Q}_p$ which are respectively unramified and tamely ramified.*

(i) Suppose $\wp' \nmid p$, then $\mathcal{T}_{\wp'}^\star \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^0}[G(\wp')]^\times)$;

(ii) suppose $\wp \mid p$ and $\wp \notin S_W$, then $\mathcal{R}_\wp \mathcal{T}_\wp^\star \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G(\wp)]^\times)$.

Proof. Note first that since $\widetilde{T}_{\wp'}^\star = 1$ when $\wp' \notin S$, the same holds for $\mathcal{T}_{\wp'}^\star$. If $\wp' \nmid p$ and $\wp' \in S_T$, our modified Galois Gauss sum $\tau_{F_{\wp'}}^\star$ coincides with $\tau_{F_{\wp'}}^*$, the usual modified Galois Gauss sum (recall the footnote in Subsection 2.3.2), so we may use [Tay81, Theorem 3] together with [CNT85, (2-7)] (for the twist of the Galois Gauss sum by the Adams operator). Suppose now that $\wp' \in S_W$. We shall prove in Lemma 3.7 below — see also Subsection 3.2.3 — that $T_{\wp'}^\star$ can then be replaced by its non modified analogue $T_{\wp'} : \chi \in R_{G(\wp')} \mapsto \tau_{F_{\wp'}}(\chi - \psi_2(\chi))$, whose behaviour is controlled by the immediate extension of the result in Lemme 4.7 of [Vin01] to the relative case (noticing that the only part of Lemme 2.1 which is required in its proof, "$G_0 = G_1$", remains true, see Remark 3.5 below). This proves assertion *(i)*.

If $\wp \mid p$ and $\wp \notin S_W$, once again our modified Galois Gauss sum is the usual one $\tau^*_{F_\wp}$, so assertion *(ii)* follows from Lemme 4.3 of [Vin01] whose proof is readily checked to apply to the current relative situation. □

In Section 3, we will show, assuming Theorem 2, that assertion *(ii)* of the preceding lemma also holds when $\wp \in S_W$. We now explain how to deduce Theorem 1 from this result. Using the functorial properties of the group determinant regarding induction on character functions [Frö83, Theorem 12], it yields

$$\iota^*(f_p) \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathbb{Q}}}[G]^\times) \ .$$

In view of (1) we know that $\iota^*(f_p)$ is $\Omega_{\mathbb{Q}_p}$-equivariant. Therefore,

$$\iota^*(f_p) \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathbb{Q}}}[G]^\times)^{\Omega_{\mathbb{Q}_p}} = \mathrm{Det}(\mathfrak{O}_{E^1_{\mathbb{Q}}}[G]^\times)^{\mathrm{Gal}(E^1_{\mathbb{Q}}/\mathbb{Q}_p)} = \mathrm{Det}(\mathbb{Z}_p[G]^\times) \ ,$$

using Taylor's fixed point theorem for group determinants [Tay81, Theorem 6]. It follows by (2) that $f_p \in \mathrm{Det}(\mathbb{Z}_p[G]^\times)$ for every rational prime p dividing the order of G, and this proves Theorem 1.

3. Preliminary results

The core of this paper is the study of the remaining factor $\mathcal{R}_\wp \mathcal{T}^\star_\wp$ when $\wp$ is a prime ideal of $\mathfrak{O}$ which is wildly ramified in N/F (hence the rational prime p below $\wp$ divides the order of G). In this case, because of the assumption in Theorem 1, the local extension is abelian and weakly ramified. In order to prepare for the extensive study of this factor in the next section, we devote Subsection 3.1 to the description of these extensions, using results from Lubin-Tate theory; in Subsection 3.2 we define the Galois Gauss sum of characters of Galois groups of such extensions, explain how we modify it and state some of its properties; finally in Subsection 3.3 we show how to deduce from Theorem 2 that $\mathcal{R}_\wp \mathcal{T}^\star_\wp \in \mathrm{Det}(\mathfrak{O}_{E^1_{\mathbb{Q}}}[G(\wp)]^\times)$ when $\wp \in S_W$.

3.1 Local abelian weakly ramified extensions

Let K denote a finite extension of $\mathbb{Q}_p$ for some rational prime p, let d denote the residual degree of $K/\mathbb{Q}_p$ and set $q = p^d$. We intend to make use of Lubin-Tate theory to describe the wildly and weakly ramified abelian extensions of K, so we fix some (standard) notations. We refer to [Ser67, §3] or [Iwa86] for a brief or more detailed exposition of the theory respectively.

If π is a uniformising parameter of K and n a non negative integer, we denote by $K_{\pi,n}$ the n-th division field associated to π over K. This is the same notation as in [Ser67], but note that the numbering is different in [Iwa86]. We set $K_\pi = \cup_{n \geqslant 1} K_{\pi,n}$. For a positive integer s, we denote by K^s_{un} the unramified extension of K of degree s contained in $\mathbb{Q}_p^c$; we let $K_{un} = \cup_{s \geqslant 1} K^s_{un}$ be the maximal unramified extension of K in $\mathbb{Q}_p^c$. Recall our notation that K^{ab} is the maximal abelian extension of K in $\mathbb{Q}_p^c$, with $\mathrm{Gal}(K^{ab}/K) = \Omega^{ab}_K$. Lubin-Tate theory states that any abelian extension of K is contained in the compositum of K_π and K_{un}:

$$K^{ab} = K_\pi K_{un} \ .$$

We remark that the fields $K_{\pi,n}$ and K_π depend on the uniformising parameter π; yet we have the following result.

Lemma 3.1. *Given uniformising parameters π and π' of K, then for all $n \in \mathbb{N}$, there exists an $s \in \mathbb{N}$ such that $K_{\pi,n} K^s_{un} = K_{\pi',n} K^s_{un}$.*

Proof. In [Ser67, §3.7] Serre proves the result $K^{ab} = K_\pi K_{un}$ by first showing that $K_\pi K_{un} = K_{\pi'} K_{un}$

for all uniformising parameters π and π'. Following this proof we can actually replace K_π (resp. $K_{\pi'}$) with $K_{\pi,n}$ (resp. $K_{\pi',n}$) at every step to give

$$K_{\pi,n}K_{un} = K_{\pi',n}K_{un} \ .$$

This means that the compositum $K_{\pi,n}K_{\pi',n}$ must be contained in $K_{\pi,n}K_{un}$ and therefore the extension $K_{\pi,n}K_{\pi',n}/K_{\pi,n}$ is unramified. We know that $[K_{\pi,n}K_{\pi',n} : K_{\pi,n}]$ is finite, and therefore $K_{\pi,n}K_{\pi',n} = K_{\pi,n}K_{un}^s$ for some s. The result now follows by symmetry. □

Proposition 3.2. *Let π be a given uniformising parameter of K and let L/K be a weakly ramified abelian extension. Then there exist fields L^{tot} and L^{un} such that $L \subseteq L^{tot}L^{un}$, $L^{tot} \subseteq K_{\pi,2}$ and $L^{tot}L^{un}/L$ and L^{un}/K are unramified.*

Note that K_π/K is totally ramified, so $L^{tot} \subseteq K_{\pi,2}$ implies L^{tot}/K totally ramified.

Proof. From [Pic10, Theorem 4.1] and its proof, we know that there exist fields $\tilde{L}^{tot}$ and $\tilde{L}^{un}$ such that $L \subseteq \tilde{L}^{tot}\tilde{L}^{un}$, $\tilde{L}^{tot}/K$ is totally ramified and $\tilde{L}^{tot}\tilde{L}^{un}/L$ and $\tilde{L}^{un}/K$ are unramified, and that $\tilde{L}^{tot}/K$ is abelian totally and weakly ramified, so there exists a uniformising parameter π' of K such that $\tilde{L}^{tot} \subset K_{\pi'}$. Further, let H denote the Galois group of $\tilde{L}^{tot}/K$ and c the valuation of its conductor: set $U_K^0 = \mathfrak{O}_K^\times$ and for any positive integer n, $U_K^n = 1 + \pi^n\mathfrak{O}_K$, then c is the minimal integer $n \geqslant 0$ such that U_K^n is contained in the norm group $N_{\tilde{L}^{tot}/K}((\tilde{L}^{tot})^\times)$. We know that $c = \frac{|H_0|+|H_1|}{|H_0|}$ by [Iwa86, Coro. to Lemma 7.14], hence $c \leqslant 2$. Combining Proposition 7.2(ii) and Lemma 7.4 of [Iwa86] (recall the numbering of division fields there is different from ours), we get:

$$\tilde{L}^{tot} \subset K_{\pi',2} \ .$$

From Lemma 3.1 we then have an integer s such that $K_{un}^s K_{\pi',2} = K_{un}^s K_{\pi,2}$. Our result then follows by taking $L^{un} = \tilde{L}^{un}K_{un}^s$ and $L^{tot} = \tilde{L}^{tot}K_{un}^s \cap K_{\pi,2}$. □

Let $\Gamma^{(n)} = \mathrm{Gal}(K_{\pi,n}/K)$ then the Artin map $\theta_K : K^\times \to \Omega_K^{ab}$ yields an isomorphism $(\mathfrak{O}_K/\pi^n\mathfrak{O}_K)^\times \cong \Gamma^{(n)}$, so that

$$\Gamma^{(2)} \cong \Gamma^{(1)} \times \Gamma \ ,$$

where $\Gamma^{(1)}$ is cyclic of order $q-1$ and $\Gamma = \{\theta_K(1+\pi u), u \in \mathfrak{O}_K/\pi\mathfrak{O}_K\}$, hence $\Gamma \cong \mathfrak{O}_K/\pi\mathfrak{O}_K$ is p-elementary abelian of order q. We state the following fact for future reference.

Proposition 3.3. *The subextension $M_{\pi,2}$ of $K_{\pi,2}/K$ fixed by $\Gamma^{(1)}$ has*

$$r = \frac{p^d - 1}{p-1} = 1 + p + \cdots + p^{d-1}$$

subextensions M_i, $1 \leqslant i \leqslant r$, of degree p over K, each of which is the fixed subextension of $M_{\pi,2}/K$ by the kernel of an irreducible character χ_i of $\mathrm{Gal}(M_{\pi,2}/K) \cong \Gamma$.

Proof. See for instance [Vin05, §2.2]. □

Notice further that $K_{\pi,2} = K_{\pi,1}M_{\pi,2}$ and $M_{\pi,2}$ is the maximal p-extension of K contained in $K_{\pi,2}$.

Corollary 3.4. *In the notations of Proposition 3.2, suppose further that L/K is wildly ramified, then the conclusion of Proposition 3.2 holds with $L^{tot} \subseteq M_{\pi,2}$. If moreover the ramification group of L/K is cyclic, then $L^{tot} = M_i$ for an integer $i \in \{1, \ldots, r\}$.*

Proof. Let $H = \mathrm{Gal}(L/K)$ and for $i \geqslant -1$, let H_i denote the i-th ramification subgroup (in lower notation). One has $H_1 \neq H_2 = 1$ since L/K is wildly and weakly ramified, so $H_0/H_1 = 1$ by [Ser68, IV.2, Coro. 2 to Prop. 9], namely H_0 is a p-group.

Let L^{tot} and L^{un} be as given by Proposition 3.2. They are linearly disjoint over K, so $\mathrm{Gal}(L^{tot}L^{un}/K)$ equals the direct product $\mathrm{Gal}(L^{tot}/K) \times \mathrm{Gal}(L^{un}/K)$ and the ramification group of $L^{tot}L^{un}/K$ equals that of L^{tot}/K. Since L^{tot}/K is totally ramified and $L^{tot}L^{un}/L$ is unramified, this yields (*e.g.* using Herbrand's theorem)

$$\mathrm{Gal}(L^{tot}/K) = \mathrm{Gal}(L^{tot}/K)_0 = H_0 \ .$$

Since H_0 is a p-group, we get that $L^{tot} \subseteq {K_{\pi,2}}^{\Gamma^{(1)}} = M_{\pi,2}$. Further $\mathrm{Gal}(L^{tot}/K)$ is a quotient of the p-elementary abelian group Γ, hence has to be of order p if cyclic. □

3.2 Local weakly ramified Galois Gauss sums

Again here p is a fixed rational prime and K is a finite extension of $\mathbb{Q}_p$. Recall from Notation 2.1 that $\mathbb{Q}^c$ denotes the algebraic closure of $\mathbb{Q}$ in the field of complex numbers. For any non negative integer n, let ξ_n be the p^n-th primitive root of unity in $\mathbb{Q}^c$ given by $\xi_n = \exp(\frac{2i\pi}{p^n})$, with the standard notations for complex numbers, in particular $\xi_0 = 1$; in the sequel we shall use the notation:

$$\zeta = \xi_1 \ , \quad \xi = \xi_2 \tag{3}$$

since we will mainly be concerned with these two p^n-th roots of unity. From now on we use the letter π to denote a uniformising parameter of K.

3.2.1 *Abelian Galois Gauss sum.* Let L be a finite abelian extension of K with Galois group H. We denote by $\widehat{H}$ the group of irreducible characters of H with values in $\mathbb{Q}^c$. Any $\chi \in \widehat{H}$ can be seen as a character of $K^\times$ using the composition of the Artin map θ_K of K with the restriction of automorphisms to L:

$$\theta_{L/K} : K^\times \to \Omega_K^{ab} \twoheadrightarrow \mathrm{Gal}(L/K) = H \ .$$

We shall also denote by χ the character of $K^\times$ obtained in this way. Set $U_K^0 = \mathfrak{O}_K^\times$ and $U_K^m = 1+\pi^m\mathfrak{O}_K$ for positive integers m. The conductor $\mathfrak{f}(\chi)$ of the character χ is $\pi^m\mathfrak{O}_K$, where m is the smallest integer such that $\chi(U_K^m) = 1$.

Let $\mathfrak{D}_K = \pi^s\mathfrak{O}_K$ denote the absolute different of $K/\mathbb{Q}_p$ and let ψ_K denote the standard additive character of K, which is defined by composing the trace $Tr = Tr_{K/\mathbb{Q}_p}$ with the additive homomorphism $\psi_p : \mathbb{Q}_p \to (\mathbb{Q}^c)^\times$ such that $\psi_p(\mathbb{Z}_p) = 1$ and, for any natural integer n, $\psi_p(\frac{1}{p^n}) = \xi_n$, the p^n-th root of unity defined above. The (local) Galois Gauss sum τ_K is then defined by [Mar77, II.2 p.29]:

$$\tau_K(\chi) = \sum_x \chi\left(\frac{x}{\pi^{s+m}}\right)\psi_K\left(\frac{x}{\pi^{s+m}}\right) \ ,$$

where m is such that $\mathfrak{f}(\chi) = \pi^m\mathfrak{O}_K$ and x runs through a set of representatives of U_K^0/U_K^m. In particular $\tau_K(\chi) = \chi(\pi^{-s})$ if χ is unramified, namely if $\mathfrak{f}(\chi) = \mathfrak{O}_K$.

The Galois Gauss sum is now defined on $\widehat{H}$. Since $\widehat{H}$ is a basis of the free group of virtual characters R_H, we extend τ_K to a function on R_H by linearity: $\tau_K(\chi+\chi') = \tau_K(\chi)\tau_K(\chi')$. Inductivity in degree 0 then enables one to extend τ_K to virtual characters of non abelian extensions of K — see [Frö83, Theorem 18]. Note that the conductor function $\mathfrak{f}$ extends to R_H the same way.

Before modifying the abelian Galois Gauss sum, we introduce the non-ramified part n_χ of $\chi \in \widehat{H}$ by $n_\chi = \chi$ if χ is unramified, $n_\chi = 0$ otherwise. The map $\chi \mapsto n_\chi$ then extends to an endomorphism of the additive group R_H by linearity ($n_{\chi+\chi'} = n_\chi + n_{\chi'}$). One easily checks that if $\chi \in R_H$ is such that $\chi = n_\chi$, then:

$$\tau_K(\chi) = \det_\chi(\pi^{-s}) = \det_\chi(\mathfrak{D}_K^{-1}) \ . \tag{4}$$

3.2.2 *Modification in the tame and weak cases.* In this paper, we will only have to consider the case where L/K is tamely or weakly ramified, namely H_1 or H_2 is trivial. Since $\theta_{L/K}$ sends U_K^m to the m-th ramification group in the upper numbering H^m [Ser67, 4.1 Theorem 1], and since $H^1 = H_1$ and $H_2 = 1 \Rightarrow H^2 = 1$, we see that for $\chi \in \widehat{H}$ we will always have $\pi^2\mathfrak{O}_K \subseteq \mathfrak{f}(\chi)$. We shall say that $\chi \in \widehat{H}$ is unramified if $\mathfrak{f}(\chi) = \mathfrak{O}_K$, tamely ramified if $\mathfrak{f}(\chi) = \pi\mathfrak{O}_K$ and weakly ramified if $\mathfrak{f}(\chi) = \pi^2\mathfrak{O}_K$. We shall also say that $\chi \in R_H$ is unramified if $\mathfrak{f}(\chi) = \mathfrak{O}_K$.

Remark 3.5. *If L/K is wildly and weakly ramified and abelian, then $H_0 = H_1$ (see the proof of Corollary 3.4), thus any $\chi \in \widehat{H}$ is either unramified or weakly ramified. Indeed in the abelian case, the tame and "wild and weak" situations do not occur simultaneously.*

We recall how the Galois Gauss sum is modified in the tame abelian situation. Fix an element $c_{K,1} \in K$ such that $c_{K,1}\mathfrak{O}_K = \pi\mathfrak{D}_K$. Suppose L/K is (at most) tamely ramified and χ is a virtual character of H. Recall the definition of the non ramified part n_χ of χ above. The (tame) non ramified characteristic of χ is $y_{K,1}(\chi) = (-1)^{\deg(n_\chi)} \det_{n_\chi}(\pi)$, and its modified Galois Gauss sum is

$$\tau_K^\star(\chi) = \tau_K(\chi) y_{K,1}(\chi)^{-1} \det_\chi(c_{K,1}) \ .$$

This function is usually denoted by τ_K^* [Frö83, IV.1], we changed the shape of the star in the exponent to stress the fact that the Galois Gauss sum will be modified in a different (yet similar) way in the wild and weak case. Indeed the above remark enables us to treat these two cases separately.

Fix an element $c_{K,2} \in K$ such that $c_{K,2}\mathfrak{O}_K = \pi^2\mathfrak{D}_K$. Note that, if K' is a finite Galois extension of K with uniformising parameter π' and Galois group H', with $H'_0 = H'_1$ and $H'_2 = 1$ (call that property "purely weakly ramified"), then $c_{K,2}\mathfrak{O}_{K'} = \pi'^2\mathfrak{D}_{K'}$.

Suppose L/K is wildly and weakly ramified and abelian.

Definition 3.6. *The (weak) non ramified characteristic of $\chi \in R_H$ is*

$$y_{K,2}(\chi) = (-1)^{\deg(n_\chi)} \det_{n_\chi}(\pi^2) \ ;$$

its modified Galois Gauss sum is

$$\tau_K^\star(\chi) = \tau_K(\chi) y_{K,2}(\chi)^{-1} \det_\chi(c_{K,2}) \ .$$

Note that since n_χ is an unramified character, $y_{K,2}(\chi)$ does not depend on the choice of the uniformising parameter π. On the contrary, $\tau_K^\star$ depends on the choice of the element $c_{K,2}$, unless χ is unramified; changing $c_{K,2}$ multiplies $\tau_K^\star$ by an element of $\mathrm{Det}(H_0)$.

For the purposes of this paper we will only need the abelian modified Galois Gauss sum. Nevertheless, this notion extends to non abelian characters as in the tame situation. First one shows using the results in Subsection 3.1 that there exists a maximal "purely weakly ramified" (see above) extension K^{pw} of K — let $R_{(K)}^{pw}$ denote the free group generated by the characters of the irreducible representations of $\mathrm{Gal}(K^{pw}/K)$ over $\mathbb{Q}^c$ with open kernel. One then easily checks that the proof of [Frö83, Theorem 29(ii)] shows *mutatis mutandis* that $y_{K,2}$ is fully inductive, *i.e.*, for $K \subseteq K' \subset K^{pw}$ and $\chi \in R_{(K')}^{pw}$:

$$y_{K',2}(\chi) = y_{K,2}(\mathrm{ind}\,\chi) \ ,$$

where $\mathrm{ind}\,\chi$ is the induced character of χ in $R_{(K)}^{pw}$. Since τ_K is inductive in degree 0 in the purely weakly ramified context as well as in the tame one — see for instance [Mar77, II.4 p.39], and since the same holds for $\det(c_{K,2})$ — see the proof of [Frö83, Prop. IV.1.1(iv)], the above definition yields modified Galois Gauss sums $\tau_{K'}^\star$ on $R_{(K')}^{pw}$ for any K'/K contained in K^{pw}, which are inductive in degree 0.

We now check that our modification only involves factors in the denominator of the Hom-description — see [Frö83, Theorem 29(i)] for the tame case.

LEMMA 3.7. *Suppose L/K is abelian, of Galois group H, and either tamely or wildly and weakly ramified. The map $\tau_K^\star/\tau_K$ belongs to* $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_H, (\mathbb{Q}^c)^\times)\,\mathrm{Det}(H)$.

Proof. Let $i = 1$ or 2 depending on whether L/K is tamely or weakly ramified, and let $\chi \in R_H$. Clearly $y_{K,i}$ is $\Omega_\mathbb{Q}$-equivariant and takes roots of unity values, since $\det_{n_\chi}$ is an abelian character; set $h_{K,i} = \theta_{L/K}(c_{K,i}) \in H$, then $\det_\chi(c_{K,i}) = \det_\chi(h_{K,i})$. Therefore, $\chi \mapsto \det_\chi(c_{K,i}) \in \mathrm{Det}(H)$. □

Note that when $\chi \in \widehat{H}$ is weakly ramified, we get $\tau_K^\star(\chi) = \tau_K(\chi)\chi(c_{K,2})$. Further recall from [Tat77, §1] that in this case, the Galois Gauss sum is linked to the local root number $W(\chi)$ by:

$$\tau_K(\chi) = p^d W(\chi^{-1}) \ , \tag{5}$$

where d is the residual degree of $K/\mathbb{Q}_p$. We now show the following very useful property — see [Frö83, Prop. IV.1.1(vi)] for the analogous one in the tame situation.

PROPOSITION 3.8. *Suppose L/K is wildly and weakly ramified with abelian Galois group H, $\chi, \phi \in \widehat{H}$ with ϕ unramified, then:*

$$\tau_K^\star(\phi) = -1 \ , \quad \tau_K^\star(\phi\chi) = \tau_K^\star(\chi) \ .$$

Proof. One has $\tau_K(\phi) = \phi(\pi^{-s})$, $y_{K,2}(\phi) = -\phi(\pi^2)$ and $\phi(c_{K,2}) = \phi(\pi^{2+s})$, hence the result for $\tau_K^\star(\phi)$. The result for $\tau_K^\star(\phi\chi)$ follows when χ is unramified. Suppose χ is ramified, thus $\mathfrak{f}(\chi) = \mathfrak{f}(\phi\chi) = \pi^2\mathfrak{O}_K$ and we get, using Formula (5) above together with [Tat77, §1 Coro. 2]:

$$\tau_K(\phi\chi) = p^d W(\phi^{-1}\chi^{-1}) = p^d\phi^{-1}(\pi^{2+s})W(\chi^{-1}) = \phi(\pi^{-2-s})\tau_K(\chi) \ .$$

Further, $y_{K,2}(\chi\phi) = 1 = y_{K,2}(\chi)$ and $\chi\phi(c_{K,2}) = \phi(\pi^{2+s})\chi(c_{K,2})$, hence the result for $\tau_K^\star(\phi\chi)$. □

More generally, when L/K is abelian and either tamely or wildly and weakly ramified, and $\phi \in R_H$ is unramified, one checks from Definition 3.6, using (4), that $\tau_K^\star(\phi) = (-1)^{\deg(\phi)}$.

3.2.3 *Twisting.* The last step to build the morphism f defined in Subsection 2.3 is to twist the modified Galois Gauss sum by ψ_2, the second Adams operation, which is the endomorphism of R_G defined by $\psi_2(\chi)(g) = \chi(g^2)$ for $\chi \in R_G$ and $g \in G$. The properties of ψ_2, together with Lemma 3.7 above, enable us to show that f is, as claimed, a representative of $(\mathcal{A})$.

Proof of Proposition 2.3. One only has to check that the quotient of f by Erez's representative $v_{N/F}$ [Ere91, Theorem 3.6] lies in the denominator of the Hom-description. Choosing the same semi-local normal basis generators $\beta_\wp$ to define f and $v_{N/F}$ — the change of semi-local generator lies in the denominator of the Hom-description, see [Frö83, Coro. to Prop. I.4.2] — this quotient is the global valued morphism on R_G given by:

$$\frac{f}{v_{N/F}} = \prod_{\ell \in S} \mathrm{Ind}_{G(\ell)}^G \left(\frac{\tau_{F_\ell}^\star/\tau_{F_\ell}}{\Psi_2(\tau_{F_\ell}^\star/\tau_{F_\ell})} \right) \ ,$$

where Ψ_2 is the second Adams operator, defined by $\Psi_2(v)(\chi) = v(\psi_2(\chi))$ if v a character function. Fix an $\ell \in S$. We know by Lemma 3.7 that $\tau_{F_\ell}^\star/\tau_{F_\ell} \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_{G(\ell)}, E^\times)\,\mathrm{Det}\big(G(\ell)\big)$. By [CNT85, (2-7)], Ψ_2 preserves $\mathrm{Det}(\mathbb{Z}_l[G(\ell)]^\times)$ for every rational prime l, hence $\Psi_2\big(\mathrm{Det}\big(G(\ell)\big)\big) \subset \mathrm{Det}(\mathbb{Z}[G(\ell)]^\times)$; further ψ_2 commutes with the action of $\Omega_\mathbb{Q}$ on $R_{G(\ell)}$, see [Ere91, Prop.-Def. 3.5], hence Ψ_2 preserves $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_{G(\ell)}, E^\times)$. Applying [Frö83, Theorem 12], we see that $f/v_{N/F}$ belongs to $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)\,\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))$ as required. □

3.2.4 *Alternative expressions of the twisted modified Galois Gauss sum.* We get back to the previous setting, so L/K is an abelian weakly ramified extension of p-adic fields, of Galois group H. The abelian hypothesis yields that if $\chi \in \widehat{H}$, then $\psi_2(\chi) = \chi^2$, hence $\tau_K^\star(\chi - \psi_2(\chi)) = \tau_K^\star(\chi)/\tau_K^\star(\chi^2)$. If further χ is weakly ramified, then

$$\tau_K^\star(\chi - \psi_2(\chi)) = \chi(c_{K,2})^{-1}\tau_K(\chi - \chi^2) \ . \tag{6}$$

Note also that, for any $\chi \in R_H$, $\psi_2(\chi)$ has the same degree as χ. If χ is unramified, it follows that

$$\tau_K^\star(\chi - \psi_2(\chi)) = 1 \ . \tag{7}$$

Recall that ψ_K is the standard additive character of K defined in Subsection 3.2.1 (and beware that ψ_2 and ψ_K are very different functions).

Proposition 3.9. *Suppose $\chi \in \widehat{H}$ is weakly ramified, then there exists $c_\chi \in K$ such that:*

$$c_\chi \mathfrak{O}_K = \mathfrak{f}(\chi)\mathfrak{D}_K \quad \text{and} \quad \forall y \in \pi\mathfrak{O}_K \ , \ \chi(1+y)^{-1} = \psi_K(c_\chi^{-1}y) \ ; \tag{8}$$

further for any such c_χ:

$$\tau_K^\star(\chi - \chi^2) = \chi\big(\tfrac{c_\chi}{4c_{K,2}}\big)\psi_K(c_\chi^{-1})^{-1} \ .$$

Proof. This result is a direct consequence of [Tat77, §1]. Using Formula (5) and applying Proposition 1 of [Tat77, §1] to $\alpha = \chi^{-1}$ and $\mathfrak{a} = \pi\mathfrak{O}_K$, we get the existence of $c_\chi \in K$ satisfying conditions (8) above and that, for any such c_χ:

$$\tau_K(\chi) = p^d\chi(c_\chi^{-1})\psi_K(c_\chi^{-1}) \ .$$

It only remains to notice that c_χ satisfies conditions (8) for χ if and only if $c_\chi/2$ satisfies them for χ^2, to get the result through Formula (6). □

We deduce the result which will be required later.

Corollary 3.10. *Suppose $K/\mathbb{Q}_p$ is unramified and set $v_{K,2} = p^2/c_{K,2} \in \mathfrak{O}_K^\times$. Suppose $\chi \in \widehat{H}$ is weakly ramified, then there exists $v_\chi \in \mathfrak{O}_K^\times$ such that $\forall u \in \mathfrak{O}_K$, $\chi(1+up)^{-1} = \zeta^{Tr(uv_\chi)}$; under this condition, one has:*

$$\tau_K^\star(\chi - \chi^2) = \chi\big(\tfrac{v_{K,2}}{4v_\chi}\big)\xi^{-Tr(v_\chi)} \ .$$

Further:

(i) v_χ is uniquely defined modulo p, but $v_\chi + ap$ also satisfies the above condition for any $a \in \mathfrak{O}_K$;

(ii) if $j \in \{1, \dots, p-1\}$, v_{χ^j} can be chosen equal to jv_χ.

Proof. Since $K/\mathbb{Q}_p$ is unramified, p is a uniformising parameter of K and $\mathfrak{f}(\chi)\mathfrak{D}_K = \mathfrak{f}(\chi) = p^2\mathbb{Z}_p$. Let $c_\chi \in K$ satisfying conditions (8) for χ and set $v_\chi = p^2/c_\chi$, then $v_\chi \in \mathfrak{O}_K^\times$ and for all $u \in \mathfrak{O}_K$ one has $\chi(1+up)^{-1} = \psi_K(uv_\chi/p) = \zeta^{Tr(uv_\chi)}$. Conversely, if v_χ satisfies these conditions, then $c_\chi = p^2/v_\chi$ satisfies conditions (8) and the formula given in Proposition 3.9 yields the formula for the Galois Gauss sum.

Let k denote the residue field of K. The trace form $T(x,y) = Tr_{k/(\mathbb{Z}_p/p\mathbb{Z}_p)}(xy)$ is a non degenerate symmetric bilinear form from $k \times k$ to $\mathbb{Z}_p/p\mathbb{Z}_p$, hence induces an isomorphism $y \mapsto T(\,.\,,y)$ between k and its dual. If $v_\chi \in \mathfrak{O}_K^\times$ satisfies the condition of the Corollary, then $T(\,.\,, v_\chi \mod p)$ is given by this condition, hence $v_\chi \mod p$ is unique. The two last assertions are readily checked. □

Remark 3.11. *Under the hypothesis of Corollary 3.10 we get:*

$$\tau_K^\star\big(\chi - \chi^2\big)^p = \zeta^{-Tr(v_\chi)} = \chi(1+p)$$

so the modified twisted Galois Gauss sum is a p-th root of unity if and only if $\chi(1+p)$ is trivial, namely when $\theta_{L/K}(1+p)$ belongs to $\ker(\chi)$. If $K/\mathbb{Q}_p$ is ramified, we get by Proposition 3.9 that $\chi(1+p)^{-1} = \psi_K(c_\chi^{-1}p) = \psi_K(c_\chi^{-1})^p$, therefore we have

$$\tau_K^\star(\chi - \chi^2)^p = \chi(1+p) = 1$$

since $p \in \pi^2\mathfrak{O}_K$. The modified abelian weakly ramified twisted Galois Gauss sum is thus always a p-th root of unity in the ramified base field case.

3.3 Reduction of the problem

Recall that p is a rational prime dividing the order of G (in particular $p \neq 2$ since $[N : F]$ is odd); $\mathcal{Q}$ is a prime ideal of $\mathfrak{O}_E$ above p; $\wp$ is a prime ideal of $\mathfrak{O}$ above p which is wildly ramified in N/F. In Subsection 2.3.2 we have fixed a prime ideal $\mathcal{P}$ of E above $\wp$ and denoted by $\iota_{\mathcal{P}/\wp}$ the corresponding embedding of E into $\mathbb{Q}_p^c$ fixing $\wp$; by $G(\wp)$ the image in G of $\mathrm{Gal}(N_\mathfrak{p}/F_\wp)$, where $\mathfrak{p} = \mathcal{P} \cap N$, by the homomorphism induced by $\iota_{\mathcal{P}/\wp}$. We introduce the following useful notations.

Notation 3.12. *If K is a finite extension of $\mathbb{Q}_p$ and L/K is weakly ramified with Galois group H, we let α_L denote a normal basis generator of the square root of the inverse different $\mathcal{A}_{L/K}$ of L/K and $\mathcal{RT}_K^\star(L)$ the morphism from $R_{H,p}$ to $E_\mathcal{Q}^\times$ given by*

$$\mathcal{RT}_K^\star(L)(\chi) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_L \,|\, \chi)\mathcal{T}_K^\star(\chi) \ .$$

We will sometimes write $\tau_K^\star(\chi - \chi^2)$ instead of $\mathcal{T}_K^\star(\chi)$, when the context makes it clear what we mean.

We are thus interested in computing $\mathcal{RT}_{F_\wp}^\star(N_\mathfrak{p}) = \mathcal{R}_\wp\mathcal{T}_\wp^\star$.

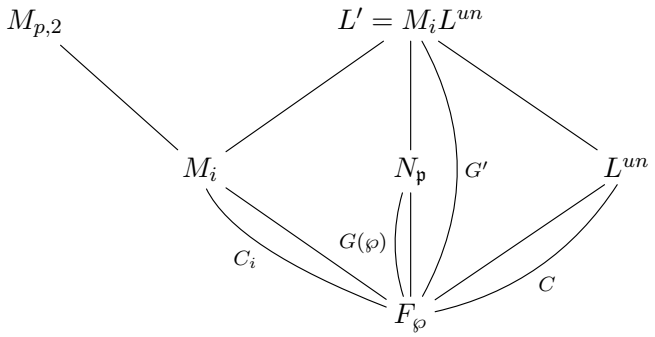
By the hypothesis in Theorem 1, $F_\wp$ is unramified over $\mathbb{Q}_p$ and $N_\mathfrak{p}/F_\wp$ is abelian, wildly and weakly ramified, with cyclic ramification group. We are therefore in a position to apply Corollary 3.4 with $K = F_\wp$, uniformising parameter $\pi = p$, and $L = N_\mathfrak{p}$. Recall that $M_{p,2}$ has $r = \frac{p^d-1}{p-1}$ subextensions M_i, $1 \leqslant i \leqslant r$, of degree p over $F_\wp$. We know that there exist an unramified extension $L^{un}/F_\wp$ and an integer $1 \leqslant i \leqslant r$, such that:

$$N_\mathfrak{p} \subseteq M_iL^{un} \ \text{ and } \ M_iL^{un}/N_\mathfrak{p} \text{ is unramified.}$$

Proposition 3.13. *Let $C_i = \mathrm{Gal}(M_i/F_\wp)$ then:*

$$\mathcal{RT}_{F_\wp}^\star(M_i) \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[C_i]^\times) \Longrightarrow \mathcal{RT}_{F_\wp}^\star(N_\mathfrak{p}) \ \in \ \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G(\wp)]^\times) \ .$$

Before giving the proof, we describe these extensions in a diagram in which we introduce some notations for the Galois groups involved.



Proof. There will be two steps in the reduction process: from M_i to $L' = M_iL^{un}$ and from L' to $N_\mathfrak{p}$. For

the first step, we shall take advantage of the fact that $L'/F_\wp$ is the compositum of the totally ramified extension $M_i/F_\wp$ and the unramified extension $L^{un}/F_\wp$.

LEMMA 3.14. *Let K be a finite Galois extension of $\mathbb{Q}_p$ and K^t be its maximal tame extension in $\mathbb{Q}_p^c$. Let L_u be an unramified extension of K such that $L_u/\mathbb{Q}_p$ is Galois, L_1/K be an abelian totally wildly and weakly ramified extension and set $L_2 = L_1L_u$, $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Then:*

$$\mathcal{RT}_K^\star(L_1) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_1]^\times) \Longrightarrow \mathcal{RT}_K^\star(L_2) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_2]^\times) \ .$$

Notice that the existence of a normal basis generator α_{L_2} for $\mathcal{A}_{L_2/K}$ is ensured by [Ere91, §2 Theorem 1] and [Vin01, Proposition 2.2(ii)].

Proof. Since L_u/K is unramified, let us denote by C its cyclic Galois group, then $G_2 = G_1 \times C$ and any irreducible character χ_2 of G_2 decomposes as a product $\chi_2 = \chi_1\chi_C$, where χ_1 (resp. χ_C) is an irreducible character of G_1 (resp. C). Let β denote a normal basis generator for $\mathfrak{O}_{L_u} = \mathcal{A}_{L_u/K}$ over $\mathfrak{O}_K$. Since L_1/K and L_u/K are linearly disjoint, one has $\mathcal{A}_{L_2/K} = \mathcal{A}_{L_1/K} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{L_u}$. This implies that $\alpha_{L_1} \otimes \beta$ is a normal basis generator for $\mathcal{A}_{L_2/K}$ over $\mathfrak{O}_K$, so there exists $u \in \mathfrak{O}_K[G_2]^\times$ such that $\alpha_{L_2} = (\alpha_{L_1} \otimes \beta)u$. By [Frö83, §I, Coro. to Prop. 4.2], this yields

$$\begin{aligned}(\alpha_{L_2} \,|\, \chi_2) &= (\alpha_{L_1} \otimes \beta \,|\, \chi_2)\,\mathrm{Det}_{\chi_2}(u) \\ &= (\alpha_{L_1} \,|\, \chi_1)(\beta \,|\, \chi_C)\,\mathrm{Det}_{\chi_2}(u) \\ &= (\alpha_{L_1} \,|\, \chi_1)\,\mathrm{Det}_{\chi_C}(B)\,\mathrm{Det}_{\chi_2}(u) \ ,\end{aligned} \tag{9}$$

where $B = \sum_{c\in C} c(\beta)c^{-1} \in \mathfrak{O}_{L_u}[C]^\times$ by [Frö83, Proposition I.4.3]. Note that χ_C is the restriction to C of χ_2 and that $[\chi_C \mapsto \mathrm{Det}_{\chi_C}(B)] \in \mathrm{Det}(\mathfrak{O}_{L_u}[C]^\times)$, so $[\chi_2 \mapsto \mathrm{Det}_{\chi_C}(B)] \in \mathrm{Det}(\mathfrak{O}_{L_u}[G_2]^\times)$ by the functorial properties of Det. Consequently, let $v \in \mathfrak{O}_{L_u}[G_2]^\times$ be such that $(\alpha_{L_2} \,|\, \chi_2) = (\alpha_{L_1} \,|\, \chi_1)\,\mathrm{Det}_{\chi_2}(v)$. To compute the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}$, we need to choose a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$. Since $\Omega_{\mathbb{Q}_p}/\Omega_K = \mathrm{Gal}(L_u/\mathbb{Q}_p)\,/\,\mathrm{Gal}(L_u/K)$, we can choose Ω so that $\Omega|_{L_u} \subset \mathrm{Gal}(L_u/\mathbb{Q}_p)$. With this choice, $v' = \prod_\Omega v^\omega \in \mathfrak{O}_{L_u}[G_2]^\times$ is such that:

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \,|\, \chi_2) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \,|\, \chi_1)\,\mathrm{Det}_{\chi_2}(v') \ .$$

We now consider the twisted modified Galois Gauss sum. Since χ_C is an unramified character, we know by Proposition 3.8 that $\tau_K^\star(\chi_2 - \chi_2^2) = \tau_K^\star(\chi_1 - \chi_1^2)$. This yields:

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \,|\, \chi_2)\tau_K^\star(\chi_2 - \chi_2^2) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \,|\, \chi_1)\tau_K^\star(\chi_1 - \chi_1^2)\,\mathrm{Det}_{\chi_2}(v') \ .$$

Suppose $\mathcal{RT}_K^\star(L_1) \in \mathrm{Det}(\mathfrak{O}_{K^t}[G_1]^\times)$, then by induction of character functions, the map

$$\chi_2 \mapsto \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \,|\, \chi_1)\tau_K(\chi_1 - \chi_1^2)$$

belongs to $\mathrm{Det}(\mathfrak{O}_{K^t}[G_2]^\times)$, and the same holds for $\chi_2 \mapsto \mathrm{Det}_{\chi_2}(v')$, thus for $\mathcal{RT}_K^\star(L_2)$. □

Suppose $\mathcal{RT}_{F_\wp}^\star(M_i) \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[C_i]^\times)$. We know that $L' = M_iL^{un}$ is unramified over $N_\mathfrak{p}$ and that $N_\mathfrak{p}/F_\wp$ is weakly ramified, therefore $L'/F_\wp$ is weakly ramified. We then apply Lemma 3.14 to $K = F_\wp$, $L_1 = M_i$, $L_u = L^{un}$, and get that $\mathcal{RT}_{F_\wp}^\star(L') \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G']^\times)$.

We consider the restriction of $F_\wp$-automorphisms of L' to $N_\mathfrak{p}$: $G' \twoheadrightarrow G(\wp)$. It induces an inflation map on characters $\mathrm{inf} : R_{G(\wp),p} \to R_{G',p}$, which in turn induces a co-inflation map on character functions

$$\mathrm{coinf} = \mathrm{coinf}_{G(\wp)}^{G'} : \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G',p}, E_\mathcal{Q}^\times) \to \mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G(\wp),p}, E_\mathcal{Q}^\times) \ ,$$

and we know by [Frö83, Theorem 12 (ii)] that

$$\mathrm{coinf}\,\mathcal{RT}_{F_\wp}^\star(L') \in \mathrm{Det}(\mathfrak{O}_{E_\mathcal{Q}^1}[G(\wp)]^\times) \ . \tag{10}$$

We now show the following result.

LEMMA 3.15. *Let K be a finite Galois extension of $\mathbb{Q}_p$, $L_2/L_1/K$ be a tower of abelian extensions such that L_2/K is weakly ramified. Set $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Then there exists $v \in \mathfrak{O}_K[G_1]^\times$ such that*

$$\mathrm{coinf}\,\mathcal{RT}_K^\star(L_2) = \mathcal{RT}_K^\star(L_1)\,\mathrm{Det}(v) \ .$$

Proof. For $\chi \in R_{G_1,p}$, one has

$$\begin{aligned}\mathrm{coinf}\,\mathcal{RT}_K^\star(L_2)\,(\chi) &= \mathcal{RT}_K^\star(L_2)(\inf\,\chi) \\ &= \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \inf\,\chi)\tau_K^\star\big(\inf\chi - (\inf\chi)^2\big) \ .\end{aligned}$$

We know that the Galois Gauss sum is inflation invariant — use (5) and see [Mar77, p.18 and 22], *i.e.*, $\tau_K(\inf\chi) = \tau_K(\chi)$. The same clearly holds for the twisted Galois Gauss sum, as well as for its modified version, thanks to (6) and since:

$$(\inf\chi)(c_{K,2}) = \chi\big(\theta_{L_2/K}(c_{K,2})|_{L_1}\big) = \chi\big(\theta_{L_1/K}(c_{K,2})\big) = \chi(c_{K,2}) \ .$$

For the resolvent, we know by Lemma 1.5 of [Frö83, III], which is readily checked to apply to non tame extensions:

$$(\alpha_{L_2} \mid \inf\,\chi)_{G_2} = \big(Tr_{L_2/L_1}(\alpha_{L_2}) \mid \chi\big)_{G_1} \ ,$$

where the subscripts stress the fact that the sums defining both resolvents are not indexed by the same group. Further since $\mathcal{A}_{L_1/K} = Tr_{L_2/L_1}(\mathcal{A}_{L_2/K})$ (see [Ere91, §5]), $Tr_{L_2/L_1}(\alpha_{L_2})$ is a normal basis generator for $\mathcal{A}_{L_1/K}$, so there exists some $u \in \mathfrak{O}_K[G_1]^\times$ such that $Tr_{L_2/L_1}(\alpha_{L_2}) = u\alpha_{L_1}$. As in formula (9), this yields:

$$\big(Tr_{L_2/L_1}(\alpha_{L_2}) \mid \chi\big) = (\alpha_{L_1} \mid \chi)\,\mathrm{Det}_\chi(u)$$

and so, for any transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$, we get:

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_2} \mid \inf\,\chi) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_{L_1} \mid \chi)\ \mathrm{Det}_\chi(v) \ ,$$

where $v = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q}_p)} u^\sigma \in \mathfrak{O}_K[G_1]^\times$. □

Proposition 3.13 now follows from Lemma 3.15 and Equation (10). □

Since we have applied Corollary 3.4 to $F_\wp$ with uniformising parameter p, we know that $M_i \subseteq (F_\wp)_{p,2}$, thus p belongs to the norm group $N_{M_i/K}(M_i^\times)$ of M_i/K by [Iwa86, Lemma 7.4]. Assuming Theorem 2 we get that $\mathcal{RT}_{F_\wp}^\star(M_i) = 1$ for appropriate choices of α_{M_i}; of the transversal Ω of $\Omega_{F_\wp}$ in $\Omega_{\mathbb{Q}_p}$ that defines the norm-resolvent; and of the element $c_{F_\wp,2}$ of $\mathfrak{O}_{F_\wp}$ that defines the modified twisted Galois Gauss sum. Therefore, it follows from Proposition 3.13 that for $\wp \in S_W$:

$$\mathcal{RT}_{F_\wp}^\star(N_\mathfrak{p}) \in \mathrm{Det}(\mathfrak{O}_{E_\mathfrak{Q}^1}[G(\wp)]^\times)$$

as announced. We are left with proving Theorem 2, which is the goal of the next section.

4. The local computation

We fix a rational prime p and an unramified finite extension K of $\mathbb{Q}_p$; we denote by k its residue field, and set $d = [K : \mathbb{Q}_p] = [k : \mathbb{Z}_p/p\mathbb{Z}_p]$. Let M be a cyclic wildly and weakly ramified extension of K, with Galois group H, such that p belongs to the norm group $N_{M/K}(M^\times)$ of M/K, namely $M \subset K_p$, thus M is one of the degree p subextensions M_i of $K_{p,2}/K$ of Proposition 3.3 applied to $\pi = p$. It follows

that M is the fixed subfield of $M_{p,2}/K$ by the kernel of an irreducible character χ of $\mathrm{Gal}(M_{p,2}/K)$, and the irreducible characters of H are the χ^j, $0 \leqslant j \leqslant p-1$ (χ^0 is the trivial character χ_0).

Let $0 \leqslant j \leqslant p-1$, then $\mathcal{RT}_K^\star(M)(\chi^j) = \mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j)\tau_K^\star(\chi^j - \chi^{2j})$. We first use the explicit construction from [Pic09] of a self-dual normal basis generator α_M for $\mathcal{A}_{M/K}$ over $\mathfrak{O}_K$, to calculate the norm-resolvent $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j)$. We then calculate the modified twisted Galois Gauss sum $\tau_K^\star(\chi^j - \chi^{2j})$, and show that $\mathcal{RT}_K^\star(M) = 1$ for appropriate choices of the transversal Ω defining the norm-resolvent and the element $c_{K,2}$ of K defining the modified Galois Gauss sum.

4.1 Dwork's exponential power series

Let $\gamma \in \mathbb{Q}_p^c$ be a root of the polynomial $X^{p-1} + p$ and note that, as this is an Eisenstein polynomial, γ will be a uniformising parameter of $K(\gamma)$.

Definition 4.1. *We define Dwork's exponential power series as*

$$E_\gamma(X) = \exp(\gamma X - \gamma X^p),$$

where the right hand side is to be thought of as the power series expansion of the exponential function.

Here we recall some important properties of Dwork's power series. Let $\mathbb{C}_p$ denote the completion of $\mathbb{Q}_p^c$ and $|\,.\,|_p : \mathbb{C}_p \to \mathbb{R}$ its absolute value such that $|p|_p = p^{-1}$. For instance:

$$|\gamma|_p = |N_{K(\gamma)/\mathbb{Q}_p}(\gamma)|_p^{1/[K(\gamma):\mathbb{Q}_p]} = |p|_p^{1/[K(\gamma):K]} = p^{-1/(p-1)} \quad ,$$

where $N_{K(\gamma)/\mathbb{Q}_p}$ stands for the norm from $K(\gamma)$ to $\mathbb{Q}_p$. We denote by ord_p the associated valuation: for $a \in \mathbb{C}_p$, $|a|_p = p^{-\mathrm{ord}_p(a)}$. For $r \in \mathbb{R}$, let $D(r^-) = \{a \in \mathbb{C}_p : |a|_p < r\}$ (resp. $D(r^+) = \{a \in \mathbb{C}_p : |a|_p \leqslant r\}$) denote the so-called open (resp. closed) disc of radius r about 0.

The radius of convergence of a series $\sum_n a_n X^n$ with coefficients in $\mathbb{C}_p$ is $\left(\limsup |a_n|_p^{1/n}\right)^{-1}$; it equals the largest real number r such that the series converges in $D(r^-)$, see [Kob77, IV1]. From standard theory, we know that the radius of convergence of exp is $p^{-1/(p-1)}$. If we write $E_\gamma(X) = \sum_{n \geqslant 0} e_n X^n$, then $|e_n|_p^{1/n} \leqslant p^{(1-p)/p^2}$ for all positive n by [Lan80, 14 Lemma 2.2(i)], therefore the radius of convergence of E_γ is at least $p^{(p-1)/p^2}$. In particular, E_γ converges on $D(1^+)$, hence on $\mathfrak{O}_K$. Note that one has $E_\gamma(a) = \exp(\gamma a - \gamma a^p)$ for $a \in D(1^-)$, because then $|\gamma a - \gamma a^p|_p = |\gamma a|_p < p^{-1/(p-1)}$, but this expression can not be used when $|a|_p = 1$: the image of the unit circle of $\mathbb{C}_p$ by $\gamma X - \gamma X^p$ is not contained in the disk of convergence of exp. For such an a, only the series in e_n's is available.

Nevertheless, if $a \in D(1^+)$ then $|p\gamma a|_p \leqslant |p\gamma|_p < p^{-1/(p-1)}$, and the same holds for $|p\gamma a^p|_p$. Using the homomorphic property of the exponential power series, we deduce that:

$$E_\gamma(a)^p = \exp(p\gamma a)\exp(-p\gamma a^p) \quad .$$

In particular $E_\gamma(1)$ is a p-th root of unity. By [Lan80, 14 Lemma 2.2(ii)] and the power series expansion of exp we get:

$$E_\gamma(X) \equiv 1 + \gamma X \mod \gamma^2 \mathfrak{O}_{\mathbb{Q}_p(\gamma)}[[X]] \quad . \tag{11}$$

This shows that $E_\gamma(1)$ is in fact a primitive p-th root of unity. Further the different choices of γ correspond to the different choices of this root of unity; therefore we may choose γ so that $E_\gamma(1) = \zeta$, where ζ was defined in subsection 3.2. We remark that $[K(\zeta) : K] = [K(\gamma) : K]$ and $\zeta \in K(\gamma)$, therefore $K(\gamma) = K(\zeta)$; we shall now denote this field by K'.

Formula (11) also shows that if we let $u \in \mathfrak{O}_K$ be a unit, then $E_\gamma(u) - 1$ is a uniformising parameter in K'.

Let $\mu \in \mathbb{Z}_p$ and set $B_\mu(X) = \sum_{n\geqslant 0} \frac{\mu(\mu-1)\ldots(\mu-n+1)}{n!} X^n$. This series belongs to $\mathbb{Z}_p[[X]]$ and converges on $D(1^-)$, see [Kob77, p.81]. For any sequence of rational integers $(\mu_i)_i$ converging towards μ, one has $B_\mu(X) = \lim_i B_{\mu_i}(X)$ (coefficient-wise). Further the μ_i's can be taken to be positive, in which case $B_{\mu_i}(X) = (1+X)^{\mu_i}$, so we may abbreviate notations writing $B_\mu(X) = (1+X)^\mu$. Using the fact that $\exp(X)^{\mu_i} = \exp(\mu_i X)$ for every i, and taking the limit of the coefficients when i goes to infinity, one deduces that:

$$\exp(\mu X) = \exp(X)^\mu \ .$$

We consider the power series $E_\gamma(X)^\mu = B_\mu\big(E_\gamma(X)-1\big)$, and see using (11) that it converges on $D(1^+)$. Substituting μX for X in E_γ yields a power series $E_\gamma(\mu X)$ that also converges on $D(1^+)$. Further, let μ_{p-1} denote the subgroup of $\mathbb{Z}_p^\times$ of $(p-1)$-th roots of unity. We get:

LEMMA 4.2. *Let $\mu \in \mu_{p-1}$, then $E_\gamma(\mu X) = E_\gamma(X)^\mu$.*

Proof. The result is straightforward since

$$\exp\big(\gamma\mu X - \gamma(\mu X)^p\big) = \exp\big(\mu(\gamma X - \gamma X^p)\big) = \exp(\gamma X - \gamma X^p)^\mu \ .$$

□

4.2 The Kummer extensions in $K_{p,2}$

Throughout this section we will sometimes identify the multiplicative groups of the residue fields k and $\mathbb{Z}_p/p\mathbb{Z}_p$ with their Teichmüller lifts. Namely let μ_{q-1} and μ_{p-1} denote the groups of roots of unity of order prime to p in K and $\mathbb{Q}_p$ respectively, then $k^\times \cong \mu_{q-1}$ and $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times \cong \mu_{p-1}$. Specifically,

$$\mathfrak{O}_K^\times = \mu_{q-1} \times (1+p\mathfrak{O}_K) \quad \text{and} \quad \mathbb{Z}_p^\times = \mu_{p-1} \times (1+p\mathbb{Z}_p) \ .$$

Since $K/\mathbb{Q}_p$ is unramified, we shall also identify its Galois group and that of the residue extension, and set $\Sigma = \mathrm{Gal}(k/(\mathbb{Z}_p/p\mathbb{Z}_p)) = \mathrm{Gal}(K/\mathbb{Q}_p)$.

We now let η be a normal basis generator for k over $\mathbb{Z}_p/p\mathbb{Z}_p$ and as described we will often think of η as actually lying in $\mathfrak{O}_K^\times$. The conjugates of η under Σ are the η^{p^j}, $0 \leqslant j \leqslant d-1$, so each $u \in k$ has a unique decomposition:

$$u = \sum_{j=0}^{d-1} u_j \eta^{p^j} \ ,$$

with coefficients $u_j \in \mathbb{Z}_p/p\mathbb{Z}_p$. For ease of notation we identify $0 \in \mathbb{Z}_p/p\mathbb{Z}_p$ and $0 \in \mathfrak{O}_K$, so that each $u_j \in \mathbb{Z}_p/p\mathbb{Z}_p$ can be seen as an element $u_j \in \{0\} \cup \mu_{p-1} \subset \mathbb{Z}_p$. To $u \in k$ as above we associate:

$$x_u = \prod_{j=0}^{d-1} E_\gamma\big(\eta^{p^j}\big)^{u_j} = \prod_{j=0}^{d-1} E_\gamma\big(u_j\eta^{p^j}\big) \ \in \ K' \tag{12}$$

(recall K' contains γ and is a complete field). The second equality comes from Lemma 4.2; note that x_u does not equal $E_\gamma(u)$ since E_γ is not a group homomorphism on the additive group $D(1)^+$. Further $x_0 = 1$ and when $u \in k^\times$, it follows from Formula (11) that $x_u \equiv 1 + \gamma u \mod \gamma^2\mathfrak{O}_{K'}$, so $x_u - 1$ is a uniformising parameter in K'.

PROPOSITION 4.3. *There are exactly $r = \frac{p^d-1}{p-1}$ degree p extensions of K' contained in $K_{p,2}$, given by $L_i = K'M_i$, $1 \leqslant i \leqslant r$. Further $k^\times/(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ is in one-to-one correspondence with the set $\{L_i,\ 1 \leqslant i \leqslant r\}$ via the map $\bar{u} \mapsto K'\big(x_u^{1/p}\big)$.*

Proof. From [Pic09, Theorem 5], we know that every degree p extension of K' contained in $K_{p,2}$ is generated by the p-th root of an element $\prod_{j=0}^{d-1} E_\gamma\big(\eta^{p^j}\big)^{n_j}$, with exponents $n_j \in \{0,1,\ldots,p-1\}$, not

all zero. (In fact the statement in [Pic09] requires one element in the basis of k over $\mathbb{Z}_p/p\mathbb{Z}_p$ to equal 1, but this is never used in the proof, so we can use a normal basis here instead.) To such an element corresponds a unique $u = \sum_j u_j \eta^{p^j} \in k^\times$, where u_j is the coset of n_j modulo $p\mathbb{Z}_p$. Let us lift each u_j in $\{0\} \cup \mu_{p-1} \subset \mathbb{Z}_p$ and write $u_j = n_j + pm_j$ with $m_j \in \mathbb{Z}_p$, then

$$x_u = \prod_{j=0}^{d-1} E_\gamma\big(\eta^{p^j}\big)^{n_j} \cdot \left(\prod_{j=0}^{d-1} E_\gamma\big(\eta^{p^j}\big)^{m_j}\right)^p .$$

We conclude that the degree p extension of K' contained in $K_{p,2}$ are the $L_{(u)} = K'\big(x_u^{1/p}\big)$ for $u \in k^\times$.

Multiplying u by an element μ in $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ changes x_u to $x_{\mu u} = {x_u}^\mu$. If we let $\mu = n + p\mu'$ with $n \in \{1, \dots, p-1\}$ and $\mu' \in \mathbb{Z}_p$, we find that $x_{\mu u}$ equals a prime to p power of x_u multiplied by the p-th power of an element of K', so its p-th root generates the same extension of K' as that of x_u. Therefore the map given in the statement is well defined and surjective. For any integer $1 \leqslant i \leqslant r$, the compositum $M_i K' = L_i$ is a degree p extension of K' contained in $K_{p,2}$, so we get that the map is a one-to-one correspondence. □

Remark 4.4. *Keeping the notations of the proof, it would be nice to show that $L_{(u)}$ is also generated by the p-th root of $E_\gamma(u)$. We would then get a generating set (for the degree p extensions of K' contained in $K_{p,2}$) that would not depend on the choice of a basis of k over $\mathbb{Z}_p/p\mathbb{Z}_p$. However, the fact that E_γ is not homomorphic on the additive group $D(1)^+$ does not make this goal easy to achieve.*

4.3 Lifting Galois automorphisms

We now set $L = K'M$, thus by the former result $L = K'(x_\varepsilon^{1/p})$ for an element ε of $k^\times$ which is uniquely determined modulo $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ by M. We fix ε for the rest of the paper and we set $x = x_\varepsilon$ for brevity. We describe our field extensions in Figure 1 below, where we let $H = \mathrm{Gal}(M/K)$, $\Delta = \mathrm{Gal}(L/M)$.

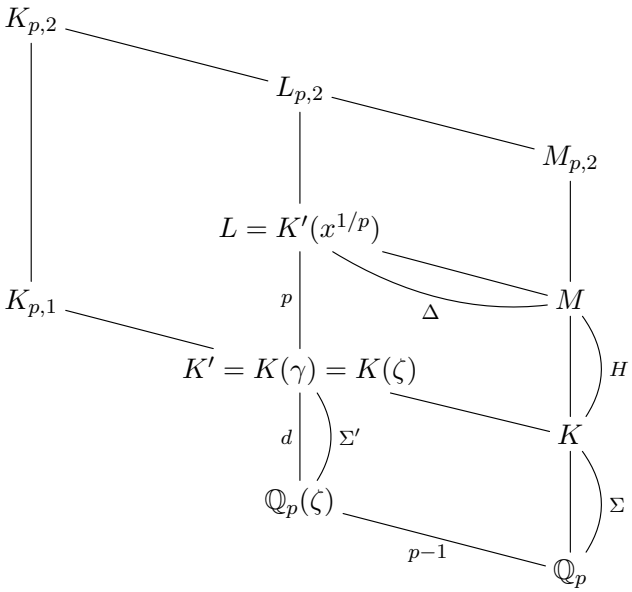


Figure 1. Extensions diagram

We need to study how the elements of $\mathrm{Gal}(K'/K)$ and $\Sigma' = \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta))$ can be respectively

lifted to automorphisms of L (recall that $L \subset K^{ab}$) and of the Galois closure $\widetilde{L}$ of $L/\mathbb{Q}_p(\zeta)$.

We have the following group isomorphisms:

$$\begin{array}{ccccc} \mu_{p-1} & \cong & (\mathbb{Z}_p/p\mathbb{Z}_p)^\times & \cong & \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \cong \mathrm{Gal}(K'/K) \\ \mu & \longmapsto & \mu \mod p & \longmapsto & (s_\mu : \zeta \mapsto \zeta^\mu) \end{array}$$

As a consequence of Formula (11) in Subsection 4.1, we know that $x-1$ is a uniformising parameter of K. As noted in [Pic09] before Lemma 9, it implies that $x^{1/p}-1$ is a uniformising parameter of L. It follows that both $x-1$ and $x^{1/p}-1$ belong to $D(1^-)$, so we may consider raising x and $x^{1/p}$ to the μ-th power for any $\mu \in \mathbb{Z}_p$. Lemma 10 of [Pic09] applied to x (with appropriate choices of the exponents n_i) yields that, for any $\mu \in \mu_{p-1}$:

$$s_\mu(x) = x^\mu \ .$$

Since $[L : K'] = p$, each automorphism $s_\mu \in \mathrm{Gal}(K'/K)$ has p distinct liftings in $\mathrm{Gal}(L/K)$, which are determined by their value at $x^{1/p}$. More precisely, let us fix a p-th root of $s_\mu(x)$ in L, by setting

$$s_\mu(x)^{1/p} = \left(x^{1/p}\right)^\mu = x^{\mu/p} \ ,$$

where $x^{1/p}$ is our previous (implicit) choice of a p-th root of x. Any lifting $\widetilde{s}$ of s_μ satisfies $\widetilde{s}\left(x^{1/p}\right)^p = s_\mu(x)$, so there exists an integer $n \in \{0, \dots, p-1\}$ such that $\widetilde{s}(x^{1/p}) = \zeta^n s_\mu(x)^{1/p}$, and n determines $\widetilde{s}$. One easily checks that, for any integer k:

$$\widetilde{s}^k(x^{1/p}) = \zeta^{nk\mu^{k-1}} x^{\mu^k/p} \ ,$$

so $\widetilde{s}^{p-1} = 1$ if and only if $n = 0$. Further, in this case, one obtains that $\widetilde{s}$ has the same order in $\mathrm{Gal}(L/K)$ as μ in μ_{p-1}. We have thus proved:

Proposition 4.5. *Let μ denote a primitive $(p-1)$-th root of unity. Then $\mathrm{Gal}(L/K)$ contains exactly one element $\widetilde{s}_\mu$ that maps ζ to ζ^μ and which is of order $p-1$, hence generates Δ and fixes M. Further $\widetilde{s}_\mu(x^{1/p}) = x^{\mu/p}$.*

We now consider extending automorphisms in $\Sigma' = \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta))$. Since γ is fixed by Σ', one checks that $\sigma(x) = x_{\sigma(\varepsilon)}$ for any $\sigma \in \Sigma'$. Therefore, by Kummer theory, $L/\mathbb{Q}_p(\zeta)$ is Galois if and only if every $x_{\sigma(\varepsilon)}$ can be written as $x^m y^p$ for some integer m prime to p and some $y \in K'$. Using the fact that the elements of Σ' act on η by raising it to its p^n-th power for $n \in \{0, 1, \dots, d-1\}$, one then checks that this only happens when $\varepsilon = t \sum_{n=0}^{d-1} s^{d-n-1} \eta^{p^n}$ for some $s, t \in (\mathbb{Z}_p/p\mathbb{Z}_p)^\times$ with s of order dividing d. In particular, $s = 1$ yields $L = K(\xi) = K.\mathbb{Q}_p(\xi)$ which is always Galois over $\mathbb{Q}_p(\zeta)$ — recall ξ and ζ were defined in Equation (3).

Since $L/\mathbb{Q}_p(\zeta)$ is not Galois in the general case, we consider the Galois closure $\widetilde{L}$ of $L/\mathbb{Q}_p(\zeta)$, given by $\widetilde{L} = K'(\{\sigma(x)^{1/p} : \sigma \in \Sigma'\})$. The extension $\widetilde{L}/K'$ is Kummer and its Galois group is p-elementary abelian, of order p^m for some integer m (equal to 1 if and only if $L/\mathbb{Q}_p(\zeta)$ is Galois). Let $\sigma_1 = 1$ and $\sigma_2, \dots, \sigma_m \in \Sigma'$ be such that $\widetilde{L}$ is the compositum of the m degree p extensions $K'(\sigma_n(x)^{1/p})$, $1 \leqslant n \leqslant m$, of K'. Any $\sigma \in \Sigma'$ extends to $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}_p(\zeta))$ in $p^m = [\widetilde{L} : K']$ different ways, determined by the values at the $\sigma_n(x)^{1/p}$, $1 \leqslant n \leqslant m$. More precisely, let us fix a p-th root of $\sigma\sigma_n(x)$ for each $n \in \{1, \dots, m\}$, then a lifting $\widetilde{\sigma}$ of σ is determined by the integers $k(n) \in \{0, 1, \dots, p-1\}$ such that, for any n, $\widetilde{\sigma}\left(\sigma_n(x)^{1/p}\right) = \zeta^{k(n)} \left(\sigma\sigma_n(x)\right)^{1/p}$. The choices of the $k(n)$ for all the n yield the p^m possible liftings of σ, hence each of these choices is realised. In particular, taking $k(1) = 0$, we see that there exists a lifting $\widetilde{\sigma}$ of σ to $\widetilde{L}$ such that

$$\widetilde{\sigma}(x^{1/p}) = \sigma(x)^{1/p} \ , \tag{13}$$

for any prior choice of a p-th root of $\sigma(x)$. We deduce the following result. Let $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ denote the norm of x from K' to $\mathbb{Q}_p(\zeta)$.

Proposition 4.6. *For any choice of a p-th root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$, there exists a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ such that each $\omega \in \Omega$ fixes ζ and*

$$\prod_{\omega\in\Omega} \left(x^{1/p}\right)^{\omega} = N_{K'/\mathbb{Q}_p(\zeta)}(x)^{1/p} \ .$$

Proof. Since $K/\mathbb{Q}_p$ is Galois, choosing a transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ is the same as choosing a way to extend the elements of $\Sigma = \mathrm{Gal}(K/\mathbb{Q}_p)$ to act on $\mathbb{Q}_p^c$. By Galois theory, we know that there is only one way to extend them to Σ'. Let $\sigma \in \Sigma'$, then for any choice of a p-th root of $\sigma(x)$, there exists $\omega_\sigma \in \Omega_{\mathbb{Q}_p}$ that extends the lifting $\widetilde{\sigma}$ of σ defined in (13), namely:

$$\left(x^{1/p}\right)^{\omega_\sigma} = \widetilde{\sigma}(x^{1/p}) = \sigma(x)^{1/p} \ .$$

The set $\Omega = \{\omega_\sigma, \sigma \in \Sigma'\}$ defined this way is a transversal of Ω_K in $\Omega_{\mathbb{Q}_p}$, and

$$\prod_{\omega\in\Omega} \left(x^{1/p}\right)^{\omega} = \prod_{\sigma\in\Sigma'} \sigma(x)^{1/p} \ ,$$

which can be made to equal any p-th root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ for a suitable choice of the p-th roots of the $\sigma(x)$, $\sigma \in \Sigma'$. By construction the restriction of each $\omega \in \Omega$ to K' belongs to Σ', hence fixes ζ. □

4.4 The Norm-Resolvent

We begin by exhibiting a (self-dual) normal basis generator for the square root of the inverse different $\mathcal{A}_{M/K}$, which we then use to compute the norm-resolvent involved in $\mathcal{RT}_K^\star(M)$. Recall x has been defined at the beginning of Subsection 4.3.

Lemma 4.7. *Let*

$$\alpha_M = \frac{1 + Tr_\Delta(x^{1/p})}{p} \ ,$$

then α_M is a self-dual normal basis generator for $\mathcal{A}_{M/K}$.

Proof. This Lemma is a consequence of [Pic09, Theorem 12]. □

The extension L/K' is Kummer with generator $x^{1/p}$ so its Galois group is generated by the automorphism defined by $x^{1/p} \mapsto \zeta x^{1/p}$. Further by Galois theory the restriction of this automorphism to M generates $H = \mathrm{Gal}(M/K)$. This enables us to fix a generator h of H and the irreducible character χ of $\mathrm{Gal}(M/K)$ such that M is the fixed subfield of $M_{p,2}$ by $\ker(\chi)$ (this condition only determines χ up to a prime to p power).

Notation 4.8. *Let $\widetilde{h} \in \mathrm{Gal}(L/K')$ be such that $\widetilde{h}\left(x^{1/p}\right) = \zeta x^{1/p}$ and set $h = \widetilde{h}|_M$. Let χ be the irreducible character of $\mathrm{Gal}(M_{p,2}/K)$ such that $\ker(\chi) = \mathrm{Gal}(M_{p,2}/M)$ and $\chi(h) = \zeta$.*

We can now state the theorem that we will prove in this subsection. Recall the notations from Equation (3) and that $Tr = Tr_{K/\mathbb{Q}_p}$.

Theorem 4.9. *There exists a choice of the transversal Ω defining the norm-resolvent such that $\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi_0) = 1$ and, for any $j \in \{1, \ldots, p-1\}$:*

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j) = \xi^{j(2-j^{1-p})Tr(\varepsilon)} \ ,$$

where j^{1-p} is the inverse of j^{p-1} in $\mathbb{Z}_p$.

Before we can prove this theorem we must calculate the properties of certain elements. We begin with the computation of the norm $N_{K'/\mathbb{Q}_p(\zeta)}(x)$, which establishes a new link between x and ε.

LEMMA 4.10. $N_{K'/\mathbb{Q}_p(\zeta)}(x) = \zeta^{Tr(\varepsilon)}$.

Proof. Recall that $\Sigma' = \mathrm{Gal}\big(K'/\mathbb{Q}_p(\zeta)\big)$ fixes $\gamma \in \mathbb{Q}_p(\zeta)$ so, if $\sigma \in \Sigma'$ and $u \in \mathfrak{O}_K$, $\sigma\big(E_\gamma(u)\big) = E_\gamma\big(\sigma(u)\big)$; further σ acts on η by raising it to the power p^n for some $0 \leqslant n \leqslant d-1$, and fixes μ_{p-1}. Therefore, writing $\varepsilon = \sum_j e_j \eta^{p^j}$ with coefficients $e_j \in \mathbb{Z}_p/p\mathbb{Z}_p$:

$$N_{K'/\mathbb{Q}_p(\zeta)}(x) = \prod_{n=0}^{d-1} \prod_{j=0}^{d-1} E_\gamma\big(\eta^{p^{n+j}}\big)^{e_j} \quad .$$

For each $0 \leqslant j, n \leqslant d-1$, consider the power series $E_\gamma\big(\eta^{p^{n+j}} X\big)$, obtained by substituting $\eta^{p^{n+j}} X$ for X in E_γ; it converges on $D(1^+)$ and

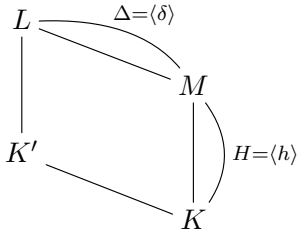
$$\begin{aligned}\prod_{n=0}^{d-1} E_\gamma\big(\eta^{p^{n+j}} X\big) &= \exp\Big(\sum_{n=0}^{d-1} \big(\gamma\eta^{p^{n+j}} X - \gamma\eta^{p^{n+j+1}} X^p\big)\Big) \\ &= \exp\big(Tr(\eta)(\gamma X - \gamma X^p)\big) \\ &= E_\gamma(X)^{Tr(\eta)} \quad ,\end{aligned}$$

that also converges on $D(1^+)$. Evaluating at $X = 1$ and using the above formula for the norm yields the result, since $Tr(\varepsilon) = Tr(\eta)\sum_j e_j$. □

In view of Proposition 4.6, we now fix our transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$ so that each $\omega \in \Omega$ fixes ζ and the product of the Ω-conjugates of $x^{1/p}$ equals $\xi^{Tr(\varepsilon)}$, which is a p-th root of $N_{K'/\mathbb{Q}_p(\zeta)}(x)$ by the preceding Lemma. We get:

LEMMA 4.11. $\prod_{\omega\in\Omega} \big(x^{1/p}\big)^\omega = \xi^{Tr(\varepsilon)}$.

Recall that $\mathrm{Gal}(M/K) = H = \langle h\rangle$, where h is as in Notation 4.8. Let $\mathrm{Gal}(L/M) = \Delta = \langle\delta\rangle$, then by Proposition 4.5, $\delta = \widetilde{s}_\mu$ for some primitive $(p-1)$-th root of unity μ, and $\delta(\zeta) = \zeta^\mu$, $\delta(x^{1/p}) = x^{\mu/p}$.



We now compute the resolvent for the normal basis generator α_M that was defined in Lemma 4.7.

PROPOSITION 4.12. *One has* $(\alpha_M \mid \chi_0) = 1$ *and, for* $j \in \{1, \ldots, p-1\}$*:*

$$(\alpha_M \mid \chi^j) = (x^{1/p})^{\mu^s} \quad ,$$

where $0 \leqslant s \leqslant p-2$ *is such that* $\mu^s \equiv j \mod p$.

Proof. The definitions of the resolvent and of α_M yield:

$$(\alpha_M \mid \chi^j) = \sum_{t=0}^{p-1} \frac{1 + h^t\big(Tr_\Delta(x^{1/p})\big)}{p}\, \chi^j(h^{-t}) \quad .$$

Let $t \in \{0, 1, \ldots, p-1\}$, then:

$$h^t\big(Tr_\Delta(x^{1/p})\big) = \sum_{s=0}^{p-2} \widetilde{h}^t\left(\big(x^{1/p}\big)^{\mu^s}\right) = \sum_{s=0}^{p-2} \zeta^{t\mu^s} \big(x^{1/p}\big)^{\mu^s} \quad .$$

If $j = 0$, then χ^j is the trivial character χ_0, so that:

$$(\alpha_M \mid \chi_0) = 1 + \frac{1}{p}\sum_{t=0}^{p-1}\sum_{s=0}^{p-2}\zeta^{t\mu^s}\left(x^{1/p}\right)^{\mu^s} = 1 + \frac{1}{p}\sum_{s=0}^{p-2}\left(\sum_{t=0}^{p-1}\zeta^{t\mu^s}\right)\left(x^{1/p}\right)^{\mu^s}$$

and $\sum_{t=0}^{p-1}\zeta^{t\mu^s} = 0$, so $(\alpha_M \mid \chi_0) = 1$.

We now assume $j \neq 0$. Since $\chi^j(h) = \zeta^j$, hence $\sum_{t=0}^{p-1}\chi^j(h^{-t}) = 0$, we get

$$(\alpha_M \mid \chi^j) = \frac{1}{p}\sum_{s=0}^{p-2}\left(\sum_{t=0}^{p-1}\zeta^{t(\mu^s-j)}\right)\left(x^{1/p}\right)^{\mu^s} \ ;$$

we observe that

$$\sum_{t=0}^{p-1}\zeta^{t(\mu^s-j)} = \begin{cases} p & \text{if } \mu^s \equiv j \mod p, \\ 0 & \text{otherwise,} \end{cases}$$

hence the result. □

We are now in a position to prove Theorem 4.9.

Proof of Theorem 4.9. When $j = 0$ the result is clear. We now assume that $j \neq 0$. Recall the choice we made before Lemma 4.11 for our transversal Ω of Ω_K in $\Omega_{\mathbb{Q}_p}$. Since χ^j takes values in $\mathbb{Q}_p(\zeta)$, which is fixed by Ω, Definition 2.2 of the norm-resolvent yields:

$$\begin{aligned}\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j) &= \prod\nolimits_{\Omega}(\alpha_M \mid \chi^j)^{\omega} = \prod\nolimits_{\Omega}\left((x^{1/p})^{\mu^s}\right)^{\omega} \\ &= \left(\prod\nolimits_{\Omega}(x^{1/p})^{\omega}\right)^{\mu^s} = \xi^{\mu^s Tr(\varepsilon)}\end{aligned}$$

using Lemma 4.11. Writing $\mu^s \equiv j + ap \mod p^2$ for some $a \in \{0, 1, \ldots, p-1\}$ and raising to the $(p-1)$-th power yields $1 \equiv j^{p-1} - apj^{p-2} \mod p^2$, thus:

$$ap \equiv (j^{p-1} - 1)j^{2-p} \equiv j - j^{2-p} \mod p^2 \ .$$

It follows that $\mu^s \equiv j(2 - j^{1-p}) \mod p^2$, which ends the proof of Theorem 4.9. □

4.5 The modified twisted Galois Gauss Sum

Recall from Notation 4.8 that χ is the character of $\mathrm{Gal}(M_{p,2}/K)$ such that M is the fixed field of $\ker(\chi)$ and $\chi(h) = \zeta$ for our choice of generator h of $H = \mathrm{Gal}(M/K)$. Our character χ is weakly ramified so we know by Corollary 3.10 that there exists $v \in \mathfrak{O}_K^{\times}$ such that:

$$\forall\, u \in \mathfrak{O}_K\ , \quad \chi(1+up)^{-1} = \zeta^{Tr(uv)} \ . \tag{14}$$

We are going to show that v can be chosen so that its trace from K to $\mathbb{Q}_p$ equals that of ε. In order to do that, we need some properties of the p-th Hilbert symbol (see [FV02, Ch.IV]). We have $\mathrm{char}(K') = 0$ and $\zeta \in K'$. Let $\mu_p = \langle\zeta\rangle$ denote the group of p-th roots of unity in $\mathbb{Q}_p^c$. The p-th Hilbert symbol of K' is defined as

$$\begin{aligned}(\ ,\ )_{p,K'}: \quad K'^{\times}\times K'^{\times} &\longrightarrow \mu_p \\ (a,b) &\longmapsto \frac{\theta_{K'}(a)(b^{1/p})}{b^{1/p}} \ .\end{aligned}$$

PROPOSITION 4.13. *For all $u \in \mathfrak{O}_K$, we have:*

$$(1+up,x)_{p,K'} = \chi(1+up)^{-1} \ .$$

Proof. The proof is in several steps. Let $L_{p,2}$ be the compositum of the fields L_i for $i \in \{1,\dots,r\}$. Recall that we identify the residue field $k = \{0\} \cup k^\times$ with $\{0\} \cup \mu_{q-1} \subset \mathfrak{O}_K$ through Teichmüller's lifting. We first show:

LEMMA 4.14. $\mathrm{Gal}(L_{p,2}/K') = \theta_{L_{p,2}/K'}(U_K^1/U_K^2) = \{\theta_{L_{p,2}/K'}(1+up) : u \in k\}$.

Proof. First note that $L_{p,2} \subset K_{p,2}$, so $\theta_{L_{p,2}/K}$ is trivial on U_K^2 and the same holds for $\theta_{L_{p,2}/K'}$ (for instance using [Iwa86, Theorem 6.16]). Hence we may consider $\theta_{L_{p,2}/K'}(U_K^1/U_K^2)$, which as a set clearly equals $\{\theta_{L_{p,2}/K'}(1+up) : u \in k\}$.

By local class field theory, $\mathrm{Gal}(M_{p,2}/K) = \theta_{M_{p,2}/K}(U_K^1)$ and the intersection of the kernel of $\theta_{M_{p,2}/K}$ with U_K^1 is U_K^2 (since $M_{p,2} \subset K_{p,2}$ and $[M : K] = q$). It follows that $\mathrm{Gal}(M_{p,2}/K) = \theta_{M_{p,2}/K}(U_K^1/U_K^2)$.

Since $L_{p,2} = M_{p,2}K'$ with K'/K and $M_{p,2}/K$ linearly disjoint, the functorial properties of the Artin reciprocity map yield [Iwa86, Theorem 6.9]:

$$\theta_{L_{p,2}/K'}\big|_{M_{p,2}} = \theta_{M_{p,2}/K} \circ N_{K'/K} \ , \tag{15}$$

where $N_{K'/K}$ stands for the norm from K' to K. For $u \in k$ we have $1+up \in \mathfrak{O}_K$, so $N_{K'/K}(1+up) = (1+up)^{p-1} \equiv 1-up \mod p^2\mathfrak{O}_K$. We get that $N_{K'/K}$ is an isomorphism from U_K^1/U_K^2 into itself, and therefore

$$\theta_{L_{p,2}/K'}(U_K^1/U_K^2)\big|_{M_{p,2}} = \mathrm{Gal}(M_{p,2}/K) \ .$$

This yields the result using Galois theory, since the restriction map $g \mapsto g|_{M_{p,2}}$ is an isomorphism from $\mathrm{Gal}(L_{p,2}/K')$ to $\mathrm{Gal}(M_{p,2}/K)$. □

LEMMA 4.15. *There exists $t \in \{1,\dots,p-1\}$ such that, for all $u \in k$,*

$$(1+up,x)_{p,K'}^t = \chi(1+up)^{-1} \ .$$

Proof. By definition, $\chi(1-up) = 1$ if and only if $\theta_{M_{p,2}/K}(1-up)$ fixes M. This is in turn equivalent to $\theta_{L_{p,2}/K'}(1+up)$ fixing L, since $L = MK'$ and we know by (15) that $\theta_{L_{p,2}/K'}(1+up)$ is the only lifting of $\theta_{M_{p,2}/K}(1-up)$ to $L_{p,2}/K'$. Since $L = K'(x^{1/p})$ and by definition of the Hilbert symbol, we get:

$$\chi(1-up) = 1 \Leftrightarrow (1+up,x)_{p,K'} = 1 \ .$$

The properties of the Hilbert symbol and the fact that $\theta_{L_{p,2}/K'}$ is trivial on U_K^2 give us

$$\begin{aligned}(1+up,x)_{p,K'}(1+u'p,x)_{p,K'} &= (1+up+u'p+uu'p^2,x)_{p,K'} \\ &= (1+(u+u')p,x)_{p,K'}\end{aligned}$$

for $u, u' \in k$, which means that $u \mapsto (1+up,x)_{p,K'}$ is a character of the additive group of k. We also know that $u \mapsto \chi(1-up)$ is a character of the additive group of k (since $u \mapsto \theta_{M_{p,2}/K}(1-up)$ is). Therefore $u \mapsto (1+up,x)_{p,K'}$ and $u \mapsto \chi(1-up)$ are characters of the same p-elementary abelian group which have the same kernel of index p. It follows that $(1+up,x)_{p,K'}^t = \chi(1-up) = \chi(1+up)^{-1}$ for some t. □

To finish the proof of Proposition 4.13, note that the arguments in the proof of Lemma 4.14 can be adjusted to show that $\mathrm{Gal}(L/K') = \langle \theta_{L/K'}(1+ap) \rangle$ for an adequate element $a \in \mathfrak{O}_K$. Hence there

exists an integer $n \in \{1, \dots, p-1\}$ such that

$$\widetilde{h} = \theta_{L/K'}(1+ap)^n = \theta_{L/K'}\big((1+ap)^n\big) = \theta_{L/K'}\big(1+wp+p^2b\big) \ ,$$

for some $b \in \mathfrak{O}_K$, where we let $w \in \mu_{q-1}$ be such that $w \equiv na \mod p\mathbb{Z}_p$. Since $\theta_{L/K'}\big(1+wp+p^2b\big)|_M = \theta_{M/K}(1-wp) = \theta_{L/K'}(1+wp)|_M$, we get that

$$\widetilde{h} = \theta_{L/K'}(1+wp) \quad \text{and} \quad h = \widetilde{h}|_M = \theta_{M/K}(1-wp) \ ,$$

hence

$$\chi(1+wp)^{-1} = \chi(1-wp) = \chi(h) = \zeta = \frac{\widetilde{h}(x^{1/p})}{x^{1/p}} = (1+wp, x)_{p,K'} \ ,$$

which implies $t = 1$ in the preceding lemma. □

We can now show the announced result, recalling that $Tr = Tr_{K/\mathbb{Q}_p}$.

Corollary 4.16. *There exists $v_\chi \in \mathfrak{O}_K^\times$ such that v_χ satisfies condition (14) from Corollary 3.10 for χ and $Tr(v_\chi) = Tr(\varepsilon)$.*

Proof. Throughout this proof we fix $u \in \mathbb{Z}_p/p\mathbb{Z}_p$. We let ver : $\Omega^{ab}_{\mathbb{Q}_p} \to \Omega^{ab}_{\mathbb{Q}_p(\zeta)}$ be the transfer map from $\mathbb{Q}_p$ to $\mathbb{Q}_p(\zeta)$. From [Iwa86, Theorem 6.16 and Formula (3) p.93], where ver is denoted as $t_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}$, we know that:

$$\theta_{\mathbb{Q}_p(\zeta)}(1+up) = \text{ver}\left(\theta_{\mathbb{Q}_p}(1+up)\right) = \prod_{\tau \in \text{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} \tau\, \theta_{\mathbb{Q}_p}(1+up)\, \tau^{-1} \ .$$

As $\text{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ and $\Omega^{ab}_{\mathbb{Q}_p}$ commute, we get $\theta_{\mathbb{Q}_p(\zeta)}(1+up) = \theta_{\mathbb{Q}_p}(1+up)^{p-1}$. By [Ser67, §3.1 Remark after Theorem 2], we know that $\theta_{\mathbb{Q}_p}(1+up)(\xi) = \xi^{1-up}$, so that:

$$\theta_{\mathbb{Q}_p(\zeta)}(1+up)(\xi) = \xi^{1+up} \ . \tag{16}$$

Using the properties of the Hilbert symbol we make the following derivation.

$$\begin{aligned}
(1+up, x)_{p,K'} &= (1+up, N_{K'/\mathbb{Q}_p(\zeta)}(x))_{p,\mathbb{Q}_p(\zeta)} && \text{(from [FV02, IV§5])} \\
&= \big(1+up, \zeta^{Tr(\varepsilon)}\big)_{p,\mathbb{Q}_p(\zeta)} && \text{(from Lemma 4.10)} \\
&= \big(1+up, \zeta\big)^{Tr(\varepsilon)}_{p,\mathbb{Q}_p(\zeta)} = \left(\frac{\theta_{\mathbb{Q}_p(\zeta)}(1+up)(\xi)}{\xi}\right)^{Tr(\varepsilon)} \\
&= \left(\frac{\xi^{1+up}}{\xi}\right)^{Tr(\varepsilon)} && \text{(from Equation (16))} \\
&= (\xi^{up})^{Tr(\varepsilon)} = \zeta^{uTr(\varepsilon)}
\end{aligned}$$

On the other hand, let $v \in \mathfrak{O}_K^\times$ satisfying condition (14). Then from Proposition 4.13 we know that $(1+up, x)_{p,K'} = \chi(1+up)^{-1} = \zeta^{Tr(uv)}$, and so we have

$$(1+up, x)_{p,K'} = \zeta^{uTr(v)} \ .$$

Comparing with the former equality, this yields $Tr(\varepsilon) \equiv Tr(v) \mod p\mathbb{Z}_p$, so let $a \in \mathbb{Z}_p$ such that $Tr(\varepsilon) = Tr(v) + pa$. Since $K/\mathbb{Q}_p$ is unramified, there exists $b \in \mathfrak{O}_K$ such that $Tr(b) = a$, so $Tr(\varepsilon) = Tr(v+pb) = Tr(v_\chi)$ if we let $v_\chi = v + pb$, which proves the result using (i) in Corollary 3.10. □

We deduce the following expression for the modified twisted Galois Gauss sum, using the statement and property (ii) of Corollary 3.10. Note that since $p \neq 2$, $\frac{p^2}{4v_\chi}\mathfrak{O}_K = \pi^2\mathfrak{O}_K$, so we may set $c_{K,2} = p^2/4v_\chi$.

THEOREM 4.17. *Let v_χ be as in Corollary 4.16 and set $c_{K,2} = p^2/4v_\chi$. Then $\tau_K^\star(\chi_0 - \chi_0^2) = 1$ and, for any $j \in \{1, \dots, p-1\}$:*

$$\tau_K^\star(\chi^j - \chi^{2j}) = \chi^j(j^{-1})\xi^{-jTr(\varepsilon)} \quad .$$

The dependency relationships between our constants might look complicated, so let us try to sum up how we fixed them. Our primitive p-th root of unity ζ came first; the extension M/K under study determined a unit ε up to $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$; we defined a Kummer generator x, then a generator h of $H = \mathrm{Gal}(M/K)$, and then a generator χ of $\widehat{H}$; with χ came the unit v_χ, but only modulo $p\mathfrak{O}_K$; the knowledge of ε enabled us to fix v_χ in Corollary 4.16 and finally $c_{K,2}$ in Theorem 4.17.

Apart from the dependency upon the choice of ζ, which is shared by the usual Galois Gauss sum, our modified Galois Gauss sum thus also depends on M. This does not prevent deducing Theorem 1 from Theorem 2 since only one extension $M_i/F_\wp$ has to be considered at each wildly and weakly ramified prime ideal $\wp$ of $\mathfrak{O}$.

4.6 The product

We can now end the proof of Theorem 2. By Theorem 4.9 and Theorem 4.17, the product of our norm-resolvent and modified twisted Galois Gauss sum is 1 when evaluated at the trivial character and we have, for $j \in \{1, \dots, p-1\}$:

$$\mathcal{N}_{K/\mathbb{Q}_p}(\alpha_M \mid \chi^j)\tau_K^\star(\chi^j - \chi^{2j}) = \left(\chi(j^{-1})\zeta^{Tr(\varepsilon)(1-j^{1-p})/p}\right)^j \quad .$$

Note that $1 - j^{1-p} \in p\mathbb{Z}_p$. We now wish to show that the above expression equals 1. We are thus left with showing that $\chi(j) = \zeta^{Tr(\varepsilon)(1-j^{1-p})/p}$, which is equivalent to $\theta_{M/K}(j) = h^{Tr(\varepsilon)(1-j^{1-p})/p}$, since $h \in H$ is such that $\chi(h) = \zeta$. It is also equivalent to showing

$$\theta_{M/K}(j)^{p-1} = h^{Tr(\varepsilon)(j^{1-p}-1)/p} \quad .$$

In order to shift this relation to $\mathrm{Gal}(L/K')$, we notice that $\theta_{M/K}(j)^{p-1} = \theta_{M/K}(N_{K'/K}(j)) = \theta_{L/K'}(j)|_M$ and recall that $\widetilde{h}|_M = h$. Thus the relation holds if and only if:

$$\theta_{L/K'}(j) = \widetilde{h}^{\,Tr(\varepsilon)(j^{1-p}-1)/p} \quad .$$

We can now evaluate these automorphisms at $x^{1/p}$, recalling that $\widetilde{h}(x^{1/p}) = \zeta x^{1/p}$ and $(j,x)_{p,K'} = \frac{\theta_{L/K'}(j)(x^{1/p})}{x^{1/p}}$, so we are left with proving:

$$(j,x)_{p,K'} = \zeta^{\,Tr(\varepsilon)(j^{1-p}-1)/p} \quad .$$

Using Lemma 4.10 and the properties of the Hilbert symbol we get:

$$(j,x)_{p,K'} = \left(j, N_{K'/\mathbb{Q}_p(\zeta)}(x)\right)_{p,\mathbb{Q}_p(\zeta)} = \left(j,\zeta\right)_{p,\mathbb{Q}_p(\zeta)}^{Tr(\varepsilon)} = \left(\frac{\theta_{\mathbb{Q}_p(\zeta)}(j)(\xi)}{\xi}\right)^{Tr(\varepsilon)} \quad .$$

From [Ser67, §3.1 Remark after Theorem 2] we know that $\theta_{\mathbb{Q}_p}(j)(\xi) = \xi^{-j}$. Therefore, reasoning as in the proof of Corollary 4.16, we get

$$\theta_{\mathbb{Q}_p(\zeta)}(j)(\xi) = \left(\mathrm{ver}\,\theta_{\mathbb{Q}_p}(j)\right)(\xi) = \theta_{\mathbb{Q}_p}(j)^{p-1}(\xi) = \xi^{j^{-(p-1)}} = \xi^{j^{1-p}} \quad ,$$

hence

$$(j,x)_{p,K'} = \left(\xi^{j^{1-p}-1}\right)^{Tr(\varepsilon)} = \left(\zeta^{(j^{1-p}-1)/p}\right)^{Tr(\varepsilon)}$$

as desired.

This ends the proof of Theorem 2, hence also of Theorem 1.

References

CNT85 Ph. Cassou-Noguès and M. J. Taylor, *Opérations d'Adams et groupe des classes d'algèbre de groupe*, J. Algebra **95** (1985), no. 1, 125–152.

Dwo64 B. Dwork, *On the Zeta Functions of a Hypersurface.II.*, Ann. of Math. **80** (1964), no. 2, 227–299.

Ere91 B. Erez, *The Galois Structure of the Square Root of the Inverse Different*, Math.Z. **208** (1991), 239–255.

Frö83 A. Fröhlich, *Galois module structure of algebraic integers*, Springer-Verlag, 1983.

FV02 I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions*, second ed., American Mathematical Society, 2002.

Iwa86 K. Iwasawa, *Local class field theory*, Oxford University Press, 1986.

Kob77 N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, New York, 1977, GTM, Vol. 58.

Lan80 S. Lang, *Cyclotomic fields ii*, Springer-Verlag, New York, 1980.

Mar77 J. Martinet, *Character theory and Artin L-functions*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 1–87.

Pic09 E. J. Pickett, *Explicit Construction of Self-Dual Integral Normal Bases for the Square-Root of the Inverse Different*, J. Number Theory **129** (2009), 1773 – 1785.

Pic10 ———, *Construction of Self-Dual Integral Normal Bases in Abelian Extensions of Finite and Local Fields*, Int. J. Number Theory **6** (2010), no. 7, 1565–1588.

Ser67 J. P. Serre, *Local class field theory*, Algebraic Number Theory (London) (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, 1967.

Ser68 ———, *Corps locaux*, Hermann, Paris, 1968.

Tat77 J. T. Tate, *Local constants*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, Prepared in collaboration with C. J. Bushnell and M. J. Taylor, pp. 89–131.

Tay81 M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), no. 1, 41–79.

Vin01 S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de* $\mathbb{Q}$, J. Number Theory **91** (2001), no. 1, 126–152.

Vin05 ———, *Galois Module Structure in Weakly Ramified 3-Extensions*, Acta Arith. **119** (2005), no. 2, 171–186.

Erik Jarl Pickett erik_pickett@hotmail.com
53, Parkfield crescent, sg4 8eq, UK.

Stéphane Vinatier stephane.vinatier@unilim.fr
XLIM - DMI, 123 avenue Albert Thomas, 87060 Limoges, France.

2.2 Sommes de Gauss, sommes de Jacobi et unités cyclotomiques associées à des modules galoisiens de torsion

Le titre de cette section est la traduction en français de l'article en préparation *Gauss sums, Jacobi sums and cyclotomic units related to torsion Galois modules*, écrit en collaboration avec Luca Caputo et en voie de soumission pour publication, d'une cinquantaine de pages. Contrairement à l'article présenté précédemment, le choix du titre de celui-ci n'a pas été évident. Il a connu de nombreux avatars, au fur et à mesure que l'article évoluait (en grossissant), jusqu'à arriver à ces *éléments explicites* qui font une bonne part de son intérêt, unités cyclotomiques (qui apparaissent habituellement plutôt en théorie d'Iwasawa) et sommes de Gauss (classiques cette fois) et de Jacobi qu'on étudie plutôt en lien avec les corps finis mais qui apparaissent aussi dans certaines versions du théorème de Stickelberger. Tous ces éléments jouent ici un rôle central (et analogues les uns aux autres) pour décrire la structure de certains modules galoisiens de torsion.

Ces modules de torsion qui apparaissent dans la seconde partie du titre font référence à un article de Chase [Cha84] qui a été une source d'inspiration importante dans cette étude. De fait la détermination de l'objet de l'étude a elle-même suivi un chemin compliqué. L'idée de départ, émanant d'une conversation avec Boas Erez, était de voir ce qu'on pouvait dire autour de la conjecture de Chinburg [Chi85] dans le cas faiblement ramifié : est-il par exemple possible de montrer que l'invariant Ω_2 est égal à la classe de la racine carrée de la codifférente, de façon analogue au théorème de Chinburg selon lequel il est égal à la classe de l'anneau d'entiers quand la ramification est modérée ? Cette question est vite apparue trop difficile à court terme (dans le cas général ; cependant il est sans doute très intéressant de l'envisager dans certains cas particulier comme le font des collègues munichois, Werner Bley et Alessandro Cobbe, d'après une discussion à Besançon en septembre 2013). D'une part la ramification faible est bien moins maniable que la modérée, d'autre part l'invariant Ω_2 n'est pas très simple à appréhender. Luca est alors tombé sur l'article de Chase cité plus haut, où est notamment étudiée la classe du quotient de la codifférente par l'anneau d'entiers, et la question s'est transformée en la comparaison de la classe de la racine carré de la codifférente avec celle de l'anneau d'entiers dans le cas modéré.

Ce problème reste nettement plus complexe que celui traité par Chase dans la mesure où, comme on le verra dans la section 2 de l'article reproduit ci-dessous, les objets à considérer dans notre situation ne sont plus « définis sur $\mathbb{Z}$ » mais seulement sur l'anneau d'entiers d'une extension cyclotomique de $\mathbb{Q}$. Il nous a donc fallu développer de nouveaux outils et étudier de nouveaux modules dans un cadre cyclotomique (qui a évidemment des avantages). Chemin faisant nous nous sommes rendus compte que la méthode que nous développions pouvait s'appliquer de façon très similaire à d'autres modules de torsion : le quotient de la codifférente par l'anneau d'entiers étudié par Chase, bien sûr, qui nous a servi de test, mais aussi un autre module considéré par Chase, en tant que $\mathcal{O}_E[G]$-module uniquement (ici $\mathcal{O}_E$ désigne l'anneau d'entiers du corps de base d'une extension galoisienne modérée N/E de groupe de Galois G). La classe de ce quotient dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres est reliée à celle du produit tensoriel de l'anneau d'entiers $\mathcal{O}_N$ par lui-même sur $\mathcal{O}_E$, dont nous établissons ainsi la trivialité (on peut aussi la déduire du théorème de Taylor sur la classe de l'anneau d'entiers).

Pour répondre à notre question de départ, nous devons supposer que l'extension modérée galoisienne N/E est localement abélienne. Nous montrons alors que les classes dans $\mathrm{Cl}(\mathbb{Z}[G])$ de l'anneau d'entiers et de la racine carrée de la codifférente sont égales. À ce stade il est important de noter que ce résultat est obtenu *sans hypothèse sur le degré*, à la seule condition que la codifférente soit un carré. En degré impair, on sait en effet par un résultat d'Erez que la classe

de la racine carrée de la codifférente d'une extension galoisienne modérée est triviale ; on déduit du théorème de Taylor que celle de l'anneau d'entiers l'est aussi. Notre résultat peut alors s'écrire sous la forme « $1 = 1$ » (en notation multiplicative). Cependant, d'une part nous l'obtenons avec des méthodes différentes de celles d'Erez et Taylor, très explicites et entièrement algébriques, d'autre part nous exhibons une extension galoisienne de $\mathbb{Q}$, localement abélienne, modérée, de degré pair, dont la codifférente est un carré, pour laquelle la classe de l'anneau d'entiers est non triviale. Notre résultat devient alors « $-1 = -1$ », égalité qui ne découle plus d'aucun résultat antérieur et fournit le premier exemple d'extension modérée dont la classe de la racine carrée de la codifférente n'est pas triviale.

Enfin, nos techniques nous permettent de reprouver très simplement un résultat de Burns ([Bur95, Theorem 1.1]) concernant les classes arithmétiquement réalisables et comparant, pour un groupe fini G, les éléments de $\mathrm{Cl}(\mathbb{Z}[G])$ réalisés par des idéaux ambiges (*i.e.* G-stables) d'extensions de corps de nombres modérées localement abéliennes, de groupe de Galois G, et ceux réalisés par l'anneau d'entiers de telles extensions.

Gauss sums, Jacobi sums and cyclotomic units related to torsion Galois modules

Luca Caputo and Stéphane Vinatier

Abstract

Let G be a finite group and let N/E be a tamely ramified G-Galois extension of number fields. We show how Stickelberger's factorization of Gauss sums can be used to determine the stable isomorphism class of various arithmetic $\mathbb{Z}[G]$-modules attached to N/E. If $\mathcal{O}_N$ and $\mathcal{O}_E$ denote the rings of integers of N and E respectively, we get in particular that $\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N$ defines the trivial class in the class group $\mathrm{Cl}(\mathbb{Z}[G])$ and, if N/E is also assumed to be locally abelian, that the square root of the inverse different (whenever it exists) defines the same class as $\mathcal{O}_N$. These results are obtained through the study of the Fröhlich representatives of the classes of some torsion modules, which are independently introduced in the setting of cyclotomic number fields. Gauss and Jacobi sums, together with the Hasse-Davenport formula, are involved in this study. These techniques are also applied to recover the stable self-duality of $\mathcal{O}_N$ (as a $\mathbb{Z}[G]$-module). Finally, when G is the binary tetrahedral group, we use our results in conjunction with Taylor's theorem to find a tame G-Galois extension whose square root of the inverse different has nontrivial class in $\mathrm{Cl}(\mathbb{Z}[G])$.

1. Introduction

Let G be a finite group and let N/E be a Galois extension of number fields with Galois group G. Let $\mathcal{O}_N$ and $\mathcal{O}_E$ denote the rings of integers of N and E, respectively; then $\mathcal{O}_N$ is an $\mathcal{O}_E[G]$-module, and in particular a $\mathbb{Z}[G]$-module, whose structure has long been studied. In the case where N/E is a tame extension, $\mathcal{O}_N$ is known to be locally free by Noether's theorem and the investigation of its Galois module structure culminated with M. Taylor's theorem [32] expressing the class $(\mathcal{O}_N)$ defined by $\mathcal{O}_N$ in the class group of locally free $\mathbb{Z}[G]$-modules $\mathrm{Cl}(\mathbb{Z}[G])$ in terms of Artin root numbers (see Theorem 5.1).

Other $\mathcal{O}_E[G]$-modules which appear naturally in our context have also been studied, among which the inverse different $\mathcal{C}_{N/E}$ of the extension and, when it exists, its square root $\mathcal{A}_{N/E}$. The existence of $\mathcal{A}_{N/E}$ is of course equivalent to $\mathcal{C}_{N/E}$ being a square, a condition which can be tested using Hilbert's valuation formula [25, IV, Proposition 4]. In particular, when N/E is tame, $\mathcal{A}_{N/E}$ exists if and only if the inertia group of every prime of $\mathcal{O}_E$ in N/E has odd order (which is the case for example if the degree $[N : E]$ is odd). In the tame case, both these modules are locally free $\mathbb{Z}[G]$-modules by a result of S. Ullom in [34] (applying to any G-stable fractional ideal of N).

The modules $\mathcal{O}_N$ and $\mathcal{C}_{N/E}$ are related by duality. For a fractional ideal I of $\mathcal{O}_N$, the dual of I with respect to the trace $\mathrm{Tr}_{N/E}$ from N to E is the fractional ideal

$$I^{\#} = \{x \in N \mid \mathrm{Tr}_{N/E}(xI) \subseteq \mathcal{O}_E\} \ .$$

Then $I^{\#}$ is G-isomorphic to the $\mathcal{O}_E$-dual of I, namely $I^{\#} \cong \mathrm{Hom}_{\mathcal{O}_E}(I, \mathcal{O}_E)$, and by definition one has

2000 Mathematics Subject Classification ????

$\mathcal{C}_{N/E} = \mathcal{O}_N^{\#}$, namely $\mathcal{O}_N$ and $\mathcal{C}_{N/E}$ are dual of each other. It can be shown that, for any fractional ideal I of $\mathcal{O}_N$, one has $I^{\#} = \mathcal{C}_{N/E} I^{-1}$, which implies that $\mathcal{A}_{N/E}$, when it exists, is the only self-dual fractional ideal of $\mathcal{O}_E$.

The duality relation between $\mathcal{C}_{N/E}$ and $\mathcal{O}_N$ accounts for comparing their $\mathbb{Z}[G]$-module structures. In the tame case, it essentially amounts to comparing their classes $(\mathcal{C}_{N/E})$ and $(\mathcal{O}_N)$ in $\mathrm{Cl}(\mathbb{Z}[G])$, and A. Fröhlich conjectured that $\mathcal{O}_N$ is stably self-dual, namely that

$$(\mathcal{O}_N) = (\mathcal{C}_{N/E}) \ . \tag{1}$$

This equality was proved later by M. Taylor [31] under slightly stronger hypotheses and by S. Chase [4] in full generality. Taylor's proof uses Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$, while Chase examines the torsion module

$$\mathcal{T}_{N/E} = \mathcal{C}_{N/E}/\mathcal{O}_N \ .$$

It is worth noting that both proofs make crucial use of the stable freeness of the Swan modules of cyclic groups, a result due to R. Swan [28].

The study of the Galois module structure of $\mathcal{A}_{N/E}$ was initiated by B. Erez, who proved in particular that, when N/E is tamely ramified and of odd degree, the class $(\mathcal{A}_{N/E})$ it defines in $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial, see [11]. His proof follows the same strategy as that of Taylor in [32], using in particular Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[G])$. Since Taylor's theorem implies the triviality of $(\mathcal{O}_N)$ when N/E is of odd degree, we get:

$$\text{if } [N:E] \text{ is odd, then } (\mathcal{O}_N) = (\mathcal{A}_{N/E}) \tag{2}$$

and both classes are in fact trivial.

In this paper, we consider a tame G-Galois extension N/E such that the square root of the inverse different $\mathcal{A}_{N/E}$ exists. We introduce the torsion module

$$\mathcal{S}_{N/E} = \mathcal{A}_{N/E}/\mathcal{O}_N \ ,$$

check it to be G-cohomologically trivial, hence to define a class in $\mathrm{Cl}(\mathbb{Z}[G])$, and show that this class is trivial, yielding a new proof of Equality (2) without any assumption on the degree of the extension. Nevertheless we need to assume that N/E is locally abelian, namely that the decomposition group of every prime ideal of $\mathcal{O}_E$ is abelian (note that this condition is automatically satisfied at unramified primes). The proofs of Erez [11] and Taylor [32] involve the study of Galois Gauss sums, which may be regarded as objects of analytic nature since they come from the functional equation of Artin L-functions. In our work instead only classical Gauss and Jacobi sums are involved, which might seem more satisfactory if one considers that (2) is a purely algebraic statement.

It turns out that the strategy of our proof also applies, without any restriction on the decomposition groups, to the torsion module $\mathcal{T}_{N/E}$ defined above as well as to another torsion module, denoted $\mathcal{R}_{N/E}$. The module $\mathcal{R}_{N/E}$, whose definition will be given in Section 2, was introduced and studied by Chase in [4]. We will prove that both $\mathcal{T}_{N/E}$ and $\mathcal{R}_{N/E}$ define the trivial class in $\mathrm{Cl}(\mathbb{Z}[G])$. This allows us on the one hand to recover Equality (1), and on the other hand to deduce that the $\mathbb{Z}[G]$-module $\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N$ defines the trivial class in $\mathrm{Cl}(\mathbb{Z}[G])$. This result looked new to us at first sight, but we show in Proposition 2.19 that $(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) = (\mathcal{O}_N)^{[N:E]}$ in $\mathrm{Cl}(\mathbb{Z}[G])$, hence it is easily deduced from Taylor's theorem.

These results are stated in Theorem 2 below. After a reduction to the case of a local totally ramified tame Galois extension with Galois group Δ, we introduce new torsion Galois modules, which define classes (R) and (S) in $\mathrm{Cl}(\mathbb{Z}[\Delta])$. The study of these classes is the core of our work. In Theorem 1 we give explicit expressions of representative morphisms of (R) and (S) in terms of Gauss and Jacobi sums, which through Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[\Delta])$ yield the triviality of (R) and (S). Theorem 3

will show a surprising consequence of the generalisation of Equality (2) to even degree extensions.

We now explain our strategy more in detail. In Section 2 we follow Chase's approach: we consider the torsion modules $\mathcal{T}_{N/E}$, $\mathcal{S}_{N/E}$ and $\mathcal{R}_{N/E}$, then we reduce to the study, for every prime $\mathcal{P}$ of N, of their $\mathbb{Z}[I_\mathcal{P}]$-module structure, where $I_\mathcal{P}$ is the inertia group at $\mathcal{P}$ (note that $I_\mathcal{P}$ is cyclic of order coprime to the residual characteristic of $\mathcal{P}$, since N/E is tame). In other words we show that it is sufficient to prove the triviality of the classes in $\mathrm{Cl}(\mathbb{Z}[\Delta])$ of the local analogues $\mathcal{T}_{K/F}$, $\mathcal{S}_{K/F}$ and $\mathcal{R}_{K/F}$, where K/F is a cyclic totally ramified tame p-adic extension with Galois group Δ of order e (prime to p). Up to this point, the only difference with Chase's study of $\mathcal{T}_{N/E}$ is that we need N/E to be locally abelian when dealing with $\mathcal{S}_{N/E}$.

It is interesting to remark that $\mathcal{T}_{N/E}$ and $\mathcal{S}_{N/E}$ are particular instances of torsion modules arising from ideals, *i.e.* modules of the form $\mathcal{O}_N/\mathcal{I}$ or $\mathcal{I}^{-1}/\mathcal{O}_N$, where $\mathcal{I}$ is a G-stable ideal of $\mathcal{O}_N$. In fact we will perform the reduction step of Section 2 for general torsion modules arising from ideals (under the assumption that N/E is locally abelian). Working in this more general situation requires no additional effort and allows us to easily recover the cases of $\mathcal{T}_{N/E}$ and $\mathcal{S}_{N/E}$ (while $\mathcal{R}_{N/E}$ needs a somehow separate treatment). Moreover we will get almost for free a new proof of a result of Burns [3, Theorem 1.1] on arithmetically realisable classes in tame locally abelian Galois extensions of number fields (see Subsection 3.5). Nonetheless, for the sake of simplicity, in this introduction we shall stick with the modules $\mathcal{T}_{N/E}$, $\mathcal{S}_{N/E}$ and $\mathcal{R}_{N/E}$.

The key ingredient in Chase's proof of the triviality of $\mathcal{T}_{N/E}$ is the link he establishes between the local torsion module $\mathcal{T}_{K/F}$ and the Swan module $\Sigma_\Delta(p) = p\mathbb{Z}[\Delta] + \mathrm{Tr}_\Delta\mathbb{Z}[\Delta]$ (here $\mathrm{Tr}_\Delta = \sum_{\delta\in\Delta}\delta \in \mathbb{Z}[\Delta]$). Consider the torsion module $T(p,\mathbb{Z}[\Delta]) = \mathbb{Z}[\Delta]/\Sigma_\Delta(p)$ associated to the Swan module, then

$$\mathcal{T}_{K/F} \cong T(p,\mathbb{Z}[\Delta])^{f_F}$$

as $\mathbb{Z}[\Delta]$-modules, where f_F is the inertia degree of $F/\mathbb{Q}_p$.

To deal with $\mathcal{S}_{K/F}$ and $\mathcal{R}_{K/F}$, we need to enlarge the coefficient ring of the group algebra of Δ. Let μ_e denote the group of eth roots of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $\mathfrak{o}$ denote the ring of integers of the cyclotomic field $\mathbb{Q}(\mu_e)$. We introduce new torsion $\mathbb{Z}[\Delta]$-modules $S_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$ and $R_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$, which depend on a character $\chi : \Delta \to \mu_e$ and a prime $\mathfrak{p}$ of $\mathfrak{o}$ not dividing p. They may be considered as analogues of $T(p,\mathbb{Z}[\Delta])$ in the sense that, for an appropriate choice of χ and $\mathfrak{p}$ (in particular $\mathfrak{p} \mid p$, the residual characteristic of K/F), we have

$$\mathcal{S}_{K/F} \cong S_\chi(\mathfrak{p},\mathfrak{o}[\Delta])^{f_F/f}, \quad \mathcal{R}_{K/F} \cong R_\chi(\mathfrak{p},\mathfrak{o}[\Delta])^{f_F/f},$$

as $\mathbb{Z}[\Delta]$-modules, where f is the inertia degree of $\mathfrak{p}$ in $\mathbb{Q}(\mu_e)/\mathbb{Q}$. These constructions are described in Section 2.3. Furthermore it is easy to see that both $S_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$ and $R_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$ are cohomologically trivial $\mathbb{Z}[\Delta]$-modules, hence they define classes in $\mathrm{Cl}(\mathbb{Z}[\Delta])$ (see Section 2.4).

Now let $\chi : \Delta \to \mu_e$ be any injective character and $\mathfrak{p}$ be a prime of $\mathfrak{o}$ not dividing e. Set $R = R_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$ and $S = S_\chi(\mathfrak{p},\mathfrak{o}[\Delta])$. The core of this paper is the study of the classes (R) and (S) in $\mathrm{Cl}(\mathbb{Z}[\Delta])$. In Section 3, we find equivariant morphisms r and s from the group of virtual characters of Δ to the idèles of $\mathbb{Q}(\mu_e)$, representing (R) and (S) respectively in Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[\Delta])$. In Section 4, we note that the contents of the values of r and s are principal ideals: this follows from Stickelberger's theorem, which also gives explicit generators of these ideals in terms of Gauss and Jacobi sums respectively. Dividing r and s by suitably modified generators c_r and c_s of their contents yields morphisms with unit idelic values. With the help of the Hasse-Davenport formula we express the resulting morphisms rc_r^{-1} and sc_s^{-1} as Fröhlich's generalized Determinants of some unit idèles of $\mathbb{Z}[\Delta]$, showing that they lie in the denominator of the Hom-description, namely that (R) and (S) are trivial.

It is worth noting that applying these techniques to $T_{\mathbb{Z}} = T(p, \mathbb{Z}[\Delta])$ yields a proof of the triviality of $(T_{\mathbb{Z}})$ in $\mathrm{Cl}(\mathbb{Z}[\Delta])$. In this proof, as in the original proof by Swan, cyclotomic units play a central role, analogous to that of the Gauss and Jacobi sums above, as it will soon be apparent.

To state our main results, we let G and J denote the Gauss and Jacobi sums defined respectively by

$$G = \sum_{x \in \mathfrak{o}/\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)^{-1} \xi^{\mathrm{Tr}(x)} , \quad J = \sum_{x \in \mathfrak{o}/\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)^{-1} \left(\frac{1-x}{\mathfrak{p}}\right)^{-1} ,$$

where $\mathrm{Tr} : \mathfrak{o}/\mathfrak{p} \to \mathbb{Z}/p\mathbb{Z}$ denotes the residue field trace homomorphism, ξ is a fixed pth root of unity in $\overline{\mathbb{Q}}$ and $\left(\frac{\cdot}{\mathfrak{p}}\right)$ is the eth power residue symbol. Then both G^e and J belong to $\mathfrak{o}$. Let δ be a fixed generator of Δ. In Section 4 we define $m_i, n_i \in \mathbb{Z}$ for $i = 0, \ldots e-1$ such that

$$G^e = \sum_{i=0}^{e-1} m_i \chi(\delta)^i , \quad J = \sum_{i=0}^{e-1} n_i \chi(\delta)^i .$$

The corresponding expression for the cyclotomic unit C is:

$$C = \frac{\chi(\delta)^p - 1}{\chi(\delta) - 1} = \sum_{i=0}^{p-1} \chi(\delta)^i .$$

We can now formulate the main result of this paper, in terms of Fröhlich's Hom-description of the class group (see Section 3.1 for more details).

Theorem 1. *The classes $(T_{\mathbb{Z}})$, (R) and (S) are trivial in* $\mathrm{Cl}(\mathbb{Z}[\Delta])$. *More precisely they are represented in* $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, J(\mathbb{Q}(\mu_e)))$ *by the morphisms with* $\mathfrak{q}$*-components equal to* 1 *at places* $\mathfrak{q}$ *of* $\mathbb{Q}(\mu_e)$ *such that* $\mathfrak{q} \nmid e$, *and to*

$$\mathrm{Det}(p^{-1}u_t) , \quad \mathrm{Det}(u_r^{-1}) , \quad \mathrm{Det}(u_s^{-1}) ,$$

respectively, at prime ideals $\mathfrak{q}$ *of* $\mathfrak{o}$ *such that* $\mathfrak{q} \mid e$, *where* $u_t, u_r, u_s \in \mathbb{Z}[\Delta]$ *are defined by*

$$u_t = \sum_{i=0}^{p-1} \delta^i , \quad u_r = \sum_{i=0}^{e-1} m_i \delta^i , \quad u_s = \sum_{i=0}^{e-1} n_i \delta^i ,$$

and satisfy $u_t, u_r, u_s \in \mathbb{Z}_q[\Delta]^\times$, *for any rational prime* q *such that* $q \mid e$.

The triviality of $(T_{\mathbb{Z}})$ is essentially Swan's theorem [28, Corollary 6.1]. Our proof using Fröhlich's Hom-description of the class group, given in Section 3.2, might be folklore, nevertheless the representative morphism we use to describe $(T_{\mathbb{Z}})$ is slightly different from the one given in [14, (I.2.23)] (see Remark 3.3). The proof for S and R will follow from the results of Sections 3 and 4 and will enlight the analogy between the torsion modules R and S we introduce and $T_{\mathbb{Z}}$ (see Theorem 4.5 and its proof).

In his early work [10] on the square root of the inverse different, Erez already establishes a link between this module and a Jacobi sum, in the case of a cyclic extension of $K/\mathbb{Q}$ of odd prime degree l. Using a result of Ullom [36, Theorem 1], he shows that the class of $\mathcal{A}_{K/\mathbb{Q}}$ in $\mathrm{Cl}(\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})])$ corresponds, through Rim's isomorphism [8, (42.16)], to the class in $\mathrm{Cl}(\mathbb{Q}(\mu_l))$ of an ideal of $\mathbb{Q}(\mu_l)$ which is defined by the action of some specific element of $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q})]$ on prime ideals. This group algebra element, which is pretty close to what ours, u_s, would yield in the prime degree case (see §3.4.3), happens to be the exponent which appears in the factorisation of the Jacobi sum, yielding the triviality of the class under study.

The factorisation of Gauss and Jacobi sums through Stickelberger's theorem is also an essential step in our proof of the triviality of the classes of R and S. In the introduction of his thesis [9], Erez gives

other examples of results on the Galois module structure of rings of integers that are proved using Stickelberger elements ([17], [6]). In [4] Chase uses such elements to give the composition series of certain primary components of the $\mathcal{O}_E[G]$-module $\mathcal{R}_{N/E}$ when N/E is cyclic or elementary abelian. Reversely, Galois module structure results can be used to build Stickelberger elements: the first statement in the theory of integral Galois modules is due to Hilbert (for the ring of integers of an abelian extension of $\mathbb{Q}$ with discriminant coprime to the degree), who used it to construct annihilating elements for the class group of some cyclotomic extensions. Finally, Stickelberger's elements also have a fundamental role in the work of L. McCulloh (see [19], [20] and the references given in those papers).

As pointed out by Fröhlich in [14, Note 6 to Chapter III], Chase remarks that the character function associated to $\mathcal{T}_{N/E}$ (in the ideal-theoretic Hom-description) is the Artin conductor. Similarly, the character function associated to $\mathcal{R}_{N/E}$ (in the idèle-theoretic Hom-description) is closely related to a resolvent map (see [4, p. 210]). Fröhlich also wonders how his method, based on the comparison of Galois Gauss sums and resolvents, could be linked to Chase's approach. We hope that the explicit connection we establish between $\mathcal{R}_{K/F}$ and a Gauss sum might be useful to answer Fröhlich's question.

Using the reduction results of Section 2, we deduce the following consequence.

Theorem 2. *Let N/E be a G-Galois tamely ramified extension of number fields. Then the classes of $\mathcal{T}_{N/E}$ and $\mathcal{R}_{N/E}$ are trivial in* $\mathrm{Cl}(\mathbb{Z}[G])$. *In particular we have*

$$(\mathcal{O}_N) = (\mathcal{C}_{N/E}) \quad \textit{and} \quad (\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) = (\mathcal{O}_N)^{[N:E]} = 1 \ .$$

If, further, N/E is locally abelian, then the class of $\mathcal{S}_{N/E}$ is trivial in $\mathrm{Cl}(\mathbb{Z}[G])$. *In particular we have*

$$(\mathcal{O}_N) = (\mathcal{A}_{N/E}) \ ,$$

thus $\mathcal{O}_N$, $\mathcal{C}_{N/E}$ and $\mathcal{A}_{N/E}$ define the same class in $\mathrm{Cl}(\mathbb{Z}[G])$.

As already mentioned, the triviality of $(\mathcal{T}_{N/E})$ in this context is due to Chase, see [4, Corollary 1.12]. In the same paper he studies the torsion module $\mathcal{R}_{N/E}$ as an $\mathcal{O}_E[G]$-module, showing that it determines the local Galois module structure of $\mathcal{O}_N$ [4, Theorem 2.10] and describing its primary components [4, Theorem 2.15]. We will show that $(\mathcal{R}_{N/E}) = 1$, which is in fact equivalent to $(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) = (\mathcal{O}_N)^{[N:E]} = 1$ (see §2.4.3). The equality $(\mathcal{O}_N)^{[N:E]} = 1$ follows of course from Taylor's theorem (which implies that $(\mathcal{O}_N)$ is of order dividing 2 and is trivial in odd degree) but was also known before Taylor's proof of Fröhlich's conjecture (it follows from [30, Corollary] using the last remark of [16, Definition 1.6]). We make more comments on the last equality of Theorem 2 in the presentation of Section 5 below.

We end this paper by focusing in Section 5 on the class of the square root of the inverse different (for the rest of this introduction we shall assume that the inverse different of every extension we consider is a square). We briefly recall some known results on this matter. In odd degree, Erez showed that $(\mathcal{A}_{N/E}) \in \mathrm{Cl}(\mathbb{Z}[G])$ is defined (*i.e.* $\mathcal{A}_{N/E}$ is $\mathbb{Z}[G]$-locally free) if and only if N/E is a weakly ramified G-Galois extension (*i.e* the second ramification group of every prime is trivial). It seems reasonable to conjecture that $(\mathcal{A}_{N/E})$ is trivial when N/E is a weakly ramified Galois extension of odd degree (see also [37, Conjecture]). As already mentioned this conjecture is true in the tame case, thanks to a result of Erez. When N/E is a weakly ramified G-Galois extension of odd degree, one also knows that

- $\mathcal{M}\otimes_{\mathbb{Z}[G]}\mathcal{A}_{N/E}$ is free over $\mathcal{M}$, where $\mathcal{M}$ is a maximal order of $\mathbb{Q}[G]$ containing $\mathbb{Z}[G]$ ([11, Theorem 2]);
- $(\mathcal{A}_{N/E}) = 1$ if, for any wildly ramified prime $\mathcal{P}$ of $\mathcal{O}_N$, the decomposition group is abelian, the inertia group is cyclic and the localized extension $E_P/\mathbb{Q}_p$ is unramified, where $P = \mathcal{P} \cap E$ and

$p\mathbb{Z} = \mathcal{P} \cap \mathbb{Q}$ ([22, Theorem 1]);

– $(\mathcal{A}_{N/\mathbb{Q}})^e = 1$ if $[N : \mathbb{Q}]$ is a power of a prime p and e is the ramification index of p in $N/\mathbb{Q}$ ([37, Théorème 1]); when $p = 3$ one even has $(\mathcal{A}_{N/\mathbb{Q}})^3 = 1$ by [38, Theorem 1].

It is interesting to observe that so far the class of $\mathcal{A}_{N/E}$ had only been studied when N/E has odd degree (except for a short local study, due to Burns and Erez, in the absolute, abelian and very wildly ramified case, see [12, §3]). Specifically the question of whether it is trivial or not for *every* tame Galois extension N/E had not been considered. The reason for this restriction is that the second Adams operation, which is fundamental in Erez's approach in [11], does not behave well with respect to induction for groups of even order.

This is precisely the point where our result above brings new information. When N/E is locally abelian and tame, Theorem 2 together with Taylor's theorem reduces the question to the study of the triviality of the image of the root number class in $\mathrm{Cl}(\mathbb{Z}[G])$ (see Corollary 5.2). This immediately gives that $(\mathcal{A}_{N/E}) = 1$ if N/E is abelian or has odd order (thus recovering Erez's result in the locally abelian case). Computing the appropriate root numbers, we show next that $(\mathcal{A}_{N/E}) = 1$ if N/E is locally abelian and no real place of E becomes complex in N. However the class of the square root of the inverse different is not trivial in general, in other words we have the following result.

Theorem 3. *There exists a tame Galois extension $N/\mathbb{Q}$ of even degree such that $\mathcal{C}_{N/\mathbb{Q}}$ is a square and the class of $\mathcal{A}_{N/\mathbb{Q}}$ is nontrivial in* $\mathrm{Cl}(\mathbb{Z}[\mathrm{Gal}(N/\mathbb{Q})])$.

In fact, in Section 5.2 we will explicitly describe a tame locally abelian $\tilde{A}_4$-Galois extension $N/\mathbb{Q}$, taken from [1], such that $(\mathcal{A}_{N/\mathbb{Q}}) \neq 1$ in $\mathrm{Cl}(\mathbb{Z}[\tilde{A}_4])$, where $\tilde{A}_4$ is the binary tetrahedral group (which has order 24). This is, to our knowledge, the first example of a tame Galois extension of number fields whose square root of the inverse different (exists and) has nontrivial class. We also show that this example is minimal in the sense that $(\mathcal{A}_{N/\mathbb{Q}}) = 1$ if $N/\mathbb{Q}$ is a tame locally abelian G-Galois extension with $\#G \leqslant 24$ and $G \neq \tilde{A}_4$.

2. Reduction to inertia subgroups

We use the notation of the Introduction, in particular N/E is a tame G-Galois extension. For a prime $\mathcal{P}$ of N, we denote by $I_{\mathcal{P}}$ (resp. $D_{\mathcal{P}}$) the inertia subgroup (resp. decomposition subgroup) of $\mathcal{P}$ in N/E. If P is the prime ideal of E below $\mathcal{P}$, we will often identify the Galois group of $N_{\mathcal{P}}/E_P$ with $D_{\mathcal{P}}$, where $N_{\mathcal{P}}$ (resp. E_P) is the completion of N at $\mathcal{P}$ (resp. of E at P). In this section we show that the G-module structure of the torsion modules we are interested in can be recovered by the knowledge, for finitely many primes $\mathcal{P}$ of N, of the $I_{\mathcal{P}}$-module structure of a certain torsion $I_{\mathcal{P}}$-module. More precisely, if $\mathrm{Ram}(N/E)$ denotes the set of primes of $\mathcal{O}_E$ which ramify in N/E, then $\mathcal{T}_{N/E}$, $\mathcal{S}_{N/E}$ and $\mathcal{R}_{N/E}$ can be written as a direct sum over $\mathrm{Ram}(N/E)$ of torsion G-modules induced from $I_{\mathcal{P}}$-modules, where, for each $P \in \mathrm{Ram}(N/E)$, $\mathcal{P}$ is any fixed prime above P. For $\mathcal{R}_{N/E}$ and $\mathcal{T}_{N/E}$ such a decomposition follows directly from Chase's results. For instance, in the case of $\mathcal{T}_{N/E}$, the corresponding $I_{\mathcal{P}}$-module is a suitable power of the quotient $T(p, \mathbb{Z}[I_{\mathcal{P}}]) = \mathbb{Z}[I_{\mathcal{P}}]/\Sigma_{I_{\mathcal{P}}}(p)$, where $\Sigma_{I_{\mathcal{P}}}(p) = p\mathbb{Z}[I_{\mathcal{P}}] + \mathrm{Tr}_{I_{\mathcal{P}}}\mathbb{Z}[I_{\mathcal{P}}]$ is the Swan module generated by the trace $\mathrm{Tr}_{I_{\mathcal{P}}} = \sum_{g \in I_{\mathcal{P}}} g \in \mathbb{Z}[I_{\mathcal{P}}]$ and the residual characteristic p of $\mathcal{P}$.

However for torsion modules arising from general G-stable ideals of $\mathcal{O}_N$ (and in particular for $\mathcal{S}_{N/E}$), we need to introduce torsion $\mathfrak{o}_{e_P}[I_{\mathcal{P}}]$-modules and also assume that N/E is locally abelian. Here e_P is the order of $I_{\mathcal{P}}$ (which indeed depends only on the prime P of $\mathcal{O}_E$ lying below $\mathcal{P}$), μ_{e_P} is the group of e_Pth roots of unity in $\overline{\mathbb{Q}}$ and $\mathfrak{o}_{e_P}$ is the ring of integers of $\mathbb{Q}(\mu_{e_P})$. These $\mathfrak{o}_{e_P}[I_{\mathcal{P}}]$-modules can be

considered as analogues of $T(p,\mathbb{Z}[I_\mathcal{P}])$ and they also give a decomposition for $\mathcal{R}_{N/E}$, which is slightly different from that of Chase and will be needed in the proof of Theorem 1. To stress their similarity with $T(p,\mathbb{Z}[I_\mathcal{P}])$, we shall denote by $R_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])$ and $S_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])$ those which correspond to $\mathcal{R}_{N/E}$ and $\mathcal{S}_{N/E}$, respectively (see (13) and (12) for a precise definition). Here $\chi_\mathcal{P}$ is an injective character of $I_\mathcal{P}$ and $\mathfrak{p}$ is a prime above p in $\mathfrak{o}_{e_P}$.

We now state the main result of this section whose proof will be given in §2.3.2.

Theorem 2.1. *For every $P\in\mathrm{Ram}(N/E)$, choose a prime $\mathcal{P}$ of N above P. Then, with the notation introduced above, there is an isomorphism of $\mathbb{Z}[G]$-modules*

$$\mathcal{T}_{N/E}\cong\bigoplus_{P\in\mathrm{Ram}(N/E)}\Big(\mathbb{Z}[G]\otimes_{\mathbb{Z}[I_\mathcal{P}]}T(p,\mathbb{Z}[I_\mathcal{P}])\Big)^{\oplus[\mathcal{O}_E/P:\mathbb{F}_p]}.$$

Furthermore, for every choice of injective characters $\chi_\mathcal{P}:I_\mathcal{P}\to\overline{\mathbb{Q}}^\times$ for every prime $\mathcal{P}$ as above, one can find primes $\mathfrak{p}\subset\mathfrak{o}_{e_P}$ and injections $\mathfrak{o}_{e_P}/\mathfrak{p}\to\mathcal{O}_N/\mathcal{P}$ such that there is an isomorphism of $\mathbb{Z}[G]$-modules

$$\mathcal{R}_{N/E}\cong\bigoplus_{P\in\mathrm{Ram}(N/E)}\Big(\mathbb{Z}[G]\otimes_{\mathbb{Z}[I_\mathcal{P}]}R_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])\Big)^{\oplus[G:D_\mathcal{P}][\mathcal{O}_N/\mathcal{P}:\mathfrak{o}_{e_P}/\mathfrak{p}]}$$

Assume moreover that N/E is locally abelian. Then the injections $\mathfrak{o}_{e_P}/\mathfrak{p}\to\mathcal{O}_N/\mathcal{P}$ factor through $\mathcal{O}_E/P\to\mathcal{O}_N/\mathcal{P}$ and there is an isomorphism of $\mathbb{Z}[G]$-modules

$$\mathcal{S}_{N/E}\cong\bigoplus_{P\in\mathrm{Ram}(N/E)}\Big(\mathbb{Z}[G]\otimes_{\mathbb{Z}[I_\mathcal{P}]}S_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])\Big)^{\oplus[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]}.$$

In Section 2.4 we will see how the above theorem, together with Theorem 1, can be used to prove Theorem 2. More precisely, we show that the torsion G-modules (resp. $I_\mathcal{P}$-modules) appearing in Theorem 2.1 are G-cohomologically trivial (resp. $I_\mathcal{P}$-cohomologically trivial) and therefore define classes in $\mathrm{Cl}(\mathbb{Z}[G])$ (resp. $\mathrm{Cl}(\mathbb{Z}[I_\mathcal{P}])$). Thus the isomorphisms of Theorem 2.1 can be translated into equalities of classes in $\mathrm{Cl}(\mathbb{Z}[G])$, which in turn will give directly Theorem 2, assuming Theorem 1.

2.1 The torsion module $\mathcal{R}_{N/E}$

The results of this subsection are due to Chase [4].

2.1.1 We shall first recall the definition of $\mathcal{R}_{N/E}$ in a wider context. Let Γ be a finite group and let K/k be a Γ-Galois extension of either global or local fields. If X and Y are sets, we denote by $\mathrm{Map}(X,Y)$ the set of mappings from X to Y. Consider the bijection

$$\psi_{K/k}:K\otimes_k K\to\mathrm{Map}(\Gamma,K)\tag{3}$$

defined by $\psi_{K/k}(x\otimes y)(\gamma)=x\gamma(y)$ for $x,y\in K$ and $\gamma\in\Gamma$. Now $K\otimes_k K$ is a $K[\Gamma]$-module with K acting on the left factor, Γ on the right and $\mathrm{Map}(\Gamma,K)$ is a $K[\Gamma]$-module with K acting pointwise and Γ acting by $(\gamma u)(\gamma')=u(\gamma'\gamma)$ for all $\gamma,\gamma'\in\Gamma$, $u\in\mathrm{Map}(\Gamma,K)$. These structures make $\psi_{K/k}$ an isomorphism of $K[\Gamma]$-modules. Restricting $\psi_{K/k}$ to the subring $\mathcal{O}_K\otimes_{\mathcal{O}_k}\mathcal{O}_K\subset K\otimes_k K$ yields an $\mathcal{O}_K[\Gamma]$-modules injection

$$\psi_{K/k}:\mathcal{O}_K\otimes_{\mathcal{O}_k}\mathcal{O}_K\to\mathrm{Map}(\Gamma,\mathcal{O}_K)$$

whose cokernel

$$\mathcal{R}_{K/k}=\mathrm{Map}(\Gamma,\mathcal{O}_K)/\psi_{K/k}(\mathcal{O}_K\otimes_{\mathcal{O}_k}\mathcal{O}_K)$$

is a torsion Γ-module. We refer the reader to [4, Sections 2, 3, 4] and [14, Note 6 to Chapter III] for more details on $\mathcal{R}_{K/k}$.

We now come back to the notation of the beginning of this section, in particular N/E is a tame G-Galois extension of number fields. Recall also that for every $P \in \mathrm{Ram}(N/E)$, we fix a prime $\mathcal{P}$ of N above P.

Proposition 2.2. *There is an isomorphism of $\mathcal{O}_E[G]$-modules*

$$\mathcal{R}_{N/E} \cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[D_{\mathcal{P}}]} \mathcal{R}_{N_{\mathcal{P}}/E_P}\right)^{\oplus [G:D_{\mathcal{P}}]}.$$

Proof. See [4, Corollary 3.11]. □

2.1.2 Proposition 2.2 shows that we can focus on the local setting. Therefore in this subsection we shall put ourselves in the following situation (which will appear again at later stages of this paper). We fix a rational prime p and a tamely ramified Galois extension K/k of p-adic fields inside a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. We denote by Γ the Galois group of K/k. Let $\Delta \subseteq \Gamma$ be the inertia subgroup of K/k, which is cyclic of order denoted by e, and set $F = K^{\Delta}$. As usual, $\mathcal{O}_K$, $\mathcal{O}_F$ and $\mathcal{O}_k$ denote the rings of integers of K, F and k, respectively, and we shall denote by $\mathcal{P}_K$, $\mathcal{P}_F$ and $\mathcal{P}_k$ the corresponding maximal ideals.

The following result shows that we can in fact focus on totally and tamely ramified local extensions.

Proposition 2.3. *There is an isomorphism of $\mathcal{O}_K[\Gamma]$-modules*

$$\mathcal{R}_{K/k} \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{R}_{K/F}.$$

Proof. See [4, Corollary 3.8]. □

By standard theory F contains the group of eth roots of unity $\mu_{e,p} \subseteq \overline{\mathbb{Q}}_p$, and we can choose a uniformizer π_K of K such that $\pi_K^e \in F$ (thus π_K^e is a uniformizer of F). Consider the map $\chi_{K/F} : \Delta \to \mu_{e,p}$ defined by

$$\chi_{K/F}(\delta) = \frac{\delta(\pi_K)}{\pi_K} \quad .$$

Since K/F is totally ramified, any unit $u \in \mathcal{O}_K^{\times}$ such that $u^e \in F$ lies in F, hence $\chi_{K/F}$ does not depend on the choice of a uniformizer π_K as above. It easily follows that $\chi_{K/F}$ is a group homomorphism, hence an isomorphism comparing cardinals: $\#\Delta = e = \#\mu_{e,p}$ (see also [25, Chapitre IV, Propositions 6(a) and 7]).

Remark 2.4. Note that Δ (resp. $\mu_{e,p}$) is a Γ/Δ-module with the conjugation (resp. Galois) action. Then $\chi_{K/F}$ is in fact an isomorphism of Γ/Δ-modules. To prove this, it is enough to verify that, for every $\gamma \in \Gamma$ and $\delta \in \Delta$, we have $\chi_{K/F}(\gamma\delta\gamma^{-1}) = \gamma(\chi_{K/F}(\delta))$. But indeed, if π_K is as above, we have

$$\chi_{K/F}(\gamma\delta\gamma^{-1}) = \frac{\gamma\delta\gamma^{-1}(\pi_K)}{\pi_K} = \gamma\left(\frac{\delta\gamma^{-1}(\pi_K)}{\gamma^{-1}(\pi_K)}\right) = \gamma(\chi_{K/F}(\delta))$$

since $\gamma^{-1}(\pi_K)$ is a uniformizer of K whose eth power belongs to F. Hence $\chi_{K/F}$ is a Γ-isomorphism and we deduce in particular that, if Γ is abelian, then $\mu_{e,p} \subset k$. The reverse implication is also true: if $\mu_{e,p} \subset k$, then Γ acts trivially on Δ. This implies that Γ is abelian, since $\Gamma = \langle \gamma, \Delta \rangle$ for any $\gamma \in \Gamma$ whose image in Γ/Δ generates Γ/Δ (which is a cyclic group).

If M is an $\mathcal{O}_K$-module, we let $M(\chi_{K/F}^i)$ denote the $\mathcal{O}_K[\Delta]$-module which is M as an $\mathcal{O}_K$-module and has Δ-action defined by $\delta \cdot m = \chi_{K/F}^i(\delta)m$.

We now show that the Δ-module $\mathcal{R}_{K/F}$ can be decomposed in smaller pieces.

Proposition 2.5. *The action of $\mathcal{O}_F$ on $\mathcal{R}_{K/F}$ factors through $\mathcal{O}_F/\mathcal{P}_F$ and there is an isomorphism of $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules*

$$\mathcal{R}_{K/F} \cong \bigoplus_{i=1}^{e-1} (\mathcal{P}_K^i/\mathcal{P}_K^{i+1})^{\oplus i}.$$

Proof. We start from Chase's decomposition [4, Theorem 2.8] which, in our notation, is an isomorphism of $\mathcal{O}_K[\Delta]$-modules:

$$\mathcal{R}_{K/F} \cong \bigoplus_{i=1}^{e-1} (\mathcal{O}_K/\mathcal{P}_K^i)(\chi_{K/F}^i) \ .$$

Note that, for $0 \leqslant i \leqslant e$, $\mathcal{O}_K/\mathcal{P}_K^i$ is an $\mathcal{O}_F/\mathcal{P}_F$-module, since $\mathcal{P}_F\mathcal{O}_K = \mathcal{P}_K^e \subseteq \mathcal{P}_K^i$ and hence the action of $\mathcal{O}_F$ on $\mathcal{O}_K/\mathcal{P}_K^i$ factors through $\mathcal{P}_F$. From its definition $\mathcal{R}_{K/F}$ is an $\mathcal{O}_F$-module, hence an $\mathcal{O}_F/\mathcal{P}_F$-module by the above isomorphism, which is thus an isomorphism of $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules. In what follows we shall be mainly concerned with $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-module structures (although some of the assertions hold true in the category of $\mathcal{O}_K[\Delta]$-modules).

Observe that the $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-module $(\mathcal{O}_K/\mathcal{P}_K^i)(\chi_{K/F}^i)$ has the filtration $\{(\mathcal{P}_K^j/\mathcal{P}_K^i)(\chi_{K/F}^i)\}_{j=0}^i$ whose corresponding subquotients are $(\mathcal{P}_K^j/\mathcal{P}_K^{j+1})(\chi_{K/F}^i)$ for $j = 0, \ldots, i-1$. It is clear that multiplication by the jth power of any uniformizer of K induces an $\mathcal{O}_F/\mathcal{P}_F$-isomorphism $\mathcal{O}_K/\mathcal{P}_K \cong \mathcal{P}_K^j/\mathcal{P}_K^{j+1}$ and hence an $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-isomorphism $(\mathcal{O}_K/\mathcal{P}_K)(\chi_{K/F}^i) \cong (\mathcal{P}_K^j/\mathcal{P}_K^{j+1})(\chi_{K/F}^i)$. Therefore using the semisimplicity of $\mathcal{O}_F/\mathcal{P}_F[\Delta]$, we get

$$(\mathcal{O}_K/\mathcal{P}_K^i)(\chi_{K/F}^i) \cong \bigoplus_{j=0}^{i-1} (\mathcal{O}_K/\mathcal{P}_K)(\chi_{K/F}^i) = (\mathcal{O}_K/\mathcal{P}_K)(\chi_{K/F}^i)^{\oplus i}.$$

Note that the Galois action of Δ on $\mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ coincides with the action given by multiplication by $\chi_{K/F}^i$ since

$$\delta[\pi_K^i x] = [\delta(\pi_K^i x)] = [\chi_{K/F}(\delta)^i \pi_K^i \delta(x)] = [\chi_{K/F}(\delta)^i \pi_K^i x] \tag{4}$$

where, for $y \in \mathcal{P}_K^i$, we let $[y]$ denote the class of y in $\mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ (the last equality of (4) follows from the fact that Δ acts trivially on $\mathcal{O}_K/\mathcal{P}_K = \mathcal{O}_F/\mathcal{P}_F$). Thus both $\mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ and $(\mathcal{O}_K/\mathcal{P}_K)(\chi_{K/F}^i)$ are $\mathcal{O}_F/\mathcal{P}_F$-vector spaces of dimension 1 on which Δ acts by multiplication by $\chi_{K/F}^i$. Therefore

$$(\mathcal{O}_K/\mathcal{P}_K^i)(\chi_{K/F}^i) \cong (\mathcal{P}_K^i/\mathcal{P}_K^{i+1})^{\oplus i}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules. □

2.2 Torsion modules arising from ideals

2.2.1 We keep the notation of the beginning of this section. Let $\mathcal{I} \subset \mathcal{O}_N$ be a G-invariant ideal. We will show that the G-module structure of $\mathcal{O}_N/\mathcal{I}$ and $\mathcal{I}^{-1}/\mathcal{O}_N$ is of local nature. We denote by $\mathrm{Div}(\mathcal{I})$ the (finite) set of primes of E dividing $\mathcal{I}$ and, for every $P \in \mathrm{Div}(\mathcal{I})$ we fix a prime $\mathcal{P}$ of N above P.

Proposition 2.6. *Let $\mathcal{I} \subset \mathcal{O}_N$ be a G-invariant ideal. For every prime $P \in \mathrm{Div}(\mathcal{I})$, let n_P be the valuation*

of $\mathcal{I}$ at any prime of $\mathcal{O}_N$ above P. Then there are isomorphisms of $\mathcal{O}_E[G]$-modules

$$\mathcal{O}_N/\mathcal{I} \cong \bigoplus_{P\in \mathrm{Div}(\mathcal{I})} \mathbb{Z}[G]\otimes_{\mathbb{Z}[D_\mathcal{P}]} (\mathcal{O}_{N_\mathcal{P}}/\mathcal{P}^{n_P}\mathcal{O}_{N_\mathcal{P}})$$
$$\mathcal{I}^{-1}/\mathcal{O}_N \cong \bigoplus_{P\in \mathrm{Div}(\mathcal{I})} \mathbb{Z}[G]\otimes_{\mathbb{Z}[D_\mathcal{P}]} \left(\mathcal{P}^{-n_P}\mathcal{O}_{N_\mathcal{P}}/\mathcal{O}_{N_\mathcal{P}}\right) \quad .$$

Proof. We begin by proving the first isomorphism. Since $\mathcal{I}$ is G-invariant, we can write

$$\mathcal{I} = \prod_{P\in \mathrm{Div}(\mathcal{I})}\prod_{\mathcal{P}|P} \mathcal{P}^{n_P}.$$

The Chinese remainder theorem gives an $\mathcal{O}_N$ isomorphism

$$\mathcal{O}_N/\mathcal{I} \cong \bigoplus_{P\in \mathrm{Div}(\mathcal{I})} \mathcal{O}_N/(\prod_{\mathcal{P}|P}\mathcal{P}^{n_P}), \tag{5}$$

which is indeed also one of $\mathcal{O}_E[G]$-modules. In a similar way we also get an isomorphism of $\mathcal{O}_E$-modules

$$\mathcal{O}_N/(\prod_{\mathcal{P}|P}\mathcal{P}^{n_P}) \cong \prod_{\mathcal{P}|P}(\mathcal{O}_N/\mathcal{P}^{n_P})$$

for every $P\in \mathrm{Div}(\mathcal{I})$. The above isomorphism is easily seen to be G-invariant, once the right-hand side is given a G-module structure by

$$(g\cdot(x_\mathcal{P}))_{\mathcal{P}_0} = g(x_{g^{-1}(\mathcal{P}_0)})$$

for every $g\in G$, $(x_\mathcal{P})\in\prod_{\mathcal{P}|P}(\mathcal{O}_N/\mathcal{P}^{-n_P})$ and $\mathcal{P}_0 \mid P$. A standard argument shows that, for any prime $\mathcal{P}_0$ above P, we have

$$\prod_{\mathcal{P}|P}(\mathcal{O}_N/\mathcal{P}^{n_P}) \cong \mathrm{Map}_{D_{\mathcal{P}_0}}(G,\mathcal{O}_N/\mathcal{P}_0^{n_P}) \cong \mathbb{Z}[G]\otimes_{\mathbb{Z}[D_{\mathcal{P}_0}]}\mathcal{O}_N/\mathcal{P}_0^{n_P} \tag{6}$$

as $\mathcal{O}_N$-modules and $\mathcal{O}_E[G]$-modules. Note also that, for every $n\in\mathbb{N}$ and every $\mathcal{P}\mid P$, the inclusion $N\to N_P$ induces an isomorphism

$$\mathcal{O}_N/\mathcal{P}^{n_P} \cong \mathcal{O}_{N_\mathcal{P}}/\mathcal{P}^{n_P}\mathcal{O}_{N_\mathcal{P}}$$

of $\mathcal{O}_E[D_\mathcal{P}]$-modules. This shows the first isomorphism of the lemma.

The proof of the second isomorphism follows the same pattern, once one has the following analogue of the Chinese remainder theorem.

Lemma 2.7. *Let $\mathcal{J}_1,\ \mathcal{J}_2\subset\mathcal{O}_N$ be ideals with $\mathcal{J}_1+\mathcal{J}_2=\mathcal{O}_N$. Then there is an isomorphism of $\mathcal{O}_N$-modules*

$$(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{O}_N \xrightarrow{\sim} (\mathcal{J}_1)^{-1}/\mathcal{O}_N \times \mathcal{J}_2^{-1}/\mathcal{O}_N.$$

Proof. We claim that the inclusions $\mathcal{J}_1^{-1}\to(\mathcal{J}_1\mathcal{J}_2)^{-1}$ and $\mathcal{J}_2^{-1}\to(\mathcal{J}_1\mathcal{J}_2)^{-1}$ induce $\mathcal{O}_N$-isomorphisms

$$\tau_1 : \mathcal{J}_1^{-1}/\mathcal{O}_N \to (\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1} \quad\text{and}\quad \tau_2 : \mathcal{J}_2^{-1}/\mathcal{O}_N \to (\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1} \tag{7}$$

and the natural projections $(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{O}_N\to(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1}$ and $(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{O}_N\to(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}$ induce an $\mathcal{O}_N$-isomorphism

$$\tau : (\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1}\times(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}. \tag{8}$$

Write $1=j_1+j_2$ with $j_1\in\mathcal{J}_1$ and $j_2\in\mathcal{J}_2$. To show that τ_1, τ_2 and τ are injective, we only need to show that $\mathcal{J}_1^{-1}\cap\mathcal{J}_2^{-1}\subseteq\mathcal{O}_N$ (the reverse inclusion being obvious). If $j\in\mathcal{J}_1^{-1}\cap\mathcal{J}_2^{-1}$, then $j=1\cdot j=j_1j+j_2j$ and both j_1j and j_2j belong to $\mathcal{O}_N$. This shows that τ_1,τ_2 and τ are injective.

To prove the surjectivity of τ_1, let $j \in (\mathcal{J}_1\mathcal{J}_2)^{-1}$. Then $j_1 j \in \mathcal{J}_2^{-1}$ and hence $j - j_1 j$ belongs to the class of j in $(\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}$. On the other hand $j - j_1 j = j_2 j \in \mathcal{J}_1^{-1}$, which shows that τ_1 is surjective and the surjectivity of τ_2 follows by a similar argument.

As for the surjectivity of τ, take $y, z \in (\mathcal{J}_1\mathcal{J}_2)^{-1}$. One easily sees that $x = yj_1 + zj_2$ belongs to $(\mathcal{J}_1\mathcal{J}_2)^{-1}$ and

$$x \equiv yj_1 \equiv y - yj_2 \equiv y \mod \mathcal{J}_1^{-1} \quad \text{and} \quad x \equiv zj_2 \equiv z - zj_1 \equiv z \mod \mathcal{J}_2^{-1}.$$

This shows that τ is surjective and complete the proof of our claim.

The lemma then follows since

$$(\tau_1 \times \tau_2)^{-1} \circ \tau : (\mathcal{J}_1\mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1)^{-1}/\mathcal{O}_N \times \mathcal{J}_2^{-1}/\mathcal{O}_N \tag{9}$$

is an $\mathcal{O}_N$-isomorphism. □

Observe also that, if $\mathcal{J}_1$ and $\mathcal{J}_2$ moreover are G-stable ideals, then the isomorphism (9) is also an isomorphism of $\mathcal{O}_E[G]$-modules. □

2.2.2 Proposition 2.6 allows us to focus on local extensions. We put ourselves in the local setting of §2.1.2. In particular, K/k is a Γ-extension of p-adic fields and F is the subfield of K which is fixed by the inertia group Δ.

We begin by considering the local analogue $\psi_{K/k}$ of the isomorphism introduced in (3), namely $\psi_{K/k} : K \otimes_k K \to \mathrm{Map}(\Gamma, K)$ sends $x \otimes y$ to $\gamma \mapsto x\gamma(y)$. We give $K \otimes_k K$ its natural $(\Gamma \times \Gamma)$-module structure: $(\gamma, \gamma')(x \otimes y) = \gamma(x) \otimes \gamma'(y)$. Then $\psi_{K/k}$ is an isomorphism of $(\Gamma \times \Gamma)$-modules if we let $(\Gamma \times \Gamma)$ act on $\mathrm{Map}(\Gamma, K)$ by

$$\big((\gamma, \gamma')u\big)(\eta) = \gamma\big(u(\gamma^{-1}\eta\gamma')\big) \ ,$$

for all $u \in \mathrm{Map}(\Gamma, K)$, $\gamma, \gamma', \eta \in \Gamma$. Note that the action of the subgroup $1 \times \Gamma$ of $\Gamma \times \Gamma$ is the same as that introduced below (3), once $1 \times \Gamma$ is identified with Γ.

We define $\mathrm{Map}(\Gamma, K)^\Delta = \mathrm{Map}(\Gamma, K)^{\Delta \times 1}$ to be the set of invariant maps under the action of the subgroup $\Delta \times 1$ of $\Gamma \times \Gamma$. More explicitely, $\mathrm{Map}(\Gamma, K)^\Delta$ is the set of maps $u : \Gamma \to K$ such that

$$\delta(u(\eta)) = u(\delta\eta)$$

for all $\delta \in \Delta$, $\eta \in \Gamma$. We may view $\mathrm{Map}(\Gamma, K)^\Delta$ as an F-algebra with the pointwise operations and as a Γ-module where Γ acts as $1 \times \Gamma$. Then there is an isomorphism of both F-algebras and $F[\Gamma]$-modules:

$$\mathrm{Map}(\Gamma, K)^\Delta \xrightarrow{\sim} \mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K \ , \quad u \longmapsto \sum_{\gamma \in \Gamma} \gamma^{-1} \otimes u(\gamma) \tag{10}$$

where $\mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K$ is the tensor product over $\mathbb{Q}[\Delta]$ of the right $\mathbb{Q}[\Delta]$-module $\mathbb{Q}[\Gamma]$ with the left $\mathbb{Q}[\Delta]$-module K. This tensor product is given the structure of a Γ-module via its left-hand factor and the structure of an F-algebra via its right-hand factor.

The isomorphism $\psi_{K/k}$ introduced above yields an isomorphism of both F-algebras and $F[\Gamma]$-modules:

$$\psi_{K/k} : F \otimes_k K \to \mathrm{Map}(\Gamma, K)^\Delta$$

(here $F \otimes_k K$ is considered an F-algebra via its left factor and as a Γ-module via its right factor). Composing with the isomorphism in (10), we get an isomorphism

$$\tilde{\psi}_{K/k} : F \otimes_k K \xrightarrow{\sim} \mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K \ .$$

Note that $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K$ is the maximal order of $\mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K$ and, using that F/k is unramified, it is not difficult to show that $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K$ is the maximal $\mathcal{O}_F$-order of $F \otimes_k K$ (see [4, p. 214]). Therefore

$\tilde{\psi}_{K/k}$ induces the following isomorphism of rings and $\mathcal{O}_F[\Gamma]$-modules:

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K \ .$$

Lemma 2.8. *For every $n \in \mathbb{N}$, the homomorphism $\tilde{\psi}_{K/k}$ induces isomorphisms of $\mathcal{O}_F[\Gamma]$-modules*

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathcal{P}_K^n \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K/\mathcal{P}_K^n;$$
$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}/\mathcal{O}_K \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n}/\mathcal{O}_K.$$

Proof. Consider the following commutative diagram of $\mathcal{O}_F[\Gamma]$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^n & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathcal{P}_K^n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\psi}_{K/k}} & & \downarrow{\scriptstyle \tilde{\psi}_{K/k}} & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^n & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K/\mathcal{P}_K^n & \longrightarrow & 0 \end{array}$$

It has exact rows since $\mathcal{O}_F$ (resp. $\mathbb{Z}[\Gamma]$) is a flat $\mathcal{O}_k$-module (resp. $\mathbb{Z}[\Delta]$-module), being free. The central vertical arrow is an isomorphism, as remarked above. In particular, the right-hand vertical arrow is surjective. But one easily verifies that

$$\#\left(\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathcal{P}_K^n\right) = \left(\#\mathcal{O}_K/\mathcal{P}_K^n\right)^{[F:k]} = \left(\#\mathcal{O}_K/\mathcal{P}_K^n\right)^{[\Gamma:\Delta]} = \#\left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K/\mathcal{P}_K^n\right).$$

Therefore the right-hand vertical arrow is an isomorphism and so is the left-hand one by the snake lemma. This proves the first isomorphism of the lemma.

The proof of the second isomorphism is similar: consider the following commutative diagram of $\mathcal{O}_F[\Gamma]$-modules with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} & \longrightarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}/\mathcal{O}_K & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\psi}_{K/k}} & & \downarrow{\scriptstyle \tilde{\psi}_{K/k}} & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n} & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n}/\mathcal{O}_K & \longrightarrow & 0 \end{array}$$

The left-hand vertical arrow is an isomorphism. Therefore it suffices to prove that the central arrow is injective (one then conclude using a cardinality argument as above). For that purpose, it is enough to show that the map $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} \to F \otimes_k K$ is injective, thanks to the following commutative diagram of $\mathcal{O}_F[\Gamma]$-modules

$$\begin{array}{ccc} \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} & \longrightarrow & F \otimes_k K \\ \downarrow{\scriptstyle \tilde{\psi}_{K/k}} & & \downarrow{\scriptstyle \tilde{\psi}_{K/k}} \\ \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n} & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} K \end{array}$$

whose right-hand arrow is an isomorphism. Note that $F \otimes_k K$ is the localization of the $\mathcal{O}_k$-module $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}$ at the multiplicative set $k^\times$. The map $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} \to F \otimes_k K$ is then injective because $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}$ is a torsion free $\mathcal{O}_k$-module. □

The above lemma is somehow unsatisfactory, if compared for example with Proposition 2.3, because it says that the Γ-modules $\mathcal{O}_K/\mathcal{P}_K^n$ and $\mathcal{P}_K^{-n}/\mathcal{O}_K$ are induced from some Δ-module only after tensoring with $\mathcal{O}_F$. In the next subsection, introducing torsion Δ-modules coming from global cyclotomic fields, we will get rid of this scalar extension, at least when K/k is abelian.

The following proposition (which may be considered as a generalization of [4, Lemma 1.4]), shows that the Δ-modules $\mathcal{O}_K/\mathcal{P}_K^n$ and $\mathcal{P}_K^{-n}/\mathcal{O}_K$ break up in smaller pieces as in Proposition 2.5. Recall that e is the order of Δ.

Proposition 2.9. *For every $n \in \mathbb{Z}$ with $0 \leqslant n \leqslant e$, the action of $\mathcal{O}_F$ on $\mathcal{O}_K/\mathcal{P}_K^n$ and $\mathcal{P}_K^{-n}/\mathcal{O}_K$ factors through an action of $\mathcal{O}_F/\mathcal{P}_F$ and we have*

$$\mathcal{O}_K/\mathcal{P}_K^n \cong \bigoplus_{i=0}^{n-1} \mathcal{P}_K^i/\mathcal{P}_K^{i+1}$$

$$\mathcal{P}_K^{-n}/\mathcal{O}_K \cong \bigoplus_{i=1}^{n} \mathcal{P}_K^{e-i}/\mathcal{P}_K^{e-i+1}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules.

Proof. Both $\mathcal{O}_K/\mathcal{P}_K^n$ and $\mathcal{P}_K^{-n}/\mathcal{O}_K$ are $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules (see the proof of Proposition 2.5) and have the filtrations $\{\mathcal{P}_K^i/\mathcal{P}_K^n\}_{i=0}^n$ and $\{\mathcal{P}_K^{-i}/\mathcal{O}_K\}_{i=0}^n$, respectively. Since $\mathcal{O}_F/\mathcal{P}_F[\Delta]$ is semisimple, we have

$$\mathcal{O}_K/\mathcal{P}_K^n \cong \bigoplus_{i=0}^{n-1} \mathcal{P}_K^i/\mathcal{P}_K^{i+1} \qquad \text{and} \qquad \mathcal{P}_K^{-n}/\mathcal{O}_K \cong \bigoplus_{i=1}^{n} \mathcal{P}_K^{-i}/\mathcal{P}_K^{-i+1}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules. This yields the first isomorphism. Furthermore multiplication by the eth power of any uniformizer of K induces a $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-isomorphism

$$\mathcal{P}_K^{-i}/\mathcal{P}_K^{-i+1} \cong \mathcal{P}_K^{e-i}/\mathcal{P}_K^{e-i+1}.$$

We thus get the second isomorphism. □

Remark 2.10. We add a comment on the hypothesis on n in the above proposition. If $n > e$, then $\mathcal{O}_K/\mathcal{P}_K^n$ is not a semisimple $\mathcal{O}_F[\Delta]$-module. For, suppose the contrary: then we would have an isomorphism of $\mathcal{O}_F[\Delta]$-modules

$$\mathcal{O}_K/\mathcal{P}_K^n \cong \bigoplus_{i=0}^{n-1} \mathcal{P}_K^i/\mathcal{P}_K^{i+1}$$

by the same arguments as in the proof of Proposition 2.9. But this implies in particular that $\mathcal{O}_K/\mathcal{P}_K^n$ is an $\mathcal{O}_F/\mathcal{P}_F$-module, which is clearly not the case since $n > e$. However Proposition 2.9 will be useful in computing the class of $\mathcal{O}_K/\mathcal{P}_K^n$ in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$ (in the sense of Section 2.4) for arbitrary $n \in \mathbb{N}$, thanks to Proposition 2.17.

2.3 Switch to a global cyclotomic field

In this subsection we will perform a further reduction, relating the modules $\mathcal{O}_K/\mathcal{P}_K^n$, $\mathcal{P}_K^{-n}/\mathcal{O}_K$ and $\mathcal{R}_{K/F}$ to new torsion Galois modules, associated to the ring of integers of a certain cyclotomic field.

Recall that Δ is cyclic of order e. As in the Introduction μ_e denotes the group of eth roots of unity in $\overline{\mathbb{Q}}$ and $\mathfrak{o}$ is the ring of integers of $\mathbb{Q}(\mu_e)$. Let $\chi : \Delta \to \mu_e$ be a character of Δ. For any $\mathfrak{o}$-module M, we shall consider the $\mathfrak{o}[\Delta]$-module $M(\chi)$ whose underlying $\mathfrak{o}$-module is M and Δ acts as $\delta \cdot m = \chi(\delta)m$. We shall be mainly concerned with the case where M is the residue field $\kappa_\mathfrak{p} = \mathfrak{o}/\mathfrak{p}$ of a prime $\mathfrak{p} \subset \mathfrak{o}$ not dividing e.

2.3.1 We now explain the relation between the modules introduced above with those of the previous subsections. We come back to the setting of §2.1.2: in particular K/F is a Δ-Galois extension of p-adic fields which is totally and tamely ramified of degree e.

Lemma 2.11. *If $\chi : \Delta \to \mu_e$ is injective, then there exists an embedding $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ such that $\iota \circ \chi = \chi_{K/F}$.*

Proof. We first define $\iota : \mathbb{Q}(\mu_e) \to \overline{\mathbb{Q}}_p$ by setting $\iota(\chi(\delta)) = \chi_{K/F}(\delta)$ for every $\delta \in \Delta$. Note that this indeed defines an injective field homomorphism, since χ and $\chi_{K/F}$ are actually isomorphisms. Then we can extend ι to an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ in infinitely many ways and any of these extensions satisfies the requirements of the lemma. □

We now fix an injective character $\chi : \Delta \to \mu_e$ and an embedding $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ such that $\iota \circ \chi = \chi_{K/F}$. Note that $\iota(\mathfrak{o}) \subseteq \mathcal{O}_F$ (since $\mu_{e,p} \subset F$) and therefore we can view any $\mathcal{O}_F$-module as a $\mathfrak{o}$-module via ι.

Proposition 2.12. *Let $\mathfrak{p} \subset \mathfrak{o}$ be the prime ideal above p such that $\iota(\mathfrak{p}) \subset \mathcal{P}_F$. For every natural integer i and every uniformizer π_K of K, we have an isomorphism of $\mathcal{O}_F[\Delta]$-modules:*

$$\mathcal{P}_K^i/\mathcal{P}_K^{i+1} \;\cong \kappa_{\mathfrak{p}}(\chi^i) \otimes_{\kappa_{\mathfrak{p}}} \mathcal{O}_F/\mathcal{P}_F \;\;,$$

where the right-hand side of the above isomorphism is an $\mathcal{O}_F/\mathcal{P}_F$-module via its right factor and a Δ-module via its left factor.

Proof. We identify $\mathcal{O}_F/\mathcal{P}_F$ with $\mathcal{O}_K/\mathcal{P}_K$ via the inclusion $\mathcal{O}_F \subset \mathcal{O}_K$. Then sending $[\pi_K^i x] \in \mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ to $[1] \otimes [x] \in \kappa_{\mathfrak{p}}(\chi^i) \otimes_{\kappa_{\mathfrak{p}}} \mathcal{O}_F/\mathcal{P}_F$ clearly gives a $\mathcal{O}_F$-isomorphism between $\mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ and $\kappa_{\mathfrak{p}}(\chi^i) \otimes_{\kappa_{\mathfrak{p}}} \mathcal{O}_F/\mathcal{P}_F$. By (4), Δ acts as multiplication by $\chi_{K/F}^i$ on $\mathcal{P}_K^i/\mathcal{P}_K^{i+1}$ and therefore $\delta \cdot [\pi_K^i x]$ maps to

$$[1] \otimes [(\chi_{K/F}^i)(\delta)\, x] = [1] \otimes \iota\chi^i(\delta)[x] = \chi^i(\delta)[1] \otimes [x] = (\delta \cdot [1]) \otimes [x] = \delta \cdot ([1] \otimes [x]) \;\;.$$

□

We are ready for the main application of the torsion $\mathfrak{o}[\Delta]$-modules we have introduced. They allow us to write the Γ-modules $\mathcal{O}_K/\mathcal{P}_K^n$ and $\mathcal{P}_K^{-n}/\mathcal{O}_K$ as induced from some Δ-modules, at least if K/k is abelian.

Proposition 2.13. *Let $\mathfrak{p} \subset \mathfrak{o}$ be the prime ideal above p such that $\iota(\mathfrak{p}) \subset \mathcal{P}_F$. Assume that K/k is abelian and let $0 \leqslant n \leqslant e$ be an integer. Then ι induces an inclusion $\kappa_{\mathfrak{p}} \to \mathcal{O}_k/\mathcal{P}_k$ (hence $\mathcal{O}_k/\mathcal{P}_k$ is a $\kappa_{\mathfrak{p}}$-module via ι) and there are isomorphisms of $\mathcal{O}_k/\mathcal{P}_k[\Gamma]$-modules*

$$\mathcal{O}_K/\mathcal{P}_K^n \cong \mathcal{O}_k/\mathcal{P}_k \otimes_{\kappa_{\mathfrak{p}}} \Big(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \Big(\bigoplus_{i=0}^{n-1} \kappa_{\mathfrak{p}}(\chi^i)\Big)\Big) \;\;,$$

$$\mathcal{P}_K^{-n}/\mathcal{O}_K \cong \mathcal{O}_k/\mathcal{P}_k \otimes_{\kappa_{\mathfrak{p}}} \Big(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \Big(\bigoplus_{i=1}^{n} \kappa_{\mathfrak{p}}(\chi^{e-i})\Big)\Big) \;\;,$$

where the right-hand sides of the above isomorphisms are $\mathcal{O}_k/\mathcal{P}_k$-modules via their left factors and Γ-modules via their right factors.

Proof. We prove the first isomorphism, the proof of the second is similar. Our proof is inspired by that of [4, Theorem 1.7]. Using Lemma 2.8, Propositions 2.9 and 2.12, we get

$$\begin{aligned}
\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{O}_K/\mathcal{P}_K^n &\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K/\mathcal{P}_K^n \\
&\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \Big(\bigoplus_{i=0}^{n-1} \mathcal{P}_K^i/\mathcal{P}_K^{i+1}\Big) \\
&\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \Big(\Big(\bigoplus_{i=0}^{n-1} \kappa_{\mathfrak{p}}(\chi^i)\Big) \otimes_{\kappa_{\mathfrak{p}}} \mathcal{O}_F/\mathcal{P}_F\Big) \;\;.
\end{aligned}$$

Observe now that, since K/k is abelian, we have $\mu_{e,p} \subset k$ by Remark 2.4 and hence $\iota(\mathfrak{o}) \subset \mathcal{O}_k$. In particular we can write the above isomorphism as

$$\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{O}_K/\mathcal{P}_K^n \cong \Big(\Big(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \Big(\bigoplus_{i=0}^{n-1} \kappa_{\mathfrak{p}}(\chi^i)\Big)\Big) \otimes_{\kappa_{\mathfrak{p}}} \mathcal{O}_k/\mathcal{P}_k\Big) \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{O}_F/\mathcal{P}_F.$$

Since the above are isomorphisms of $\mathcal{O}_F/\mathcal{P}_F[\Gamma]$-modules of finite length, we can apply the Krull-Schmidt theorem to conclude (see [7, §6, Exercise 2]). □

Remark 2.14. If K/k is unramified, then Proposition 2.13 simply asserts that $\mathcal{O}_K/\mathcal{P}_K$ and $\mathcal{P}_K^{-1}/\mathcal{O}_K$ are free $\mathcal{O}_k/\mathcal{P}_k[\Gamma]$-modules (which is well-known and can be proved directly). In fact, if K/k is unramified, then of course it is abelian (even cyclic) and Δ is trivial. In particular $e = 1$, χ is trivial and $\kappa_{\mathfrak{p}} = \mathbb{F}_p$. Then, by Proposition 2.13, we get

$$\begin{aligned} \mathcal{O}_K/\mathcal{P}_K &\cong \mathcal{O}_k/\mathcal{P}_k \otimes_{\mathbb{F}_p} \Big(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathbb{F}_p\Big) \cong \mathcal{O}_k/\mathcal{P}_k[\Gamma]; \\ \mathcal{P}_K^{-1}/\mathcal{O}_K &\cong \mathcal{O}_k/\mathcal{P}_k \otimes_{\kappa_{\mathfrak{p}}} \Big(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathbb{F}_p\Big) \cong \mathcal{O}_k/\mathcal{P}_k[\Gamma]. \end{aligned}$$

as $\mathcal{O}_k/\mathcal{P}_k[\Gamma]$-modules.

In view of Proposition 2.13 and since we are mainly interested in $\mathcal{T}_{K/k}, \mathcal{S}_{K/k}$ and $\mathcal{R}_{K/k}$ we introduce the following notation for any prime $\mathfrak{p} \subset \mathfrak{o}$ not dividing e:

$$T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) = \bigoplus_{i=1}^{e-1} \kappa_{\mathfrak{p}}(\chi^i) \ , \tag{11}$$

$$S_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) = \bigoplus_{i=\frac{e+1}{2}}^{e-1} \kappa_{\mathfrak{p}}(\chi^i) \ , \tag{12}$$

$$R_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) = \bigoplus_{i=1}^{e-1} \kappa_{\mathfrak{p}}(\chi^i)^{\oplus i} \ . \tag{13}$$

For $S_\chi(\mathfrak{p}, \mathfrak{o}[\Delta])$ to be defined, e is required to be odd, an assumption that will always be implicit when needed.

Remark 2.15. There is a link between $T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta])$ and the Swan module $\Sigma_\Delta(p) = p\mathbb{Z}[\Delta] + \mathrm{Tr}_\Delta \mathbb{Z}[\Delta]$, where $\Delta = \langle \delta \rangle$, $\mathrm{Tr}_\Delta = \sum_{i=0}^{e-1} \delta^i \in \mathbb{Z}[\Delta]$ and p is the residual characteristic of $\mathfrak{p}$. Using the decomposition of $\kappa_{\mathfrak{p}}[\Delta]$ given by primitive idempotents, one easily gets that

$$\kappa_{\mathfrak{p}}[\Delta] \cong \bigoplus_{i=0}^{e-1} \kappa_{\mathfrak{p}}(\chi^i) \tag{14}$$

as $\mathfrak{o}[\Delta]$-modules. It follows that

$$\kappa_{\mathfrak{p}}[\Delta]/\langle \mathrm{Tr}_\Delta \rangle = T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) \ .$$

This already shows that $T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta])$ is independent of the injective character χ. Further, since

$$T(p, \mathbb{Z}[\Delta]) = \mathbb{Z}[\Delta]/\Sigma_\Delta(p) = \mathbb{F}_p[\Delta]/\langle \mathrm{Tr}_\Delta \rangle \ ,$$

we get

$$T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) = T(p, \mathbb{Z}[\Delta]) \otimes_{\mathbb{F}_p} \kappa_{\mathfrak{p}} \ .$$

The above isomorphism can be used to eliminate the hypothesis K/k abelian, at least for $\mathcal{T}_{K/k} = \mathcal{P}_K^{1-e}/\mathcal{O}_K$. Choosing $\mathfrak{p}$ as in Proposition 2.13 and arguing as in the proof of that proposition, we get

$$\begin{aligned}\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{T}_{K/k} &\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \left(\mathcal{O}_F/\mathcal{P}_F \otimes_{\kappa_\mathfrak{p}} T_\chi(\mathfrak{p}, \mathfrak{o}[\Delta])\right)\\ &\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \left(\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathbb{F}_p} T(p, \mathbb{Z}[\Delta])\right)\\ &\cong \mathcal{O}_F/\mathcal{P}_F \otimes_{\mathbb{F}_p} \left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} T(p, \mathbb{Z}[\Delta])\right)\\ &\cong \mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{O}_k/\mathcal{P}_k \otimes_{\mathbb{F}_p} \left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} T(p, \mathbb{Z}[\Delta])\right) \quad .\end{aligned}$$

Then, as in the proof of Proposition 2.13, by the Krull-Schmidt theorem we get

$$\mathcal{T}_{K/k} \cong \mathcal{O}_k/\mathcal{P}_k \otimes_{\mathbb{F}_p} \left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} T(p, \mathbb{Z}[\Delta])\right)$$

as $\mathcal{O}_k/\mathcal{P}_k[\Gamma]$-modules.

2.3.2 We now collect the results obtained so far to complete our reduction step. We recall the setting described at the beginning of this section. Let N/E be a tame G-Galois extension of number fields. For any prime P of $\mathcal{O}_E$ we fix a prime $\mathcal{P} \subseteq \mathcal{O}_N$ dividing P. Let $D_\mathcal{P}$ (resp. $I_\mathcal{P}$) denote the decomposition group (resp. the inertia subgroup) of $\mathcal{P}$ in G. Then the cardinality of $I_\mathcal{P}$ only depends on P and we denote it by e_P. Using Lemma 2.11, we fix an injective character $\chi_\mathcal{P} : I_\mathcal{P} \to \overline{\mathbb{Q}}^\times$ and an embedding $\iota_\mathcal{P} : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ (where p is the rational prime below $\mathcal{P}$ and $\overline{\mathbb{Q}}_p$ is an algebraic closure of $\mathbb{Q}_p$ containing the completion $N_\mathcal{P}$ of N at $\mathcal{P}$), such that $\iota_\mathcal{P} \circ \chi_\mathcal{P} = \chi_{N_\mathcal{P}/F_\mathcal{P}}$ where $F_\mathcal{P} = N_\mathcal{P}^{I_\mathcal{P}}$. These choices determine a prime ideal $\mathfrak{p}$ in the ring of integers $\mathfrak{o}_{e_P}$ of $\mathbb{Q}(\mu_{e_P}) \subset \overline{\mathbb{Q}}$ (where $e_P = \#I_\mathcal{P}$) satisfying $\iota_\mathcal{P}(\mathfrak{p}) \subseteq \mathcal{P}\mathcal{O}_{N_\mathcal{P}}$. Moreover $\mathcal{O}_{F_\mathcal{P}}$ is an $\mathfrak{o}_{e_P}$-module via $\iota_\mathcal{P}$. Recall that $\mathrm{Ram}(N/E)$ is the set of primes of E that ramify in N/E.

Proof of Theorem 2.1. Using Proposition 2.6 and Remark 2.15:

$$\begin{aligned}\mathcal{T}_{N/E} &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \mathcal{T}_{N_\mathcal{P}/E_P}\\ &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \left(\mathbb{Z}[D_\mathcal{P}] \otimes_{\mathbb{Z}[I_\mathcal{P}]} T(p, \mathbb{Z}[I_\mathcal{P}])\right)^{\oplus[\mathcal{O}_E/P:\mathbb{F}_p]}\end{aligned}$$

as $\mathbb{Z}[G]$-modules.

By Propositions 2.2, 2.3, 2.5 and 2.12 and with the choices of χ_P and $\iota_\mathcal{P}$ described above, we have isomorphisms of $\mathbb{Z}[G]$-modules:

$$\begin{aligned}\mathcal{R}_{N/E} &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \mathcal{R}_{N_\mathcal{P}/E_P}\right)^{\oplus[G:D_\mathcal{P}]}\\ &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \left(\mathbb{Z}[D_\mathcal{P}] \otimes_{\mathbb{Z}[I_\mathcal{P}]} R_{\chi_\mathcal{P}}(\mathfrak{p}, \mathfrak{o}_{e_P}[I_\mathcal{P}])\right)\right)^{\oplus[G:D_\mathcal{P}][\mathcal{O}_N/\mathcal{P}:\mathfrak{o}_{e_P}/\mathfrak{p}]} \quad .\end{aligned}$$

Suppose now that N/E is locally abelian. Then E_P contains the e_Pth roots of unity in $\overline{\mathbb{Q}}_p$ (as explained in Remark 2.4) and therefore $\iota_\mathcal{P}$ induces an inclusion $\mathfrak{o}_{e_P}/\mathfrak{p} \to \mathcal{O}_{E_P}/P\mathcal{O}_{E_P} \cong \mathcal{O}_E/P$. Moreover using Propositions 2.6 and 2.13 we have isomorphisms of $\mathbb{Z}[G]$-modules:

$$\begin{aligned}\mathcal{S}_{N/E} &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \mathcal{S}_{N_\mathcal{P}/E_P}\\ &\cong \bigoplus_{P \in \mathrm{Ram}(N/E)} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \left(\mathbb{Z}[D_\mathcal{P}] \otimes_{\mathbb{Z}[I_\mathcal{P}]} S_{\chi_\mathcal{P}}(\mathfrak{p}, \mathfrak{o}_{e_P}[I_\mathcal{P}])\right)^{\oplus[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]} \quad .\end{aligned}$$

□

For torsion modules arising from general G-stable ideals we no more have isomorphisms as in Theorem 2.1 but still equalities of classes in $\mathrm{Cl}(\mathbb{Z}[G])$, in the sense we shall now explain.

2.4 Classes of cohomologically trivial modules

2.4.1 In this subsection G is an arbitrary finite group (we do not need it to be the Galois group of a particular extension of number fields). We will interpret the results we have obtained so far in terms of classes in the locally free class group. Recall that a G-module M is G-cohomologically trivial if, for every $i \in \mathbb{Z}$ and every subgroup $G' < G$, the Tate cohomology group $\hat{H}^i(G', M)$ is trivial. If A is the ring of integers of a number field, let $\mathrm{Cl}(A[G])$ be the locally free class group of $A[G]$ (see [14, I, §2] for locally free modules and the locally free class group).

Lemma 2.16. *Let A be the ring of integers of a number field. Let M be a finitely generated $A[G]$-module.*

(i) M is $A[G]$-projective if and only if it is $A[G]$-locally free.

(ii) M is G-cohomologically trivial if and only if there exists an $A[G]$-resolution $0 \to P_1 \to P_0 \to M \to 0$ of M with P_0 and P_1 locally free. In this case the class $(P_0)^{-1}(P_1)$ in $\mathrm{Cl}(A[G])$ is independent of the chosen locally free resolution of M and will be denoted by $(M)_{A[G]}$.

(iii) If G is a subgroup of a finite group $\tilde{G}$ and M is G-cohomologically trivial, then $M \otimes_{A[G]} A[\tilde{G}]$ is $\tilde{G}$-cohomologically trivial and

$$(M \otimes_{A[G]} A[\tilde{G}])_{A[\tilde{G}]} = \mathrm{Ind}_G^{\tilde{G}}\big((M)_{A[G]}\big)$$

where $\mathrm{Ind}_G^{\tilde{G}} : \mathrm{Cl}(A[G]) \to \mathrm{Cl}(A[\tilde{G}])$ is the map which sends the class $(P)_{A[G]} \in \mathrm{Cl}(A[G])$ of a locally free $A[G]$-module P to the class $(P \otimes_{A[G]} A[\tilde{G}]) \in \mathrm{Cl}(A[\tilde{G}])$.

Proof. For (i) and the first assertion of (ii) see for example [5, Proposition 4.1] ((i) is a classical result of Swan). The last assertion of (ii) follows immediately from Schanuel's lemma.

To prove (iii), suppose that M is G-cohomologically trivial. Then, by (i) and (ii), there exists exact sequence of $A[G]$-modules

$$0 \to P_1 \to P_0 \to M \to 0$$

with P_0, P_1 projective. Observe that $A[\tilde{G}]$ is a free $A[G]$-module. In particular the functor $- \otimes_{A[G]} A[\tilde{G}]$ from the category of $A[G]$-modules to that of $A[\tilde{G}]$-modules is exact and we get an exact sequence of $A[\tilde{G}]$-modules

$$0 \to P_1 \otimes_{A[G]} A[\tilde{G}] \to P_0 \otimes_{A[G]} A[\tilde{G}] \to M \otimes_{A[G]} A[\tilde{G}] \to 0. \tag{15}$$

Note that, for $i = 0, 1$, $P_i \otimes_{A[G]} A[\tilde{G}]$ is $A[\tilde{G}]$-projective since P_i is $A[G]$-projective (this can be easily seen using the characterization of projective modules as direct summand of free modules). In particular, the exact sequence (15) implies that $M \otimes_{A[G]} A[\tilde{G}]$ is $\tilde{G}$-cohomologically trivial by (i) and (ii). Moreover we have

$$\begin{aligned}
(M \otimes_{A[G]} A[\tilde{G}])_{A[\tilde{G}]} &= (P_0 \otimes_{A[G]} A[\tilde{G}])^{-1}(P_1 \otimes_{A[G]} A[\tilde{G}]) \\
&= \mathrm{Ind}_G^{\tilde{G}}\big((P_0)_{A[G]}\big)^{-1}\mathrm{Ind}_G^{\tilde{G}}\big((P_1)_{A[G]}\big) \\
&= \mathrm{Ind}_G^{\tilde{G}}\big((P_0)_{A[G]}^{-1}(P_1)_{A[G]}\big) \\
&= \mathrm{Ind}_G^{\tilde{G}}\big((M)_{A[G]}\big)
\end{aligned}$$

in $\mathrm{Cl}(A[\tilde{G}])$. □

In this section we will use the above lemma when $A = \mathbb{Z}$ but later we will also need the case where A is the ring of integers of a cyclotomic field. If M is a finitely generated $\mathbb{Z}[G]$-module which is cohomologically trivial, we will denote $(M)_{\mathbb{Z}[G]} \in \mathrm{Cl}(\mathbb{Z}[G])$ simply by (M).

2.4.2 We first put ourselves in the local setting of §2.1.2. In particular K/k is a tame Γ-Galois extension of p-adic fields with inertia subgroup Δ and $F = K^{\Delta}$. Note that for every $a, b \in \mathbb{Z}$ with $b \geqslant a$, the $\mathbb{Z}[\Gamma]$-module $\mathcal{P}_K^a/\mathcal{P}_K^b$ is Γ-cohomologically trivial. This follows immediately from the fact that $\mathcal{P}_K^a$ and $\mathcal{P}_K^b$ are Γ-cohomologically trivial (see [34, Theorem 2]).

Proposition 2.17. *For every $m, n \in \mathbb{N}$ such that $n \equiv m \mod e$, we have*

$$(\mathcal{O}_K/\mathcal{P}_K^n) = (\mathcal{O}_K/\mathcal{P}_K^m) \in \mathrm{Cl}(\mathbb{Z}[\Gamma]) \ . \tag{16}$$

Proof. Without loss of generality we may assume that $n \geqslant m$ and write $n = m + ae$ for some $a \in \mathbb{N}$. It is clear that

$$(\mathcal{O}_K/\mathcal{P}_K^n) = (\mathcal{O}_K/\mathcal{P}_K^m)(\mathcal{P}_K^m/\mathcal{P}_K^n) = (\mathcal{O}_K/\mathcal{P}_K^m)\prod_{j=1}^{a}(\mathcal{P}_K^{m+(j-1)e}/\mathcal{P}_K^{m+je})$$

in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$. Thus we only have to prove that, for every $b \in \mathbb{N}$, $(\mathcal{P}_K^b/\mathcal{P}_K^{b+e}) = 0$ in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$. Arguing as in the proof of Proposition 2.5, we observe that $\mathcal{P}_K^b/\mathcal{P}_K^{b+e}$ is an $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-module and, since $\mathcal{O}_F/\mathcal{P}_F[\Delta]$ is semisimple, we have an isomorphism of $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules

$$\mathcal{P}_K^b/\mathcal{P}_K^{b+e} \cong \bigoplus_{i=0}^{e-1} \mathcal{P}_K^{b+i}/\mathcal{P}_K^{b+i+1} \ .$$

As remarked in the proof of Proposition 2.5, $\mathcal{P}_K^{b+i}/\mathcal{P}_K^{b+i+1}$ is an $\mathcal{O}_F/\mathcal{P}_F$-vector space of dimension 1 on which Δ acts by multiplication by $\chi_{K/F}^{b+i}$. Thus using the decomposition of $\mathcal{O}_F/\mathcal{P}_F[\Delta]$ given by primitive idempotents we get

$$\bigoplus_{i=0}^{e-1} \mathcal{P}_K^{b+i}/\mathcal{P}_K^{b+i+1} \cong \mathcal{O}_F/\mathcal{P}_F[\Delta] \cong \mathcal{O}_F/\mathcal{P}_F \otimes_{\mathbb{F}_p} \mathbb{F}_p[\Delta] \tag{17}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules. Now it easily follows from Lemma 2.8 that

$$\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{P}_K^b/\mathcal{P}_K^{b+e} \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^b/\mathcal{P}_K^{b+e}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Gamma]$-modules. Therefore using (17) we get isomorphisms

$$\begin{aligned}\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \mathcal{P}_K^b/\mathcal{P}_K^{b+e} &\cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \left(\mathcal{O}_F/\mathcal{P}_F \otimes_{\mathbb{F}_p} \mathbb{F}_p[\Delta]\right) \\ &\cong \mathcal{O}_F/\mathcal{P}_F \otimes_{\mathbb{F}_p} \mathbb{F}_p[\Gamma] \\ &\cong \mathcal{O}_F/\mathcal{P}_F \otimes_{\mathcal{O}_k/\mathcal{P}_k} \left(\mathcal{O}_k/\mathcal{P}_k \otimes_{\mathbb{F}_p} \mathbb{F}_p[\Gamma]\right)\end{aligned}$$

of $\mathcal{O}_F/\mathcal{P}_F[\Gamma]$-modules. As in the proof of Proposition 2.13, we can apply the Krull-Schmidt theorem and deduce that $\mathcal{P}_K^b/\mathcal{P}_K^{b+e}$ and $\mathcal{O}_k/\mathcal{P}_k \otimes_{\mathbb{F}_p} \mathbb{F}_p[\Gamma]$ are isomorphic $\mathcal{O}_k[\Gamma]$-modules (and hence in particular as $\mathbb{Z}[\Gamma]$-modules). Now $\mathbb{F}_p[\Gamma]$ is a cohomologically trivial Γ-module whose class in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$ is trivial, thanks to the $\mathbb{Z}[G]$-free resolution

$$0 \to p\mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{F}_p[G] \to 0.$$

We have thus proved what we wanted. □

2.4.3 We now come back to the global setting of §2.3.2. Thus N/E is a tame G-Galois extension of number fields. Note that every G-stable fractional ideal of N is $\mathbb{Z}[G]$-projective (see [35, Proposition 1.3]) hence locally free by Lemma 2.16 (i). In particular, if $\mathcal{I}$ is a G-stable ideal of $\mathcal{O}_N$, then $\mathcal{O}_N/\mathcal{I}$ and $\mathcal{I}^{-1}/\mathcal{O}_N$ are G-cohomologically trivial (by Lemma 2.16 (ii)). Therefore we can consider the classes $(\mathcal{O}_N/\mathcal{I})$ and $(\mathcal{I}^{-1}/\mathcal{O}_N)$ in $\mathrm{Cl}(\mathbb{Z}[G])$ and in fact

$$(\mathcal{O}_N/\mathcal{I}) = (\mathcal{I})(\mathcal{O}_N)^{-1} \quad \text{and} \quad (\mathcal{I}^{-1}/\mathcal{O}_N) = (\mathcal{O}_N)(\mathcal{I}^{-1})^{-1}.$$

Similarly, $\mathcal{R}_{N/E}$ defines a class in $\mathrm{Cl}(\mathbb{Z}[G])$. In fact $\mathrm{Map}(G, \mathcal{O}_N)$ is $\mathcal{O}_N[G]$-free of rank 1 (hence $\mathbb{Z}[G]$-free of rank $[N:\mathbb{Q}]$) and $\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N$ is $\mathcal{O}_N[G]$-locally free (since $\mathcal{O}_N$ is $\mathcal{O}_E[G]$-locally free by Noether's theorem). Thus, in this case,

$$(\mathcal{R}_{N/E}) = (\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) \in \mathrm{Cl}(\mathbb{Z}[G]) \ .$$

Note also that, for every prime P of $\mathcal{O}_E$ and any integer i, the $I_\mathcal{P}$-module $(\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi_\mathcal{P}^i)$ is cohomologically trivial. In fact, for every $i \in \mathbb{Z}$ and every subgroup $I < I_\mathcal{P}$, $\hat{H}^i(I, (\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi_\mathcal{P}^i))$ is annihilated by e_P (see [25, Chapitre VIII, Corollaire 1 to Proposition 3]) and p (since p annihilates $(\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi_\mathcal{P}^i)$). Since N/E is tame, we have $(p, e_P) = 1$ and hence $\hat{H}^i(I, (\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi_\mathcal{P}^i)) = 0$. Thanks to Lemma 2.16 (ii) this allows us to consider the class $\big((\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi_\mathcal{P}^i)\big) \in \mathrm{Cl}(\mathbb{Z}[I_\mathcal{P}])$.

Proposition 2.18. *Let $\mathcal{I}$ be a G-stable ideal of $\mathcal{O}_N$ and assume that N/E is locally abelian at $P \in \mathrm{Div}(\mathcal{I})$. For every prime $P \in \mathrm{Div}(\mathcal{I})$, fix a prime $\mathcal{P}$ of $\mathcal{O}_N$ dividing P and let n_P be the valuation of $\mathcal{I}$ at $\mathcal{P}$ (this indeed depends only on P). For every choice of injective characters $\chi_\mathcal{P} : I_\mathcal{P} \to \overline{\mathbb{Q}}^\times$ for every prime $\mathcal{P}$ as above, one can find primes $\mathfrak{p} \subset \mathfrak{o}_{e_P}$ and injections $\mathfrak{o}_{e_P}/\mathfrak{p} \to \mathcal{O}_N/\mathcal{P}$ such that we have equalities*

$$(\mathcal{O}_N/\mathcal{I}) = \prod_{P \in \mathrm{Div}(\mathcal{I})} \prod_{i=0}^{m_P-1} \mathrm{Ind}_{I_\mathcal{P}}^G \left((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi_\mathcal{P}^i)\right)^{[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]}$$

$$(\mathcal{I}^{-1}/\mathcal{O}_N) = \prod_{P \in \mathrm{Div}(\mathcal{I})} \prod_{i=1}^{m_P} \mathrm{Ind}_{I_\mathcal{P}}^G \left((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi_\mathcal{P}^{e-i})\right)^{[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]}$$

in $\mathrm{Cl}(\mathbb{Z}[G])$, where m_P is the smallest nonnegative integer congruent to n_P modulo e_P. In particular, if $\mathcal{I}$ is coprime with the different of N/E, then $(\mathcal{O}_N/\mathcal{I}) = (\mathcal{I}^{-1}/\mathcal{O}_N) = 1$.

Proof. We prove only one of the two displayed equalities, namely the first one, since the other follows by similar arguments. First of all note that we have an isomorphism of $\mathcal{O}_E[G]$-modules

$$\mathcal{O}_N/\mathcal{I} \cong \bigoplus_{P \in \mathrm{Div}(\mathcal{I})} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_\mathcal{P}]} \mathcal{O}_{N_\mathcal{P}}/\mathcal{P}^{n_P}\mathcal{O}_{N_\mathcal{P}} \tag{18}$$

by Proposition 2.6. By Propositions 2.17 and 2.13 we have

$$\begin{aligned}(\mathcal{O}_{N_\mathcal{P}}/\mathcal{P}^{n_P}\mathcal{O}_{N_\mathcal{P}}) &= (\mathcal{O}_{N_\mathcal{P}}/\mathcal{P}^{m_P}\mathcal{O}_{N_\mathcal{P}}) \\ &= \left(\mathbb{Z}[D_\mathcal{P}] \otimes_{\mathbb{Z}[I_\mathcal{P}]} \Big(\bigoplus_{i=0}^{m_P-1} (\mathfrak{o}_{e_P}/\mathfrak{p})(\chi_\mathcal{P}^i)\Big)\right)^{[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]}\end{aligned}$$

in $\mathrm{Cl}(\mathbb{Z}[D_\mathcal{P}])$, which together with (18) and Lemma 2.16 (iii) gives the first equality of the proposition.

To prove the last assertion, note that if $\mathcal{I}$ is coprime with the different of N/E, then for every $\mathcal{P} \mid \mathcal{I}$ we have $I_\mathcal{P} = 1$. In particular, $\chi_\mathcal{P}$ is trivial, $e_P = 1$ and $\mathfrak{o}_{e_P}/\mathfrak{p} = \mathbb{F}_p$ (thus we are in situation similar to

that of Remark 2.14). Therefore, for every $i \in \mathbb{Z}$, using Lemma 2.16 (iii)

$$\begin{aligned}\mathrm{Ind}_{I_\mathcal{P}}^G\left((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi_\mathcal{P}^i)\right) &= \left((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi_\mathcal{P}^i)\otimes_{\mathbb{Z}[I_\mathcal{P}]}\mathbb{Z}[G]\right)\\ &= (\mathbb{F}_p\otimes_{\mathbb{Z}}\mathbb{Z}[G])\\ &= (\mathbb{F}_p[G]).\end{aligned}$$

As in the proof of Proposition 2.17, we observe that $(\mathbb{F}_p[G]) = 1$, which concludes the proof of the proposition. □

The above proposition can be used to prove the following interesting result. Recall that we regard $\mathcal{O}_N\otimes_{\mathcal{O}_E}\mathcal{O}_N$ as a $\mathbb{Z}[G]$-module with the action defined in §2.1.1, *i.e.* G only acts on the right-hand factor.

Proposition 2.19. *We have*

$$(\mathcal{O}_N\otimes_{\mathcal{O}_E}\mathcal{O}_N) = (\mathcal{O}_N)^{[N:E]} \quad \textit{in } \mathrm{Cl}(\mathbb{Z}[G]).$$

Proof. Set $n = [N : E]$. By the structure theorem for $\mathcal{O}_E$-modules, we know that $\mathcal{O}_N$ is $\mathcal{O}_E$-isomorphic to $\mathcal{O}_E^{\oplus(n-1)}\oplus J$, where J is an ideal of $\mathcal{O}_E$. By Chebotarev's density theorem, we can find an ideal I of $\mathcal{O}_E$ belonging to the ideal class of J and such that I is coprime with the discriminant of N/E. In particular $\mathcal{O}_N$ is also $\mathcal{O}_E$-isomorphic to $\mathcal{O}_E^{\oplus(n-1)}\oplus I$ and

$$\mathcal{O}_N\otimes_{\mathcal{O}_E}\mathcal{O}_N \cong \left(\mathcal{O}_E\otimes_{\mathcal{O}_E}\mathcal{O}_N\right)^{\oplus(n-1)}\oplus\left(I\otimes_{\mathcal{O}_E}\mathcal{O}_N\right)\cong\mathcal{O}_N^{\oplus(n-1)}\oplus I\mathcal{O}_N$$

as $\mathcal{O}_E[G]$-modules (since G only acts on the right-hand term of $\mathcal{O}_N\otimes_{\mathcal{O}_E}\mathcal{O}_N$). In particular we get

$$(\mathcal{O}_N\otimes_{\mathcal{O}_E}\mathcal{O}_N) = (\mathcal{O}_N)^{n-1}(I\mathcal{O}_N) \quad \text{in } \mathrm{Cl}(\mathbb{Z}[G]). \tag{19}$$

Now $I\mathcal{O}_N$ is of course a G-stable ideal of $\mathcal{O}_N$ since I is an ideal of $\mathcal{O}_E$. In particular $I\mathcal{O}_N$ is locally free because N/E is tame (see [35, Proposition 1.3]) and $\mathcal{O}_N/I\mathcal{O}_N$ is G-cohomologically trivial by Lemma 2.16 (ii). Moreover we have

$$(I\mathcal{O}_N) = (\mathcal{O}_N)(\mathcal{O}_N/I\mathcal{O}_N) \quad \text{in } \mathrm{Cl}(\mathbb{Z}[G]).$$

Note that $I\mathcal{O}_N$ is coprime with the different of N/E. In particular $(\mathcal{O}_N/I\mathcal{O}_N) = 1$ by Proposition 2.18 and therefore $(I\mathcal{O}_N) = (\mathcal{O}_N)$. Plugging this equality in (19) we get the statement of the proposition. □

2.4.4 We end this section by showing how Theorem 2.1 can be used to reduce the proof of Theorem 2 to that of Theorem 1

Proof of Theorem 2 assuming Theorem 1. By Theorem 2.1 and using Lemma 2.16 (iii), we have the following equalities in $\mathrm{Cl}(\mathbb{Z}[G])$:

$$(\mathcal{R}_{N/E}) = \prod_{P\in\mathrm{Ram}(N/E)}\mathrm{Ind}_{I_\mathcal{P}}^G\left(R_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])\right)^{[G:D_\mathcal{P}][\mathcal{O}_N/\mathcal{P}:\mathfrak{o}_{e_P}/\mathfrak{p}]},$$

$$(\mathcal{T}_{N/E}) = \prod_{P\in\mathrm{Ram}(N/E)}\mathrm{Ind}_{I_\mathcal{P}}^G\left(T(p,\mathbb{Z}[I_\mathcal{P}])\right)^{[\mathcal{O}_E/P:\mathbb{F}_p]}$$

and, if N/E is locally abelian,

$$(\mathcal{S}_{N/E}) = \prod_{P\in\mathrm{Ram}(N/E)}\mathrm{Ind}_{I_\mathcal{P}}^G\left(S_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])\right)^{[\mathcal{O}_E/P:\mathfrak{o}_{e_P}/\mathfrak{p}]}.$$

By Theorem 1, for every prime $P\in\mathrm{Ram}(N/E)$ and every prime $\mathcal{P}\mid P$ in $\mathcal{O}_N$, we have

$$(T(p,\mathbb{Z}[I_\mathcal{P}])) = (S_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])) = (R_{\chi_\mathcal{P}}(\mathfrak{p},\mathfrak{o}_{e_P}[I_\mathcal{P}])) = 1$$

in $\mathrm{Cl}(\mathbb{Z}[I_{\mathcal{P}}])$. Thus $(\mathcal{T}_{N/E}) = 1$ which implies $(\mathcal{O}_N) = (\mathcal{C}_{N/E})$. Moreover $(\mathcal{R}_{N/E}) = 1$ which gives $(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) = (\mathcal{O}_N[G])$ and, since $\mathcal{O}_N[G]$ is $\mathbb{Z}[G]$-free of rank $[N:\mathbb{Q}]$, we deduce $(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N) = 1$. In particular we also have $(\mathcal{O}_N)^{[N:E]} = 1$ by Proposition 2.19. Finally, if N/E is locally abelian, we have $(\mathcal{S}_{N/E}) = 1$ which implies $(\mathcal{O}_N) = (\mathcal{A}_{N/E})$. The proof of Theorem 2 is then achieved. □

3. Hom-representatives

We now come to the proof of Theorem 1, which will be achieved in two steps. In this section, we apply Fröhlich's machinery to get a first description of Hom-representatives of the classes involved in its statement. Then in the next section we use Stickelberger's theorem to refine this description and complete the proof.

We are thus in the cyclotomic setting introduced in the previous section, namely we fix an integer e, a cyclic group Δ of order e and an injective character $\chi : \Delta \to \mu_e$, where μ_e is the group of eth roots of unity in $\overline{\mathbb{Q}}$. We let $\mathfrak{o}$ denote the ring of integers of the cyclotomic field $\mathbb{Q}(\mu_e)$. Let p denote a rational prime such that $p \nmid e$ and let $\mathfrak{p} \subset \mathfrak{o}$ denote a prime ideal above p. We set $\kappa = \mathfrak{o}/\mathfrak{p}$,

$$T_{\mathbb{Z}} = T(p, \mathbb{Z}[\Delta]) \ , \quad R = R_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) \ , \quad S = S_\chi(\mathfrak{p}, \mathfrak{o}[\Delta]) \ .$$

We fix a primitive eth root of unity $\zeta \in \mu_e$ and we let $\delta \in \Delta$ be defined by $\chi(\delta) = \zeta$.

3.1 Hom description of the class group

In this section and the following one, we are interested in determining classes in the class group $\mathrm{Cl}(\mathbb{Z}[\Delta])$. In order to do so, at some point we shall have to consider class groups of a group algebra with a larger coefficient ring. Further in Section 5 we shall also need a description of the class group of the group algebra $\mathbb{Z}[G]$ where G is any finite group. So we will recall Fröhlich's Hom-description in its most general form. If L is any number field with $L \subset \overline{\mathbb{Q}}$, we set $\Omega_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and we let $\mathfrak{o}_L$ and $J(L)$ denote the ring of integers and the idèle group of L, respectively.

3.1.1 Fröhlich's Hom-description of $\mathrm{Cl}(\mathfrak{o}_L[G])$, where L is a number field and G is a finite group, is the group isomorphism

$$\mathrm{Cl}(\mathfrak{o}_L[G]) \cong \frac{\mathrm{Hom}_{\Omega_L}(R_G, J(L'))}{\mathrm{Hom}_{\Omega_L}(R_G, (L')^\times)\mathrm{Det}(\mathcal{U}(\mathfrak{o}_L[G]))} \tag{20}$$

given by the explicit construction of a representative homomorphism of the class of any locally free rank one module, see [14, Theorem 1]. This construction will be shown and used in the next subsections. We now briefly explain the objects involved in (20), referring to [14] for a more complete account of Fröhlich's Hom-description.

We begin with the upper part, where R_G is the additive group of virtual characters of G with values in $\overline{\mathbb{Q}}$. The number field L' is "big enough", in particular it is Galois over $\mathbb{Q}$, contains L and the values of the characters of G. In our cyclotomic setting described above, we shall only be concerned with the cases where $L = \mathbb{Q}$ or $\mathbb{Q}(\mu_e)$ and $G = \Delta$: since Δ is cyclic of order e, in these cases one can take $L' = \mathbb{Q}(\mu_e) \subset \overline{\mathbb{Q}}$. The homomorphisms in $\mathrm{Hom}_{\Omega_L}(R_G, J(L'))$ are those which commute with the natural actions of Ω_L on R_G and $J(L')$.

In the lower part, $\mathrm{Hom}_{\Omega_L}(R_G, (L')^\times)$ is the subgroup of $\mathrm{Hom}_{\Omega_L}(R_G, J(L'))$ yielded by the diagonal embedding of $(L')^\times$ in $J(L')$. The second factor needs more explanations. First

$$\mathcal{U}(\mathfrak{o}_L[G]) = \prod_{\mathfrak{l}} \mathfrak{o}_{L_\mathfrak{l}}[G]^\times \subseteq \prod_{\mathfrak{l}} L_\mathfrak{l}[G]^\times \ ,$$

where $\mathfrak{l}$ runs over all places of L and $\mathfrak{o}_{L_\mathfrak{l}}$ denotes the ring of integers of a completion $L_\mathfrak{l}$ of L at $\mathfrak{l}$ (with $\mathfrak{o}_{L_\mathfrak{l}} = L_\mathfrak{l}$ if $\mathfrak{l}$ is archimedean). Let $x = (x_\mathfrak{l})_\mathfrak{l} \in \prod_\mathfrak{l} L_\mathfrak{l}[G]^\times$, the character function $\mathrm{Det}(x) = (\mathrm{Det}(x_\mathfrak{l}))_\mathfrak{l}$ is defined componentwise. For each place $\mathfrak{l}$ of L the 'semi-local' component $\mathrm{Det}(x_\mathfrak{l})$ takes values in $(L' \otimes_L L_\mathfrak{l})^\times$, embedded in $J_\mathfrak{l}(L') = \prod_{\mathfrak{L}|\mathfrak{l}}(L'_\mathfrak{L})^\times$, where $\mathfrak{L}$ runs over the prime ideals of $\mathfrak{o}_{L'}$ above $\mathfrak{l}$, through the isomorphism of L'-algebras

$$L' \otimes_L L_\mathfrak{l} \cong \prod_{\mathfrak{L}|\mathfrak{l}} L'_\mathfrak{L} \tag{21}$$

built on the various embeddings of L' in $\bar{L}_\mathfrak{l}$, a given algebraic closure of $L_\mathfrak{l}$, that fix $\mathfrak{l}$. By linearity we only need to define the character function $\mathrm{Det}(x_\mathfrak{l})$ on the irreducible characters θ of G. Write $x_\mathfrak{l} = \sum_{g\in G} x_{\mathfrak{l},g} g$, then $\mathrm{Det}_\theta(x_\mathfrak{l})$ is the image in $J_\mathfrak{l}(L')$, under isomorphism (21), of the determinant of the matrix

$$\sum_{g\in G} x_{\mathfrak{l},g}\Theta(g) \ ,$$

where Θ is any matrix representation of character θ and the (i,j)-entry of the above matrix $\sum_{g\in G}\Theta_{i,j}(g)\otimes x_{\mathfrak{l},g}$ indeed belongs to $L' \otimes_L L_\mathfrak{l}$.

Note that, by Ω_L-equivariance, the values of $\mathrm{Det}(x_\mathfrak{l}) = \big(\mathrm{Det}(x_\mathfrak{l})_\mathfrak{L}\big)_{\mathfrak{L}|\mathfrak{l}}$ in $J_\mathfrak{l}(L')$ are determined by those of any component $\mathrm{Det}(x_\mathfrak{l})_\mathfrak{L}$, see [14, II, Lemma 2.1]. In the following we may thus implicitely assume that a place $\mathfrak{L}$ of L' is fixed above each place $\mathfrak{l}$ of L and focus on the $\mathfrak{L}$-component $\mathrm{Det}(x_\mathfrak{l})_\mathfrak{L}$, that we shall indeed plainly denote by $\mathrm{Det}(x_\mathfrak{l})$, omitting the unnecessary subscript. Let l denote the rational place below $\mathfrak{l}$ and $\overline{\mathbb{Q}}_l$ an algebraic closure of $\mathbb{Q}_l$ containing $L'_\mathfrak{L}$. The resulting local function $\mathrm{Det}(x_\mathfrak{l})$ belongs to $\mathrm{Hom}_{\Omega_{L_\mathfrak{l}}}(R_{G,l}, (L'_\mathfrak{L})^\times)$, where $R_{G,l}$ is the group of virtual characters of G with values in $\overline{\mathbb{Q}}_l$ and $\Omega_{L_\mathfrak{l}} = \mathrm{Gal}(\overline{\mathbb{Q}}_l, L_\mathfrak{l})$.

3.1.2 We now assume that G is abelian. With the above notation and conventions, we get

$$\mathrm{Det}_\theta(x_\mathfrak{l}) = \sum_{g\in G} x_{\mathfrak{l},g}\theta(g) \in L'_\mathfrak{L} \ ,$$

where we have implicitely embedded L' in $L'_\mathfrak{L}$ (in accordance with the above choice of a place $\mathfrak{L}$ above $\mathfrak{l}$).

Proposition 3.1. *With the above notation and assuming that G is abelian, the group homomorphism* $\mathrm{Det} : L_\mathfrak{l}[G]^\times \to \mathrm{Hom}_{\Omega_{L_\mathfrak{l}}}(R_{G,l}, (L'_\mathfrak{L})^\times)$ *is injective.*

Proof. See [14, (II.5.2)]. □

We shall use the above result in Section 4.

3.2 Hom-representative of $(T_\mathbb{Z})$

We shall consider, as in Remark 2.15, the Swan module $\Sigma_\Delta(p) = p\mathbb{Z}[\Delta] + \mathrm{Tr}_\Delta\mathbb{Z}[\Delta]$ and its associated torsion module $T_\mathbb{Z} = \mathbb{Z}[\Delta]/\Sigma_\Delta(p)$. In other words we have the following exact sequence of $\mathbb{Z}[\Delta]$-modules:

$$0 \to \Sigma_\Delta(p) \to \mathbb{Z}[\Delta] \to T_\mathbb{Z} \to 0.$$

As remarked by Swan (see [28, §6]), $\Sigma_\Delta(p)$ is $\mathbb{Z}[\Delta]$-projective hence locally free by Lemma 2.16 (i). In particular, by Lemma 2.16 (ii), $T_\mathbb{Z}$ is Δ-cohomologically trivial and we have an equality $\big(T_\mathbb{Z}\big) = \big(\Sigma_\Delta(p)\big)$ in $\mathrm{Cl}(\mathbb{Z}[\Delta])$. We now follow Fröhlich's recipe to build a representative morphism v for this class.

If x and y are elements of a same set, we let $\delta_{x,y}$ denote their Kronecker delta, namely $\delta_{x,y} = 1$ if $x = y$, 0 otherwise.

Lemma 3.2. *Let $v \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, J(\mathbb{Q}))$ be defined by*

$$v(\chi^h)_q = \begin{cases} 1 & \text{if } q \neq p, \\ p^{1-\delta_{h,e}} & \text{if } q = p, \end{cases}$$

where q is any rational prime and $h \in \{1, \dots, e\}$. Then v represents the class of $\Sigma_\Delta(p)$ through Fröhlich's Hom-description of $\mathrm{Cl}(\mathbb{Z}[\Delta])$.

Proof. As remarked above the $\mathbb{Z}[\Delta]$-module $\Sigma_\Delta(p)$ is locally free. For any rational prime q, we will now find a generator α_q of the free $\mathbb{Z}_q[\Delta]$-module $\mathbb{Z}_q \otimes_\mathbb{Z} \Sigma_\Delta(p)$.

- $q \neq p$: since p is invertible in $\mathbb{Z}_q$, we have $\mathbb{Z}_q \otimes_\mathbb{Z} \Sigma_\Delta(p) = \mathbb{Z}_q[\Delta]$, so we can take $\alpha_q = 1$.
- $q = p$: set $\varepsilon_0 = \frac{1}{e}\mathrm{Tr}_\Delta$ and $\varepsilon_1 = 1 - \varepsilon_0$. Note that $\varepsilon_0, \varepsilon_1 \in \mathbb{Z}_p[\Delta]$ since $e \in \mathbb{Z}_p^\times$. We have $\mathbb{Z}_p \otimes_\mathbb{Z} \Sigma_\Delta(p) = p\mathbb{Z}_p[\Delta] + \varepsilon_0\mathbb{Z}_p[\Delta]$ and, since $\varepsilon_i\varepsilon_j = \delta_{i,j}\varepsilon_i$ for $i, j \in \{0, 1\}$,

  $$p = (\varepsilon_0 + p\varepsilon_1)(p\varepsilon_0 + \varepsilon_1) \quad \text{and} \quad \varepsilon_0 = (\varepsilon_0 + p\varepsilon_1)\varepsilon_0 \ ,$$

  so that

  $$p\mathbb{Z}_p[\Delta] + \varepsilon_0\mathbb{Z}_p[\Delta] \subseteq (\varepsilon_0 + p\varepsilon_1)\mathbb{Z}_p[\Delta].$$

  On the other hand $\varepsilon_0 + p\varepsilon_1$ clearly belongs to $p\mathbb{Z}_p[\Delta] + \varepsilon_0\mathbb{Z}_p[\Delta]$, hence $\mathbb{Z}_p \otimes_\mathbb{Z} \Sigma_\Delta(p) = (\varepsilon_0 + p\varepsilon_1)\mathbb{Z}_p[\Delta]$ and we can take $\alpha_p = \varepsilon_0 + p\varepsilon_1$.

By Fröhlich's theory, the morphism $\chi^h \mapsto \left(\mathrm{Det}_{\chi^h}(\alpha_q)\right)_q$ represents the class of $\Sigma_\Delta(p)$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, J(\mathbb{Q}))$. The basic computations $\mathrm{Det}_{\chi^h}(\varepsilon_0) = \delta_{h,e}$ and $\mathrm{Det}_{\chi^h}(\varepsilon_1) = 1 - \delta_{h,e}$ yield the result. □

Remark 3.3. Dividing v by the global valued equivariant morphism $\tilde{c}_v$ defined by $\tilde{c}_v(\chi^h) = p^{1-\delta_{h,e}}$, $1 \leqslant h \leqslant e$, yields another representative morphism of the class of $\Sigma_\Delta(p)$ in $\mathrm{Cl}(\mathbb{Z}[\Delta])$, with values in $J(\mathbb{Q})$: for any $1 \leqslant h \leqslant e$,

$$(v\tilde{c}_v^{-1})(\chi^h)_q = \begin{cases} p^{\delta_{h,e}-1} & \text{if } q \neq p, \\ 1 & \text{if } q = p. \end{cases}$$

If $q \nmid pe$, then $p^{1-\delta_{h,e}} = \mathrm{Det}_{\chi^h}(\varepsilon_0 + p\varepsilon_1)$, where ε_0, ε_1 are defined as in the proof of Lemma 3.2, and satisfy $\varepsilon_0 + p\varepsilon_1 \in \mathbb{Z}_q[\Delta]^\times$. If $q \mid e$, then $p \in \mathbb{Z}_q^\times \subset \mathbb{Z}_q[\Delta]^\times$ and $\mathrm{Det}_{\chi^h}(p) = p$ for every $1 \leqslant h \leqslant e$. Let $\beta \in \mathcal{U}(\mathbb{Z}[\Delta])$ be defined by $\beta_q = p$ if $q \mid e$, $\beta_q = \varepsilon_0 + p\varepsilon_1$ if $q \nmid pe$ and $\beta_q = 1$ otherwise. Then $v\tilde{c}_v^{-1}\mathrm{Det}(\beta)$ is Ullom's representative morphism of the class of $\Sigma_\Delta(p)$ given for instance in [14, (I.2.23)].

3.3 Hom-representatives of (R) and (S)

In this subsection we use Fröhlich's construction of a representative homomorphism of the class of $\kappa(\chi^i)$, where i is any integer such that $0 \leqslant i \leqslant e-1$. These representative homomorphisms yield representatives for the classes of the torsion modules under study, namely R and S.

Recall that $\Delta = \langle\delta\rangle$ and that the $\mathfrak{o}[\Delta]$-module $\kappa(\chi^i)$ is defined to be $\kappa = \mathfrak{o}/\mathfrak{p}$ as $\mathfrak{o}$-module, with action of Δ given by $\delta \cdot x = \chi^i(\delta)x = \zeta^i x$ for any $x \in \kappa$.

3.3.1 Let us fix an integer $0 \leqslant i \leqslant e-1$, and let $\phi_i : \mathfrak{o}[\Delta] \to \kappa(\chi^i)$ be the only $\mathfrak{o}[\Delta]$-module homomorphism which sends 1 to 1, hence δ to $[\zeta^i]$, the class of ζ^i in κ. Note that ϕ_i is surjective and set

$$M_i = \mathfrak{p}\mathfrak{o}[\Delta] + (\delta - \zeta^i)\mathfrak{o}[\Delta] \subset \mathfrak{o}[\Delta] \ .$$

Then the sequence of $\mathfrak{o}[\Delta]$-modules

$$0 \to M_i \to \mathfrak{o}[\Delta] \xrightarrow{\phi_i} \kappa(\chi^i) \to 0 \tag{22}$$

is exact (since clearly $M_i \subseteq \ker(\phi_i)$ and $\#(\mathfrak{o}[\Delta]/M_i) = \#(\mathfrak{o}/\mathfrak{p}[\Delta]/(\delta - [\zeta^i])) = \#\mathfrak{o}/\mathfrak{p}$).

In the next proposition, we will show, by finding explicit local generators, that M_i is a locally free $\mathfrak{o}[\Delta]$-module. Anyway, this fact can be also shown as follows (see also the proof of [5, Proposition 4.1]): $\mathfrak{o}[\Delta]$ is Δ-cohomologically trivial (it is a free $\mathbb{Z}[\Delta]$-module) and the same holds $\kappa(\chi^i)$ as observed in §2.4.3. Therefore from the above exact sequence, we see that M_i is Δ-cohomologically trivial. Since it is also $\mathfrak{o}$-torsion free (being a submodule of $\mathfrak{o}[\Delta]$), we deduce that it is $\mathfrak{o}[\Delta]$-projective (this can be seen following the proof of [25, Chapitre IX, Théorème 7], with $\mathbb{Z}$ replaced by $\mathfrak{o}$, and using [26, Section 14.4, Exercice 1]). In particular, by Lemma 2.16 (i), the $\mathfrak{o}[\Delta]$-module M_i is locally free and we have, by Lemma 2.16 (ii),

$$(\kappa(\chi^i))_{\mathfrak{o}[\Delta]} = (\mathfrak{o}[\Delta])^{-1}_{\mathfrak{o}[\Delta]}(M_i)_{\mathfrak{o}[\Delta]} = (M_i)_{\mathfrak{o}[\Delta]} \quad \text{in } \mathrm{Cl}(\mathfrak{o}[\Delta]) \ . \tag{23}$$

For any place $\mathfrak{q}$ of $\mathfrak{o}$ we denote by $\mathfrak{o}_\mathfrak{q}$ the completion of $\mathfrak{o}$ at $\mathfrak{q}$ (note that $\mathfrak{o}_\mathfrak{q} = \mathbb{C}$ when $\mathfrak{q}$ is infinite). With a harmless abuse of notation, we will denote by ζ the image of ζ under the embedding $\mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$.

Proposition 3.4. *For every place $\mathfrak{q}$ of $\mathfrak{o}$, $\mathfrak{o}_\mathfrak{q} \otimes_\mathfrak{o} M_i = x_{i,\mathfrak{q}}\mathfrak{o}_\mathfrak{q}[\Delta]$ with*

$$x_{i,\mathfrak{q}} = \begin{cases} 1 & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ 1 + (p-1)\varepsilon_i & \text{if } \mathfrak{q} = \mathfrak{p}, \end{cases}$$

where $\varepsilon_i = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{ij}\delta^{-j} \in \mathfrak{o}_\mathfrak{p}[\Delta]$.

Proof. If $\mathfrak{q} \neq \mathfrak{p}$, since $\mathfrak{p}\mathfrak{o}_\mathfrak{q} = \mathfrak{o}_\mathfrak{q}$, we have $\mathfrak{o}_\mathfrak{q}[\Delta] = \mathfrak{o}_\mathfrak{q} \otimes_\mathfrak{o} M_i$, so we can take $x_{i,\mathfrak{q}} = 1$.

Assume $\mathfrak{q} = \mathfrak{p}$. For every $0 \leqslant k \leqslant e-1$, consider the idempotent

$$\varepsilon_k = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{kj}\delta^{-j} \in \mathfrak{o}_\mathfrak{p}[\Delta] \ .$$

Then $1 = \sum_{k=0}^{e-1} \varepsilon_k$ and $\varepsilon_h\varepsilon_k = \delta_{h,k}\varepsilon_h$ and therefore

$$\mathfrak{o}_\mathfrak{p}[\Delta] = \bigoplus_{k=0}^{e-1} \varepsilon_k\mathfrak{o}_\mathfrak{p}[\Delta] \ .$$

Now set $\tilde{\phi}_i = \phi_i \otimes \mathrm{id} : \mathfrak{o}[\Delta] \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}[\Delta] \to \kappa(\chi^i) \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p} = \kappa(\chi^i)$, then $\tilde{\phi}_i(\varepsilon_i) = 1$ and

$$\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] + (1-\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta] \subseteq \ker(\tilde{\phi}_i) = \mathfrak{o}_\mathfrak{p} \otimes_\mathfrak{o} M_i \ .$$

By the above properties of the idempotents we have

$$\mathfrak{o}_\mathfrak{p}[\Delta]/\big(\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] + (1-\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta]\big) \cong \varepsilon_i\mathfrak{o}_\mathfrak{p}[\Delta]/\varepsilon_i\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] \cong \kappa(\chi^i) \ ,$$

so that

$$\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] + (1-\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta] = \mathfrak{o}_\mathfrak{p} \otimes_\mathfrak{o} M_i \ .$$

We have indeed $\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] + (1-\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta] = (1+(p-1)\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta]$: using the equalities

$$p = (1+(p-1)\varepsilon_i)(p-(p-1)\varepsilon_i) \ ,$$
$$1-\varepsilon_i = (1+(p-1)\varepsilon_i)(1-\varepsilon_i) \ ,$$

we get $\mathfrak{p}\mathfrak{o}_\mathfrak{p}[\Delta] + (1-\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta] \subseteq (1+(p-1)\varepsilon_i)\mathfrak{o}_\mathfrak{p}[\Delta]$, since $(p) = \mathfrak{p}\mathfrak{o}_\mathfrak{p}$; the reverse inclusion follows from

$$1 + (p-1)\varepsilon_i = p\varepsilon_i + 1 - \varepsilon_i \ .$$

Therefore we can take $x_{i,\mathfrak{p}} = 1 + (p-1)\varepsilon_i$. □

In view of (23), we get the following representative homomorphism of the class of $\kappa(\chi^i)$ in $\mathrm{Cl}(\mathfrak{o}[\Delta])$.

Corollary 3.5. *The homomorphism v_i with values in the idèles group $J(\mathbb{Q}(\zeta))$, defined at any place $\mathfrak{q}$ of $\mathfrak{o}$ by*

$$v_i(\chi^h)_{\mathfrak{q}} = \mathrm{Det}_{\chi^h}(x_{i,\mathfrak{q}}) = \begin{cases} p & \text{if } \mathfrak{q} = \mathfrak{p},\ i \equiv h \pmod e, \\ 1 & \text{otherwise.} \end{cases}$$

represents the class $(\kappa(\chi^i))_{\mathfrak{o}[\Delta]}$ in $\mathrm{Hom}_{\Omega_{\mathbb{Q}(\zeta)}}(R_\Delta, J(\mathbb{Q}(\zeta)))$.

Proof. By Fröhlich's theory, Equality (23) and Proposition 3.4, we know that $(v_i)_{\mathfrak{q}} = \mathrm{Det}(x_{i,\mathfrak{q}})$ represents the class $(\kappa(\chi^i))_{\mathfrak{o}[\Delta]}$. Let $h \in \{0, \dots, e-1\}$, then

$$\mathrm{Det}_{\chi^h}(\varepsilon_i) = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{(i-h)j} = \begin{cases} 0 & \text{if } i \not\equiv h \pmod e \\ 1 & \text{if } i \equiv h \pmod e \end{cases},$$

because ζ^{i-h} is a root of the polynomial $\sum_{j=0}^{e-1} X^j$ precisely when $(i-h) \not\equiv 0 \pmod e$. The result follows. □

In order to get a representative homomorphism for the class $(\kappa(\chi^i)) \in \mathrm{Cl}(\mathbb{Z}[\Delta])$, we just need to take the norm of v_i, namely

$$\mathscr{N}(v_i) = \mathscr{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(v_i)$$

represents $(\kappa(\chi^i))$ in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, J(\mathbb{Q}(\zeta)))$, see [14, Theorem 2]. Before recalling the definition of $\mathscr{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, we introduce some notation and make a remark.

For any $\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times$, let $\sigma_\alpha \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be the automorphism defined by $\sigma_\alpha(\zeta) = \zeta^\alpha$. For any integer n, we let $\bar{n} = n \mod e$ denote its class modulo e, and we may write σ_n instead of $\sigma_{\bar{n}}$ if n is coprime with e.

Remark 3.6. The map $\alpha \mapsto \sigma_\alpha$ is in fact a group isomorphism

$$\sigma : (\mathbb{Z}/e\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

which sends the subgroup $\langle \bar{p} \rangle$ to the decomposition subgroup of $\mathfrak{p} \mid p$ (see [15, §13.2, Corollary to Theorem 2]), specifically $\mathfrak{p}^{\sigma_p} = \mathfrak{p}$. Hence, if $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$, we may denote by $\mathfrak{p}^{\sigma_\Lambda}$ the ideal $\mathfrak{p}^{\sigma_\lambda}$ where λ is any lift of Λ in $(\mathbb{Z}/e\mathbb{Z})^\times$. The prime ideals above p in $\mathfrak{o}$ are exactly the conjugates $\mathfrak{p}^{\sigma_\Lambda}$ with $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$ and, for $\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times$,

$$\mathfrak{p}^{\sigma_\alpha} = \mathfrak{p}^{\sigma_\Lambda} \iff \alpha \in \Lambda \ . \tag{24}$$

By definition, one has

$$\mathscr{N}(v_i)(\chi^h)_{\mathfrak{q}} = \left(\prod_k v_i\big((\chi^h)^{\sigma_k}\big)^{{\sigma_k}^{-1}} \right)_{\mathfrak{q}} = \prod_k \left(v_i(\chi^{hk})_{\mathfrak{q}^{\sigma_k}} \right)^{\sigma_k^{-1}} ,$$

where the product runs over the integers k such that $0 \leqslant k \leqslant e-1$ and k is coprime to e.

Proposition 3.7. *For any place $\mathfrak{q}$ of $\mathfrak{o}$ and for any $0 \leqslant h \leqslant e-1$, we have*

$$\mathscr{N}(v_i)(\chi^h)_{\mathfrak{q}} = \begin{cases} 1 & \text{if } \mathfrak{q} \nmid p, \\ p^{n(\Lambda,i,h)} & \text{if } \mathfrak{q} = \mathfrak{p}^{\sigma_\Lambda} \text{ for some } \Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle, \end{cases}$$

where we have set $n(\Lambda, i, h) = \#\{\alpha \in \Lambda : \alpha\bar{i} = \bar{h}\}$.

Proof. The case $\mathfrak{q} \nmid p$ follows immediately from the above, so we assume that $\mathfrak{q} = \mathfrak{p}^{\sigma_\Lambda}$ for some $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$. Then $\mathfrak{q}^{\sigma_k} = \mathfrak{p}$ if and only if $\bar{k}^{-1} \in \Lambda$, by (24). Thus, using Corollary 3.5,

$$v_i(\chi^{hk})_{\mathfrak{q}^{\sigma_k}} = \begin{cases} p & \text{if } \bar{k}^{-1} \in \Lambda,\ i \equiv hk \pmod e; \\ 1 & \text{otherwise.} \end{cases}$$

The result follows. □

3.3.2 Since the Hom-description (20) is a group isomorphism, the classes

$$(R) = \prod_{i=1}^{e-1} \big(\kappa(\chi^i)\big)^i \quad \text{and, if } e \text{ is odd,} \quad (S) = \prod_{i=\frac{e+1}{2}}^{e-1} \big(\kappa(\chi^i)\big)$$

are represented respectively in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, J(\mathbb{Q}(\zeta)))$ by the homomorphisms:

$$r = \prod_{i=1}^{e-1} \mathscr{N}(v_i)^i \quad \text{and} \quad s = \prod_{i=\frac{e+1}{2}}^{e-1} \mathscr{N}(v_i) \ .$$

We immediately get the following result.

Corollary 3.8. *let $0 \leqslant h \leqslant e-1$ then, if $\mathfrak{q} \nmid p$:*

$$r(\chi^h)_{\mathfrak{q}} = s(\chi^h)_{\mathfrak{q}} = 1$$

and, if $\mathfrak{q} = \mathfrak{p}^{\sigma_\Lambda}$ for some $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$:

$$r(\chi^h)_{\mathfrak{q}} = p^{\sum_{i=1}^{e-1} in(\Lambda,i,h)} \ , \quad s(\chi^h)_{\mathfrak{q}} = p^{\sum_{i=\frac{e+1}{2}}^{e-1} n(\Lambda,i,h)} \ .$$

3.3.3 We compute the numbers $n(\Lambda, i, h)$ introduced above for $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$, $i, h \in \{0, \dots, e-1\}$. We extend the definition to $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \mod e')\rangle$ for any divisor e' of e, $i', h' \in \mathbb{Z}$, by setting:

$$n(\Lambda', i', h') = \#\{\alpha' \in \Lambda' : \alpha'(i' \mod e') = (h' \mod e')\} \ .$$

Of course $n(\Lambda', i', h')$ only depends on Λ' and the residue classes $(i' \bmod e')$ and $(h' \bmod e')$ of i' and h' modulo e'. For any divisor d of e, let f_d denote the (multiplicative) order of p modulo d (thus $f_e = f$). The greatest common divisor of integers a, b is denoted by $\gcd(a, b)$.

Lemma 3.9. *Let $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$, $i, h \in \{0, \dots, e-1\}$, then:*

(i) $n(\Lambda, i, h) \neq 0 \Rightarrow \gcd(i, e) = \gcd(h, e)$;

(ii) suppose $\gcd(i, e) = \gcd(h, e) = d$ *and set* $i = di'$, $h = dh'$, $e = de'$, *one has*

$$n(\Lambda, i, h) = \begin{cases} f/f_{e'} & \text{if } (h' \mod e') \in (i' \mod e')\Lambda', \\ 0 & \text{otherwise,} \end{cases}$$

where $\Lambda' = (\Lambda \mod e') \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \mod e')\rangle$.

Proof. Suppose $n(\Lambda, i, h) \neq 0$. Let $\alpha \in \Lambda$ be such that $\alpha\bar{i} = \bar{h}$ and let $a \in \alpha$ (so $a \in \mathbb{Z}$), then $ai \equiv h \pmod e$ and the equality $\gcd(i, e) = \gcd(h, e)$ follows since $\gcd(a, e) = 1$.

We now assume the condition of assertion (ii) is satisfied and use the same notations. If $d = e$, $n(\Lambda, i, h) = n(\Lambda, 0, 0) = \#\Lambda = f = f/f_1$ and $0 \in 0\Lambda'$ is always satisfied. Otherwise, $(i', e') = 1$ and one has, for any $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$:

$$\alpha'(i' \mod e') = (h' \mod e') \Longleftrightarrow \alpha' = (h' \mod e')(i' \mod e')^{-1} \ ,$$

hence $n(\Lambda', i', h') = 1$ or 0 depending on whether $(h' \bmod e')(i' \bmod e')^{-1}$ belongs to Λ' or not. We thus only have to show that

$$n(\Lambda, i, h) = \frac{f}{f_{e'}}\, n(\Lambda', i', h') \ . \tag{25}$$

As above, let $\alpha \in \Lambda$ and $a \in \alpha$. We may rewrite $n(\Lambda, i, h)$ as

$$\begin{aligned} n(\Lambda, i, h) &= \#\{0 \leqslant k \leqslant f-1 : \alpha \bar{p}^k \bar{i} = \bar{h}\} \\ &= \#\{0 \leqslant k \leqslant f-1 : ap^k i \equiv h \pmod{e}\} \\ &= \#\{0 \leqslant k \leqslant f-1 : ap^k i' \equiv h' \pmod{e'}\} \ . \end{aligned}$$

Note that, if we set $\alpha' = (\alpha \mod e')$, then $a \in \alpha'$ and $\alpha' \in \Lambda'$, hence, similarly:

$$n(\Lambda', i', h') = \#\{0 \leqslant k \leqslant f_{e'} - 1 : ap^k i' \equiv h' \pmod{e'}\} \ .$$

The result follows since $f_{e'}$ is the order of p in $(\mathbb{Z}/e'\mathbb{Z})^\times$. □

3.4 The contents of s and r

In this subsection we compute the contents of the idèles $\mathscr{N}(v_i)(\chi^h)$, $s(\chi^h)$ and $r(\chi^h)$ for $0 \leqslant i, h \leqslant e-1$. Recall that the content of an idèle $x = (x_\mathfrak{q})_\mathfrak{q} \in J(\mathbb{Q}(\zeta))$ is the fractional ideal $cont(x) = \prod_\mathfrak{q} \mathfrak{q}^{\mathrm{val}_\mathfrak{q}(x_\mathfrak{q})}$ of $\mathbb{Q}(\zeta)$, where $\mathrm{val}_\mathfrak{q}$ is the $\mathfrak{q}$-valuation and the product runs over finite prime ideals $\mathfrak{q}$ of $\mathfrak{o}$.

Since the valuation of p at a prime ideal $\mathfrak{q} = \mathfrak{p}^{\sigma_\Lambda}$ with $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$ equals 1, it follows from Proposition 3.7 and Corollary 3.8 that

$$cont(\mathscr{N}(v_i)(\chi^h)) = \mathfrak{p}^{\sum_\Lambda n(\Lambda,i,h)\,\sigma_\Lambda} \tag{26}$$

$$cont(s(\chi^h)) = \mathfrak{p}^{\sum_\Lambda \sum_{i=\frac{e+1}{2}}^{e-1} n(\Lambda,i,h)\,\sigma_\Lambda} \tag{27}$$

$$cont(r(\chi^h)) = \mathfrak{p}^{\sum_\Lambda \sum_{i=1}^{e-1} in(\Lambda,i,h)\,\sigma_\Lambda} \tag{28}$$

where in each sum Λ runs over $(\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$.

3.4.1 Since $\mathscr{N}(v_i)$, s and r are $\Omega_\mathbb{Q}$-equivariant, their values on R_Δ are determined by the values at χ^d, with $d \mid e$. Namely, if h is an integer and d is the greatest common divisor of h and e, we write $h = dh'$ and get

$$\mathscr{N}(v_i)(\chi^h) = \mathscr{N}(v_i)\big((\chi^d)^{\sigma_{h'}}\big) = \mathscr{N}(v_i)(\chi^d)^{\sigma_{h'}} \tag{29}$$

and analogously for s and r.

For any $d \mid e$, write $e = de'$ and set $\zeta_{e'} = \zeta^d$ (thus $\zeta_e = \zeta$); for $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$, let $\sigma_{e',\alpha'} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})$ be the automorphism sending $\zeta_{e'}$ to $\zeta_{e'}^{\alpha'}$ (thus $\sigma_{e,\alpha'} = \sigma_{\alpha'}$). Since $e' \mid e$, $\mathbb{Q}(\zeta_{e'}) \subseteq \mathbb{Q}(\zeta)$, hence $\sigma_{e',\alpha'}$ can be lifted in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ (in $\varphi(e)/\varphi(e')$ different ways). To ease notation, if j is an integer with $(j, e') = 1$, we may write $\sigma_{e',j}$ instead of $\sigma_{e',(j \mod e')}$.

We also set $\mathfrak{o}_{e'} = \mathbb{Z}[\zeta_{e'}]$ and $\mathfrak{p}_{e'} = \mathfrak{p} \cap \mathfrak{o}_{e'}$ (thus $\mathfrak{o}_e = \mathfrak{o}$ and $\mathfrak{p}_e = \mathfrak{p}$). If $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$, the ideal $\mathfrak{p}_{e'}^{\sigma_{e',\alpha'}}$ only depends on the class of α' modulo $(p \mod e')$. So if $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle (p \mod e') \rangle$, we denote by $\mathfrak{p}_{e'}^{\sigma_{\Lambda'}}$ the ideal $\mathfrak{p}_{e'}^{\sigma_{e',\alpha'}}$ where α' is any lift of Λ' in $(\mathbb{Z}/e'\mathbb{Z})^\times$.

Lemma 3.10. *Let $d \mid e$ and set $e = de'$. Let $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle (p \mod e') \rangle$, then*

$$\mathfrak{p}^{\sum_{\Lambda \in \Lambda'} \sigma_\Lambda} = \mathfrak{p}_{e'}^{\sigma_{\Lambda'}} \mathfrak{o} \ ,$$

where the sum is on the elements Λ of the coset Λ' in $(\mathbb{Z}/e\mathbb{Z})^\times/\langle (p \mod e) \rangle$.

Proof. Let $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$ and $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle (p \bmod e') \rangle$ then, since $\mathfrak{p} \mid \mathfrak{p}_{e'}\mathfrak{o}$,

$$\Lambda \in \Lambda' \ \Rightarrow \ \sigma_{\Lambda|_{\mathbb{Q}(\zeta_{e'})}} = \sigma_{\Lambda'} \ \Rightarrow \ \mathfrak{p}^{\sigma_\Lambda} \mid \mathfrak{p}_{e'}^{\sigma_{\Lambda'}} \mathfrak{o} \ .$$

It follows that $\mathfrak{p}^{\sum_{\Lambda\in\Lambda'}\sigma_\Lambda} \mid \mathfrak{p}_{e'}^{\sigma_{\Lambda'}}\mathfrak{o}$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_{e'})$ is unramified at $\mathfrak{p}_{e'}$, the number of primes above $\mathfrak{p}_{e'}$ in $\mathfrak{o}$ equals $\frac{\varphi(e)}{\varphi(e')}/\frac{f}{f_{e'}} = \frac{\#(\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle}{\#(\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \mod e')\rangle} = \#\Lambda'$ (as a coset in $(\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$). The result follows. □

Proposition 3.11. *Let $d \mid e$ and set $e = de'$, then*

$$cont(\mathscr{N}(v_i)(\chi^d)) = \begin{cases} \mathfrak{o} & \text{if } \gcd(i,e) \neq d \\ \left(\mathfrak{p}_{e'}^{\sigma_{\Lambda'_i}}\mathfrak{o}\right)^{f/f_{e'}} & \text{if } \gcd(i,e) = d \end{cases}$$

where $i = di'$ and $\Lambda'_i \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \mod e')\rangle$ is such that $(i' \mod e')^{-1} \in \Lambda'_i$.

Proof. Since $\gcd(d,e) = d$, the result is clear from (26) and Lemma 3.9 in the case $\gcd(i,e) \neq d$, hence we now assume $\gcd(i,e) = d$ and write $i = di'$. Then i' and e' are coprime so let $\Lambda'_i \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \mod e')\rangle$ be such that $(i' \mod e')^{-1} \in \Lambda'_i$. From Lemma 3.9 we know that $n(\Lambda,i,d) = f/f_{e'}$ if $\Lambda \in \Lambda'_i$, 0 otherwise, hence from (26) we get

$$cont(\mathscr{N}(v_i)(\chi^d)) = \mathfrak{p}^{\frac{f}{f_{e'}}\sum\limits_{\Lambda\in\Lambda'_i}\sigma_\Lambda}$$

and the result follows using Lemma 3.10. □

Remark 3.12. Using (29), it follows that, for every $i,h \in \{0,\ldots,e-1\}$, the ideal $cont(\mathscr{N}(v_i)(\chi^h))$ is either trivial or, if $\gcd(i,e) = \gcd(h,e) = d$, the extension to $\mathfrak{o}$ of an ideal of $\mathfrak{o}_{e'}$ ($e' = e/d$) whose absolute norm is congruent to 1 modulo e. (Indeed, by definition of $f_{e'}$, the absolute norm of $\mathfrak{p}_{e'}^{f/f_{e'}}$ and of its conjugates is $(p^{f/f_{e'}})^{f_{e'}} = p^f$ which is congruent to 1 modulo e.)

3.4.2 We begin by computing the content of r: the strategy for the content of s will be similar but the calculations for r are simpler.

For any divisor e' of e, we denote by $\mathscr{Z}_{e'}$ the subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$ of elements congruent to 1 modulo e', namely

$$\mathscr{Z}_{e'} = \sigma^{-1}\big(\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_{e'}))\big) \ ,$$

where $\sigma : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_{e'})) \to (\mathbb{Z}/e\mathbb{Z})^\times$ is the isomorphism of Remark 3.6. We also introduce the relative norm and Stickelberger's element:

$$N_{e,e'} = \sum_{\alpha\in\mathscr{Z}_{e'}}\sigma_\alpha \quad \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_{e'}))] \ ;$$

$$\Theta_{e'} = \frac{1}{e'}\sum_{\substack{1\leqslant j\leqslant e'-1\\(j,e')=1}} j\sigma_{e',j}^{-1} \quad \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})] \ .$$

Note that $N_{e,1}$ equals the absolute norm $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}$.

Proposition 3.13. *Let $d \mid e$ and set $e = de'$, then*

$$cont(r(\chi^d)) = \mathfrak{p}^{e\Theta_{e'}N_{e,e'}} \ .$$

Proof. We begin with the right-hand side. First $\mathfrak{p}^{N_{e,e'}} = \mathfrak{p}_{e'}^{f/f_{e'}}\mathfrak{o}$, so that $\mathfrak{p}^{e\Theta_{e'}N_{e,e'}}$ equals $\mathfrak{p}_{e'}\mathfrak{o}$ to the exponent:

$$d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{1\leqslant j\leqslant e'-1\\ j \mod e'\in\Lambda'}} j\right)\sigma_{\Lambda'}^{-1} \ ,$$

where the first sum is on $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \bmod e')\rangle$.

We go on with the left-hand side. We start from Formula (28). Since $\gcd(d,e)=d$, using Lemma 3.9, $cont(r(\chi^d))$ equals $\mathfrak{p}$ to the exponent:

$$\sum_{\Lambda}\left(\sum_{\substack{1\leqslant i'\leqslant e'-1\\ 1\in(i'\Lambda \bmod e')}} di'\frac{f}{f_{e'}}\right)\sigma_\Lambda = d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{1\leqslant i'\leqslant e'-1\\ 1\in(i' \bmod e')\Lambda'}} i'\right)\sum_{\Lambda\in\Lambda'}\sigma_\Lambda \ ,$$

where Λ runs over $(\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$ in the first sum to the left, Λ' runs over $(\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \bmod e')\rangle$ in the first sum to the right, and is seen as a coset of $(\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$ in the last sum to the right (for the reduction modulo e'). Using Lemma 3.10, we get that $cont(r(\chi^d))$ equals $\mathfrak{p}_{e'}\mathfrak{o}$ to the exponent:

$$d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{1\leqslant i'\leqslant e'-1\\ 1\in(i' \bmod e')\Lambda'}} i'\right)\sigma_{\Lambda'} = d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{1\leqslant i'\leqslant e'-1\\ (i' \bmod e')\in\Lambda'^{-1}}} i'\right)\sigma_{\Lambda'} \ ,$$

and the equality follows. □

3.4.3 To deal with s, we need to introduce further elements in various group algebras. For any divisors d and e' of e, let

$$\mathscr{H}_{e'} = \{\beta' \in (\mathbb{Z}/e'\mathbb{Z})^\times \ : \ \exists\ b\in\beta',\ \frac{e'+1}{2}\leqslant b\leqslant e'-1\}$$

and set

$$H_{e'} = \sum_{\alpha'\,\in\,\mathscr{H}_{e'}} \sigma_{e',\alpha'}^{-1} \quad \in\ \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})] \ ,$$

$$H_{e,d} = \sum_{\substack{\alpha\in(\mathbb{Z}/e\mathbb{Z})^\times\\ \alpha\bar{d}\,\in\,\mathscr{H}_e}} \sigma_\alpha^{-1} \quad \in\ \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})] \ .$$

Note that $H_e = H_{e,1}$.

Lemma 3.14. *Let $d \mid e$, then $cont(s(\chi^d)) = \mathfrak{p}^{H_{e,d}}$.*

Proof. Rewrite $H_{e,d}$ as

$$H_{e,d} = \sum_{\Lambda}\sum_{\substack{\beta\in\Lambda\\ \beta^{-1}\bar{d}\,\in\,\mathscr{H}_e}} \sigma_\beta \ ,$$

where Λ runs over $(\mathbb{Z}/e\mathbb{Z})^\times/\langle\bar{p}\rangle$. It follows that

$$\mathfrak{p}^{H_{e,d}} = \mathfrak{p}^{\sum_\Lambda \#\{\beta\in\Lambda\,:\,\beta^{-1}\bar{d}\,\in\,\mathscr{H}_e\}\sigma_\Lambda} \ .$$

But $\#\{\beta\in\Lambda\ :\ \beta^{-1}\bar{d}\in\mathscr{H}_e\} = \sum_{i=\frac{e+1}{2}}^{e-1} n(\Lambda,i,d)$, which yields the result using (27). □

Lemma 3.15. *Let $d \mid e$ and set $e = de'$, then*

$$H_{e,d} = H_{e'}N_{e,e'} \quad \text{and} \quad H_{e'} = (2-\sigma_{e',2})\Theta_{e'} \ .$$

Remark 3.16. Note that the first equality is not ambiguous, even though it contains a slight abuse of notation: $H_{e'}$ belongs to $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})]$ whereas $N_{e,e'}$ and $H_{e,d}$ belong to $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})]$. Nevertheless, if $\alpha'\in(\mathbb{Z}/e'\mathbb{Z})^\times$, then $\sigma_\alpha N_{e,e'}$ does not depend on the choice of a lift α of α' in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Indeed

$$\sigma_\alpha N_{e,e'} = \sum_{\beta \in \mathcal{Z}_{e'}} \sigma_{\alpha\beta}$$

is the sum of all the lifts of $\sigma_{e',\alpha'}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus in order to get an equality in $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})]$, one just has to replace each term $\sigma_{e',\alpha'^{-1}} N_{e,e'}$ of the sum $H_{e'} N_{e,e'}$ by $\sigma_{\alpha^{-1}} N_{e,e'}$, where α is any lift of α' in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Proof. We begin with the first equality. We suppose we have fixed a lift $\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times$ of each $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$. In view of the previous remark,

$$H_{e'} N_{e,e'} = \sum_{\substack{\alpha' \in \mathscr{H}_{e'} \\ \beta \in \mathcal{Z}_{e'}}} \sigma_{\alpha^{-1}\beta} = \sum_{\substack{\alpha' \in \mathscr{H}_{e'} \\ \beta \in \mathcal{Z}_{e'}}} \sigma_{\alpha\beta}^{-1} \ ,$$

since $\mathcal{Z}_{e'}$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. We are thus left to show that the map

$$(\alpha', \beta) \in \mathscr{H}_{e'} \times \mathcal{Z}_{e'} \longmapsto \alpha\beta \in \{\gamma \in (\mathbb{Z}/e\mathbb{Z})^\times : \gamma \bar{d} \in \mathscr{H}_e\} \tag{30}$$

is a well-defined one-to-one correspondence.

We first show that the if $(\alpha', \beta) \in \mathscr{H}_{e'} \times \mathcal{Z}_{e'}$, then indeed $\alpha\beta \in \{\gamma \in (\mathbb{Z}/e\mathbb{Z})^\times : \gamma \bar{d} \in \mathscr{H}_e\}$. Of course $\alpha\beta \in (\mathbb{Z}/e\mathbb{Z})^\times$, so we have to show that $\alpha\beta\bar{d} \in \mathscr{H}_e$. Let $a \in \alpha'$ be such that $\frac{e'+1}{2} \leqslant a \leqslant e'-1$. Observe that $ad \in \alpha\beta\bar{d}$. In fact $\beta \in \mathcal{Z}_{e'}$, there exists $t \in \mathbb{Z}$ such that $1 + te' \in \beta$ and clearly

$$ad \equiv ad(1 + te') \pmod{e}.$$

Since clearly $ad(1 + te') \in \alpha\beta\bar{d}$, we deduce $ad \in \alpha\beta\bar{d}$. Now $\frac{e+1}{2} \leqslant \frac{e+d}{2} \leqslant ad \leqslant e - d \leqslant e - 1$, hence $\alpha\beta\bar{d} \in \mathscr{H}_e$. Thus the map in (30) is well-defined.

To show that it is one-to-one, we define its inverse. Suppose $\gamma \in (\mathbb{Z}/e\mathbb{Z})^\times$ is such that $\gamma\bar{d} \in \mathscr{H}_e$. Since $d \mid e$, there exists $c \in \gamma$ such that $\frac{e+1}{2} \leqslant cd \leqslant e - 1$, hence $\frac{e'+1}{2} \leqslant c \leqslant e' - 1$. This shows that $\alpha' = (c \mod e') \in (\mathbb{Z}/e'\mathbb{Z})^\times$ belongs to $\mathscr{H}_{e'}$. In particular α' is the image of γ in $(\mathbb{Z}/e'\mathbb{Z})^\times$. Since α' is also the image of α in $(\mathbb{Z}/e'\mathbb{Z})^\times$, there exists a unique $\beta \in \mathcal{Z}_{e'}$ such that $\gamma = \alpha\beta$. It is clear that the map sending γ to (α', β) is the inverse of (30).

We now show the second equality of the lemma. To simplify notations in this proof, we write σ_k instead of $\sigma_{e',k}$. We note that $\sigma_2 = \sigma_{\frac{e'+1}{2}}^{-1}$ and compute

$$e'(2 - \sigma_2)\Theta_{e'} = \sum_{\substack{1 \leqslant j \leqslant e'-1 \\ (j,e')=1}} 2j\sigma_j^{-1} - \sum_{\substack{1 \leqslant j \leqslant e'-1 \\ (j,e')=1}} j\sigma_{\frac{e'+1}{2}j}^{-1} \ .$$

Let $j, j' \in \{k \in \mathbb{Z} : 1 \leqslant k \leqslant e' - 1, (k, e') = 1\}$, then $j' \equiv \frac{e'+1}{2} j \pmod{e'}$ if and only if $j \equiv 2j' \pmod{e'}$, hence the coefficient of $\sigma_{j'}^{-1}$ in the second sum above is $2j'$ if $1 \leqslant j' \leqslant \frac{e'-1}{2}$, $2j' - e'$ otherwise. Therefore

$$e'(2 - \sigma_2)\Theta_{e'} = e' \sum_{\substack{\frac{e'+1}{2} \leqslant j \leqslant e'-1 \\ (j,e')=1}} \sigma_j^{-1}$$

and the result follows.

□

Combining Lemmas 3.14 and 3.15 yields:

Proposition 3.17. *Let $d \mid e$ and set $e = de'$, then*

$$cont(s(\chi^d)) = \mathfrak{p}^{(2-\sigma_{e',2})\Theta_{e'} N_{e,e'}} \ .$$

3.5 Arithmetically realizable classes

The result we have obtained so far in this section, combined with those of Section 2.4 allow us to give an alternative proof of a result of Burns, concerning the Galois module structure of ideals in tame locally abelian extensions of number fields.

We start by recalling Burns's definitions and notation. Let G be a finite group and let $\mathfrak{R}^a_{\mathbb{Q}}(G)$ denote the subgroup of $\mathrm{Cl}(\mathbb{Z}[G])$ which is generated by classes of G-stable (integral) ideals of tame locally abelian G-Galois extensions of number fields. Let also $\mathfrak{R}^a_{\mathbb{Q},0}(G)$ denote the subgroup of $\mathfrak{R}^a_{\mathbb{Q}}(G)$ consisting of classes of rings of integers of tame locally abelian G-Galois extensions of number fields. To describe the difference between $\mathfrak{R}^a_{\mathbb{Q},0}(G)$ and $\mathfrak{R}^a_{\mathbb{Q}}(G)$, consider the subgroup $\mathrm{Cl}(\mathbb{Z}[G])_{\mathscr{C},\Sigma}$ of $\mathrm{Cl}(\mathbb{Z}[G])$ which is defined as follows. Let first C be a cyclic subgroup of G and denote by $\mathrm{Cl}(\mathbb{Z}[C])_\Sigma$ the subgroup of $\mathrm{Cl}(\mathbb{Z}[C])$ generated by classes which can be represented in the ideal-theoretic Hom-description (see [14, Note 4 to Chapter I]) by functions whose value on a character $\chi : C \to \overline{\mathbb{Q}}$ is a fractional ideal of $\mathbb{Q}(\chi)$ supported only above rational primes congruent to 1 modulo $\#C$. If $\mathscr{C}$ is the set of cyclic subgroups of G, then

$$\mathrm{Cl}(\mathbb{Z}[G])_{\mathscr{C},\Sigma} = \prod_{C\in\mathscr{C}} \mathrm{Ind}_C^G \mathrm{Cl}(\mathbb{Z}[C])_\Sigma \ .$$

The result of Burns [3, Theorem 1.1] which we are going to reprove reads as follows.

Theorem 3.18. *There is an inclusion*

$$\mathfrak{R}^a_{\mathbb{Q}}(G) \subseteq \mathfrak{R}^a_{\mathbb{Q},0}(G) \cdot \mathrm{Cl}(\mathbb{Z}[G])_{\mathscr{C},\Sigma} \ .$$

Remark 3.19. Burns also proves that one has equality in the above theorem when G is abelian. Moreover his result holds with $\mathbb{Q}$ replaced by any number field L which is absolutely unramified at primes dividing $\#G$ and $\mathbb{Z}$ replaced by the ring of integers of L.

Proof. Let N/E be a tame locally abelian G-Galois extension of number fields and let $\mathcal{I}$ be a G-stable ideal of $\mathcal{O}_N$. We have to show that

$$(\mathcal{I}) \in \mathfrak{R}^a_{\mathbb{Q},0}(G) \cdot \mathrm{Cl}(\mathbb{Z}[G])_{\mathscr{C},\Sigma} \ .$$

Of course it is enough to show that

$$(\mathcal{O}_N/\mathcal{I}) = (\mathcal{I})(\mathcal{O}_N)^{-1} \in \mathrm{Cl}(\mathbb{Z}[G])_{\mathscr{C},\Sigma} \ .$$

Note that, for any prime $\mathcal{P}$ of $\mathcal{O}_N$, the inertia subgroup $I_\mathcal{P}$ of $\mathcal{P}$ in N/E is cyclic, since N/E is tame. Thanks to Proposition 2.18, we are then reduced to show that, for every $0 \leqslant i \leqslant e_P - 1$, $(\mathfrak{o}_{e_P}/\mathfrak{p}(\chi^i_\mathcal{P})) \in \mathrm{Cl}(\mathbb{Z}[I_\mathcal{P}])_\Sigma$ with notation as in §2.3.2. Let $\mathscr{N}(v_i)$ be the representative homomorphism of $\big((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi^i_\mathcal{P})\big)$ described in Proposition 3.7. Since $\mathscr{N}(v_i)$ is $\Omega_\mathbb{Q}$-equivariant, we deduce that $\mathscr{N}(v_i)(\chi^h_\mathcal{P}) \in J(\mathbb{Q}(\chi^h_\mathcal{P}))$. By Propositon 3.7, $\mathscr{N}(v_i)(\chi^h_\mathcal{P})$ has component 1 at every prime dividing e_P. Thus to obtain a function representing $\big((\mathfrak{o}_{e_P}/\mathfrak{p})(\chi^i_\mathcal{P})\big)$ in the ideal-theoretic Hom-description, one only needs to take the content of $\mathscr{N}(v_i)(\chi^h_\mathcal{P})$, as an ideal of $\mathbb{Q}(\chi^h_\mathcal{P})$ (see for instance [13, p. 429]). By Remark 3.12, the content of $\mathscr{N}(v_i)(\chi^h_\mathcal{P})$, as an ideal of $\mathbb{Q}(\chi^h_\mathcal{P})$, has absolute norm 1 modulo $e_P = \#I_\mathcal{P}$. This implies that $\big((\mathfrak{o}_{e_\mathcal{P}}/\mathfrak{p})(\chi^i_\mathcal{P})\big) \in \mathrm{Cl}(\mathbb{Z}[I_\mathcal{P}])_\Sigma$, thanks to the following result, whose proof uses the arguments of [3, pp. 388-389]. □

Proposition 3.20. *Let C be a cyclic group and let $\mathrm{Cl}'(\mathbb{Z}[C])_\Sigma$ be the subgroup of $\mathrm{Cl}(\mathbb{Z}[C])$ generated by classes which can be represented in the ideal-theoretic Hom-description by functions whose values are fractional ideals of absolute norm congruent to 1 modulo $c = \#C$. Then $\mathrm{Cl}'(\mathbb{Z}[C])_\Sigma = \mathrm{Cl}(\mathbb{Z}[C])_\Sigma$.*

Proof. Let $\chi : C \to \overline{\mathbb{Q}}^\times$ be a fixed injective character of C. Then the $\Omega_\mathbb{Q}$-conjugacy classes of characters of C are represented by χ^d, with d running through the divisors of c. In particular, as remarked in §3.4.1

for the idèle-theoretic Hom-description, a representative homomorphism of an element of $\mathrm{Cl}(\mathbb{Z}[C])$ in the ideal-theoretic Hom-description is determined by its value on χ^d for every divisor d of c. For any such divisor d, let $\mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d))$ denote the ray class group of $\mathbb{Q}(\chi^d)$ modulo $\mathfrak{c}$, where $\mathbb{Q}(\chi^d)$ is the extension of $\mathbb{Q}$ generated by the values of χ^d and $\mathfrak{c}$ is the product of the ideal generated by c and the archimedean primes of $\mathbb{Q}(\chi^d)$. Consider the homomorphism

$$\pi_C : \bigoplus_{d|c} \mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d)) \to \mathrm{Cl}(\mathbb{Z}[C])$$

which is defined as follows. For any $d \mid c$, let a_d be a class in $\mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d))$ and choose a fractional ideal $\mathfrak{a}_d$ of $\mathbb{Q}(\chi^d)$ with the following properties:

(i) the numerator and denominator of $\mathfrak{a}_d$ are coprime with c;

(ii) the class of $\mathfrak{a}_d$ in $\mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d))$ is a_d.

Define $\pi_C((a_d)_{d|c}) \in \mathrm{Cl}(\mathbb{Z}[C])$ to be the class represented by the function which, for any divisor $d \mid c$, sends χ^d to $\mathfrak{a}_d$. In fact $\pi_C((a_d)_{d|c})$ is independent of the choice of the ideals $\mathfrak{a}_d$ with the above properties, as we now show. For every $d \mid c$, choose a fractional ideal $\mathfrak{b}_d$ with properties (i) and (ii). Then, for every $d \mid c$, there exists a totally positive element $x_d \in \mathbb{Q}(\chi^d)$ such that $x_d \equiv 1 \pmod{(c)}$ and $\mathfrak{b}_d = x_d\mathfrak{a}_d$. We claim that the map $\chi^d \mapsto x_d\mathbb{Z}[\chi^d]$ lies in the denominator of the ideal theoretic Hom-description of $\mathrm{Cl}(\mathbb{Z}[C])$. In other words we have to show that for every place $\mathfrak{q}$ dividing $\mathfrak{c}$, there exists $u_q \in \mathbb{Z}_q[C]^\times$ such that $\mathrm{Det}_{\chi^d}(u_q) = x_d$ for every $d \mid c$, where q is the place of $\mathbb{Q}$ below $\mathfrak{q}$ and we identify x_d with its image in $\mathbb{Q}(\chi^d)_{\mathfrak{q}}^\times$. When $\mathfrak{q}$ is archimedean this follows from the second part of [14, I, Proposition 2.2], while when $\mathfrak{q}$ is finite it is a consequence of the following lemma.

Lemma 3.21. *Let q be a rational prime dividing c and let ξ_c be a primitive cth root of unity in an algebraic closure $\overline{\mathbb{Q}}_q$ of $\mathbb{Q}_q$. Then*

$$\mathrm{Hom}_{\Omega_{\mathbb{Q}_q}}(R_{C,q}, 1 + c\mathbb{Z}_q[\xi_c]) \subset \mathrm{Det}(\mathbb{Z}_q[C]^\times).$$

Proof. Let $\widehat{C}$ be the group of $\overline{\mathbb{Q}}_q$-characters of C. Consider the isomorphism of $\overline{\mathbb{Q}}_q$-algebras

$$\overline{\mathbb{Q}}_q[C] \to \mathrm{Map}(\widehat{C}, \overline{\mathbb{Q}}_q)$$

which sends $\sum_{\gamma\in C} a_\gamma\gamma \in \mathbb{Q}_q[C]$ to the map $\chi \mapsto \sum_{\gamma\in C} a_\gamma\chi(\gamma)$. Note that $\Omega_{\mathbb{Q}_q}$ acts on both $\overline{\mathbb{Q}}_q[C]$ (via its action on $\overline{\mathbb{Q}}_q$) and $\mathrm{Map}(\widehat{C}, \overline{\mathbb{Q}}_q)$ (via its actions on $\widehat{C}$ and $\overline{\mathbb{Q}}_q$) and the above isomorphism is $\Omega_{\mathbb{Q}_q}$-equivariant. Taking invariants we get an isomorphism of $\mathbb{Q}_q$-algebras

$$\mathbb{Q}_q[C] \to \mathrm{Map}_{\Omega_{\mathbb{Q}_q}}(\widehat{C}, \mathbb{Q}_q).$$

In particular, if $\mathfrak{M}_q$ is the maximal order of $\mathbb{Q}_q[C]$, we get an isomorphism of rings

$$\mathfrak{M}_q \to \mathrm{Map}_{\Omega_{\mathbb{Q}_q}}(\widehat{C}, \mathbb{Z}_q[\xi_c]),$$

since $\mathbb{Z}_q[\xi_c]$ is the maximal order of $\mathbb{Q}_q(\xi_c)$. From this we get a group isomorphism

$$1 + c\mathfrak{M}_q \to \mathrm{Map}_{\Omega_{\mathbb{Q}_q}}(\widehat{C}, 1 + c\mathbb{Z}_q[\xi_c]).$$

Extending maps on characters by linearity, we can identify $\mathrm{Map}_{\Omega_{\mathbb{Q}_q}}(\widehat{C}, 1+c\mathbb{Z}_q[\xi_c])$ with $\mathrm{Hom}_{\Omega_{\mathbb{Q}_q}}(R_{C,q}, 1+c\mathbb{Z}_q[\xi_c])$. Thus the above isomorphism is the usual Det map

$$\mathrm{Det} : 1 + c\mathfrak{M}_q \to \mathrm{Hom}_{\Omega_{\mathbb{Q}_q}}(R_{C,q}, 1 + c\mathbb{Z}_q[\xi_c]).$$

This implies in particular that $1 + c\mathfrak{M}_q \subset \mathfrak{M}_q^\times$, since $1 + c\mathbb{Z}_q[\xi_c] \subset \mathbb{Z}_q[\xi_c]^\times$ because $q \mid c$. Moreover $c\mathfrak{M}_q \subset \mathbb{Z}_q[C]$ (see [23, Theorem 41.1]) and in particular $1 + c\mathfrak{M}_q \subset \mathbb{Z}_q[C] \cap \mathfrak{M}_q^\times = \mathbb{Z}_q[C]^\times$ (for the last equality see [23, Exercise 4, Section 25]). Hence

$$\mathrm{Hom}_{\Omega_{\mathbb{Q}_q}}(R_{C,q}, 1 + c\mathbb{Z}_q[\xi_c]) = \mathrm{Det}(1 + c\mathfrak{M}_q) \subset \mathrm{Det}(\mathbb{Z}_q[C]^\times).$$

□

So the map π_C is well-defined and one easily checks that it is a group homomorphism. Moreover it follows immediately from the ideal-theoretic Hom-description that π_C is surjective.

Now let $\mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$ (resp. $\mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$) be the subgroup of $\mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d))$ which is generated by the classes of fractional ideals of $\mathbb{Q}(\chi^d)$ supported only above rational primes congruent to 1 modulo c (resp. by the classes of fractional ideals of $\mathbb{Q}(\chi^d)$ which have absolute norm congruent to 1 modulo c). Observe that π_C maps $\bigoplus_{d|c} \mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$ (resp. $\bigoplus_{d|c} \mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$) surjectively onto $\mathrm{Cl}(\mathbb{Z}[C])_\Sigma$ (resp. $\mathrm{Cl}'(\mathbb{Z}[C])_\Sigma$). We claim that $\mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d)) \subseteq \mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$ for any divisor d of c. In fact, fix $d \mid c$ and let for the moment $x \in \mathrm{Cl}_{\mathfrak{c}}(\mathbb{Q}(\chi^d))$ be any class. Then Chebotarev's density theorem implies that the set of primes of $\mathbb{Q}(\chi^d)$ belonging to x has positive Dirichlet's density $\delta > 0$ (see for instance [21, Chapter VII, Theorem 7.2]). Note that δ is also equal to the density of the set of primes of $\mathbb{Q}(\chi^d)$ belonging to x and splitting completely in $\mathbb{Q}(\chi^d)/\mathbb{Q}$ ([21, Chapter IV, Corollary 4.6]). In particular there exists a prime $\mathfrak{p}$ of $\mathbb{Q}(\chi^d)$ representing x and splitting completely in $\mathbb{Q}(\chi^d)/\mathbb{Q}$. Now suppose that $x \in \mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$: then the absolute norm of x is the trivial class in the ray class group of $\mathbb{Q}$ modulo (c) times the archimedean prime of $\mathbb{Q}$. This means that the absolute norm of $\mathfrak{p}$ is generated by a positive integer congruent to 1 modulo c. But since $\mathfrak{p}$ splits completely, the absolute norm of $\mathfrak{p}$ coincides with the prime ideal $p\mathbb{Z}$ below $\mathfrak{p}$. Hence x contains a prime whose underlying rational prime is congruent to 1 modulo c, which means that $x \in \mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$. Thus $\mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d)) \subset \mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$ for every divisor d of c as claimed and clearly the reverse inclusion $\mathrm{Cl}_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d)) \subset \mathrm{Cl}'_{\mathfrak{c},\Sigma}(\mathbb{Q}(\chi^d))$ also holds. Therefore

$$\mathrm{Cl}(\mathbb{Z}[C])_\Sigma = \pi_C(\bigoplus_{d|c} \mathrm{Cl}_{c,\Sigma}(\mathbb{Q}(\chi^d))) = \pi_C(\bigoplus_{d|c} \mathrm{Cl}'_{c,\Sigma}(\mathbb{Q}(\chi^d))) = \mathrm{Cl}'(\mathbb{Z}[C])_\Sigma.$$

□

4. Explicit unit elements

This section is devoted to finding explicit unit elements associated to the classes of $T_\mathbb{Z}$, S and R in $\mathrm{Cl}(\mathbb{Z}[\Delta])$, yielding the proof of their triviality. We stick to the notation introduced in the previous section.

4.1 A cyclotomic unit to describe $(T_\mathbb{Z})$

In this subsection we will prove the triviality of $T_\mathbb{Z}$ in $\mathrm{Cl}(\mathbb{Z}[\Delta])$, which has already been proved by Chase using a well-known result of Swan. We hope that our proof could serve as a guiding path for the cases of S and R. As to our knowledge, every proof of the triviality of $(T_\mathbb{Z})$ uses cyclotomic units. In our approach, we need them to modify the representative homomorphism v of $T_\mathbb{Z}$ (constructed in §3.2) by an equivariant function on characters of Δ with values in $\overline{\mathbb{Q}}^\times$. When we deal with the classes of S and R, we will essentially replace cyclotomic units by Jacobi and Gauss sums (compare (31) with (35) and (36)).

Proposition 4.1. *The class of* $\Sigma_\Delta(p) = p\mathbb{Z}[\Delta] + \mathrm{Tr}_\Delta\mathbb{Z}[\Delta]$ *is represented in* $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, J(\mathbb{Q}(\zeta)))$ *by*

the morphism whose $\mathfrak{q}$-component at a prime ideal $\mathfrak{q}$ of $\mathfrak{o}$ is

$$\begin{cases} 1 & \text{if } \mathfrak{q} \nmid e \ , \\ \mathrm{Det}(p^{-1}u_t) & \text{if } \mathfrak{q} \mid e \ , \end{cases}$$

where $u_t = 1 + \delta + \cdots + \delta^{p-1} \in \mathbb{Z}[\Delta]$. Further, if $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$ with $q \neq p$, then $u_t \in \mathbb{Z}_q[\Delta]^\times$. As a direct consequence, we get:

$$\big(T_{\mathbb{Z}}\big) = \big(\Sigma_\Delta(p)\big) = 1 \quad \text{in } \mathrm{Cl}(\mathbb{Z}[\Delta]) \ .$$

Proof. Recall the expression of the representative homomorphism v of $(T_{\mathbb{Z}})$ given in Lemma 3.2. In order to show that v belongs to the denominator of the Hom-description, we shall modify it by a global valued equivariant morphism, with values in the cyclotomic field $\mathbb{Q}(\zeta)$. We thus now look at v as a morphism with values in the idèles of $\mathbb{Q}(\zeta)$, through the natural embedding $J(\mathbb{Q}) \subseteq J(\mathbb{Q}(\zeta))$ given by $(x_q)_q \mapsto (x_{\mathfrak{q}})_{\mathfrak{q}}$ with $x_{\mathfrak{q}} = x_q$ if $\mathfrak{q}$ is a prime ideal of $\mathfrak{o}$ above the rational prime q. The content of the idèle $v(\chi^h) \in J(\mathbb{Q}(\zeta))$ is then the principal ideal $(p^{1-\delta_{h,e}})$ of $\mathfrak{o}$.

We consider the morphism $c_v \in \mathrm{Hom}(R_\Delta, \mathbb{Q}(\zeta)^\times)$ defined by

$$c_v(\chi^e) = 1 \ , \quad c_v(\chi^h) = \frac{1-\zeta^h}{1-\zeta^{ph}}\, p \tag{31}$$

for $h \in \{1, \ldots, e-1\}$. This morphism clearly commutes with the action of $\Omega_{\mathbb{Q}}$, hence vc_v^{-1} also represents the class of $\Sigma_\Delta(p)$. Note that $\frac{1-\zeta^{ph}}{1-\zeta^h}$ is a cyclotomic unit, thus belongs to $\mathfrak{o}^\times$. It follows that vc_v^{-1} takes unit idelic values, namely belongs to $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, \mathcal{U}\big(\mathbb{Q}(\zeta)\big))$. We deduce from [14, (I.2.19)], in which the $+$ sign disappears since the abelian group Δ has no symplectic character, that

$$vc_v^{-1} \in \mathrm{Det}(\mathcal{U}(\mathcal{M})) \ , \tag{32}$$

where $\mathcal{M}$ denote the maximal order in $\mathbb{Q}[\Delta]$. Since $\mathcal{M}_q (= \mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_q) = \mathbb{Z}_q[\Delta]$ whenever $q \nmid e$ (see [7, Proposition 27.1]) and $\mathcal{M}_\infty = \mathbb{R}[\Delta]$, we get that $(vc_v^{-1})_{\mathfrak{q}} \in \mathrm{Det}(\mathbb{Z}_q[\Delta]^\times)$ if $\mathfrak{q} \nmid e$ and $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$. We now prove that the same relationship holds when $\mathfrak{q} \mid e$. It will follow from the next result.

Lemma 4.2. *Let $\mathfrak{q}$ be a prime ideal of $\mathfrak{o}$ above a rational prime q different from p, then*

$$(vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(p^{-1}u_t)$$

and $u_t \in \mathbb{Z}_q[\Delta]^\times$. Hence $(vc_v^{-1})_{\mathfrak{q}} \in \mathrm{Det}(\mathbb{Z}_q[\Delta]^\times)$.

Proof. Let $h \in \{1, \ldots, e\}$, then

$$\mathrm{Det}_{\chi^h}(u_t) = \begin{cases} p & \text{if } h = e, \\ 1 + \zeta^h + \cdots + \zeta^{h(p-1)} = \frac{1-\zeta^{ph}}{1-\zeta^h} & \text{otherwise,} \end{cases} \ .$$

Since $\mathfrak{q} \nmid p$, one has $v(\chi^h)_{\mathfrak{q}} = 1$, hence $p^{-1}\mathrm{Det}_{\chi^h}(u_t) = (vc_v^{-1})_{\mathfrak{q}}(\chi^h)$. It follows that $(vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(p^{-1}u_t)$ as announced.

Further, we know by (32) that there exists $w_q \in \mathcal{M}_q^\times$ such that

$$(vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(w_q) \ .$$

It follows that $\mathrm{Det}(w_q) = \mathrm{Det}(p^{-1}u_t)$, so by Proposition 3.1 we must have $w_q = p^{-1}u_t$. Since $q \neq p$,

$$p^{-1}u_t \in \mathcal{M}_q^\times \cap \mathbb{Z}_q[\Delta] = \mathbb{Z}_q[\Delta]^\times \ ,$$

(see [23, §25, Exercise 4]); the same holds for u_t. □

Combining with the above result, we get that $vc_v^{-1} \in \mathrm{Det}(\mathcal{U}(\mathbb{Z}[\Delta]))$, namely vc_v^{-1} lies in the denominator of the Hom-Description of $\mathrm{Cl}(\mathbb{Z}[\Delta])$ and thus $(\Sigma_\Delta(p)) = 1$. Further we can change vc_v^{-1} by multiplying its $\mathfrak{q}$-component, whenever by $\mathfrak{q} \nmid e$, by its inverse (which also belongs to $\mathrm{Det}(\mathbb{Z}_q[\Delta]^\times)$ if $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$), to get the announced representative of $(\Sigma_\Delta(p))$. This ends the proof of Proposition 4.1. □

Clearly the trivial homomorphism sending any character to 1 also represents the class of $\Sigma_\Delta(p)$, since this class is trivial. In the representative morphism given in Proposition 4.1 (and in Theorem 1) we have chosen to keep the $\mathfrak{q}$-components for $\mathfrak{q} \mid e$ as they appeared in the proof because of their arithmetic meaning, in order to recall the link between the Galois structure of the Swan module and the cyclotomic units.

The above proposition proves the assertions concerning $(T_\mathbb{Z})$ in Theorem 1. In the rest of this section we will deal with the assertions concerning (S) and (R).

4.2 Gauss and Jacobi sums to describe (R) and (S)

4.2.1 We start introducing Gauss and Jacobi sums associated to the residue fields of the intermediate extensions of $\mathbb{Q}(\zeta)/\mathbb{Q}$. We denote by μ_∞ the subgroup of roots of unity in $\overline{\mathbb{Q}}^\times$ and we let ξ denote an element of order p of μ_∞.

Let e' be any divisor of e and recall that $\mathfrak{o}_{e'} = \mathbb{Z}[\zeta_{e'}]$ and $\mathfrak{p}_{e'} = \mathfrak{p} \cap \mathfrak{o}_{e'}$ respectively denote the ring of integers and the prime ideal below $\mathfrak{p}$ in the subfield $\mathbb{Q}(\zeta_{e'})$ of $\mathbb{Q}(\zeta)$. Let θ denote a multiplicative character of $\mathfrak{o}_{e'}/\mathfrak{p}_{e'}$, namely an homomorphism $(\mathfrak{o}_{e'}/\mathfrak{p}_{e'})^\times \to \mu_\infty$, extended to $\mathfrak{o}_{e'}/\mathfrak{p}_{e'}$ by the convention $\theta(0) = 0$. The Gauss sum relative to θ is defined as:

$$G(\theta) = \sum_{x \in \mathfrak{o}_{e'}/\mathfrak{p}_{e'}} \theta(x)\xi^{\mathrm{Tr}_{e'}(x)} \ ,$$

where $\mathrm{Tr}_{e'} : \mathfrak{o}_{e'}/\mathfrak{p}_{e'} \to \mathbb{Z}/p\mathbb{Z}$ denotes the residue field trace homomorphism. We will mostly be concerned with the case where $\theta = \left(\frac{\cdot}{\mathfrak{p}_{e'}}\right)^{-1}$ is the inverse of the e'th power residue symbol, and we set $G_{e'} = G(\left(\frac{\cdot}{\mathfrak{p}_{e'}}\right)^{-1})$. Specifically, for any $x \in (\mathfrak{o}_{e'}/\mathfrak{p}_{e'})^\times$, $\left(\frac{x}{\mathfrak{p}_{e'}}\right)$ is the e'th root of unity defined by the congruence

$$\left(\frac{x}{\mathfrak{p}_{e'}}\right) \equiv x^{\frac{p^{f_{e'}}-1}{e'}} \qquad (\mathrm{mod}\ \mathfrak{p}_{e'}) \ .$$

Suppose θ is a multiplicative character of $\mathfrak{o}_{e'}/\mathfrak{p}_{e'}$ that takes values in $\{0\} \cup \mu_{e'}$, then $G(\theta) \in \mathfrak{o}_{e'}[\xi]$. Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{e'}, \xi)/\mathbb{Q}(\zeta_{e'}))$ and let $\beta \in \mathbb{F}_p^\times$ be such that $\tau(\xi) = \xi^\beta$, then the multiplication-by-β map is a bijection of $\mathfrak{o}_{e'}/\mathfrak{p}_{e'}$ onto itself and

$$G(\theta)^\tau = \sum_{x \in \mathfrak{o}_{e'}/\mathfrak{p}_{e'}} \theta(x)\xi^{\beta\mathrm{Tr}_{e'}(x)} = \sum_{x \in \mathfrak{o}_{e'}/\mathfrak{p}_{e'}} \theta(\beta^{-1}x)\xi^{\mathrm{Tr}_{e'}(x)} = \theta(\beta)^{-1}G(\theta) \ . \tag{33}$$

It follows that

$$G(\theta)^{e'} \ \in \ \mathfrak{o}_{e'} \ , \tag{34}$$

in particular ${G_{e'}}^{e'} \in \mathfrak{o}_{e'}$.

In the same setting, let θ, θ' be multiplicative characters of $\mathfrak{o}_{e'}/\mathfrak{p}_{e'}$. The Jacobi sum relative to θ and θ' is:

$$J(\theta, \theta') = \sum_{x \in \mathfrak{o}_{e'}/\mathfrak{p}_{e'}} \theta(x)\theta'(1-x) \ .$$

If $\theta\theta'$ is a non trivial character, then one has ([15, §8, Theorem 1]):

$$J(\theta,\theta') = \frac{G(\theta)G(\theta')}{G(\theta\theta')} \ .$$

We set $J_{e'} = J(\left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1}, \left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1})$. Since e is odd, one has $\left(\frac{}{\mathfrak{p}_{e'}}\right)^2 \neq 1$, hence

$$J_{e'} = {G_{e'}}^{2-\sigma_{e',2}}$$

(where, with a slight abuse of notation, $\sigma_{e',2}$ is lifted to $\mathrm{Gal}(\mathbb{Q}(\zeta_{e'},\xi)/\mathbb{Q})$ in such a way that $\sigma_{e',2}(\xi)=\xi$) and, using (33),

$$J_{e'} \ \in \ \mathfrak{o}_{e'} \ .$$

As it is well-known, the factorization of Gauss and Jacobi sums can be written in a nice way using the Stickelberger element. More precisely, we have the following classical result about the ideals of $\mathfrak{o}_{e'}$ generated respectively by ${G_{e'}}^{e'}$ and $J_{e'}$. For details and for a proof see for instance [15, Theorem 2 in Chapter 14, Proposition 15.3.2 and its proof in Chapter 15].

Theorem 4.3 Stickelberger. *One has* $(2-\sigma_{e',2})\Theta_{e'} \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})]$, *and*

$$({G_{e'}}^{e'}) = {\mathfrak{p}_{e'}}^{e'\Theta_{e'}} \quad , \qquad (J_{e'}) = {\mathfrak{p}_{e'}}^{(2-\sigma_{e',2})\Theta_{e'}} \ .$$

4.2.2 In view of Propositions 3.13 and 3.17 we deduce, since $\mathfrak{p}^{N_{e,e'}} = \mathfrak{p}_{e'}^{f/f_{e'}}$, that the contents of the representative homomorphisms s and r, evaluated at χ^d with $d \mid e$ and $e = de'$, are principal ideals given by:

$$cont(s(\chi^d)) = \left({J_{e'}}^{f/f_{e'}}\right) \ ,$$
$$cont(r(\chi^d)) = \left({G_{e'}}^{ef/f_{e'}}\right) \ .$$

We now use the above generators of the content ideals to define elements c_s and c_r in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, \mathbb{Q}(\zeta)^\times)$. We have to multiply $J_{e'}^{f/f_{e'}}$ and $G_{e'}^{ef/f_{e'}}$ by suitable units in order to ensure that sc_s^{-1} and rc_r^{-1} lie in $\mathrm{Det}(\mathcal{U}(\mathbb{Z}[\Delta]))$. Let c_s and c_r denote the only homomorphisms in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, \mathbb{Q}(\zeta)^\times)$ such that, for any $d \mid e$,

$$c_s(\chi^d) = -(-J_{e'})^{f/f_{e'}} \ , \tag{35}$$
$$c_r(\chi^d) = (-1)^e(-G_{e'})^{ef/f_{e'}} \ , \tag{36}$$

where $e = de'$.

The first step to our goal is easy. Let $\mathcal{M}$ denote the maximal order in $\mathbb{Q}[\Delta]$.

Corollary 4.4. *The homomorphisms* sc_s^{-1} *and* rc_r^{-1} *belong to* $\mathrm{Det}(\mathcal{U}(\mathcal{M}))$.

Proof. It is clear from above that, for any divisor d of e, one has the following equalities of ideals:

$$\big(c_s(\chi^d)\big) = cont\big(s(\chi^d)\big) \ , \ \big(c_r(\chi^d)\big) = cont\big(r(\chi^d)\big) \ .$$

It follows that $(sc_s^{-1})_\mathfrak{q}$ (resp. $(rc_r^{-1})_\mathfrak{q}$) takes unit values for every place $\mathfrak{q}$. The result thus follows from [14, (I.2.19)] as in the proof of Proposition 4.1. □

The former result does not depend on the signs that appear in the definitions of c_s and c_r. The importance of the choice of these signs will become clear in the proof of our next result, which will occupy the rest of this subsection.

Theorem 4.5. *The homomorphisms sc_s^{-1} and rc_r^{-1} belong to* $\mathrm{Det}(\mathcal{U}(\mathbb{Z}[\Delta]))$. *In particular* (S) *and* (R) *are trivial in* $\mathrm{Cl}(\mathbb{Z}[\Delta])$.

This result, together with Lemmas 4.6 and 4.8, is a reformulation of Theorem 1, as far as (S) and (R) are concerned.

As in the proof of Proposition 4.1, one deduces from Corollary 4.4 that whenever $\mathfrak{q} \nmid e$, the $\mathfrak{q}$-component of sc_s^{-1} and rc_r^{-1} belongs to $\mathrm{Det}(\mathbb{Z}_q[\Delta]^\times)$ where $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$, so we focus on the case $\mathfrak{q} \mid e$. Recall from Corollary 3.8 that, when $\mathfrak{q} \mid e$,

$$(sc_s^{-1})_\mathfrak{q} = c_s^{-1} \ , \quad (rc_r^{-1})_\mathfrak{q} = c_r^{-1} \ , \tag{37}$$

where c_s^{-1} (resp. c_r^{-1}) is seen as a morphism with values in $\mathbb{Q}(\zeta)$, diagonally embedded in $J_q(\mathbb{Q}(\zeta)) = \prod_{\mathfrak{q}|q} \mathbb{Q}(\zeta)_\mathfrak{q}$.

4.2.3 *The proof for S.* For any $i = 0, \dots, e-1$, set

$$A_i = \left\{ x \in \mathfrak{o}/\mathfrak{p} \ : \ \left(\frac{x}{\mathfrak{p}}\right)^{-1} \left(\frac{1-x}{\mathfrak{p}}\right)^{-1} = \zeta^i \right\}$$

and $n_i = \#A_i$, then

$$J_e = \sum_{i=0}^{e-1} n_i \zeta^i.$$

The main result is the following.

Lemma 4.6. *Let* $u_s = \sum_{i=0}^{e-1} n_i \delta^i \in \mathbb{Z}[\Delta]$. *For any prime ideal* $\mathfrak{q}$ *of* $\mathfrak{o}$ *above a rational prime* q *such that* $q \mid e$, $u_s \in \mathbb{Z}_q[\Delta]^\times$, *and*

$$(sc_s^{-1})_\mathfrak{q} = \mathrm{Det}(u_s^{-1}) \ \in \ \mathrm{Det}(\mathbb{Z}_q[\Delta]^\times) \ .$$

Proof. We first show that, for any $d \mid e$

$$\mathrm{Det}_{\chi^d}(u_s) = -(-J_{e'})^{f/f_{e'}} \ , \tag{38}$$

where $e = de'$ as usual. Thanks to the Davenport-Hasse theorem [15, Theorem 1 and Exercice 18 in Chapter 11]

$$(-1)^{f/f_{e'}-1} {J_{e'}}^{f/f_{e'}} = \sum_{x \in \mathfrak{o}/\mathfrak{p}} \left(\frac{\overline{N}_{e,e'}(x)}{\mathfrak{p}_{e'}}\right)^{-1} \left(\frac{\overline{N}_{e,e'}(1-x)}{\mathfrak{p}_{e'}}\right)^{-1} \ ,$$

where $\overline{N}_{e,e'} : \mathfrak{o}/\mathfrak{p} \to \mathfrak{o}_{e'}/\mathfrak{p}_{e'}$ is the residual relative norm map. For any $x \in \mathfrak{o}/\mathfrak{p}$,

$$\left(\frac{x}{\mathfrak{p}}\right)^d \equiv \left(x^{\frac{p^f-1}{e}}\right)^d \equiv \left(x^{\sum_{t=0}^{f/f_{e'}-1} p^t f_{e'}}\right)^{\frac{p^{f_{e'}}-1}{e'}} \equiv \overline{N}_{e,e'}(x)^{\frac{p^{f_{e'}}-1}{e'}} \pmod{\mathfrak{p}} \ .$$

Thus

$$\left(\frac{x}{\mathfrak{p}}\right)^d = \left(\frac{\overline{N}_{e,e'}(x)}{\mathfrak{p}_{e'}}\right) \tag{39}$$

and therefore

$$-(-J_{e'})^{f/f_{e'}} = \sum_{x \in \mathfrak{o}/\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)^{-d} \left(\frac{1-x}{\mathfrak{p}}\right)^{-d} = \sum_{i=0}^{e-1} \sum_{x \in A_i} \zeta^{id} = \sum_{i=0}^{e-1} n_i \zeta^{id} = \mathrm{Det}_{\chi^d}(u_s) \ .$$

Assume that $\mathfrak{q} \mid e$. For any divisor d of e (once again $e = de'$), we deduce from (37) and (38) that

$$(sc_s^{-1})_{\mathfrak{q}}(\chi^d) = -(-J_{e'})^{-f/f_{e'}} = \mathrm{Det}_{\chi^d}(u_s^{-1}) \ .$$

The assertion of Corollary 4.4 implies that there exists $w_q \in \mathcal{M}_q^\times$ such that

$$(sc_s^{-1})_{\mathfrak{q}} = \mathrm{Det}(w_q^{-1}) \ .$$

It follows that $\mathrm{Det}(w_q) = \mathrm{Det}(u_s)$, so by Proposition 3.1 we must have $w_q = u_s \in \mathcal{M}_{\mathfrak{q}}^\times \cap \mathbb{Z}_q[\Delta] = \mathbb{Z}_q[\Delta]^\times$ (using again [23, Exercise 4, Section 25]). □

The rest of the proof of Theorem 4.5 and Theorem 1, concerning S, is similar to that of Proposition 4.1 above.

4.2.4 *The proof for R.* The proof for R goes the same way as that for S, with the additional difficulty that the expression of ${G_e}^e$ is not as explicit as that of J_e. Nevertheless, we can make it explicit using the multinomial formula. Let θ denote a multiplicative character of $\mathfrak{o}/\mathfrak{p}$ and let $\mathscr{C}_e$ denote the set of p^f-uples of integers $(k_1, \cdots, k_{p^f})$ such that $\sum_{h=1}^{p^f} k_h = e$. We number arbitrarily the elements of $\mathfrak{o}/\mathfrak{p}$ as x_h, $1 \leqslant h \leqslant p^f$, then

$$G(\theta)^e = \sum_{\mathscr{C}_e} \frac{e!}{\prod_{h=1}^{p^f} k_h!}\, \theta\Big(\prod_{h=1}^{p^f} x_h^{k_h}\Big)\xi^{\mathrm{Tr}(\sum_{h=1}^{p^f} k_h x_h)} \ ,$$

where Tr is the trace from $\mathfrak{o}/\mathfrak{p}$ to $\mathbb{F}_p$. For $j \in \mathbb{F}_p$ let $\mathscr{C}_{e,j}$ denote the set of p^f-uples $(k_1, \cdots, k_{p^f})$ of $\mathscr{C}_e$ such that $\mathrm{Tr}(\sum_{h=1}^{p^f} k_h x_h) = j$ and set

$$g_j(\theta) = \sum_{\mathscr{C}_{e,j}} \frac{e!}{\prod_{h=1}^{p^f} k_h!}\, \theta\Big(\prod_{h=1}^{p^f} x_h^{k_h}\Big) \ ,$$

then

$$G(\theta)^e = \sum_{j \in \mathbb{F}_p} g_j(\theta)\xi^j = \sum_{j \in \mathbb{F}_p \setminus \{1\}} \big(g_j(\theta) - g_1(\theta)\big)\xi^j \ .$$

We now assume that θ takes values in $\{0\} \cup \mu_e$, so $G(\theta)^e \in \mathfrak{o}$ by (34) and hence

$$G(\theta)^e = g_0(\theta) - g_1(\theta) \ .$$

Note incidentally that the $g_j(\theta)$ for $j \neq 0$ are all equal. For $j \in \mathbb{F}_p$ and $i \in \{0, \ldots, e-1\}$, we let $\mathscr{C}_{e,j,i}(\theta)$ denote the set of p^f-uples $(k_1, \cdots, k_{p^f})$ of $\mathscr{C}_{e,j}$ such that $\theta\big(\prod_{h=1}^{p^f} x_h^{k_h}\big) = \zeta^i$, and we set

$$m_i(\theta) = \sum_{\mathscr{C}_{e,0,i}(\theta)} \frac{e!}{\prod_{h=1}^{p^f} k_h!} - \sum_{\mathscr{C}_{e,1,i}(\theta)} \frac{e!}{\prod_{h=1}^{p^f} k_h!} \ ,$$

so that $m_i(\theta) \in \mathbb{Z}$ for each i and

$$G(\theta)^e = \sum_{i=0}^{e-1} m_i(\theta)\zeta^i \ .$$

The main interest of this construction lies in the following result.

Proposition 4.7. *Let θ denote a multiplicative character of $\mathfrak{o}/\mathfrak{p}$ taking values in $\{0\} \cup \mu_e$. Let $d \mid e$, then*

$$G\big(\theta^d\big)^e = \sum_{i=0}^{e-1} m_i(\theta)\zeta^{id} \ .$$

Proof. As usual we set $e = de'$. Let $i \in \{0, \dots, e-1\}$. If $d \nmid i$, then clearly $\mathscr{C}_{e,j,i}(\theta^d)$ is empty for any $j \in \mathbb{F}_p$, thus $m_i(\theta^d) = 0$. Further, if $i \in \{0, \dots, e'-1\}$ and $j \in \mathbb{F}_p$, one easily checks the equality of sets:

$$\mathscr{C}_{e,j,id}(\theta^d) = \bigcup_{k=0}^{d-1} \mathscr{C}_{e,j,i+ke'}(\theta) \ .$$

It follows that

$$m_{id}(\theta^d) = \sum_{k=0}^{d-1} m_{i+ke'}(\theta) \ ,$$

hence

$$G\big(\theta^d\big)^e = \sum_{i=0}^{e'-1} m_{id}(\theta^d)\zeta^{id} = \sum_{i=0}^{e'-1}\sum_{k=0}^{d-1} m_{i+ke'}(\theta)\zeta^{id} = \sum_{i=0}^{e-1} m_i(\theta)\zeta^{id} \ .$$

□

We can now show a statement which is similar to those of the previous subsections. Recall that $G_e = G(\big(\tfrac{}{\mathfrak{p}}\big)^{-1})$. For each $i \in \{0, \dots, e-1\}$, we set $m_i = m_i(\big(\tfrac{}{\mathfrak{p}}\big)^{-1})$.

Lemma 4.8. *Let* $u_r = \sum_{i=0}^{e-1} m_i \delta^i \in \mathbb{Z}[\Delta]$. *For any prime ideal* $\mathfrak{q}$ *of* $\mathfrak{o}$ *above a rational prime* q *such that* $q \mid e$, $u_r \in \mathbb{Z}_q[\Delta]^\times$ *and*

$$(rc_r^{-1})_{\mathfrak{q}} = \mathrm{Det}(u_r^{-1}) \ \in \ \mathrm{Det}(\mathbb{Z}_q[\Delta]^\times) \ .$$

Proof. Let $d \mid e$ and set $e = de'$. The Davenport-Hasse theorem for the lifted Gauss sum [15, Theorem 1 in Chapter 11] states that

$$-G(\left(\frac{\overline{N}_{e,e'}(\ )}{\mathfrak{p}_{e'}}\right)^{-1}) = (-G_{e'})^{f/f_{e'}} \ .$$

Raising to the power e, using (39) and Proposition 4.7, we get

$$(-1)^e(-G_{e'})^{ef/f_{e'}} = G(\Big(\frac{}{\mathfrak{p}}\Big)^{-d})^e = \sum_{i=0}^{e-1} m_i\zeta^{id} = \mathrm{Det}_{\chi^d}(u_r) \ ,$$

namely

$$\mathrm{Det}_{\chi^d}(u_r^{-1}) = c_r^{-1}(\chi^d) = (rc_r^{-1})_{\mathfrak{q}}(\chi^d)$$

whenever $\mathfrak{q} \mid e$. The end of the proof is as in §4.2.3. □

Using Lemma 4.8 we easily conclude the proof of Theorem 4.5 and Theorem 1 (as far as R is concerned), as in the proof of Proposition 4.1.

5. The class of the square root of the inverse different in locally abelian extensions

In this section we put ourselves in the global setting described in the Introduction. In particular N/E is a tame G-Galois extension of number fields. When N/E is locally abelian and $\mathcal{C}_{N/E}$ is a square, Theorem 2, together with Taylor's theorem, implies that $(\mathcal{A}_{N/E}) \in \mathrm{Cl}(\mathbb{Z}[G])$ is determined by the Artin root numbers of symplectic representations of G (see Corollary 5.2). Using this, one immediately deduces that $(\mathcal{A}_{N/E}) = 1$ if N/E has odd degree (in fact this is true even without assuming that N/E is locally abelian by a result of Erez, [11, Theorem 3]) or is abelian. We will also prove that $(\mathcal{A}_{N/E}) = 1$ if no

real place of E becomes complex in N/E. We will then show that this hypothesis is necessary and get Theorem 3 as a consequence. In fact, in the case where G is the binary tetrahedral group, we will exhibit a totally complex tame G-Galois extension $N/\mathbb{Q}$ such that $\mathcal{C}_{N/\mathbb{Q}}$ is a square and $(\mathcal{A}_{N/\mathbb{Q}}) \neq 1$. To explain how we found this example, we shall first verify that $(\mathcal{A}_{N/\mathbb{Q}}) = 1$ if $N/\mathbb{Q}$ is a tame locally abelian G-Galois extension such that $\mathcal{C}_{N/\mathbb{Q}}$ is a square and G is a group of order at most 24 which is not isomorphic to the binary tetrahedral group.

5.1 Root numbers of extensions unramified at infinity

In order to describe explicitly the relation between $(\mathcal{A}_{N/E})$ and the Artin root numbers, we need to recall some properties of these numbers and the definition of the Fröhlich–Cassou-Noguès class $t_G W_{N/E} \in \mathrm{Cl}(\mathbb{Z}[G])$.

5.1.1 We will omit the definition of the root numbers and just recall some of their standard properties (see [18]). Let Γ be a finite group and let K/k be a Γ-extension of local or global fields of characteristic 0. Let $\chi : \Gamma \to \mathbb{C}$ be a complex virtual character and let $W(K/k, \chi) \in \mathbb{C}$ denote the root number of χ. Then:

- if $\chi_1, \chi_2 : \Gamma \to \mathbb{C}$ are virtual characters, then $W(K/k, \chi_1 + \chi_2) = W(K/k, \chi_1)W(K/k, \chi_2)$;
- if Γ' is a subgroup of Γ, corresponding to the subextension K/k', and $\phi : \Gamma' \to \mathbb{C}$ is a virtual character, then $W(K/k, \mathrm{Ind}_{\Gamma'}^{\Gamma}\phi) = W(K/k', \phi)$;
- if $\overline{\Gamma}$ is a quotient of Γ, corresponding to the subextension K'/k, and $\phi : \overline{\Gamma} \to \mathbb{C}$ is a virtual character, then $W(K/k, \mathrm{Inf}_{\overline{\Gamma}}^{\Gamma}\phi) = W(K'/k, \phi)$.

If K/k is an extension of local fields, we have

$$W(K/k, \chi)W(K/k, \overline{\chi}) = \det_{\chi}(-1). \tag{40}$$

Here $\overline{\chi}$ denotes the conjugate character of χ and $\det_{\chi} : k^{\times} \to \mathbb{C}^{\times}$ is the map obtained by composing determinant of χ with the local reciprocity map $k^{\times} \to \Gamma$.

If K/k is an extension of number fields, there is a decomposition

$$W(K/k, \chi) = \prod_{P} W(K_{\mathcal{P}}/k_P, \chi_{D_{\mathcal{P}}}). \tag{41}$$

Here the product is taken over all places P of k; for a such P, $\mathcal{P}$ is any fixed place of K above P and $\chi_{D_{\mathcal{P}}}$ denotes the restriction of χ to the decomposition group $D_{\mathcal{P}}$ of $\mathcal{P}$ (which we view as a character of $\mathrm{Gal}(K_{\mathcal{P}}/k_P)$).

5.1.2 We come back to the global setting where N/E is a tame G-Galois extension of number fields. Let S_G denote the group of symplectic characters, namely the free abelian group generated by the characters of the irreducible symplectic representations of G. Recall (see [26, Section 13.2], [18, III]) that an irreducible representation $\rho : G \to GL(V)$ on a complex vector space V is called symplectic if V admits a nontrivial G-invariant alternating bilinear form. Symplectic characters are real-valued and their degree is even. Moreover an irreducible character $\chi : G \to \mathbb{C}$ is symplectic if and only if its Frobenius-Schur indicator is -1:

$$\frac{1}{\#G}\sum_{g \in G} \chi(g^2) = -1.$$

Let $W_{N/E} \in \mathrm{Hom}(S_G, \mathbb{C}^{\times})$ be defined by $W_{N/E}(\theta) = W(N/E, \theta)$ for $\theta \in S_G$. As shown by Fröhlich, we actually have $W_{N/E} \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_G, \{\pm 1\})$ ([14, I, Proposition 6.2]).

Let $L'/\mathbb{Q}$ be a Galois extension containing all the values of the characters of G. We now recall the definition of the map

$$t_G : \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_G, \{\pm 1\}) \to \mathrm{Cl}(\mathbb{Z}[G])$$

which is due to Ph. Cassou-Noguès. One first defines a map

$$t'_G : \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_G, \{\pm 1\}) \to \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(L'))$$

as follows. Let $f \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_G, \{\pm 1\})$ and let θ be an irreducible character of G. If $\mathfrak{l}$ is a place of L', the idèle $t'_G(f)(\theta) \in J(L')$ has $\mathfrak{l}$-component

$$\tilde{f}(\theta)_\mathfrak{l} = \begin{cases} f(\theta) & \text{if } \mathfrak{l} \text{ is finite and } \theta \text{ is symplectic} \\ 1 & \text{otherwise.} \end{cases}$$

The map t_G is then obtained by composing t'_G with the projection

$$\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(L')) \to \mathrm{Cl}(\mathbb{Z}[G])$$

induced by the Hom-description (see Section 3.1).

The class $t_G W_{N/E}$ appears in the following celebrated result of M. Taylor ([32, Theorem 1]).

Theorem 5.1 M. Taylor. *Let N/E be a tame G-Galois extension of number fields. Then*

$$(\mathcal{O}_N) = t_G W_{N/E} \quad \textit{in } \mathrm{Cl}(\mathbb{Z}[G]).$$

Combining the above theorem with Theorem 2 we get the following result.

Corollary 5.2. *Let N/E be a tame locally abelian G-Galois extension of number fields such that $\mathcal{C}_{N/E}$ is a square. Then*

$$(\mathcal{A}_{N/E}) = t_G W_{N/E} \quad \textit{in } \mathrm{Cl}(\mathbb{Z}[G]).$$

In particular, if G has no symplectic representations (for instance if G is abelian or has odd order), then $(\mathcal{A}_{N/E})$ is trivial.

5.1.3 We now want to prove that $(\mathcal{A}_{N/E})$ is also trivial if N/E is a tame locally abelian G-Galois extension which is unramified at infinite places, namely if real places of E do not become complex in N. Under this assumption we will show that $W_{N/E}$ is in fact trivial and for this we need some results on symplectic characters, which we now recall.

We dispose of a useful induction theorem for symplectic characters which is due to Martinet (see [18, III, Theorem 5.1]). Before giving its statement, recall that an irreducible complex character of G is said to be quaternionic if it has degree 2 and is lifted from a symplectic character of a quotient of G isomorphic to the generalized quaternion group H_{4n} for some $n \geqslant 2$. For every natural number $n \geqslant 2$, the quaternion group H_{4n} of order $4n$ is given by the following presentation

$$H_{4n} = \langle \sigma, \tau \mid \sigma^n = \tau^2, \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle. \tag{42}$$

Theorem 5.3 Martinet. *A symplectic character of G can be written as a $\mathbb{Z}$-linear combination of characters of the form $\mathrm{Ind}_H^G \theta$ for some subgroups H of G where either*

- *$\theta = \psi + \overline{\psi}$ with $\psi : H \to \mathbb{C}$ an irreducible character of degree 1 or*
- *θ is a quaternionic character of H.*

In order to use the above theorem, we will need some facts about generalized quaternions H_{4n} and their complex characters. Note first that $\langle \sigma \rangle$ is normal in H_{4n} since it has index 2. One easily sees

that the maximal abelian quotient of H_{4n} is $H_{4n}/\langle\sigma^2\rangle$, which has order 4. Thus H_{4n} has precisely four irreducible characters of degree 1. As for the remaining irreducible characters of H_{4n}, let $\varphi : \langle\sigma\rangle \to \mathbb{C}^\times$ be an injective homomorphism. Thus φ can be also thought as an irreducible character of $\langle\sigma\rangle$ of degree 1. Using Mackey's criterion ([26, Proposition 23]), it is easy to show that, if $1 \leqslant k \leqslant 2n-1$ and $k \neq n$, then $\mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\varphi^k$ is an irreducible character of G of degree 2. Computing explicitly the values $\mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\varphi^k$ (via [26, Théorème 12]), one finds that $\mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\varphi^k$ is always real-valued and

$$\mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\varphi^k = \mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\varphi^h$$

if and only if $\varphi^h = \overline{\varphi}^k$, *i.e.* $h = 2n-k$. Hence we have $n-1$ distinct irreducible characters of degree 2 and a standard counting argument (see [26, Corollary 2 to Proposition 5]) shows that these, together with the four degree-one characters mentioned above, give the set of all irreducible complex characters of H_{4n}.

Remark 5.4. When $n = 2$, we recover the classical quaternion group H_8. In particular H_8 has four one-dimensional characters, which we denote by ψ_i, $i = 1, 2, 3, 4$ (with ψ_1 denoting the trivial character) and one two-dimensional irreducible character, which we denote by ϕ. It is well-known that ϕ is symplectic (this can be shown by computing its Frobenius-Schur indicator, using the explicit values of ϕ given for instance in [26, Exercice 3, Section 12.2]).

In the following lemma, which will be useful in the proof of the next proposition, we describe the abelian subgroups of H_{4n} and the restriction to such subgroups of an irreducible character of H_{4n} of degree 2.

Lemma 5.5. *Let $\theta : H_{4n} \to \mathbb{C}$ be an irreducible character of degree 2. Let H' be an abelian subgroup of H_{4n}. Then either*

- *$H' \subseteq \langle\sigma\rangle$ and there exists a character $\rho : H' \to \mathbb{C}$ of degree 1 such that $\mathrm{Res}_{H'}^{H_{4n}}\theta = \rho + \overline{\rho}$ or*
- *H' is cyclic of order 4, contains $\langle\tau^2\rangle$ and $\mathrm{Res}_{H'}^{H_{4n}}\theta = \mathrm{Ind}_{\langle\tau^2\rangle}^{H'}\rho$ where $\rho : \langle\tau^2\rangle \to \mathbb{C}$ is a character of degree 1.*

Proof. By the above discussion, we know that there exists a character $\chi : \langle\sigma\rangle \to \mathbb{C}$ of degree 1 such that $\theta = \mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\chi$. Then we have (see [26, Proposition 22])

$$\mathrm{Res}_{H'}^{H_{4n}}\theta = \mathrm{Res}_{H'}^{H_{4n}}\mathrm{Ind}_{\langle\sigma\rangle}^{H_{4n}}\chi = \sum_{s\in\mathscr{S}} \mathrm{Ind}_{H'\cap\langle\sigma\rangle}^{H'}\chi_s$$

where $\mathscr{S}$ is a set of representatives of $H'\backslash H_{4n}/\langle\sigma\rangle$ and, for $s \in \mathscr{S}$, $\chi_s : H' \cap \langle\sigma\rangle \to \mathbb{C}$ is the character defined by $\chi_s(x) = \chi(s^{-1}xs)$ for every $x \in H' \cap \langle\sigma\rangle$.

We now distinguish two cases. First suppose that $H' \subset \langle\sigma\rangle$, *i.e.* $H' \cap \langle\sigma\rangle = H'$. Then we can take $\mathscr{S} = \{\mathrm{id}, \tau\}$ and $\chi_{\mathrm{id}} = \mathrm{Res}_{H'}^{\langle\sigma\rangle}\chi$, $\chi_\tau = \mathrm{Res}_{H'}^{\langle\sigma\rangle}\overline{\chi}$ (since $\chi(\tau^{-1}x\tau) = \chi(x^{-1}) = \overline{\chi(x)}$ for $x \in H'$). Thus we can take $\rho = \mathrm{Res}_{H'}^{\langle\sigma\rangle}\chi$ to get the result.

Now suppose that $H' \not\subset \langle\sigma\rangle$. We first show that H' contains $\langle\tau^2\rangle$ and is cyclic of order 4. Let $x \in H'$ and $x \notin \langle\sigma\rangle$. One easily sees that $x\sigma x^{-1} = \sigma^{-1}$, in particular x acts as -1 on the cyclic group $H' \cap \langle\sigma\rangle$. Since H' is abelian we also have $xyx^{-1} = y$ for every $y \in H' \cap \langle\sigma\rangle$. This shows that $H' \cap \langle\sigma\rangle$ is a subgroup of exponent 2 of $\langle\sigma\rangle$. Therefore we have $H' \cap \langle\sigma\rangle = \langle\tau^2\rangle$. Note that $H' \cap \langle\sigma\rangle$ has index 2 in H' because

$$4n = \#(H' \cdot \langle\sigma\rangle) = \frac{\#\langle\sigma\rangle\#H'}{\#(H' \cap \langle\sigma\rangle)} = \frac{2n\#H'}{\#(H' \cap \langle\sigma\rangle)}.$$

Hence H' has order 4 and is cyclic since τ^2 is the only element of order 2 in H_{4n} (as it follows by an easy calculation using the presentation of H_{4n} given in (42)). We now come to the character $\mathrm{Res}^{H_{4n}}_{H'}\theta$. Since $H' \not\subset \langle\sigma\rangle$, we can choose the set of representatives $\mathscr{S}$ to be $\{\mathrm{id}\}$, obtaining

$$\mathrm{Res}^{H_{4n}}_{H'}\theta = \mathrm{Ind}^{H'}_{\langle\tau^2\rangle}\chi_{\mathrm{id}}.$$

Hence taking $\rho = \chi_{\mathrm{id}} = \mathrm{Res}^{\langle\sigma\rangle}_{\langle\tau^2\rangle}\chi$ we get the result. □

Recall from the Introduction that in a tame Galois extension the inverse different is a square if and only if the inertia subgroups all have odd order.

Proposition 5.6. *Let N/E be a tame locally abelian G-Galois extension of number fields whose inverse different is a square. Suppose moreover that no archimedean place of E ramify in N (i.e. real places stay real). Then $W_{N/E} = 1$.*

Proof. We have to prove that $W(N/E,\chi) = 1$ for every symplectic character χ of G. Thanks to Theorem 5.3, χ can be written as

$$\theta = \sum_{H<G} n_H \mathrm{Ind}^G_H \theta_H$$

where $n_H \in \mathbb{Z}$ and $\theta_H : H \to \mathbb{C}$ is either a quaternionic character of H or can be written as $\theta_H = \psi + \overline{\psi}$ for some irreducible character $\psi : H \to \mathbb{C}$ of degree 1. Thanks to the properties of the Artin root number recalled in §5.1.1, we have

$$W(N/E,\chi) = \prod_{H<G} W(N/N^H,\theta_H)^{n_H}.$$

Of course, to prove that $W(N/E,\chi) = 1$, it is sufficient to prove that $W(N/N^H,\theta_H) = 1$ for every subgroup $H < G$. Observe that, for every subgroup $H < G$, N/N^H is a tame locally abelian extension whose inverse different is a square (since its inertia subgroups have odd order) and no archimedean place of N^H ramify in N (in other words N/N^H satisfy the hypotheses of the proposition). Therefore, replacing if necessary G by one of its subgroup H and N/E by N/N^H, it suffices to show that $W(N/E,\theta) = 1$ where $\theta : G \to \mathbb{C}$ is either a quaternionic character of G or $\theta = \psi + \overline{\psi}$ for some irreducible character $\psi : G \to \mathbb{C}$ of degree 1.

Suppose first that θ is quaternionic. In particular, for some $n \geqslant 2$, there exists a surjection $G \to H_{4n}$ and a symplectic character $\theta' : H_{4n} \to \mathbb{C}$ such that $\theta = \mathrm{Inf}^G_{H_{4n}}\theta'$. Then, if N/N' is the subextension corresponding to the kernel of $G \to H_{4n}$ (thus $H_{4n} \cong \mathrm{Gal}(N'/E)$), we have $W(N/E,\theta) = W(N'/E,\theta')$. So we are reduced to show that $W(N'/E,\theta') = 1$ and to do this we can assume that θ' is irreducible. In particular θ' has degree 2 (see the list of irreducible characters of H_{4n} given in §5.1.3). By (41), it is sufficient to show that, for every place P of E, we have $W(N'_{\mathcal{P}}/E_P,\theta'_{D_{\mathcal{P}}}) = 1$, where $\theta'_{D_{\mathcal{P}}}$ denotes the restriction of θ' to the decomposition group $D_{\mathcal{P}}$ of a fixed place $\mathcal{P}$ of N' above P. Note that N'/E is locally abelian since N/E is. In particular $D_{\mathcal{P}}$ is abelian and by Lemma 5.5 we have either

(a) $\theta'_{D_{\mathcal{P}}} = \rho + \overline{\rho}$ for some character $\rho : D_{\mathcal{P}} \to \mathbb{C}$ of degree 1 or

(b) $D_{\mathcal{P}}$ is cyclic of order 4, contains $\langle\tau^2\rangle$ and $\theta'_{D_{\mathcal{P}}} = \mathrm{Ind}^{D_{\mathcal{P}}}_{\langle\tau^2\rangle}\rho$ for some character $\rho : \langle\tau^2\rangle \to \mathbb{C}$ of degree 1.

In case (a) we have

$$W(N'_{\mathcal{P}}/E_P,\theta'_{D_{\mathcal{P}}}) = W(N'_{\mathcal{P}}/E_P,\rho)W(N'_{\mathcal{P}}/E_P,\overline{\rho}) = \det_\rho(-1).$$

Let $r_P : E_P^\times \to D_{\mathcal{P}}$ denote the local reciprocity map so that $\rho \circ r_P = \det_\rho$ (since ρ has degree 1). If P is archimedean, then $N'_{\mathcal{P}}/E_P$ is trivial by hypothesis and in particular $r_P(-1) = 1$ and $\det_\rho(-1) = 1$.

If instead P is a finite place, then, by class field theory, $r_P(-1)$ belongs to the inertia subgroup $I_\mathcal{P}$ of $\mathcal{P}$ in N'/E, since -1 is a unit of E_P. In particular, $r_P(-1)^{e_P} = 1$ and $e_P = \#I_\mathcal{P}$ is odd (N'/E has inertia subgroups of odd order since the same holds for N/E). But we also have $r_P(-1)^2 = 1$ and therefore $r_P(-1) = 1$, which implies that $\det_\rho(-1) = 1$ also in this case.

In case (b), if ρ is trivial, then $W(N'_\mathcal{P}/E_P, \theta'_{D_\mathcal{P}}) = W(N'_\mathcal{P}/E'_{P'}, \rho) = 1$ (here $N'_\mathcal{P}/E'_{P'}$ is the subextension corresponding to $\langle\tau^2\rangle \subset D_\mathcal{P}$), since the local root number of the trivial character is trivial. If instead ρ is nontrivial (*i.e.* ρ is the sign character of $\langle\tau^2\rangle$), then one easily sees that $\theta'_{D_\mathcal{P}} = \mathrm{Ind}_{\langle\tau^2\rangle}^{D_\mathcal{P}}\rho = \nu + \overline{\nu}$, where $\nu : D_\mathcal{P} \to \mathbb{C}^\times$ is a character of order 4. Thus we conclude as in case (a).

The case where $\theta = \psi + \overline{\psi}$ for some irreducible character $\psi : H \to \mathbb{C}^\times$ is also similar to the above case (a). □

Remark 5.7. Let $\mathcal{P}$ be a non-real archimedean place of N and suppose that $\mathcal{P}$ lies above a real place P of E. Then $E_P = \mathbb{R}$ and $N_\mathcal{P} = \mathbb{C}$ and the reciprocity map $r_P : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is nontrivial on -1 (in fact $\mathrm{Ker}(r_P) = \{x \in \mathbb{R}^\times, x > 0\}$). For this reason the arguments of the proof of the above proposition do not apply in the case where real places of E are allowed to become complex in N. In fact, as we shall see, the hypothesis on real places of Proposition 5.6 is necessary.

Combining Proposition 5.6 with Corollary 5.2 and Theorem 2, we get the following result.

Theorem 5.8. *Let N/E be a tame locally abelian G-Galois extension of number fields whose inverse different is a square. Suppose moreover that no archimedean place of E ramifies in N. Then*

$$(\mathcal{A}_{N/E}) = (\mathcal{O}_N) = 1$$

in $\mathrm{Cl}(\mathbb{Z}[G])$.

5.2 An inverse different whose square root has nontrivial class

In this section we want to find a group G and a tame locally abelian G-Galois extension $N/\mathbb{Q}$ whose inverse different is a square and $(\mathcal{A}_{N/\mathbb{Q}}) \neq 1$ in $\mathrm{Cl}(\mathbb{Z}[G])$. The first step is to find a good candidate for the group G, which we would also like to be of smallest possible order. For this reasons, we deduce some conditions G has to satisfy in order for an extension with the above properties to exist.

Lemma 5.9. *Suppose that $N/\mathbb{Q}$ is a tame locally abelian G-Galois extension whose inverse different is a square and $(\mathcal{A}_{N/\mathbb{Q}}) \neq 1$ in $\mathrm{Cl}(\mathbb{Z}[G])$. Then*

(i) G is generated by elements of odd order;

(ii) G has an irreducible symplectic representation.

Proof. Since $\mathbb{Q}$ has no nontrivial extension unramified at every finite prime, G is generated by the inertia subgroups of finite primes. As recalled before Proposition 5.6, these subgroups have odd order in our situation. Furthermore, if G has no symplectic representation, then $(\mathcal{A}_{N/\mathbb{Q}}) = 1$ by Corollary 5.2. □

5.2.1 We now show that there is no group of order smaller than 24 satisfying properties (i) and (ii) of Lemma 5.9.

Lemma 5.10. *Let H be a group. Then the following are equivalent:*

- *H has no proper normal subgroup of index a power of 2;*
- *H is generated by elements of odd order.*

Proof. Let H' be the subgroup generated by the elements of odd order of H. Then H' is normal since conjugation preserves the order of elements. We claim that H/H' has order a power of 2: let $x \in H/H'$ be a class represented by $h \in H$. Write the order of h as $2^a b$ with $a, b \in \mathbb{N}$ and b odd. Then x has order dividing 2^a since h^{2^a} has odd order, hence it belongs to H'. This shows our claim. Moreover any normal subgroup H'' of H of index a power of 2 contains H', since any element of odd order of H has trivial image in H/H''. From this we easily deduce the equivalence of the two assertions in the statement. □

Lemma 5.11. *Let H be a group of order 20. Then H is not generated by elements of odd order.*

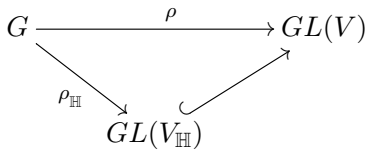
Proof. Observe that, by Sylow's theorem, H acts transitively by conjugation on the set of Sylow 5-subgroups. Let a denote the cardinality of this set. Then a equals the index of the normalizer of any Sylow 5-subgroup in H and thus divides 4, which is the index of any Sylow 5-subgroup in H. We also know that a is congruent to 1 modulo 5, by Sylow's theorem. Then $a = 1$, that is there is only one Sylow 5-subgroup which is therefore normal in H and has index 4. We conclude using Lemma 5.10. □

We shall use the following fact in the proof of the next result.

Remark 5.12. Let $\rho : G \to GL(V)$ be an irreducible symplectic representation on a complex vector space V of dimension $2m$. By scalar restriction, ρ defines a real representation $V_{\mathbb{R}}$ of G, of dimension $4m$. The commuting algebra

$$D = \{f \in \mathrm{End}(V_{\mathbb{R}}) \,:\, f \text{ is } G\text{-invariant}\}$$

clearly contains $\mathbb{C}$ (*i.e.* scalar multiplications by elements of $\mathbb{C}$) and is in fact isomorphic to the division algebra of quaternions $\mathbb{H}$ (see [26, Remarque 2, §13.2]). Thus V becomes a $\mathbb{H}$-vector space of dimension m, which we denote by $V_{\mathbb{H}}$, and we get a homomorphism $\rho_{\mathbb{H}} : G \to GL(V_{\mathbb{H}})$ which fits in a commutative diagram



Proposition 5.13. *Let H be a group of order less than 24 which is generated by elements of odd order. Then H has no irreducible symplectic representations.*

Proof. Recall that, for any irreducible representation ρ of H, we have $\deg\rho \mid \#H$ (see [26, Corollaire 2 to Proposition 16]) and $\deg\rho \leqslant 4$ since $(\deg\rho)^2 \leqslant \#H < 24$ (see [26, Corollaire 2 to Proposition 5]).

We argue by contradiction. Suppose that H has an irreducible symplectic representation $\rho_s : H \to GL_d(\mathbb{C})$ where $d = \deg\rho_s$. Then $d = 2$ or 4, since irreducible symplectic representations have even degree, and $\#H$ is even.

Suppose that $d = 4$, then $\#H \geqslant d^2 = 16$ and $d = 4 \mid \#H$. This implies that $\#H = 16$ or 20. The first possibility is trivially excluded (a nontrivial 2-group is certainly not generated by elements of odd order), while the second is ruled out by Lemma 5.11.

Then we must have $d = 2$. By Remark 5.12, this implies that ρ_s factors through an homomorphism $\rho_{s,\mathbb{H}} : H \to \mathbb{H}^\times \subset GL_2(\mathbb{C})$. In particular H has a quotient $\bar{H}$ isomorphic to a finite subgroup of $\mathbb{H}^\times$. The finite subgroups of $\mathbb{H}^\times$ are well-known (see for instance [8, p. 305]): since $\#\bar{H} < 24$, $\bar{H}$ is either cyclic or generalized quaternion. On the one hand, $\bar{H}$ cannot be cyclic, since otherwise ρ_s would be the inflation of a representation of a cyclic group and would not be irreducible since $d = 2$. On the other hand $\bar{H}$ cannot be isomorphic to H_{4n} for any $n \geqslant 2$, since otherwise $\bar{H}$ (and hence H) would have a subgroup of index 2 ($\langle\sigma\rangle$ has index 2 in H_{4n}, with notation as in §5.1.3), which is forbidden by Lemma 5.10. □

5.2.2 We now recall the definition and some properties of the binary tetrahedral group $\tilde{A}_4$. We will then show that $\tilde{A}_4$ is the only group of order 24 satisfying property (i) of Lemma 5.9 (we will see in §5.2.3 that it also satisfies property (ii)). We refer the reader to [24, Section 8.2] for any unproven assertion concerning $\tilde{A}_4$. This group is isomorphic to $SL_2(\mathbb{F}_3)$ and can be presented as

$$\tilde{A}_4 = \langle \alpha, \beta \,|\, \alpha^3 = \beta^3 = (\alpha\beta)^2 \rangle.$$

The center $Z(\tilde{A}_4) = \langle \alpha^3 \rangle$ is the only subgroup of order 2 of $\tilde{A}_4$ and $\tilde{A}_4/Z(\tilde{A}_4)$ is isomorphic to A_4, the alternating group on four elements. We thus have an exact sequence

$$1 \to Z(\tilde{A}_4) \to \tilde{A}_4 \to A_4 \to 1. \tag{43}$$

Moreover, $\tilde{A}_4$ has no subgroup of index 2: in particular, thanks to Lemma 5.10, it satisfies property (i) of Lemma 5.9 (and the above exact sequence is non-split). The group $\tilde{A}_4$ has other properties which will be useful later: every subgroup of $\tilde{A}_4$ is cyclic, except for its Sylow 2-subgroup, which is normal and isomorphic to the quaternion group H_8. For simplicity we will denote the Sylow 2-subgroup of $\tilde{A}_4$ by H_8. In fact, $\tilde{A}_4$ is also isomorphic to $H_8 \rtimes_\eta \mathbb{Z}/3\mathbb{Z}$ where $\eta : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(H_8) \cong S_4$ is any nontrivial homomorphism and S_4 is the permutation group on four elements.

Remark 5.14. The extension (43) is a *representation group* for A_4, in the sense of Schur, as we now recall. Let H be a finite group and let $M(H)$ denote its Schur multiplier (thus $M(H) = H^2(H, \mathbb{C}^\times) \cong H_2(H, \mathbb{Z})$, see [27, Definition 9.6, Chapter 2]). A representation group for H (see [27, Definition 9.10, Chapter 2]) is a central extension of H by a group Z

$$1 \to Z \to \tilde{H} \to H \to 1$$

such that

(RG1) $\tilde{H}$ has no proper subgroup H' such that $\tilde{H} = H'Z$;

(RG2) $\#M(H) = \#\big(Z \cap [\tilde{H}, \tilde{H}]\big)$, where $[\tilde{H}, \tilde{H}]$ denotes the commutator subgroup of $\tilde{H}$;

(RG3) $\#\tilde{H} = \#H \cdot \#M(H)$.

One can show that if the above properties are satisfied, then $Z \cong M(H)$ (see [27, (9.15), Chapter 2]). Schur showed that $M(A_4)$ has order 2 (see [27, (2.22), Chapter 3]) and it is easy to check that the extension (43) is indeed a representation group for A_4. In fact, Schur also showed that the extension (43) is the only representation group for A_4 up to isomorphism (see [27, Exercise 5, Chapter 2, §9]). One often says briefly that $\tilde{A}_4$ is the representation group of A_4.

Proposition 5.15. *A group of order* 24 *which is generated by elements of odd order is isomorphic to* $\tilde{A}_4$.

Proof. Let $\tilde{H}$ be a group of order 24 which is generated by elements of odd order. We will first prove that the center $Z(\tilde{H})$ of $\tilde{H}$ has order 2 and $\tilde{H}$ fits into an exact sequence

$$1 \to Z(\tilde{H}) \to \tilde{H} \to A_4 \to 1. \tag{44}$$

The second step will consist in showing that the above sequence is a representation group for A_4, which implies in particular that $\tilde{H}$ is isomorphic to $\tilde{A}_4$ by Remark 5.14.

In order to prove the first step, we argue as in the proof of Lemma 5.11. Observe that, by Sylow's theorem, $\tilde{H}$ acts transitively by conjugation on the set of its Sylow 3-subgroups, which has cardinality, say, a. Then a equals the index of the normalizer of any Sylow 3-subgroup in $\tilde{H}$ and thus divides the index of any Sylow 3-subgroup of $\tilde{H}$, which is 8. We also know that a is congruent to 1 modulo 3, by Sylow's theorem. Then $a = 1$ or 4 but the case $a = 1$ is excluded since otherwise $\tilde{H}$ would have a normal Sylow 3-subgroup of index a power of 2, which is impossible by Lemma 5.10. Hence $a = 4$.

Since conjugation permutes the Sylow 3-subgroups of $\tilde{H}$, we get an homomorphism $\varphi : \tilde{H} \to S_4$ and we want to determine $\#\ker(\varphi)$. Observe that, by the definition of φ, $\ker(\varphi)$ is contained in the normalizer of any Sylow 3-subgroup of $\tilde{H}$, which has index $a = 4$ in $\tilde{H}$. Thus $\#\ker(\varphi)$ divides 6. Since $\ker(\varphi)$ is normal, $\#\ker(\varphi)$ is not divisible by 3, otherwise $\tilde{H}$ would have a normal subgroup of index a power of 2, which is impossible by Lemma 5.10. The case $\#\ker(\varphi) = 1$ is also excluded because otherwise $\tilde{H} \cong S_4$ and S_4 has a subgroup of index 2 (namely A_4), again contradicting Lemma 5.10. Thus $\ker(\varphi)$ is a normal subgroup of order 2 of $\tilde{H}$ and $\tilde{H}/\ker(\varphi)$ is isomorphic to a subgroup of index 2 of S_4. It is well-known (and easy to check) that A_4 is the only subgroup of index 2 of S_4, hence $\tilde{H}/\ker(\varphi) \cong A_4$. In other words $\tilde{H}$ fits into an exact sequence

$$1 \to \ker(\varphi) \to \tilde{H} \to A_4 \to 1 \ .$$

Of course $\ker(\varphi)$ is contained in $Z(\tilde{H})$, being a normal subgroup of order 2. Furthermore the image of $Z(\tilde{H})$ in A_4 is trivial since $Z(A_4)$ is trivial. Hence $\ker(\varphi) = Z(\tilde{H})$ and we get (44), completing the first step of the proof.

To prove the second step, we have to show that (44) satisfies the properties of a representation group for A_4 (see Remark 5.14). Let $\tilde{H}'$ be a subgroup of $\tilde{H}$ such that $\tilde{H}'Z(\tilde{H}) = \tilde{H}$. Then, since $Z(\tilde{H})$ is normal in $\tilde{H}$, we have

$$\#\tilde{H}' = \frac{\#\tilde{H} \cdot \#(\tilde{H}' \cap Z(\tilde{H}))}{\#Z(\tilde{H})} = 12 \cdot \#(\tilde{H}' \cap Z(\tilde{H})) \ .$$

Thus $\#\tilde{H}'$ is either 12 or 24. Since the case $\#\tilde{H}' = 12$ is excluded by Lemma 5.10, we deduce that $\tilde{H}$ has no proper subgroup $\tilde{H}'$ such that $\tilde{H}'Z(\tilde{H}) = \tilde{H}$. Thus $\tilde{H}$ satisfies property (RG1).

Observe that the surjection $\tilde{H} \to A_4$ induces a surjection $[\tilde{H}, \tilde{H}] \to [A_4, A_4]$ on commutator subgroups, whose kernel is $Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}]$. In particular

$$4 = \#[A_4, A_4] = \frac{\#[\tilde{H}, \tilde{H}]}{\#(Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}])} \ .$$

This shows that $\#[\tilde{H}, \tilde{H}]$ is either 8 or 4, according to whether $Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}] = Z(\tilde{H})$ or not. We claim that $\#[\tilde{H}, \tilde{H}]$ cannot be 4. For, if $\#[\tilde{H}, \tilde{H}] = 4$, then $\tilde{H}$ has a quotient of order 6 (note that $[\tilde{H}, \tilde{H}]$ is normal in $\tilde{H}$) and any group of order 6 has a subgroup of index 2. Thus, by the homomorphism theorem, $\tilde{H}$ has a subgroup of index 2 which is a contradiction by Lemma 5.10. Thus $\#[\tilde{H}, \tilde{H}] = 8$ and $Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}] = Z(\tilde{H})$, so that $\tilde{H}$ satisfies (RG2).

Finally since $\#Z(\tilde{H}) = 2 = \#M(A_4)$, $\tilde{H}$ also satisfies (RG3) and hence (44) is a representation group for A_4. In particular by Schur's uniqueness result recalled in Remark 5.14, $\tilde{H} \cong \tilde{A}_4$. □

5.2.3 We now want to verify that $\tilde{A}_4$ also satisfies property (ii) of Lemma 5.9. Let us first recall the list and some properties of the irreducible complex characters of $\tilde{A}_4$.

We start with the group A_4, which has four irreducible complex characters (see [26, §5.7]). Three have degree 1 and are inflated from characters of the maximal abelian quotient of A_4 (which is cyclic of oder 3), while the remaining one has degree 3 and is real. Inflating these characters to $\tilde{A}_4$, we get three characters χ_1, χ_2 and χ_3 of degree 1 (one of these, say χ_1, is the trivial character, the other two are non-real) and a real character χ_4 of degree 3. Now $\tilde{A}_4$ has seven conjugacy classes (see [24, Section 8.2]), so $\tilde{A}_4$ must have three more irreducible characters χ_5, χ_6 and χ_7 (see [26, Théorème 7]). A standard counting argument (see [26, Corollary 2 to Proposition 5]) shows that these three characters all have degree 2. Moreover, using [26, Exercice 1, §13.2] and the explicit description of the conjugacy classes of $\tilde{A}_4$ given in [24, Section 8.2], one can easily show that $\tilde{A}_4$ has precisely three irreducible real-valued

characters. Therefore, since χ_1 and χ_4 are real while χ_2 and χ_3 are not, one of χ_5, χ_6 and χ_7 must be real-valued. Renumbering these characters if necessary, we may suppose that χ_5 is real-valued and χ_6 and χ_7 are non-real. Since complex conjugation acts on the set of irreducible complex characters of $\tilde{A}_4$ of degree 2, we must have $\chi_7 = \overline{\chi_6}$.

The character χ_5 is in fact symplectic, as we shall show in the next proposition. We first need a lemma, which will also be useful later. We are going to use some standard notation and results on complex characters (see [26]). For a group H, we denote by $(-,-)_H$ the scalar product defined on the set of complex-valued function on H. Then any complex character χ of H can be written uniquely as a linear combination with integral coefficients of the irreducible characters of H and in fact

$$\chi = \sum_{\rho} (\chi, \rho)_H \rho \tag{45}$$

where the sum is taken over the set of irreducible complex character of H. In particular

$$\deg \chi = \sum_{\rho} (\chi, \rho)_H \deg \rho. \tag{46}$$

and, if χ is the character of a representation of H, then $(\chi, \rho)_H \geqslant 0$ for any irreducible character ρ. If H' is a subgroup of H, χ' is a character of H' and χ is a character of H, then we have

$$(\mathrm{Ind}_{H'}^{H} \chi', \chi)_H = (\chi', \mathrm{Res}_{H'}^{H} \chi)_{H'}$$

(Frobenius reciprocity). If $\chi_{H'}$ (resp. χ_H) denotes the regular representation of H' (resp. H), we have

$$\chi_H = \mathrm{Ind}_{H'}^{H} \chi_{H'} \tag{47}$$

and in particular

$$(\chi_H, \rho)_H = (\chi_{H'}, \mathrm{Res}_{H'}^{H} \rho)_{H'}$$

for any character ρ of H. Applying this to $H' = \langle \mathrm{id} \rangle$, we get

$$(\chi_H, \rho)_H = \deg \rho. \tag{48}$$

We shall now describe the induction of an irreducible character of H_8 in terms of the χ_i (see Remark 5.4 for notation). This will be used not only to show that χ_5 is the only irreducible symplectic character of $\tilde{A}_4$ but also to compute root numbers (see Proposition 5.19).

Lemma 5.16. *We have*

$$\begin{aligned} \mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1 &= \chi_1 + \chi_2 + \chi_3 \ , \\ \mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_i &= \chi_4 \qquad \textit{for } i = 2,3,4 \ , \\ \mathrm{Ind}_{H_8}^{\tilde{A}_4} \phi &= \chi_5 + \chi_6 + \overline{\chi}_6 \ . \end{aligned}$$

Proof. Note that χ_1, χ_2 and χ_3 are trivial on H_8 (they are inflated from the maximal abelian quotient of $\tilde{A}_4$ which is $\tilde{A}_4/H_8$). Hence if $i \in \{1,2,3\}$, then $\mathrm{Res}_{H_8}^{\tilde{A}_4} \chi_i = \psi_1$ and

$$(\mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1, \chi_i)_{\tilde{A}_4} = (\psi_1, \mathrm{Res}_{H_8}^{\tilde{A}_4} \chi_i)_{H_8} = 1 \quad \text{for } i = 1,2,3$$

by Frobenius reciprocity. Moreover $\deg\left(\mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1\right) = [\tilde{A}_4 : H] \deg \psi_1 = 3$ and $(\mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1, \chi_i)_{\tilde{A}_4} \geqslant 0$ for any $1 \leqslant i \leqslant 7$, since $\mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1$ is the character of a representation of $\tilde{A}_4$. We deduce from (46) that $(\mathrm{Ind}_{H_8}^{\tilde{A}_4} \psi_1, \chi_i)_{\tilde{A}_4} = 0$ if $4 \leqslant i \leqslant 7$. Then we get the first equality of the lemma by (45).

Next we show the second equality. We fix $i \in \{2,3,4\}$. It is sufficient to show that $\mathrm{Ind}_{H_8}^{\tilde{A}_4}\psi_i$ is irreducible, since it has degree 3 and χ_4 is the only irreducible character of $\tilde{A}_4$ of degree 3. To prove that $\mathrm{Ind}_{H_8}^{\tilde{A}_4}\psi_i$ is irreducible, we shall use Mackey's irreducibility criterion (see [26, Proposition 23]). Since H_8 is normal in $\tilde{A}_4$, we have to check that, for every $g \in \tilde{A}_4 \setminus H_8$, ψ_i is different from the representation $\psi_i^g : H_8 \to \mathbb{C}^\times$ defined by $\psi_i^g(x) = \psi_i(g^{-1}xg)$ for every $x \in H_8$. Observe that the kernel of ψ_i has order 4 and therefore is not normal in $\tilde{A}_4$ (see §5.2.2). We deduce that the normalizer of $\ker\psi_i$ in $\tilde{A}_4$ is H_8. Hence, for every $g \in \tilde{A}_4 \setminus H_8$, there exists $y \in \ker\psi_i$ such that $g^{-1}yg \notin \ker\psi_i$ and in particular $\psi_i^g(y) = \psi_i(g^{-1}yg) \neq 1$. Thus ψ_i is trivial on y, while ψ_i^g is not. This shows that, for every $g \in \tilde{A}_4 \setminus H_8$, ψ_i^g and ψ_i are different and hence $\mathrm{Ind}_{H_8}^{\tilde{A}_4}\psi_i$ is irreducible and equals χ_4.

To prove the last equality of the lemma, let χ_{H_8} (resp. $\chi_{\tilde{A}_4}$) be the regular representation of H_8 (resp. $\tilde{A}_4$). Then, combining (45) and (48), we have

$$\begin{aligned}\chi_{H_8} &= \psi_1 + \psi_2 + \psi_3 + \psi_4 + 2\phi,\\ \chi_{\tilde{A}_4} &= \chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\chi_5 + 2\chi_6 + 2\chi_7.\end{aligned}$$

Using the first two equalities of the statement of the present lemma and (47), we deduce that

$$\begin{aligned}\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi &= \mathrm{Ind}_{H_8}^{\tilde{A}_4}\chi_{H_8}\\ &= \chi_{\tilde{A}_4}\\ &= \chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\chi_5 + 2\chi_6 + 2\chi_7\end{aligned}$$

and therefore $\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi = \chi_5 + \chi_6 + \chi_7$. □

Proposition 5.17. *The character χ_5 is the only irreducible symplectic character of $\tilde{A}_4$.*

Proof. Observe first that if $i \neq 5$, then χ_i is not symplectic because either it has odd degree or it takes non real values. So we are left to prove that χ_5 is symplectic. We will use the fact that an irreducible representation is symplectic if and only if its Frobenius-Schur indicator is -1 (see [26, Proposition 38]). So we have to prove that

$$\frac{1}{24}\sum_{g\in\tilde{A}_4}\chi_5(g^2) = -1 \ .$$

Thanks to Lemma 5.16 we have

$$\frac{1}{24}\sum_{g\in\tilde{A}_4}\chi_5(g^2) = \frac{1}{24}\sum_{g\in\tilde{A}_4}\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(g^2) - \frac{1}{24}\sum_{g\in\tilde{A}_4}\chi_6(g^2) - \frac{1}{24}\sum_{g\in\tilde{A}_4}\overline{\chi}_6(g^2) \ .$$

The terms involving χ_6 and $\overline{\chi}_6$ are trivial since the Frobenius-Schur indicator of an irreducible character which takes non real values is trivial (see [26, Proposition 38]). As for the term involving $\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi$, since H_8 is normal in $\tilde{A}_4$, the formula for the character of an induced representation (see [26, Théorème 12]) gives $\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(g^2) = 0$ if $g^2 \notin H_8$. Now observe that, if $g \in \tilde{A}_4$, then $g \in H_8$ if and only if $g^2 \in H_8$ (since $\tilde{A}_4/H_8$ has order coprime with 2) and, if $g \in H_8$, then

$$g^2 = \begin{cases} \mathrm{id} & \text{if } g = \mathrm{id}, z\\ z & \text{otherwise,}\end{cases}$$

where z is the only nontrivial square of H_8 (thus $z = \tau^2$ in the presentation of H_8 given in §5.1.3). We

deduce that

$$\sum_{g\in\tilde{A}_4}\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(g^2)=\sum_{g\in H_8}\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(g^2)$$
$$=2\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(\mathrm{id})+6\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(z)\ .$$

We have

$$\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(\mathrm{id})=\deg\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)=[\tilde{A}_4:H_8]\deg\phi=6\ .$$

The formula for the character of an induced representation, together with the fact that H_8 is normal in $\tilde{A}_4$ and $z\in Z(\tilde{A}_4)$, gives

$$\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(z)=\frac{1}{\#H_8}\sum_{g\in\tilde{A}_4}\phi(g^{-1}zg)=3\phi(z)=-6\ ,$$

where the last equality follows from the explicit computation of the values of ϕ (see for instance [26, Exercice 3, Section 12.2]). It follows that

$$\sum_{g\in\tilde{A}_4}\big(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\phi\big)(g^2)=-24$$

as desired. □

Thus $\tilde{A}_4$ satisfies the properties of Lemma 5.9 and has smallest possible order. In fact we also have that a tame $\tilde{A}_4$-Galois extension whose inverse different is a square of $\mathbb{Q}$ is automatically locally abelian, even locally cyclic.

Theorem 5.18. *The group $\tilde{A}_4$ is the group of smallest order satisfying properties (i) and (ii) of Lemma 5.9. Moreover, if $N/\mathbb{Q}$ is a tame $\tilde{A}_4$-Galois extension whose inverse different is a square, then $N/\mathbb{Q}$ is locally cyclic.*

Proof. The first assertion follows by Propositions 5.13, 5.15 and 5.17. As for the last assertion, $\tilde{A}_4$ and H_8, the only noncyclic subgroups of $\tilde{A}_4$, cannot be the decomposition subgroup of an archimedean place of N, since the latter is of order dividing 2. Suppose one of $\tilde{A}_4$ and H_8 is the decomposition subgroup of a finite place of N, then this place has to be ramified since decomposition subgroups of unramified places are cyclic. But finite primes have odd inertia degree in $N/\mathbb{Q}$, since $\mathcal{C}_{N/\mathbb{Q}}$ is a square, thus H_8 cannot be a decomposition subgroup. The same holds for $\tilde{A}_4$ itself: its quotient by the inertia subgroup would have to be cyclic, hence the commutator $[\tilde{A}_4,\tilde{A}_4]$ would have to be contained in the inertia subgroup. But $[\tilde{A}_4,\tilde{A}_4]=H_8$ (as we showed in the proof of Proposition 5.15) and therefore $\tilde{A}_4$ cannot be the decomposition group of a place of N. It follows that $N/\mathbb{Q}$ is locally cyclic. □

5.2.4 We now explicitly describe a tame $\tilde{A}_4$-Galois extension $N/\mathbb{Q}$ whose inverse different is a square. We use the results of Bachoc and Kwon [1], who studied the embedding problem of A_4-extensions in $\tilde{A}_4$-extensions.

We briefly recall how the $\tilde{A}_4$-Galois extension we are interested in is constructed, although this construction is not strictly necessary for us. We begin with the polynomial

$$X^4-2X^3-7X^2+3X+8$$

which is irreducible over $\mathbb{Q}$ and let γ be any fixed root of it (in an algebraic closure of $\mathbb{Q}$). Then, up to conjugation, $K=\mathbb{Q}(\gamma)$ is the totally real field of degree four over $\mathbb{Q}$ of smallest discriminant having trivial class number and Galois closure with Galois group isomorphic to A_4 (see [2, tables at pp.

395-396]). An easy computation with PARI [33] reveals that the Galois closure $M/\mathbb{Q}$ of K is explicitly given by the polynomial

$$X^{12} - 23X^{10} + 125X^8 - 231X^6 + 125X^4 - 23X^2 + 1 \ .$$

A further computation gives that the discriminant of $M/\mathbb{Q}$ is 163^8 (in particular $M/\mathbb{Q}$ is tame) and the four primes above 163 in $M/\mathbb{Q}$ have ramification index 3 (in particular $\mathcal{C}_{M/\mathbb{Q}}$ is a square). Let k denote the only degree 3 subextension of $M/\mathbb{Q}$, it follows that $k/\mathbb{Q}$ is totally ramified above 163 and unramified elsewhere, and M/k is unramified at every finite place.

Using again PARI, we get that the narrow class number of K equals 2. In other words the narrow Hilbert class field of K, namely its maximal abelian extension which is unramified at finite places, is of degree 2 over K. Moreover $K/\mathbb{Q}$ has the same discriminant as $k/\mathbb{Q}$. Therefore K satisfies the hypotheses of [1, Proposition 3.1(1)] and there exists a unique number field $\tilde{K}$ of degree 8 over $\mathbb{Q}$ with the following properties:

- $K \subset \tilde{K}$ and $\tilde{K}/K$ is unramified outside the primes ramifying in M/k (i.e. $\tilde{K}$ is a *pure* embedding of K);
- the Galois closure $N/\mathbb{Q}$ of $\tilde{K}$ has Galois group $\tilde{A}_4$.

It follows from $K \subset \tilde{K}$ and the definition of M and N that $M \subset N$ (see Figure 1). From the above we get that $\tilde{K}/K$ is unramified at every finite place, thus the same holds for N/M and for N/k. This shows that $N/\mathbb{Q}$ is tame and that its inverse different is a square (since the same holds for $k/\mathbb{Q}$).

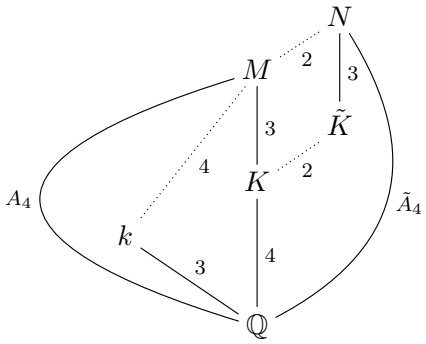


Figure 1: Extensions diagram

Since the class number of K is trivial, $\tilde{K}/K$ is ramified at some archimedean place (in fact $\tilde{K}$ is the narrow Hilbert class field of K). In particular $\tilde{K}$ is not totally real and therefore N is totally complex (being a non-totally real Galois extension of $\mathbb{Q}$). In other words the archimedean place of $\mathbb{Q}$ is ramified in N, so the extension $N/\mathbb{Q}$ does not satisfy the hypotheses of Proposition 5.6.

Bachoc and Kwon also compute a polynomial defining $\tilde{K}$ (see [1, table of p. 9, first line]):

$$X^8 + 14X^6 + 23X^4 + 9X^2 + 1.$$

With the help of PARI, we get that $N/\mathbb{Q}$ is explicitly given by the polynomial

$$\begin{aligned} &X^{24} - 3X^{23} - 2X^{22} + 16X^{21} - 12X^{20} + 52X^{19} - 324X^{18} - 436X^{17} + \\ &3810X^{16} - 1638X^{15} - 8012X^{14} - 12988X^{13} + 67224X^{12} - 76152X^{11} + \\ &41175X^{10} - 39587X^9 + 70068X^8 - 66440X^7 + 38488X^6 - 23248X^5 \\ &+16672X^4 - 6976X^3 + 2816X^2 - 1280X + 512. \end{aligned}$$

5.2.5 We now want to verify that $t_{\tilde{A}_4} W_{N/\mathbb{Q}} \in \mathrm{Cl}(\mathbb{Z}[\tilde{A}_4])$ is nontrivial. We first show that $W_{N/\mathbb{Q}} \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_{\tilde{A}_4}, \{\pm 1\})$ is not trivial.

Proposition 5.19. *We have $W(N/\mathbb{Q}, \chi_5) = -1$, i.e. $W_{N/\mathbb{Q}}$ is not trivial.*

Proof. By Lemma 5.16 and the properties of root numbers recalled in §5.1.1, we have

$$W(N/\mathbb{Q}, \chi_5) = W(N/k, \phi) W(N/\mathbb{Q}, \chi_6)^{-1} W(N/\mathbb{Q}, \overline{\chi}_6)^{-1} \ . \tag{49}$$

We first show that $W(N/k, \phi) = -1$. Since $k/\mathbb{Q}$ is cyclic of degree 3, it is totally real with three real places and $\mathrm{Gal}(N/k) = H_8$, the unique Sylow 2-subgroup of $\tilde{A}_4$. We will show that

$$W(N_\mathcal{P}/k_P, \phi_{D_\mathcal{P}}) = \begin{cases} -1 & \text{if } P \text{ is a real place of } k \\ 1 & \text{otherwise} \end{cases}$$

which implies, by (41), that $W(N/k, \phi) = -1$ (recall that $\phi_{D_\mathcal{P}}$ denotes the restriction of ϕ at $\mathcal{P}$). If P is a finite prime of k, then one shows the triviality of $W(N_\mathcal{P}/k_P, \phi_{D_\mathcal{P}})$ as in the proof of Proposition 5.6 (case (a)). Suppose that P is a real place of k, then the decomposition subgroup $D_\mathcal{P}$ of a place $\mathcal{P}$ of N above P is cyclic of order 2, since N is totally imaginary, and therefore $D_\mathcal{P} = Z(\tilde{A}_4) = \langle \alpha^3 \rangle$ since the center is the only subgroup of order 2 of $\tilde{A}_4$. In particular, by kemma 5.5, we must have $\phi_{D_\mathcal{P}} = \nu + \overline{\nu}$ where $\nu : D_\mathcal{P} \to \{\pm 1\}$ is a character (thus in fact $\nu = \overline{\nu}$ and $\phi_{D_\mathcal{P}} = 2\nu$). Actually, since $\phi(\alpha^3) = -2$ (as remarked in the proof of kemma 5.16), ν must be the sign character, *i.e.* the only nontrivial character of $D_\mathcal{P}$. We therefore obtain

$$W(N_\mathcal{P}/k_P, \phi_{D_\mathcal{P}}) = W(N_\mathcal{P}/k_P, \nu) W(N_\mathcal{P}/k_P, \overline{\nu}) = \det_\nu(-1) = \nu \circ r_P(-1) = -1,$$

where as usual $r_P : k_P^\times = \mathbb{R}^\times \to D_\mathcal{P}$ is the local reciprocity map at P (which is nontrivial on -1 precisely because P is ramified in N/k).

As for the factor $W(N/\mathbb{Q}, \chi_6)^{-1} W(N/\mathbb{Q}, \overline{\chi}_6)^{-1}$ in (49), using (41) as above, we are reduced to the local setting (here local means corresponding to a place of $\mathbb{Q}$). Again, if $\mathcal{P}$ is a place of N, either finite or archimedean,

$$W(N/\mathbb{Q}, (\chi_6)_{D_\mathcal{P}}) W(N/\mathbb{Q}, (\overline{\chi}_6)_{D_\mathcal{P}}) = \det{}_{(\chi_6)_{D_\mathcal{P}}}(-1) \ .$$

Observe that the determinant of χ_6 is trivial on H_8 (which is the commutator subgroup of $\tilde{A}_4$). If $\mathcal{P}$ is archimedean, $D_\mathcal{P}$ is cyclic of order 2 and therefore $D_\mathcal{P} \subset H_8$, since H_8 is the Sylow 2-subgroup of $\tilde{A}_4$. In particular $\det{}_{(\chi_6)_{D_\mathcal{P}}} = 1$. If instead $\mathcal{P}$ lies above a finite rational prime p, then, as in the proof of Proposition 5.6, the reciprocity map $r_p : \mathbb{Q}_p^\times \to D_\mathcal{P}$ is trivial on -1, since $r_p(-1)$ is of order dividing 2 and belongs to the inertia subgroup $I_\mathcal{P}$ which has odd order. In particular $\det{}_{(\chi_6)_{D_\mathcal{P}}}(-1) = 1$ also in this case. □

Concerning the map $t_{\tilde{A}_4}$, we have the following result.

Lemma 5.20. *The map*

$$t_{\tilde{A}_4} : \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_{\tilde{A}_4}, \{\pm 1\}) \to \mathrm{Cl}(\mathbb{Z}[\tilde{A}_4])$$

is an isomorphism between groups of order 2.

Proof. Consider the following diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_{\tilde{A}_4}, \{\pm 1\}) & \xrightarrow{t_{\tilde{A}_4}} & \mathrm{Cl}(\mathbb{Z}[\tilde{A}_4]) \\ \varphi \big\downarrow & & \big\downarrow res \\ \mathrm{Hom}_{\Omega_\mathbb{Q}}(S_{H_8}, \{\pm 1\}) & \xrightarrow{t_{H_8}} & \mathrm{Cl}(\mathbb{Z}[H_8]) \end{array} \tag{50}$$

where res is induced by restriction of scalars from $\mathbb{Z}[\tilde{A}_4]$ to $\mathbb{Z}[H_8]$. To define φ, observe that each of $\tilde{A}_4$ and H_8 has precisely one irreducible symplectic representation (χ_5 and ϕ, respectively). This means that $S_{\tilde{A}_4}$ and S_{H_8} both have $\mathbb{Z}$-rank 1 and $\Omega_{\mathbb{Q}}$ acts trivially on them. Of course $\Omega_{\mathbb{Q}}$ acts trivially on $\{\pm 1\}$ too, so that $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{\tilde{A}_4}, \{\pm 1\})$ and $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{H_8}, \{\pm 1\})$ both have order 2. Then we let φ be the only isomorphism between $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{\tilde{A}_4}, \{\pm 1\})$ and $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{H_8}, \{\pm 1\})$. In particular

$$\varphi(f)(\phi) = f(\chi_5)$$

for $f \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{\tilde{A}_4}, \{\pm 1\})$.

We claim that the above diagram is commutative. First observe that, thanks to [14, Theorem 12], we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\tilde{A}_4}, J(L')) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}[\tilde{A}_4]) \\ {\scriptstyle res}\downarrow & & \downarrow{\scriptstyle res} \\ \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{H_8}, J(L')) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}[H_8]) \end{array}$$

where L' is a large enough number field, the horizontal arrows are the projections induced by the Hom-description and the map res on the left satisfies $res(g)(\chi) = g(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\chi)$ for any $g \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\tilde{A}_4}, J(L'))$ and any character χ of H_8. Thus it is sufficient to prove that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{\tilde{A}_4}, \{\pm 1\}) & \xrightarrow{t'_{\tilde{A}_4}} & \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\tilde{A}_4}, J(L')) \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle res} \\ \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{H_8}, \{\pm 1\}) & \xrightarrow{t'_{H_8}} & \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{H_8}, J(L')) \end{array}$$

is commutative (the definition of $t'_{\tilde{A}_4}$ and t'_{H_8} is recalled in §5.1.2). Take $f \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(S_{\tilde{A}_4}, \{\pm 1\})$, then, on the one hand, by Lemma 5.16 we have

$$res(t'_{\tilde{A}_4}(f))(\chi) = t'_{\tilde{A}_4}(f)(\mathrm{Ind}_{H_8}^{\tilde{A}_4}\chi) = \begin{cases} t'_{\tilde{A}_4}(f)(\chi_5+\chi_6+\chi_7) & \text{if } \chi = \phi \\ t'_{\tilde{A}_4}(f)(\chi_1+\chi_2+\chi_3) & \text{if } \chi = \psi_1 \\ t'_{\tilde{A}_4}(f)(\chi_4) & \text{otherwise,} \end{cases}$$

for any irreducible character χ of H_8. In particular, using the definition of $t'_{\tilde{A}_4}$ and Proposition 5.17, we get, for every place $\mathfrak{l}$ of L',

$$res(t'_{\tilde{A}_4}(f))(\chi)_{\mathfrak{l}} = \begin{cases} f(\chi_5) & \text{if } \mathfrak{l} \text{ is finite and } \chi = \phi \\ 1 & \text{otherwise.} \end{cases}$$

On the other hand we have

$$\begin{aligned} t'_{H_8}(\varphi(f))(\chi)_{\mathfrak{l}} &= \begin{cases} \varphi(f)(\chi) & \text{if } \mathfrak{l} \text{ is finite and } \chi = \phi \\ 1 & \text{otherwise} \end{cases} \\ &= \begin{cases} f(\chi_5) & \text{if } \mathfrak{l} \text{ is finite and } \chi = \phi \\ 1 & \text{otherwise,} \end{cases} \end{aligned}$$

and we have proved our claim.

Now the bottom horizontal arrow of (50) is an isomorphism, by a result of Fröhlich (see [14, I, Proposition 7.2]). Swan showed that the right-hand vertical arrow of (50) is also an isomorphism (see [29, Theorem 14.1]). Thus $t_{\tilde{A}_4}$ is an isomorphism and all groups have order 2. □

Combining the above lemma (in fact just the injectivity of $t_{\tilde{A}_4}$) with Proposition 5.19 and Corollary 5.2, we get the main result of this section and prove Theorem 3 of the Introduction.

Theorem 5.21. *For the above $\tilde{A}_4$-extension $N/\mathbb{Q}$ one has $t_{\tilde{A}_4} W_{N/\mathbb{Q}} \neq 1$ in* $\mathrm{Cl}(\mathbb{Z}[\tilde{A}_4])$. *In particular the classes of $\mathcal{A}_{N/\mathbb{Q}}$ and $\mathcal{O}_N$ are both equal to the nontrivial element in* $\mathrm{Cl}(\mathbb{Z}[\tilde{A}_4])$.

Remark 5.22. Recall that N/k is unramified at every finite place and that $\mathrm{Gal}(N/k) = H_8$. Therefore $\mathcal{A}_{N/k} = \mathcal{O}_N$ and in particular $(\mathcal{A}_{N/k}) = (\mathcal{O}_N)$ in $\mathrm{Cl}(\mathbb{Z}[H_8])$. Note that, in the proof of Proposition 5.17, we have shown that $W_{N/k}$ is nontrivial. Moreover, since t_{H_8} is an isomorphism by [14, I, Proposition 7.2], we get that $t_{H_8} W_{N/k}$ is the nontrivial element of $\mathrm{Cl}(\mathbb{Z}[H_8])$. Thus N/k gives another example of a tame (in fact unramified at finite places) Galois extension whose codifferent is a square and the square root of the codifferent has nontrivial class in the locally free class group. Anyway, the case of $N/\mathbb{Q}$ is perhaps more suggestive, since $\mathcal{A}_{N/\mathbb{Q}} \neq \mathcal{O}_N$.

References

1 C. Bachoc and S.-H. Kwon. Sur les extensions de groupe de Galois $\tilde{A}_4$. *Acta Arith.*, 62(1):1–10, 1992.

2 J. Buchmann, M. Pohst, and J. von Schmettow. On the computation of unit groups and class groups of totally real quartic fields. *Math. Comp.*, 53(187):387–397, 1989.

3 D. Burns. On arithmetically realizable classes. *Math. Proc. Cambridge Philos. Soc.*, 118(3):383–392, 1995.

4 S. U. Chase. Ramification invariants and torsion Galois module structure in number fields. *J. Algebra*, 91(1):207–257, 1984.

5 T. Chinburg. Galois structure of de Rham cohomology of tame covers of schemes. *Ann. of Math. (2)*, 139(2):443–490, 1994.

6 J. Cougnard. Propriétés galoisiennes des anneaux d'entiers des p-extensions. *Compos. Math.*, 33:303–336, 1976.

7 C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981.

8 C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. II.* John Wiley & Sons Inc., New York, 1987.

9 B. Erez. *Structure galoisienne et forme trace dans les corps de nombres.* Thèse de doctorat, Université de Genève, 1987.

10 B. Erez. The Galois Structure of the Trace Form in Extensions of Odd Prime Degree. *J. Algebra*, 118:438–446, 1988.

11 B. Erez. The Galois Structure of the Square Root of the Inverse Different. *Math. Z.*, 208: 239–255, 1991.

12 B. Erez. A survey of recent work on the square root of the inverse different. *Astérisque*, (198-200):133–152 (1992), 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

13 A. Fröhlich. Arithmetic and Galois module structure for tame extensions. *J. Reine Angew. Math.*, 286/287:380–440, 1976.

14 A. Fröhlich. *Galois module structure of algebraic integers*, volume 1 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1983.

15 K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

16 T.-Y. Lam. Artin exponent of finite groups. *J. Algebra*, 9:94–119, 1968.

17 J. Martinet. Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$. *Ann. Inst. Fourier*, 19(1):1–80, 1969.

18 J. Martinet. Character theory and Artin L-functions. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

19 L. R. McCulloh. A class number formula for elementary-abelian-group rings. *J. Algebra*, 68(2):443–452, 1981.

20 L. R. McCulloh. Galois module structure of abelian extensions. *J. Reine Angew. Math.*, 375/376:259–306, 1987.

21 J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

22 E. J. Pickett and S. Vinatier. Self-Dual Integral Normal Bases and Galois Module Structure. *Compos. Math.*, 149(7):1175–1202, 2013.

23 I. Reiner. *Maximal Orders*. Academic Press, London, 1975.

24 H. E. Rose. *A course on finite groups*. Universitext. Springer-Verlag London Ltd., London, 2009.

25 J.-P. Serre. *Corps Locaux*. Hermann, Paris, 1968.

26 J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, 1978.

27 M. Suzuki. *Group theory I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1982.

28 R. G. Swan. Periodic resolution for finite groups. *Ann. of Math. (2)*, 72:267–291, 1960.

29 R. G. Swan. Projective modules over binary polyhedral groups. *J. Reine Angew. Math.*, 342:66–172, 1983.

30 M. J. Taylor. Galois module structure of integers of relative abelian extensions. *J. Reine Angew. Math.*, 303/304:97–101, 1978.

31 M. J. Taylor. On the self-duality of the ring of integers as a galois module. *Invent. Math.*, 46(2):173–178, 1978.

32 M. J. Taylor. On Fröhlich's conjecture for rings of integers of tame extensions. *Invent. Math.*, 63(1):41–79, 1981.

33 The PARI Group, Bordeaux. *PARI/GP, version* `2.5.3`, 2012. available from `http://pari.math.u-bordeaux.fr/`.

34 S. Ullom. Galois Cohomology of Ambiguous Ideals. *J. Number Theroy*, (1):11–15, 1969.

35 S. Ullom. Normal Bass in Galois extensions of number fields. *Nagoya Math J.*, (34):153–167, 1969.

36 S. Ullom. Integral representations afforded by ambiguous ideals in some abelian extensions. *J. Number Theory*, 6:32–49, 1974.

37 S. Vinatier. Sur la Racine Carrée de la Codifférente. *J. Théor. Nombres Bordeaux*, 15:393–410, 2003.

38 S. Vinatier. Galois Module Structure in Weakly Ramified 3-Extensions. *Acta Arith.*, 119(2):171–186, 2005.

Luca Caputo
Stéphane Vinatier

2.3 Structure galoisienne dans les 3-extensions faiblement ramifiées

Le travail qui termine ce chapitre sur les modules galoisiens est le plus ancien des trois. La plus grande partie en a été réalisée lors de mon année d'assistant post-doctoral à l'École Polytechnique Fédérale de Lausanne, le résultat principal présenté aux Journées Arithmétiques de Graz en 2003, l'article achevé l'automne suivant à Limoges et soumis pour publication peu après. Il est paru en 2005 dans la revue Acta Arithmetica sous le titre *Galois module structure in weakly ramified 3-extensions*, dans le volume 119, numéro 2, pages 171-186. Il améliore assez nettement, dans le cas $p = 3$, la majoration de l'ordre de la classe de la racine de la codifférente d'une p-extension faiblement ramifiée de $\mathbb{Q}$ établie dans ma thèse (voir [Vin03]), en donnant un majorant indépendant de la 3-extension faiblement ramifiée de $\mathbb{Q}$ considérée. En dehors de la trivialité escomptée de cette classe, qu'on ne sait pas prouver dans cette situation, ce majorant est aussi petit que possible puisqu'il vaut 3.

Ce résultat est obtenu à l'aide de calculs très explicites d'une expression bâtie sur le cube de la résolvante et faisant intervenir les conjugués du générateur de base normale de la racine carrée de la codifférente. L'action du groupe de Galois de l'extension sur cette expression est largement utilisée pour en faire ressortir les symétries et parvenir à y factoriser les plus grandes puissances de 3 possibles. Cela permet d'arriver au résultat annoncé en utilisant un critère d'intégralité portant sur la valuation en 3 de l'expression étudiée.

Comme écrit plus haut, cette méthode ne se généralise malheureusement pas aux p-extensions faiblement ramifiées de $\mathbb{Q}$ pour $p > 3$, du fait que la combinatoire de l'expression analogue devient beaucoup plus complexe pour $p \geq 5$. Ceci apparaîtra plus clairement dans l'article [Vin09] reproduit dans le chapitre 5. Du coup cet article n'a jusqu'alors pas eu de suite, du moins à ma connaissance.

Galois module structure in weakly ramified 3-extensions

Stéphane Vinatier

Abstract

Let $N/\mathbb{Q}$ be a weakly ramified 3-extension of Galois group G. We show that the class of the square root of the inverse different of the extension is of order dividing 3 in the class group of locally free $\mathbb{Z}[G]$-modules. The proof goes through the computation of a sum of cubes of resolvents, using an expression of this sum in terms of symmetric functions.

1. Introduction

Let p be an odd prime number, N a finite Galois p-extension of $\mathbb{Q}$, $\mathcal{O}$ its ring of integers, $\mathcal{D}$ its different and G its Galois group. Since G is of odd order, there exists a unique fractional ideal $\mathcal{A}$ of $\mathcal{O}$ such that

$$\mathcal{A}^2 = \mathcal{D}^{-1} \ ;$$

$\mathcal{A}$ is called the *square root of the inverse different*. It has the structure of a $\mathbb{Z}[G]$-module, which Erez has shown to be locally free if and only if the extension is *weakly ramified*, that is, if the second ramification groups are trivial at all places. We assume this condition is fulfilled (it is only relevant for places above p here) and we denote by $(\mathcal{A})$ the class of $\mathcal{A}$ in the class group $\mathrm{Cl}(\mathbb{Z}[G])$ of locally free $\mathbb{Z}[G]$-modules. The main result of this paper focusses on the case $p = 3$.

Theorem 1. *Let $N/\mathbb{Q}$ be a weakly ramified 3-extension. Then $(\mathcal{A})^3 = 1$ in $Cl(\mathbb{Z}[G])$.*

This is an improvment, in the case $p = 3$ considered here, of [V3, Theorem 1], which states that $(\mathcal{A})^e = 1$ (for any odd p, e standing for the ramification index of p in $N/\mathbb{Q}$). In other situations, the class $(\mathcal{A})$ is known to be trivial (and then $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module) when $N/\mathbb{Q}$ is a tame extension of odd degree (see [E], which deals more generally with relative extensions) and when $N/\mathbb{Q}$ is a weakly ramified extension of odd degree with abelian decomposition groups at wild places [V1].

The majorization of the order of $(\mathcal{A})$ obtained here for the non-locally abelian and non-tame case does not depend on the weakly ramified 3-extension under consideration (examples of these are constructed in [V2]); further it is as close as possible to the expected result that $(\mathcal{A})$ is trivial. There are at least two technical reasons, to be given below, that make $(\mathcal{A})^3$ much easier to handle than $(\mathcal{A})$ itself. Dealing with the general p case is another problem to solve. The importance of $p = 3$ will appear in the combinatorial computations of Section 3, which we are currently able to make only under this assumption.

The proof of Theorem 1 builds on results of [V3], namely those preceding Lemma 2.9 there, which is our starting point. In the next section we recall useful notations and results from that paper and from the literature; we also establish useful preliminary results, especially an integrality criterion. This is done

2000 Mathematics Subject Classification 11R33.

Keywords: Galois module structure; Wealky ramified extensions; Resolvents; Symmetric polynomials.

[1]Large part of this work has been completed while the author held a GTEM post-doctoral position at the "Chaire de Structures Algébriques et Géométriques" of Prof. Bayer, EPFL, Switzerland.

for all p. Eventually, in Section 3, we restrict to the case $p = 3$, reformulate our main result in terms of the former integrality criterion (Theorem 3.1) and give its proof, which makes a crucial use of the symmetries in the sum of p-th powers of resolvents appearing in the criterion.

Let us fix some notations before going any further: if K is a finite extension of $\mathbb{Q}_p$ contained in a fixed algebraic closure $\mathbb{Q}_p^c$ of $\mathbb{Q}_p$, we let Ω_K denote its absolute Galois group $\mathrm{Gal}(\mathbb{Q}_p^c/K)$, v_K its discrete valuation from $K^\times$ onto $\mathbb{Z}$, $\mathcal{O}_K$ its valuation ring, π_K a uniformizing parameter, and $\wp_K = \pi_K\mathcal{O}_K$ its valuation ideal. If L is a finite Galois p-extension of K, we denote by $\mathcal{D}_{L/K}$ and $\mathcal{A}_{L/K}$ the different of the extension and the square root of its inverse. The order of a finite group Λ is denoted by $|\Lambda|$, the subgroup generated by some $\lambda \in \Lambda$ by $\langle\lambda\rangle$ and the set of irreducible characters of Λ with values in $\mathbb{Q}_p^c$ by $\widehat{\Lambda}$.

2. Preliminaries

2.1 Prerequisites

We need some tools first developed by Fröhlich and Taylor to study the class of the ring of integers $(\mathcal{O})$ in $\mathrm{Cl}(\mathbb{Z}[G])$ when the extension $N/\mathbb{Q}$ is tamely ramified, and adjusted by Erez to the study of our class $(\mathcal{A})$. Details may be found in [F], [T] and [E]. The most important tool is Fröhlich's Hom-description of the class group, which is the following explicit isomorphism of groups:

$$\mathrm{Cl}(\mathbb{Z}[G]) \simeq \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))} \ ,$$

where R_G is the additive group of virtual characters of G with values in an algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$, $E \subset \mathbb{Q}^c$ is a "big enough" number field, $J(E)$ its idèle group, $\Omega_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ and $\mathcal{U}(\mathbb{Z}[G]) = \mathbb{R}[G]^\times \times \prod_l \mathbb{Z}_l[G]^\times$, l running over all prime numbers. We shall define the Det morphism at the finite components of $\mathcal{U}(\mathbb{Z}[G])$ below in formula (1).

The class $(\mathcal{A})$ is represented by an $\Omega_\mathbb{Q}$-equivariant morphism f (namely $f(\chi^\omega) = f(\chi)^\omega$ for all $\chi \in R_G, \omega \in \Omega_\mathbb{Q}$), which can be explicitly expressed in terms of resolvents and twisted Galois Gauss sums [E, Theorem 3.6]. For each prime number l, we denote by f_l the semi-local component of f in $J_l(E) = \prod_{\mathcal{L}|l} E_\mathcal{L}^\times$, where $\mathcal{L}$ runs through the prime ideals of $\mathcal{O}_E$ above l and $E_\mathcal{L}$ is the completion of E with respect to its $\mathcal{L}$-adic valuation. Our ultimate goal is to show that, up to multiplication of f by a suitable global $\Omega_\mathbb{Q}$-equivariant morphism (namely in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)$), f_l lies in $\mathrm{Det}(\mathbb{Z}_l[G]^\times)$ for every prime number l. In this paper we shall content ourselves with proving it for the p-th power of f_l when $p = 3$.

There are several simplifications due to former results at this stage: by [E, Theorem 2], we know that f_l belongs to $\mathrm{Det}(\mathbb{Z}_l[G]^\times)$ for $l \neq p$, so we only have to deal with f_p. Further, f_p can be written as a product [V3, Prop. 2.2]: $f_p = f_{(p),p} \prod_{l\neq p} f^*_{(l),p}$, in which the factors indexed by $l \neq p$ only involve tame ramification, so they are dealt with by adapting [T, Theorem 3] (see [V1, Lemma 4.4]). Since the absolute Galois group $\Omega_\mathbb{Q}$ acts transitively on the prime ideals $\wp$ above p in E, it is sufficient to look at what happens for one of them. We thus fix an embedding $j_p : \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c$ and we denote by M_p the closure in $\mathbb{Q}_p^c$ of the image $j_p(M)$ of a number field $M \subset \mathbb{Q}^c$; it yields a surjective morphism that we also denote by $j_p : J_p(E) \twoheadrightarrow E_p$, and an isomorphism between R_G and $R_{G,p}$, the group of virtual characters of G with values in $\mathbb{Q}_p^c$. We also get an embedding $j_p^* : \Omega_{\mathbb{Q}_p} \hookrightarrow \Omega_\mathbb{Q}$, $\omega \mapsto j_p^{-1} \circ \omega \circ j_p$, which yields the following isomorphism (see [CNT] for details):

$$j_p^* : \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J_p(E))}{\mathrm{Det}(\mathbb{Z}_p[G]^\times)} \xrightarrow{\sim} \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_p^\times)}{\mathrm{Det}(\mathbb{Z}_p[G]^\times)} \ ,$$

such that $j_p^*(f_{(p),p}) = j_p \circ f_{(p),p} \circ j_p^{-1}$. In fact, $j_p^*(f_{(p),p})$ is easily seen [V1, §3.4] to be induced from a morphism g_p on the group of virtual characters of $G(p)$, the decomposition group at the place of N above p corresponding to j_p, which we identify through j_p^* with $\Gamma = \mathrm{Gal}(N_p/\mathbb{Q}_p)$. In other words,

$$j_p^*(f_{(p),p})(\theta) = \mathrm{Ind}_G^\Gamma(g_p)(\theta) = g_p(\mathrm{Res}\,\theta) \ ,$$

where $\mathrm{Res}\,\theta$ is the restriction of a character θ of G to Γ. Showing that $(\mathcal{A})$ is trivial is now equivalent to showing that, up to multiplication of f by a suitable global $\Omega_\mathbb{Q}$-equivariant morphism, the resulting morphism g_p belongs to $\mathrm{Det}(\mathbb{Z}_p[\Gamma]^\times)$, that is, there exists $u = \sum_\Gamma u_\gamma \gamma \in \mathbb{Z}_p[\Gamma]^\times$ such that $g_p = \mathrm{Det}(u)$. By definition, $\mathrm{Det}(u)$ is the $\Omega_{\mathbb{Q}_p}$-equivariant morphism from $R_{\Gamma,p}$ to $E_p^\times$ such that, for any irreducible character θ of Γ,

$$\mathrm{Det}_\theta(u) = \det\Big(\sum_{\gamma\in\Gamma} u_\gamma \Theta(\gamma)\Big) \ , \tag{1}$$

where Θ is a matrix representation of Γ of character θ.

Now we take advantage of studying the p-th power of $(\mathcal{A})$, instead of $(\mathcal{A})$ itself. The class $(\mathcal{A})^p$ is represented in Fröhlich's Hom-description by f^p so, by the same arguments as above, we are reduced to showing that g_p^p belongs to $\mathrm{Det}(\mathbb{Z}_p[\Gamma]^\times)$. By [V3, Prop. 2.5], we can get rid of the p-th power of the twisted Galois Gauss sum involved in g_p^p, hence we only have to deal with the p-th power of the resolvent function $h_p \in \mathrm{Hom}(R_{\Gamma,p}, \mathcal{O}_{E_p}^\times)$, defined by

$$h_p(\theta) = (\alpha_p \,|\, \theta) = \mathrm{Det}_\theta\Big(\sum_{\gamma\in\Gamma} \gamma(\alpha_p)\gamma^{-1}\Big) \ , \tag{2}$$

where α_p denotes a basis of $\mathcal{A}_{N_p/\mathbb{Q}_p}$ as a $\mathbb{Z}_p[\Gamma]$-module. Further, if we denote by Γ_0 the inertia group of the extension $N_p/\mathbb{Q}_p$, by N_0 the fixed subfield and by β a basis of $\mathcal{A}_{N_p/N_0}$ as a $\mathcal{O}_{N_0}[\Gamma_0]$-module (it was denoted by β_p in [V3], but we wish to keep the notation β_i for another purpose in Section 3), we know by [E, (6.3)] that there exists $\lambda \in \mathcal{O}_{N_0}[\Gamma]^\times$ such that, for every $\theta \in R_{\Gamma,p}$,

$$(\alpha_p \,|\, \theta) = (\beta \,|\, \mathrm{Res}\,\theta)\mathrm{Det}_\theta(\lambda) \ ,$$

where Res is now the restriction of the characters of Γ to the inertia group. We shall characterize bases of $\mathcal{A}_{N_p/N_0}$ over $\mathcal{O}_{N_0}[\Gamma_0]$ in Subsection 2.3. Let $k_p \in \mathrm{Hom}(R_{\Gamma_0,p}, E_p^\times)$ be defined by $k_p(\chi) = (\beta \,|\, \chi)$ for every $\chi \in R_{\Gamma_0,p}$. We deduce that, for some $\lambda \in \mathcal{O}_{N_0}[\Gamma]^\times$,

$$h_p = \mathrm{Ind}_\Gamma^{\Gamma_0}(k_p)\mathrm{Det}(\lambda) \ .$$

[V3, Lemma 2.9] states that the p-th power of k_p is Ω_{N_0}-equivariant and takes values in the unit group, namely

$$k_p^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, \mathcal{O}_{E_p}^\times) = \mathrm{Det}(\mathcal{M}_0^\times) \ ,$$

where $\mathcal{M}_0$ is the maximal order of $N_0[\Gamma_0]$. By arguments similar to those used at the end of [V3, §2.2], we obtain:

Proposition 2.1. *If $k_p^p \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^\times)$, then $(\mathcal{A})^p = 1$.*

We are thus reduced to studying a function on the characters of Γ_0 instead of a function on the characters of Γ. We will see in the next subsection that Γ_0 is a very convenient group to work in (to begin with, it is abelian in our situation). Further in Subsection 2.4, we give an integrality criterion in order to establish the hypothesis of Proposition 2.1.

2.2 "Linear duality" of Γ_0

Since the second ramification group Γ_2 of N_p/N_0 is trivial, we know by [S1, IV2 Cor. 3 and 4] that $\Gamma_0 = \Gamma_1$ is abelian of exponent p, namely isomorphic, as an abelian group, to the product of say $m \geqslant 1$ copies of the field $\mathbb{F}_p$ with p elements. This gives Γ_0 the structure of an $\mathbb{F}_p$-vector space of dimension m. Notice that a subgroup of index p of Γ_0 becomes a hyperplane for this structure, whereas a subgroup of order p becomes a line. Further, fixing a group isomorphism from μ_p, the group of p-th roots of unity in $\mathbb{Q}_p^c$, to $\mathbb{F}_p$, enables identifying a character χ of Γ_0 with a linear form, so that the group of irreducible characters $\widehat{\Gamma}_0$ becomes the dual of Γ_0 as an $\mathbb{F}_p$-vector space, namely the "linear dual" of Γ_0.

One easily checks that Γ_0 has

$$r = \frac{p^m - 1}{p - 1} = 1 + p + \cdots + p^{m-1}$$

subgroups of order p, just by considering the elements of order p. By duality we get:

Lemma 2.2. *The number of subgroups of index p of Γ_0 equals r.*

The following result, as well as analogous ones, will be used repeatedly in Section 3.

Lemma 2.3. *(i) If $\gamma \in \Gamma_0 \setminus \{1\}$, then the number of characters $\chi \in \widehat{\Gamma}_0$ such that $\chi(\gamma) = 1$ equals p^{m-1}.*
(ii) If $m \geqslant 2$, $\gamma \in \Gamma_0 \setminus \{1\}$ and $\gamma' \in \Gamma_0 \setminus \langle\gamma\rangle$, then the number of characters $\chi \in \widehat{\Gamma}_0$ such that $\chi(\gamma) = \chi(\gamma') = 1$ equals p^{m-2}.

Proof. The map $\widehat{\gamma} : \widehat{\Gamma}_0 \to \mu_p$, $\chi \mapsto \chi(\gamma)$, is a linear form with the previous identifications, so its kernel is a hyperplane of $\widehat{\Gamma}_0$ (since $\gamma \neq 1$), thus of cardinality p^{m-1}. The conditions on γ and γ' ensure that they are linearly independent, so the set of characters which are trivial on both of them is the intersection of two distinct hyperplanes, hence of dimension $m - 2$ and of cardinality p^{m-2}. □

2.3 Normal basis for the square root of the inverse different

Here we consider a slightly more general situation: we let K denote any finite extension of $\mathbb{Q}_p$, L/K a finite abelian totally and weakly ramified p-extension, and we set $\Lambda = \mathrm{Gal}(L/K)$. We characterize bases of $\mathcal{A}_{L/K}$ over $\mathcal{O}_K[\Lambda]$ and, for every extension K' of K contained in L, we find a particular basis of $\mathcal{A}_{K'/K}$ over $\mathcal{O}_K[\mathrm{Gal}(K'/K)]$.

By [B, Lemma 4.2], there exists a uniformizing parameter π of K such that L is contained in the second Lubin-Tate division field $K_\pi^{(2)}$ of K corresponding to π. This implies in particular that for K' as above, K'/K is also weakly ramified. Further, by [B, Theorem 2], any uniformizing parameter π_L of L generates $\mathcal{O}_L$ as a module over its associated order in the group algebra $K[\Lambda]$ (see (3) below). We deduce the following.

Proposition 2.4. *Any uniformizing parameter π_L of L is a basis of $\wp_L$ over $\mathcal{O}_K[\Lambda]$.*

By Ullom's results [U, Theorem 2], we know that $\wp_L$ is a free $\mathcal{O}_K[\Lambda]$-module; it is clear that any generator is of valuation 1. Byott's work implies that the converse is true.

Proof. By [B, Lemma 3.1], the order associated to $\mathcal{O}_L$ satisfies:

$$\{x \in K[\Lambda] \mid x\mathcal{O}_L \subseteq \mathcal{O}_L\} = \mathcal{O}_K[\Lambda] + \mathcal{O}_K(\pi_K^{-1} T_\Lambda) \ , \tag{3}$$

where $T_\Lambda = \sum_{\lambda \in \Lambda} \lambda$. Thus by [B, Theorem 2], any $x \in \wp_L \subset \mathcal{O}_L$ may be expressed as

$$x = \sum_{\lambda \in \Lambda} n_\lambda \lambda(\pi_L) + y\pi_K^{-1} T_\Lambda(\pi_L) \ ,$$

where $y \in \mathcal{O}_K$ and $n_\lambda \in \mathcal{O}_K$ for every $\lambda \in \Lambda$. Notice that $\sum_\Lambda n_\lambda \lambda(\pi_L) \in \wp_L$, and thus $y\pi_K^{-1} T_\Lambda(\pi_L) \in \wp_L \cap \mathcal{O}_K = \wp_K$. We deduce that $y \in \wp_K$: indeed, since L/K is weakly ramified, [S1, III Prop. 7] shows that $\mathrm{Tr}_{L/K}(\wp_L) = \wp_K$ and $\mathrm{Tr}_{L/K}(\wp_L^2) = \wp_K^2$. This yields the following surjective additive morphism:

$$\mathrm{Tr}_{L/K} \ : \ \frac{\wp_L}{\wp_L^2} \longrightarrow\!\!\!\!\!\rightarrow \frac{\wp_K}{\wp_K^2} \ ,$$

where the quotients involved are both isomorphic to the residue field of K, so that the map is a 1-to-1 correspondence. Thus $T_\Lambda(\pi_L) = \mathrm{Tr}_{L/K}(\pi_L) \in \wp_K \setminus \wp_K^2$ and $y \in \wp_K$. Writing $y = \pi_K z$ with $z \in \mathcal{O}_K$ yields $x = \sum_\Lambda (n_\lambda + z)\lambda(\pi_L)$, so $\wp_L \subseteq \mathcal{O}_K[\Lambda]\,\pi_L$, which implies the proposition. □

Let $e = |\Lambda|$ denote the ramification index in L/K.

Corollary 2.5. *(i) If $\beta \in L$, then β is a basis of $\mathcal{A}_{L/K}$ over $\mathcal{O}_K[\Lambda]$ if and only if $v_L(\beta) = 1 - e$.*

(ii) Assume the previous condition is fulfilled and let K' be any intermediate extension of L/K. Then $\mathrm{Tr}_{L/K'}(\mathcal{A}_{L/K}) = \mathcal{A}_{K'/K} = \mathcal{O}_K[\mathrm{Gal}(K'/K)]\beta'$, where $\beta' = \mathrm{Tr}_{L/K'}(\beta)$.

Proof. By Hilbert's formula for the valuation of the different [S1, IV2 Prop. 4], $\mathcal{A}_{L/K} = \wp_L^{1-e} = \pi_K^{-1}\wp_L$; thus $\mathcal{A}_{L/K} = \mathcal{O}_K[\Lambda]\beta \Leftrightarrow \wp_L = \mathcal{O}_K[\Lambda](\pi_K\beta)$, and (i) is implied by Proposition 2.4. Set $e' = [K' : K]$. By [S1, III Prop. 7], one has

$$\mathrm{Tr}_{L/K'}(\mathcal{A}_{L/K}) = \mathrm{Tr}_{L/K'}(\wp_L^{1-e}) = \wp_{K'}^{1-e'} = \mathcal{A}_{K'/K} \ ,$$

so $v_{K'}(\beta') \geqslant 1 - e'$. Further, any $x \in \mathcal{A}_{L/K}$ can be written $x = \sum_\Lambda x_\lambda \lambda(\beta)$ with $x_\lambda \in \mathcal{O}_K$, hence $\mathrm{Tr}_{L/K'}(x) = \sum_\Lambda x_\lambda \lambda(\beta')$, which implies $v_{K'}(\beta') \leqslant 1 - e'$, and (i) yields (ii). □

2.4 An integrality criterion

Let again K be a finite extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_p^c$ and let Λ be any finite abelian group. We denote by $\mathcal{M}_\Lambda$ the maximal order of $K[\Lambda]$. Wedderburn's isomorphism of $\mathbb{Q}_p^c$-algebras reads [S2, Prop. 10]:

$$\mathbb{Q}_p^c[\Lambda] \simeq \bigoplus_{\chi \in \widehat{\Lambda}} \mathbb{Q}_p^c \ , \quad u = \sum_{\lambda \in \Lambda} u_\lambda \lambda \mapsto \left(\sum_{\lambda \in \Lambda} u_\lambda \chi(\lambda) \right)_{\chi \in \widehat{\Lambda}} .$$

Notice that $\sum_\Lambda u_\lambda \chi(\lambda) = \mathrm{Det}_\chi(u)$ by (1). This morphism yields

$$\mathcal{M}_\Lambda \simeq \bigoplus_{\chi \in \widehat{\Lambda}} \mathcal{O}_{K(\chi)} \ ,$$

where $K(\chi)$ is the extension of K generated by the values of χ. Fourier's inversion formula [S2, Prop. 11] links the coordinates u_λ of u to its image by the former isomorphism:

$$u_\lambda = \frac{1}{|\Lambda|} \sum_{\chi \in \widehat{\Lambda}} \chi(\lambda^{-1}) \mathrm{Det}_\chi(u) \ .$$

We deduce the integrality criterion we are looking for.

Proposition 2.6. *If $\psi \in \mathrm{Det}(\mathcal{M}_\Lambda^\times)$, then $\psi \in \mathrm{Det}(\mathcal{O}_K[\Lambda]^\times)$ if and only if, for every $\lambda \in \Lambda$, the sum*

$$S_\psi(\lambda) = \sum_{\chi \in \widehat{\Lambda}} \chi(\lambda^{-1}) \psi(\chi)$$

belongs to $|\Lambda|\mathcal{O}_K$.

Proof. Let $u \in \mathcal{M}_\Lambda^\times$ be such that $\psi = \mathrm{Det}(u)$. Write $u = \sum_\Lambda u_\lambda \lambda$ with $u_\lambda \in K$. Then $u \in \mathcal{O}_K[\Lambda]^\times$ if and only if $u_\lambda \in \mathcal{O}_K$ for every $\lambda \in \Lambda$, since $\mathcal{O}_K[\Lambda] \cap \mathcal{M}_\Lambda^\times = \mathcal{O}_K[\Lambda]^\times$. So we are done thanks to the above formula. □

3. The $p = 3$ case

We now suppose $p = 3$, so our weakly ramified extension $N/\mathbb{Q}$ is a 3-extension. We still denote by N_3 the closure in $\mathbb{Q}_3^c$ of $j_3(N)$, by Γ the Galois group of the local extension $N_3/\mathbb{Q}_3$, by Γ_0 its inertia group, by N_0 the fixed subfield of N_3 under Γ_0 and by β a basis of $\mathcal{A}_{N_3/N_0}$ over $\mathcal{O}_{N_0}[\Gamma_0]$. The 3-extension N_3/N_0 is abelian, totally and weakly ramified, so we may apply the results of Subsection 2.3. In order to prove Theorem 1, thanks to Propositions 2.1 and 2.6, we are reduced to showing:

Theorem 3.1. *For every $\gamma \in \Gamma_0$, $S(\gamma) = \sum_{\chi \in \widehat{\Gamma}_0} \chi(\gamma^{-1})(\beta \,|\, \chi)^3$ belongs to $|\Gamma_0|\mathcal{O}_{N_0}$.*

Let m be such that $|\Gamma_0| = 3^m$. We suppose $m \geqslant 2$ in the following, since [V3, Theorem 1] implies Theorem 1 when $m = 1$. By Lemma 2.2, Γ_0 has $r = \frac{3^m-1}{2}$ subgroups of index 3; to each of them, we attach an irreducible character $\chi_i \in \widehat{\Gamma}_0$, $1 \leqslant i \leqslant r$, which has this subgroup as kernel. We denote by χ_0 the trivial character of Γ_0; then the set $\{\chi_i \mid 0 \leqslant i \leqslant r\}$ represents the orbits of $\widehat{\Gamma}_0$ under the action of Ω_{N_0}. Indeed, two characters χ and χ' are conjugate under the action of Ω_{N_0} if and only if $\ker(\chi) = \ker(\chi')$; one then has $\chi' = \chi$ or $\chi' = \chi^2$.

For each $1 \leqslant i \leqslant r$, we let K_i denote the fixed subfield of N_3 under $\ker(\chi_i)$, we set $\Delta_i = \mathrm{Gal}(K_i/N_0)$ and $\beta_i = \mathrm{Tr}_{N_3/K_i}(\beta)$. Then, by Corollary 2.5, β_i is a basis of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}[\Delta_i]$. Further we set $\beta_0 = \mathrm{Tr}_{N_3/N_0}(\beta)$.

The following diagram sums up the notations for the local extension.

$$\begin{array}{ccccc} & N_3 & \ni & \beta & \\ \ker(\chi_i)\Big(& \big| 3^{m-1} & & & \\ & K_i & \ni & \beta_i\,, & \qquad 1 \leqslant i \leqslant r\ . \\ \Delta_i\Big(& \big| 3 & & & \\ & N_0 & \ni & \beta_0 & \\ & \big| & & & \\ & \mathbb{Q}_3 & & & \end{array}$$

From the definition (2) of the resolvent, one easily sees that $(\beta \,|\, \chi_0) = \beta_0$. Further, if χ is a non-trivial character of Γ_0, there exists $1 \leqslant i \leqslant r$ such that $\ker(\chi) = \ker(\chi_i)$, and one has

$$(\beta \,|\, \chi)_{\Gamma_0} = (\beta_i \,|\, \chi)_{\Delta_i}\ ,$$

where the subscripts mean that χ is viewed as a character of Γ_0 (inflated from Δ_i) on the left side and as a character of Δ_i on the right side. We shall omit such subscripts in the following. We set, for $1 \leqslant i \leqslant r$,

$$T_i(\gamma) = \chi_i(\gamma^{-1})(\beta_i \,|\, \chi_i)^3 + \chi_i^2(\gamma^{-1})(\beta_i \,|\, \chi_i^2)^3\ ;$$

we then get

$$S(\gamma) = \beta_0^3 + \sum_{i=1}^{r} T_i(\gamma)\ . \tag{4}$$

3.1 Computation of $S(1)$

We let ζ be a primitive 3rd root of unity and for each $1 \leqslant i \leqslant r$, we choose δ_i in Γ_0 such that $\chi_i(\delta_i) = \zeta$; consequently, $\Gamma_0 = \langle \delta_i \rangle \times \ker(\chi_i)$ and $\Delta_i = \langle \delta_{i|K_i} \rangle$. For $k \in \{1, 2, 3\}$, we denote by $\sigma_{k,i}$ the sum of

all products of k distinct conjugates of β_i in K_i/N_0 and by $\tau_{k,i}$ the sum of the k-th powers of all these conjugates. We compute:

$$\begin{aligned} T_i(1) &= (\beta_i \,|\, \chi_i)^3 + (\beta_i \,|\, \chi_i^2)^3 \\ &= (\beta_i + \zeta^2\delta_i(\beta_i) + \zeta\delta_i^2(\beta_i))^3 + (\beta_i + \zeta\delta_i(\beta_i) + \zeta^2\delta_i^2(\beta_i))^3 \\ &= 2\tau_{3,i} + 12\sigma_{3,i} + 3\mathrm{Tr}_{K_i/N_0}\Big(\beta_i^2(-\delta_i(\beta_i) - \delta_i^2(\beta_i))\Big) \\ &= 2\tau_{3,i} + 12\sigma_{3,i} + 3(\tau_{3,i} - \beta_0\tau_{2,i}) \ . \end{aligned}$$

Using the relations between σ's and τ's [vW, Exercise 5.18] yields

$$T_i(1) = 2\beta_0^3 - 9\beta_0\sigma_{2,i} + 27\sigma_{3,i} \ ,$$

so that

$$S(1) = (2r+1)\beta_0^3 - 9\beta_0\sum_{i=1}^{r}\sigma_{2,i} + 27\sum_{i=1}^{r}\sigma_{3,i} \ . \tag{5}$$

Since $\beta_0 = \mathrm{Tr}_{N_3/N_0}(\beta)$ and $\mathcal{A}_{N_0/N_0} = \mathcal{O}_{N_0}$, β_0 is a unit by Corollary 2.5; further, $2r+1 = 3^m$, so we only have to deal with $9\sum_{i=1}^{r}\sigma_{2,i}$ and $27\sum_{i=1}^{r}\sigma_{3,i}$.

We first notice that the $\sigma_{k,i}$ are evaluations at the $\gamma(\beta)$'s, $\gamma \in \Gamma_0$, of polynomials in indeterminates X_γ's, $\gamma \in \Gamma_0$. As an abuse of language, we shall say that a property is *formally* satisfied by the evaluation at the $\gamma(\beta)$'s of such a polynomial when we mean that it is satisfied by this polynomial. Notice that Γ_0 acts on polynomials in the X_γ's by permutation of the indeterminates.

Lemma 3.2. *Each $\sigma_{k,i}$, $1 \leqslant i \leqslant r$ and $1 \leqslant k \leqslant 3$, is formally invariant under the action of Γ_0.*

Since $\sigma_{k,i}$ lies in N_0, this is of course stronger than stating that $\sigma_{k,i}$ is invariant under Γ_0. It means for instance that the polynomial $\sum_{\gamma\in\Gamma_0} X_\gamma$, whose evaluation at the $\gamma(\beta)$'s is $\beta_0 = \mathrm{Tr}_{K_i/N_0}(\beta_i) = \sigma_{1,i}$ for any i, is invariant under the action of Γ_0. In other words, each $\sigma_{k,i}$ is a symmetric function of the conjugates of β over N_0 with respect to the action of Γ_0.

Proof. By definition, $\sigma_{k,i}$ is a symmetric function of the conjugates of β_i with respect to the action of $\langle\delta_i\rangle$; further $\beta_i = \mathrm{Tr}_{N_3/K_i}(\beta)$ is formally invariant under the action of $\ker(\chi_i)$, as are its conjugates under $\langle\delta_i\rangle$, so the same holds for $\sigma_{k,i}$, and the result follows since $\Gamma_0 = \ker(\chi_i)\times\langle\delta_i\rangle$. □

We denote by σ_2 the second elementary symmetric function of the conjugates of β over N_0.

Lemma 3.3. $9\sum_{i=1}^{r}\sigma_{2,i} = 3^{m+1}\sigma_2$ *belongs to* $3^{m+1}\mathcal{O}_{N_0}$.

Proof. By definition,

$$\sigma_{2,i} = \beta_i\delta_i(\beta_i) + \delta_i(\beta_i)\delta_i^2(\beta_i) + \delta_i^2(\beta_i)\beta_i \ ,$$

so a product $\beta\delta(\beta)$ with $\delta \in \Gamma_0\setminus\{1\}$ may formally appear in $\sigma_{2,i}$ only in the first or in the third product, that is, in

$$\beta_i(\delta_i(\beta_i) + \delta_i^2(\beta_i)) = \Big(\sum_{\gamma\in\ker(\chi_i)}\gamma(\beta)\Big)\Big(\sum_{\gamma'\in\ker(\chi_i)}\Big(\delta_i\gamma'(\beta) + \delta_i^2\gamma'(\beta)\Big)\Big) \ ,$$

and we see that $\beta\delta(\beta)$ formally appears in $\sigma_{2,i}$ if and only if $\delta \notin \ker(\chi_i)$. We deduce from Lemma 2.3 that

$$\#\{i \in \{1,\dots,r\} \,|\, \delta \notin \ker(\chi_i)\} = 3^{m-1} \ ,$$

so for each $\delta \in \Gamma_0 \setminus \{1\}$, the product $\beta\delta(\beta)$ formally appears 3^{m-1} times in $\sum_{i=1}^{r}\sigma_{2,i}$. Thanks to Lemma 3.2, the same happens for its conjugates under Γ_0. It is easy to check that all these conjugates are

formally different, that $\beta\delta(\beta)$ and $\beta\delta^2(\beta)$ give rise to the same set of conjugates and that no other formal coincidence occurs. Hence there are $3^m\frac{3^m-1}{2}$ formally different products $\gamma_1(\beta)\gamma_2(\beta)$ occurring 3^{m-1} times each in $\sum_{i=1}^r \sigma_{2,i}$; but σ_2 is precisely the sum of these $\binom{3^m}{2}$ products, so the equality of the Lemma holds. It remains to write $\sigma_2 = \frac{1}{2}\mathrm{Tr}_{N_3/N_0}(\sum_{\gamma\in\Gamma_0\setminus\{1\}}\beta\gamma(\beta))$ and to notice that $\beta\gamma(\beta)\in\mathcal{A}_{N_3}^2 = \mathcal{D}_{N_3}^{-1}$ to get $\sigma_2\in\mathcal{O}_{N_0}$, hence the result. □

LEMMA 3.4. *$27\sum_{i=1}^r\sigma_{3,i}$ belongs to $3^m\mathcal{O}_{N_0}$.*

Proof. We follow the same path as in the former proof:

$$\sigma_{3,i} = \Big(\sum_{\gamma_1\in\ker(\chi_i)}\gamma_1(\beta)\Big)\Big(\sum_{\gamma_2\in\ker(\chi_i)}\delta_i\gamma_2(\beta)\Big)\Big(\sum_{\gamma_3\in\ker(\chi_i)}\delta_i^2\gamma_3(\beta)\Big)\ ,$$

so a product $\beta\delta(\beta)\delta'(\beta)$, with $\delta,\delta'\in\Gamma_0$ and $\#\{1,\delta,\delta'\}=3$, formally appears in $\sigma_{3,i}$ if and only if $\Gamma_0 = \ker(\chi_i)\amalg\delta\ker(\chi_i)\amalg\delta'\ker(\chi_i)$, which is also equivalent to

$$\delta\notin\ker(\chi_i),\quad \delta\delta'\in\ker(\chi_i)\ .$$

We now have to consider two cases:

• if $\delta'=\delta^2$, the two conditions above amount to $\delta\notin\ker(\chi_i)$, which happens for 3^{m-1} values of i, so $\beta\delta(\beta)\delta^2(\beta)$ formally appears 3^{m-1} times in $\sum_i\sigma_{3,i}$;

• if $\delta'\neq\delta^2$, that is, $\delta'\notin\langle\delta\rangle$, there are 3^{m-1} characters χ of Γ_0 such that $\delta\delta'\in\ker(\chi)$, among which 3^{m-2} are such that δ belongs to $\ker(\chi)$ (indeed $\delta\delta'\notin\langle\delta\rangle$, so Lemma 2.3(ii) applies). This gives $3^{m-1}-3^{m-2}=2\times3^{m-2}$ characters of Γ_0 whose kernels contain $\delta\delta'$ but not δ, hence there are 3^{m-2} values of i such that $\beta\delta(\beta)\delta'(\beta)$ formally appears in $\sigma_{3,i}$ (recall χ_i and χ_i^2 share the same kernel). We infer that $\beta\delta(\beta)\delta'(\beta)$ formally appears 3^{m-2} times in $\sum_i\sigma_{3,i}$.

By Lemma 3.2, each $\beta\delta(\beta)\delta^2(\beta)$ ($\delta\neq1$) formally appears with its 3^{m-1} formally distinct conjugates under Γ_0 (this product is fixed under $\langle\delta\rangle$), so that the sum of these conjugates equals one third of the trace of $\beta\delta(\beta)\delta^2(\beta)$, whereas a product $\beta\delta(\beta)\delta'(\beta)$ satisfying the previous conditions has 3^m formally distinct conjugates under Γ_0. This implies

$$\sum_{i=1}^r\sigma_{3,i} = \frac{3^{m-1}}{3}\mathrm{Tr}_{N_3/N_0}\Big(\frac{1}{2}\sum_{\delta\neq1}\beta\delta(\beta)\delta^2(\beta)\Big) + 3^{m-2}\mathrm{Tr}_{N_3/N_0}\Big(\frac{1}{2}\sum_{\delta,\delta'}\beta\delta(\beta)\delta'(\beta)\Big)\ ,$$

where the last sum runs over the $\delta\in\Gamma_0\setminus\{1\}$ and $\delta'\in\Gamma_0\setminus\langle\delta\rangle$, and the $\frac{1}{2}$'s correspond to the fact that each given product formally appears twice in the sums. We eventually get

$$27\sum_{i=1}^r\sigma_{3,i}\ \in\ 3^{m+1}\mathrm{Tr}_{N_3/N_0}(\mathcal{A}_{N_3/N_0}^3) = 3^{m+1}\times\frac{1}{3}\mathcal{O}_{N_0} = 3^m\mathcal{O}_{N_0}\ .$$

□

Notice that, unlike $\sum_i\sigma_{2,i}$, $\sum_i\sigma_{3,i}$ is not a symmetric function of the conjugates of β over N_0 with respect to the whole permutation group $\mathfrak{S}_{3^m}$ of these conjugates, since the products of the first kind formally appear three times more often in $\sum_i\sigma_{3,i}$ than those of the second kind.

Lemmas 3.3 and 3.4 together with Formula (5) yield

$$S(1)\in3^m\mathcal{O}_{N_0}\ . \tag{6}$$

Before dealing with $S(\gamma)$ in the case $\gamma\neq1$, we have the following interlude.

3.2 The square root of the discriminant of $\mathcal{A}_{K_i/N_0}$

Let $i \in \{1,\dots,r\}$ and δ_i as above; the set $\{\beta_i, \delta_i(\beta_i), \delta_i^2(\beta_i)\}$ is a basis of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}$, so the discriminant of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}$ is the principal fractional ideal generated by

$$(\beta_i - \delta_i(\beta_i))^2(\delta_i(\beta_i) - \delta_i^2(\beta_i))^2(\delta_i^2(\beta_i) - \beta_i)^2 \ .$$

We define R_i to be the following square root of this generator:

$$R_i = (\beta_i - \delta_i(\beta_i))(\delta_i(\beta_i) - \delta_i^2(\beta_i))(\delta_i^2(\beta_i) - \beta_i) \ ;$$

then $R_i \in N_0$, since R_i is in K_i, $R_i^2 \in N_0$ and $[K_i : N_0]$ is odd. Of course R_i is not formally invariant under the action of the whole permutation group $\mathfrak{S}_{3^m}$. Yet one has:

Lemma 3.5. *R_i is formally invariant under the action of Γ_0 and*

$$R_i = \mathrm{Tr}_{K_i/N_0}\Big(\beta_i^2(\delta_i^2(\beta_i) - \delta_i(\beta_i))\Big) = \mathrm{Tr}_{N_3/N_0}\Big(\beta \sum_{(\gamma_1,\gamma_2)} \gamma_1(\beta)\gamma_2(\delta_i^2(\beta) - \delta_i(\beta))\Big) \ ,$$

where the sum runs over $\ker(\chi_i) \times \ker(\chi_i)$.

Proof. The first equality is straightforward, it proves the assertion and yields the second one immediatly. □

In fact, the formal invariance property of R_i will not be needed, since we shall make use of the second trace formula instead. We are now ready to finish the proof of Theorem 3.1.

3.3 Computation of $S(\gamma)$ for $\gamma \neq 1$

We fix $\gamma \in \Gamma_0$ with $\gamma \neq 1$ and we define the partition $I_\gamma \amalg J_\gamma$ of $\{1,\dots,r\}$ by

$$I_\gamma = \{1 \leqslant i \leqslant r \,|\, \gamma \notin \ker(\chi_i)\} \ , \quad J_\gamma = \{1 \leqslant j \leqslant r \,|\, \gamma \in \ker(\chi_j)\} \ .$$

One easily deduces from Lemma 2.3 that $\#I_\gamma = 3^{m-1}$ and $\#J_\gamma = \frac{3^{m-1}-1}{2}$. For each $i \in I_\gamma$, we ensure $\chi_i(\gamma) = \zeta$ (the primitive 3rd root of unity introduced at the beginning of this section), replacing χ_i by its square if necessary, and we choose $\delta_i \in \Gamma_0 \setminus \ker(\chi_i)$ such that $\chi_i(\delta_i) = \zeta$. We wish to compute (4):

$$S(\gamma) = \beta_0^3 + \sum_{i=1}^{r} T_i(\gamma) \ ,$$

where $T_i(\gamma) = \chi_i(\gamma^{-1})(\beta_i \,|\, \chi_i)^3 + \chi_i^2(\gamma^{-1})(\beta_i \,|\, \chi_i^2)^3$. For $j \in J_\gamma$, we know from Subsection 3.1 that

$$T_j(\gamma) = T_j(1) = 2\beta_0^3 - 9\beta_0\sigma_{2,j} + 27\sigma_{3,j} \ .$$

We compute $T_i(\gamma)$ for $i \in I_\gamma$:

$$\begin{aligned} T_i(\gamma) &= \zeta^2(\beta_i \,|\, \chi_i)^3 + \zeta(\beta_i \,|\, \chi_i^2)^3 \\ &= \zeta^2(\beta_i + \zeta^2\delta_i(\beta_i) + \zeta\delta_i^2(\beta_i))^3 + \zeta(\beta_i + \zeta\delta_i(\beta_i) + \zeta^2\delta_i^2(\beta_i))^3 \\ &= -\tau_{3,i} - 6\sigma_{3,i} + 3\mathrm{Tr}_{K_i/N_0}\Big(\beta_i^2(2\delta_i^2(\beta_i) - \delta_i(\beta_i))\Big) \\ &= -\beta_0^3 + 3\beta_0\sigma_{2,i} - 9\sigma_{3,i} + 3\mathrm{Tr}_{K_i/N_0}\Big(\beta_i^2(2\delta_i^2(\beta_i) - \delta_i(\beta_i))\Big) \ , \end{aligned}$$

whereas $T_i(\gamma^2) = -\beta_0^3 + 3\beta_0\sigma_{2,i} - 9\sigma_{3,i} + 3\mathrm{Tr}_{K_i/N_0}(\beta_i^2(2\delta_i(\beta_i) - \delta_i^2(\beta_i)))$, so that

$$T_i(\gamma) - T_i(\gamma^2) = 9R_i \ ,$$

where R_i is the square root of the discriminant of $\mathcal{A}_{K_i/N_0}$ introduced in the previous subsection. On the other hand, $T_i(1)+T_i(\gamma)+T_i(\gamma^2)=0$, so $T_i(\gamma)+T_i(\gamma^2)=-2\beta_0^3+9\beta_0\sigma_{2,i}-27\sigma_{3,i}$ and we get

$$T_i(\gamma)=-\beta_0^3+\frac{9}{2}\beta_0\sigma_{2,i}-\frac{27}{2}\sigma_{3,i}+\frac{9}{2}R_i\ ,$$

which yields

$$S(\gamma)=\frac{9}{2}\beta_0\sum_{i=1}^{r}\sigma_{2,i}-\frac{27}{2}\sum_{i=1}^{r}\sigma_{3,i}-\frac{27}{2}\beta_0\sum_{j\in J_\gamma}\sigma_{2,j}+\frac{81}{2}\sum_{j\in J_\gamma}\sigma_{3,j}+\frac{9}{2}\sum_{i\in I_\gamma}R_i\ .$$

The first two terms have already been dealt with in Lemmas 3.3 and 3.4, whose proofs we may now adjust in order to deal with the third and fourth terms.

Lemma 3.6. *$-\frac{27}{2}\beta_0\sum_{J_\gamma}\sigma_{2,j}$ belongs to $3^{m+1}\mathcal{O}_{N_0}$.*

Proof. Recall from the proof of Lemma 3.3 that a product $\beta\delta(\beta)$ formally appears in $\sigma_{2,j}$ if and only if $\delta\notin\ker(\chi_j)$. This implies that the products $\beta\gamma(\beta)$ and $\beta\gamma^2(\beta)$ do not formally appear in $\sum_{J_\gamma}\sigma_{2,j}$, and that any product $\beta\delta(\beta)$ with $\delta\in\Gamma_0\setminus\langle\gamma\rangle$ formally appears in $\sigma_{2,j}$ for some $j\in J_\gamma$, since $\langle\gamma\rangle=\bigcap_{J_\gamma}\ker(\chi_j)$.

Let $\delta\in\Gamma_0\setminus\langle\gamma\rangle$. Then $\delta\in\ker(\chi_j)$ with $j\in J_\gamma$ if and only if $\chi_j\in\ker(\widehat{\delta})\cap\ker(\widehat{\gamma})$, where $\widehat{\delta}$ denotes the linear form $\widehat{\Gamma}_0\to\mu_3$, $\chi\mapsto\chi(\delta)$ (see Subsection 2.2). This intersection of two distinct hyperplanes of $\widehat{\Gamma}_0$ is of codimension 2 and of cardinality 3^{m-2}, so δ happens to be in $\ker(\chi_j)$ for $\frac{3^{m-2}-1}{2}$ values of $j\in J_\gamma$. Hence $\delta\notin\ker(\chi_j)$ is true for $\frac{3^{m-1}-1}{2}-\frac{3^{m-2}-1}{2}=3^{m-2}$ values of $j\in J_\gamma$ and $\beta\delta(\beta)$ formally appears 3^{m-2} times in $\sum_{J_\gamma}\sigma_{2,j}$, together with its distinct conjugates under Γ_0 by Lemma 3.2. All of them being formally different but generated by both products $\beta\delta(\beta)$ and $\beta\delta^2(\beta)$, we get

$$\sum_{j\in J_\gamma}\sigma_{2,j}=3^{m-2}\mathrm{Tr}_{N_3/N_0}\Big(\frac{1}{2}\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\Big)\ \in\ 3^{m-2}\mathcal{O}_{N_0}\ ,$$

which gives the result. □

Lemma 3.7. *$\frac{81}{2}\sum_{J_\gamma}\sigma_{3,j}$ belongs to $3^m\mathcal{O}_{N_0}$.*

Proof. We deduce from the proof of Lemma 3.4 that a product $\beta\delta(\beta)\delta'(\beta)$ with $\#\{1,\delta,\delta'\}=3$ formally appears in $\sigma_{3,j}$ with $j\in J_\gamma$ if and only if

$$\delta\notin\ker(\chi_j)\ ,\quad \delta\delta'\in\ker(\chi_j)\quad\text{and}\ \ \gamma\in\ker(\chi_j)\ .$$

These conditions imply as before that δ and δ' do not belong to $\langle\gamma\rangle$, but also that $\delta'\notin\delta\langle\gamma\rangle$ (otherwise $\delta\delta'\in\ker(\chi_j)$ would never be possible for $j\in J_\gamma$).

We now fix δ and δ' in Γ_0 such that $\delta\notin\langle\gamma\rangle$ and $\delta'\notin\langle\gamma\rangle\amalg\delta\langle\gamma\rangle$. Observe first that $\delta\notin\langle\gamma,\delta\delta'\rangle$, because otherwise $\delta\delta'$ would belong to $\delta\langle\gamma\rangle\amalg\delta^2\langle\gamma\rangle$, which contradicts our hypothesis. We have to consider two cases:

• if $\delta'\in\delta^2\langle\gamma\rangle$, the three preceding conditions amount to $\gamma\in\ker(\chi_j)$ and $\delta\notin\ker(\chi_j)$, so each of the three terms: $\beta\delta(\beta)\delta^2(\beta)$, $\beta\delta(\beta)\delta^2\gamma(\beta)$ and $\beta\delta(\beta)\delta^2\gamma^2(\beta)$, formally appears in $\sigma_{3,j}$ for 3^{m-2} values of j in J_γ;

• if $\delta'\notin\delta^2\langle\gamma\rangle$, then $\delta\delta'\notin\langle\gamma\rangle$. If $m=2$, this yields $\Gamma_0=\langle\gamma,\delta\delta'\rangle$, which contradicts $\delta\notin\langle\gamma,\delta\delta'\rangle$, so that no such product occurs in $\sum_{J_\gamma}\sigma_{3,j}$. If $m\geqslant 3$, the two conditions: $\gamma\in\ker(\chi)$ and $\delta\delta'\in\ker(\chi)$, define a codimension 2 subspace of $\widehat{\Gamma}_0$, in which the additional condition $\delta\in\ker(\chi)$ defines a hyperplane, since $\delta\notin\langle\gamma,\delta\delta'\rangle$. Thus there are $2\times 3^{m-3}$ characters χ of Γ_0 such that $\gamma\in\ker(\chi)$,

$\delta\delta' \in \ker(\chi)$ and $\delta \notin \ker(\chi)$, and our product $\beta\delta(\beta)\delta'(\beta)$ formally appears in $\sigma_{3,j}$ for 3^{m-3} values of $j \in J_\gamma$.

Using Lemma 3.2 we obtain

$$\begin{aligned}\textstyle\sum_{J_\gamma} \sigma_{3,j} \;&=\; 3^{m-3}\mathrm{Tr}_{N_3/N_0}\Big(\tfrac{1}{2}\textstyle\sum_{\delta\notin\langle\gamma\rangle} \beta\delta(\beta)\delta^2(\beta)\Big)\\ &+\; 3^{m-2}\mathrm{Tr}_{N_3/N_0}\Big(\tfrac{1}{2}\textstyle\sum_{\delta\notin\langle\gamma\rangle} (\beta\delta(\beta)\delta^2\gamma(\beta)+\beta\delta(\beta)\delta^2\gamma^2(\beta))\Big)\\ &+\; 3^{m-3}\mathrm{Tr}_{N_3/N_0}\Big(\tfrac{1}{2}\textstyle\sum_{\delta\notin\langle\gamma\rangle} \beta\delta(\beta)\sum_{\delta'\notin\langle\gamma,\delta\rangle}\delta'(\beta)\Big)\;,\end{aligned}$$

(the last term vanishes if $m = 2$) and we conclude as in the proof of Lemma 3.4, taking advantage of the fact that the gain in the valuation of $81 = 3 \times 27$ balances the loss in the valuation of $3^{m-3} = \frac{1}{3} \times 3^{m-2}$. □

Lemma 3.8. *$\frac{9}{2}\sum_{I_\gamma} R_i$ belongs to $3^m\mathcal{O}_{N_0}$.*

Proof. We start with the second expression of R_i given in Lemma 3.5, and we note that the only constraint on δ_i for $i \in I_\gamma$ is that $\chi_i(\delta_i) = \zeta$, so we may choose $\delta_i = \gamma$ for any $i \in I_\gamma$. We get

$$R_i = \mathrm{Tr}_{N_3/N_0}\Big(\sum_{\gamma_1,\gamma_2} \beta\gamma_1(\beta)\gamma_2(\beta'))\Big)\;,$$

where γ_1 and γ_2 both run through $\ker(\chi_i)$ and $\beta' = \gamma^2(\beta)-\gamma(\beta)$. We have the following decomposition of the sum inside brackets:

$$\beta^2\beta' + \beta^2\sum_{\gamma_2\neq 1}\gamma_2(\beta') + \beta\sum_{\gamma_1\neq 1}\gamma_1(\beta)(\beta'+\gamma_1(\beta')+\gamma_1^2(\beta')) + \beta\sum_{\gamma_1\neq 1}\gamma_1(\beta)\sum_{\gamma_2\notin\langle\gamma_1\rangle}\gamma_2(\beta')\;.$$

Clearly $\beta^2\beta'$ formally appears in each R_i, so its trace comes with a factor 3^{m-1} in $\sum_{I_\gamma} R_i$. The products involving only one parameter $\delta \in \Gamma_0 \setminus \{1\}$, that is, $\beta^2\delta(\beta')$, $\beta\delta(\beta)\beta'$, $\beta\delta(\beta)\delta(\beta')$ and $\beta\delta(\beta)\delta^2(\beta')$, formally appear in R_i if and only if $\delta \in \ker(\chi_i)$, so δ may be any element of $\Gamma_0 \setminus \langle\gamma\rangle$. If this is the case, each of the former products formally appears in R_i for 3^{m-2} values of $i \in I_\gamma$ (there are 3^{m-1} characters χ of Γ_0 such that $\delta \in \ker(\chi)$, among which $2 \times 3^{m-2}$ are not trivial on γ), and their traces come with a factor 3^{m-2} in $\sum_{I_\gamma} R_i$.

The last term contains products of the shape $\beta\delta(\beta)\delta'(\beta')$ with $\delta \in \Gamma_0\setminus\{1\}$ and $\delta' \in \Gamma_0\setminus\langle\delta\rangle$. Clearly, δ and δ' cannot lie in $\langle\gamma\rangle$. Further γ cannot belong to $\langle\delta,\delta'\rangle$, in other words $\delta' \notin \langle\delta,\gamma\rangle$. Consequently, this term vanishes when $m = 2$. Suppose $m \geqslant 3$, $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$ and $\delta' \in \Gamma_0 \setminus \langle\delta,\gamma\rangle$. The characters χ of Γ_0 such that $\chi(\delta) = \chi(\delta') = 1$ form a codimension 2 subspace of $\widehat{\Gamma}_0$, in which the additional condition $\chi(\gamma) = 1$ defines a hyperplane; thus there are 3^{m-3} values of $i \in I_\gamma$ such that $\beta\delta(\beta)\delta'(\beta')$ formally appears in R_i, and its trace comes with a factor 3^{m-3} in $\sum_{I_\gamma} R_i$.

Eventually we get

$$\begin{aligned}\textstyle\sum_{I_\gamma} R_i \;&=\; 3^{m-1}\mathrm{Tr}_{N_3/N_0}(\beta^2\beta')\\ &+\; 3^{m-2}\mathrm{Tr}_{N_3/N_0}\Big(\beta^2\textstyle\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta')\Big)\\ &+\; 3^{m-2}\mathrm{Tr}_{N_3/N_0}\Big(\beta\textstyle\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)(\beta'+\delta(\beta')+\delta^2(\beta'))\Big)\\ &+\; 3^{m-3}\mathrm{Tr}_{N_3/N_0}\Big(\textstyle\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\sum_{\delta'\notin\langle\delta,\gamma\rangle}\delta'(\beta')\Big)\;,\end{aligned}$$

keeping in mind that the last term vanishes when $m = 2$. In fact, it also vanishes if $m \geqslant 3$: fix $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$; then

$$\sum_{\delta'\notin\langle\delta,\gamma\rangle}\delta'(\beta') = \sum_{\delta'\notin\langle\delta,\gamma\rangle}\delta'\gamma^2(\beta) - \sum_{\delta'\notin\langle\delta,\gamma\rangle}\delta'\gamma(\beta) = 0$$

since $\gamma^2\langle\delta,\gamma\rangle = \langle\delta,\gamma\rangle = \gamma\langle\delta,\gamma\rangle$. Let us now have a look at the other sums involved:

$$\beta^2 \sum_{\delta\notin\langle\gamma\rangle} \delta(\beta') = \beta^2\Big(\sum_{\delta\notin\langle\gamma\rangle} \delta\gamma^2(\beta) - \sum_{\delta\notin\langle\gamma\rangle} \delta\gamma(\beta)\Big) = 0 \ ,$$

$$\begin{aligned}\beta \sum_{\delta\notin\langle\gamma\rangle} \delta(\beta)\beta' &= \beta\beta_0\beta' - \beta(\beta+\gamma(\beta)+\gamma^2(\beta))\beta' \\ &= \beta_0\beta\beta' - (\beta^2\gamma^2(\beta)+\beta\gamma^2(\beta^2)) + \gamma(\beta^2\gamma^2(\beta)+\beta\gamma^2(\beta^2)) \ ,\end{aligned}$$

so that $\mathrm{Tr}_{N_3/N_0}\Big(\beta\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)\beta'\Big) = \beta_0\mathrm{Tr}_{N_3/N_0}(\beta\beta')$; and

$$\beta \sum_{\delta\notin\langle\gamma\rangle} \delta(\beta)\delta(\beta') = \beta\Big(\sum_{\delta\notin\langle\gamma\rangle} \delta(\beta)\delta\gamma^2(\beta) - \sum_{\delta\notin\langle\gamma\rangle} \delta(\beta)\delta\gamma(\beta)\Big) = 0 \ .$$

In order to study the only remaining sum $\beta\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)\delta^2(\beta')$, we introduce the binary relation $\overset{\gamma}{\sim}$ on $\Gamma_0\setminus\langle\gamma\rangle$, defined by

$$\delta \overset{\gamma}{\sim} \delta' \ \text{ if } \ \delta' \in \langle\delta,\gamma\rangle\setminus\langle\gamma\rangle \ .$$

It is easily verified that $\overset{\gamma}{\sim}$ is an equivalence relation, and that each class of $\Gamma_0\setminus\langle\gamma\rangle$ under $\overset{\gamma}{\sim}$ contains 6 elements. Further, one checks that $\beta\delta(\beta)\delta'^2\gamma^2(\beta)$ and $\beta\delta(\beta)\delta^2\gamma^2(\beta)$ (respectively $\beta\delta(\beta)\delta'^2\gamma(\beta)$ and $\beta\delta(\beta)\delta^2\gamma(\beta)$) are conjugate if $\delta\overset{\gamma}{\sim}\delta'$, hence

$$\mathrm{Tr}_{N_3/N_0}\Big(\beta\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)\delta^2(\beta')\Big) = 6\mathrm{Tr}_{N_3/N_0}\Big(\beta\sum_{\delta\in\Gamma_\gamma}\delta(\beta)\delta^2(\beta')\Big) \ ,$$

where Γ_γ denotes a set of coset representatives of $\overset{\gamma}{\sim}$ in $\Gamma_0\setminus\langle\gamma\rangle$.

Collecting the results yields

$$\sum_{I_\gamma} R_i = 3^{m-1}\mathrm{Tr}_{N_3/N_0}(\beta^2\beta') + 3^{m-2}\beta_0\mathrm{Tr}_{N_3/N_0}(\beta\beta') + 2\times 3^{m-1}\mathrm{Tr}_{N_3/N_0}\Big(\beta\sum_{\delta\in\Gamma_\gamma}\delta(\beta)\delta^2(\beta')\Big) \ ,$$

which clearly belongs to $3^{m-2}\mathcal{O}_{N_0}$. □

Putting everything together with (6), we obtain

$$\forall\gamma\in\Gamma_0,\ S(\gamma)\in 3^m\mathcal{O}_{N_0} \ ,$$

which is Theorem 3.1 and implies Theorem 1.

Remark. One may compute $\sum_{I_\gamma}\sigma_{k,i}$ for $k\in\{2,3\}$ in order to check the coherence of the results for the analogous sums over J_γ with the expressions of $\sum_{i=1}^r\sigma_{k,i}$ given in subsection 3.1. These computations turn out to be more complicated than the ones presented above.

Aknowledgments. The author wishes to thank the Copy Editor for his valuable advice on the use of the English language, and Prof. Cougnard for his careful reading of the manuscript.

References

B Byott N.P., Integral Galois module structure of some Lubin-Tate extensions, *J. Number Theory*, **77** (1999), *no. 2*, 252–273.

CNT Cassou-Noguès Ph., Taylor M.J., Galois module structure for wild extensions, in *Algebraic number theory and diophantine analysis, Proc. Conf. Graz 1998*, ed. Halter-Koch F. and Tichy R.F., de Gruyter, New York (2000), 69–91.

E Erez B., The Galois structure of the square root of the inverse different, *Math. Z.*, **208** (1991), 239–255.

F Fröhlich A., *Galois module structure of algebraic integers*, Ergebnisse der Mathematik, 3. Folge, Bd. 1, Springer, Berlin (1983).

S1 Serre J.P., *Corps locaux*, 3^{e}édition, Hermann, Paris (1968).

S2 Serre J.P., *Représentations linéaires des groupes finis*, 3^{e}édition, Hermann, Paris (1978).

T Taylor M.J., On Fröhlich's conjecture for rings of integers of tame extensions, *Invent. Math.*, **63** (1981), 41–79.

vW van der Waerden B. L., *Algebra, Vol. I*, Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger, Springer-Verlag, New York (1991).

U Ullom S., Integral normal bases in Galois extensions of local fields, *Nagoya Math. J.* **39** (1970), 141–148.

V1 Vinatier S., Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$, *J. Number Theory*, **91** (2001), *no. 1*, 126–152.

V2 Vinatier S., Une famille infinie d'extensions faiblement ramifiées, *Math. Nachr.*, **243** (2002), 165–187.

V3 Vinatier S., Sur la racine carrée de la codifférente, Actes des J.A. Lille 2001, *J. Théor. Nombres Bordeaux*, **15** (2003), *no. 1*, 393–410.

Stéphane Vinatier
LACO – Université de Limoges, 123 avenue Albert Thomas, F-87060 Limoges cedex

Chapitre 3

Constructions d'extensions explicites

Dans ce chapitre nous présentons le travail en commun avec Bill Allombert, qui a donné lieu à un article intitulé *Ramification in a family of $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extensions of the rationals* et actuellement soumis pour publication dans une revue internationale avec comité de lecture. La version soumise est légèrement plus courte que celle qui est présentée ci-dessous, les considérations concernant les groupes de classes des extensions de la famille en ont été retirées pour être développées dans un autre article (en projet). Je les ai réintégrées ici, en attendant que la suite voit le jour, car elles me semblent rajouter de l'intérêt à la construction et à l'étude qui les précèdent.

Les produits semi-directs $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$ sont les plus petits p-groupes non abéliens, pour p premier impair. Ils sont d'ordre 27 tandis que les « suivants » sont d'ordre $5^3 = 125$. Si l'on veut mener des calculs numériques un peu poussés sur des p-extensions galoisiennes non abéliennes, pour p premier impair, on n'a donc guère le choix pour le groupe de Galois qu'entre les deux présentés ci-dessus. Dans ce travail, nous construisons des extensions de $\mathbb{Q}$ de groupe de Galois isomorphe à $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$, par une méthode très élégante et efficace.

L'étude de la ramification des extensions obtenues est assez proche de celle menée dans un travail précédent sur le même type d'extensions ([Vin02]). Notons toutefois que l'aspect plus explicite de la nouvelle construction permet d'éviter les calculs fastidieux de congruences qui permettaient, grâce à des résultats de Greither sur les extensions kummériennes de degré une puissance de premier ([Gre89]), de déterminer l'indice de ramification dans celle utilisée alors (qui provenait de la thèse d'Yves Eichenlaub [Eic96] et avait l'avantage d'être bien plus générale). Nous poussons l'étude jusqu'à la détermination des groupes de ramification en 3, ce qui a incité mon co-auteur à développer un algorithme de calcul de ces groupes, maintenant implémenté dans le logiciel d'arithmétique PARI/GP.

Voilà où nous en étions lorsque j'ai présenté notre travail au séminaire de théorie des nombres de Caen en janvier 2009. Après l'exposé, Bruno Anglès a posé une question sur le groupe de classes de ces extensions, que nous n'avions pas encore calculé. Denis Simon a presque aussitôt lancé quelques calculs sur ordinateur. Il s'est avéré que cette famille d'extensions se prêtait bien à ce genre d'expérimentations et certaines propriétés ont semblé se dessiner. Des calculs plus poussés menés par mon co-auteur ont permis de faire un tri assez sévère entre celles-ci. Les résultats sont présentés dans des tables à la fin de l'article ci-dessous, avec la seule conjecture qui a survécu aux tests. L'article est demeuré quelque temps ainsi, en attendant que nous nous décidions à le soumettre. Dans l'intervalle, Franz Lemmermeyer est tombé dessus par un moyen que j'ignore (peut-être en passant par une de nos pages web, il était

du moins accessible par la mienne) et a proposé, dans un `email` à Bill, une esquisse de preuve de notre conjecture. Celle-ci stipule que deux congruences entraînent, indépendamment l'une de l'autre, que le nombre de classes est divisible par 3. Lemmermeyer remarque que dans le cas de la première congruence, la conjecture découle directement du lemme d'Abhyankar ; pour la seconde, il suppose de plus une propriété que nous n'avons pas réussi à démontrer (mais qui est étayée par des calculs numériques poussés). Il reste donc encore une part de mystère dans ce travail…

J'ai laissé cette partie de l'article dans l'état antérieur à cette contribution bienvenue, dans la mesure où Bill et moi avons décidé de repousser la rédaction des propriétés relatives au groupe des classes à un prochain article, qui devrait de plus voir les deux groupes non abéliens d'ordre 27 présentés ci-dessus apparaître comme groupes de classes d'extensions de $\mathbb{Q}$ (cependant nos discussions concernant cette partie n'ont pas encore été rédigées proprement).

Ramification in a family of $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extensions of the rationals

Bill Allombert and Stéphane Vinatier

Abstract

We construct for each prime number $p \equiv 1 \pmod 3$, a $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extension of the rationals that is ramified exactly at 3 and p, and we describe the discriminant and the ramification groups as functions of p.

1. Introduction

In this paper we present a simple and explicit way to construct an infinite family of Galois extensions of the rationals, of Galois group isomorphic to the non abelian group of order 27 and exponent 9, namely the semi-direct product $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. These extensions are parametrized by the prime numbers p congruent to 1 modulo 3. They are only ramified at two places, 3 and the parametrizing prime p. It follows from [P3, Proposition 2.5] that this is the minimal number of ramified places for Galois extensions with this Galois group. Our extensions can be described as the splitting field of a surprisingly simple degree 9 polynomial depending on p only in its constant coefficient.

The simplicity of our construction enables us to achieve the complete study of the ramification above 3. Its decomposition as a product of prime ideals takes five different patterns, depending on the integers a and b such that $p = a^2 + 3b^2$. We explicit a uniformizing parameter and the sequence of ramification groups in every case. In particular we find that the extension is weakly ramified (*i.e.* with trivial second ramification groups) in some of the cases, which yields a family of weakly ramified extensions with Galois group isomorphic to $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ that is different from that studied in [V].

Computations performed with PARI/GP[P1] for a number of elements of this family are presented in the last section of this paper, as well as a brief outline of the algorithm we designed to compute ramification groups. The results have been checked to be in agreement with the theory.

Such extensions have already been constructed by several authors, by several means, and in several contexts. In particular a construction for any prime number p of generic Galois extensions of $\mathbb{Q}$ of Galois group $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ can be found in [L1], with an application to the $p = 3$ case. Our construction is far less general, but has revealed extremely easy to handle for the study of the ramification, which was our main goal.

Furthermore, we present partial theoretical results and numerical computations about the 3-part of the class group of these extensions (and some of their subextensions).

2000 Mathematics Subject Classification 11R20, 11S15, 11Y40 (primary), 11R32, 12F10, 12F12 (secondary).
Keywords: Metabelian extensions, Discriminant, Ramification groups

2. Construction of $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$-extensions

We let ζ_9 denote a primitive 9-th root of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and we set $\zeta_3 = {\zeta_9}^3$ and $\sqrt{-3} = 2\zeta_3 + 1$.

If L/K is an extension of number fields, we denote by $\mathcal{N}_{L/K}$ the norm, by $\mathcal{D}_{L/K}$ the different ideal and by $\mathrm{d}_{L/K}$ the relative discriminant ideal. We also denote by $\mathcal{O}_K$ the ring of integers of K and by d_K its absolute discriminant. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ of uniformizing parameter π, we denote by $K_\mathfrak{p}$ or K_π the completion of K for the $\mathfrak{p}$–adic topology, and by v_π the $\mathfrak{p}$–adic valuation in $K_\mathfrak{p}$.

Let p be a prime number so that $p \equiv 1 \pmod 3$, then by a theorem of Fermat there exist two integers a and b, unique up to sign, such that

$$p = a^2 + 3b^2 \ .$$

We chose the sign of a so that $a \equiv 1 \pmod 3$ and we denote by a' the integer such that $a = 1 + 3a'$. If $b \not\equiv 0 \pmod 3$, we chose the sign of b so that $b \equiv 1 \pmod 3$ and we denote by b' the integer such that $b = 1 + 3b'$; otherwise, we set $b = 3b'$ and if $b' \not\equiv 0 \pmod 3$ we chose the sign of b so that $b' \equiv -1 \pmod 3$. We set $\alpha = a + b\sqrt{-3}$ and

$$\beta = \frac{a + b\sqrt{-3}}{a - b\sqrt{-3}} \ ,$$

so α and β belong to the field $\mathbb{Q}(\zeta_3)$.

We construct the fields

$$M = \mathbb{Q}(\sqrt[9]{\beta}) \quad \text{and} \quad L = \mathbb{Q}(\zeta_9, \sqrt[9]{\beta})$$

where $\sqrt[9]{\beta}$ denotes a fixed 9-th root of β in $\overline{\mathbb{Q}}$. Note that $\beta = \frac{a^2 - 3b^2 + 2ab\sqrt{-3}}{p}$, so $\sqrt{-3}$ and ζ_3 lie in M.

Proposition 1. *The extension of number fields $L/\mathbb{Q}$ is Galois, with Galois group generated by σ and τ defined by:*

$$\sigma(\zeta_9) = \zeta_9^2 \quad \textit{and} \quad \sigma(\sqrt[9]{\beta}) = \tfrac{1}{\sqrt[9]{\beta}} \ ,$$
$$\tau(\zeta_9) = \zeta_9 \quad \textit{and} \quad \tau(\sqrt[9]{\beta}) = \zeta_9 \sqrt[9]{\beta} \ .$$

The following relations hold:

$$\sigma^6 = 1, \quad \tau^9 = 1 \quad \textit{and} \quad \sigma\tau\sigma^{-1} = \tau^{-2} \ .$$

Proof. The extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is cyclic, let us call s the generator of its Galois group such that $s(\zeta_9) = {\zeta_9}^2$. The extension $L/\mathbb{Q}(\zeta_9)$ is cyclic by Kummer theory, with Galois group generated by an element τ satisfying $\tau(\zeta_9) = \zeta_9$ and $\tau(\sqrt[9]{\beta}) = \zeta_9 \sqrt[9]{\beta}$. By Kummer theory, $L/\mathbb{Q}$ is Galois if and only if $s(\beta) = \beta^u \gamma^9$ for some integer u prime to 9 and some $\gamma \in \mathbb{Q}(\zeta_9)$. Since $s(\zeta_3) = {\zeta_3}^{-1}$, we get $s(\sqrt{-3}) = -\sqrt{-3}$ and $s(\beta) = \beta^{-1}$, so the condition holds and $L/\mathbb{Q}$ is Galois and s can be extended to an automorphism σ of $L/\mathbb{Q}$. We have

$$\sigma\tau\sigma^{-1}(\zeta_9) = \zeta_9 = \tau^{-2}(\zeta_9)$$
$$\sigma\tau\sigma^{-1}(\sqrt[9]{\beta}) = \zeta_9^{-2} \sqrt[9]{\beta} = \tau^{-2}(\sqrt[9]{\beta})$$

so $\sigma\tau\sigma^{-1} = \tau^{-2}$ holds. □

We then construct the field

$$K = L^{\langle \sigma^3 \rangle} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}, \sqrt[9]{\beta} + \sqrt[9]{\beta}^{-1}) \ .$$

We sum up the construction in the diagram of Figure 1.

Theorem 1. *The extension $K/\mathbb{Q}$ is Galois with Galois group isomorphic to the non abelian semi-direct product $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ of order 27 and exponent 9.*

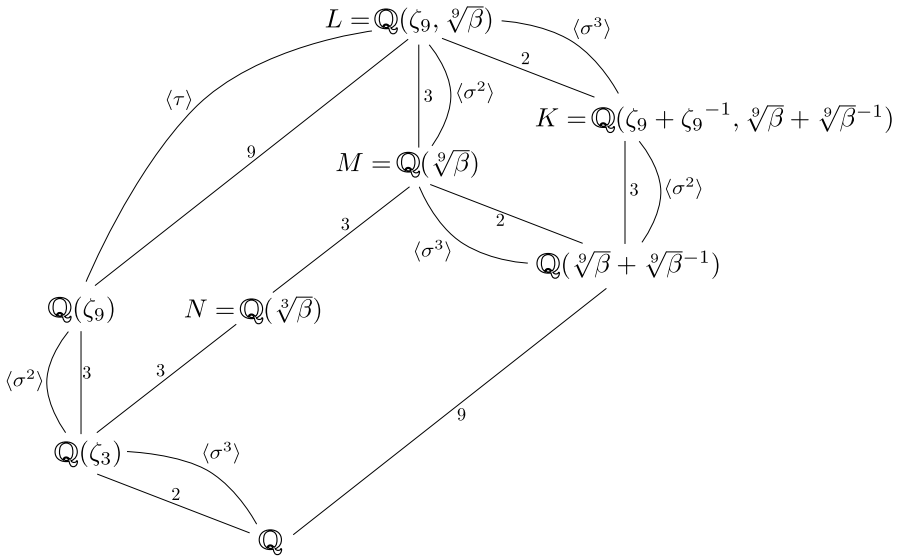


FIGURE 1. Extensions diagram

Proof. We have $\sigma^3\tau\sigma^{-3} = \tau$, so $\tau\sigma^3\tau^{-1} = \sigma^3$ and the subgroup $\langle\sigma^3\rangle$ is normal in $\langle\sigma, \tau\rangle$. Hence $K/\mathbb{Q}$ is Galois with group $\langle\sigma, \tau\rangle/\langle\sigma^3\rangle$ and relations

$$\overline{\sigma}^3 = 1, \quad \overline{\tau}^9 = 1, \quad \text{and} \quad \overline{\sigma}\,\overline{\tau}\,\overline{\sigma}^{-1} = \overline{\tau}^{-2}$$

which is isomorphic to $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. □

For effective computation in the field L, the following is useful:

PROPOSITION 2. *The minimal polynomial of the element $\sqrt[9]{\beta} + \sqrt[9]{\beta}^{-1}$ is given by*

$$X^9 - 9X^7 + 27X^5 - 30X^3 + 9X + 2 - 4a^2/p \tag{1}$$

Proof. This is a straightforward computation best performed using a computer algebra system, for example PARI/GP [P1]. □

3. Ramification

In this section, we make a complete and explicit study of the ramification in the extension $K/\mathbb{Q}$. We begin by stating the main results.

THEOREM 2. *The extension $K/\mathbb{Q}$ is unramified outside 3 and p with discriminant:*

$$\mathrm{d}_K = \begin{cases} 3^{66}p^{24} & \text{if } v_3(b) = 0 \ , \\ 3^{48}p^{24} & \text{if } v_3(b) = 1 \ , \\ 3^{36}p^{24} & \text{if } v_3(b) \geqslant 2 \ . \end{cases}$$

The ramification index above p in $K/\mathbb{Q}$ equals 9. The ideal generated by 3 in the ring of integers of K is the product of g prime ideals, each of residual degree f and ramification index e, as given in the following

table:

$v_3(b)$	0		1	2	$\geqslant 3$
	$a'\equiv b'$	$a'\not\equiv b'$			
e	9	9	9	3	3
f	1	3	3	3	1
g	3	1	1	3	9

in which the indicated congruences are modulo 3.

The proof of Theorem 2 occupies the rest of this section; we divide its presentation into several subsections for clarity.

3.1 Classical results

Let us recall some classical results without proof for further reference. We begin with results concerning extensions of local fields with finite residue field (so that a polynomial that is irreducible on the residue field is separable).

Lemma 1. *Let E/F be an unramified extension of local fields and D a local field, then the extension ED/FD is unramified.*

Lemma 2. *Let E be a local field with uniformizing parameter π, f be a monic polynomial with integral coefficients in E and α a root of f in an algebraic closure of E. Denote by $\bar{f}$ the reduction of f modulo π, then:*

(i) if $\bar{f}$ is irreducible, the extension $E(\alpha)/E$ is unramified;

(ii) if $\bar{f}$ is a square-free totally split polynomial, then $E(\alpha)=E$;

(iii) if f is an Eisenstein polynomial, the extension $E(\alpha)/E$ is totally ramified, α is a uniformizing parameter of $E(\alpha)$, and $v_\pi(\mathrm{d}_{E(\alpha)/E})$ equals the valuation of the discriminant of the polynomial f.

The second case (ii) is a consequence of Hensel's Lemma; for cases (i) and (iii), see [S, I.6]. Recall that an extension E/F of local fields is said to be *tamely ramified* if the ramification index is prime to the characteristic of the residue field of F. We know by Proposition 13 of [S, III.7]:

Lemma 3. *Let E/F be a tamely ramified extension of local fields, of ramification index e, then the valuation in E of the different of E/F equals $e-1$.*

The next result is valid for local and global fields as well [S, III.4 Prop. 8].

Lemma 4. *Let $D/E/F$ be a tower of extensions of number fields, then $\mathcal{D}_{D/F}=\mathcal{D}_{D/E}\mathcal{D}_{E/F}$ and $\mathrm{d}_{D/F}=\mathcal{N}_{E/F}(\mathrm{d}_{D/E})\mathrm{d}_{E/F}{}^{[D:E]}$.*

3.2 Ramification outside 3

First note that the cyclotomic extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ is unramified outside 3. Remind that $p=a^2+3b^2$ and $\alpha=a+b\sqrt{-3}$, so $\beta=\alpha/\sigma(\alpha)$. The extension $L/\mathbb{Q}(\zeta_9)$ is the splitting field of the polynomial $X^9-\alpha\sigma(\alpha)^8$, whose discriminant is $3^{18}\alpha^8\sigma(\alpha)^{64}$, of norm $3^{108}p^{216}$, so this extension is unramified outside 3 and p. It follows that $L/\mathbb{Q}$ and *a fortiori* its subextension $K/\mathbb{Q}$ are unramified outside 3 and p.

Now we compute the ramification of p. The prime p splits in $\mathbb{Q}(\zeta_3)$ as $(p)=(\alpha)(\sigma(\alpha))$. Remind that $\zeta_3\in M=\mathbb{Q}(\sqrt[9]{\beta})$, so the extension $M/\mathbb{Q}(\zeta_3)$ is the splitting field of the polynomial $X^9-\frac{\alpha}{\sigma(\alpha)}$, which

is an Eisenstein polynomial for the prime (α). It follows from Lemma 2 that (α) is totally (and tamely) ramified, and that the (α)–adic valuation of $\mathrm{d}_{M/\mathbb{Q}(\zeta_3)}$ is 8. Since $M = \mathbb{Q}(\sqrt[9]{\beta}^{-1})$, the same result holds for the $(\sigma(\alpha))$–adic valuation, and so by Lemma 4 the p–adic valuation of the absolute discriminant is 16. Since the extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)$ is unramified above p, it follows from Lemma 1 that the extension L/M is unramified above p. By Lemma 4, the p–adic valuation of the absolute discriminant of L is 48. Similarly the extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is unramified above p, so by Lemma 1 the same is true for the extension L/K. Eventually by Lemma 4, the p–adic valuation of the discriminant of K is half the p–adic valuation of the discriminant of L, hence is 24.

3.3 Ramification above 3

From now on we consider the ramification above 3. As in the preceding subsection, we shall make computations in the very explicit extension $L/\mathbb{Q}$, then infer the result we are interested in about the valuation of the absolute discriminant of K thanks to the equality:

Lemma 5. $2v_3(\mathrm{d}_K) = v_3(\mathrm{d}_L) - \dfrac{54}{e(3, L/\mathbb{Q})}$.

Proof. From Lemma 4 one gets $v_3(\mathrm{d}_L) = v_3\left(\mathcal{N}_{K/\mathbb{Q}}(\mathrm{d}_{L/K})\right) + 2v_3(\mathrm{d}_K)$. The extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is totally ramified at 3 and $(3) = (\sqrt{-3})^2$ as ideals of $\mathbb{Z}[\zeta_3]$. Since $\mathbb{Q}(\zeta_3) \subseteq L$, the ramification index $e(3, L/\mathbb{Q})$ of 3 in $L/\mathbb{Q}$ is even. Further, $[L : K] = 2$ whereas $[K : \mathbb{Q}]$ is odd, so L/K is totally and tamely ramified above 3, and by Lemma 3 the exponent in $\mathcal{D}_{L/K}$ of the prime ideals of L lying above 3 is 1. The same is true for the exponent in $\mathrm{d}_{L/K}$ of the prime ideals of K lying above 3, so taking the norm to $\mathbb{Q}$ yields $v_3\left(\mathcal{N}_{K/\mathbb{Q}}(\mathrm{d}_{L/K})\right) = fg$, where $fg = \frac{[K:\mathbb{Q}]}{e(3,K/\mathbb{Q})}$ happens to equal $\frac{[L:\mathbb{Q}]}{e(3,L/\mathbb{Q})}$. □

The extension $M/\mathbb{Q}(\zeta_3)$ is the splitting field of the polynomial $X^9 - \beta$. Setting $X = Y + 1$ yields:

$$S(Y) = Y^9 + 3s(Y)Y + 1 - \beta \ ,$$

where $s(Y)$ is a polynomial with integral coefficients. S is an Eisenstein polynomial for the prime $(\sqrt{-3})$ if and only if the $(\sqrt{-3})$–adic valuation of $1 - \beta$ is 1. The ideal $(\sigma(\alpha))$ being coprime to $(\sqrt{-3})$, we have

$$v_{\sqrt{-3}}(1 - \beta) = v_{\sqrt{-3}}(\sigma(\alpha) - \alpha) = v_{\sqrt{-3}}(-2b\sqrt{-3}) = 1 + 2v_3(b) \ . \tag{2}$$

3.3.1 *The case $v_3(b) = 0$* Here we suppose $v_3(b) = 0$. S is an Eisenstein polynomial for the prime $(\sqrt{-3})$, hence by Lemma 2, the prime $(\sqrt{-3})$ is totally ramified in $M/\mathbb{Q}(\zeta_3)$, $\pi = \sqrt[9]{\beta} - 1$ is a uniformizing parameter for the completion of M at the only prime above $(\sqrt{-3})$ and the $(\sqrt{-3})$–adic valuation of $\mathrm{d}_{M/\mathbb{Q}(\zeta_3)}$ and of the discriminant of S are equal. This discriminant is also the discriminant of $X^9 - \beta$, which is equal to $3^{18}\beta^8$, so its $(\sqrt{-3})$–adic valuation is 36. Then by Lemma 4, the 3–adic valuation of the absolute discriminant of M is 45.

The extension L/M is a Kummer extension of prime degree generated by $\zeta_9 = \sqrt[3]{\zeta_3}$, hence we could apply Hecke's theorem (see for example [C2, 10.2.3]), but we prefer to stick with elementary arguments, since we are looking for an explicit result. Since we suppose $v_3(b) = 0$, we may write $a = 1 + 3a'$ and $b = 1 + 3b'$ with $a', b' \in \mathbb{Z}$. We also write $p = 1 + 3p'$ with $p' \in \mathbb{Z}$. Note that $p' \equiv 2a' + 1 \pmod 3$. We consider the element of L defined by

$$\theta = \frac{\zeta_9 - \sqrt[3]{\beta}}{\sqrt{-3}} \ .$$

It generates L over M and is a root of the polynomial $(\sqrt{-3}X + \sqrt[3]{\beta})^3 - \zeta_3$, whose coefficients are in M. We have the identity

$$(\sqrt{-3}X + \sqrt[3]{\beta})^3 - \zeta_3 = -3\sqrt{-3}X^3 - 9\sqrt[3]{\beta}X^2 + 3\sqrt{-3}\sqrt[3]{\beta^2}X + \beta - \zeta_3 \ .$$

Now $\zeta_3 = \frac{-1+\sqrt{-3}}{2} = \frac{1-\sqrt{-3}}{1-3}$, so $\zeta_3 = (1-\sqrt{-3})\sum_{i\geqslant 0} 3^i$ in $\mathbb{Q}_3(\zeta_3)$ and

$$\zeta_3 \equiv 1 - \sqrt{-3} + 3 - 3\sqrt{-3} \pmod 9 \tag{3}$$

Further, $\beta = 1 + 2\frac{ab\sqrt{-3}-3b^2}{p}$, which yields:

$$\beta \equiv 1 - \sqrt{-3} + 3 + (-1 + a' - b')3\sqrt{-3} \pmod 9 \tag{4}$$

with the notations introduced above. We get from this computation that $\beta \equiv \zeta_3 \pmod{3\sqrt{-3}}$, so $\eta = \frac{\beta-\zeta_3}{3\sqrt{-3}}$ is integral in $\mathbb{Q}_3(\zeta_3)$. More precisely, $\eta \equiv a' - b' \pmod{\sqrt{-3}}$. It follows that θ is a root of the polynomial:

$$T(X) = X^3 - \sqrt{-3}\sqrt[3]{\beta}X^2 - \sqrt[3]{\beta^2}X - \eta$$

with integral coefficients in M. Note that $\sqrt[3]{\beta^2} - 1 = (\sqrt[9]{\beta} - 1)(\sqrt[9]{\beta} + 1)(\zeta_3\sqrt[9]{\beta^2} - 1)(\zeta_3^2\sqrt[9]{\beta^2} - 1)$, so T reduces modulo $\pi = \sqrt[9]{\beta} - 1$ to the polynomial $\overline{T}(X) = X^3 - X + b' - a'$. We have to consider two possibilities:

- if $a' \not\equiv b' \pmod 3$, $\overline{T}$ is an Artin-Schreier polynomial, hence is irreducible over $\mathbb{F}_3$, so by Lemma 2 the primitive element θ generates an unramified extension in which the prime above 3 is inert;
- if $a' \equiv b' \pmod 3$, $\overline{T}(X) = X^3 - X$ is a square-free totally split polynomial so, by Hensel's Lemma, T is totally split over M_π, θ belongs to this field, and the prime above 3 splits in L/M.

In both cases, the extension is unramified, and so by Lemma 4, the 3–adic valuation of the discriminant of L is 135. The ramification index of $L/\mathbb{Q}$ is 18 so, by Lemma 5, the 3–adic valuation of the discriminant of K is 66.

3.3.2 *Ramification above* 3 *when* $v_3(b) \geqslant 1$ Now we suppose $v_3(b) \geqslant 1$. We first study the extension $\mathbb{Q}(\sqrt[3]{\beta})/\mathbb{Q}(\zeta_3)$. It is a Kummer extension and we will use the same technique as above. Let us consider the element $\frac{\sqrt[3]{\beta}-1}{\sqrt{-3}}$. It generates the extension and is a root of the polynomial

$$(\sqrt{-3}X + 1)^3 - \beta = -3\sqrt{-3}X^3 - 9X^2 + 3\sqrt{-3}X + 1 - \beta \ .$$

It is also a root of

$$U(X) = X^3 - \sqrt{-3}X^2 - X + \frac{\beta - 1}{3\sqrt{-3}}$$

which, by equation (2), has integral coefficients in $\mathbb{Q}(\zeta_3)$ under our assumption. We deduce from $\frac{\beta-1}{3\sqrt{-3}} = \frac{2(a+b\sqrt{-3})}{p}\frac{b}{3}$ and $b = 3b'$ that

$$\frac{\beta - 1}{3\sqrt{-3}} \equiv -b' \pmod 3 \ . \tag{5}$$

This leads to two possibilities:

- $v_3(b) = 1$, then the reduction of $U(X)$ modulo $\sqrt{-3}$ is $X^3 - X - b'$ which is irreducible, hence $\sqrt{-3}$ is inert in the extension;
- $v_3(b) \geqslant 2$, then the reduction of $U(X)$ modulo $\sqrt{-3}$ is $X^3 - X$ which is square-free and totally split, hence $\sqrt{-3}$ is totally split in the extension.

Note that in both cases the extension is unramified above 3.

3.3.3 *The case* $v_3(b) \geqslant 2$ We begin with the second case $v_3(b) \geqslant 2$. Denote by N the field $\mathbb{Q}(\sqrt[3]{\beta})$, and by $\wp_1, \wp_2, \wp_3$ the prime ideals of $\mathcal{O}_N$ above $\sqrt{-3}$, since $N/\mathbb{Q}(\zeta_3)$ is totally split above $\sqrt{-3}$ by the preceding result. The reduction of $U(X)$ modulo $\wp = \wp_1$ equals $X(X-1)(X+1)$, so one of the roots of U belongs to $\wp$ and we set γ to be the cubic root of β such that $\frac{\gamma-1}{\sqrt{-3}} \equiv 0 \pmod{\wp}$. Using congruence (3), we get that the other roots of U satisfy:

$$\frac{\zeta_3\gamma - 1}{\sqrt{-3}} \equiv -1 \pmod{\wp}\ ; \quad \frac{\zeta_3^2\gamma - 1}{\sqrt{-3}} \equiv 1 \pmod{\wp}\ ,$$

so $v_\wp(\zeta_3\gamma - 1) = v_\wp(\zeta_3^2\gamma - 1) = v_\wp(\sqrt{-3}) = 1$. The identity $1-\beta = (1-\gamma)(1-\zeta_3\gamma)(1-{\zeta_3}^2\gamma)$ yields

$$v_\wp(1-\gamma) = v_\wp(1-\beta) - 2 = 2v_3(b) - 1 \geqslant 3\ ,$$

so that $\frac{\gamma-1}{3\sqrt{-3}}$ is integral in $N_\wp$.

The element $\frac{1-\sqrt[3]{\gamma}}{\sqrt{-3}}$ is a generator of the extension M/N and a root of the polynomial

$$X^3 + \sqrt{-3}X^2 - X + \frac{1-\gamma}{3\sqrt{-3}}$$

with integral coefficients in $N_\wp$, so as above either $v_3(b) = 2$ and $\wp$ is inert in M/N, either $v_3(b) \geqslant 3$ and $\wp$ is totally split. Let $\mathfrak{p}$ denote a prime ideal of $\mathcal{O}_L$ above $\wp$ and set $\wp' = \mathfrak{p} \cap \mathcal{O}_M$, then in both cases the extension $M/\mathbb{Q}(\zeta_3)$ is unramified at $\wp'$. By Lemma 1, we deduce that the extension $L/\mathbb{Q}(\zeta_9)$ is unramified at $\mathfrak{p}$. The discriminant of the cyclotomic field $\mathbb{Q}(\zeta_9)$ is -3^9, so $v_\mathfrak{p}(\mathcal{D}_{L/\mathbb{Q}}) = 9$; further $v_{\mathfrak{p}'}(\mathcal{D}_{L/\mathbb{Q}}) = 9$ for any prime $\mathfrak{p}'$ above 3 in $\mathcal{O}_L$ since the different is an ambiguous ideal. This yields that the 3–adic valuation of the discriminant of L is 81. The ramification index in $L/\mathbb{Q}$ is 6, so by Lemma 5 we conclude that the 3–adic valuation of the discriminant of K is 36.

Remark. Contrary to $\wp_1$, the ideals $\wp_2$ and $\wp_3$ of $\mathcal{O}_N$ are ramified in M/N. As we shall see more precisely in subsection 4.2 for the extension $K/\mathbb{Q}$, of Galois group isomorphic to that of $L/\mathbb{Q}(\zeta_3)$, the three conjugated subgroups of order 3 of $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3))$ appear as ramification groups of prime ideals above 3 in $\mathcal{O}_L$, hence some of these ideals are not ramified in $L/M = L^{\langle\sigma^2\rangle}$ and have to be above ideals that ramify in M/N.

3.3.4 *The case* $v_3(b) = 1$ Finally we consider the case $v_3(b) = 1$. Let us denote by γ a cubic root of β. The identity

$$1 - \beta = (1-\gamma)(1-\zeta_3\gamma)(1-{\zeta_3}^2\gamma)$$

and the fact that $1-\gamma$, $1-\zeta_3\gamma$ and $1-{\zeta_3}^2\gamma$ are conjugated give us that

$$v_{\sqrt{-3}}(1-\gamma) = 1\ ,$$

so the minimal polynomial of $\sqrt[3]{\gamma} - 1$, namely $X^3 + 3X^2 + 3X + 1 - \gamma$, is an Eisenstein polynomial. By Lemma 2 the extension $M/\mathbb{Q}(\sqrt[3]{\beta})$ is totally ramified and the $(\sqrt{-3})$–adic valuation of the relative discriminant ideal is equal to the $(\sqrt{-3})$–adic valuation of the polynomial $X^3 - \gamma$. The discriminant of this polynomial is $3^3\gamma^2$ and its $(\sqrt{-3})$–adic valuation is 6, so by Lemma 4, the $(\sqrt{-3})$–adic valuation of the discriminant of $M/\mathbb{Q}(\zeta_3)$ is 18 and the 3–adic valuation of the absolute discriminant of M is 27.

We now deal with the extension L/M. We set $\pi = \sqrt[9]{\beta} - 1$; it is a uniformizing parameter for the only prime above 3 in $\mathcal{O}_M$. Since the residual degree of $M_\pi/\mathbb{Q}_3$ equals 3, we know that the group of local units $\mathcal{O}_{M_\pi}^\times$ contains a cyclic subgroup of order $26 = 3^3 - 1$, which we denote by μ_{26}. Recall that

any integral element x of M_π may be written uniquely as $x = \sum_{i\geqslant 0} x_i\pi^i$ with $x_i \in \mu_{26} \cup \{0\}$ for all i. We first show that $\sqrt{-3}$ is —almost— a cube in M_π modulo π^8.

Lemma 6. *There exists $\delta \in \mu_{26} \setminus \{\pm 1\}$ such that $\sqrt{-3} \equiv \Big(\delta\pi(1+\pi)\Big)^3 - \delta^9\pi^7 \pmod{\pi^8}$.*

Proof. Recall from section 2 that $b = 3b'$ with $b' \equiv -1 \pmod 3$. From congruence (5) we get

$$\sqrt{-3} \equiv \frac{\beta - 1}{3} \pmod{3\sqrt{-3}} \ .$$

On the other hand, developing $\pi^3 = (\sqrt[9]{\beta} - 1)^3$ yields $\gamma - 1 = \pi^3 + 3\pi\sqrt[9]{\beta}$; developing $(\gamma-1)^3$ yields $\beta - 1 \equiv \pi^9 + 3\pi^3 + 3\pi^6 + 9\pi\sqrt[9]{\beta} \pmod{\pi^{16}}$, hence

$$\sqrt{-3} \equiv \frac{\pi^9}{3} + \pi^3 + \pi^6 + 3\pi \pmod{\pi^8} \tag{6}$$

since $\sqrt[9]{\beta} \equiv 1 \pmod\pi$. Let $a_0 \in \mu_{26}, a_1, a_2, \ldots \in \mu_{26} \cup \{0\}$ be such that

$$\sqrt{-3} = \sum_{i\geqslant 0} a_i\pi^{3+i} = a_0\pi^3\Big(1 + \sum_{i\geqslant 1} b_i\pi^i\Big) \ ,$$

where $b_i = \frac{a_i}{a_0}$ for $i \geqslant 1$, then we have the congruence modulo π^{11}:

$$3 \equiv -a_0^2\pi^6\Big(1 - b_1\pi + (b_1^2 - b_2)\pi^2 - (b_1b_2 + b_3)\pi^3 + (b_2^2 - b_1b_3 - b_4)\pi^4\Big) \ . \tag{7}$$

Consequently $3\pi \equiv -a_0^2\pi^7 \pmod{\pi^8}$ and

$$\frac{\pi^9}{3} \equiv -\frac{\pi^3}{a_0^2}\Big(1 + b_1\pi + b_2\pi^2 + (b_3 - b_1^3)\pi^3 + (b_4 - b_1^4)\pi^4\Big) \pmod{\pi^8} \ .$$

Congruence (6) yields the system of equations:

$$\begin{cases} a_0^3 = -1 + a_0^2 & (i) \\ a_0^3b_1 = -b_1 & (ii) \\ a_0^3b_2 = -b_2 & (iii) \\ a_0^3b_3 = a_0^2 + b_1^3 - b_3 & (iv) \\ a_0^3b_4 = -a_0^4 + b_1^4 - b_4 & (v) \end{cases}$$

From equation (i), a_0 is a root of $t^3 - t^2 + 1$ (which is irreducible over $\mathbb{F}_3$), hence $a_0^3 \neq -1$, so (ii) and (iii) imply $b_1 = b_2 = 0$. Then the system easily yields $b_3 = 1$ and $b_4 = -a_0^2$, so $\sqrt{-3} \equiv a_0\pi^3 + a_0\pi^6 - a_0^3\pi^7 \pmod{\pi^8}$. Let $\delta \in \mu_{26}$ be such that $\delta^3 = a_0$ to get the result. □

Consider the polynomial

$$V(X) = X^3 + \frac{3(1+\pi)^2}{\pi^4}\zeta_3 X - \frac{(1+\pi)^3}{\pi^6}\sqrt{-3}$$

and let $x = \frac{\delta(1+\pi)^2}{\pi}$. We claim that $V(X+x)$, which equals:

$$X^3 + 3xX^2 + \left(3x^2 + \frac{3(1+\pi)^2}{\pi^4}\zeta_3\right)X + \frac{3(1+\pi)^2}{\pi^4}\zeta_3 x + x^3 - \frac{(1+\pi)^3}{\pi^6}\sqrt{-3} \ ,$$

is an Eisenstein polynomial for the prime (π): it is clear that the coefficients of X and X^2 have valuation greater than 1; further, congruence (7) yields:

$$\frac{3(1+\pi)^2}{\pi^4}\zeta_3 x \equiv \frac{3}{\pi^5}\delta \equiv -\delta^7\pi \pmod{\pi^2}$$

and we deduce from Lemma 6 that

$$x^3 - \frac{(1+\pi)^3}{\pi^6}\sqrt{-3} = \frac{(1+\pi)^3}{\pi^6}\left(\delta^3\pi^3(1+\pi)^3 - \sqrt{-3}\right) \equiv \delta^9\pi \pmod{\pi^2} \ ,$$

so that

$$\frac{3(1+\pi)^2}{\pi^4}\zeta_3 x + x^3 - \frac{(1+\pi)^3}{\pi^6}\sqrt{-3} \equiv \delta^7(\delta^2-1)\pi \not\equiv 0 \pmod{\pi^2} \ ,$$

namely the constant coefficient of $V(X+x)$ is of π–adic valuation 1.

By Lemma 2, the extension L/M is totally ramified above π, and the π–adic valuation of its discriminant equals that of the discriminant of V, which is easily computed:

$$\mathrm{disc}(V) = -\frac{27(1+\pi)^6}{\pi^{12}} \ ,$$

hence $v_\pi(\mathrm{d}_{L/M}) = 6$. Lemma 4 then shows $v_3(\mathrm{d}_{L/\mathbb{Q}}) = 99$ and we conclude using Lemma 5 that $v_3(\mathrm{d}_{K/\mathbb{Q}}) = 48$.

This ends the proof of Theorem 2.

4. Some consequences

4.1 Uniformizing parameters

In the proof of Theorem 2, we managed to find a uniformizing parameter of L at any prime ideal above 3 when $v_3(b) = 0$ or $v_3(b) \geqslant 2$, and to construct an Eisentein polynomial $V(X+x)$ for L/M when $v_3(b) = 1$. Since Cardano's formulas [C1] enable computing the roots of V, we get an explicit uniformizing parameter in every case:

Corollary 1. *With the notations introduced above, a uniformizing parameter of L at any prime ideal above 3 is $\pi = \sqrt[9]{\beta} - 1$ when $v_3(b) = 0$; $\zeta_9 - 1$ when $v_3(b) \geqslant 2$; when $v_3(b) = 1$, let $\mathfrak{p}$ denote the only prime ideal of $\mathcal{O}_L$ above 3, we get a* local *uniformizing parameter:*

$$\frac{1+\pi}{\pi^2}\zeta_9(1-\zeta_9) - \delta\frac{(1+\pi)^2}{\pi} \in L_\mathfrak{p} \ ,$$

where δ is defined as in Lemma 6.

Taking the norm from L to K, or from $L_\mathfrak{p}$ to $K_\wp$ where $\wp = \mathcal{O}_K \cap \mathfrak{p}$, one easily deduces formulas for a uniformizing parameter of K or of $K_\wp$ at any prime ideal above 3: $2 - \sqrt[9]{\beta} - \sqrt[9]{\beta}^{-1}$ when $v_3(b) = 0$, $2 - \zeta_9 - \zeta_9^{-1}$ when $v_3(b) \geqslant 2$; when $v_3(b) = 1$, we would prefer not to write the formula unless we really need to.

4.2 Ramification subgroups

Let E/F denote a Galois extension of number fields, of Galois group G, and let $\mathfrak{p}$ denote a prime ideal of $\mathcal{O}_E$, of decomposition group $G_{-1}(\mathfrak{p}) \subseteq G$. Recall that $G_{-1}(\mathfrak{p})$ is isomorphic to the Galois group of the extension of local fields $E_\mathfrak{p}/F_\wp$, where $\wp = \mathfrak{p} \cap \mathcal{O}_F$, and that there exists a filtration

$$G_{-1}(\mathfrak{p}) \supseteq G_0(\mathfrak{p}) \supseteq G_1(\mathfrak{p}) \supseteq G_2(\mathfrak{p}) \cdots$$

of (finitely many non trivial) normal subgroups $G_i(\mathfrak{p})$ of $G_{-1}(\mathfrak{p})$, such that $G_0(\mathfrak{p})$ is the ramification group of E/F above $\wp$ (hence its order $|G_0(\mathfrak{p})|$ equals the ramification index of E/F above $\wp$) and $G_1(\mathfrak{p})$ is the p–Sylow subgroup of $G_0(\mathfrak{p})$, where p stands for the characteristic of the residual field $\mathcal{O}_E/\mathfrak{p}$.

We shall say that an integer $n \geqslant -1$ is a *jump* for the ramification filtration $\big(G_i(\mathfrak{p})\big)_{i\geqslant -1}$ if $G_{n+1}(\mathfrak{p}) \neq G_n(\mathfrak{p})$. The valuation at the prime ideal $\mathfrak{p}$ of the different of E/F is given by Hilbert's formula [S, IV.1 Prop.4]:

$$v_{\mathfrak{p}}(\mathcal{D}_{E/F}) = \sum_{i\geqslant 0}(|G_i(\mathfrak{p})| - 1) \ . \tag{8}$$

The extension E/F is *weakly ramified* if $G_2(\mathfrak{p})$ is trivial for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_E$, in other words if no prime ideal of $\mathcal{O}_E$ has a jump larger than 1 in its ramification filtration. See for instance [E, §2] for the interest of this definition in terms of Galois module structure.

We can now state the following easy consequence of Theorem 2 about the jumps of the ramification filtration above 3 in $K/\mathbb{Q}$.

Corollary 2. *The set of jumps in the ramification filtration of any prime ideal of $\mathcal{O}_K$ above 3 is: $\{1,4\}$ if $v_3(b) = 0$ and $a' \equiv b' \pmod 3$; $\{-1,1,4\}$ if $v_3(b) = 0$ and $a' \not\equiv b' \pmod 3$; $\{-1,1\}$ if $v_3(b) = 1$ or 2; $\{1\}$ if $v_3(b) \geqslant 3$.*
Consequently, the extension $K/\mathbb{Q}$ is weakly ramified if and only if $v_3(b) \geqslant 1$.

Proof. Denote by $(G_i)_{i\geqslant -1}$, the ramification filtration for a prime $\mathfrak{p}$ above 3 in $\mathcal{O}_K$. Using the notations of Theorem 2, one has $|G_{-1}| = ef$; further since $K/\mathbb{Q}$ is a 3-extension, one also has $|G_0| = |G_1| = e$, and Hilbert's formula (8) yields:

$$v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}) = 2(e-1) + \sum_{i\geqslant 2}(|G_i| - 1) \ .$$

Since $\mathrm{d}_{K/\mathbb{Q}} = \mathcal{N}_{K/\mathbb{Q}}(\mathcal{D}_{K/\mathbb{Q}})$, one has $v_3(d_{K/Q}) = fgv_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}}) = \frac{27}{e}v_{\mathfrak{p}}(\mathcal{D}_{K/\mathbb{Q}})$. The computation of the jumps follows in each case using Theorem 2 and recalling that $G_{i+1} \subseteq G_i$ for all i. Further, $K/\mathbb{Q}$ is unramified outside 3 and p and tamely ramified at p, which implies $G_1(\wp) = \{1\}$ for any prime ideal $\wp$ of $\mathcal{O}_E$ above p. □

Note that cases $v_3(b) = 1$ and $v_3(b) = 2$ are quite different, even though they share the same set of jumps above 3, since the decomposition group above 3 is G in the first case and a subgroup of G of order 9 in the second. In particular, the local extension $K_{\mathfrak{p}}/\mathbb{Q}_3$, where $\mathfrak{p}$ stands for a prime ideal of $\mathcal{O}_K$ above 3, is non abelian in the first case, abelian in the second. In fact, we are able to state the following more precise result about the ramification subgroups above 3 in $K/\mathbb{Q}$. Before doing so, recall that $G = \mathrm{Gal}(K/\mathbb{Q})$ has the following presentation:

$$G = \big\langle\, \overline{\sigma}\,, \overline{\tau} \mid \overline{\sigma}^{\,3} = 1,\ \overline{\tau}^{\,9} = 1,\ \overline{\sigma}\,\overline{\tau}\,\overline{\sigma}^{\,-1} = \overline{\tau}^{\,-2} \,\big\rangle \ ,$$

from which one easily checks that G has the subgroups diagram of Figure 2, in which all subgroups of index 3 (second line) are normal, whereas only one subgroup of index 9 (third line) is normal: $\big\langle\, \overline{\tau}^{\,3} \,\big\rangle$, the three other ones being conjugated.

It follows that K has four subextensions of degree 9 over $\mathbb{Q}$: $K^{\langle \overline{\sigma}\,\rangle} = \mathbb{Q}(\sqrt[9]{\beta} + \sqrt[9]{\beta}^{-1})$, $K^{\langle \overline{\sigma}\,\overline{\tau}^{\,3}\rangle}$ and $K^{\langle \overline{\sigma}\,\overline{\tau}^{\,6}\rangle}$ are conjugated, whereas $K^{\langle \overline{\tau}^{\,3}\rangle}$ is normal, with Galois group isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$, namely $K^{\langle \overline{\tau}^{\,3}\rangle}/\mathbb{Q}$ is bicyclic bicubic, and contains the four subextensions of K of degree 3 over $\mathbb{Q}$. All of these are normal, with $K^{\langle \overline{\tau}\,\rangle}$ having the property to be of conductor a power 3 (see Lemma 8 below).

We now describe the ramification filtrations in $K/\mathbb{Q}$.

Proposition 3. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p, then $G_0(\mathfrak{p}) = \langle\, \overline{\tau}\,\rangle$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ denote the prime ideals of $\mathcal{O}_K$ above 3, then:*

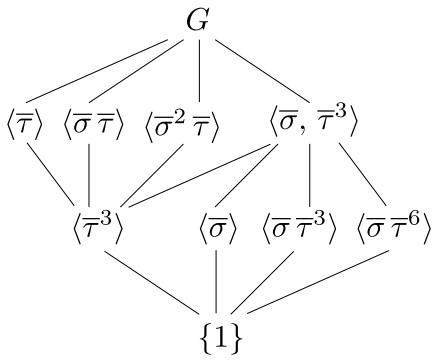


Figure 2. Subgroups diagram of G

(i) $v_3(b) = 0$*: for* $1 \leqslant k \leqslant g$, $G_{-1}(\mathfrak{p}_k)$ *equals* G *if* $a' \not\equiv b' \pmod 3$*, the ramification group otherwise; in both cases,* $G_0(\mathfrak{p}_k) = G_1(\mathfrak{p}_k) = \left\langle\, \overline{\sigma}^{\,2}\,\overline{\tau}\,\right\rangle$ *and* $G_2(\mathfrak{p}_k) = G_3(\mathfrak{p}_k) = G_4(\mathfrak{p}_k) = \left\langle\, \overline{\tau}^{\,3}\,\right\rangle$*, the only subgroup of order* 3 *of* $G_0(\mathfrak{p}_k)$*;*

(ii) $v_3(b) = 1$*:* $G_{-1}(\mathfrak{p}_1) = G$ *and* $G_0(\mathfrak{p}_1) = G_1(\mathfrak{p}_1)$ *is the only normal subgroup of* G *of order* 9 *and exponent* 3*, namely* $\left\langle\, \overline{\tau}^{\,3}, \overline{\sigma}\,\right\rangle$*;*

(iii) $v_3(b) = 2$*:* $G_{-1}(\mathfrak{p}_k) = \left\langle\, \overline{\tau}^{\,3}, \overline{\sigma}\,\right\rangle$ *for every* $1 \leqslant k \leqslant 3$ *and the groups* $G_0(\mathfrak{p}_k) = G_1(\mathfrak{p}_k)$, $1 \leqslant k \leqslant 3$*, are the three conjugated subgroups of order* 3 *of* G*, namely* $\left\langle\, \overline{\sigma}\,\right\rangle$, $\left\langle\, \overline{\sigma}\,\overline{\tau}^{\,3}\,\right\rangle$ *and* $\left\langle\, \overline{\sigma}\,\overline{\tau}^{\,6}\,\right\rangle$*;*

(iv) $v_3(b) \geqslant 3$*: each of the three conjugated subgroups of order* 3 *of* G *equals* $G_{-1}(\mathfrak{p}_k) = G_0(\mathfrak{p}_k) = G_1(\mathfrak{p}_k)$ *for exactly three values of* $1 \leqslant k \leqslant 9$*.*

Proof. The assertion about p is easy since we have seen in Subsection 3.2 that p is unramified in $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ and that any prime ideal of $\mathcal{O}_L$ above p is totally ramified in $L/\mathbb{Q}(\zeta_9) = L^{\langle\,\tau\,\rangle}$. So the ramification group in $L/\mathbb{Q}$ of such a prime ideal is $\langle\,\tau\,\rangle$ and we get the result using Herbrand's theorem [S, IV.3 Lemme 5].

A study of the group

$$\mathcal{G} = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^6 = 1,\ \tau^9 = 1,\ \sigma\tau\sigma^{-1} = \tau^{-2}\rangle$$

shows that $\mathcal{G}$ has four subgroups of order 9, three of which are cyclic: $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\left\langle\, \sigma^4\tau\,\right\rangle$, and one is of exponent 3: $\left\langle\, \sigma^2,\ \tau^3\,\right\rangle$. We already know by Theorem 2 that $L/L^{\langle\,\tau\,\rangle} = \mathbb{Q}(\zeta_9)$ is never totally ramified above the prime ideal $(1-\zeta_9)$, hence τ never belongs to the ramification group of a prime ideal of $\mathcal{O}_L$ above 3. Let us show that the same is true for $\sigma^4\tau$, and for $\sigma^2\tau$ when $v_3(b) \geqslant 1$; we shall see below that the assertion about $\sigma^2\tau$ does not extend to the case $v_3(b) = 0$.

Lemma 7. *Set* $\gamma = (\sqrt[9]{\beta})^3$*, then* $L^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(\zeta_9^2\gamma)$ *is ramified over* $\mathbb{Q}(\zeta_3)$ *above* $\sqrt{-3}$ *when* $v_3(b) \geqslant 1$*, and* $L^{\langle\sigma^4\tau\rangle} = \mathbb{Q}(\zeta_9\gamma)$ *is always ramified over* $\mathbb{Q}(\zeta_3)$ *above* $\sqrt{-3}$*.*

We illustrate the result in Figure 3.

Proof. One easily checks that $\sigma^2\tau(\zeta_9^2\gamma) = \zeta_9^2\gamma$ and $\sigma^4\tau(\zeta_9\gamma) = \zeta_9\gamma$, then comparing degrees yields $L^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(\zeta_9^2\gamma)$ and $L^{\langle\sigma^4\tau\rangle} = \mathbb{Q}(\zeta_9\gamma)$. Further, $\zeta_9^2\gamma$ is a root of $R(X) = X^3 - \zeta_3^2\beta \in \mathbb{Z}_3[\zeta_3][X]$ and

$$R(X+1) = X^3 + 3X^2 + 3X + 1 - \zeta_3^2\beta\ ,$$

which is an Eisenstein polynomial for the prime ideal $(\sqrt{-3}) = (1-\zeta_3^2)$ when $v_3(b) \geqslant 1$, since $1 - \zeta_3^2\beta = \zeta_3^2(1-\beta) + (1-\zeta_3^2)$ and $v_{\sqrt{-3}}(1-\beta) \geqslant 3$ in this case; the case $v_3(b) = 0$ is different:

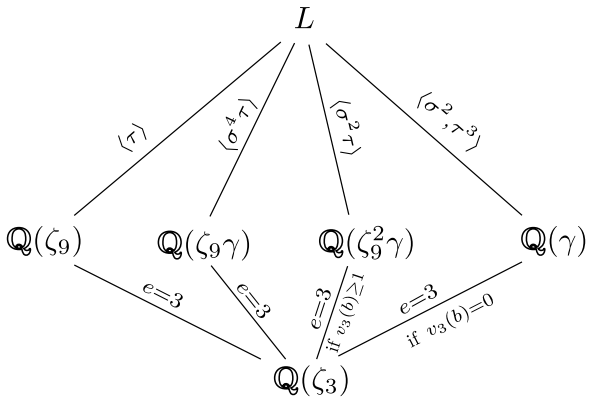


Figure 3. Ramification above $\sqrt{-3}$ in the subextensions of L of index 9

congruences (3) and (4) shown in subsection 3.3.1 yield

$$\zeta_3^2\beta \equiv 1 \pmod 3 \ ,$$

hence $R(X+1)$ is no longer Eisenstein for the prime ideal $(\sqrt{-3})$. Analogously, the minimal polynomial of $\zeta_9\gamma - 1$ is $X^3 + 3X^2 + 3X + 1 - \zeta_3\beta$, which is always an Eisenstein polynomial for the prime ideal $(\sqrt{-3}) = (1 - \zeta_3)$, since $\zeta_3\beta \not\equiv 1 \pmod 3$ when $v_3(b) = 0$, hence the extension $\mathbb{Q}(\zeta_9^2\gamma)/\mathbb{Q}(\zeta_3)$ is always totally ramified above this prime. □

Let us deduce the first two statements of Proposition 3 from Lemma 7. Suppose $v_3(b) = 0$: $L^{\langle\sigma^4\tau\rangle} = \mathbb{Q}(\zeta_9\gamma)$ and $\mathbb{Q}(\gamma) = L^{\langle\,\sigma^2,\,\tau^3\,\rangle}$ are ramified over $\mathbb{Q}(\zeta_3)$ above $\sqrt{-3}$, just as $L^{\langle\,\tau\,\rangle} = \mathbb{Q}(\zeta_9)$, hence neither $\langle\,\sigma^4\tau\,\rangle$, nor $\langle\,\sigma^2,\,\tau^3\,\rangle$, nor $\langle\,\tau\,\rangle$, may be contained in the ramification group of a prime ideal $\wp$ of $\mathcal{O}_L$ above 3; by Theorem 2, such a group is of order 18, its 3–Sylow subgroup $\mathcal{G}_1(\wp)$ of order 9 thus has to be $\langle\,\sigma^2\tau\,\rangle$ (which implies that $\mathbb{Q}(\zeta_9^2\gamma)/\mathbb{Q}(\zeta_3)$ is unramified above $\sqrt{-3}$ as announced). Set $\mathfrak{p} = \wp\cap\mathcal{O}_K$, one knows (using Herbrand's theorem, substitute u for 1 in [S, IV.3 Lemme 5]) that:

$$G_1(\mathfrak{p}) = \big(\mathcal{G}_1(\wp)\,\langle\,\sigma^3\,\rangle\big)/\,\langle\,\sigma^3\,\rangle \ , \tag{9}$$

so $G_0(\mathfrak{p}) = G_1(\mathfrak{p}) = \langle\,\overline{\sigma}^2\overline{\tau}\,\rangle$. The result concerning the ramification subgroups of higher index is straightforward in view of Corollary 2 and of the subgroups diagram of G (Figure 2).

In the case $v_3(b) = 1$, the result of Lemma 7 implies that $L/L^{\langle\sigma^2\tau\rangle}$ and $L/L^{\langle\sigma^4\tau\rangle}$ are not totally ramified above 3, hence neither $\sigma^2\tau$ nor $\sigma^4\tau$ may belong to the first ramification group $\mathcal{G}_1(\wp)$ of a prime ideal $\wp$ of $\mathcal{O}_L$ above 3. This was already known for τ, consequently $\mathcal{G}_1(\wp)$ contains no element of order 9 of $\mathcal{G}$, hence can only equal $\langle\,\sigma^2,\,\tau^3\,\rangle$ since its order is 9. This proves the assertion of the Proposition for the case $v_3(b) = 1$ using (9).

Before dealing with the case $v_3(b) \geqslant 2$, let us state an auxiliary result that is valid in all cases. Consider the abelian subgroup $\langle\tau, \sigma^3\rangle$ of $\mathcal{G}$ of order 18, the corresponding subextension W of L satisfies

$$W = L^{\langle\tau,\sigma^3\rangle} = \mathbb{Q}(\zeta_9)^{\langle\sigma^3\rangle} = K^{\langle\tau\rangle} \ ,$$

in other words:

Lemma 8. *The only subextension W of $\mathbb{Q}(\zeta_9)$ of degree 3 over $\mathbb{Q}$ is the fixed field of K under $\langle\overline{\tau}\rangle$.*

Suppose $v_3(b) \geqslant 2$. The extension $W/\mathbb{Q}$ is ramified (weakly ramified indeed) above 3, hence by Theorem 2 the extension K/W can not be ramified at a prime ideal $\mathfrak{p}$ above 3. The ramification group

$G_0(\mathfrak{p})$ then has to be one of the three conjugated subgroups of order 3 of G (see Figure 3): $\langle\, \overline{\sigma}\, \rangle$, $\langle\, \overline{\sigma}\, \overline{\tau}^{\,3} \,\rangle$ or $\langle\, \overline{\sigma}\, \overline{\tau}^{\,6} \,\rangle$. Since 3 splits in $K/\mathbb{Q}$, these three subgroups occur as ramification groups, of one prime ideal above 3 each in case $v_3(b) = 2$, of three of these each in case $v_3(b) \geqslant 3$. The three cyclic subgroups of order 9 of G only contain one subgroup of order 3: $\langle\, \overline{\tau}^{\,3} \,\rangle$, hence the; decomposition group of a prime ideal of $\mathcal{O}_K$ above 3 can only be $\langle\, \overline{\sigma}\,,\, \overline{\tau}^{\,3} \,\rangle$ in the case $v_3(b) = 2$. □

The proof of Proposition 3 given above involves arguments already used in [V, §4.2], which we present here in a more complete and systematic manner.

5. Class groups

We are interested in the 3-part of the class group of the field K. We begin by considering the bicyclic bicubic subextension B of K fixed by $\langle \overline{\tau}^{\,3} \rangle$, the (only) normal subgroup of order 3. Recall our conventions for a and b such that $p = a^2 + 3b^2$ at the beginning of Section 2.

Proposition 4. *The class number h_B of B is divisible by 3 if and only if*

$$p \equiv 1 \mod 9 \text{ and } (\, a \equiv b \text{ or } b \equiv 0 \mod 9\,) \ .$$

Proof. We know that 3 and p are the only ramified primes in $K/\mathbb{Q}$, as well as in $B/\mathbb{Q}$. By [P2, Theorem 9], we deduce that 3 divides h_B if and only if p is a cubic residue modulo 9 and 3 is a cubic residue modulo p. Since $p \equiv 1 \mod 3$, p is a cubic residue modulo 9 if and only if $p \equiv 1 \mod 9$.

Further p can be uniquely written as $p = \frac{1}{4}(L^2 + 3M^2)$ up to the signs of L and M (see [IR, Proposition 8.3.2]). To do that, note that exactly one out of $s = a + b$, $d = a - b$, b is divisible by 3, and that $4p = (2a)^2 + 3(2b)^2 = (2s - d)^2 + 3d^2 = (2d - s)^2 + 3s^2$. By [L2, Proposition 7.2], 3 is a cube modulo p if and only if 3 divides M, namely if and only if one of $a + b$, $a - b$, b is divisible by 9. This yields the result since $a \equiv -b \mod 9$ is not possible with our conventions. □

The preceding result can be expressed in the following condensed way.

Corollary 3. *One has:* $3 \mid h_B \Leftrightarrow a' \equiv b' \equiv b \mod 3$. *Therefore* $3 \mid h_B$ *can only occur when* $v_3(b) = 0$ *with* $a' \equiv b' \mod 3$, *and when* $v_3(b) \geqslant 2$.

Not every p with $v_3(b) = 0$ and $a' \equiv b' \mod 3$ has h_B divisible by 3, see $p = 61$ in the Table given in Subsection 6.3 below.

Proof. Since $p \equiv 1 + 3(2a' + b) \mod 9$ (note that $b^2 \equiv b \mod 3$ with our conventions),

$$p \equiv 1 \mod 9 \Longleftrightarrow a' \equiv b \mod 3 \ .$$

Assume $p \equiv 1 \mod 9$. If $b \equiv 0 \mod 9$ then $b = 3b'$ with $b' \equiv 0 \mod 3$, thus $a' \equiv b' \equiv b (\equiv 0) \mod 3$. If $a \equiv b \mod 9$ then $a \equiv a' \equiv b \equiv 1 \mod 3$, so $b = 1 + 3b' \equiv 1 + 3a' \mod 9$, hence $b' \equiv a' \mod 3$. We get by Proposition 4 that $3 \mid h_B$ implies $a' \equiv b' \equiv b \mod 3$.

Assume $a' \equiv b' \equiv b \mod 3$ (so $p \equiv 1 \mod 9$). If $b \equiv 0 \mod 3$ then the same holds for b' thus $b = 3b' \equiv 0 \mod 9$; otherwise $b \equiv 1 \mod 3$ and the same holds for a' and b', which yields $a \equiv b (\equiv 4) \mod 9$. In both cases we get $3 \mid h_B$ by Proposition 4.

The second assertion is clear. □

One easily extends the former proof to show the extra characterization:

$$3 \mid h_B \Longleftrightarrow (\, a \equiv 1,\ b \equiv 0 \mod 9\,) \text{ or } (\, a \equiv b \equiv 4 \mod 9\,) \ .$$

We now deduce a result for the class group of the field K.

Corollary 4. *Suppose* ($p \equiv 1$ *and* $a \equiv b \mod 9$) *or* ($p \equiv 1$ *and* $b \equiv 0 \mod 9$), *then* 3 *divides the class number* h_K *of* K.

Proof. The Hilbert class field H_B of B is unramified over B of degree h_B. Since K/B is totally ramified above p by Proposition 3, it is linearly disjoint with H_B/B, hence the compositum KH_B is unramified of degree h_B above K. We get that $h_B \mid h_K$, so Proposition 4 yields the result. □

Reversing the argument, we can show the following result about the subfield $\mathbb{Q}(\sqrt[9]{\beta} + \sqrt[9]{\beta}^{-1})$ of K of minimal polynomial f_p defined in Proposition 2.

Proposition 5. *Suppose* $v_3(b) = 0$ *then the class group of* $K^{\langle\,\overline{\sigma}\,\rangle} = \mathbb{Q}(\sqrt[9]{\beta} + \sqrt[9]{\beta}^{-1})$ *contains a subgroup of order* 3.

Proof. By Proposition 3, the ramification group of the ideals above 3 in K is $\langle\,\overline{\sigma}^{\,2}\,\overline{\tau}\,\rangle$, so $K/K^{\langle\,\overline{\sigma}\,\rangle}$ is unramified above 3. Since $L/\mathbb{Q}(\zeta_9)$ (resp. $\mathbb{Q}(\zeta_9)/\mathbb{Q}$) is totally ramified (resp. unramified) above p, we deduce that the ramification group of the prime ideals above p in K is $\langle\,\overline{\tau}\,\rangle$. Hence $K/K^{\langle\,\overline{\sigma}\,\rangle}$ is unramified, and its Galois group, which is cyclic of order 3, is isomorphic to a subgroup of the class group of $K^{\langle\,\overline{\sigma}\,\rangle}$. □

6. Numerical instances

We have devised an algorithm to compute ramification groups in finite Galois extensions of $\mathbb{Q}$, based on the computation of valuations. This algorithm has been incorporated to the computer algebra system PARI/GP[P1], version 2.4.3, and is available as the GP function `idealramgroups`.

We now give the results of the computations — which agree with the results of the previous sections; then we briefly describe the algorithm.

6.1 The results

The next table presents examples of prime numbers p congruent to 1 modulo 3, which are the smallest ones corresponding to each entry in the table of Theorem 2 (the congruences appearing in the table are modulo 3). We give the ramification groups for the prime ideals above 3. All unspecified ramification groups are trivial.

p	61	7	31	307	2 203
$v_3(b)$	0 ($a' \equiv b'$)	0 ($a' \not\equiv b'$)	1	2	3
e	9	9	9	3	3
f	1	3	3	3	1
g	3	1	1	3	9
$3\mathcal{O}_K$	$\mathfrak{p}_1^9\mathfrak{p}_2^9\mathfrak{p}_3^9$	$\mathfrak{p}_1^9$	$\mathfrak{p}_1^9$	$\mathfrak{p}_1^3\mathfrak{p}_2^3\mathfrak{p}_3^3$	$\prod_{i=1}^{9}\mathfrak{p}_i^3$
$G_{-1}(\mathfrak{p}_i)$	$\langle\,\overline{\sigma}^{\,2}\,\overline{\tau}\,\rangle$	G	G	$\langle\,\overline{\sigma}\,,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,3i}\,\rangle$
$G_0(\mathfrak{p}_i)$	$\langle\,\overline{\sigma}^{\,2}\,\overline{\tau}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,2}\,\rangle$	$\langle\,\overline{\sigma}\,,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,3i}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,3i}\,\rangle$
$G_1(\mathfrak{p}_i)$	$\langle\,\overline{\sigma}^{\,2}\,\overline{\tau}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,2}\,\rangle$	$\langle\,\overline{\sigma}\,,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,3i}\,\rangle$	$\langle\,\overline{\sigma}\,\overline{\tau}^{\,3i}\,\rangle$
$G_2(\mathfrak{p}_i)$	$\langle\,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\tau}^{\,3}\,\rangle$			
$G_3(\mathfrak{p}_i)$	$\langle\,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\tau}^{\,3}\,\rangle$			
$G_4(\mathfrak{p}_i)$	$\langle\,\overline{\tau}^{\,3}\,\rangle$	$\langle\,\overline{\tau}^{\,3}\,\rangle$			

6.2 The algorithm

Let K be a Galois extension of $\mathbb{Q}$, G the Galois group of $K/\mathbb{Q}$, $\mathfrak{p}$ a prime ideal of K.

Let D be the decomposition group of $\mathfrak{p}$. The algorithm relies on the computation of the function ι_D from D to $\mathbb{Z}$ defined by the relation $\iota_D(\sigma) = k \geqslant 0$ if and only if $\sigma \in G_{k-1}$ and $\sigma \notin G_k$ (c.f. [S, VI]). We extend ι_D to G by setting $\iota_D(\sigma) = -1$ for all $\sigma \notin D$. Once this function is computed, the ramification groups can be easily identified.

Let $\pi \in \mathfrak{p}$ be a local uniformiser for $\mathfrak{p}$. For $\sigma \in G_0$, we have the identity $\iota_D(\sigma) = v_\mathfrak{p}(\sigma(\pi) - \pi)$ (*loc. cit.*) and we note that σ belongs to D if and only if $v_\mathfrak{p}(\sigma(\pi) - \pi) \geqslant 1$.

Algorithm 1. *Let K, G and $\mathfrak{p}$ as above. We assume that we can compute the valuation $v_\mathfrak{p}$ and that we know a local uniformiser π for $\mathfrak{p}$ and an element $x_\mathfrak{p} \in \mathcal{O}_K$ whose residue class $x_\mathfrak{p} \mod \mathfrak{p}$ generates the residual field $\mathcal{O}_K/\mathfrak{p}$. Then the following algorithm computes $\iota_D(\sigma)$ for any $\sigma \in G$.*

(i) Compute $v = v_\mathfrak{p}(\sigma(\pi) - \pi)$.

(ii) If $v = 0$ then $\sigma \notin D$ and $\iota_D(\sigma) = -1$.

(iii) Otherwise if $\sigma(x_\mathfrak{p}) \not\equiv x_\mathfrak{p} \mod \mathfrak{p}$ then $\sigma \notin G_0$ and $\iota_D(\sigma) = 0$.

(iv) Otherwise $\sigma \in G_0$ and $\iota_D(\sigma) = v$.

Once some values of ι_D are known it is usually possible to know some more for free by using the properties of ι_D:

- If $(\sigma, \tau) \in G \times D$ then $\iota_D(\tau^{-1}\sigma\tau) = \iota_D(\sigma)$.
- If $\sigma \in G$ and a is an integer coprime to the order of σ then $\iota_D(\sigma^a) = \iota_D(\sigma)$.

6.3 Class groups

Here is a table presenting the structure of the class group of K and of its bicubic bicyclic subextension $B = K^{\langle \overline{\tau}^3 \rangle}$, for the values of the parameter p congruent to 1 mod 3 in the range $[7, 307]$. The computations have been achieved using PARI/GP[P1]; the validity of the results relies on the General Riemann Hypothesis. All unspecified class groups are trivial.

p	a	b	a'	b'	$Cl(B)$	$Cl(K)$
7	-2	1	-1	0		
13	1	-2	0	-1		
19	4	**1**	**1**	0		3
31	-2	-3	-1	-1		
37	-5	**-2**	**-2**	-1		3
43	4	-3	1	-1		
61	**7**	**-2**	2	-1		3
67	**-8**	**1**	-3	0		3
73	**-5**	**4**	**-2**	**1**	3	9×3
79	-2	-5	-1	-2	2×2	2×2
97	7	4	2	1		
103	**10**	**1**	3	0		3
109	1	**6**	**0**	2		3
127	10	**-3**	**3**	-1	2×2	6×2
139	-8	-5	-3	-2		
151	**-2**	**7**	-1	2		3

p	a	b	a'	b'	$Cl(B)$	$Cl(K)$
157	7	6	2	−1	2×2	2×2
163	4	**7**	**1**	2	2×2	6×2
181	13	**−2**	**4**	−1		3
193	**1**	**−8**	0	−3		3
199	−14	**1**	**−5**	0		3
211	−8	7	−3	2	$2\times 2\times 2\times 2$	$2\times 2\times 2\times 2$
223	−14	−3	−5	−1		
229	−11	6	−4	2		
241	7	−8	2	−3	$2\times 2\times 2\times 2$	$2\times 2\times 2\times 2$
271	**−14**	**−5**	**−5**	**−2**	3×3	$9\times 3\times 3$
277	13	6	4	2	2×2	2×2
283	16	3	5	−1		
307	−8	**9**	**−3**	**3**	21	21

In the table we have bold faced the value of a when it is congruent to that of b modulo **9**, the value of a' when it is congruent to that of b modulo **3**; we have bold faced the value of b in any of these two cases, and that of b' when $b\equiv a'\equiv b' \mod 3$, which is equivalent to $3\mid h_B$ by Proposition 4. We then see that $3\mid h_K$ exactly when some of a,b,a',b' are bold faced. Consequently we are in a position to make the following conjecture. (Recall that $p\equiv 1 \mod 9$ is equivalent to $a'\equiv b \mod 3$.)

Conjecture 1. *Each of the following conditions implies* $v_3(h_K)\geqslant 1$ *:*

$$(i)\quad p\equiv 1 \mod 9\ ; \qquad (ii)\quad a\equiv b \mod 9\ .$$

This statement amounts to saying that the logical connective "and" in the first case of the statement of Corollary 4 can be replaced by "or". One may check in the preceding table that $v_3(h_K)\geqslant 1$ is in fact *equivalent* to ($p\equiv 1$ or $a\equiv b \mod 9$) for the values of the parameter in the range $[7,307]$.

On the other hand, the other condition that appears in the statement of Corollary 4, namely $b\equiv 0 \mod 9$, is not sufficient to get $v_3(h_K)\geqslant 1$, as is readily shown by the computation of the class group of K associated to the next value of p with $9\mid b$, 439, which yields a principal extension. We take advantage of the fact that the 3-power of the discriminant is the smallest possible in the case $9\mid b$ to present a few more computations that confirm our conjecture (even the equivalence is satisfied for the values of p with $9\mid b$ in the range $[307,1399]$).

p	a	b	a'	b'	$Cl(B)$	$Cl(K)$
307	−8	**9**	**−3**	**3**	21	21
439	−14	9	−5	3		
499	16	9	5	3	2×2	2×2
643	−20	9	−7	3		
727	22	9	7	3	2×2	2×2
919	−26	**9**	**−9**	**3**	39×3	39×3
997	−5	18	−2	6		
1021	7	18	2	6		
1093	−11	18	−4	6		
1399	34	9	11	3		$2\times 2\times 2\times 2$

References

A Allombert B., An efficient algorithm for the computation of Galois automorphisms, *Math. Comp.*, **73**, 245, 2001, 359–375.

C1 Cardano G., *Artis Magnæ, Sive de Regulis Algebraicis Liber Unus* (1570).

C2 Cohen H., *Advanced topics in Computational number theory*, Springer-Verlag, GTM **193** (2000).

E Erez B., The Galois structure of the square root of the inverse different, *Math. Z.*, **208** (1991), 239–255.

IR Ireland K., Rosen M., *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, GTM **84** (1990).

L1 Ledet A., *Brauer type embedding problems*, Fields Institute Monographs, **21**, American Mathematical Society (2005).

L2 Lemmermeyer F., *Reciprocity laws. From Euler to Eisenstein*, Springer Monographs in Mathematics (2000).

P1 The PARI Group, *PARI/GP*, `http://pari.math.u-bordeaux.fr/`, version `2.4.3`, 2010.

P2 Parry C.J., Bicyclic bicubic fields, *Can. J. Math.* **42**, No. 3, 491–507 (1990).

P3 Plans B., On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$., *Pacific J. Math.* , **215**, 2004, no. 2, 381–391.

S Serre J.P., *Corps locaux*, 3^e édition, Hermann, Paris (1968).

V Vinatier S., Une famille infinie d'extensions faiblement ramifiées, *Math. Nachr.*, **243** (2002), 165–187.

Bill Allombert Bill.Allombert@math.u-bordeaux1.fr
Université Bordeaux 1, 351 Cours de la Libération, F-33405 Talence cedex, FRANCE

Stéphane Vinatier stephane.vinatier@unilim.fr
XLIM - DMI, 123 avenue Albert Thomas, 87060 Limoges, France.

Chapitre 4

Bases normales auto-duales explicites pour les corps finis

Dans ce chapitre sont présentés deux travaux sur les corps finis : un article en collaboration avec F. Arnault et E. J. Pickett, intitulé *Construction of self-dual normal bases and their complexity* et paru à Finite Fields and their Applications, volume 18, année 2012, numéro 2, pages 458-472 ; et un article en préparation, inachevé, intitulé *The complexity of cyclotomic self-dual normal bases.*

4.1 Construction et complexité de bases normales auto-duales

La motivation du premier était d'explorer l'intérêt des bases normales auto-duales pour la multiplication dans les corps finis qui en possèdent. Dans son article paru en 2010 [Pic10], Erik Pickett avait trouvé un moyen de construire de telles bases en toute caractéristique et s'était fait l'écho de leur utilisation en cryptographie, ce qui m'avait intrigué. Il nous a vite paru clair que nous ne pourrions en savoir beaucoup plus sur cette question sans l'aide d'un spécialiste et nous avons demandé à mon collègue cryptographe limougeaud François Arnault de nous guider dans ce monde si étrange pour nous, ce qu'il a très gentiment accepté. Le plus gros du travail mathématique a finalement été de traduire la construction d'Erik, originellement présentée dans des algèbres de groupes, en termes de polynômes sur des corps finis, plus proches de l'implémentation qui était notre but. Ce qui nous a aussi rapproché de la littérature sur le sujet et nous a permis d'en utiliser certains résultats, notamment sur le groupe orthogonal-circulant, de changement de base normale auto-duale, qui permet de les retrouver toutes à partir d'une seule.

Nous avons ainsi pu vérifier expérimentalement, en caractéristique impaire, que les bases normales auto-duales atteignent souvent la complexité minimale des bases normales, comme cela avait déjà été remarqué en caractéristique paire. Cette complexité est le nombre de cœfficients non nuls dans la « table de multiplication » associée à la base normale, et traduit de façon simple la complexité de la multiplication de deux éléments exprimés dans cette base (la somme et le Frobenius sont très faciles à exécuter). C'est ainsi que nous avons finalement interprété l'utilité des bases normales auto-duales pour la cryptographie, par l'efficacité avec laquelle elles permettent, si elles sont bien choisies, d'exécuter les opérations arithmétiques dans les corps finis, avec l'avantage supplémentaire, par rapport aux bases normales, que leur table de multiplication est (très) symétrique, et peut donc être stockée dans moins d'espace, ce qui pourrait avoir un intérêt pratique dans certaines situations.

Il faut noter cependant que l'intérêt de la communauté mathématique pour les bases normales auto-duales a quelque peu décru depuis le passage au XXI^{e} siècle, ce qui pourrait laisser

penser que le gros des applications est plutôt derrière nous…

Qu'à cela ne tienne ! Les calculs effectués grâce aux algorithmes brièvement évoqués ci-dessus ont fait apparaître un certain nombre de phénomènes, que nous avons tenté d'expliquer au mieux. Le plus frappant était peut-être la répétition, dans la table dont les colonnes donnent la meilleure complexité en fonction du cardinal du corps de base, à degré fixé, de la même valeur, avec des exceptions. Il est vite apparu (je me rappelle à quel point Erik m'a épaté à cette occasion) qu'il pouvait s'agir des réductions locales d'une base auto-duale globale (d'une extension de $\mathbb{Q}$) aux premiers non décomposés dans l'extension. La suite après le premier article…

Construction of self-dual normal bases and their complexity

François Arnault, Erik Jarl Pickett and Stéphane Vinatier

Abstract

Recent work of Pickett has given a construction of self-dual normal bases for extensions of finite fields, whenever they exist. In this article we present these results in an explicit and constructive manner and apply them, through computer search, to identify the lowest complexity of self-dual normal bases for extensions of low degree. Comparisons to similar searches amongst normal bases show that the lowest complexity is often achieved from a self-dual normal basis.

Introduction

Let q be a power of a prime, n an integer, and let $\mathbb{F}_q$ be the field of q elements. The Galois group G of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic group, generated by the Frobenius automorphism $\phi : x \mapsto x^q$.

A basis for $\mathbb{F}_{q^n}/\mathbb{F}_q$ consisting of the orbit $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ of a single element α under the action of the Frobenius is known as a normal basis. We call it the *normal basis generated by* α (note that in this paper we consider the basis generated by any other conjugate of α to be different, as its elements are in a different order). Using such a basis, both exponentiation by q and computation of traces are straightforward operations; the former being simply a cyclic shift of coordinates. The difficulty of multiplying two elements written as linear combinations of the conjugates of α is measured by the so-called *complexity* of α, defined as the number of non zero entries in the multiplication-by-α matrix [MBG+93, §4.1]. It has been shown in [MOVW89] to be at least $2n-1$, in which case the basis is called *optimal*, but this occurs only for very special values of n [GL92].

The search for normal bases with low complexity has taken two complementary directions. On the theoretical side, several authors have attempted to build them either from roots of unity in larger extensions, using Gauss periods [ABV89, CGPT11, GL92, LF09] or traces of optimal normal bases [CGPT08, CGPT11], again with some limitations on the degree; or from the extension itself, using division points of a torus [BGM94, Gao93] or of an elliptic curve [CL09]. In the latter case the authors show that fast arithmetic can be implemented using their bases, as was also shown to be the case for normal bases generated by Gauss periods in [GvzGPS00].

More precisely, the normal basis generated by α is said to be self-dual if $\mathrm{Tr}(\alpha^{q^i}\alpha^{q^j}) = \delta_{i,j}$ for $0 \leqslant i, j \leqslant n-1$, where Tr is the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and δ is the Kronecker delta. Its complexity is the number of non zero entries in the matrix:

$$\left(\mathrm{Tr}(\alpha\alpha^{q^i}\alpha^{q^j})\right)_{0\leqslant i,j\leqslant n-1} .$$

Self-dual normal bases are useful for arithmetic and Fourier transform, and have applications in coding theory and cryptography. Contrary to normal bases, not all extensions of finite fields admit self-dual

2000 Mathematics Subject Classification ????

normal bases, but the existence conditions, recalled in Theorem 1 below, are mild. The theoretical techniques used to construct normal bases with low complexity sometimes yield self-dual normal bases, see for example [Gao93, §5.4] or [BGM94, §5], [GvzGPS00, Corollary 3.5], [CGPT08, Theorem 5], [NNMU08].

On the experimental side, exhaustive searches of all normal bases of a given extension have been carried out. Mullin, Onyszchuk, Vanstone and Wilson [MOVW89] have given a first list of lowest complexities in degree less than 30 over $\mathbb{F}_2$. This list was extended up to degree 33 by Geiselmann [Jun93, Table 5.1]. In odd characteristic, Blake, Gao and Mullin [BGM94] computed the lowest complexities of normal bases for a handful of small degree extensions. Recently, Masuda, Moura, Panario and Thomson [MMPT08] have reached degree 39 over $\mathbb{F}_2$ and given appealing statistics and conjectures about the distribution of complexities. It is clear that the cost of the exhaustive enumeration of the elements of $\mathbb{F}_{2^n}$ used to look for normal basis generators is a severe limitation to their method when the degree grows. On the other hand, their Table 4 shows that the minimal complexity for normal bases is very often reached by so-called self-dual bases (in all degrees not divisible by 4 up to 35 apart from 7, 10, 21). Restricting to self-dual normal bases enables one to push computations further; Geiselmann [Jun93] was indeed able to compute the lowest complexity for self-dual normal bases over $\mathbb{F}_2$ up to degree 47. Comparing his results and [MMPT08, Table 5], we see that the best found complexity for normal bases in degree over 40, obtained by theoretical constructions or random search, is also reached by a self-dual normal basis for odd degrees up to 47.

In this paper we focus on the experimental side and give the lowest complexity of self-dual normal bases in various characteristics and degrees. At present, the only known strategy to reach this goal is to compute the complexity of all the self-dual normal bases of the extension (unless it admits an optimal self-dual normal basis, which is easily predictable, see [GvzGPS00, §3] or [LS06, Theorem 2] for a compact statement). In order to do so, we first construct a self-dual normal basis for the extension, then act on it by the *orthogonal circulant* group, namely the group of change of self-dual normal basis matrices. This group has been extensively studied, with accurate descriptions being given in [BV78, JBG94, Mac71]. Its size is in $O(q^{n/2})$ (see Remark 2.5 below), roughly the square root of the number of normal bases in view of [MBG$^+$93, Corollary 4.14]. It follows that exhaustive enumeration of self-dual normal bases is easier than that of normal bases. We shall restrict ourselves to extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ which are either *semi-simple* (the degree n prime to the characteristic p) or *ramified* (n a power of p), the description of the orthogonal circulant group in the "mixed" case being a bit more elaborate.

We now describe our work more precisely. First we recall the necessary and sufficient conditions for the existence of self-dual normal bases [LW88].

Theorem 1 Lempel-Weinberger. *The extension field $\mathbb{F}_{q^n}/\mathbb{F}_q$ has a self-dual normal basis if and only if either the degree n is odd, or $n \equiv 2$ modulo 4 and q is even.*

The existence proof in [LW88] is constructive in the sense that, given a normal basis for the extension, it describes a procedure to transform it into a self-dual normal basis. Wang [Wan89] proposed another transformation procedure when $q = 2$ and n is odd, involving solving a system of equations. Poli [Pol95] extended Wang's method to deal with the general characteristic 2 case. Recently, Pickett [Pic10] designed a construction that extends the former ones to the odd characteristic case, dealing separately with the semi-simple case and the ramified case.

The construction of a normal basis for a given extension is well known and widely implemented. Therefore, the methods described above enable one to construct a self-dual normal basis under the existence conditions of Theorem 1. To our knowledge, this has not been implemented before, except in the restrictive case in which Wang's method applies. In this paper we apply Pickett's construction to compute a self-dual normal basis of a given extension whenever it exists. Note that for this first goal, the

method in [LW88] is simpler and faster, but most of the computations involved in Pickett's construction must be implemented if one wants to compute the action of the orthogonal circulant group as well.

The criterion used in [Wan89] to determine which changes of basis are appropriate has been generalised to any characteristic and degree, see [Jun93, Lemma 5.5.3], where it is expressed in terms of circulant matrices. Here we restate it in terms of the group algebra $\mathbb{F}_q[G]$ as in [Pic10]. Conjugation $u \mapsto \overline{u}$ in $\mathbb{F}_q[G]$ is the $\mathbb{F}_q$-algebra automorphism obtained from $g \mapsto g^{-1}$ for all $g \in G$; if $u = \sum_{k=0}^{n-1} u_k \phi^k \in \mathbb{F}_q[G]$ and $\alpha \in \mathbb{F}_{q^n}$, we put $u \circ \alpha = \sum_{k=0}^{n-1} u_k \phi^k(\alpha) \in \mathbb{F}_{q^n}$.

Theorem 2. *Assume that α is a generator of a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let*

$$R = \sum_{g \in G} \mathrm{Tr}\left(\alpha g(\alpha)\right) g \ \in \ \mathbb{F}_q[G] \ . \tag{1}$$

Any $v \in \mathbb{F}_q[G]$ such that $v\overline{v} = R$ is invertible, and the map $v \mapsto v^{-1} \circ \alpha$ is a one-to-one correspondence between the set of solutions of the equation $v\overline{v} = R$ in $\mathbb{F}_q$ and the set of elements of $\mathbb{F}_{q^n}$ that generate a self-dual normal basis.

In Section 1 we first explain how this result can be deduced from the statement on circulant matrices [Jun93, Lemma 5.5.3]. Our main interest is in implementing Pickett's method as an algorithm, and since the language he uses to describe his construction of a solution of the equation $v\overline{v} = R$ in [Pic10, §3] is quite elaborate — his framework is wider than ours — we reformulate it in terms of the polynomial ring $\mathbb{F}_q[X]/(X^n - 1)$; the resulting algorithm to compute a self-dual normal basis is described in the last section. We remark that this construction gives an alternative proof of the sufficiency of the conditions of Theorem 1; for interest we give a proof of their necessity, mainly based on Theorem 2, and simpler than the original (see [Jun93, Propositions 4.3.4 and 5.2.2]).

Section 2 deals with the orthogonal circulant group $O(n, q)$. Its elements are the $n \times n$ matrices P over $\mathbb{F}_q$ that are circulant ($P_{i+k \bmod n, j+k \bmod n} = P_{i,j}$ for $0 \leqslant i, j, k \leqslant n-1$) and orthogonal ($P^t \cdot P = I$, where P^t is the transpose matrix of P and I the identity $n \times n$ matrix). It follows from Theorem 2 that $O(n, q)$ is isomorphic to the subgroup of $\mathbb{F}_q[G]^\times$ consisting of the solutions of the equation $v\overline{v} = 1$. In both the semi-simple and the ramified case we indicate how this equation can be solved; the resulting algorithms are described in the last section. Doing so we recover the number of self-dual normal bases, as derived in [JBG94, JMV90] from MacWilliams' results about the orthogonal circulant group [Mac71] (see [Jun93, 5.3] for a summary). In the ramified (and odd characteristic) case our construction is a variation, adjusted to our situation, of MacWilliams' iterative construction; we also present a new explicit formula for the solutions.

In Section 3 we present our algorithms, experimental results and conclusions. For semi-simple extensions in odd characteristic, the lowest complexity we find is close to that obtained for normal bases from exhaustive computer search [BGM94] or from theoretical constructions [LF09], as this was already the case in even characteristic. We also observe an interesting behaviour under base field extension. When the extension is of degree p in odd characteristic p we recover the basis with very low complexity $3p-2$ described in [BGM94].

1. Construction of a self-dual normal basis

Our algorithm to find a self-dual normal basis relies on the interpretation in terms of polynomial rings of Pickett's construction of a solution v of the equation $v\overline{v} = R$ of Theorem 2 (under the necessary conditions of Theorem 1). The majority of this section is devoted to presenting this interpretation. First, however, we deduce Theorem 2 from statements in terms of circulant matrices. At the end of the section

we show how to deduce the necessity of the conditions of Theorem 1 from Theorem 2.

Proof of Theorem 2. Consider the one-to-one correspondence between $\mathbb{F}_q[G]$ and circulant $n \times n$ matrices over $\mathbb{F}_q$, given by

$$v = \sum_{j=0}^{n-1} \rho_j \phi^j \in \mathbb{F}_q[G] \mapsto C_v = \left(\rho_{j-i \bmod n}\right)_{0 \leqslant i,j \leqslant n-1} \ . \tag{2}$$

One has $C_1 = I$ and, for any $v, w \in \mathbb{F}_q[G]$, $C_v \cdot C_w = C_{vw}$, so (2) yields a group isomorphism between $\mathbb{F}_q[G]^\times$ and the abelian group of invertible circulant $n \times n$ matrices over $\mathbb{F}_q$. Note that the matrix $C_R = \left(\mathrm{Tr}(\alpha^{q^i+q^j})\right)$ is invertible since α generates a normal basis, see [MBG+93, Corollary 1.3]. Hence, $R \in \mathbb{F}_q[G]^\times$ and $v\overline{v} = R$ implies v invertible as well.

Moreover one has $C_{\overline{v}} = (C_v)^t$. It follows that the equation $v\overline{v} = R$ is equivalent to

$$C_v \cdot (C_v)^t = \left(\mathrm{Tr}(\alpha^{q^i+q^j})\right)_{0 \leqslant i,j \leqslant n-1} \ . \tag{3}$$

For $x \in \mathbb{F}_{q^n}$, let $[x]$ denote the $n \times n$ matrix whose j-th column, $0 \leqslant j \leqslant n-1$, consists of the coordinates of x^{q^j} in a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. Then one has, for any $v \in \mathbb{F}_q[G]$, $x \in \mathbb{F}_{q^n}$:

$$[v \circ x] = [x] \cdot C_v \ .$$

Let P be some invertible $n \times n$ matrix over $\mathbb{F}_q$, then the columns of $B = [\alpha]P$ are the coordinates in the fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ of a normal basis if and only if P is a circulant matrix, see [Jun93, Lemma 3.1.3]. Further, for such a P, its inverse P^{-1} is also circulant and from [Jun93, Lemma 5.5.3] we know that the columns of B form a self-dual normal basis if and only if

$$P^{-1} \cdot (P^{-1})^t = \left(\mathrm{Tr}(\alpha^{q^i+q^j})\right)_{0 \leqslant i,j \leqslant n-1} \ . \tag{4}$$

If $v\overline{v} = R$, then C_v is circulant invertible and $(C_v)^{-1} = C_{v^{-1}}$ satisfies (4). Hence $B = [\alpha]C_{v^{-1}} = [v^{-1} \circ \alpha]$ is a self-dual normal basis. If β generates a self-dual normal basis, let P be such that $[\beta] = [\alpha]P$, then P is circulant and so is its inverse. By (3) the element $v \in \mathbb{F}_q[G]$ such that $P^{-1} = C_v$ satisfies $v\overline{v} = R$. These two maps are clearly mutual inverses, which completes the proof. □

1.1 Interpretation of Pickett's construction in terms of polynomial rings

The Galois group G of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic of order n and generated by the Frobenius ϕ, so we may identify the $\mathbb{F}_q$-algebras $\mathbb{F}_q[G]$ and $\mathbb{F}_q[X]/(X^n - 1)$ through the isomorphism mapping ϕ to X.

Write $n = p^e n_1$, where p is the characteristic of $\mathbb{F}_q$ and n_1 is prime to p. We take advantage of the following result [Jun93, Theorems 3.3.13 and 5.1.9] to split the extension into two parts.

Lemma 1.1. *Let m, n be two co-prime integers. Suppose α (resp. β) is a generator of a self-dual normal basis of $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_{q^n}$) over $\mathbb{F}_q$, then $\alpha\beta$ is a generator of a self-dual normal basis of the compositum $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. Moreover, the complexity of $\alpha\beta$ is the product of the complexities of α and of β.*

By the former result, we may deal separately with the two cases $n = p^e$ which we call the ramified case, and n co-prime to p, the so-called semi-simple case. We show how to construct a solution v of the equation $v\overline{v} = R$ of Theorem 2 in each of these two cases, under the existence conditions of a self-dual normal basis of Theorem 1. Multiplying the bases obtained this way then yields self-dual normal bases for the extensions with "mixed degree" $n = n_1 p^e$ with $n_1 \geqslant 2$ and $e \geqslant 1$.

1.1.1 *The ramified case ($n = p^e$)* In this case, the algebra $\mathbb{F}_q[G]$ is isomorphic to $\mathbb{F}_q[X]/(X-1)^n$. Let $\epsilon : \mathbb{F}_q[G] \to \mathbb{F}_q$ be the augmentation map given by $\epsilon(\sum_{k=0}^{n-1} a_k\phi^k) = \sum_{k=0}^{n-1} a_k$. This is a homomorphism of $\mathbb{F}_q$-algebras whose kernel is a codimension 1 subspace of $\mathbb{F}_q[G]$. Further $\epsilon(\sum_{k=0}^{n-1} a_k\phi^k) = 0$ implies $\sum_{k=0}^{n-1} a_k\phi^k = \sum_{k=0}^{n-1} a_k(\phi^k - 1)$, and therefore the kernel is $(\phi-1)\mathbb{F}_q[G]$. Invertible elements in $\mathbb{F}_q[G]$ are those which have non-zero image under the map ϵ (because invertible modulo $(X-1)^n$ means invertible modulo $X-1$), hence the group $\mathbb{F}_q[G]^\times$ has order $q^{n-1}(q-1)$. In fact, it is the direct product of $\mathbb{F}_q^\times$ by $U = 1 + (\phi-1)\mathbb{F}_q[G]$, the inverse image of 1 under the map ϵ.

Under the necessary conditions of Theorem 1, we have two cases to consider.

Proposition 1.2. *Let p be the characteristic of $\mathbb{F}_q$. If $p = n = 2$, $\beta \in \mathbb{F}_{q^2}$ generates a self-dual normal basis if and only if $\mathrm{Tr}(\beta) = 1$. If p is odd and $n = p^e$, there exists $\omega \in \mathbb{F}_q[G]$ such that $\omega^2 = R$. Furthermore, $\omega = \overline{\omega}$.*

Proof. The even characteristic case is straightforward. We proceed with the odd characteristic case. Recall that $R \in \mathbb{F}_q[G]^\times$ and note that $\overline{R} = R$, which is clear from (1). One can easily see that $\epsilon(R) = \mathrm{Tr}(\alpha)^2$ (detailed in the proof of Lemma 1.6 below), so that the decomposition of R in the direct product $\mathbb{F}_q^\times \times U$ is $R = \mathrm{Tr}(\alpha)^2 \cdot (1 + (\phi-1)R')$ for some $R' \in \mathbb{F}_q[G]$. The second factor is also a square as it belongs to the group U which is of odd order, hence $R = \omega^2$ for some ω. Further $\overline{R} = R$ implies $\overline{\omega}^2 = \omega^2$, so that $\overline{\omega}/\omega$ is a square root of 1 living in the group U of odd order. Thus $\overline{\omega} = \omega$. □

1.1.2 *The semi-simple case ($\gcd(n, q) = 1$)* We assume that n is odd to fit with the conditions of Theorem 1 (but q could be odd or even). The polynomial $X^n - 1$ is square free and has monic irreducible factors over $\mathbb{F}_q$:

$$X^n - 1 = \prod_{i=1}^{\sigma} f_i(X) \prod_{j=1}^{\tau} g_j(X) \cdot g_j^*(X) \tag{5}$$

where g_j^* denotes the reciprocal polynomial (up to a constant) of g_j and where the f_i are the self-reciprocal (also up to a constant) irreducible factors. We will now express the equation $R = v\overline{v}$ in this decomposition, solve it, and then lift back the solution to $\mathbb{F}_q[G]$.

Let m be the order of q modulo n. The field $\mathbb{F}_{q^m}$ contains a primitive n-th root ζ of 1. On the set $\{0, \ldots, n-1\}$ we define the *cyclotomic equivalence relation: $s \sim s'$* if there exists k such that $s \equiv q^k s' \mod n$. Note that 0 forms a class on its own and that the integers prime to n belong to classes with the same cardinality equal to the order of q modulo n. Namely, since n and q are co-prime, the cyclotomic equivalence relation restricts to $(\mathbb{Z}/n\mathbb{Z})^\times$ and for s, s' invertible modulo n, $s \sim s'$ if and only if s and s' belong to the same coset in $(\mathbb{Z}/n\mathbb{Z})^\times/\langle q\rangle$.

The following proposition justifies the terminology. Recall that by "self-reciprocal", we mean "self-reciprocal up to a constant factor".

Proposition 1.3. *(a) If ζ^s is a root of an irreducible factor of $X^n - 1$, then the other roots are the $\zeta^{s'}$ where $s' \sim s$.*
(b) The ζ^s such that $s \sim (n-s)$ are roots of a self-reciprocal factor f_i. The ζ^s such that $s \not\sim n - s$ are roots of a non self-reciprocal factor g_j.
(c) The number of cyclotomic classes is equal to the number $\sigma + 2\tau$ of irreducible factors of $X^n - 1$.
(d) The self-reciprocal factors f_i have even degree, except $f_1 = X - 1$.

Proof. (a), (b), (c) are clear. Let us prove (d). If ζ^s is a root of an f_i, then ζ^{n-s} is also a root. If we exclude the case $s = 0$ corresponding to the factor $X - 1$, the two roots ζ^s and ζ^{n-s} are distinct, because n is odd. Hence f_i has en even number of roots in an algebraic closure. □

From the Chinese Remainder Theorem, the algebra $\mathbb{F}_q[X]/(X^n-1)$ is isomorphic to a product of $\sigma+2\tau$ fields:

$$\frac{\mathbb{F}_q[X]}{(X^n-1)} \simeq \prod_{i=1}^{\sigma} \frac{\mathbb{F}_q[X]}{\big(f_i(X)\big)} \times \prod_{j=1}^{\tau} \left(\frac{\mathbb{F}_q[X]}{\big(g_j(X)\big)} \times \frac{\mathbb{F}_q[X]}{\big(g_j^*(X)\big)} \right). \tag{6}$$

Each factor in the RHS of this equation is a an extension of $\mathbb{F}_q$ contained in $\mathbb{F}_{q^m}$ (recall m is the order of q modulo n). The evaluation map $u(X) \in \mathbb{F}_q[X]/(f) \mapsto u(\zeta^s) \in \mathbb{F}_q(\zeta^s)$, where f is an irreducible factor of X^n-1 and $s \in \{0,\dots,n-1\}$ is such that $f(\zeta^s)=0$, is a field isomorphism. We obtain the following result:

Proposition 1.4. *Let S be a set of representatives of cyclotomic classes. The map*

$$\begin{cases} \mathbb{F}_q[X]/(X^n-1) & \longrightarrow \prod_{s\in S} \mathbb{F}_q(\zeta^s) \\ u(X) & \longmapsto \big(u(\zeta^s)\big)_{s\in S} \end{cases} \tag{7}$$

is an $\mathbb{F}_q$-algebra isomorphism.

For practical reasons (mainly to deal with square matrices), we also consider the map $\mathcal{F}$ (a Fourier Transform)

$$\mathcal{F} : \begin{cases} \mathbb{F}_q[X]/(X^n-1) & \longrightarrow (\mathbb{F}_{q^m})^n \\ u(X) & \longmapsto \big(u(\zeta^s)\big)_{0\leqslant s\leqslant n-1} \end{cases} \tag{8}$$

which is a homomorphism of $\mathbb{F}_q$-algebras, with matrix $F(\zeta)=(\zeta^{ij})_{0\leqslant i,j\leqslant n-1}$. Compared with isomorphism (7), we now compute a component at every $0 \leqslant s \leqslant n-1$; the components corresponding to indices in the same coset under $\sim$ are cyclically permuted when applying the Frobenius ϕ.

We note the following easy but useful relation involving the matrices $F(\zeta)$ and $F(\zeta^{-1})=(\zeta^{-ji})_{0\leqslant i,j\leqslant n-1}$.

Lemma 1.5. *We have, with the previous notation, $F(\zeta^{-1})F(\zeta)=nI$.*

As a consequence, the following linear map $\overline{\mathcal{F}}$, with matrix $F(\zeta^{-1})$, can be used to compute the inverse of $\mathcal{F}$.

$$\overline{\mathcal{F}} : \begin{cases} (\mathbb{F}_{q^m})^n & \longrightarrow \mathbb{F}_{q^m}[X]/(X^n-1) \\ (r_0,\dots,r_{n-1}) & \longmapsto \sum_{t=0}^{n-1} u_t X^t \quad \text{where } u_t = \sum_{i=0}^{n-1} r_i \zeta^{-ti} \ . \end{cases} \tag{9}$$

This is because $\overline{\mathcal{F}}\big(\mathcal{F}(u)\big) = nu$ for each $u \in \mathbb{F}_q[X]/(X^n-1)$.

The idea here is to express R as an element of the RHS of (7), to solve the equation in each component, and to bring back the solution to $\mathbb{F}_q[X]/(X^n-1)$. The conjugation map, induced by $X \mapsto X^{n-1}$ in $\mathbb{F}_q[X]/(X^n-1)$ is given by $\zeta \mapsto \zeta^{-1}$ and will sometimes be denoted by J in the RHS of (7).

Let R be as in Theorem 2. The s-coordinate of $\mathcal{F}(R)$ is $R_s = \sum_{i=0}^{n-1} \mathrm{Tr}(\alpha^{1+q^i})\zeta^{si}$.

We begin with the cyclotomic class $s=0$. Here, $\mathbb{F}_q(\zeta^s)=\mathbb{F}_q$ and the conjugation map J acts trivially. Note that $R_0=\epsilon(R)$.

Lemma 1.6 3.5 in [Pic10]. *With $v_0=\mathrm{Tr}(\alpha)$, we have $v_0\overline{v_0}=R_0$.*

Proof. We have $J\big(\mathrm{Tr}(\alpha)\big)=\mathrm{Tr}(\alpha)$ and

$$\mathrm{Tr}(\alpha)^2 = \Big(\sum_{i=0}^{n-1} \alpha^{q^i}\Big)^2 = \sum_{i,j=0}^{n-1} \alpha^{q^i+q^j} = \sum_{i,k=0}^{n-1} \alpha^{q^i(1+q^k)} = \sum_{k=0}^{n-1} \mathrm{Tr}(\alpha^{1+q^k}) = R_0.$$

□

We now consider the cyclotomic classes s such that $s \not\sim n - s$.

Lemma 1.7 3.6 in [Pic10]. *Let $s' \in S$ such that $s' \sim n - s$. We have $R_s = R_{s'}$. Putting $v_{s,s'} = (R_s, 1) \in \mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{s'})$, we have $v_{s,s'}\overline{v_{s,s'}} = (R_s, R_s)$.*

Proof. The conjugation map J exchanges coordinates in $\mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{s'})$: $J(u, u^*) = (u^*, u)$. As R is invariant by conjugation, we have $R_s = R_{s'}$. Therefore $v_{s,s'}J(v_{s,s'}) = (R_s, 1)(1, R_s) = (R_s, R_s)$. □

We finally deal with the cyclotomic classes s such that $s \neq 0$ and $s \sim n - s$.

Lemma 1.8 3.7 in [Pic10]. *Let $s \in S$ such that $0 \neq s$ and $s \sim n - s$. Then the field $\mathbb{F}_q(\zeta^s)$ is stable under the conjugation map J, and we denote by $\mathbb{F}_q(\zeta^s)^J$ the fixed subfield. Furthermore R_s (resp. $-R_s$) has a square root u (resp. u') in $\mathbb{F}_q(\zeta^s)$. We consider three cases:*

(a) If $u \in \mathbb{F}_q(\zeta^s)^J$, then $v_s = u$ satisfies $v_s\overline{v_s} = R_s$;

(b) If $u' \notin \mathbb{F}_q(\zeta^s)^J$, then $v_s = u'$ satisfies $v_s\overline{v_s} = R_s$;

(c) If $u \notin \mathbb{F}_q(\zeta^s)^J$ and $u' \in \mathbb{F}_q(\zeta^s)^J$, then there exists an integer n such that $-n$ is a non-zero square η^2 modulo the characteristic p of $\mathbb{F}_q$, but $-(n-1)$ is not a square modulo p, and there exists an integer ν such that $\nu^2 \equiv n - 1$ modulo p. We put $v_s = (\nu u + u')/\eta$, then $v_s\overline{v_s} = R_s$.

Proof. From Proposition 1.3, the field $\mathbb{F}_q(\zeta^s)$ is stable under J and of even degree over $\mathbb{F}_q$. Furthermore, we have $\overline{\zeta^s} = \zeta^{-s} \neq \zeta^s$ because n is odd, hence J restricted to $\mathbb{F}_q(\zeta^s)$ is an order 2 field automorphism. By Galois theory $\mathbb{F}_q(\zeta^s)^J$ is the unique index 2 subextension of $\mathbb{F}_q(\zeta^s)/\mathbb{F}_q$. Moreover, $\mathbb{F}_q(\zeta^s)$ is the only degree 2 extension of $\mathbb{F}_q(\zeta^s)^J$ in a given algebraic closure. It follows that every element of $\mathbb{F}_q(\zeta^s)^J$ is a square in $\mathbb{F}_q(\zeta^s)$. Since R_s and $-R_s$ are both invariant under J, the existence of their square roots u and u' in $\mathbb{F}_q(\zeta^s)$ is proved.

If $\overline{u} = u$, namely in case (a), then $u\overline{u} = u^2 = R_s$. Note that the condition $u \in \mathbb{F}_q(\zeta^s)^J$ is automatically fulfilled in characteristic 2, since the Frobenius from the prime field $\mathbb{F}_2$ is an automorphism of $\mathbb{F}_q(\zeta^s)^J$ in that case. The same argument shows that q has to be odd in cases (b) and (c). If $\overline{u'} \neq u'$, namely in case (b), then $\overline{u'} = -u'$ and $u'\overline{u'} = -u'^2 = R_s$. Suppose now (case c) that $\overline{u} = -u$ and $\overline{u'} = u'$. As $-1 = -R_s/R_s$, we know that -1 is not a square in $\mathbb{F}_q(\zeta^s)^J$, nor in $\mathbb{F}_p$. Hence the first $n > 1$ such that $-n$ is a square modulo p exists and satisfies the required conditions. Also, because neither -1 nor $-(n-1)$ are squares modulo p, there exists an integer ν such that $\nu^2 \equiv (n-1)$ modulo p. Taking the residues of η and ν modulo p, we have $\overline{\eta} = \eta$ and $\overline{\nu} = \nu$ because $\mathbb{F}_p \subseteq \mathbb{F}_q(\zeta^s)^J$. With $v_s = (\nu u + u')/\eta$, we have $\overline{v_s} = (-\nu u + u')/\eta$ and it follows that $v_s\overline{v_s} = (-\nu^2 u^2 + u'^2)/\eta^2 = (-(n-1)R_s - R_s)/(-n) = R_s$. □

We have solved the equation $v_s\overline{v_s} = R_s$ for every cyclotomic class s, thus by the $\mathbb{F}_q$-algebra isomorphism (7) we get a solution $v \in \mathbb{F}_q[G]$ of the equation $v\overline{v} = R$.

1.2 The necessity of the conditions of Theorem 1

If α is a generator of a self-dual normal basis of $\mathbb{F}_{q^{nm}}$ over $\mathbb{F}_q$, then $\mathrm{Tr}_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^n}}(\alpha)$ is a generator of a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, see [Pic10, Lemma 4.3]. Therefore, to prove the necessity of the conditions in Theorem 1 we need just consider the cases $\mathbb{F}_{q^2}/\mathbb{F}_q$ for q odd and $\mathbb{F}_{q^4}/\mathbb{F}_q$ for q even.

When q is odd, $\mathrm{Tr}(\alpha\alpha^q) = 2N(\alpha)$ for any $\alpha \in \mathbb{F}_{q^2}$, where $N(\alpha)$ denotes the norm of α in the extension, hence $\mathrm{Tr}(\alpha\alpha^q) = 0$ would imply $\alpha = 0$.

Let q be even, and assume for contradiction that there exists a normal basis generator α of $\mathbb{F}_{q^4}/\mathbb{F}_q$ and an element $v \in \mathbb{F}_q[G]$ such that $v\overline{v} = \mathrm{Tr}(\alpha^2) + \mathrm{Tr}(\alpha\alpha^q)\phi + \mathrm{Tr}(\alpha\alpha^{q^2})\phi^2 + \mathrm{Tr}(\alpha\alpha^{q^3})\phi^3$. Note that

$\mathrm{Tr}(\alpha\alpha^{q^3}) = \mathrm{Tr}(\alpha\alpha^q)$ and $\mathrm{Tr}(\alpha\alpha^{q^2}) = 2\,\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\left(N_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}(\alpha)\right) = 0$. Writing $v = a + b\phi + c\phi^2 + d\phi^3$ with $a, b, c, d \in \mathbb{F}_q$ and letting $\beta = \alpha + \alpha^{q^2}$, we easily get the equations:

$$a + b + c + d = \mathrm{Tr}(\alpha) = \beta + \beta^q, \quad (a + c)(b + d) = \mathrm{Tr}(\alpha\alpha^q) = \beta\beta^q.$$

It follows that $\{\beta, \beta^q\} = \{a + c, b + d\}$, namely $\beta \in \mathbb{F}_q$, which is impossible since it would imply $\alpha + \alpha^{q^2} = \alpha^q + \alpha^{q^3}$, contradicting the fact that α generates a normal basis. The result now follows using Theorem 2.

2. Change of self-dual normal basis

The orthogonal circulant group $O(n, q)$ can be seen abstractly as the group of vector space automorphisms that map a self-dual normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$ to another one. Once a vector space basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ has been fixed, it identifies with the more concrete group of orthogonal and circulant $n \times n$ matrices with entries in $\mathbb{F}_q$. We now give a third interpretation in terms of the group algebra $\mathbb{F}_q[G]$. Our result, which is essentially a different formulation of the "key" lemmas 2 and 3 of [JMV90], is an immediate consequence of Theorem 2 and the observations that if α generates a self-dual normal basis, then $R = 1$, and that if $v\overline{v} = 1$, then $v^{-1} = \overline{v}$.

Corollary 2.1. *Let α generate a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The map $v \mapsto \overline{v} \circ \alpha$ is an isomorphism between the group of solutions of the equation $v\overline{v} = 1$ in $\mathbb{F}_q[G]$ and the group of elements of $\mathbb{F}_{q^n}$ that generate a self-dual normal basis.*

It follows that computing all self-dual normal bases from one is equivalent to finding all the solutions $v \in \mathbb{F}_q[G]^\times$ of the equation $v\overline{v} = 1$. We devote the rest of this section to explain how this equation can be solved, first in the semi-simple case and then in the ramified case.

2.1 The semi-simple case

The decomposition (7) from Section 1 is useful to find the solutions of the equation $v\overline{v} = 1$. Let $V(X) \in \mathbb{F}_q[X]/(X^n - 1)$.

Proposition 2.2. *The polynomial $V(X)$ satisfies the equation $V(X)V(X^{n-1}) = 1$ modulo $X^n - 1$ if and only if the following conditions hold:*

$$\begin{cases} V(1) = \pm 1 & \text{(case } s = 0\text{)}, \\ V(\zeta^s)V(\zeta^{-s}) = 1 & \text{for } s \not\sim n - s, \\ V(\zeta^s)^{q^{r/2}+1} = 1 & \text{for } 0 \neq s \sim n - s, \text{ where } r \text{ is such that } \mathbb{F}_q(\zeta^s) = \mathbb{F}_{q^r}. \end{cases}$$

Note that r is the degree of the irreducible factor f_i of $X^n - 1$ such that $f_i(\zeta^s) = 0$.

Proof. The component at $s = 0$ is $V(1)$ and the equation we need to solve in $\mathbb{F}_q(\zeta^0) = \mathbb{F}_q$ is simply $V(1)^2 = 1$ because the action of conjugation in $\mathbb{F}_q$ is trivial.

For $s \not\sim n - s$, we have to consider the product $\mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{-s})$. We have seen in the proof of Lemma 1.7 that conjugation swaps coordinates in these two factors. The solutions are the powers of (g_s, g_s^{-1}) where g_s is any primitive element of the $\mathbb{F}_q(\zeta^s)$.

For $0 \neq s \sim n - s$, we have seen in the proof of Lemma 1.8 that the set of invariants under conjugation J is the subfield $\mathbb{F}_{q^{r/2}}$ of $\mathbb{F}_{q^r} = \mathbb{F}_q(\zeta^s)$. Conjugation J is an $\mathbb{F}_{q^{r/2}}$-automorphism of $\mathbb{F}_{q^r}$ of order 2, hence $J(x) = x^{q^{r/2}}$ for $x \in \mathbb{F}_{q^r}$. The equation we want to solve can be written $x^{q^{r/2}+1} = 1$. Note that $q^{r/2} + 1$ divides $q^r - 1$ so we find exactly $q^{r/2} + 1$ solutions, generated by any element of order $q^{r/2} + 1$ in $\mathbb{F}_q(\zeta^s)$. □

We remark that this proof provides generators for the group of solutions of $v\overline{v} = 1$, so we can easily derive the cardinality of this group, which by Corollary 2.1 is also the number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. As expected, this calculation agrees with the result in [JMV90] which was obtained using the formulas given in [Mac71] — note that the cyclic shift of a basis is considered to be the same basis in [JMV90], but not here, so our formula differs from the one found there by a factor n.

Theorem 2.3. *Consider the decomposition (5) of $X^n - 1$ over $\mathbb{F}_q$. The number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by*

$$2^a \prod_{i=2}^{\sigma} (q^{c_i} + 1) \prod_{j=1}^{\tau} (q^{d_j} - 1) \quad \textit{with} \begin{cases} a = 0 \textit{ for even } q \textit{ and } a = 1 \textit{ for odd } q, \\ 2c_i = \deg f_i \textit{ and } d_j = \deg g_j. \end{cases}$$

Proof. The case $s = 0$ has solutions ± 1 in odd characteristic, and only 1 for even q. For the case $0 \neq s \sim n - s$, we found a generator of order $q^c + 1$ for the set of solutions in the field $\mathbb{F}_q(\zeta)$. For the case $s \not\sim n - s$, let g be a primitive element in $\mathbb{F}_q[X]/(f) \simeq \mathbb{F}_q(\zeta)$, the solutions are the powers of (g, g^{-1}). □

2.2 The ramified case

We deal only with the odd characteristic case, so we let p be an odd prime number, and q and n be powers of p.

Theorem 2.4. *There are $2q^{\frac{n-1}{2}}$ solutions $v \in \mathbb{F}_q[G]$ to the equation $v\overline{v} = 1$.*

This result can easily been derived from [JBG94, Theorem 2], which states that if $n = sp$, where s is any integer, then the following equality, about sizes of orthogonal circulant groups, holds: $|O(sp, q)| = q^{(p-1)s/2}|O(s, q)|$. The original statement is due to MacWilliams in the prime base field case [Mac71, Theorem 2.6]. We now reinterpret MacWilliams' constructive proof in our specific case: n a power of p, so as to explain the structure of the algorithm we use to compute the orthogonal circulant group in the ramified case.

Proof. First note that the solutions of the equation $v\overline{v} = 1$ all lie in $\mathbb{F}_q[G]^\times$, and recall from Subsection 1.1.1 that $\mathbb{F}_q[G]^\times$ is the (internal) direct product $\mathbb{F}_q^\times \times (1 + (\phi - 1)\mathbb{F}_q[G])$, the first component being simply the image by the augmentation map ϵ. For $v \in \mathbb{F}_q[G]^\times$, let $w \in (\phi - 1)\mathbb{F}_q[G]$ be such that $v = \epsilon(v)(1 + w)$, then $v\overline{v} = 1$ if and only if $\epsilon(v) = \pm 1$ and $w + \overline{w} + w\overline{w} = 0$. Setting $r = w + \frac{w\overline{w}}{2}$, the second condition becomes $r = -\overline{r}$, namely

$$r = \sum_{i=1}^{\frac{n-1}{2}} r_i(\phi^i - \phi^{n-i}) \tag{10}$$

for some $r_i \in \mathbb{F}_q$, hence r can take $q^{\frac{n-1}{2}}$ values in $\mathbb{F}_q[G]$. We now show that w is uniquely defined by r, and how it can be computed, see [Mac71, Appendix A]. One has $w = -r + \frac{w\overline{w}}{2}$, hence $\overline{w} = r + \frac{w\overline{w}}{2}$ and $w\overline{w} = -r^2 + \frac{(w\overline{w})^2}{4}$, so that:

$$w = -r - \frac{r^2}{2} + \frac{(w\overline{w})^2}{8} \quad .$$

Replacing iteratively $w\overline{w}$ by $-r^2 + \frac{(w\overline{w})^2}{4}$ in the above formula increases the (even) power to which $w\overline{w}$ appears; this process terminates since, as an element of $(\phi - 1)\mathbb{F}_q[G]$, $w = (\phi - 1)y$ for some $y \in \mathbb{F}_q[G]$, so $w^n = (\phi^n - 1)y^n = 0$. □

Remark 2.5. *In the odd characteristic case, the formula in Theorem 2.3 reads:*

$$2\prod_{i=2}^{\sigma}(q^{c_i}+1)\prod_{j=1}^{\tau}(q^{d_j}-1) \approx 2q^{\sum_i c_i+\sum_j d_j} = 2q^{(n-1)/2} \ .$$

In both semi-simple and ramified cases, the size of the trace-orthogonal group is close to $2\sqrt{q^{n-1}}$, which means that an exhaustive search quickly becomes lengthy when q or n increases.

We now show that one can also get an explicit formula for the solutions of the equation.

Theorem 2.6. *The solutions $v \in \mathbb{F}_q[G]$ to the equation $v\overline{v}=1$ are exactly the sums $v=\sum_{i=0}^{n-1} v_i(\phi-1)^i$ with $v_0=\pm 1$ and, for $1 \leqslant i \leqslant \frac{n-1}{2}$, v_{2i-1} is any element of $\mathbb{F}_q$ and $v_{2i} \in \mathbb{F}_q$ is such that:*

$$\sum_{j=1}^{2i}\sum_{k=0}^{j}(-1)^k\binom{n-k}{2i-j}v_k v_{j-k}=0 \ . \tag{11}$$

Note that (11) gives a formula for v_{2i} in terms of the v_k with $0 \leqslant k \leqslant 2i-1$, for instance $-2v_0v_2 = -v_1^2+v_0v_1$ and $-2v_0v_4 = v_0v_2 - v_1v_2 - 2v_1v_3 + v_2^2 + 3v_0v_3$.

Our proof begins as a specialisation to the case $s=1$ of that of [BG90, Satz 3.3] — note that [JBG94] points out a mistake in the end of the proof of this statement; dealing with this simpler case enables us to deduce a constructive formula.

Before starting the proof, let us recall the isomorphism

$$\mathbb{F}_q[G] \cong \mathbb{F}_q[X]/(X-1)^n \tag{12}$$

mapping ϕ to X. The family $\big((X-1)^i\big)_{0\leqslant i\leqslant n-1}$ is a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[X]/(X-1)^n$. As an auxiliary result we compute the conjugates $\overline{(X-1)^i} = (\overline{X}-1)^i$ of our basis elements.

Lemma 2.7. *For $0 \leqslant i \leqslant n-1$, $(X-1)^i$ divides $(\overline{X}-1)^i$ and, more precisely:*

$$(\overline{X}-1)^i = (-1)^i\sum_{k=0}^{n-i-1}\binom{n-i}{k}(X-1)^{k+i} \equiv (-1)^i(X-1)^i \mod (X-1)^{i+1} \ .$$

Proof. Let $0 \leqslant i \leqslant n-1$, then

$$(\overline{X}-1)^i = (X^{n-1}-1)^i = \big((1-X)X^{n-1}\big)^i = (-1)^i(X-1)^iX^{n-i} \ ,$$

hence the equality, using Newton's formula for $X^{n-i} = (X-1+1)^{n-i}$. □

Proof of Theorem 2.6. We wish to solve the equation $v\overline{v}=1$ in $\mathbb{F}_q[G]$. We shall proceed by successive approximation, solving $v\overline{v} \equiv 1$ modulo $(X-1)^i$ for $1 \leqslant i \leqslant n$, where we identify v and its image under (12), that we write $v=\sum_{k=0}^{n-1} v_k(X-1)^k$ with $v_k \in \mathbb{F}_q$.

The first step is obvious: $\mathbb{F}_q[X]/(X-1) \cong \mathbb{F}_q$ is conjugation invariant, hence the equation reads $v^2 \equiv 1$ modulo $(X-1)$, namely $v \equiv \pm 1$ modulo $(X-1)$, in other words $v_0 = \pm 1$.

The second step is about the coefficients of v of odd index.

Lemma 2.8. *Let $1 \leqslant i \leqslant \frac{n-1}{2}$ and assume $v\overline{v} \equiv 1 \mod (X-1)^{2i-1}$, then*

$$v\overline{v} \equiv 1 \mod (X-1)^{2i} \ .$$

Proof. Write $v\overline{v} \equiv 1 + u(X-1)^{2i-1} \mod (X-1)^{2i}$ for some $u \in \mathbb{F}_q$. Applying conjugation we get that $(\overline{X}-1)^{2i}$ divides $v\overline{v} - 1 - u(\overline{X}-1)^{2i-1}$, therefore

$$v\overline{v} \equiv 1 + u(\overline{X}-1)^{2i-1} \mod (X-1)^{2i} \ ,$$

thanks to Lemma 2.7. We get:

$$0 \equiv u\big((X-1)^{2i-1} - (\overline{X}-1)^{2i-1}\big) \equiv 2u(X-1)^{2i-1} \mod (X-1)^{2i} \ ,$$

hence $u = 0$. □

In particular we get that, if $v_0 = \pm 1$, then $v\overline{v} \equiv 1 \mod (X-1)^2$ for any value of $v_1 \in \mathbb{F}_q$. The third step is a formula for the coefficients of v of even positive index.

Lemma 2.9. *Suppose $v\overline{v} \equiv 1 \mod (X-1)^{2i}$ for some integer $1 \leqslant i \leqslant \frac{n-1}{2}$, then $v\overline{v} \equiv 1 \mod (X-1)^{2i+1}$ if and only if v_{2i} satisfies (11).*

Proof. Without any hypothesis on $v\overline{v}$, one checks using Lemma 2.7 that:

$$v\overline{v} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} \sum_{k=0}^{j} (-1)^k \binom{n-k}{i-j} v_k v_{j-k} \right) (X-1)^i \ .$$

With our assumption on $v\overline{v}$, we get:

$$v\overline{v} \equiv 1 + \sum_{j=0}^{2i} \sum_{k=0}^{j} (-1)^k \binom{n-k}{2i-j} v_k v_{j-k} \mod (X-1)^{2i+1} \ ,$$

hence the result, noticing that $\binom{n}{2i} \equiv 0 \mod p$. □

This ends the proof of Theorem 2.6. □

3. Experiments

3.1 Algorithms

Using MAGMA, we have implemented two algorithms based on the results of this paper. The first finds a self-dual normal basis for a given extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ satisfying the existence conditions of Theorem 1 and such that the degree n is either prime to the characteristic or a power of it. The second (when run after the first) computes the orthogonal circulant group and uses it to construct all self-dual normal bases of the extension from the former one, then selects those which have the lowest complexity. Both of these algorithms have a semi-simple and a ramified version.

3.1.1 *Computation of a self-dual normal basis* Our first algorithm permits us to find a self-dual normal basis for somewhat large extensions. For example, one can find a self-dual normal basis (of complexity $44\,431$) for $q = 1009$ and $n = 211$. Here is the structure of this algorithm in the semi-simple case $\gcd(n, q) = 1$:

Step 1. Compute the q-cyclotomic classes of the set $\{0, \ldots, n-1\}$.

Step 2. Let m be the size of the largest class (the class which contains 1) and choose ζ of order n in $\mathbb{F}_{q^m}$.

Step 3. Build the matrices $F(\zeta) = (\zeta^{ij})_{1 \leqslant i \leqslant j}$ and $F(\zeta^{-1})$.

Step 4. Find a normal element α in $\mathbb{F}_{q^n}$. *(This was already implemented in MAGMA, and uses methods which can be found in the book [MBG+ 93]).*

Step 5. Compute $R \in \mathbb{F}_q[G]$ defined in Theorem 2. Using the matrix $F(\zeta)$, map R to $R' = \mathcal{F}(R) \in (\mathbb{F}_{q^m})^n$.

Step 6. Use Lemmas 1.6, 1.7 and 1.8 to find a solution $v' \in \operatorname{Im}\mathcal{F} \subseteq (\mathbb{F}_q^m)^n$ of $v'\overline{v}' = R'$. Bring back v' to $\mathbb{F}_q[G]$ using matrix $F(\zeta^{-1})$ to obtain v such that $v\overline{v} = R$. Compute $w = v^{-1}$.

Step 7. Compute and output $\gamma = w \circ \alpha$.

In the odd characteristic, ramified case, we pick a normal element α in $\mathbb{F}_{q^n}$ and compute $R \in \mathbb{F}_q[G]$; by Proposition 1.2, solving the equation $v\overline{v} = R$ reduces to computing a square root of R in $\mathbb{F}_q[G] \simeq \mathbb{F}_q[X]/(X-1)^n$, which can be achieved by computing a square root of R modulo $X-1$ and then using Hensel lifting.

3.1.2 *Computation of all self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$* The second algorithm can be used whenever the orthogonal circulant group is not too large for an exhaustive enumeration, see Remark 2.5 and the tables in the next subsection. It uses the data computed by the previous algorithm which must be run first. Its structure in the semi-simple case $\gcd(n, q) = 1$ follows.

Step 1. Use Proposition 2.2 to find generators (and their orders) of the group U of solutions of $u\overline{u} = 1$ in $\mathbb{F}_q[G]$ (this is actually done in the right hand side with generators of $\mathbb{F}_{q^{m_k}}$ where m_k is the size of the cyclotomic class).

Step 2. For each u in U (elements of U are enumerated using the generators found above), compute: the generator $\gamma = (uw) \circ \alpha$ of a self-dual normal basis, the multiplication-by-γ matrix $\left(\operatorname{Tr}(\gamma^{1+q^i+q^j})\right)_{i,j}$, and the complexity of γ. Update statistics accordingly (the best complexity found up to now, the list of best self-dual normal bases).

Step 3. Finally, output the statistics (mainly the best complexity, and the number of times this complexity was achieved).

In the ramified case, we list all the elements of $r \in \mathbb{F}_q[G]$ satisfying (10), compute the associated w as the proof of Theorem 2.4 (*i.e.*, iteratively); the group of solutions of $v\overline{v} = 1$ consists of the elements $1 + w$ obtained in this way together with their opposites $-1 - w$. We let each of these elements act on the self-dual normal basis constructed above and we determine the complexity of the resulting self-dual normal basis.

3.2 Tables

The following tables show the complexity of the best self-dual normal basis obtained with the above algorithms, for some extensions. We give separate tables for extensions in characteristic 2 and for extensions of small prime fields of odd characteristic. Blank entries have not been computed since the cost of exhaustive enumeration grows rapidly.

3.2.1 *Even characteristic* The lowest complexity for self-dual normal bases of extensions over $\mathbb{F}_2$ has been computed by Geiselmann [Jun93, Table 5.1] for odd degree up to 47. With our method we were able to verify these values up to $n = 45$ (the computation for degree 45 took approximately 25 hours

on a 64-bit Xeon quad core running at 2.33 GHz). We include our table for completeness.

n	3	5	7	9	11	13	15	17	19	21	23
min	5	9	21	17	21	45	45	81	117	105	45
n	25	27	29	31	33	35	37	39	41	43	45
min	93	141	57	237	65	69	141	77	81	165	153

Note that [MMPT08, Table 4] gives a minimal complexity of 171 for normal bases in degree 37, where we find a self-dual normal basis of complexity 141, agreeing with Geiselmann. Since only one digit differs between these two results, we suspected that there could be a typo in [MMPT08], and this was confirmed by the authors of that paper.

Using Lemma 1.1, one gets an upper bound for the best self-dual normal complexities in even degree up to $n = 90$, using the fact that any element of $\mathbb{F}_4/\mathbb{F}_2$ of trace 1 generates an optimal self-dual normal basis (of complexity 3). Comparing to the results in [MMPT08, Table 4] for n up to 34, we see that this construction yields the best possible complexity in degrees 10, 22 and 34, and a reasonably good one in degrees 6, 14, 18, 26 and 30.

We get optimal self-dual normal bases in degrees $n = 3, 5, 9, 11, 23, 29, 33, 35, 39$ and 41. We know by [MOVW89, Corollary 3.6] that $2n + 1$ has to be prime and 2 of order n or $2n$ modulo $2n + 1$ for this to happen, therefore we do not get optimal self-dual bases in degrees 15 and 21, since 2 is of order 5 modulo 31 and of order 14 modulo 43.

We give also a table for other small even $q = 2^r$. Note that α^{q^i} for $0 \leqslant i \leqslant n-1$ generates the same normal basis as α, so the number of times the lowest complexity is obtained is a multiple of n. When we found more than n bases with the lowest complexity, we indicate the multiplier between parentheses. For example, we found 27 bases with complexity 45 for $q = 8$ and $n = 9$.

$q\backslash n$	3	5	7	9	11	13	15	17	19	21	23	25
2	5	9	21	17	21	45	45	81	117(2)	105	45	93
4	5	9	21	17	21	45	45	81	117(2)	105	45	93
8	9(3)	9	21	45(3)	21	45	81(3)	81				
16	5	9	21	17	21	45						
32	5	19(15)	21	17	21							
64	9(21)	9	21	45(3)								
128	5	9	37(98)									
256	5	9										

When $\gcd(n, r) = 1$ we always found the same best complexity for the extension $\mathbb{F}_{2^{rn}}$ over $\mathbb{F}_{2^r}$ as for the extension $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. This observation is partially explained by the following fact, which is also valid for odd q (see [MBG+93, Lemma 4.2] for a partial proof).

Lemma 3.1. *If α generates a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $\gcd(n, r) = 1$, then α generates a self-dual normal basis of $\mathbb{F}_{q^{rn}}$ over $\mathbb{F}_{q^r}$, with the same complexity.*

One easily checks that if an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ admits both a self-dual normal basis and an optimal normal basis of type I (see [GL92]), then q and n have to be even, say $q = 2^r$ and $n = 2m$, with m odd and $2m + 1$ prime. If this is the case, the extension is the compositum of the fields $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^m}$, each of which may admit an optimal self-dual normal basis or not. Specifically, one can show that $\mathbb{F}_{q^2}/\mathbb{F}_q$ admits one if and only if r is odd, and that $\mathbb{F}_{q^m}/\mathbb{F}_q$ admits one if 2 is of order m or $2m$ modulo $2m + 1$ and m is co-prime to r. If all these conditions are satisfied, the self-dual normal basis of $\mathbb{F}_{q^n}$ obtained

by multiplying these two bases is, by Lemma 1.1, of complexity $3(2m-1) = 3n-3$, which is also the complexity of the dual basis of the optimal normal basis of $\mathbb{F}_{q^n}$, see [Jun93, Theorem 5.4.10] ([WZ07] even shows that the dual of any basis which is equivalent to the optimal one has complexity $3n-3$). This holds for instance for the extensions of $\mathbb{F}_2$ of degrees 6, 10, 18, 22, 46, ..., and those of $\mathbb{F}_8$ of degrees 10, 22, 46, ...

3.2.2 *Odd characteristic* Now we give the table showing some experiments for odd q. Here, the number of bases with least complexity is a multiple of $2n$ because $\pm\alpha^{q^i}$ for $0 \leqslant i \leqslant n-1$ generates a normal basis with same complexity as the one generated by α. When this multiple is greater than $2n$, we indicate the multiplier between parentheses. For example, we found $4 \times 2n = 8n$ bases with complexity 51 for $q = 13$ and $n = 9$.

$q\backslash n$	3	5	7	9	11	13	15	17	19	21	23	25
3	**7**	13	25	**37**	55(2)	67	−−	91	172	−−	127	135
5	6	**13**	25	46	64	85	−−	157	153	150		
7	6	16	**19**	41	61	96	87			−−		
11	6	13	25	52	**31**	100	78					
13	6	13	25	51(4)	64	**37**						
17	8	13	25	51(5)	64	100		−−				
19	8	13	31	51	67				−−			

Bold-faced entries correspond to the best complexity in the case when the degree n is a power of the characteristic. In this case, whenever n is prime, the best complexity is $3n-2$, and is obtained with the basis exhibited in [BGM94, Theorem 5.3]. This basis is rather explicit since it is generated by the root of a trinomial, yielding a very interesting family of self-dual normal bases of complexity fairly close to the optimal one.

We have made no computation for "mixed degree" $n = n_1 p^e$ with $\gcd(n_1, p) = 1$, $n_1 > 1$ and $e > 0$, but one gets an upper bound for the lowest complexity in that case by multiplying the lowest complexity in degree n_1 by that in degree p^e, thanks to Lemma 1.1. For instance, the best complexity for $q = 5$ and $n = 15$ is at most $6 \cdot 13 = 78$. Note that when $n = \ell\ell'$ for prime numbers $\ell \neq \ell'$, both different from p, the best complexity for the compositum is not necessarily the product of those for degrees ℓ and ℓ' extensions ($n = 15$, $q = 7$); however it can be so ($n = 15$, $q = 11$; $n = 21$, $q = 5$).

In the semi-simple case, we also computed the best complexity for some odd non prime values $q = p^r$, which do not appear in this table. When $\gcd(n, r) = 1$ we always found the same best complexity for the extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ as for the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, as well as the same multiplier for the number of bases with the best complexity (as in the even characteristic case).

In odd characteristic, the only exhaustive search for lowest complexities among normal bases we are aware of is in [BGM94], over prime base fields. The lowest complexity for self-dual normal bases is the same as the one they obtain for normal bases when $n = 3$ and $q = 7$ or 13; slightly larger when $n = 3$ and $q = 19$ (8 instead of 6) and when $n = 5$ and $q = 11$ (13 instead of 12). Note that in this last case, Liao and Feng give in [LF09, Example 2] a construction of a normal basis with minimal complexity 12, using Gauss periods, whose dual basis has complexity 13. Their construction remains valid when replacing the base field $\mathbb{F}_{11}$ by an extension of degree prime to 5.

3.3 Conclusion

Our algorithms enable us to compute the minimal complexity for self-dual normal bases in various extensions of finite fields, including some for which the exhaustive enumeration of normal bases would not be reasonable. In odd characteristic, the lowest complexities we obtain are either the same as or close to that obtained in former computations on normal bases using theoretical constructions or exhaustive search, analogously to what could already be observed in even characteristic. However the cost of the exhaustive search of all self-dual normal bases (once one has been constructed) is still a limitation of this method. In order to make self-dual normal bases practical, it would thus be desirable to find a direct construction of those with low complexity.

A striking fact when looking at the tables above is the repetition of values along columns, albeit with some exceptions. We have a partial explanation for this phenomenon, that may also help in achieving the former goal, in terms of global considerations of cyclotomic extensions of the rationals generated by n^2-th roots of unity, where n is a prime. A known construction yields a global self-dual normal basis generator α_n such that, for any prime $p \neq n$ which does not split in the considered extension, the residue modulo p of α_n is a candidate for a best complexity basis for $\mathbb{F}_{p^n}/\mathbb{F}_p$. We hope to give full details about this construction in a future paper.

Acknowledgments. The authors would like to thank the anonymous referees for their valuable and insightful remarks and advice.

References

ABV89 D. W. Ash, I. F. Blake, and S. A. Vanstone, *Low complexity normal bases*, Discrete Applied Mathematics **25** (1989), no. 3, 191–210.

BG90 T. Beth and W. Geiselmann, *Selbstduale Normalbasen über* GF(q), Arch. Math. (Basel) **55** (1990), no. 1, 44–48.

BGM94 I. F. Blake, S. Gao, and R. C. Mullin, *Normal and self-dual normal bases from factorization of* $cx^{q+1} + dx^q - ax - b$, SIAM J. on Discrete Mathematics **7** (1994), no. 3, 499–512.

BV78 K. A. Byrd and T. P. Vaughan, *Counting and constructing orthogonal circulants*, J. of Combinatorial Theory, Series A **24** (1978), no. 1, 34–49.

CGPT08 M. Christopoulou, T. Garefalakis, D. Panario, and D. Thomson, *The trace of an optimal normal element and low complexity normal bases*, Designs, Codes and Cryptography **49** (2008), no. 1-3, 199–215.

CGPT11 ———, *Gauss periods as constructions of low complexity normal bases*, Designs, Codes and Cryptography (2011), , to appear.

CL09 J.-M. Couveignes and R. Lercier, *Elliptic periods for finite fields*, Finite Fields and Their Applications **15** (2009), no. 1, 1–22.

Gao93 S. Gao, *Normal Bases Over Finite Fields*, PhD in Combinatorics and Optimisation, University of Waterloo, Waterloo, Ontario, Canada, 1993.

GL92 S. Gao and H. W. Lenstra, Jr., *Optimal normal bases*, Designs, Codes and Cryptography **2** (1992), no. 4, 315–323.

GvzGPS00 S. Gao, J. von zur Gathen, D. Panario, and V. Shoup, *Algorithms for exponentiation in finite fields*, J. of Symbolic Computation **29** (2000), no. 6, 879–889. MR 1765928 (2002e:68152a)

JBG94 Dieter Jungnickel, Thomas Beth, and Willi Geiselmann, *A note on orthogonal circulant matrices over finite fields*, Arch. Math. (Basel) **62** (1994), no. 2, 126–133.

JMV90 D. Jungnickel, A. J. Menezes, and S. A. Vanstone, *On the number of self-dual bases of* GF(q^m) *over* GF(q), Proc. of the American Math. Society **109** (1990), no. 1, 23–29.

Jun93 Dieter Jungnickel, *Finite fields*, Bibliographisches Institut, Mannheim, 1993, Structure and Arithmetics.

LF09 Q. Liao and K. Feng, *On the complexity of the normal bases via prime Gauss period over finite fields*, J. of Systems, Science and Complexity **22** (2009), no. 3, 395–406.

LS06 Q. Liao and Q. Sun, *Normal bases and their dual-bases over finite fields*, Acta Mathematica Sinica (Engl. Ser.) **22** (2006), no. 3, 845–848. MR 2220177 (2006k:12010)

LW88 A. Lempel and M. J. Weinberger, *Self-complementary normal bases in finite fields*, SIAM J. on Discrete Mathematics **1** (1988), no. 2, 193–198.

Mac71 F. J. MacWilliams, *Orthogonal circulant matrices over finite fields, and how to find them.*, J. Combinatorial Theory, Series A **10** (1971), 1–17.

MBG+93 A. J. Menezes, I. F. Blake, S. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian (eds.), *Applications of finite fields*, Kluwer Academic Publishers, 1993.

MMPT08 Ariane M. Masuda, Lucia Moura, Daniel Panario, and David Thomson, *Low complexity normal elements over finite fields of characteristic two*, IEEE Transactions on Computers **57** (2008), no. 7, 990–1001.

MOVW89 R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, *Optimal normal bases in* GF(p^n), Discrete Applied Mathematics **22** (1988/89), no. 2, 149–161.

NNMU08 Y. Nogami, H. Nasu, Y. Morikawa, and S. Uehara, *A method for constructing a self-dual normal basis in odd characteristic extension fields*, Finite Fields and Their Applications **14** (2008), 867–876.

Pic10 E. J. Pickett, *Construction of self-dual integral normal bases in abelian extensions of finite and local fields*, Int. J. of Number Theory **6** (2010), no. 7, 1565–1588.

Pol95 Alain Poli, *Constructing SCN bases in characteristic* 2, IEEE Transactions on Information Theory **41** (1995), no. 3, 790–794.

Wan89 C. C. Wang, *An algorithm to design finite field multipliers using a self-dual normal basis*, IEEE Transactions on Computers **38** (1989), no. 10, 1457–1460.

WZ07 Z.-X. Wan and K. Zhou, *On the complexity of the dual basis of a type I optimal normal basis*, Finite Fields and Their Applications **13** (2007), no. 2, 411–417.

François Arnault, Erik Jarl Pickett and Stéphane Vinatier

4.2 La complexité des bases normales auto-duales cyclotomiques

Reprenons le fil de la discussion ci-dessus pour préciser l'idée d'Erik, qui était que la clef de ce mystère pouvait se trouver dans la base normale auto-duale de la racine carrée de la codifférente introduite par Erez pour les extensions de degré premier de $\mathbb{Q}$ ([Ere88]). Nous nous sommes donc lancés, Erik et moi, dans le calcul de la table de multiplication de cette base, dont le résultat est la Proposition 2.2 de l'article présenté ci-dessous. Des calculs sur ordinateur à partir de cette expression ont rapidement confirmé cette intuition. Il va sans dire que nous étions très étonnés de retrouver cette base, que nous connaissions tous deux de par notre travail en théorie des modules galoisiens, dans un contexte qui nous semblait fortement déconnecté de celui-ci.

Toujours est-il que nous tenions là une base normale auto-duale dont on pouvait espérer qu'elle allait donner, par réduction de l'extension aux places non décomposées, une base normale auto-duale de bonne complexité pour l'extension de corps finis correspondante. Pour s'en assurer, il fallait essayer de trouver une expression générale plus explicite de la complexité avant réduction (c'est-à-dire du nombre de cœfficients non nuls dans la table de multiplication). Cet objectif s'est révélé difficile à atteindre. Par ailleurs, Erik s'est alors intéressé à un autre sujet, plus proche de ses préoccupations antérieures, dans lequel il s'est complètement investi. J'ai continué à creuser celui-ci de mon côté.

Je présente le résultat de ce travail ci-dessous. J'y montre que la table de multiplication est reliée par une relation très simple (donnée dans le Corollaire 2.9) à la matrice d'incidence d'un arrangement de droites du plan projectif du corps fini de même cardinal que le degré de l'extension de $\mathbb{Q}$ dont on est parti. En guise d'illustration, voici les matrices d'incidence de l'arrangement en degrés 5 et 7 :

$$\begin{pmatrix} 0 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 2 \\ 0 & 2 & 1 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 2 & 1 \\ 1 & 1 & 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Cette très jolie construction ne règle pas pour autant le problème : je ne parviens en effet à calculer exactement les nombres d'incidence que pour une droite particulière de l'arrangement et ses symétriques, voir la Proposition 2.12. Dans une version précédente de l'article (l'arrangement n'était alors pas complété par la diagonale et les axes) je trouvais une minoration très large du nombre de 1 dans la matrice d'incidence (égal au nombre de 0 dans la table de multiplication de la base normale), qui ne donnait rien au niveau asymptotique (sinon que la complexité était inférieure au nombre de cœfficients, ce qui est trivial). Les calculs numériques reproduits en fin d'article semblent pourtant confirmer l'intérêt de cette base normale auto-duale en termes de complexité.

The complexity of cyclotomic self-dual normal bases

Stéphane Vinatier

Let d be an odd prime number. Let ζ_{d^2} denote a primitive d^2-th root of unity. We wish to compute the « global » complexity of Erez's self-dual normal basis of the unique subextension M of degree d over $\mathbb{Q}$ of $\mathbb{Q}(\zeta_{d^2})$, generated by

$$\alpha = \frac{1 + \mathrm{Tr}_{\mathbb{Q}(\zeta_{d^2})/M}(\zeta_{d^2})}{d} \ .$$

One checks that, for any $g, h \in \mathrm{Gal}(M/\mathbb{Q})$, $\mathrm{Tr}_{M/\mathbb{Q}}\big(g(\alpha)h(\alpha)\big) = \delta_{g,h}$. From this one deduces that the conjugates of α under the action of $\mathrm{Gal}(M/\mathbb{Q})$ form a self-dual normal basis of M over $\mathbb{Q}$. Erez has proved that they also form a self-dual normal basis over $\mathbb{Z}$ of the square root of the inverse different $\mathcal{A}_{M/\mathbb{Q}}$ of the extension.

1. Complexity of a self-dual normal basis

Let K denote a finite Galois extension of $\mathbb{Q}$, of degree n. Let $a \in K$ generate a self-dual normal basis of K over $\mathbb{Q}$. The global complexity $c(a)$ of the self-dual normal basis generated by a is by definition the number of non zeros entries of any of its multiplication tables: given a numbering ϕ_i, $0 \leqslant i \leqslant n-1$, of the elements of $\mathrm{Gal}(K/\mathbb{Q})$, such a table consists of the symmetric matrix:

$$\Big(\mathrm{Tr}_{K/\mathbb{Q}}\big(a\phi_i(a)\phi_j(a)\big)\Big)_{0\leqslant i,j\leqslant n-1}$$

Notice that changing the numbering of the Galois group of $K/\mathbb{Q}$ permutes the entries of the matrix without modifying their value, in particular without modifying the number of non zero entries. The same holds when replacing a by one of its conjugates.

1.1 Symmetries in the cyclic case

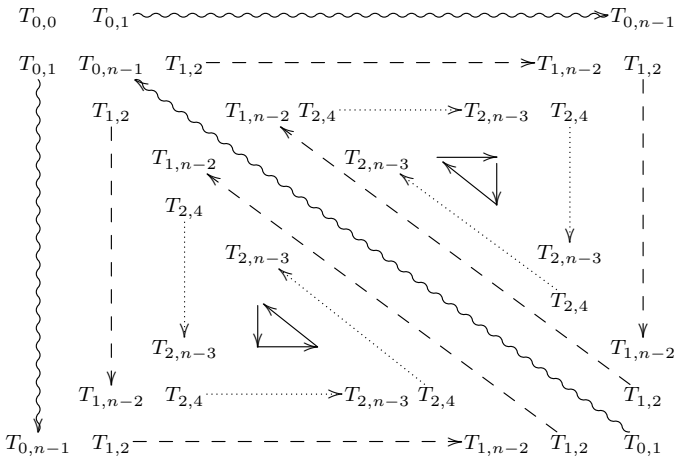
We now suppose that the extension $K/\mathbb{Q}$ is cyclic of degree n. Let ϕ denote a generator of $\mathrm{Gal}(K/\mathbb{Q})$ and denote by $T_\phi(a)$ the matrix obtained as above for the numbering $\phi_i = \phi^i$ of the Galois group. Since $\mathrm{Tr}_{K/\mathbb{Q}}\big(\phi(b)\big) = \mathrm{Tr}_{K/\mathbb{Q}}(b)$ for every $b \in K$, the entries of $T_\phi(a)$ satisfy:

$$\begin{aligned} &T_\phi(a)_{i,j} = T_\phi(a)_{j-i,n-i} = T_\phi(a)_{n-j,n-j+i} \quad \text{for } j > i \geqslant 0 \ , \\ &T_\phi(a)_{j,j} = T_\phi(a)_{0,n-j} \quad \text{for } j \geqslant 1 \ . \end{aligned} \tag{1}$$

It follows that, except for $T_\phi(a)_{0,0}$, the entries of the line $i = 0$ appear thrice in the matrix: they are repeated on the first column and on the diagonal (in reverse order). Similarly, the other entries appear six times in the matrix, as indicated in the following diagram, where for brevity we have written $T_{i,j}$

2000 Mathematics Subject Classification ????

instead of $T_\phi(a)_{i,j}$:



We now restrict to the case n coprime to 6. Write $n = 3q+r$ where $r = 1$ if q is even, $r = 2$ otherwise. Once the $1 + (n-1)$ entries of the line $i = 0$ have been computed, there remains $n - 3 = 3(q-1) + r$ entries to compute in the line $i = 1$ (those such that $2 \leqslant j \leqslant n-2$), $n - 6 = 3(q-2) + r$ in the line $i = 2$ (those such that $4 \leqslant j \leqslant n-3$), ..., $n - 3q = r$ entries to compute in the line $i = q$ (those such that $2q \leqslant j \leqslant n-1-q$), in order to complete the multiplication table. Indeed, one checks using that $r \in \{1, 2\}$ that the following equality holds:

$$n^2 = 1 + 3(n-1) + 6\sum_{k=0}^{q-1}(r+3k) \ .$$

The number of terms to compute in order to complete the multiplication table is

$$\sum_{k=0}^{q}(r+3k) = \frac{(n+1)(n+2)}{6} \ .$$

Denoting by $c_0(a)$ the number of non zero entries among the $n-1$ entries $T_\phi(a)_{0,j}$ with $1 \leqslant j \leqslant n-1$ of line $i = 0$, and for $1 \leqslant i \leqslant q$ by $c_i(a)$ the number of non zero entries among the $n - qi$ entries $T_\phi(a)_{i,j}$ with $2i \leqslant j \leqslant n-1-i$ of line i, we get the following equality for the global complexity:

$$c(a) = (1 - \delta_{0,T_\phi(a)_{0,0}}) + 3c_0(a) + 6\sum_{i=1}^{q} c_i(a) \ , \tag{2}$$

where $\delta_{0,t}$ is the Kronecker delta: $\delta_{0,t} = 1$ if $t = 0$, 0 otherwise.

1.2 Geometric interpretation in the prime degree case

Here we suppose that the extension $K/\mathbb{Q}$ is cyclic of prime degree at least 5. We now let d denote the degree of $K/\mathbb{Q}$. The set $\{0, \ldots, d-1\}$ of indexes of the rows and columns of $T_\phi(a)$ is a system of representatives of $\mathbb{F}_d = \mathbb{Z}/d\mathbb{Z}$ in $\mathbb{Z}$. Each entry $T_\phi(a)_{i,j}$ can thus be interpreted as the value $T(i \mod d, j \mod d)$ of a function T defined on $(\mathbb{F}_d)^2$ and taking values in $\mathbb{Q}$.

Let ι and θ in $GL_2(\mathbb{F}_d)$ be defined by $\iota(x,y) = (y,x)$, $\theta(x,y) = (y-x, -x)$ for $(x,y) \in (\mathbb{F}_d)^2$. One checks that ι is of order 2, θ of order 3, and that $\iota \circ \theta \circ \iota(x,y) = (-y, x-y) = \theta^2(x,y)$, hence $\Gamma = \langle \iota, \theta \rangle$ is isomorphic to the permutation group on three letters $\mathfrak{S}_3$. The two other elements of Γ of order 2 are:

$$\kappa = \theta \circ \iota : (x,y) \mapsto (x-y, -y) \ , \quad \lambda = \iota \circ \theta : (x,y) \mapsto (-x, y-x) \ .$$

The (order 2) symmetry of the multiplication table — the invariance under transposition — yields that $T \circ \iota = T$. Together with equalities (1), we get:

Proposition 1.1. *For any $\gamma \in \Gamma$, $T \circ \gamma = T$. In other words, the multiplication table $T_\phi(a)$ is invariant under Γ.*

2. The cyclotomic self-dual normal basis

We get back to the setting of the introduction: d is an odd prime number and $\zeta = \zeta_{d^2}$ a primitive d^2-th root of unity.

2.1 Erez' self-dual normal basis generator

Any automorphism of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is defined by its value on the primitive element ζ, which is necessarily a prime to d power of ζ. This yields the isomorphism

$$(\mathbb{Z}/d^2\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \ , \tag{3}$$

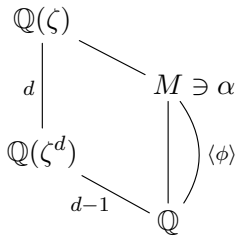
sending $n \mod d^2$ to $\zeta \mapsto \zeta^n$. It follows that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic, hence has exactly one subgroup of order d (resp. $d-1$), generated by the image under (3) of any integer of order d (resp. $d-1$) modulo d^2. By Galois theory, $\mathbb{Q}(\zeta)/\mathbb{Q}$ has exactly one subextension of degree d that we denote $M/\mathbb{Q}$. Furthermore $\phi : \zeta \mapsto \zeta^{1+d}$ generates $\mathrm{Gal}\big(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^d)\big)$ and its restriction to M (also denoted by ϕ) generates $\mathrm{Gal}(M/\mathbb{Q})$. On the other hand, any integer a which is prime to d satisfies $a^d \equiv a \mod d$ and a^d is of order dividing $d-1$ modulo d^2, hence isomorphism (3) yields a one-to-one correspondence between $\mathrm{Gal}(\mathbb{Q}(\zeta)/M)$ and the set $\{a^d \mod d^2 : 1 \leqslant a \leqslant d-1\}$.

Proposition 2.1. *Let $t = \mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta)$, then $\alpha = \frac{1+t}{d}$ satisfies, for $0 \leqslant i \leqslant d-1$:*

$$\mathrm{Tr}_{M/\mathbb{Q}}(\alpha\phi^i(\alpha)) = \delta_{0,i} \ ,$$

where $\delta_{0,i}$ is the Kronecker delta: $\delta_{0,i} = 1$ if $i = 0$, 0 otherwise.

It follows from the above property that α generates a self-dual normal basis for M over $\mathbb{Q}$. This basis was first introduced by Erez in [Ere88]. Before giving a proof, let us illustrate the situation in the following extension diagram.



Proof. Let $0 \leqslant i \leqslant d-1$, then $d\alpha\phi^i(d\alpha) = 1 + t + \phi^i(t) + t\phi^i(t)$, and $\mathrm{Tr}_{M/\mathbb{Q}}(t) = \mathrm{Tr}_{M/\mathbb{Q}}(\phi^i(t)) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = 0$, the minimal polynomial of ζ over $\mathbb{Q}$ being $(X^{d^2}-1)/(X^d-1) = 1 + X^d + X^{2d} + \cdots + X^{d(d-1)}$, thus $d^2\mathrm{Tr}_{M/\mathbb{Q}}(\alpha\phi^i(\alpha)) = d + \mathrm{Tr}_{M/\mathbb{Q}}(t\phi^i(t))$. Since $\phi^i(\zeta) = \zeta^{(1+d)^i} = \zeta^{1+id}$, one has

$$t\phi^i(t) = \left(\sum_{a=1}^{d-1} \zeta^{a^d}\right)\left(\sum_{b=1}^{d-1} \zeta^{(1+id)b^d}\right) = \sum_{1\leqslant b,c\leqslant d-1} \zeta^{(c^d+1+id)b^d}$$

by letting $c = a/b$, hence

$$\mathrm{Tr}_{M/\mathbb{Q}}(t\phi^i(t)) = \sum_{b,c} \mathrm{Tr}_{M/\mathbb{Q}}\left(\zeta^{(c^d+1+id)b^d}\right) = \sum_{c=1}^{d-1} \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\zeta^{c^d+1+id}\right) \ .$$

Whenever c^d+1+id is prime to d, ζ^{c^d+1+id} is a primitive d^2-th root of unity, hence its trace from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$ is zero as above; further d divides c^d+1+id if and only if $c \equiv -1 \mod d$, namely $c = d-1$, and $(d-1)^d \equiv -1 \mod d^2$. Therefore $\mathrm{Tr}_{M/\mathbb{Q}}(t\phi^i(t)) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\zeta^{id}\right)$, which equals $d(d-1)$ when $i = 0$, $d\mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\zeta^d) = -d$ otherwise, which proves the result. □

2.2 Multiplication table

We consider the multiplication table $T = T_\phi(\alpha)$ of the self-dual normal basis of $M/\mathbb{Q}$ generated by α, associated to ϕ. Its entries satisfy:

$$\begin{aligned} d^3T_{i,j} &= \mathrm{Tr}_{M/\mathbb{Q}}\big((1+t)(1+\phi^i(t))(1+\phi^j(t))\big) \\ &= \mathrm{Tr}_{M/\mathbb{Q}}\big(1+t+\phi^i(t)+\phi^j(t)+t\phi^i(t)+t\phi^j(t)+\phi^i(t)\phi^j(t)+t\phi^i(t)\phi^j(t)\big) \\ &= d + \mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)+t\phi^j(t)+\phi^i(t)\phi^j(t)\big) + \mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\phi^j(t)\big) \end{aligned}$$

since $\mathrm{Tr}_{M/\mathbb{Q}}\big(\phi^i(t)\big) = \mathrm{Tr}_{M/\mathbb{Q}}\big(\phi^j(t)\big) = \mathrm{Tr}_{M/\mathbb{Q}}(t) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = 0$ (as seen above). We derive from Proposition 2.1 that $\mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\big) = d^2\delta_{0,i} - d$, hence

$$d^3T_{i,j} = -2d + d^2(\delta_{0,i}+\delta_{0,j}+\delta_{i,j}) + \mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\phi^j(t)\big) \ .$$

The remaining trace is the hardest one to compute. Recall that $\phi^i(\zeta) = \zeta^{(1+d)^i} = \zeta^{1+id}$ and that ϕ commutes with $\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}$, since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian. With the same description of $\mathrm{Gal}(\mathbb{Q}(\zeta)/M)$ as in Subsection 2.1, this yields:

$$\begin{aligned} \mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\phi^j(t)\big) &= \mathrm{Tr}_{M/\mathbb{Q}}\big(\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta)\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta^{1+di})\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta^{1+dj})\big) \\ &= \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\big(\zeta\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta^{1+di})\mathrm{Tr}_{\mathbb{Q}(\zeta)/M}(\zeta^{1+dj})\big) \\ &= \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\zeta\sum_{a=1}^{d-1}\zeta^{(1+di)a^d}\sum_{b=1}^{d-1}\zeta^{(1+dj)b^d}\right) \\ &= \sum_{1\leqslant a,b\leqslant d-1}\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\big(\zeta^{1+a^d+b^d+d(ia^d+jb^d)}\big) \ . \end{aligned}$$

Whenever $1+a^d+b^d \not\equiv 0 \mod d$, $\zeta^{1+a^d+b^d+d(ia^d+jb^d)}$ is a primitive d^2-th root of unity, hence its trace from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$ is zero. In particular this is always the case if $a \equiv -1 \mod d$. When $a \neq d-1$, then $1+a^d+b^d \equiv 0 \mod d$ if and only if $b \equiv -(1+a) \mod d$, which implies $b^d \equiv -(1+a)^d \mod d^2$, so

$$\begin{aligned} \mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\phi^j(t)\big) &= \sum_{a=1}^{d-2}\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\big(\zeta^{1+a^d-(1+a)^d+d(ia-j(1+a))}\big) \\ &= d\sum_{a=1}^{d-2}\mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}\big(\zeta^{d(ia-j(1+a)-p(a))}\big) \ , \end{aligned}$$

where we let

$$p(a) = \frac{(1+a)^d - 1 - a^d}{d} \in \mathbb{Z}$$

and note that $p(a) \mod d$ only depends on $a \mod d$.

Let $N_{i,j}$ denote the cardinal of $\{a\ :1\leqslant a\leqslant d-2\,,\ ia-j(1+a)-p(a)\equiv 0 \mod d\}$, then

$$\mathrm{Tr}_{M/\mathbb{Q}}\big(t\phi^i(t)\phi^j(t)\big)=d^2(N_{i,j}-1)+2d\ ,$$

since $\mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}\big(\zeta^{dn}\big)=d-1$ if $n\equiv 0 \mod d$, -1 otherwise. We obtain:

Proposition 2.2. *For any $(i,j)\in\{0,\dots,d-1\}^2$, one has:*

$$d\,T_{i,j}=\delta_{0,i}+\delta_{0,j}+\delta_{i,j}+N_{i,j}-1=\begin{cases}2+N_{0,0} & \text{if } |\{0,i,j\}|=1\ ;\\ N_{i,j} & \text{if } |\{0,i,j\}|=2\ ;\\ N_{i,j}-1 & \text{otherwise.}\end{cases}$$

We are left with evaluating the numbers $N_{i,j}$.

2.3 Geometric interpretation

For each $a\in\{1,\dots,d-2\}$, we let L_a be the line of $(\mathbb{F}_d)^2$ of equation:

$$L_a\ :\ xa-y(1+a)-p(a)=0\ , \tag{4}$$

where we have identified integers with their reduction modulo d — we shall go on doing this identification without mention from now on. It follows from the above definition of $N_{i,j}$ that it equals the number of lines L_a that go through $(i,j)\in(\mathbb{F}_d)^2$, for $1\leqslant a\leqslant d-2$. In other words, $N=(N_{i,j})_{0\leqslant i,j\leqslant d-1}$ is the incidence matrix of the arrangement of lines $\{L_a:1\leqslant a\leqslant d-2\}$. The next two facts are a motivation for what follows:

- the numbers $N_{i,j}$ are linked to the entries of the multiplication table $T_\phi(\alpha)$ by Proposition 2.2, so the symmetry properties of Proposition 1.1 should have a counterpart in terms of the lines L_a;
- for each $1\leqslant a\leqslant d-2$, L_a has the same direction as the vector $(a+1,a)$ in $(\mathbb{F}_d)^2$, namely its direction is represented in $\mathbb{P}(\mathbb{F}_d)$, the one dimensional projective space over $\mathbb{F}_d$, by the point with homogeneous coordinates $(a+1:a)$; in other words, the slope of L_a is given by the map $s(a)=\frac{a}{a+1}$, which is clearly injective, so the lines L_a are pairwise distinct and convergent.

Note further that s yields a one-to-one correspondence between $\mathbb{F}_d\setminus\{-1\}$ and $\mathbb{F}_d\setminus\{1\}$. It follows that the map

$$\epsilon:a\in\mathbb{F}_d\mapsto(a+1:a)\in\mathbb{P}(\mathbb{F}_d) \tag{5}$$

is an embedding of $\mathbb{F}_d$ in $\mathbb{P}(\mathbb{F}_d)$, such that $\mathbb{P}(\mathbb{F}_d)=\epsilon(\mathbb{F}_d)\cup\{(1:1)\}$, namely the "point at infinity" corresponds to the diagonal (of slope 1).

One easily extends the definition of L_a to any $a\in\mathbb{F}_d$, using equation (4) with $p(0)=p(-1)=0$. We get two more lines with directions corresponding to $(1:0)$ and $(0:1)$ in $\mathbb{P}(\mathbb{F}_d)$, and that go through the origin, namely L_0 and L_{-1} are respectively the horizontal and vertical axes. We shall now extend the definition of the lines L_a to $\mathbb{P}(\mathbb{F}_d)$, using the above embedding ϵ of $\mathbb{F}_d$ into $\mathbb{P}(\mathbb{F}_d)$, namely we shall define the line $L_{(1:1)}$ associated with the direction of the diagonal (of slope 1). This will go through expressing the constant coefficient $p(a)$ of equation (4) as an homogeneous function in $(a+1,a)$. The symmetry properties of this function will reflect that of the multiplication table; they will enable to show that the extended arrangement of lines is stable under the action of Γ.

2.4 Lazard polynomial and arrangement

We let P denote the polynomial with integral coefficients:

$$P(X,Y)=\frac{X^d+(-Y)^d+(Y-X)^d}{d}\ , \tag{6}$$

which is Lazard polynomial $\frac{(X+Y)^d - X^d - Y^d}{d}$ composed with a mild change of variable. We note that for $0 \leqslant a \leqslant d-1$, $P(a+1,a) = p(a)$, and specifically $P(1,0) = P(0,-1) = 0$. Furthermore, P is homogeneous of degree d as a polynomial in $\mathbb{Z}[X,Y]$, thus homogeneous of degree 1 as a function on $(\mathbb{F}_d)^2$.

Recall that ι and θ in $GL_2(\mathbb{F}_d)$ are defined by $\iota(x,y) = (y,x)$, $\theta(x,y) = (y-x,-x)$ for $(x,y) \in (\mathbb{F}_d)^2$. We let ι and θ act the same way on $(X,Y) \in \mathbb{Z}[X,Y]^2$, and denote again $\Gamma = \langle \iota, \theta \rangle$ the group they generate, which is (still) isomorphic to the permutation group on three letters $\mathfrak{S}_3$. Let $\sigma(\gamma)$ denote the signature of $\gamma \in \Gamma$, so $\sigma(\iota) = -1$ and $\sigma(\theta) = 1$.

Proposition 2.3. *As a polynomial in $\mathbb{Z}[X,Y]$, P satisfies, for all $\gamma \in \Gamma$:*

$$P = \sigma(\gamma)\, P \circ \gamma \ .$$

Proof. The formula is straightforward for ι and θ; it follows for any $\gamma \in \Gamma = \langle \iota, \theta \rangle$ since σ is a group homomorphism. □

We denote the same way the reduction of P in $\mathbb{F}_d[X,Y]$. For $(b:a) \in \mathbb{P}(\mathbb{F}_d)$, let $L_{(b:a)}$ be the line of $(\mathbb{F}_d)^2$ of equation:

$$L_{(b:a)} \ : \ ax - by - P(b,a) = 0 \ , \tag{7}$$

where, with some abuse in the notation, (b,a) is any element of $(\mathbb{F}_d)^2$ with image $(b:a)$ in $\mathbb{P}(\mathbb{F}_d)$ — the line $L_{(b:a)}$ is well defined since P is homogeneous of degree 1 as a function on $(\mathbb{F}_d)^2$. Further $(b:a)$ is the point of $\mathbb{P}(\mathbb{F}_d)$ corresponding to the direction of $L_{(b:a)}$, $L_{(a+1:a)} = L_a$ for $a \in \mathbb{F}_d$ and $L_{(1:1)}$ is the diagonal (since $P(1,1) = 0$).

Definition 2.4. We denote by $\mathcal{L}$ the arrangement of these lines, namely

$$\mathcal{L} = \{ L_{(b:a)} \ : \ (b:a) \in \mathbb{P}(\mathbb{F}_d) \} \ ,$$

and we call $\mathcal{L}$ the Lazard arrangement.

We shall now show that $\mathcal{L}$ is preserved by the symmetries of the multiplication table $T_\phi(\alpha)$. For $\gamma \in \Gamma$, we denote by $\mathbb{P}(\gamma)$ the induced projective application on $\mathbb{P}(\mathbb{F}_d)$, *e.g.* $\mathbb{P}(\iota)(x:y) = (y:x)$ and $\mathbb{P}(\theta)(x:y) = (y-x:-x)$ for any $(x:y) \in \mathbb{P}(\mathbb{F}_d)$.

Theorem 2.5. *For any $(b:a) \in \mathbb{P}(\mathbb{F}_d)$ and $\gamma \in \Gamma$, one has*

$$\gamma(L_{(b:a)}) = L_{\mathbb{P}(\gamma)(b:a)} \ .$$

Proof. Since $\mathbb{P}(\mu \circ \nu) = \mathbb{P}(\mu) \circ \mathbb{P}(\nu)$ for any $\mu, \nu \in GL_2(\mathbb{F}_d)$, we only have to check the result for $\gamma \in \{\iota, \theta\}$. Proposition 2.3 applied to ι yields, for $(b:a) \in \mathbb{P}(\mathbb{F}_d)$ and $(x,y) \in (\mathbb{F}_d)^2$:

$$ax - by - P(b,a) = 0 \iff by - ax - P(a,b) = 0 \ ,$$

namely $(x,y) \in L_{(b:a)} \Leftrightarrow (y,x) \in L_{(a:b)}$, hence the result for ι. Similarly, Proposition 2.3 applied to θ yields:

$$ax - by - P(b,a) = 0 \iff -b(y-x) - (a-b)(-x) - P(a-b,-b) = 0 \ ,$$

namely $(x,y) \in L_{(b:a)} \Leftrightarrow (y-x,-x) \in L_{(a-b:-b)}$, hence the result for θ. □

Corollary 2.6. *Under the action of Γ, the Lazard arrangement $\mathcal{L}$ always has two orbits of cardinal 3, $\{L_0, L_{-1}, L_{(1:1)}\}$ and $\{L_1, L_{\frac{d-1}{2}}, L_{-2}\}$; it has one orbit of cardinal 2 exactly when $d \equiv 1 \mod 3$, in which case it is given by $\{L_\omega, L_{\omega^2}\}$ where ω is a primitive cubic root of unity in $\mathbb{F}_d$; all other orbits have cardinal 6.*

Proof. By Theorem 2.5, we only have to look at the action of $\mathbb{P}(\Gamma)$ on $\mathbb{P}(\mathbb{F}_d)$. First, $\mathbb{P}(\iota)(1:0)=(0:1)$ and $\mathbb{P}(\iota)(1:1)=(1:1)$ so ι fixes $L_{(1:1)}$ and permutes $L_0=L_{(1:0)}$ and $L_{-1}=L_{(0:1)}$; similarly $\theta(1:0)=(-1:-1)=(1:1)$, $\theta(1:1)=(0,1)$ and $\theta(0:1)=(1:0)$, hence θ permutes L_0, $L_{(1:1)}$ and L_{-1} cyclically. It follows that $\{(1:0),(1:1),(0:1)\}$ is an orbit of $\mathbb{P}(\mathbb{F}_d)$ under Γ.

Furthermore, since $\mathbb{P}(\mathbb{F}_d)$ is the disjoint union of this orbit with $\epsilon(\mathbb{F}_d\setminus\{0,-1\})$, we get that $\epsilon(\mathbb{F}_d\setminus\{0,-1\})$ is stable under the action of $\mathbb{P}(\Gamma)$. We thus now restrict to $\mathbb{F}_d\setminus\{0,-1\}$.

Lemma 2.7. *For $\gamma\in\Gamma$, let $\overline{\gamma}=(\epsilon^{-1}\circ\mathbb{P}(\gamma)\circ\epsilon)|_{\mathbb{F}_d\setminus\{0,-1\}}$ and set $\overline{\Gamma}=\langle\overline{\iota},\overline{\theta}\rangle$. Then $\overline{\Gamma}\simeq\mathfrak{S}_3$ and, for all $a\in\mathbb{F}_d\setminus\{0,-1\}$,*

$$\overline{\iota}(a)=-1-a\ ,\quad \overline{\theta}(a)=-1-\frac{1}{a}\ .$$

Further $\overline{\iota}$ has exactly one fixed point $\frac{d-1}{2}$; if $d\equiv -1 \mod 3$, $\overline{\theta}$ has no fixed points; if $d\equiv 1 \mod 3$, $\overline{\theta}$ has two fixed points ω and ω^2, where ω is a primitive cubic root of unity in $\mathbb{F}_d$.

Proof. One checks that $(a:a+1)=(b+1:b)\Leftrightarrow b=-1-a$, and that $-1-a=a\Leftrightarrow a=\frac{d-1}{2}$, hence the assertions about $\overline{\iota}$; similarly, $(-1:-1-a)=(b+1:b)\Leftrightarrow b=-1-\frac{1}{a}$, and $-1-\frac{1}{a}=a\Leftrightarrow a^2+a+1=0$, hence the assertions about θ. The assertion about $\overline{\Gamma}$ is a straightforward verification. □

One also shows that $\overline{\kappa}(a)=-\frac{a}{a+1}$ (fixed point: -2), $\overline{\lambda}(a)=\frac{1}{a}$ (fixed point: 1), $\overline{\theta}^2(a)=-\frac{1}{1+a}$ (same fixed points as θ).

It follows that the orbit of $\frac{d-1}{2}$ under $\overline{\Gamma}$ consists of itself, $\overline{\theta}(\frac{d-1}{2})=1$ and $\overline{\theta}^2(\frac{d-1}{2})=-2$; when $d\equiv 1 \mod 3$, the orbit of ω such that $1+\omega+\omega^2=0$ consists of itself and $\iota(\omega)=\omega^2$. Since there are no more fixed points, all other orbits of elements of $\mathbb{F}_d\setminus\{0,-1\}$ have full cardinal 6. This completes the proof of Corollary 2.6. □

Remark 2.8. For $a\in\mathbb{F}_d\setminus\{0,-1\}$, $\epsilon(a)=(a+1:a)=(1:s(a))=(-1:\overline{\kappa}(a))$. It follows that

$$\mathbb{P}(\theta)(a+1:a)=\mathbb{P}(\theta)\circ\epsilon(a)=\epsilon(\overline{\theta}(a))=(-1:\overline{\kappa}\circ\overline{\theta}(a))=(-1:\overline{\iota}(a))\ ,$$

and similar equalities with the other elements of $\overline{\Gamma}$, *e.g.* $\mathbb{P}(\iota)(a+1:a)=(-1:\overline{\theta}(a))$.

Since $\{L_0,L_{-1},L_{(1:1)}\}$ is an orbit of $\mathcal{L}$ under the action of Γ, we could have expressed an analogous statement to that of Theorem 2.5 for the original arrangement $\{L_a:1\leqslant a\leqslant d-2\}$ of lines. The next result, which is a direct consequence of Proposition 2.2, justifies considering the Lazard arrangement instead.

Corollary 2.9. *For $(i,j)\in(\mathbb{F}_d)^2$, let $\mathcal{N}_{i,j}$ denote the number of lines in $\mathcal{L}$ containing (i,j). Then, for any such (i,j):*

$$dT_{i,j}=\mathcal{N}_{i,j}-1\ .$$

In other words, the incidence matrix $\mathcal{N}$ of the Lazard arrangement $\mathcal{L}$ equals $(dT_{i,j}+1)_{i,j}$. It follows that the number of zero entries of the multiplication table, namely $d^2-c(\alpha)$, equals the number of points in $(\mathbb{F}_d)^2$ that belong to exactly one line of $\mathcal{L}$.

2.5 Complexity

In view of Corollary 2.9, we wish to count the number of entries equal to 1 in the incidence matrix $\mathcal{N}$ of the Lazard arrangement $\mathcal{L}$, namely the number of points in $(\mathbb{F}_d)^2$ that belong to exactly one line of $\mathcal{L}$. In order to do so, we may count, for each $(b:a)\in\mathbb{P}(\mathbb{F}_d)$, the number of points of $L_{(b:a)}$ that belong

to no other line of $\mathcal{L}$. We first explicit the intersection point of two such lines — recall they are pairwise convergent, since they all have different slopes.

Proposition 2.10. *For $a \in \mathbb{F}_d$, $L_{(a+1:a)} \cap L_{(1:1)}$ consists of the point with both coordinates equal to $P(1,-a)$; for $a \neq a' \in \mathbb{F}_d$, $L_{(a+1:a)} \cap L_{(a'+1:a')}$ consists of the point of coordinates*

$$x_a(a') = \frac{(a+1)P(1,-a') - (a'+1)P(1,-a)}{a-a'}, \quad y_a(a') = \frac{aP(1,-a') - a'P(1,-a)}{a-a'} .$$

Proof. Let $(b:a) \neq (b':a')$ in $\mathbb{P}(\mathbb{F}_d)$, then the coordinates of the intersection point of $L_{(b:a)}$ and $L_{(b':a')}$ are obtained solving the linear system:

$$\left(\frac{b'P(b,a) - bP(b',a')}{ab'-a'b}, \frac{a'P(b,a) - aP(b',a')}{ab'-a'b} \right) .$$

Specialising at $b = a+1, a' = b' = 1$ yields the point with both coordinates equal to $-P(a+1,a)$, which also equals $P(1,-a)$ using Proposition 2.3 applied to κ. Together with this equality, the specialisation at $b = a+1$, $b' = a'+1$ yields the result. □

Remark 2.11. One checks for $a \in \mathbb{F}_d \setminus \{0,-1\}$: if $a \neq 1$, $x_a(\overline{\lambda}(a)) = x_a(\frac{1}{a}) = 0$, so $L_a \cap L_{\overline{\lambda}(a)} = L_a \cap L_{-1}$; if $a \neq -2$, $y_a(\overline{\kappa}(a)) = y_a(-\frac{a}{1+a}) = 0$, so $L_a \cap L_{\overline{\kappa}(a)} = L_a \cap L_0$. Of course one also has, if $a \neq \frac{d-1}{2}$: $L_a \cap L_{\overline{\iota}(a)} = L_a \cap L_{(1:1)}$.

We can now compute the number of 1s on the diagonal of $\mathcal{N}$, namely the number of zeros on the diagonal of the multiplication table.

Proposition 2.12. *The number of zero entries on the diagonal of the multiplication table $T_\phi(\alpha)$ equals $d - |\{P(1,-a) : a \in \mathbb{F}_d\}|$ and is at least $\frac{d-1}{2}$. The same holds for the first row and column.*

Proof. Note that $\mathcal{N}_{i,i} \geqslant 1$ for $0 \leqslant i \leqslant d-1$, since (i,i) belongs to the diagonal $L_{(1:1)}$. Further $\mathcal{N}_{i,i} \geqslant 2$ if and only if there exists $a \in \mathbb{F}_d$ such that $(i,i) \in L_{(a+1:a)}$, namely such that $i = P(1,-a)$ in view of Proposition 2.10. This proves the claimed equality. Note in passing that $\mathcal{N}_{0,0}$ is never 0 since $P(1,1) = P(1,0) = 0$ (it is at least 3).

Proposition 2.3 applied to λ, together with P being homogeneous of order 1 as a function on $(\mathbb{F}_d)^2$, yields $P(x,y) = -P(-x,y-x) = P(x,x-y)$, hence $P(1,-a) = P(1,-(-1-a))$ for all $a \in \mathbb{F}_d$; furthermore, $a \mapsto -1-a$ is an order 2 permutation of $\mathbb{F}_d$ with unique fixed point $\frac{d-1}{2}$, so $a \mapsto P(1,-a)$ takes at most $1 + \frac{d-1}{2} = \frac{d+1}{2}$ values on $\mathbb{F}_d$. The claimed inequality follows.

The assertion about the first row (resp. column) of the multiplication table can be proved analogously, replacing the diagonal of $\mathcal{N}$ by its first row (resp. column), or using Proposition 1.1 since Γ exchanges the diagonal and the axes of $(\mathbb{F}_d)^2$, thus the diagonal and the first row and column of $\mathcal{N}$. □

Remark 2.13. It is possible to show that the number of zero entries in the multiplication table is at least $\frac{3}{2}(3d-7)$, namely that the complexity of α satisfies $c(\alpha) \leqslant d^2 - \frac{9}{2}d + \frac{21}{2}$. This is not an asymptotically good bound, since the ratio $(d^2 - \frac{9}{2}d + \frac{21}{2})/d^2$ tends to 1 when d goes to infinity, indicating than the number of non zero entries is at most the total number of entries, which is obvious.

On the other hand, Equality (2) and the definition of $N_{i,j}$ enable to write a computer program that computes the exact complexity of α for a large number of prime numbers d. We present the results of these experiments in the following table, where N_d denotes the effective number of zeros in the multiplication table and B_d the lower bound given in the preceding theorem.

d	5	7	11	13	17	19	23	29	31
N_d	12	24	54	69	126	132	195	393	336
N_d/B_d	1.00	1.14	1.38	1.44	1.91	1.76	2.10	3.27	2.60
N_d/d^2	0.48	0.49	0.45	0.41	0.44	0.37	0.37	0.47	0.35

For larger values of d, one observes that the ratio N_d/B_d is roughly bounded up by $d/10$, whereas N_d/d^2 tends to a value close to $1/3$ (between 0.36 and 0.37 to be more precise).

We now compare these results with the lowest complexities found in [APV12], for finite fields extensions. For each prime d between 5 and 17, and each prime p between 2 and 19, we indicate the **global** complexity $C_d = d^2 - N_d$ of the cyclotomic self-dual normal basis and the complexity of its reduction at various primes p (when it makes sense), as well as the lowest complexity among all self-dual normal bases for the extension $\mathbb{F}_{p^d}/\mathbb{F}_p$ (when it has been computed, between curly brackets).

d	5	7	11	13	17	19	23
$\mathbb{F}_2$	9 (9)	21 (21)	57 (21)	81 (45)	141 (81)	189 (117)	285 (45)
$\mathbb{F}_3$	13 (13)	25 (25)	− (55)	100 (67)	160 (91)	229 (172)	328 (127)
$\mathbb{F}_5$	− (13)	25 (25)	67 (64)	100 (85)	163 (157)	229 (153)	334 (?)
$\mathbb{F}_7$	− (16)	− (19)	67 (61)	100 (96)	163 (?)	229 (?)	334 (?)
$\mathbb{F}_{11}$	13 (13)	25 (25)	− (31)	100 (100)	163 (?)	229 (?)	334 (?)
$\mathbb{F}_{13}$	13 (13)	25 (25)	67 (64)	− (37)	163 (?)	229 (?)	334 (?)
$\mathbb{F}_{17}$	13 (13)	25 (25)	67 (64)	100 (100)	163 (?)	229 (?)	334 (?)
$\mathbb{F}_{19}$	13 (13)	− (31)	67 (67)	− (?)	163 (?)	229 (?)	334 (?)
C_d	**13**	**25**	**67**	**100**	**163**	**229**	**334**

The large hyphens "−" indicate that the number field extension $M_d/\mathbb{Q}$ does not reduce to a finite field extension of degree d modulo p. This happens in two cases, namely when $p = d$ or when p splits into d prime ideals of the ring of integers of M_d. The residual extension is trivial in both cases. To determine the decomposition of a prime p in $M_d/\mathbb{Q}$, we use the following.

Lemma 2.14. *Let p, d be primes with $d \geqslant 3$, then p splits in $M_d/\mathbb{Q}$ if and only if $p^{d-1} \equiv 1 \mod d^2$.*

Proof. If $p = d$ then p is totally ramified in $M_d/\mathbb{Q}$ and $p^{d-1} \equiv 0 \mod d^2$. If $p \neq d$, we know from [Was82, Theorem 2.13] that p splits into $\frac{d(d-1)}{f}$ prime ideals in $\mathbb{Q}(\zeta_{d^2})/\mathbb{Q}$, where f denotes the order of p modulo d^2. It follows that p splits in $M_d/\mathbb{Q}$ if and only if d divides $\frac{d(d-1)}{f}$, namely f divides $d-1$, which yields the result. □

When p splits or ramifies in $M_d/\mathbb{Q}$, our construction has no utility to study the residual extension $\mathbb{F}_{p^d}/\mathbb{F}_p$. However when $p = d$, the lowest complexity $3d - 2$ is obtained by the self-dual normal basis described in [BGM94]. When p splits in $M_d/\mathbb{Q}$, one may use a similar construction, replacing ζ_{d^2} by ζ_{d^n} for some integer $n \geqslant 3$, such that the residual degree of p in $\mathbb{Q}(\zeta_{d^n})/\mathbb{Q}$ is d. Denoting by $M_d^{(n)}$ the subextension of $\mathbb{Q}(\zeta_{d^n})/\mathbb{Q}$ of index $d-1$, and letting $\alpha_d^{(n)} = \frac{1+\mathrm{Tr}(\zeta_{d^n})}{d}$, where the trace is from $\mathbb{Q}(\zeta_{d^n})$ to $M_d^{(n)}$, we get a self-dual normal basis generator for $M_d^{(n)}$ over $\mathbb{Q}$, which reduces to an element with the same property for $\mathbb{F}_{p^d}$ over $\mathbb{F}_p$.

References

APV12 F. Arnault, E. J. Pickett, and S. Vinatier, *Construction of self-dual normal bases and their complexity.*, Finite Fields Appl. **18** (2012), no. 2, 458–472.

BGM94 I. F. Blake, S. Gao, and R. C. Mullin, *Normal and self-dual normal bases from factorization of* $cx^{q+1} + dx^q - ax - b$, SIAM J. Discrete Math. **7** (1994), no. 3, 499–512.

Ere88 B. Erez, *The Galois Structure of the Trace Form in Extensions of Odd Prime Degree*, J. Algebra **118** (1988), 438–446.

Was82 L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

Stéphane Vinatier

Chapitre 5

Combinatoire

Dans ce dernier chapitre nous rendons compte d'un travail sur un thème un peu éloigné des précedents, qui a donné lieu à l'article *Permuting the partitions of a prime*, publié au Journal de Théorie des Nombres Bordeaux, volume 21 de l'année 2009, numéro 2, pages 455–465. Son objet est l'étude des partitions d'un premier impair p dont la somme des parts, pondérée par leurs indices, est tantôt divisible par p, tantôt non, selon l'ordre dans lequel on les range. La caractérisation de ces partitions est relativement simple et fait apparaître nettement un phénomène particulier lorsque $p = 3$, qui se trouve être le seul premier impair pour lequel de telles partitions n'existent pas.

Dans la deuxième section de l'article ci-dessous, on tente de montrer de quelle manière cette propriété est liée à la théorie des modules galoisiens, plus précisément à l'étude qui en est faite dans l'article [Vin05] reproduit en fin de chapitre 2, dans lequel les symétries (sous l'action de la conjugaison par le groupe de Galois de l'extension) sont utilisées de façon cruciale pour factoriser une expression bâtie sur un générateur de base normale auto-duale de la racine carrée d'une 3-extension faiblement ramifiée de $\mathbb{Q}$. Ce qui est montré en fin de section 2 est justement la disparition de ces symétries dès lors qu'il existe des partitions comme ci-dessus.

Ce résultat pourrait paraître essentiellement négatif, en ce qu'il indique que la méthode explicite utilisée dans [Vin05] ne peut être étendue au cas des p-extensions pour $p \geq 5$. Cependant il est déjà positif d'avoir une bonne raison de ne pas se lancer dans des calculs complexes et sans espoir. Par ailleurs, la caractérisation qui est donnée des partitions satisfaisant la propriété ci-dessus a attiré l'attention de quatre combinatoristes hongrois (A. Gàcs, T. Héger, Z.L. Nagy et D. Pàlvölgyi). Dans [GHNP10], ils reformulent ce résultat en termes de multiset sur un corps fini (et généralisent à tous les corps finis), en donnent une nouvelle preuve beaucoup plus combinatoire, basée sur le *Combinatorial Nullstellensatz* d'Alon ([Alo99]), le réinterprètent en termes de multisets des valeurs d'un polynôme sur un corps finis, d'arrangements d'hyperplans (ce que j'annonçais vouloir faire à la fin de la première section de l'article ci-dessous), et le relient à la conjecture de Snevily ([Sne99]).

Celle-ci stipule que, étant donnés un groupe abélien d'ordre impair G, un entier naturel n inférieur ou égal à l'ordre de G et deux ensembles $\{a_1, \ldots, a_n\}$ et $\{b_1, \ldots, b_n\}$ d'éléments de G de même cardinal n, il existe une permutation π telle que les produits $a_i b_{\pi(i)}$ soient tous distincts. C'est dans la version prouvée par Alon dans [Alo00], où G est d'ordre premier et l'un des ensembles peut être remplacé par un multiset, que cette conjecture est la plus proche du problème de partitions dont nous sommes partis. La conjecture sous sa forme initiale a été récemment prouvée par Arsovski dans [Ars11].

Permuting the partitions of a prime

Stéphane Vinatier

Abstract

Given an odd prime number p, we characterize the partitions $\underline{\ell}$ of p with p *non negative* parts $\ell_0 \geqslant \ell_1 \geqslant \ldots \geqslant \ell_{p-1} \geqslant 0$ for which there exist permutations σ, τ of the set $\{0, \ldots, p-1\}$ such that p divides $\sum_{i=0}^{p-1} i\ell_{\sigma(i)}$ but does not divide $\sum_{i=0}^{p-1} i\ell_{\tau(i)}$. This happens if and only if the maximal number of equal parts of $\underline{\ell}$ is less than $p-2$. The question appeared when dealing with sums of p-th powers of resolvents, in order to solve a Galois module structure problem.

1. Formulation of the main result

Let p denote an odd prime number and consider the set $\mathcal{C}$ of all p-uples $\underline{\ell} = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ of non negative integers such that

$$\ell_0 + \ell_1 + \cdots + \ell_{p-1} = p \ .$$

We call the elements of the set $\mathcal{C}$ the *compositions* of p and the integers ℓ_i appearing in the composition $\underline{\ell}$ its *parts*, even for the zero ones. The *length* of the composition $\underline{\ell}$ is the number of its non zero parts.

Let $\mathfrak{S}$ denote the permutation group of $\{0, 1, \ldots, p-1\}$. We let $\mathfrak{S}$ act on $\mathcal{C}$ through its action on the indices of the compositions:

$$\sigma(\underline{\ell}) = (\ell_{\sigma(0)}, \ell_{\sigma(1)}, \ldots, \ell_{\sigma(p-1)})$$

for all $\sigma \in \mathfrak{S}$, $\underline{\ell} \in \mathcal{C}$. Each coset of $\mathcal{C}$ for this action has a unique representative with non increasing parts:

$$\ell_0 \geqslant \ell_1 \geqslant \cdots \geqslant \ell_{p-1} \ ;$$

such a composition is called a *partition* of p. We shall also call *partition* its coset and we let $\mathcal{P}$ denote the set of all partitions of p.

Given a composition $\underline{\ell}$, we are interested in the divisibility by p of the sum $S(\underline{\ell})$ of its parts multiplied by their index:

$$S(\underline{\ell}) = \sum_{i=0}^{p-1} i\ell_i \ .$$

The main result of this paper is a characterization of the cosets that contain compositions $\underline{\ell}$ for which $S(\underline{\ell})$ is divisible by p and compositions for which it is not. In other words, we are interested in determining those partitions $\underline{\ell} \in \mathcal{P}$ such that:

$$\exists\, \sigma, \tau \in \mathfrak{S}, \quad p \mid S(\sigma(\underline{\ell})) \quad \text{and} \quad p \nmid S(\tau(\underline{\ell})) \ . \tag{1}$$

Considering the most basic partitions of p, $(p, 0, \ldots, 0)$ and $(1, \ldots, 1)$, one sees at once that p divides $S(\sigma(\underline{\ell}))$ for all $\sigma \in \mathfrak{S}$ in both cases. At the contrary, using the fact that p is prime, one checks that p never

2000 Mathematics Subject Classification 05A17; 05A10; 11P83.
Keywords: partitions of a prime; sums of resolvents; multinomials.

divides $S(\sigma(\underline{\ell}))$ when $\underline{\ell}$ is chosen among the partitions of the kind $(p-k,k,0,\dots,0)$, $1 \leqslant k \leqslant \frac{p-1}{2}$ or $\underline{\ell} = (2,1,\dots,1,0)$. All these "basic" partitions are clearly characterized by the fact that their *maximal number of equal parts*, denoted $m(\underline{\ell})$, is at least $p-2$. Indeed the main result states that they are the only ones that do not satisfy condition (1).

In order to get one further characterization, let $e_k(\underline{\ell})$ denote, for $0 \leqslant k \leqslant p$, the number of parts of $\underline{\ell}$ equal to k:

$$e_k(\underline{\ell}) = \#\{0 \leqslant i \leqslant p-1 \mid \ell_i = k\} \ .$$

Obviously, $m(\underline{\ell}) = \max\{e_k(\underline{\ell}),\ 0 \leqslant k \leqslant p-1\}$. Consider the p-uple:

$$\underline{e}(\underline{\ell}) = \big(e_0(\underline{\ell}),\dots,e_{p-1}(\underline{\ell})\big) \ .$$

If $\underline{\ell}$ is distinct from $(p,0,\dots,0)$, all its parts are less than p; their total number is always p in our setting, therefore $\underline{e}(\underline{\ell})$ is a composition of p, namely

$$\sum_{k=0}^{p-1} e_k(\underline{\ell}) = p \ .$$

Further we note $\underline{e}(\underline{\ell})! = e_0(\underline{\ell})! \cdot e_1(\underline{\ell})! \cdots e_{p-1}(\underline{\ell})!$; this expression equals the cardinal of the stabilizer of $\underline{\ell}$ under the action of $\mathfrak{S}$. The main result is as follows.

Theorem. *Let $\underline{\ell}$ be a partition of p. The following assertions are equivalent:*

(i) $\exists\, \sigma,\tau \in \mathfrak{S}$ *such that* $p \mid S(\sigma(\underline{\ell}))$ *and* $p \nmid S(\tau(\underline{\ell}))$;

(ii) $m(\underline{\ell}) < p-2$;

(iii) $\underline{e}(\underline{\ell})! < (p-2)!$.

We prove the Theorem in section 3. The heart of the proof is Lemma 3.2, which is proven in two parts, depending on the length of $\underline{\ell}$, both elementary. One more characterization, involving a larger family of partitions, will be given in section 4.

Such problems about "permuted partitions" do not seem to have appeared in combinatorics or in number theory so far; in particular, the very rich account on the theory of partitions by Andrews [And98] does not mention such questions. In section 2, we explain how this problem came up while trying to compute sums of p-th powers of resolvents (in order to solve a Galois module structure question), starting from case $p=3$ where the computation is a part of Lagrange's resolvent method to solve the general cubic equation.

Applications of this result will be given in a forthcoming paper, in terms of arrangements of hyperplanes over the finite field with p elements $\mathbb{F}_p$.

2. A motivation for the main result

Lagrange's resolvent method for the cubic equation has the following pattern. Let t_0,t_1,t_2 denote the roots of a given monic cubic polynomial P in some fixed algebraic closure of the base field, let ζ denote a primitive cubic root of unity and define

$$y = t_0 + \zeta t_1 + \zeta^2 t_2 \ ,\ z = t_0 + \zeta^2 t_1 + \zeta t_2 \ .$$

Then y^3 and z^3, the *Lagrange resolvents*, are the roots of a polynomial of degree 2 which coefficients are invariant under the permutation group of $\{t_0,t_1,t_2\}$, hence can be expressed in terms of the coefficients of P. Therefore y^3 and z^3 have an expression in terms of these coefficients, from which one easily

deduces one for t_0, t_1, t_2 (see [DM96] for technical and historical details). The coefficients of the degree 2 polynomial are $y^3 + z^3$ and $y^3 z^3$ and are both easy to compute. In particular,

$$y^3 + z^3 = 2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3 \ ,$$

where $\sigma_1, \sigma_2, \sigma_3$ denote the elementary symmetric functions of the roots and equal the coefficients of P modulo a sign.

Considering the analogous computation when 3 is replaced by any odd prime p may be of some interest. Given p conjugate numbers[(1)] $t_0, t_1, \dots, t_{p-1}$ and a primitive p-th root of unity ζ, one may define *generalized resolvents*

$$y_k = \sum_{i=0}^{p-1} \zeta^{ik} t_i \ , \quad 1 \leqslant k \leqslant p-1 \ ,$$

and may be willing to compute the sum of their p-th powers

$$y_1^p + y_2^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \Big(\sum_{i=0}^{p-1} \zeta^{ik} t_i \Big)^p \ .$$

Of course for p greater than 3, this expression is no longer symmetric under the permutation group of $\{t_0, \dots, t_{p-1}\}$, hence not expressible in terms of the elementary symmetric functions. Yet a sum of such expressions appears in [Vin05], and it is shown that its valuation at p bears information about the Galois module structure of the "square root of the inverse different" ideal of a weakly ramified p-extension of the rationals. In that paper, the author was able to achieve the computation only in the case $p = 3$, using the above calculation.

Developping the p-th power with the help of Newton's multinomial formula yields

$$y_1^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \sum_{\underline{\ell} \in \mathcal{C}} \frac{p!}{\underline{\ell}!} \prod_{i=0}^{p-1} \Big(\zeta^{ik} t_i \Big)^{\ell_i},$$

where we let $\underline{\ell}!$ denote the product of the factorials of the parts of $\underline{\ell}$:

$$\underline{\ell}! = \ell_0! \cdot \ell_1! \cdots \ell_{p-1}! \ ,$$

so $p!/\underline{\ell}!$ equals the multinomial coefficient $\binom{p}{\ell_0, \dots, \ell_{p-1}}$. Since this coefficient only depends on the partition containing $\underline{\ell}$, we index the second sum by partitions instead of compositions and use the action of $\mathfrak{S}$ on partitions to recover all the compositions. Taking into account the fact that a composition $\underline{\ell}$ is fixed by exactly $\underline{e}(\underline{\ell})!$ permutations (this number also only depends on the partition containing $\underline{\ell}$), we get

$$y_1^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \sum_{\mathcal{P} \times \mathfrak{S}} \frac{p!}{\underline{\ell}!\, \underline{e}(\underline{\ell})!} \Big(\prod_{i=0}^{p-1} \Big(\zeta^{ik} t_i \Big)^{\ell_{\sigma(i)}} \Big) \ ,$$

where the second sum is on couples $(\underline{\ell}, \sigma) \in \mathcal{P} \times \mathfrak{S}$. Further

$$\prod_{i=0}^{p-1} \Big(\zeta^{ik} t_i \Big)^{\ell_{\sigma(i)}} = \zeta^{k \sum_{i=0}^{p-1} i\ell_{\sigma(i)}} \cdot \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \ \text{ and } \ \sum_{k=1}^{p-1} \zeta^{k \sum_{i=0}^{p-1} i\ell_{\sigma(i)}} = p-1 \text{ or } -1 \ ,$$

(1) $t_0, t_1, \dots, t_{p-1}$ may equally be considered as indeterminates in fact.

depending on whether p divides $S(\sigma(\underline{\ell})) = \sum_{i=0}^{p-1} i\ell_{\sigma(i)}$ or not, hence

$$\begin{aligned} y_1^p + \cdots + y_{p-1}^p &= \sum_{\mathcal{P}\times\mathfrak{S}} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!}\Big(\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}}\Big)\Big(\sum_{k=1}^{p-1}\zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}}\Big) \\ &= (p-1)\sum_{\mathcal{P}\times\mathfrak{S}} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!}\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \;-\; p\sum_{(\mathcal{P}\times\mathfrak{S})^*} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!}\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \\ &= (p-1)(t_0+\cdots+t_{p-1})^p \;-\; p\sum_{(\mathcal{P}\times\mathfrak{S})^*} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!}\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \;\;, \end{aligned}$$

where the subscript $(\mathcal{P}\times\mathfrak{S})^*$ means that $(\underline{\ell},\sigma)$ runs among the couples in $\mathcal{P}\times\mathfrak{S}$ such that p does not divide $S(\sigma(\underline{\ell}))$.

It now clearly appears that the non-symmetric aspect of the expression $y_1^p + \cdots + y_{p-1}^p$ is linked to the existence of partitions of p satisfying condition (1). This happens as soon as p is greater than 3, as is easily deduced from the Theorem, for which we shall now give a proof.

3. The proof of the main result

Let $\underline{\ell}$ denote a partition of p. Recall that the Theorem states the equivalence of the following assertions:

(i) $\exists\,\sigma,\tau\in\mathfrak{S}$ such that $p \mid S(\sigma(\underline{\ell}))$ and $p \nmid S(\tau(\underline{\ell}))$;

(ii) the maximal number of equal parts of $\underline{\ell}$ satisfies: $m(\underline{\ell}) < p-2$;

(iii) the cardinal of the stabilizer of $\underline{\ell}$ under $\mathfrak{S}$ satisfies: $\underline{e}(\underline{\ell})! < (p-2)!$.

Proof. First assume assertion (ii) is not satisfied, namely $m(\underline{\ell}) \geqslant p-2$, then $m(\underline{\ell}) = e_0(\underline{\ell})$ or $e_1(\underline{\ell})$, and $\underline{\ell}$ is one of the "basic partitions" listed above the Theorem in section 1, hence does not satisfy assertion (i). Further $m(\underline{\ell})! \mid \underline{e}(\underline{\ell})!$, hence (iii) is not satisfied either.

Let us show now that (ii) $\Rightarrow$ (iii). First notice that (ii) never occurs when $p = 3$. If $p \in \{5,7\}$, the implication is easily verified by considering each partition of p separately. For the general case we use the following result.

LEMMA 3.1. *Assume $p \geqslant 11$. Let $\underline{d} = (d_0,\ldots,d_{p-1})$ be a partition of p of length s, such that $d_i \leqslant p-3$ for all i, then*

$$\frac{p!}{\underline{d}!} > 2^{s-2}p(p-1) \;\;.$$

Proof. We shall prove the lemma by induction on s. The case $s = 1$ is irrelevant here. If $s = 2$, $\frac{p!}{\underline{d}!}$ equals the binomial coefficient $\binom{p}{d_0}$. Since $3 \leqslant d_0 \leqslant p-3$,

$$\binom{p}{d_0} \geqslant \binom{p}{3} = p(p-1)\frac{p-2}{6} \;\;.$$

Further $\frac{p-2}{6} > 1$ when $p > 8$, hence the result.

Assume the result is true for some $s \geqslant 2$ and let $\underline{d} = (d_0,\ldots,d_s,0,\ldots,0)$ denote a partition of p with $s+1$ non zero parts, all at most $p-3$. Then we claim that $d_{s-1} + d_s \leqslant p-3$. Otherwise, one would have $d_i \geqslant \frac{d_{s-1}+d_s}{2} > \frac{p-3}{2}$ for all $0 \leqslant i \leqslant s-1$, and

$$p = (d_0+\cdots+d_{s-2}) + (d_{s-1}+d_s) > (s-1)\frac{p-3}{2} + (p-3) \;\;,$$

which implies $p < 3 + \frac{6}{s-1} \leqslant 9$ and contradicts our hypothesis about p. We apply the induction hypothesis to the partition in the coset of $(d_0, \dots, d_{s-2}, d_{s-1}+d_s, 0, \dots, 0)$, it yields

$$\frac{p!}{\underline{d}!} = \frac{p!}{d_0! \dots d_{s-2}!(d_{s-1}+d_s)!} \frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} > 2^{s-2} p(p-1) \frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} \ .$$

Notice that $\frac{(d_{s-1}+d_s)!}{d_{s-1}!d_s!} \geqslant d_{s-1}+d_s \geqslant 2$ to end the proof of the lemma. □

Under assertion (ii), $\underline{\ell}$ is distinct from $(p, 0 \dots, 0)$, hence we may consider the partition $\underline{d}$ of p in the coset of $\underline{e}(\underline{\ell})$; since $m(\underline{\ell}) = \max\{e_k(\ell), 0 \leqslant k \leqslant p-1\}$, all the parts of $\underline{d}$ are less than $p-2$ (and s is at least 2). The lemma yields:

$$\underline{e}(\underline{\ell})! = \underline{d}! < \frac{(p-2)!}{2^{s-2}} \ ,$$

hence assertion (iii) is verified.

We now have to prove (ii) ⇒ (i). We assume again $p \neq 3$ and we denote by s the length of $\underline{\ell}$; then $s = p - e_0(\underline{\ell})$ and one easily checks that, under condition (ii), $3 \leqslant s \leqslant p-2$.

Lemma 3.2. *Let $\underline{\ell}$ be a partition of p with length s satisfying $3 \leqslant s \leqslant p-2$. Then there exist s distinct numbers $a_0, \dots, a_{s-1} \in \{0, \dots, p-1\}$ such that*

$$a_0\ell_0 + \dots + a_{s-1}\ell_{s-1} \equiv 0 \mod p \ .$$

Proof. We first prove the assertion for $3 \leqslant s \leqslant \frac{p+1}{2}$ by induction on s. If $s = 3$, take any $a_0 \in \{0, \dots, p-1\}$, then let $a_1, a_2 \in \{0, \dots, p-1\}$ be such that $a_1 \equiv \ell_2 + a_0 \mod p$ and $a_2 \equiv -\ell_1 + a_0 \mod p$ to get the result.

Assume the assertion is true for the partitions of p of length $s-1$ ($s \geqslant 4$). Then there exist $s-1$ distinct numbers $a_0, \dots, a_{s-2}$ in $\{0, \dots, p-1\}$ such that

$$a_0\ell_0 + \dots + a_{s-2}(\ell_{s-2} + \ell_{s-1}) \equiv 0 \mod p \ .$$

Further we may assume $a_{s-2} \neq 0$, since the same relation is satisfied by the numbers $a_0+1, \dots, a_{s-2}+1$. Let d denote the greatest common divisor of ℓ_{s-2} and ℓ_{s-1}, and let $a, b \in \mathbb{Z}$ be such that $a\ell_{s-2} + b\ell_{s-1} = d$ (Bézout relationship); further set $\alpha = \frac{\ell_{s-2}}{d}$, $\beta = \frac{\ell_{s-1}}{d}$ and $\gamma = \alpha + \beta$. Then the couples $(x, y) \in \mathbb{Z}^2$ satisfying $x\ell_{s-2} + y\ell_{s-1} = d$ are exactly those for which there exists $n \in \mathbb{Z}$ such that $x = a - n\beta$ and $y = b + n\alpha$. Since α and β are invertible modulo p, x and y may take any value modulo p. Further

$$x \equiv y \mod p \Leftrightarrow \gamma n \equiv a - b \mod p \ ,$$

hence $x \not\equiv y \mod p$ occurs for $p-1$ values of the residue of n modulo p. Eventually, $a_{s-2}(\ell_{s-2}+\ell_{s-1}) = a_{s-2}\gamma d = a_{s-2}\gamma x\ell_{s-2} + a_{s-2}\gamma y\ell_{s-1}$ and $a_{s-2}\gamma x \not\equiv a_{s-2}\gamma y \mod p$ simultaneously occur for $p-1$ couples $(x, y) \in \{0, \dots, p-1\}^2$. There remain $p-1-(s-2)$ such couples if one requires further that $a_{s-2}\gamma x \not\equiv a_0, \dots, a_{s-3} \mod p$. Since $s \leqslant \frac{p+1}{2}$ implies $p-1-(s-2) > s-2$, at least one of the values of y is such that $a_{s-2}\gamma y$ is also distinct from the $a_i \bmod p$ for $0 \leqslant i \leqslant s-3$, hence the result when $s \leqslant \frac{p+1}{2}$.

We now consider the case $\frac{p+3}{2} \leqslant s \leqslant p-2$. This assumption is equivalent to

$$2 \leqslant e_0(\underline{\ell}) = p - s \leqslant \frac{p-3}{2} \ .$$

Further, one easily checks that $e_1(\underline{\ell}) \geqslant s - (p-s) = p - 2e_0(\underline{\ell}) \geqslant 3$: starting from the partition $(1, \dots, 1)$, one has to move $p-s$ parts to get a partition of length s. Consider the sum $S_0 = 0 \times \ell_0 + 1 \times \ell_1 + \dots + (s-1)\ell_{s-1}$. Each of the ℓ_i equals 1 when $s - e_1 \leqslant i \leqslant s-1$, hence replacing the coefficient i of ℓ_i in S_0 by $a_i = i+1$ for the last t ($\leqslant e_1$) values of i changes S_0 to $S_t = S_0 + t$. This can be done for any

$t \in \{0, \dots, e_1\}$. If $t > 0$, the largest coefficient in S_t is $a_{s-1} = s$, hence $\leqslant p-2$, so we may perform the operation again without any collision among coefficients modulo p, at most $p-1-(s-1) = e_0$ times. Hence we are able to transform S_0 into a sum S taking any integer value between S_0 and $S_0 + e_0e_1$ (included), with distinct coefficients mod p.

From the above, we know that $e_0e_1 \geqslant pe_0 - 2e_0^2$; when $p \geqslant 11$, one easily shows under our assumption that e_0 lies in the interval where the trinomial $-2e_0^2 + pe_0 - p$ is positive. Hence for $p \geqslant 11$, S can be chosen congruent to 0 mod p, with distinct coefficients a_i mod p as required. The result is easily checked for $p \in \{5, 7\}$. □

The proof of (ii) ⇒ (i) is almost finished. Assuming $m(\underline{\ell}) \leqslant p-3$, the Lemma shows the existence of $\sigma \in \mathfrak{S}$ such that $p \mid S(\sigma(\underline{\ell})) = \sum_{i=0}^{p-1} i\ell_{\sigma(i)}$, taking σ such that $\sigma^{-1}(i) = a_i$ for $0 \leqslant i \leqslant s-1$ (since $\ell_s = \cdots = \ell_{p-1} = 0$). Since the parts ℓ_i are not all equal (otherwise $m(\underline{\ell}) = p$), let j, k be such that $\ell_{\sigma(j)} \neq \ell_{\sigma(k)}$ and let $\tau \in \mathfrak{S}$ be the product of σ with the transposition (j, k). Then

$$\sum_{i=0}^{p-1} i\ell_{\tau(i)} = \sum_{i=0}^{p-1} i\ell_{\sigma(i)} + (j-k)\big(\ell_{\sigma(k)} - \ell_{\sigma(j)}\big) \not\equiv 0 \mod p \ ,$$

since $\ell_{\sigma(k)} - \ell_{\sigma(j)} \equiv 0 \mod p$ can only occur when $\underline{\ell} = (p, 0, \dots, 0)$, which contradicts our hypothesis. This ends the proof of the Theorem. □

Remark. The two parts of the proof of Lemma 3.2, which is the heart of the proof of the Theorem, correspond to two different kinds of partitions: the first case ($s \leqslant \frac{p+1}{2}$) deals with partitions of *small length*, hence there are not too many distinct coefficients to find compared to the number of possibilities, whereas the second case deals with partitions of *large length*, in which case we use the fact that a large number of parts equal 1. Thus the proof is entirely different in the two cases, and one may wonder whether there exists a unifying proof.

The author is not able to give one at the moment. Instead, we shall give in the next section one more characterization of partitions satisfying condition (1) or, almost equivalently, satisfying the conclusion of Lemma 3.2. It involves a larger family of partitions.

4. Around the main result: "derived" partitions

As we have noticed above, given a partition $\underline{\mathcal{L}}$ of p which is distinct from $(p, 0, \dots, 0)$, the associated p-uple $\underline{e}(\underline{\mathcal{L}}) = \big(e_0(\underline{\mathcal{L}}), \dots, e_{p-1}(\underline{\mathcal{L}})\big)$ is a composition of p. Consider the sum $S(\underline{e}(\underline{\mathcal{L}}))$: in $\sum_{k=0}^{p-1} ke_k(\underline{\mathcal{L}})$, each integer k appears $e_k(\underline{\mathcal{L}})$ times as in $\underline{\mathcal{L}}$, hence

$$\sum_{k=0}^{p-1} ke_k\big(\underline{\mathcal{L}}\big) = \sum_{i=0}^{p-1} \mathcal{L}_i = p \ .$$

Consequently, the conclusion of Lemma 3.2 becomes obvious for $\underline{\ell}$ if there exists a partition $\underline{\mathcal{L}}$ of p distinct from $(p, 0, \dots, 0)$ such that $\underline{\ell}$ is the partition in the coset of $\underline{e}(\underline{\mathcal{L}})$.

Let us say that $\underline{\ell}$ *derives from* $\underline{\mathcal{L}}$ in this situation, that is when there exists $\sigma \in \mathfrak{S}$ such that $\sigma(\underline{\ell}) = \underline{e}(\underline{\mathcal{L}})$. More precisely, one has the following equivalence.

Lemma 4.1. *A partition $\underline{\ell}$ of p derives from a partition of p if and only if there exists $\sigma \in \mathfrak{S}$ such that $S(\sigma(\underline{\ell})) = p$.*

Proof. If $\underline{\ell}$ derives from $\underline{\mathcal{L}}$, let $\sigma \in \mathfrak{S}$ be such that $\sigma(\underline{\ell}) = \underline{e}(\underline{\mathcal{L}})$, then $S(\sigma(\underline{\ell})) = p$. If $S(\sigma(\underline{\ell})) = p$ for

some $\sigma \in \mathfrak{S}$, let

$$\underline{\mathcal{L}} = (p-1, \dots, p-1, p-2, \dots, p-2, \quad \dots \quad , 1, \dots, 1, 0, \dots, 0) \ ,$$

where each $0 \leqslant i \leqslant p-1$ appears $\ell_{\sigma(i)}$ times. One easily checks that $\underline{\mathcal{L}} \in \mathcal{P}$, and that $\underline{\ell}$ derives from it. □

For instance, the partition $(5,1,1,0,\dots,0)$ of 7 derives from $(4,3,0,\dots,0)$, for which $e_0 = 5$ and $e_3 = e_4 = 1$, hence we get that $0 \times 5 + 3 \times 1 + 4 \times 1 = 7$; the conclusion of Lemma 3.2 is true for the partitions $(p,0,\dots,0)$ and $(1,\dots,1)$ (even though the assumptions are not), and the first one is derived from the second. But, except if $p = 3$, there is no partition of p from which $(1,\dots,1)$ would derive. More generally we show the following criterium.

Lemma 4.2. *Assume $p > 3$ and $\underline{\ell}$ derives from a partition of p, then the length s of $\underline{\ell}$ satisfies:*

$$s \leqslant \frac{1+\sqrt{8p-7}}{2} \ .$$

This implies in particular $s \leqslant \frac{p-1}{2}$ when $p \geqslant 11$.

Proof. By Lemma 4.1, there exists a permutation $\sigma \in \mathfrak{S}$ such that $S(\sigma(\underline{\ell})) = p$, hence $\sum_{i=0}^{p-1} \sigma^{-1}(i)\ell_i = p$; in other words there exist s distinct numbers $a_i \in \{0,\dots,p-1\}$ such that

$$\sum_{i=0}^{s-1} a_i \ell_i = p \ .$$

The smallest sum $\sum_{i=0}^{s-1} a_i\ell_i$ with distinct coefficients $a_i \in \{0,\dots,p-1\}$ is obtained when choosing $a_i = i$ for all i, namely when affecting the biggest parts with the smallest coefficients. Further, since $(1,\dots,1)$ does not derive from any partition of p (here $p \neq 3$), one has $e_1(\underline{\ell}) \leqslant s-1$ hence

$$\sum_{i=0}^{s-1} a_i\ell_i \geqslant \sum_{i=1}^{s-1} i\ell_i \geqslant 2 + \sum_{i=2}^{s-1} i = 1 + \frac{s(s-1)}{2} \ ,$$

which is larger than p when $s > \frac{1+\sqrt{8p-7}}{2}$. □

The condition on the length given in the Lemma is not a sufficient one, even when adding the obvious condition $s \neq 2$: for $p = 7$, it yields $s \leqslant 4$, but $(2,2,2,1,0,0,0)$ is not derived from any partition of 7. Nevertheless, it is optimal since $(3,2,1,1,0,0,0)$ is derived from itself (analogous examples may be found for $p = 11$).

Even so, the conclusion of Lemma 3.2 is true for $(2,2,2,1,0,0,0)$ as well as for $(1,\dots,1)$, hence there are in both cases distinct numbers a_i such that p divides $\sum_{i=0}^{s-1} a_i\ell_i$. Let $\sigma \in \mathfrak{S}$ be such that $\sigma^{-1}(i) = a_i$ for $0 \leqslant i \leqslant s-1$, we get $p \mid S(\sigma(\underline{\ell}))$, and we may build a non increasing p-uple $\underline{\mathcal{L}}$ as in the proof of Lemma 4.1. The difference is that the sum of the parts of $\underline{\mathcal{L}}$ is now divisible by p, but not necessarily equal to p.

Define a *partition of a multiple of p with p parts* to be a p-uple of non negative integers $(\mathcal{L}_0,\dots,\mathcal{L}_{p-1})$ such that $\mathcal{L}_0 \geqslant \mathcal{L}_1 \geqslant \cdots \geqslant \mathcal{L}_{p-1}$ and $\mathcal{L}_0 + \mathcal{L}_1 + \cdots + \mathcal{L}_{p-1} = np$ for some positive integer n. Given such an $\underline{\mathcal{L}}$, say that a partition $\underline{\ell}$ of p *derives from* $\underline{\mathcal{L}}$ if there exists $\sigma \in \mathfrak{S}$ such that

$$\sigma(\underline{\ell}) = \big(e_0(\underline{\mathcal{L}}), \dots, e_{p-1}(\underline{\mathcal{L}})\big) \ .$$

Notice that the parts of $\underline{\mathcal{L}}$ have to be all less than p for this to happen. The proof of Lemma 4.1 readily extends to show the following.

Lemma 4.3. *A partition $\underline{\ell}$ of p derives from a partition of a multiple of p if and only if there exists $\sigma \in \mathfrak{S}$ such that $p \mid S(\sigma(\underline{\ell}))$.*

For instance $(2,2,2,1,0,0,0)$ derives from the partition of 14 with 7 parts $(5,5,2,1,1,0,0)$; $(1,\dots,1)$ derives from the partition of $\frac{p(p-1)}{2}$ with p parts $(p-1,p-2,\dots,1,0)$.

The study of the basic partitions and the help of the Theorem yield the following new characterization.

Corollary 4.1. *Let $\underline{\ell}$ denote a partition of p. Then the following are equivalent:*

(i) $m(\underline{\ell}) \neq p-2$.

(ii) $\exists\, \sigma \in \mathfrak{S}$ *such that* $p \mid S(\sigma(\underline{\ell}))$.

(iii) $\underline{\ell}$ *is derived from a partition of a multiple of* p *with* p *parts.*

Remark. Notice that the partition $(p-2,1,1,0\dots,0)$ derives from all the partitions with maximal number of equal parts $m(\underline{\ell}) = p-2$, namely $(2,1,\dots,1,0)$ and $(p-k,k,0,\dots,0)$, $1 \leqslant k \leqslant \frac{p-1}{2}$. Further, replacing $\underline{e}(\underline{\ell})$ by $\underline{e}'(\underline{\ell}) = \big(e'_0(\underline{\ell}),\dots,e'_{p-1}(\underline{\ell})\big)$ defined by

$$e'_k(\underline{\ell}) = \#\{0 \leqslant i \leqslant p-1 \mid \ell_i \equiv k \mod p\} \ ,$$

we get an analogous characterization of the partitions such that $p \mid S(\sigma(\underline{\ell}))$ for all $\sigma \in \mathfrak{S}$, namely $(1,\dots,1)$ and $(p,0,\dots,0)$: they both satisfy $\underline{e}'(\underline{\ell}) \in (p,0,\dots,0) -$ here we see a partition as a coset of compositions. We obtain:

$$\begin{array}{lll} \exists\, \sigma \in \mathfrak{S},\ p \mid S(\sigma(\underline{\ell})) & \Longleftrightarrow & \underline{e}'(\underline{\ell}) \notin (p-2,1,1,0\dots,0)\ ; \\ \exists\, \tau \in \mathfrak{S},\ p \nmid S(\tau(\underline{\ell})) & \Longleftrightarrow & \underline{e}'(\underline{\ell}) \notin (p,0\dots,0)\ . \end{array}$$

It follows that assertion (1) is also equivalent to:

$$\underline{e}'(\underline{\ell}) \notin (p-2,1,1,0\dots,0) \cup (p,0\dots,0)\ .$$

References

And98 E. G. Andrews, *The theory of partitions*, Cambridge Mathematical Library. Cambridge: Cambridge University Press. xvi, 255 p., 1998.

DM96 J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics. 163. New York, Springer-Verlag. xii, 346 p., 1996.

Vin05 S. Vinatier, *Galois Module Structure in Weakly Ramified 3-Extensions*, Acta Arith. **119** (2005), no. 2, 171–186.

Stéphane Vinatier

XLIM UMR 6172 CNRS / Université de Limoges, Faculté des Sciences et Techniques, 123 avenue Albert Thomas, 87060 Limoges Cedex, France

Bibliographie

[Alo99] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29, Recent trends in combinatorics (Mátraháza, 1995). 157

[Alo00] _____, *Additive Latin transversals*, Israel J. Math. **117** (2000), 125–130. 157

[APV12] F. Arnault, E. J. Pickett, and S. Vinatier, *Construction of self-dual normal bases and their complexity*, Finite Fields Appl. **18** (2012), no. 2, 458–472. 1, 2, 4

[Ars11] B. Arsovski, *A proof of Snevily's conjecture*, Israel J. Math. **182** (2011), 505–508. 157

[AV12] B. Allombert and S. Vinatier, *Ramification in a family of $F/9F \rtimes F/3F$-extensions of the rationals*, submitted (2012). 1, 2, 4

[BC96] D. Burns and T. Chinburg, *Adams operations and integral Hermitian-Galois representations*, Am. J. Math. **118** (1996), no. 5, 925–962. 3

[BF01] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients.*, Doc. Math., J. DMV **6** (2001), 501–570. 6

[BG03] D. Burns and C. Greither, *On the equivariant Tamagawa number conjecture for Tate motives*, Invent. Math. **153** (2003), no. 2, 303–359. 6

[BGS06] N. P. Byott, C. Greither, and B. Sodaïgui, *Realizable classes of non abelian extensions (Classes réalisables d'extensions non abéliennes)*, J. Reine Angew. Math. **601** (2006), 1–27. 6

[Bur95] D. Burns, *On arithmetically realizable classes*, Math. Proc. Cambridge Philos. Soc. **118** (1995), no. 3, 383–392. 6, 37

[Cha84] S. U. Chase, *Ramification invariants and torsion Galois module structure in number fields*, J. Algebra **91** (1984), no. 1, 207–257. 2, 36

[Chi85] T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. (2) **121** (1985), 351–376. 6, 36

[CV13] L. Caputo and S. Vinatier, *Cyclotomic units, Gauss and Jacobi sums related to torsion galois modules*, preprint (2013). 1, 2, 3

[Eic96] Y. Eichenlaub, *Problèmes effectifs de théorie de galois en degrés 8 à 11*, Thèse de doctorat, Université Bordeaux 1, 1996. 107

[Ere88] B. Erez, *The Galois Structure of the Trace Form in Extensions of Odd Prime Degree*, J. Algebra **118** (1988), 438–446. 1, 2, 4, 7, 145

[Ere91] _____, *The Galois Structure of the Square Root of the Inverse Different*, Math.Z. **208** (1991), 239–255. 2, 7

[Frö83] A. Fröhlich, *Galois module structure of algebraic integers*, Springer-Verlag, 1983. 2

[GHNP10] A. Gács, T. Héger, Z. L. Nagy, and D. Pálvölgyi, *Permutations, hyperplanes and polynomials over finite fields*, Finite Fields Appl. **16** (2010), no. 5, 301–314. 4, 157

[Gre89] C. Greither, *Unramified Kummer extensions of prime power degree*, Manuscr. Math. **64** (1989), no. 3, 261–290. 107

[Joh15] H. Johnston, *Explicit integral Galois module structure of weakly ramified extensions of local fields*, Proc. Am. Math. Soc. **143** (2015), no. 12, 5059–5071 (English). 2

[McC87] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. (1987), 259–306. 6

[Pic09] E. J. Pickett, *Explicit Construction of Self-Dual Integral Normal Bases for the Square-Root of the Inverse Different*, J. Number Theory **129** (2009), 1773 – 1785. 3, 7

[Pic10] _____, *Construction of Self-Dual Integral Normal Bases in Abelian Extensions of Finite and Local Fields*, Int. J. Number Theory **6** (2010), no. 7, 1565–1588. 1, 4, 127

[PT13] E. J. Pickett and L. Thomas, *Formal group exponentials and weakly ramified extensions*, submitted (2013). 8

[Pul07] A. Pulita, *Rank one solvable p-adic differential equations and finite abelian characters via Lubin-Tate groups*, Math. Ann. **337** (2007), no. 3, 489–555. 3

[PV12] E. J. Pickett and S. Vinatier, *Exponential power series, Galois module structure and differential modules*, soumis (2012), 21pp. 2, 3

[PV13] _____, *Self-dual integral normal bases and Galois module structure*, Compos. Math. **149** (2013), no. 7, 1175–1202. 1, 2, 3, 8

[Sne99] H. S. Snevily, *Unsolved Problems : The Cayley Addition Table of Z_n*, Amer. Math. Monthly **106** (1999), no. 6, 584–585. 157

[Tay81] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), no. 1, 41–79. 2, 6, 7, 8

[Ull69] S. Ullom, *Galois Cohomology of Ambiguous Ideals*, J. Number Theroy (1969), no. 1, 11–15. 2

[Ull70] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148. 2

[Vin01] S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$*, J. Number Theory **91** (2001), no. 1, 126–152. 2, 7

[Vin02] _____, *Une Famille Infinie d'Extensions Faiblement Ramifiées*, Math. Nachr. **243** (2002), 165–187. 4, 107

[Vin03] _____, *Sur la Racine Carrée de la Codifférente*, J. Théor. Nombres Bordeaux **15** (2003), 393–410. 4, 93

[Vin05] _____, *Galois Module Structure in Weakly Ramified 3-Extensions*, Acta Arith. **119** (2005), no. 2, 171–186. 1, 2, 3, 4, 157

[Vin09] _____, *Permuting the partitions of a prime*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 455–465. 1, 2, 4, 93

[Vin13] _____, *The complexity of cyclotomic self-dual normal bases*, en préparation (2013), 10pp. 1, 2

Éléments explicites en théorie algébrique des nombres

Résumé : Ce mémoire présente une synthèse de mes travaux de recherche en théorie algébrique des nombres menés entre 2003 et 2013, seul ou en collaboration. Ils portent principalement sur l'étude de la structure galoisienne de modules associés à des extensions de corps de nombres, sous diverses hypothèses en particulier de ramification. Ils abordent aussi des thèmes rencontrés chemin faisant : construction d'un certain type d'extensions galoisiennes du corps des rationnels, complexité des bases normales auto-duales pour la multiplication dans les corps finis, un peu de combinatoire. Dans la présentation de tous ces travaux, l'accent est mis sur l'aspect explicite des objets étudiés.

Mots clés : Structure galoisienne, ramification, corps de nombres, sommes de Gauss, résolvantes, bases normales auto-duales.

Explicit elements in algebraic number theory

Abstract: This report consists in a synthesis of my research activities in algebraic number theory, between 2003 and 2013, on my own or with colleagues. The main goal is the study of the Galois module structure of modules associated to number field extensions, under various hypothesis, specifically about ramification. We also present results about other subjects which came into the way of the previous study: the construction of a certain type of Galois extensions of the field of rationals, the complexity of self-dual normal bases for multiplication in finite fields, and a bit of combinatorics. We stress the importance of an explicit knowledge of the objects under study.

Keywords: Galois module structure, ramification, number fields, Gauss sums, resolvants, self-dual normal bases.

XLIM - UMR 7252 CNRS - Université de Limoges
123, avenue Albert Thomas - 87060 LIMOGES cedex