université de BORDEAUX

THÈSE PRÉSENTÉE
POUR OBTENIR LE GRADE DE
DOCTEUR DE L'UNIVERSITÉ DE BORDEAUX

ECOLE DOCTORALE MATHEMATIQUES ET INFORMATIQUE

Par **Fabrice ETIENNE**

Applications algorithmiques des opérateurs de Hecke des groupes finis pour les représentations galoisiennes

Sous la direction de : **Aurel PAGE**

Soutenue le 7 juillet 2025

Membres du jury :

M. Alex Bartel	Professeur	Université de Glasgow	Rapporteur
M. Claus FIEKER	Professeur	Université de Kaiserslautern-Landau	Rapporteur
M. Christian MAIRE	Professeur	Université de Franche-Comté	Examinateur
Mme. Céline MAISTRET	Maitresse de conférence	Université de Bristol	Examinatrice
Mme. Alice PELLET-MARY	Chargée de Recherche	CNRS	Examinatrice
M. Aurel PAGE	Chargé de recherche	INRIA	Directeur

Applications algorithmiques des opérateurs de Hecke des groupes finis pour les représentations galoisiennes

Résumé : Soit G un groupe fini, H, J des sous groupes de G, R un anneau commutatif, et V un $R[G]$-module. À chaque élément de $R[H\backslash G/J]$, le R-module libre sur l'ensemble des doubles classes, on peut associer de manière canonique un morphisme de R-modules qui va de V^J dans V^H, les ensembles des points fixes de V sous les actions de J et de H respectivement. Les morphismes associés de cette manière aux classes HgJ avec $g \in G$ sont appelés *opérateurs de Hecke*. Dans cette thèse, nous étudions les propriétés de ces opérateurs de Hecke, et en particulier dans le cas où $R = \mathbb{Z}$ et où le module V est le groupe des inversibles d'un corps de nombres $\tilde{K}$ galoisien sur $\mathbb{Q}$, de groupe de Galois G. L'action d'un opérateur de Hecke associé à une classe HgJ va alors de $(\tilde{K}^J)^\times$ vers $(\tilde{K}^H)^\times$. Nous développons deux applications principales algorithmiques de ces propriétés. Tout d'abord, un algorithme permettant de calculer de manière inductive le groupe des classes d'un corps de nombres de la forme $\tilde{K}^H$, en se ramenant au calcul sur des corps de plus petits degrés, de la forme $\tilde{K}^{J_i}$, à condition que les groupes G, H et les J_i satisfassent un certain type de relations, que nous appelons "relations de normes généralisées", et dont nous étudions également les propriétés. Ensuite, étant donné un module galoisien fini M, nous décrivons un algorithme permettant de trouver une résolution de M où les morphismes s'expriment sous la forme de sommes d'opérateurs de Hecke. Puis à partir d'une telle résolution, nous concevons un algorithme permettant de calculer les groupes de Selmer du module M.

Mots-clés : Opérateurs de Hecke, Représentations galoisiennes, Cohomologie galoisienne, Foncteurs de Mackey, Algorithmes, Groupes des classes, Groupes de Selmer, Conjecture de Leopoldt

Algorithmic applications of Hecke operators of finite groups for Galois representations

Abstract: Let G be a finite group, H, J two subgroups of G, R a commutative ring, and V a $R[G]$-module. To each element of $R[H\backslash G/J]$, the free R-module on the set of double cosets, we can canonically associate a morphism of R-modules from V^J to V^H, the sets of fixed points of V under the actions of J and H respectively. The morphism associated with the double cosets HgJ with $g \in G$ are called *Hecke operators*. In this thesis, we study the properties of Hecke operators, and in particular the case where $R = \mathbb{Z}$ and where the module V is the group of invertible elements of a number field $\tilde{K}$, Galois over $\mathbb{Q}$, and of Galois group G. Then the action of a Hecke operator associated with a double coset HgJ goes from $(\tilde{K}^J)^\times$ to $(\tilde{K}^H)^\times$. We develop two main algorithmic applications of these properties. First, an algorithm that can compute inductively the class group of a number field of the form $\tilde{K}^H$, by reducing the problem to the same computation for smaller fields, of the form $\tilde{K}^{J_i}$, on the condition that the groups G, H and the J_i satisfy a certain type of relations, that we will call "generalised norm relations", and that we will study. Then, given a finite Galois module M, we will describe an algorithm that can find a resolution of M where the morphisms can be written as sums of Hecke operators. And with such a resolution, we will describe an algorithm to obtain the Selmer groups of the module M.

Keywords: Hecke operators, Galois representations, Galois cohomology, Mackey functors, Algorithms, Class groups, Selmer groups, Leopoldt conjecture

---

Unité de recherche
IMB, UMR 5251 CNRS - Université de Bordeaux - Bordeaux INP.

Acknoledgements /Remerciements

First, I would like to thank all members of the jury, and in particular the two referees, Alex Bartel and Claus Fieker, for taking the time to read this thesis, and for their precious feedback and advice.

Je voudrais remercier chaleureusement Aurel Page, mon directeur de thèse, pour m'avoir proposé ce beau sujet, ainsi que pour la disponibilité, la pédagogie, et la gentillesse dont il a fait preuve. C'était un plaisir et un privilège de pouvoir travailler avec toi.

Mes remerciements vont aussi à tous les autres membres de l'Institut de Mathématiques de Bordeaux, qui participent à créer cette ambiance de travail si riche et chaleureuse à la fois. J'ai une pensée particulière pour les chercheurs et chercheuses de l'équipe CANARI, que je remercie pour leur accueil, leurs conseils, et pour toutes les conversations intéressantes que nous avons pu avoir, qu'elles soient mathématiques ou non. Je n'oublie pas bien sûr les autres doctorant·es de l'équipe. Votre soutien dans les moments difficiles a été pour moi extrèmement précieux, et nos sorties au cinéma, nos soirées jeux de société/ échecs, nos discussions, resteront d'excellents souvenirs. Je vous souhaite le meilleur dans la poursuite de vos parcours accadémiques.

Je suis reconnaissant également pour tous·tes les amis·es que j'ai rencontré·es tout au long de mon parcours, au lycée, en classe préparatoire et à l'ENS. Et aussi pour les amis·es et les camarades que j'ai eu le plaisir de rencontrer dans cette ville de Bordeaux qui était nouvelle pour moi. Une pensée aussi pour les collocataires successif·ves avec qui j'ai habité au cours de ces trois années, qui sont tous·tes des personnes formidables. Mais la plus belle surprise que me réservait cette ville, c'était de faire la rencontre de Sylvain. Merci du fond du coeur pour tous ces moments passés ensemble, et pour ton soutien et tes encouragements pendant la rédaction de cette thèse!

Un immense merci, bien sûr, pour toute ma famille et en particulier mes parents, Sonia et Jean Paul, et ma soeur Lucie. Je vous aime très fort!

Résumé étendu en français

Dans cette thèse, nous étudions les propriétés des opérateurs de Hecke, et nous les utilisons pour obtenir des relations entre certains modules galoisiens. Puis, grâce à ces relations, nous concevons des algorithmes pour calculer des objets arithmétiques tels que des groupes de classes de corps de nombres ou bien des groupes de Selmer de modules galoisiens finis.

Corps de nombres et groupes des classes

Un *corps de nombre* est une extension de corps de degré fini de $\mathbb{Q}$, le corps des rationnels. Si K est un corps de nombre, on notera $\mathbb{Z}_K$ son anneau des entiers, c'est à dire l'anneau de tous les éléments de K qui sont racines d'un polynôme unitaire à coefficients entiers.

Un *idéal fractionnaire* I de l'anneau des entiers $\mathbb{Z}_K$ est un sous $\mathbb{Z}_K$-module de K tel que il existe α un élément non nul de $\mathbb{Z}_K$ qui vérifie $\alpha I \subset \mathbb{Z}_K$.

On dit que deux idéaux fractionnaires J et J' de $\mathbb{Z}_K$ sont *equivalents*, et on note $J \sim J'$, si il existe $x \in K$ non nul tel que $J' = xJ$. C'est une relation d'équivalence. On note $\mathrm{Cl}(K)$ le groupe des classes d'équivalence pour cette relation. C'est le *groupe des classes d'idéaux* de K. Par le théorème du nombre de classes (voir [25]), le groupe des classes d'un corps de nombres K est toujours fini. Son cardinal est apellé le *nombre de classes* de K.

L'étude des groupes des classes de corps de nombres est centrale en théorie des nombres. Ce groupe mesure le "défaut de principalité" de l'anneau $\mathbb{Z}_K$, dans le sens où $\mathbb{Z}_K$ est un anneau principal si et seulement si le groupe $\mathrm{Cl}(K)$ est trivial. Ce groupe joue un rôle important par exemple dans la résolution de certains problèmes Diophantiens.

Dans [13], Buchmann donne un algorithme qui prend en entrée un corps de nombres K et son anneau des entiers $\mathbb{Z}_K$, et donne en sortie la structure du groupe des classes $\mathrm{Cl}(K)$ ainsi qu'une base du groupe des unités $\mathbb{Z}_K^\times$.

La preuve de la correction de cet algorithme suppose l'hypothèse de Riemann généralisée (GRH). Voir [17] pour plus de détails sur cette conjecture, qui est l'une des plus importantes de la théorie des nombres moderne.

La complexité en temps de l'algorithme de Buchmann augmente rapidement avec le degré n du corps de nombres K: en notant Δ_K le discriminant de K (voir [37]), la complexité pour un n fixé est en $\mathcal{O}(e^{a\sqrt{\ln|\Delta_K|\ln\ln|\Delta_K|}})$, où a est une constante, et où la constante implicite du $\mathcal{O}$ dépend de n de manière

exponentielle. Notons aussi que le discriminant croît au moins exponentiellement avec n. C'est en raison de cette croissance rapide de la complexité qu'il est avantageux de trouver des méthodes inductives pour calculer le groupe des classes d'un corps de nombres, en se ramenant au même problème sur des corps auxiliaires de degrés plus petits.

Théorie de Galois et représentations galoisiennes

Théorème fondamental

Soit K/F une extension de corps algébrique finie. Notons $\mathrm{Aut}_F(K)$ le groupe des automorphismes de corps de K dans K qui fixent F, c'est à dire que pour tout $\sigma \in \mathrm{Aut}_F(K)$ et pour tout $x \in F$, on a $\sigma(x) = x$.

Si H est un sous groupe de $\mathrm{Aut}_F(K)$, alors on notera K^H le *corps fixé par* H, défini par $K^H = \{x \in K | \sigma(x) = x \text{ for all } \sigma \in H\}$. C'est un sous-corps de K, contenant F (voir par exemple [32] pour toutes les preuves de cette section).

Si $K^{\mathrm{Aut}_F(K)} = F$, alors on dit que K/F est une *extension galoisienne*, et le groupe $G = \mathrm{Aut}_F(K)$ est appelé son *groupe de Galois*. De plus, on a $G = [K : F]$. Une extension K/F est galoisienne si et seulement si elle est normale et séparable. C'est aussi équivalent à dire que K est le corps de décomposition d'un polynôme séparable $f \in F[X]$.

Soit K/F une extension galoisienne, de groupe de Galois $G = \mathrm{Aut}_K(K)$. Le *théorème fondamental de la théorie de Galois* donne une bijection entre l'ensemble $\mathcal{L}$ des sous-corps de K contenant F et l'ensemble $\mathcal{H}$ des sous groupes de G. La bijection est donnée par les applications

$$\Phi \colon \mathcal{L} \to \mathcal{H}, L \mapsto \mathrm{Aut}_F(L)$$
$$\Phi^{-1} \colon \mathcal{H} \to \mathcal{L}, H \mapsto L^H.$$

De plus, si L est un corps intermédiaire $F \subset L \subset K$, et si $H < G$ est tel que $L = K^H$, alors K est une extension galoisienne de L, de groupe de Galois H. En outre, le corps L est une extension galoisienne de F si et seulement si H est un sous groupe normal de G, et dans ce cas, le groupe de Galois de L/F est isomorphe à G/H.

Les applications Φ et Φ^{-1} forment la *correspondance de Galois*. Notons qu'elle renversent l'inclusion, dans le sens où, si L_1, L_2 sont deux sous corps de K tels que $F \subset L_1 \subset L_2 \subset K$, et si H_1, H_2 sont les sous groupes de G tels que $L_1 = K^{H_1}$ et $L_2 = K^{H_2}$, alors on a $H_2 < H_1$, et vice versa.

Représentations galoisiennes

Dans cette sous-section, nous allons définir les représentations linéaires d'un groupe fini G, ainsi que les modules à gauches et l'algèbre de groupe $R[G]$, avec R un anneau. Puis nous verrons que les représentations linéaires de G sur un corps F sont exactement les $F[G]$-modules. (Voir [45] ou [41]).

Soit V un espace vectoriel sur un corps F, et soit $\mathrm{GL}(V)$ le groupe des isomorphismes de V dans lui même. Soit G un groupe fini. Une *représentation linéaire* de G dans V est un morphisme $\rho\colon G \to \mathrm{GL}(V)$. Notons qu'une représentation linéaire ρ de G dans V donne une action de groupe de G sur V définie par $g \cdot x = \rho(g)(x)$, pour tout $g \in G, x \in V$. Donc V est un G-module.

Soit R un anneau, un R-module à gauche M est un groupe abélien muni d'une opération $\cdot\colon R \times M \to M$ telle que pour tout $r, s \in R$ et $m, n \in M$, on a

- $1 \cdot m = m$
- $r \cdot (m + n) = r \cdot m + r \cdot n$
- $(r + s) \cdot m = r \cdot m + s \cdot m$
- $(rs) \cdot m = r \cdot (s \cdot m)$.

De plus, si M, N sont deux R-modules, alors une application $f\colon M \to N$ est appelé *morphisme de R-modules* si pout tous $x, y \in R$ et pour tout $r \in R$, on a

- $f(x + y) = f(x) + f(y)$,
- $f(r \cdot x) = r \cdot f(x)$.

Si R est un anneau commutatif, alors on peut définir *l'algèbre de groupe de G sur R*, l'ensemble des sommes formelles d'éléments de G, à coefficients dans R:

$$R[G] = \{\sum_{g \in G} a_g g | a_g \in R\}.$$

C'est une R-algèbre, avec la multiplication qui étend celle de G.

Soit V un R-module et soit $\rho\colon G \to \mathrm{GL}(V)$ une représentation linéaire de G dans V. Si on étend par linéarité l'action de groupe $G \times V \to V$ associée à ρ, on voit que V est doté d'une structure de $R[G]$-module à gauche. Et

réciproquement, un $R[G]$-module définit une représentation linéaire de G dans V.

Si le groupe G est le groupe de Galois d'une extension de corps, alors les $R[G]$-modules sont appelés *modules galoisiens* et les représentations de groupe associées sont des *représentations galoisiennes*. Par exemple, si $K/\mathbb{Q}$ est une extension de corps galoisienne, de groupe de Galois G, alors $K^\times$ et $\mathbb{Z}_K^\times$ sont des modules galoisiens, avec $R = \mathbb{Z}$.

Cohomologie des groupes et groupes de Selmer

Rappelons la définition d'un groupe de cohomologie, tel que dans [44]. Soit G un groupe fini et M un G-module. Pour tout entier i, notons $C^i(G, M)$ le groupe abélien des fonctions $f\colon G^i \to M$.

Considérons les applications $d^i\colon C^i(G, M) \to C^{i+1}(G, M)$ sont définies par

$$\begin{aligned}(d^i f)(g_1, \cdots, g_{i+1}) =& f(g_1, \cdots, g_i) + \sum_{j=1}^{i} (-1)^i f(g_1, \cdots, g_j g_{j+1}, \cdots, g_{i+1}) \\ &+ (-1)^{i+1} f(g_2, \cdots, g_{i+1})\end{aligned}$$

On peut définir l'espace des *i-cocycles* $Z^i(G, M) = \ker(d^i)$ et l'espace des *i-cobords* $B^i(G, M) = \mathrm{Im}(d^{i-1})$. Le i-ième groupe de cohomologie de G à coefficients dans M est

$$H^i(G, M) = \frac{Z^i(G, M)}{B^i(G, M)}.$$

Notons par exemple que $H^0(G, M) = M^G$ où M^G est l'ensemble des points fixes.

La propriété principale des groupes de cohomologie est la suivante. Soient A, B, C des G-modules tels qu'il existe une suite exacte courte

$$0 \to A \to B \to C \to 0.$$

Alors, on a une suite exacte infinie de groupes de cohomologie

$$\begin{aligned}0 \to& H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \\ & H^2(G, A) \to H^2(G, B) \to \cdots\end{aligned}$$

L'étude de la cohomologie de groupes des modules galosiens est appelé la *cohomologie galoisienne*.

Les groupes de cohomologie ne sont pas de type fini en général, ce qui les rend souvent difficiles à utiliser en pratique. C'est pourquoi il est intéressant de travailler avec des *groupes de Selmer*. Ce sont des sous-groupes finis des groupes de cohomologie, définis de telle sorte qu'ils contiennent des informations locales importantes. Voir le chapitre 7 pour une définition plus précise.

Organisation et contributions de la thèse

Chapitre 2: Algèbres de Hecke des groupes finis

Ce chapitre est basé sur la première section de l'article [22]. On y définit les opérateurs de Hecke et les algèbres de Hecke, et on décrit certaines de leurs propriétés. Puis on définit la notion de compositums de deux corps de nombres.

Notre contribution est la suivante. Si $\tilde{K}$ est un corps de nombre tel que l'extension $\tilde{K}/\mathbb{Q}$ est galoisienne, de groupe de Galois G, soient H, J deux sous-groupes de G et soient $K = \tilde{K}^H$ et $L = \tilde{K}^J$. Alors on montre qu'il existe une bijection entre l'ensemble des compositums de K et L et l'ensemble des doubles classes $J\backslash G/H$ (voir proposition 2.17).

Alors, il y a une "action" naturelle de l'ensemble des compositums sur l'ensemble des points fixes de diférents $R[G]$-modules, que nous décrivons entre la proposition 2.19 et la proposition 2.23.

Enfin, nous décrivons l'action d'un compositum de K et L, de $L^\times$ vers $K^\times$:

Theorem A. *[Théorème 2.24] Soit x un élément de $K^\times$ et soit (C, ι_K, ι_L) un compositum de K et L. Alors on a $C \cdot x = N_{C/L}(\iota_K(x))$.*

Ce théorème sera surtout utile pour des applications algorithmiques, dans le chapitre 5.

Bien que la bijection entre l'ensemble des doubles classes et l'ensemble des compositums était probablement connue, nous n'avons pas trouvé de références dans la littérature. Il nous semble que le théorème A est bien nouveau, ainsi que ses applications algorithmiques.

Chapitre 3: foncteurs de Mackey

Dans la première section de ce chapitre, nous donnons la définition des foncteurs de Mackey (cohomologiques), ainsi que certaines propriétés, qu'on peut trouver dans [51] et dans [9], et qui permettent de faire un lien entre le formalisme des foncteurs de Mackey et les opérateurs de Hecke.

Ensuite, dans la seconde section, basée sur l'article [1], encore en préparation, nous introduisons la notion de foncteurs de Mackey normés (voir définition 3.14), et donnons quelques exemples. Le résultat principal est le théorème 3.16:

Theorem B. *Soit R un anneau normé, et k son corps des fractions, et soit M un R-foncteur de Mackey normé sur un groupe fini G. Soient $U_1, \cdots U_n$ and $U'_1, \cdots U'_m$ des sous-groupes de G tels qu'il existe un épimorphisme de $k[G]$-modules*

$$\Phi \colon \bigoplus_i k[G/U_i] \to \bigoplus_j k[G/U'_j].$$

Alors, on a une application R-linéaire

$$\phi \colon \bigoplus_{i,j} M(U_i)^{U_i \backslash G / U'_j} \to \bigoplus_j M(U'_j)$$

telle que le changement de base $\phi \otimes k$ est surjectif et telle que ϕ a son opérateur norme borné par

$$\max\{1, \max\{|[U'_i : gU_j g^{-1}]| \text{ for } g \in G, i = 1, \cdots m, \text{ and } j = 1, \cdots, n\}.$$

Ce théorème est intéressant car il peut être utilisé pour obtenir une borne sur l'opérateur norme d'applications linéaires dans des contextes très divers.

Chapitre 4: Relations de normes

Dans [7], les auteurs étudient les propriétés des relations de normes, et les utilisent pour produire des algorithmes pour calculer des invariants arithmétiques de certains corps de nombres par induction, et en particulier la structure de leurs groupes des classes. Le but de ce chapitre est de définir et d'étudier une généralisation des relations de normes.

Dans la première section (4.1), nous rappelons la définition des relations de normes, ainsi que certaines conditions nécessaires et suffisantes à leur

existence, qui ont été démontrées dans [7]. Notre contribution est dans les autres sections, qui sont basées sur [22].

Dans la section 4.2, nous définissons les relations de normes généralisées:

Definition C. *Soit G un groupe fini, et $H < G$ un sous-groupe. Soit $\mathcal{J}$ un ensemble de sous-groupes de G et R un anneau commutatif. Une* relation de norme généralisée sur R par rapport à H et $\mathcal{J}$ *est une égalité dans $R[G]$ de la forme*

$$N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$$

avec $a_i, b_i \in R[G]$, $J_i \in \mathcal{J}$, et $J_i \neq 1$, et avec $N_{J_i} = \sum_{j \in J_i} j$, et $N_H = \sum_{h \in H} h$ les éléments normes de J_i et H.

Et nous donnons des conditions nécessaires et suffisantes à l'existence de relations de normes généralisées. En particulier la proposition suivante (4.14) établit un lien entre les relations de normes généralisées et les opérateurs de Hecke:

Proposition D. *Soit H un sous-groupe de G, et $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ un ensemble de sous-groupes non triviaux de G. Alors, G admet une relation de norme généralisée sur $\mathbb{Q}$ par rapport à H et J si et seulement si il existe un morphisme surjectif de $\mathbb{Q}[G]$-modules*

$$\phi \colon \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$$

où pour tout i, $n_i \in \mathbb{Z}_{>0}$.

Nous définissons aussi une notion de relations de normes généralisées entre corps de nombres (définition 4.15) et dans le théorème 4.22, nous donnons un critère basé sur l'action des compositums:

Theorem E. *Si $L_1, \cdots, L_\ell$ sont des corps de nombres, définis par les polynômes $f_1, \cdots, f_\ell$, et si on note R_i l'ensemble des racines complexes de f_i, alors un corps de nombres $K = \mathbb{Q}(\alpha)$ admet une* relation de norme généralisée par rapport à $L_1, \cdots, L_\ell$, *si et seulement si il existe une relation de la forme*

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in Compo(K, L_i)} \sum_{\beta \in R_i} a_{i,C,\beta} C \cdot \beta$$

où les coefficients $a_{i,C,\beta}$ sont dans $\mathbb{Q}$.

Dans la section 4.3, on définit le coefficient optimal d'une relation de norme généralisée (voir définition 4.24), et nous donnons une borne (théorème 4.28 qui sera utile dans le chapitre suivant pour étudier la complexité en temps de certains algorithmes.

Dans ce chapitre et dans le suivant, on parle surtout de relations de normes généralisées sur $\mathbb{Q}$ ou sur $\mathbb{Z}$, mais dans la section 4.4, on parle brièvement de relations de normes généralisées sur des corps finis, et nous donnons des critères de leur existence (proposition 4.31).

Ensuite, dans la section 4.5, nous donnons des algorithmes pour la recherche de relations de normes généralisées. Enfin, dans la section 4.6, nous comparons notre généralisation des relations de normes et la définition classique, afin de montrer que notre généralisation est bien pertinente.

Chapitre 5: Calcul de groupes des classes

Dans ce chapitre, nous décrivons des algorithmes pour calculer les groupes des classes de certains corps de nombres par induction, en utilisant les propriétés des relations de normes généralisées. Ces méthodes sont similaires à celles décrites dans [7].

Dans la première section, nous présentons des algorithmes pour calculer le groupe des S-unités d'un corps de nombre, ce qui permet indirectement de calculer son groupe des classes. Et les algorithmes présentés dans la deuxième section permettent de calculer plus directement le groupe des classes. Le résultat principal de ce chapitre est le suivant:

Theorem F. *En supposant l'hypothèse de Riemann généralisée, il existe un algorithme en temps polynomial, qui prends en entrée*

- *un corps de nombre K,*
- *un ensemble S de nombres premieers,*
- *des sous-corps K_i de la cloture galoisienne $\tilde{K}$,*
- *pour chaque i, une base du groupe des S-unités de K_i,*

et qui, si K admet une relation de norme généralisée par rapport aux K_i, renvoie une base du groupe des S-unités de K.

Voir l'algorithme 5.9, et le théorème 5.10.

Puis, dans la section 5.3, nous utilisons ces algorithmes (et en particulier l'algorithme 5.12, dont la complexité n'est pas toujours polynomiale, mais qui est plus rapide dans la plupart des cas), implémentés en Pari/GP ([40]), pour calculer le groupe des classes de certains corps de nombres de très grands discriminants. Dans l'exemple 5.18, nous calculons le groupe des classes d'un corps de degré 105 et de discriminant $2^{126} \cdot 29^{90} \cdot 67^{42} \simeq 1.7 \cdot 10^{246}$.

Chapitre 6: Une application des relations de normes généralisées à la conjecture de Leopoldt

Soit L/K une extension galoisienne de corps de nombres, de groupe de Galois G. Dans l'article [23], les auteurs prouvent que si G admet une relation de norme par rapport à un ensemble de sous-groupes $\mathcal{H} = \{H_1, \cdots, H_\ell\}$, alors, pour un nompre premier p fixé, la conjecture de Leopoldt en p est vraie pour L si et seulement si elle est vraie pour tous les L^{H_i}.

Dans ce chapitre, après avoir rappelé quelques formulations de la conjecture de Leopoldt, nous montrons que ce résultat peut être généralisé de la manière suivante:

Proposition A (proposition 6.9)**.** *Soit L/K une extension galoisienne de corps de nombres, et soit G son groupe de Galois. Supposons que G admet une relation de norme généralisée par rapport à $\Gamma < G$, et à un ensemble de sous-groupes $\mathcal{H}$. Soit $\mathcal{I} \subseteq \mathcal{H}$ tel que $1 \notin \mathcal{I}$ et pour tout $H \in \mathcal{H}$, il existe $I \in \mathcal{I}$ et $g \in G$ tel que $gIg^{-1} \leq H$. Soit p un nombre premier. Si la conjecture de Leopoldt en p est vraie pour tous les L^I avec $I \in \mathcal{I}$, alors elle est vraie pour L^Γ.*

Chapitre 7: Calcul des groupes de Selmer

Ce chapitre est basé sur l'article [21]. Etant donnés un corps de nombre de groupe de Galois absolu $\mathcal{G}$, un module galoisien fini M, et un système de Selmer $\mathcal{L}$, l'objectif est de donner une méthode pour calculer $\mathrm{Sel}_\mathcal{L}$, le groupe de Selmer de M lié à $\mathcal{L}$.

Dans la première section, nous décrivons une méthode pour obtenir une résolution de M, où les morphismes sont donnés par des opérateurs de Hecke. Ensuite, dans la deuxième section, nous définissons un autre groupe $H^1_S(\mathcal{G}, M)$, et nous prouvons, avec les propriétés des opérateurs de Hecke, que $H^1_S(\mathcal{G}, M)$ est un groupe de Selmer qui contient $\mathrm{Sel}_\mathcal{L}$.

Le résultat principal de la troisième section est le suivant:

Theorem G. *Soit $\mathcal{G}$ le groupe de Galois absolu d'un corps de nombres K, et soit M un $\mathcal{G}$-module fini. Il existe un algorithme qui prend en entrée*

- *le module M,*
- *le groupe fini G qui est l'image de l'action $\mathcal{G} \to \mathrm{Aut}(M)$,*
- *un système de Selmer $\mathcal{L}$,*

et qui donne en sortie le groupe de Selmer $\mathrm{Sel}_{\mathcal{L}}$ lié à $\mathcal{L}$ pour M. De plus, chaque étape de cet algorithme a une complexité en temps polynomiale, à part le calcul des sous-corps de $\overline{K}$ fixés par des sous-groupes de $\mathcal{G}$, et les calculs de groupes de S-unités et de groupes de classes de certaines extensions de corps de K.

Contents

1 Introduction **18**
1.1 Number fields and class groups 18
1.1.1 Ideal class group 18
1.1.2 Analytic class number formula 18
1.1.3 Buchmann's algorithm 20
1.2 Galois theory and Galois representations 20
1.2.1 Fundamental theorem 20
1.2.2 Galois representations 21
1.2.3 Brauer relations 22
1.3 Group cohomology and Selmer groups 23
1.3.1 Group cohomology 23
1.3.2 Selmer groups 24
1.4 Organisation and contributions of the thesis 24

2 Hecke algebras of finite groups **30**
2.1 Hecke algebras 30
2.2 Compositums 35

3 Mackey functors **42**
3.1 Definitions and properties 42
3.2 Normed Mackey functors 47

4 Norm relations **54**
4.1 Classical norm relation 54
4.2 Generalised norm relations 57
4.3 Optimal coefficient 64
4.4 Norm relation over finite fields 67
4.5 Looking for generalised norm relations 70
4.6 Comparing classical and generalised norm relations 73

5 Computing class groups **80**
5.1 Algorithms using S-units 80
5.2 Algorithms for direct computation 86
5.3 Examples 89

6 An application of generalised norm relations to Leopoldt's conjecture **91**

7 Computing Selmer groups **95**
7.1 Finding a resolution with Hecke operators 96
7.2 A remarkable Selmer group 99
7.3 Algorithm and complexity 105

Notations and conventions

When R is a ring and M, N are left R-modules, we will denote by $\mathrm{Hom}_R(M, N)$ the group of R-module homomorphisms from M to N.

If G is a group, $H < G$ a subgroup and M a G-module, we will denote by M^H the set of fixed points of M under the action of H.

If K is a number field, we will call $\tilde{K}$ the Galois closure of K, that is to say the Galois closure of the field extension $\mathbb{Q} : K$.

If K is a field, we will denote by $\overline{K}$ the algebraic closure of K.

For the structure descriptions of groups, we will use the following notations (where n is a positive integer, q a power of a prime number and G, H are two groups):

- C_n: cyclic group of order n,
- A_n: alternating group of degree n,
- S_n: symetric group of degree n,
- D_n: dihedral group of size n,
- Q_n: quaternion group of size n,
- QD_n: quasidihedral group of size n,
- $\mathrm{GL}(n, q)$: general linear group of $\mathbb{F}_q^n$,
- $\mathrm{PSL}(n, q)$: projective special linear group of $\mathbb{F}_q^n$,
- $G \times H$: direct product of G and H,
- $G \rtimes H$: semidirect product of G and H.

1 Introduction

In this thesis, we study the properties of Hecke operators, and how we can use them to obtain relations between some Galois modules. We then use these relations to derive efficient algorithms to compute arithmetic objects such as class groups of number fields, or Selmer groups of finite Galois modules.

In the introduction, we will first recall some background knowledge about class groups of number fields (section 1.1), about Galois theory (section 1.2) and Galois cohomology (section 1.3). Then, in section 1.4, we will present the plan of the thesis and our contributions in each chapter.

1.1 Number fields and class groups

1.1.1 Ideal class group

A *number field* is a field extension of the rational field $\mathbb{Q}$, of finite degree. If K is a number field, we denote by $\mathbb{Z}_K$ the *ring of integers* of K, that is to say the ring of all elements of K that are roots of a monic polynomial with integer coefficients.

A *fractional ideal* I of the ring of integer $\mathbb{Z}_K$ is a $\mathbb{Z}_K$-submodule of K such that there exists a non zero element $\alpha \in \mathbb{Z}_K$ such that $\alpha I \subset \mathbb{Z}_K$.

We say that two fractional ideals J, J' of $\mathbb{Z}_K$ are *equivalent*, and we write $J \sim J'$ if there exists a non zero x in K such that $J' = xJ$. This is an equivalence relation. We denote by $\mathrm{Cl}(K)$ the group of equivalence classes for this relation. This is the *ideal class group* of K. An important result is that the ideal class group of a number field K is always finite. (This is the class number theorem, see for example [25] for a proof). Its order is called the *class number* of K.

The study of class groups of number fields is central in number theory. It measures the "defect of $\mathbb{Z}_K$ from being a principal ideal domain", in the sense that $\mathbb{Z}_K$ is a principal ideal domain if and only if $\mathrm{Cl}(K)$ is the trivial group, and thus it measures the degree of failure of unique factorisation in $\mathbb{Z}_K$. It plays an important role in the study of some Diophantine problems (see [25]).

1.1.2 Analytic class number formula

A way of computing the class number of a number field is through the *analytic class number formula* (see for example [37]).

First, let us define all the terms involved in the formula.

Let K be a number field. Let $u_1, \cdots, u_r$ be a basis of the unit group of $\mathbb{Z}_K$ (i.e. the group of invertible elements in $\mathbb{Z}_K$) modulo the torsion. Let $\sigma_1, \cdots, \sigma_{r_1}$ be the real embeddings of K, and $\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}$ the complex embeddings of K, up to complex conjugacy. Dirichlet's units theorem gives us $r = r_1 + r_2 + 1$.

Consider the matrix $(\epsilon_j \log|\sigma_j(u_i)|)_{\substack{1\leq i\leq r\\ 1\leq j\leq r}}$, where ϵ_j is 1 if σ_j is a real embedding and 2 otherwise. Then the *regulator* $\mathrm{Reg}(K)$ of K is the absolute value of the determinant of this matrix.

Let $b_1, \cdots, b_n$ be an integral basis of $\mathbb{Z}_K$. We have $n = r_1 + r_2$. Let $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ for all $1 \leq i \leq r_2$. Then the *discriminant* Δ_K of K is the square of the determinant of the matrix $(\sigma_j(b_i))_{1\leq i,j\leq n}$.

Recall that the *Riemann ζ-function* is defined for any complex number s with $\mathrm{Re}(s) > 1$ by the formula

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

We define the *Dedekind ζ-function* of K by the formula

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a}\neq 0\\ \text{ideal of } \mathbb{z}_K}} [\mathbb{Z}_K : \mathfrak{a}]^{-s} = \prod_{\substack{\mathfrak{p}\subset\mathbb{Z}_K\\ \text{non zero prime ideal}}} (1 - [\mathbb{Z}_K : \mathfrak{p}]^{-s})^{-1}.$$

Note that when $K = \mathbb{Q}$, we have $\zeta_K = \zeta$.

Then, for every number field K, the sum $\zeta_K(s)$ converges absolutely for every complex number s with $\mathrm{Re}(s) > 1$, and ζ_K extends to a meromorphic function over $\mathbb{C}$, with a simple pole at $s = 1$.

The analytic class number formula gives the residue at $s = 1$:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot h_K}{w_K \cdot \sqrt{|\Delta_K|}}$$

where $r_1, 2r_2$ are the number of real and complex embeddings of K, Reg_K is the regulator, h_K the class number, w_K the number of roots of unity contained in K, and Δ_K is the discriminant.

1.1.3 Buchmann's algorithm

In [13], Buchmann gives an algorithm that on input a number field K and its ring of integers $\mathbb{Z}_K$, outputs the structure of the class group $\mathrm{Cl}(K)$ and a basis of the unit group $\mathbb{Z}_K^\times$.

The proof of the correctness of the algorithm assumes the generalised Riemann hypothesis (GRH). See [17] for more details about this conjecture, one of the most important in modern number theory.

The heuristic time complexity of Buchmann's algorithm grows quickly with the degree n of the number field K: if we denote by Δ_K the discriminant of K, the time complexity of this algorithm for fixed n is in $\mathcal{O}(e^{a\sqrt{\ln|\Delta_K|\ln\ln|\Delta_K|}})$ where a is a constant, and the implicit constant of the $\mathcal{O}$ depends on n exponentially; note in addition that the absolute value of the discriminant of K is bounded from below by a function that is exponential in n.

1.2 Galois theory and Galois representations

1.2.1 Fundamental theorem

Let K/F be a finite algebraic field extension, and let $\mathrm{Aut}_F(K)$ denote the group of field automorphisms of K fixing F, that is to say, for all $\sigma \in \mathrm{Aut}_F(K)$ and for all $x \in F$, we have $\sigma(x) = x$.

If H is a subgroup of $\mathrm{Aut}_F(K)$, then we denote by K^H the *fixed field* of H, defined by $K^H = \{x \in K | \sigma(x) = x \text{ for all } \sigma \in H\}$. It is a subfield of K containing F (see for example [32] for all the proofs in this section).

If $K^{\mathrm{Aut}_F(K)} = F$, then we say that K/F is a *Galois extension*, and the group $G = \mathrm{Aut}_F(K)$ is its *Galois group*. Moreover, we have $|G| = [K : F]$. An extension K/F is Galois if and only if it is normal and separable. This is also equivalent to saying that K is the splitting field of a separable polynomial $f \in F[X]$.

Let K/F be a Galois extension, with Galois group $G = \mathrm{Aut}_F(K)$. Then, the *fundamental theorem of Galois theory* states that there is a bijection between the set $\mathcal{L}$ of subfields L of K containing F, and the set $\mathcal{H}$ of subgroups H of G. The bijection and its inverse are given by the maps

$$\Phi \colon \mathcal{L} \to \mathcal{H}, L \mapsto \mathrm{Aut}_L(K)$$
$$\Phi^{-1} \colon \mathcal{H} \to \mathcal{L}, H \mapsto L^H.$$

What's more, if L is an intermediate field $F \subset L \subset K$, and H such that $L = K^H$, then K is Galois over L, with Galois group H. And the field L is Galois over F if and only if H is normal in G. In that case, the Galois group of L/F is isomorphic to G/H.

The maps Φ and Φ^{-1} are known as the *Galois correspondence*. Note that they are inclusion reversing, in the sense that if we have two subfields L_1, L_2 such that $F \subset L_1 \subset L_2 \subset K$, and H_1, H_2 the subgroups of G such that $L_1 = K^{H_1}$ and $L_2 = K^{H_2}$, then $H_2 < H_1$, and conversely, if $H_1 < H_2$ are two subgroups of G, then we have $K^{H_2} \subset K^{H_1}$.

Note that, even though we will mostly use the Galois group of finite field extensions in this thesis, we will also need to use absolute Galois groups in chapter 7. The absolute Galois group of a field K is the automorphism group of K^{sep}/K, where K^{sep} is a separable closure of K. When K is a perfect field, K^{sep} is equal to an algebraic closure of K.

1.2.2 Galois representations

In this section, we will give the definitions of linear representations of a finite group G, of left modules, and of the group algebra $R[G]$, with R a ring. Then we will see that the linear representations of G over F are the same as $F[G]$-modules. (See [45] or [41]).

Let V be a vector space over a field F, and let $\mathrm{GL}(V)$ be the group of automorphisms of V. Let G be a finite group. A *linear representation* of G in V is an homomorphism $\rho\colon G \to \mathrm{GL}(V)$. Note that a linear representation ρ of G in V gives a left group action of G on V defined by $g \cdot x = \rho(g)(x)$, for all $g \in G, x \in V$. So V is a left G-module.

Let ρ be a linear representation of a finite group G in a vector space V. The *character* of the representation ρ is the function $\chi_\rho\colon G \to \mathbb{C}, s \mapsto \mathrm{Tr}(\rho(s))$, where for every element $a \in \mathrm{GL}(V)$, $\mathrm{Tr}(a)$ denotes the trace of a.

Let R be a ring, a *left R-module* M is an abelian group with an operation $\cdot : R \times M \to M$ such that for $r, s \in R$ and $m, n \in M$, we have

- $1 \cdot m = m$
- $r \cdot (m + n) = r \cdot m + r \cdot n$
- $(r + s) \cdot m = r \cdot m + s \cdot m$
- $(rs) \cdot m = r \cdot (s \cdot m)$.

What's more, if M, N are two R-modules, then a map $f\colon M \to N$ is called a *morphism of R-modules* if for all $x, y \in M$ and for all $r \in R$, we have

- $f(x+y) = f(x) + f(y)$,
- $f(r \cdot x) = r \cdot f(x)$.

If R is a commutative ring, we can define the *group algebra of G over R*, of formal sums of elements of G, with coefficients in R:

$$R[G] = \{\sum_{g \in G} a_g g | a_g \in R\}.$$

It is a R-algebra, with the multiplication that extends the one in G.

Let V be a R-module and let $\rho\colon G \to \mathrm{GL}(V)$ be a linear representation of G in V. If we extend the associated group action $G \times V \to V$ by linearity, we see that V is endowed with a structure of left $R[G]$-module. And conversely, a structure of $R[G]$-module on a set V defines a linear representation of G in V.

When the group G is the Galois group of a field extension, then any $R[G]$-module is called *Galois module*, and the associated representation is a *Galois representation*. For example, if $K/\mathbb{Q}$ is a finite Galois extension of Galois group G, then $K^\times$ or $\mathbb{Z}_K^\times$ are Galois modules with $R = \mathbb{Z}$.

1.2.3 Brauer relations

Suppose K/F is a Galois extension of number fields, of Galois group G. By studying relations between the subgroups of G arising from character theory, we can find corresponding relations between the arithmetic invariants of the intermediate fields.

Let H be a subgroup of G, and let W be a $\mathbb{C}[H]$-module. The induction of W is the $\mathbb{C}[G]$-module $\mathrm{Ind}_{G/H}(W) = \mathbb{C}[G] \otimes_{C[H]} W$.

For a subgroup $H < G$, denote by $\mathrm{Ind}_{G/H}(1_H)$ the permutation character of G induced from the trivial representation of H. A *Brauer relation* is a relation of the form

$$\sum_{H<G} a_H \,\mathrm{Ind}_{G/H}(1_H) = 0$$

with $a_H \in \mathbb{Z}$. In [10], Brauer proved that when such a relation exists, there is a corresponding relation between certain arithmetic invariants of the fields K^H.

In [7], Biasse, Fieker, Hofmann and Page studied another type of relation called *norm relation*. In their paper, they derive from such a relation an inductive algorithm to compute the class group or the groups of S-units of K by reducing the problem to a similar problem on the subfields K^H.

1.3 Group cohomology and Selmer groups

1.3.1 Group cohomology

Let us recall the basic definition of group cohomology, as in [44] for example.

Let G be a finite group and M a G-module. For any integer $i \leq 0$, let $C^i(G, M)$ denote the abelian group of functions $f\colon G^i \to M$. By convention, we define $C^{-1}(G, M) = \{0\}$.

The *coboundary maps* $d^i\colon C^i(G, M) \to C^{i+1}(G, M)$ are defined by

$$\begin{aligned}(d^i f)(g_1, \cdots, g_{i+1}) =& g_1 \cdot f(g_2, \cdots, g_{i+1}) + \sum_{j=1}^{i} (-1)^i f(g_1, \cdots, g_j g_{j+1}, \cdots, g_{i+1}) \\ &+ (-1)^{i+1} f(g_1, \cdots, g_i)\end{aligned}$$

By convention, we let $d^{-1}\colon C^{-1}(G, M) \to C^0(G, M)$ be the zero map.

Then we can define the space of *i-cocycles* $Z^i(G, M) = \ker(d^i)$ and the space of *i-coboundaries* $B^i(G, M) = \mathrm{Im}(d^{i-1})$. The *$i$-th cohomology group of G with coefficients in M* is

$$H^i(G, M) = \frac{Z^i(G, M)}{B^i(G, M)}.$$

The main property of cohomology groups is the following:

Let A, B, C be G-modules such that there is an exact sequence

$$0 \to A \to B \to C \to 0.$$

Then there is an infinite exact sequence of cohomology groups

$$\begin{aligned}0 \to & H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \\ & H^2(G, A) \to H^2(G, B) \to \cdots\end{aligned}$$

The study of the group cohomology of Galois modules is called *Galois cohomology*.

1.3.2 Selmer groups

Cohomology groups are not finitely generated in general, which makes them often hard to use in practice. This is why it is interesting to work with *Selmer groups*. Those are finite subgroups of the cohomology groups, defined in such a way that they still contain some important local information. See chapter 7 for the precise definition.

Selmer groups are powerful tools in modern number theory. Introduced in the study of descent in elliptic curves ([46, Chapter X, §4]), they have been crucial for progress toward the BSD conjecture (see for example [31]) and arithmetic statistics on ranks of elliptic curves (see [6]), conjecturally predict the order of vanishing of L-functions (see [8]), control deformations of Galois representations (see [35, §1.10]) and therefore play an important role in modularity theorems (see [50]) and have many other applications, for instance in effective class field theory (see [15, §5.2.2]). It is therefore important to design efficient algorithms to compute Selmer groups.

1.4 Organisation and contributions of the thesis

Chapter 2: Hecke algebra of finite groups

This chapter corresponds to [22, section 1]. We define Hecke operators and Hecke algebras, and describe some of their properties. Then we define the notion of compositum of two number fields.

Our contribution is the following. If $\tilde{K}$ is a number field Galois over $\mathbb{Q}$, of Galois group G, and H, J are two subgroups of G, let $K = \tilde{K}^H$ and $L = \tilde{K}^J$. Then we show that there is a bijection between the set of compositums of K and L and the set of double cosets $J\backslash G/H$ (see proposition 2.17).

Let K and L be number fields. A *compositum* of K and L is a triple (C, ι_K, ι_L) where $C/\mathbb{Q}$ is a number field, $\iota_K \colon K \to C$ and $\iota_L \colon L \to C$ are fields homeomorphisms, and where C is generated by $\iota_K(K)$ and $\iota_L(L)$ as a ring.

Up to isomorphism, there is only a finite number of compositums of K and L, we denote by $\mathrm{Compos}(K, L)$ a set of representatives.

Then, there is a natural "action" of the set of compositum on the set of fixed points of various $R[G]$-modules, which we describe from proposition 2.19 to proposition 2.23.

Finally, we describe the "action" of a compositum of K and L from $L^\times$ to $K^\times$:

Theorem B. *[Theorem 2.24] Let x be an element of $K^\times$ and let (C, ι_K, ι_L) be a compositum of K and L. Then $C \cdot x = N_{C/L}(\iota_K(x))$.*

This theorem will be useful especially for algorithmic applications, in chapter 5.

Though the bijection between double cosets and compositums was probably a folklore result, we did not know a reference for it. But it seems to us that theorem B is new, as well as its algorithmic applications.

Chapter 3: Mackey functors

In the first section of this chapter, we give the definition of (cohomological) Mackey functors, as well as some properties, that can be found in [51] and [9], linking the formalism of Mackey functors to Hecke operators.

Then, in the second section, based on the article [1], still in preparation, we introduce the notion of normed Mackey functors (see definition 3.14), and give some examples. The main result is theorem 3.16:

Theorem C. *Let R be a normed domain with field of fractions k, and let M be a normed R-Mackey functor on a finite group G. Let $U_1, \cdots U_n$ and $U'_1, \cdots U'_m$ be subgroups of G for which there exists an epimorphism of $k[G]$-modules*

$$\Phi \colon \bigoplus_i k[G/U_i] \to \bigoplus_j k[G/U'_j].$$

Then there is a R-linear map

$$\phi \colon \bigoplus_{i,j} M(U_i)^{U_i \backslash G / U'_j} \to \bigoplus_j M(U'_j)$$

such that the base change $\phi \otimes k$ is surjective and such that ϕ has operator norm bounded from above by

$$\max\{1, \max\{|[U'_i : gU_j g^{-1}]| \text{ for } g \in G, i = 1, \cdots m, \text{ and } j = 1, \cdots, n\}.$$

This theorem is interesting because it can be used to obtain a bound on the operator norm of linear maps in a large variety of different contexts.

Chapter 4: Norm relations

In [7], the authors study the properties of norm relations, and use them to produce some algorithms to compute arithmetic invariants of some number fields by induction, and in particular the structure of the class group. The goal of this chapter is to study a generalisation of the definition of norm relations.

In section 4.1, we recall the definition of norm relation, as well as some necessary and sufficient criteria for their existence, as proven in [7].

Our contribution is in the other sections, which are largely based on [22].

In section 4.2, we define generalised norm relations:

Definition D. *Let H be a subgroup of a finite group G, $\mathcal{J}$ a set a subgroups of G and R a commutative ring. A* generalised norm relation over R with respect to H and $\mathcal{J}$ *is an equality in $R[G]$ of the form*

$$N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$$

where $a_i, b_i \in R[G]$, $J_i \in \mathcal{J}$, and $J_i \neq 1$, and where $N_{J_i} = \sum_{j \in J_i} j$, and $N_H = \sum_{h \in H} h$ are the norm elements of the J_i and H.

And we give some necessary and sufficient criteria for their existence. In particular, the following proposition (4.14) establishes a strong link between generalised norm relations and Hecke operators:

Proposition E. *Let H be a subgroup of G, and $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ a set of non trivial subgroups of G. Then, G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}$ if and only if there exists a surjective morphism of $\mathbb{Q}[G]$-modules*

$$\phi\colon \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$$

where for all i, $n_i \in \mathbb{Z}_{\geq 0}$.

By Galois theory, we get a corresponding notion of generalised norm relations between number fields (see definition 4.15), and in theorem 4.22 we also give a criterion based on the action of compositums:

Theorem F. *If $L_1, \cdots, L_\ell$ are number fields, defined by the polynomials $f_1, \cdots, f_\ell$, and if we denote by R_i the set of roots of f_i in $\mathbb{C}$, then a number field $K = \mathbb{Q}(\alpha)$ admits a* generalised norm relation with respect to $L_1, \cdots, L_\ell$, *if and only if there is a relation of the form*

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in Compo(K, L_i)} \sum_{\beta \in R_i} a_{i,C,\beta} C \cdot \beta$$

where the coefficients $a_{i,C,\beta}$ are in $\mathbb{Q}$.

In section 4.3, we define the optimal coefficient of a generalised norm relation (see definition 4.24), show that it is well defined and give a bound (see theorem 4.28) that will mainly be useful in the next chapter, to study the time complexity of some algorithms. The main result in this section is the following:

Theorem G. *Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. If there is a norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}$, then there is a positive integer c such that there exists an injective morphism of $\mathbb{Z}[G]$-modules $\psi \colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$ with $n_i \in \mathbb{Z}_{>0}$ for all i, and a morphism of $\mathbb{Z}[G]$-modules $\phi \colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ such that $\phi \circ \psi = c \cdot \mathrm{id}$.*

What's more, the smallest such integer c divides $|G|^2$.

Even though throughout this chapter and the next one, we focus mainly on generalised norm relations over $\mathbb{Q}$ or over $\mathbb{Z}$, in section 4.4, we briefly discuss generalised norm relations over finite fields, and give some criteria for their existence (proposition 4.31).

Next, in section 4.5, we give some algorithms to look for generalised norm relations.

Finally, in section 4.6, we compare our generalisation of norm relations to the classical definition of norm relations, to show that our generalisation is indeed relevant.

Chapter 5: Computing class groups

In this chapter, we describe some algorithms to compute the class groups of some number fields by induction, using the properties of generalised norm relations. The methods are similar to those used in [7].

In the first section, we present an algorithm (5.7) to compute the group of S-units of a number field, which allows for an indirect computation of the class group, whereas the algorithms presented in the second section compute the class group more directly. The main result in this chapter is the following:

Theorem H. *Assuming the generalised Riemann hypothesis, there exists a polynomial time algorithm that, on input*

- *a number field K,*
- *a set S of prime numbers,*
- *subfields K_i of the Galois closure $\tilde{K}$,*
- *for each i, a basis of the S-unit group of K_i,*

if K admits a generalised norm relation with respect to the K_i, outputs a basis of the S-unit group of K.

See algorithm 5.9, and see theorem 5.10 for the proof of correctness and the proof of complexity assuming GRH.

Then in section 5.3, we use these algorithms, (and in particular algorithm 5.12, not provably polynomial time, but often faster in practice), implemented in Pari/GP ([40]), to compute the class groups of some number fields with very large discriminant, that we were unable to compute with the standard functions in Pari/GP or with the methods in [7]. In particular, in example 5.18, we manage to compute the class group of a number field of degree 105 and of discriminant $2^{126} \cdot 29^{90} \cdot 67^{42} \simeq 1.7 \cdot 10^{246}$.

Chapter 6: An application of generalised norm relations to Leopoldt's conjecture

Let L/K be a Galois extension of number fields, of Galois group G. In [23], the authors prove that if G admits a norm relation with respect to a set of subgroups $\mathcal{H} = \{H_1, \cdots, H_\ell\}$, then for a fixed prime number p, Leopoldt's conjecture at p holds for L if and only if it holds for all of the L^{H_i}.

In this chapter, after recalling some formulations of Leopoldt's conjecture, we show that this result can be generalised in the following way:

Proposition I (proposition 6.9)**.** *Let L/K be a Galois extension of number fields, and let G be its Galois group. Suppose that G has a generalised norm relation with respect to a subgroup $\Gamma < G$, and a set of subgroups $\mathcal{H}$. Let $\mathcal{I} \subseteq \mathcal{H}$ be such that the trivial group 1 is not in $1\mathcal{I}$ and for every $H \in \mathcal{H}$, there exists $I \in \mathcal{I}$ and $g \in G$ such that $gIg^{-1} \leq H$. Let p be a prime number. If Leopoldt's conjecture at p for L^I holds for every $I \in \mathcal{I}$, then Leopoldt's conjecture at p for L^Γ holds.*

Chapter 7: Computing Selmer groups

This chapter is based on the preprint [21]. Given a number field with absolute Galois group $\mathcal{G}$, a finite Galois module M, and a Selmer system $\mathcal{L}$, the goal is to give a method to compute $\mathrm{Sel}_\mathcal{L}$, the Selmer group of M attached to $\mathcal{L}$.

In the first section, we describe a method to obtain a resolution of M where the morphisms are given by Hecke operators. Then in the second section, we define another group $H^1_S(\mathcal{G}, M)$ and we prove, using the properties of Hecke operators, that $H^1_S(\mathcal{G}, M)$ is a Selmer group containing $\mathrm{Sel}_\mathcal{L}$.

The main result of the third section is the following:

Theorem J. *Let $\mathcal{G}$ be the absolute Galois group of a number field K, and M be a finite left $\mathcal{G}$-module. There exists an algorithm that on input*

- *the module M,*
- *the finite group G that is the image of the action $\mathcal{G} \to \mathrm{Aut}(M)$,*
- *a Selmer system $\mathcal{L}$,*

outputs the Selmer group $\mathrm{Sel}_\mathcal{L}$ attached to $\mathcal{L}$ for M. Moreover, every step of this algorithm is polynomial, except for the computation of subfields of $\overline{K}$ fixed by subgroups of $\mathcal{G}$, and the computation of the group of S-units and the class group of some field extensions of K.

We will describe this algorithm (see algorithm 7.19), and discuss the complexity in proposition 7.21.

2 Hecke algebras of finite groups

One common theme between every part of this thesis will be the use of Hecke operators and Hecke algebras. In section 2.1, we will give a definition of Hecke operators and Hecke algebras (see definitions 2.5 and 2.6) based on group theory and module theory. Then in section 2.2, we will define the notion of compositums of number fields (definition 2.10), and use it to give a more field-theory-oriented interpretation of Hecke operators. In all of this chapter, G will be a finite group, and H, J will be subgroups of G.

2.1 Hecke algebras

Let R be a commutative ring. The module $R[G/H]$ is the free R-module on the finite set G/H, with a G-action linearly extending the one of G/H. The main objects in this section will be $R[G]$-modules of the form $\bigoplus_i R[G/H_i]$, where the H_i are subgroups of G. We call $R[G]$-modules of this form *permutation modules*.

First, let us introduce some useful isomorphisms of R-modules. These isomorphisms (lemma 2.1 and lemma 2.2) are well known and can be found for example in [51].

Lemma 2.1. *Let V be a G-module. The map*

$$\Phi_1 \colon \mathrm{Hom}_{R[G]}(R[G/H], V) \to V^H, \phi \mapsto \phi(1 \cdot H)$$

where V^H is the set of points of V fixed under the action of H, is an isomorphism of R-modules. And its inverse is

$$\Phi_1^{-1} \colon V^H \to \mathrm{Hom}_{R[G]}(R[G/H], V), x \mapsto \begin{cases} \text{The unique morphism } \phi \text{ of} \\ R[G]\text{-modules in } V \text{ such that} \\ \phi(1 \cdot H) = x \end{cases}.$$

Proof. Consider the map $\Phi_1 : \mathrm{Hom}_{R[G]}(R[G/H], V) \to V^H, \phi \mapsto \phi(1 \cdot H)$, First, let us show that the image of Φ_1 is included in V^H. Let ϕ be an element of $\mathrm{Hom}_{R[G]}(R[G/H], V)$, and let $h \in H$. Then $h \cdot \phi(1 \cdot H) = \phi(h \cdot 1 \cdot H) = \phi(1 \cdot H)$. Where the first equality is due to ϕ being a morphism of $R[G]$-modules. This shows that $\phi(1 \cdot H) = \Phi_1(\phi)$ is indeed in V^H.

For every $x \in V^H$, there exists a $\phi \in \mathrm{Hom}_{R[G]}(R[G/H], V)$ such that $\phi(1 \cdot H) = x$. It is given by the formula $\phi(gH) = g \cdot x$ for all $gH \in G/H$, and it is independent from the choice of the representative g since $x \in V^H$.

What's more, since $R[G/H]$ is spanned by $1 \cdot H$ as a $R[G]$-module, we know that any morphism of $R[G]$-modules $\phi \in \mathrm{Hom}_{R[G]}(R[G/H], V)$ is entirely determined by the choice of $\phi(1 \cdot H)$. So ϕ is unique.

So Φ_1^{-1} is well defined and is the inverse of Φ_1, hence the conclusion.

□

Lemma 2.2. *There is an isomorphism of R-modules*

$$\Phi_2 \colon R[H\backslash G/J] \to R[G/J]^H, \sum_{HgJ \in H\backslash G/J} \alpha_{HgJ} HgJ \mapsto \sum_{gJ \in G/J} \alpha_{HgJ} gJ.$$

Its inverse is

$$\Phi_2^{-1} \colon R[G/J]^H \to R[H\backslash G/J], \sum_{gJ \in G/J} \alpha_{gJ} gJ \mapsto \sum_{HgJ \in H\backslash G/J} \alpha_{gJ} HgJ.$$

Proof. Let $x = \sum_{g \in G/J} \alpha_g gJ$ be an element of $R[G/J]$. Then x is fixed under the action of H if and only if for all $h \in H$, $h \cdot x = \sum_{g \in G/J} \alpha_g (hg)J = \sum_{g' \in G/J} \alpha_{h^{-1}g'} g'J = x$. Hence for all g in G/H, $\alpha_{h^{-1}g} = \alpha_g$.

This proves that the image of Φ_2 is in $R[G/J]^H$, and also that Φ_2^{-1} is well defined.

Since Φ_2^{-1} is trivially the inverse of Φ_2, this proves the lemma.

□

Combining the two previous lemma, we can get another useful isomorphism of R-modules.

Proposition 2.3. *There is an isomorphism of R-modules*

$$\Phi \colon R[H\backslash G/J] \to \mathrm{Hom}_{R[G]}(R[G/H], R[G/J])$$

$$\sum_{HgJ \in H\backslash G/J} \alpha_{HgJ} HgJ \mapsto \left\{ \begin{array}{l} \phi \text{ such that} \\ \phi(1 \cdot H) = \sum_{g \in G/J} \alpha_{HgJ} gJ \end{array} \right. .$$

Its inverse is

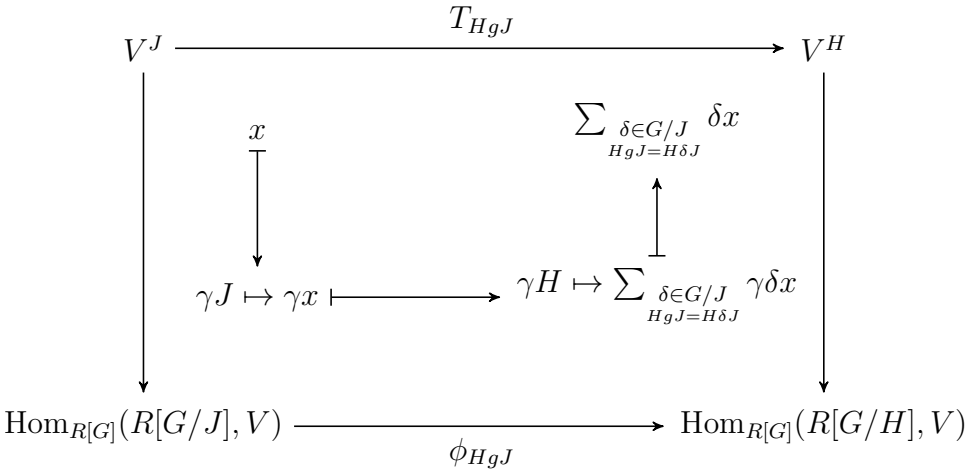
$$\Phi^{-1} \colon \mathrm{Hom}_{R[G]}(R[G/H], R[G/J]) \mapsto R[H\backslash G/J]$$

$$\phi \mapsto \left\{ \begin{array}{l} \sum_{HgJ \in H\backslash G/J} \alpha_{gJ} H\delta J \\ \text{where } \phi(1 \cdot H) = \sum_{g \in G/J} \alpha_{gJ} gJ \end{array} \right. .$$

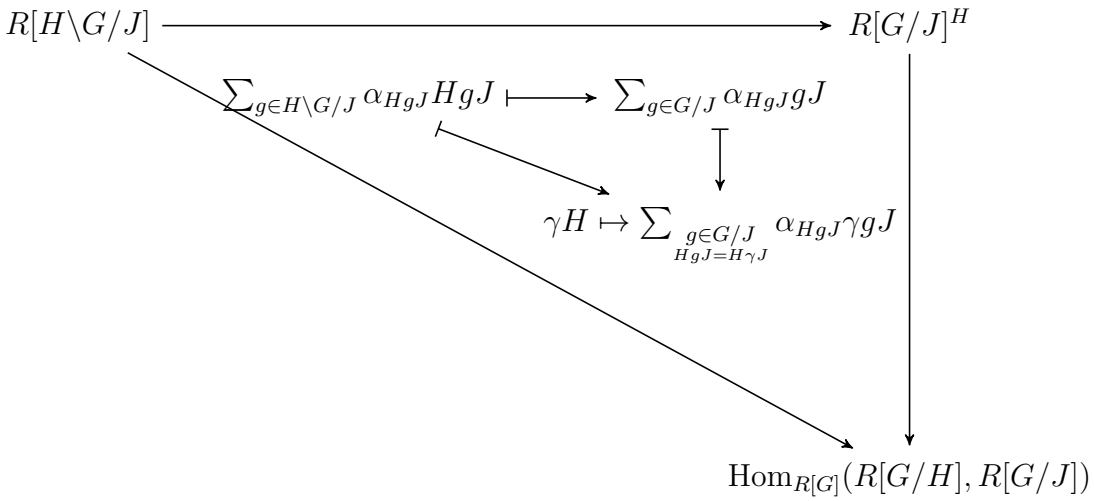
Proof. We can obtain the isomorphism Φ simply by composing Φ_1 from lemma 2.1 and Φ_2 from lemma 2.2.

□

Fact 2.4. By considering both the isomorphism Φ in proposition 2.3 and the isomorphism Φ_1 in lemma 2.1, we deduce that given any $R[G]$-module V, for every element HgJ of $R[H\backslash G/J]$ we get a morphism T_{HgJ} of R-modules from V^J to V^H given by the following diagram:



where the expression of ϕ_{HgJ} is obtained via the following diagram:



This "action" of the double cosets on the set of fixed points of any $R[G]$-module will be one of the corner stones of this thesis. With the two following definitions, let us name the operators involved.

Definition 2.5. If R is a commutative ring and V an $R[G]$-module, then the morphisms of R-modules $V^J \to V^H$ associated with double cosets of the form HgJ for $g \in G$, by the morphism described in fact 2.4 are called *Hecke operators*.

Definition 2.6. We can define a multiplication in $R[H\backslash G/H]$ as inherited from the $\circ$ law in $\mathrm{End}_{R[G]}(R[G/H])$, by the isomorphism of proposition 2.3. Then $R[H\backslash G/H]$ is an algebra over R, isomorphic to $\mathrm{End}_{R[G]}(R[G/H])$. We call algebras of this form *Hecke algebras*.

Example 2.7. Set $R = \mathbb{Q}$, $G = S_3$ and $H = \{\mathrm{id}, (1,2)\}$ as a subgroup of G.

- There are two equivalence classes in $H\backslash G/H$, which are $\{\mathrm{id}, (1,2)\}$ and $\{(1,2,3), (1,3), (2,3), (2,3,1)\}$. Indeed, $(1,2,3)(1,2) = (1,3)$, $(1,2)(1,2,3) = (2,3)$ and$(1,2)(1,2,3)(1,2) = (2,1,3)$.

  So we have $\mathbb{Q}[H\backslash G/H] = \{a(H\,\mathrm{id}\,H) + b(H(1,3)H); (a,b) \in \mathbb{Q}^2\} = \mathbb{Q} \cdot H\,\mathrm{id}\,H \oplus \mathbb{Q}H(1,3)H$.

- There are three equivalence classes in G/H, which are $\{\mathrm{id}, (1,2)\}$, $\{(1,2,3), (1,3)\}$ and $\{(2,1,3), (2,3)\}$.

  Therefore, an element of $\mathrm{End}_{R[G]}(R[G/H])$ is entirely determined by the images of $1 \cdot \mathrm{id}$, $1 \cdot (1,3)H$ and $1 \cdot (2,3)H$.

- Let $x = a(H\,\mathrm{id}\,H) + b(H(1,3)H)$ be an element of $\mathbb{Q}[H\backslash G/H]$. By the second diagram of fact 2.4, x is associated with the element of $\mathrm{End}_{R[G]}(R[G/H])$ that sends $\gamma H \in G/H$ to

$$\begin{cases} a\gamma H & \text{if} \quad H\gamma H = H\,\mathrm{id}\,H \\ b\gamma(1,3)H + b\gamma(2,3)H & \text{if} \quad H\gamma H = H(1,3)H \end{cases}.$$

- We can define the $+$ law on $\mathbb{Q}[H\backslash G/H]$ by

$$\begin{aligned}(a_1(H\,\mathrm{id}\,H) + b_1(H(1,3)H)) + (a_2(H\,\mathrm{id}\,H) + b_2(H(1,3)H)) \\ = ((a_1+a_2)(H\,\mathrm{id}\,H) + (b_1+b_2)(H(1,3)H)),\end{aligned}$$

  and the $\cdot$ law as inherited from the $\circ$ in $\mathrm{End}_{R[G]}(R[G/H])$ by the isomorphism of proposition 2.3. Then we have:

– $H\,\mathrm{id}\,H \cdot H\,\mathrm{id}\,H = H\,\mathrm{id}\,H$
– $H\,\mathrm{id}\,H \cdot H(1,3)H = H(1,3)H$
– $H(1,3)H \cdot H\,\mathrm{id}\,H = H(1,3)H$
– $H(1,3)H$ is associated with

$$f : \gamma H \mapsto \begin{cases} 0 & \text{if} \quad H\gamma H = H\,\mathrm{id}\,H \\ \gamma(1,3)H + \gamma(2,3)H & \text{if} \quad H\gamma H = H(1,3)H \end{cases},$$

so if $\gamma \in \overline{(1,3)}$, then $\underline{f(\gamma)} = \mathrm{id}\,H + (1,3)H$ so $f^2(\gamma) = f(\gamma)$,
and similarly, if $\gamma \in \overline{(2,3)}$, then $f(\gamma) = (2,3)H + \mathrm{id}\,H$ so $f^2(\gamma) = f(\gamma)$,
Hence finally, $H(1,3)H \cdot H(1,3)H = H(1,3)H$.

And, $\mathbb{Q}[H\backslash G/H]$ is indeed an algebra.

Finaly, let us state two more isomorphisms (proposition 2.8 and proposition 2.9) that will prove useful in the rest of the section.

Let K be a number field. If we choose an embedding $\sigma_0 \colon K \to \mathbb{C}$, then we can define $\tilde{K}$ the Galois closure of K in $\mathbb{C}$. Let us suppose that $\tilde{K}/\mathbb{Q}$ has Galois group G.

Let α be an element of $\mathbb{C}$ such that $\sigma_0(K) = \mathbb{Q}(\alpha)$, and f the minimal polynomial of α over $\mathbb{Q}$, and let Z be the set of complex roots of f. Let $\sigma \in \mathrm{Hom}(K, \mathbb{C}) \simeq \mathrm{Hom}(K, \tilde{K})$ and $g \in G$. The embedding σ sends α to a complex root of f. Then $g \cdot \sigma$ is the element of $\mathrm{Hom}(K, \mathbb{C})$ that sends α to $\sigma(g \cdot \alpha)$.

The Galois group G acts on the set $\mathrm{Hom}(K, \mathbb{C})$ by $g \cdot \sigma = g \circ \sigma$.

Proposition 2.8. *Let H be a subgroup of G. The map*

$$\Phi : G/H \to Z, gH \mapsto g \cdot \alpha$$

is a well-defined isomorphism of G-sets, whose inverse is given by

$$\Phi^{-1} : Z \to G/H, a = g \cdot \alpha \mapsto gH.$$

Proof. Let us prove that the definition of $\Phi(gH)$ does not depend of the choice of g. Let $g_1, g_2 \in G$ such that $g_1 H = g_2 H$. So there exists $h \in H$ such that $g_2 = g_1 h$. Since α is in K, and H fixes K, we have $h \cdot \alpha = \alpha$. So $g_2 \cdot \alpha = g_1 \cdot \alpha$.

What's more, it is easy to check that Φ is G-equivariant and that Φ^{-1} is indeed the inverse of Φ. □

Proposition 2.9. *We write $E = \mathrm{Hom}(K, \mathbb{C})$ for the set of embeddings of K in $\mathbb{C}$, and σ_g for the embedding that maps α to $g \cdot \alpha$ for all $g \in G$.*

There is an isomorphism of G-sets

$$\Phi \colon G/H \to E, gH \mapsto \sigma_g.$$

Its inverse is

$$\Phi^{-1} \colon S \to G/H, \tau_g \alpha \mapsto gH.$$

And $\Phi(gH)$ is independent from the choice of g.

Proof. Let $g_1, g_2 \in G$ such that $g_1 H = g_2 H$, and let $h \in H$ such that $g_2 = g_1 h$. Then, σ_{g_2} maps α to $g_1 \cdot (h \cdot \alpha) = g_1 \cdot \alpha$. So $\sigma_{g_2} = \sigma_{g_1}$. So $\Phi(gH)$ is indeed independent from the choice of g.

What's more, it is easy to check to Φ is G-equivariant and that Φ^{-1} is the inverse of Φ.

□

The propositions 2.8 and 2.9 are very similar. In practice, the formulation of proposition 2.8 with roots of polynomials is more useful for implementation purposes, whereas in theoretical results, we will often prefer the formulation of 2.9 with complex embeddings.

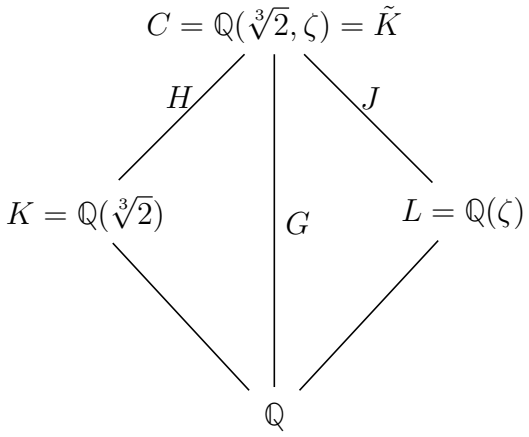
2.2 Compositums

Compositums are well know objects, useful for the study of algebraic fields extensions. (See for example [32, Chapter 5]). In this section, we will be interested in particular in the notion of compositum of two number fields (see definition 2.10).

In this section, $\tilde{K}$ will denote a Galois extension of $\mathbb{Q}$, of finite degree and of Galois group G. Moreover, H and J will be two subgroups of G and we will consider the fields $K = \tilde{K}^H$ and $L = \tilde{K}^J$.

Definition 2.10. Let K and L be number fields. A *compositum* of K and L is a triple (C, ι_K, ι_L) where $C/\mathbb{Q}$ is a number field, $\iota_K \colon K \to C$ and $\iota_L \colon L \to C$ are fields homeomorphisms, and where C is generated by $\iota_K(K)$ and $\iota_L(L)$ as a ring.

Example 2.11. Consider the following diagram, with $\zeta := e^{\frac{2i\pi}{3}}$.



Let $\iota_K \colon K \to C$ be the inclusion, and $\iota_L \colon L \to C$ also the inclusion. It is clear that C is generated by $\iota_K(K)$ and $\iota_L(L)$, so C is a compositum of K and L.

Here, we have $C = \tilde{K}$. We will see that up to isomorphism, every compositum of K and $L \subset \tilde{K}$ is included in $\tilde{K}$.

Note that if we take $\iota_{K,2} \colon K \to C$ the inclusion and $\iota_{L,2} \colon L \to C, \zeta \mapsto \overline{\zeta}$, then $(C, \iota_{K,2}, \iota_{L,2})$ is another compositum of K and L.

Example 2.12. Note that the compositums of two number fields do not necessarily have the same degree.

Let $C = K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\zeta\sqrt[3]{2})$, with $\zeta = e^{\frac{2i\pi}{3}}$. Let ι_K be the identity $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$, and $\iota_L \colon L \to C, \zeta\sqrt[3]{2} \mapsto \sqrt[3]{2}$. Then $(C = \mathbb{Q}(\sqrt[3]{2}), \iota_K, \iota_L)$ is a compositum of K and L, and C is a field of degree 3.

Now let $C' = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, and let $\iota_{L,2} \colon L \to C', \zeta\sqrt[3]{2} \mapsto \zeta\sqrt[3]{2}$. Then $(C', \iota_K, \iota_{L,2})$ is also a compositum of K and L, and C' is a field of degree 6.

Definition 2.13. A *morphism of compositums* between two compositums (C, ι_K, ι_L) and (C', ι'_K, ι'_L) is a field morphism $f \colon C \to C'$, such that $\iota'_K = f \circ \iota_K$ and $\iota'_L = f \circ \iota_L$.

Example 2.14. With the notations of example 2.11, the field isomorphism $f \colon C = \mathbb{Q}(\sqrt[3]{2}, \zeta) \to C, \zeta \mapsto \overline{\zeta}$ induces an isomorphism of compositums from (C, ι_K, ι_L) to $(C, \iota_{K,2}, \iota_{L,2})$.

From now on, we will want to consider compositums up to isomorphisms. This will be possible thanks to the following lemma.

Lemma 2.15. *Up to isomorphism, there is a finite number of compositums of K and L, we denote by* $\mathrm{Compos}(K, L)$ *a set of representatives. There is a bijection between this set and the set of quotients of $K \otimes_{\mathbb{Q}} L$. For every surjective $\mathbb{Q}$-algebra homomorphism $f\colon K \otimes_{\mathbb{Q}} L \to C$, the associated compositum is (C, ι_K, ι_L) and $\iota_K = f \circ (\mathrm{id}_K \otimes 1)$, $\iota_L = f \circ (\mathrm{id}_L \otimes 1)$. Every compositum of K and L is isomorphic to a compositum whose underlying field is contained in $\tilde{K}$.*

Proof. The second statement is a direct application of the universal property of the tensor product of algebras.

Since $K \otimes_{\mathbb{Q}} L$ is of finite dimension over $\mathbb{Q}$, the set $\mathrm{Compos}(K, L)$ is finite.

Now let us prove the last statement. Write $K = \mathbb{Q}[X]/p(X)$, with $p(X) \in \mathbb{Q}[X]$ irreducible. Write $p(X) = \prod_i p_i(X)$ the decomposition of $p(X)$ into a product of irreducible polynomials in $L[X]$. Then $K \otimes_{\mathbb{Q}} L = \prod_i L[X]/(p_i(X))$. What's more, the polynomial p is split in $\tilde{K}[X]$, so the p_i are also split in $\tilde{K}[X]$. So for every i, we have $L[X]/(p_i(X)) \subset \tilde{K}$, since $\tilde{K}$ contains L and a splitting field of the p_i. Hence the conclusion. □

Now, the next few results, from lemma 2.16 to proposition 2.17, will be dedicated to explaining the link between compositums and Hecke algebras.

Lemma 2.16. *The map*

$$\Psi\colon \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K}) \to \mathrm{Compos}(K, L), \phi \mapsto (\phi(K).L, \phi, \mathrm{incl}_{L/\tilde{K}})$$

induces a bijection from $J \backslash \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$ to $\mathrm{Compos}(K, L)/\sim$, where $\sim$ is the isomorphism equivalence relation.

Proof. Let $\phi \in \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$. The composition by $g \in J$ induces an isomorphism $(\phi(K).L, \phi, \mathrm{incl}_{L/\tilde{K}}) \to (g.\phi(K).L, g.\phi, g.\,\mathrm{incl}_{L/\tilde{K}})$. Since $g \in J$, g fixes L, so $g.\,\mathrm{incl}_{L/\tilde{K}} = \mathrm{incl}_{L/\tilde{K}}$. So the isomorphism induced by g is of the form $\Psi(\phi) \to \Psi(g \cdot \phi)$. Let us check that the map induced by Ψ is injective. Let $\phi, \phi' \in \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \tilde{K})$ and let $f\colon \phi(K) \cdot L \to \phi'(K) \cdot L$ an isomorphism of compositums. Then $f \circ \mathrm{incl}_{\tilde{K}/L} = \mathrm{incl}_{\tilde{K}/L}$ and f is the identity over L, so f can be extended as an isomorphism $g \in J$. Since f is a morphism of compositums, $g\phi = \phi'$, hence $\phi \sim \phi'$.

Let us check it is surjective. By lemma 2.15, every compositum in $\mathrm{Compos}(K, L)$ is isomorphic to a compositum where $\iota_L = \mathrm{incl}_{L/\tilde{K}}$. Let $\iota_K\colon K \to \tilde{K}$ be an embedding, then we can always pick $\phi = \iota_K$. □

Proposition 2.17. *There is a bijection*

$$\Phi\colon J\backslash G/H \to \mathrm{Compos}(K,L), JgH \mapsto (gK\cdot L, k\mapsto g\cdot k, \mathrm{incl}_{L/\tilde{K}}).$$

Its inverse is

$$\Phi^{-1}\colon \mathrm{Compos}(K,L)\to J\backslash G/H, (C,\iota_K,\iota_L)\mapsto \left\{\begin{array}{l} JgH \\ \textit{with } g \textit{ such that} \\ \iota_K(\alpha)=g\cdot\alpha\in\tilde{K}\end{array}\right. .$$

Proof. The proposition derives from the two lemmas 2.15 and 2.16. □

Example 2.18. With the notations of example 2.7, we saw that $H\backslash G/H$ has two equivalence classes: the class of 1 and the class of $(1,3)$.

Let $\tilde{K}$ be a Galois extension of $\mathbb{Q}$, of Galois group S_3, and let K be the subfield of $\tilde{K}$ fixed by H, the subgroup of G spanned by a transposition τ. Then $\mathrm{Compos}(K,K)$ will have two elements. One of them will be $(K,\mathrm{id}_K,\mathrm{id}_K)$ and the other one will be $(\tilde{K},\iota_1,\mathrm{incl}_{K,\tilde{K}})$ where $\iota_1\colon K\to\tilde{K}$ is the action of τ.

Now, using the bijection described in proposition 2.17 and the isomorphisms described in section 2.1, we obtain an "action" of $\mathrm{Compos}(K,L)$ on various R-modules. In the rest of the section we will describe these actions.

Proposition 2.19. *The map*

$$\Phi\colon \mathrm{Compos}(K,L)\to \mathrm{Hom}_{R[G]}(R[G/J],R[G/H])$$

$$(C,\iota_K,\iota_L)\mapsto \left\{\begin{array}{l} \phi \textit{ such that} \\ \phi(1\cdot J)=\sum_{\substack{\gamma H\in G/H\\ J\gamma H=JgH}}\gamma H \\ \textit{with } g \textit{ such } g\cdot\alpha=\iota_K(\alpha)\end{array}\right.$$

is injective.

Proof. This is derived from the proposition 2.17, using the isomorphism of proposition 2.3. □

Let us choose an embedding of K in $\mathbb{C}$ and an embedding of L in $\mathbb{C}$. By the primitive element theorem, we can consider elements α,β of $\mathbb{C}$ such that $K\simeq\mathbb{Q}(\alpha)$ and $L\simeq\mathbb{Q}(\beta)$. Let f, f_L be the minimal polynomials of α and β, and let Z, Z_L be the sets of roots of f and f_L respectively.

Proposition 2.20. *There is an injective morphism*

$$\Phi\colon \mathrm{Compos}(K,L) \to \mathrm{Hom}_{R[G]}(R[Z_L], R[Z])$$

$$(C,\iota_K,\iota_L) \mapsto \begin{cases} \phi \text{ such that} \\ \phi(\beta) = \sum_{\substack{a\in Z_L \\ J\cdot a = J\cdot \iota_K(\alpha)}} \gamma H \\ \text{with } g \text{ such that } g\cdot\alpha = \iota_K(\alpha) \end{cases}.$$

Proof. This is derived from proposition 2.19, using the isomorphism of proposition 2.8. □

For roots α' of f in $\mathbb{C}$, we denote by $\sigma_{\alpha'}$ the embedding of K in $\mathbb{C}$ that sends α to α'. Similarly, denote by $\tau_{\beta'}$ the embedding of L in $\mathbb{C}$ that sends β to β'.

Proposition 2.21. *The map*

$$\begin{aligned} \Phi\colon \mathrm{Compos}(K,L) \to \quad & \mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})], R[\mathrm{Hom}(K,\mathbb{C})]), \\ (C,\iota_K,\iota_L) \mapsto \quad & \begin{cases} \phi \text{ such that} \\ \phi(\tau_\beta) = \sum_{\substack{\sigma\in\mathrm{Hom}(K,\mathbb{C}) \\ (C,\iota_K,\iota_L)\sim(C',\sigma,\tau_\beta)}} \sigma \end{cases} \end{aligned}$$

is injective.

Proof. This is derived from proposition 2.19, using the isomorphism of proposition 2.9. □

As for the propositions 2.8 and 2.9, these two previous propositions are very similar. The formulation with roots of polynomial will often be more useful for implementation, while the formulation with complex embedding will be prefered for theoretical results.

Remark 2.22. Let (C,ι_K,ι_L) be a compositum of K and L, and let ϕ the corresponding element of $\mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})], R[\mathrm{Hom}(K,\mathbb{C})])$. We can obtain a nicer way to write $\phi(\tau_\beta)$:

$$\phi(\tau_\beta) = \sum_{\substack{\sigma\in\mathrm{Hom}(K,\mathbb{C}) \\ (C,\iota_K,\iota_L)\sim(C',\sigma,\tau_\beta)}} \sigma = \sum_{\sigma\in\mathrm{Hom}(K,\mathbb{C})} |E_{\sigma,\tau_\beta}|\cdot\sigma$$

where $E_{\sigma,\tau_\beta} = \{f \in \mathrm{Hom}(C,\mathbb{C}) | \sigma = f\circ\iota_K \text{ and } \tau_\beta = f\circ\iota_L\}$.

And from that form we can deduce a general expression for $\phi(\tau)$ for every complex embedding τ.

Proposition 2.23. *Let (C, ι_K, ι_L) be a compositum of K and L, and let ϕ the corresponding element of $\mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L,\mathbb{C})], R[\mathrm{Hom}(K,\mathbb{C})])$. For all $\tau \in \mathrm{Hom}(L,\mathbb{C})$,*

$$\phi(\tau) = \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |E_{\sigma,\tau}| \cdot \sigma$$

where $E_{\sigma,\tau} = \{f \in \mathrm{Hom}(C,\mathbb{C}) | \sigma = f \circ \iota_K \text{ and } \tau = f \circ \iota_L\}$.

Proof. Let $\tau = \gamma \cdot \tau_\beta$ with $\gamma \in G$. (We can always write τ in that form, because g acts transitively on the elements of $\mathrm{Hom}(L,\mathbb{C})$).

Then,

$$\phi(\tau) = \gamma \cdot \phi(\tau_\beta) = \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |E_{\sigma,\tau_\beta}|(\gamma \cdot \sigma)$$

$$= \sum_{\gamma^{-1}\cdot\sigma \in \mathrm{Hom}(K,\mathbb{C})} |E_{\gamma^{-1}\cdot\sigma,\tau_\beta}| \cdot \sigma.$$

But we have $E_{\gamma^{-1}\cdot\sigma,\tau_\beta} = E_{\sigma,\gamma\cdot\tau_\beta} = E_{\sigma,\tau}$ because $\gamma\colon \mathrm{Hom}(K,\mathbb{C}) \to \mathrm{Hom}(K,\mathbb{C})$ is a bijection.

So finally,

$$\phi(\tau) = \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |E_{\sigma,\tau}| \cdot \sigma$$

because $\gamma\colon \mathrm{Hom}(C,\mathbb{C}) \to \mathrm{Hom}(C,\mathbb{C})$ is a bijection.

□

Similarly, for every $R[G]$-module V, a compositum C of K and L induces a map from V^H to V^J. (The proof is similar to that of proposition 2.23.)

From now on, if x is an element of V^H, we will denote by $C \cdot x$ the image of x by this map.

Theorem 2.24. *Let x be an element of $K^\times$ and let $\mathcal{C} = (C, \iota_K, \iota_L)$ be a compositum of K and L. Then $\mathcal{C} \cdot x = N_{C/L}(\iota_K(x))$.*

Proof. The bijection described in proposition 2.17 allows us to identify the compositum (C, ι_K, ι_L) with an element $J\backslash g/H$ of $J\backslash G/H$.

First, let us prove that the subfield of $\tilde{K}$ fixed by $H \cap (gJg^{-1}) < G$ is C. The subfield fixed by gJg^{-1} is $g(L) = \iota_L(L)$. Denote by $\tilde{C}$ the field fixed by $H \cap (gJg^{-1})$. All elements of K and $\iota_L(L)$ are in $\tilde{C}$ so $C \subset \tilde{C}$. What's more,

if we denote by N the subgroup of G fixing C, then N is included both in H and in gJg^{-1}, so it is included in $H \cap gJg^{-1}$. We get $\tilde{C} \subset C$, so we indeed have $\tilde{K}^{H\cap(gJg^{-1})} = C$.

Now, we know that $C \cdot x = \prod_{\delta \in HgJ/J} \delta x = \prod_{\substack{\delta \in G/J \\ HgJ = H\delta J}} \delta x$, we want to make the change of variables $\delta = hg$. For $h, h' \in H$, we have $hgJ = h'gJ$ if and only if there exists $j \in J$ such that $h = h'(gjg^{-1})$, that is to say if and only if $\overline{h} = \overline{h'}$ in $H/(H \cap (gJg^{-1}))$. This gives $\mathcal{C} \cdot x = \prod_{h \in H/(H\cap(gJg^{-1}))} hgx$. Finally, we obtain

$$\mathcal{C} \cdot x = N_{C/L}(\iota_L(x))$$

as claimed.

□

In practice, to compute the action of Hecke operators between number fields, the most efficient method is often to use the formula from theorem 2.24. This will prove useful in particular in sections 5.2 and 7.3.

We also have the following additive version of theorem 2.24.

Proposition 2.25. *Let x be an element of K and let $\mathcal{C} = (C, \iota_K, \iota_L)$ be a compositum of K and L. Then $\mathcal{C} \cdot x = \mathrm{Tr}_{C/L}(\iota_K(x))$, where $\mathrm{Tr}_{C/L}$ is the trace map.*

Proof. The proof is similar to that of theorem 2.24. □

3 Mackey functors

A Mackey functor is an algebraic structure endowed with operations (induction, restriction and conjugation), satisfying some axioms (see definition 3.1) similar to the induction, restriction and conjugation in group representation theory (see [45, section 7]). They were first introduced by Dress ([20], [19]) and Green ([28]). However, they appear in a large variety of different contexts, which makes their study interesting.

3.1 Definitions and properties

First let us recall the definition of a Mackey functor, as in [9].

Definition 3.1. Let G be a finite group and R a commutative ring. An *R-Mackey functor* $M = (M, c, \mathrm{Res}, \mathrm{Ind})$ on G is a quadruple consisting of

- a family of R-modules $M(H)$ for each $H \leq G$,
- a family of homomorphisms of R-modules $c_{g,H} \colon M(H) \to M({}^gH)$, the *conjugation* maps, for each $g \in G$, $H \leq G$ and ${}^gH = gHg^{-1}$,
- a family of homomorphisms of R-modules $\mathrm{Res}^H_J \colon M(H) \to M(J)$, the *restriction maps*, for each $J \leq H \leq G$, and
- a family of homomorphisms of R-modules $\mathrm{Ind}^H_J \colon M(J) \to M(H)$, the *induction* maps, for each $J \leq H \leq G$,

such that the following axioms are satified:

- (Triviality) $c_{h,H} = \mathrm{Res}^H_H = \mathrm{Ind}^H_H = \mathrm{id}_{M(H)}$ for all $H \leq G$ and $h \in H$.
- (Transitivity) $c_{g'g,H} = c_{g',{}^gH} \circ c_{g,H}$, $\mathrm{Res}^J_L \circ \mathrm{Res}^H_J = \mathrm{Res}^H_L$ and $\mathrm{Ind}^H_J \circ \mathrm{Ind}^J_L = \mathrm{Ind}^H_L$ for all $L \leq J \leq H \leq G$ and $g, g' \in G$.
- (G-equivariance) $c_{g,J} \circ \mathrm{Res}^H_J = \mathrm{Res}^{{}^gH}_{{}^gJ} \circ c_{g,H}$ and $c_{g,J} \circ \mathrm{Ind}^H_J = \mathrm{Ind}^{{}^gH}_{{}^gJ} \circ c_{g,J}$ for all $J \leq H \leq G$ and $g \in G$.
- (Mackey formula) For all $H \leq G$, $U, J \leq H$, one has

$$\mathrm{Res}^H_U \circ \mathrm{Ind}^H_J = \sum_{h \in U\backslash H/J} \mathrm{Ind}^U_{U\cap {}^hJ} \circ \mathrm{Res}^{{}^hJ}_{U\cap {}^hJ} \circ c_{h,J}$$

  where $h \in H$ runs through a set of representatives for the double cosets $U\backslash H/K$.

Definition 3.2. An R-Mackey functor M on G is called *cohomological* if the axiom

$$\mathrm{Ind}_J^H \circ \mathrm{Res}_J^H = [H : J]\,\mathrm{id}_{M(H)}, \text{ for all } J \leq H \leq G$$

holds.

Now, in the rest of the section, let us see two results (theorem 3.3 and theorem 3.4) that will link the formalism of Mackey functors to the objects sudied in section 2.1.

Theorem 3.3. *Let R be a commutative ring and G a group. The association $H \mapsto R[G/H]$ for every subgroups $H < G$ forms a cohomological Mackey functor with the following operations:*

- $\mathrm{Ind}_K^H \colon R[G/K] \to R[G/H], gH \mapsto gK$ *for* $K < H$.
- $\mathrm{Res}_K^H \colon R[G/H] \to R[G/K], gH \mapsto \sum_{h \in H/K} ghK$ *for* $K < H$.
- $c_{g,H} \colon R[G/H] \to R[G/{}^gH], xH \mapsto xg^{-1}\ {}^gH$

Proof. This result can be deduced from [51, example 4.1], with D the trivial group. However, we will give here a more basic proof, by simply verifying all the axioms.

1. Triviality
   - For $h \in H$, we have $c_{h,H} : xH \mapsto xh^{-1}H = xH$.
   - What's more, $\mathrm{Res}_H^H : gH \mapsto \sum_{h \in H/H} ghH = gH$.
   - Finally, $\mathrm{Ind}_H^H : gH \mapsto gH$.
2. Transitivity:
   - For all $g, g' \in G$ et $H < G$, we have $c_{g'g,H} : xH \mapsto xg^{-1}g'^{-1}.{}^{g'g}H$, and $c_{g',{}^gH} \circ c_{g,H} : xH \mapsto c_{g',{}^gH}(xg^{-1}.{}^gH) = xg^{-1}g'^{-1}.{}^{g'g}H$.
   - For all $L < K < H < G$, we have $\mathrm{Ind}_K^H \circ \mathrm{Ind}_L^K = \mathrm{Ind}_L^H$.
   - For all $L < K < H < G$, we have

$$\mathrm{Res}_L^K \circ \mathrm{Res}_K^H : gH \mapsto \sum_{k \in K/L} \sum_{h \in H/K} gkhH.$$

Let us show that this last expression is equal to $\sum_{x\in H/L} gxH$.
Let $hK \in H/K$ and $kL \in K/L$, to which we associate $hkL \in H/L$. Let us show that this association induces a bijection from a set of representatives (h,k) of $H/K \times K/L$ to a set of representatives of H/L.

Let $h' \in H/L$, let h be a representative of the class of h' in H/K, we have $k \in K$ a representative of $h'^{-1}h$ in K/L such that $hk = h' \mod L$.

Then we have to show it is injective. Consider $(h,k),(h',k')$ with $h,h' \in H$ in a set of representatives modulo K and $k,k' \in K$ in a set of representatives modulo L, such that there exists $l \in L$ such that $hk = h'k'l$. Then $h = h'(k'lk^{-1})$ so $h = h' \mod K$ so $h = h'$. And then $hk = hk'l$ so $k = k'l$, so $k = k' \mod L$ hence $k = k'$.

3. G-equivariance:

   - For $g \in G$ and $K < H < G$, we have

   $$c_{g,K} \circ \mathrm{Res}^H_K(xH) = c_{g,K}(\sum_{h\in H/K} xhK) = \sum_{h\in H/K} xhg^{-1}.{}^gK.$$

   And

   $$\mathrm{Res}^{{}^gH}_{{}^gK} \circ c_{g,H}(xH) = \mathrm{Res}^{{}^gH}_{{}^gK}(xg^{-1}H) = \sum_{h\in H/K} xhK) = \sum_{h\in {}^gH/{}^gK} xhg^{-1}.{}^gK.$$

   Those two sums are equal because we have $h = \tilde{h}k$ if and only if $ghg^{-1} = g\tilde{h}g^{-1}[{}^gK]$.

   - What's more,

   $$\begin{aligned} &c_{g,H} \circ \mathrm{Ind}^H_K(xK) = c_{g,H}(xH) = xg^{-1}.{}^gH \\ &= \mathrm{Ind}^{{}^gK}_{{}^gH} \circ c_{g,H}(xH). \end{aligned}$$

4. Mackey formula:

   For $H < G$ et $U, K < H$, we have

   $$\mathrm{Res}^H_U \circ \mathrm{Ind}^H_K(xK) = \mathrm{Res}^H_U(xH) = \sum_{h\in H/U} xhU.$$

And

$$\sum_{h\in U\backslash H/K} \mathrm{Ind}_{U\cap {}^hK}^{U} \circ \mathrm{Res}_{U\cap {}^hK}^{{}^hK} \circ c_{h,k}(xK) = \sum_{h\in U\backslash H/K} \sum_{{}^hK/U\cap {}^hK} xh^{-1}kU.$$

So we want to show that $\sum_{h\in U\backslash H/K} \sum_{{}^hK/U\cap {}^hK} h^{-1}kU = \sum_{g\in H/U} gU$. We have $\sum_{g\in H/U} gU = \sum_{\eta\in K\backslash H/U} \sum_{\substack{g\in H/U \\ KgU=K\eta U}} gU$, and $\sum_{\substack{g\in H/U \\ KgU=K\eta U}} gU = \sum_{\delta\in K/\eta U\cap K} \delta\eta U = \sum_{\delta'\in \eta^{-1}K/U\cap \eta^{-1}K} \delta'\eta U$. Hence the conclusion.

5. Cohomological property:

   For $K < H < G$, we have

$$\mathrm{Ind}_K^H \circ \mathrm{Res}_K^H(gH) = \mathrm{Ind}_K^H(\sum_{h\in H/K} ghK) = \sum_{h\in H/K} ghH = [H:K]gH.$$

□

Theorem 3.4. *Let M be a cohomological Mackey functor. If H, K are subgroups of G and g an element of G, let us define the operator*

$$T_{HgK}\colon M(K) \to M(H), x \mapsto \mathrm{Ind}_{{}^gK\cap H}^{H} \circ \mathrm{Res}_{{}^gK\cap H}^{{}^gK} \circ c_{g,K}(x).$$

Then, all operators of this form follow the rules of compositions of $R[H\backslash G/K]$ coming from the isomorphism of proposition 2.3.

Proof. One can find the proof in [51, theorem 4.1]. However, here is a more down to earth proof:

Consider $H, K, J < G$ and $g, \delta \in G$. Let us consider

$$T_{HgK} : M(K) \to M(H)$$

and

$$T_{J\delta H} : M(H) \to M(J).$$

Then

$$
\begin{aligned}
&T_{J\delta H}\circ T_{HgK}(x) = \mathrm{Ind}_{\delta H\cap J}^{J}\circ \mathrm{Res}_{\delta H\cap J}^{\delta H}\circ c_{\delta,H}\circ \mathrm{Ind}_{gK\cap H}^{H}\circ \mathrm{Res}_{gK\cap H}^{gK}\circ c_{g,K}(x)\\
&= \mathrm{Ind}_{\delta H\cap J}^{J}\circ \mathrm{Res}_{\delta H\cap J}^{\delta H}\circ \left(\mathrm{Ind}_{\delta(gK\cap H)}^{\delta H}\circ c_{\delta,gK\cap H}\right)\circ \mathrm{Res}_{gK\cap H}^{gK}\circ c_{g,K}(x)\\
&= \mathrm{Ind}_{\delta H\cap J}^{J}\circ \mathrm{Res}_{\delta H\cap J}^{\delta H}\circ \mathrm{Ind}_{\delta(gK\cap H)}^{\delta H}\circ \left(\mathrm{Res}_{\delta(gK\cap H)}^{\delta gK}\circ c_{\delta,gK}\right)\circ c_{g,K}(x)\\
&= \mathrm{Ind}_{\delta H\cap J}^{J}\circ \mathrm{Res}_{\delta H\cap J}^{\delta H}\circ \mathrm{Ind}_{\delta(gK\cap H)}^{\delta H}\circ \mathrm{Res}_{\delta(gK\cap H)}^{\delta gK}\left(\circ c_{\delta g,K}\right)\\
&= \mathrm{Ind}_{\delta H\cap J}^{J}\circ \left(\sum_{h\in {}^{\delta}H\cap H\backslash {}^{\delta}H/{}^{\delta}(gK\cap H)} \mathrm{Ind}_{\Gamma_h}^{{}^{\delta}H\cap J}\circ \mathrm{Res}_{\Gamma_h}^{{}^{h\delta}(gK\cap H)}\circ c_{h,{}^{\delta}(gK\cap H)}\right)\circ \mathrm{Res}_{\delta(gK\cap H)}^{\delta gK}\circ c_{\delta g,K}
\end{aligned}
$$

(with $\Gamma_h = (\delta H\cap J)\cap {}^{h\delta}({}^{g}K\cap H)$.)

$$
\begin{aligned}
&= \mathrm{Ind}_{\delta H\cap J}^{J}\circ \sum_{h\in {}^{\delta}H\cap H\backslash {}^{\delta}H/{}^{\delta}(gK\cap H)} \mathrm{Ind}_{\Gamma_h}^{{}^{\delta}H\cap J}\circ \mathrm{Res}_{\Gamma_h}^{{}^{h\delta}(gK\cap H)}\circ \left(\mathrm{Res}_{h\delta(gK\cap H)}^{h\delta gK}\circ c_{h,{}^{\delta}gK}\right)\circ c_{\delta g,K}\\
&= \sum_{h\in {}^{\delta}H\cap H\backslash {}^{\delta}H/{}^{\delta}(gK\cap H)} \mathrm{Ind}_{\Gamma_h}^{J}\circ \mathrm{Res}_{\Gamma_h}^{{}^{h\delta g}K}\circ c_{h\delta g,K}.
\end{aligned}
$$

But we also have

$$\mathrm{Ind}_{\Gamma_h}^{J} = \mathrm{Ind}_{J\cap {}^{h\delta g}K}\circ \mathrm{Ind}_{\Gamma_h}^{J\cap {}^{h\delta g}K}$$

and

$$\mathrm{Res}_{\Gamma_h}^{{}^{h\delta g}K} = \mathrm{Res}_{\Gamma_h}^{J\cap {}^{h\delta g}K}\circ \mathrm{Res}_{J\cap h\delta gK}^{{}^{h\delta g}K}$$

and

$$\mathrm{Ind}_{\Gamma_h}^{J\cap {}^{h\delta g}K}\circ \mathrm{Res}_{\Gamma_h}^{J\cap {}^{h\delta g}K} = [H:K]id_{M(H)}$$

since M is a cohomological Mackey functor.

Hence finaly

$$
\begin{aligned}
T_{J\delta H}\circ T_{HgK} &= [H:K]\sum_{h\in {}^{\delta}H\cap H\backslash {}^{\delta}H/{}^{\delta}(gK\cap H)} \mathrm{Ind}_{J\cap {}^{h\delta g}K}^{J}\circ \mathrm{Res}_{J\cap {}^{h\delta g}K}^{{}^{h\delta g}K}\circ c_{h\delta g,K}\\
&= [H:K]\sum_{h\in {}^{\delta}H\cap H\backslash {}^{\delta}H/{}^{\delta}(gK\cap H)} T_{H(h\delta g)K}.
\end{aligned}
$$

□

Proposition 3.5. *Let R be a ring, G a group, $H < G$ a subgroup and $\{J_i\}$ a set of subgroups. If we have $\phi\colon \bigoplus_{i=1}^m R[G/J_i] \to R[G/H]$ a morphism of $R[G]$-modules and $\psi\colon R[G/H] \to \bigoplus_{i=1}^m R[G/J_i]$ a morphism of $R[G]$-modules, such that $\phi \circ \psi = d \cdot \mathrm{id}_{R[G/H]}$, then for every cohomological Mackey functor M, there exists $\phi_M\colon \bigoplus_{i=1}^m M(J_i) \to M(H)$ and $\psi_M\colon M(H) \to \bigoplus_{i=1}^m M(J_i)$ such that $\phi_M \circ \psi_M = d \cdot \mathrm{id}_{M(H)}$.*

Proof. One can find a proof in [9, corollary 1.4]. However, here is an other proof using theorem 3.4.

We can view the morphism $\phi\colon \bigoplus_{i=1}^m R[G/J_i] \to R[G/H]$ as a sum of morphisms $\phi_i\colon R[G/J_i] \to R[G/H]$.

Similarly, if we denote by π_j the projection $\bigoplus_{i=1}^m R[G/J_i] \to R[G/J_j]$, we can view the morphism $\psi\colon R[G/H] \to \bigoplus_{i=1}^m R[G/J_i]$ as a sum of morphisms $\psi_j\colon R[G/H] \to R[G/J_j]$, with $\psi_j = \pi_j \circ \psi$.

Then, by proposition 2.3, we can associate every ϕ_i with an element of $R[J_i\backslash G/H]$, and every ψ_j with an element of $R[H\backslash G/J_j]$.

By theorem 3.4, we can then associate to every ϕ_i an operator $T_{\phi_i}\colon M(J_i) \to M(H)$, and to every ψ_j an operator $T_{\psi_j}\colon M(H) \to M(J_j)$.

Then, we take $\phi_M = \sum_i T_{\phi_i}$ and $\psi_M = \sum_j T_{\psi_j}$.

Since ϕ_M and ψ_M follow the same composition law as ϕ and ψ, by theorem 3.4, then we have $\phi_M \circ \psi_M = d \cdot \mathrm{id}_{M(H)}$ as claimed.

□

Remark 3.6. The statement of proposition 3.5 does not describe the forms of ϕ_M and ψ_m, but we see in the proof that we can describe them more precisely. They are obtained by decomposing ϕ and ψ into sums of morphisms respectively $R[G/J_i] \to R[G/H]$ and $R[G/H] \to R[G/J_i]$, expressing these morphisms as elements of $H\backslash G/J_i$ or $J_i\backslash G/H$ and then applying theorem 3.4.

3.2 Normed Mackey functors

In several cases of applications of Mackey functors, the modules $M(H)$ naturally come equipped with a lattice structure (ie they are **normed R-modules**). The goal of this section is to enrich the theory of Mackey functors to take into account such norms on the modules $M(H)$ and keep track of the relations between the lattice structures of the various $M(H)$. This section is largely based on the article [1], which is still in preparation.

First, let us give some context to motivate the study of normed Mackey functors.

In [48], the author studies relations between the successive minima of arithmetically equivalent number fields (see definitions 3.7 and 3.8).

Definition 3.7.

- Let K be a number field. The *Dedekind zeta function* of K is the map ζ_K defined for complex numbers s such that $\mathrm{Re}(s) > 1$, by

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \neq 0 \\ \text{ideal of } z_K}} [\mathbb{Z}_K : \mathfrak{a}]^{-s}.$$

- Two number fields K and K' are said to be *arithmetically equivalent* if they have the same Dedekind zeta function.

Definition 3.8. Let K be a number field of degree d and let $\sigma_1, \cdots, \sigma_d$ be the complex embeddings of K.

- The *Minkowski embedding* of K is the map

$$\iota \colon K \to \mathbb{C}^d, v \mapsto (\sigma_1(v), \cdots, \sigma_d(v)).$$

- We can then define a euclidean norm $||.||$ on K, by

$$\forall v \in K, ||v|| = \sqrt{\frac{1}{d}(|\sigma_1(v)|^2 + \cdots + |\sigma_d(v)|^2)}.$$

- The i-th *successive minimum* of K is the smallest $\lambda_i \in \mathbb{R}$ such that the set $\{v \in \mathbb{Z}_K, ||v|| \leq \lambda_i\}$ contains i $\mathbb{Q}$-linearly independent elements.

The main result in [48] is the following theorem:

Theorem 3.9 (Theorem 1 of [48])**.** *Let $d \geq 1$ be an integer. There exists a constant $c_d > 0$ such that the following holds. Let K and K' be two arithmetically equivalent number fields of degree d. Let $\lambda_1 \leq \cdots \leq \lambda_d$ and $\lambda'_1 \leq \cdots \leq \lambda'_d$ be the multisets of successive minima of K and K'. Then for all i, we have*

$$\lambda_i \leq c_d \lambda'_i.$$

To obtain a bound on the constant c_d, one method (used in [48, proposition 6]) is to find a linear map $\phi \colon K \to K'$ such that

1. ϕ is an morphism of $\mathbb{Q}$-vector space,

2. we have the inclusion $\phi(\mathbb{Z}_K) \subseteq \mathbb{Z}_{K'}$,

3. for every non zero $v \in \mathbb{Z}_K$, we find a bound on $\frac{||\phi(v)||}{||v||}$.

We know that the maps $K \to K'$ induced by Hecke operators satisfy the conditions 1 and 2 by proposition 2.25. The results in this section will allow us to find a bound for condition 3. (See in particular lemma 3.15 and theorem 3.16).

Now, let us recall some preliminary definitions, before defining the main objects of this section, normed Mackey functors, in definition 3.14.

Definition 3.10. A **normed domain** R is a domain equipped with a norm map $|\cdot|\colon R \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in R$,

1. we have $|x| = 0$ if and only if $x = 0$,

2. and $|xy| = |x||y|$,

3. and $|x + y| \leq |x| + |y|$.

Note that a norm on a normed domain R can be extended to the field of fractions of R.

Definition 3.11. If R is a normed domain, a **semi-normed** R-module A is an R-module equipped with a semi-norm $||\cdot||\colon A \to \mathbb{R}_{\geq 0}$, ie a map such that for all $x, y \in A$, and for all $r \in R$,

1. there exists some $z \in A$ such that $||z|| \neq 0$,

2. we have $||rx|| = |r| \cdot ||x||$,

3. and $||x + y|| \leq ||x|| + ||y||$.

Definition 3.12. If $f\colon A \to B$ is a R-module homomorphism between semi normed R-modules, then the **operator norm** of f is

$$||f|| = \inf\{r \in \mathbb{R}; ||f(a)|| \leq r||a||, \text{ for all } a \in A\}.$$

It can be either a real number or ∞. We say the map f is **bounded** if $||f|| < \infty$.

Proposition 3.13. *With the notations of definition 3.12, if* $||f|| < \infty$*, then for every* $a \in A$*, we have* $||f(a)|| \leq ||f|| \cdot ||a||$*, i.e. the* inf *in the definition is actually a* min*.*

Proof. For all $a \in A$, the set $S_a = \{r \in \mathbb{R}; ||f(a)|| \leq r||a||\}$ is a closed interval in $\mathbb{R}$, so it contains its infimum. □

Definition 3.14. If R is a normed domain, then a **normed R-Mackey functor** is a cohomological Mackey functor M such that

- for every subgroup $H < G$, the R-module $M(H)$ is semi-normed,
- for every subgroup $K < H$ of G, and every $g \in G$, the maps $c_{g,H}$ and Res^H_K have operator norm bounded by 1,
- for every subgroup $K < H$ of G, the map Ind^H_K has operator norm bounded by $\max\{1, |[H : K]|\}$.

A normed $\mathbb{Z}$-Mackey functor where we use the absolute value on $\mathbb{Z}$ will be called a **normed Mackey functor**.

The max in the definition is superfluous in the examples that we will develop here, but it is necessary for examples over function fields that will be presented in [1].

In the rest of the section, we will apply these definitions to the context of Hecke operators. The main result will be theorem 3.16. Then we will give some examples.

Lemma 3.15. *Let M be a normed Mackey functor. If U_1, U_2 are subgroups of G, g an element of G, and x in $M(U_1)$, then, with the notations of theorem 3.4, we have*

$$||T_{U_1 g U_2}|| \leq \max\{1, |[U_2 : {}^{g^{-1}}U_1 \cap U_2]|\}.$$

Proof. By definition, we have $||T_{U_1 g U_2}(x)|| = ||\mathrm{Ind}^{U_1}_{{}^g U_2 \cap u_1} \circ \mathrm{Res}^{{}^g U_2}_{{}^g U_2 \cap U_1} \circ c_{g,U_2}(x)||$.

The result then follows from the definition 3.14 of normed Mackey functors, since c_{g,U_2} and $\mathrm{Res}^{{}^g U_2}_{{}^g U_2 \cap U_1}$ have operator norm bounded by 1, and $\mathrm{Ind}^{U_1}_{{}^g U_2 \cap U_1}$ has operator norm bounded by $\max\{1, |[U_2 : {}^{g^{-1}}U_1 \cap U_2]|\}$. □

Theorem 3.16. *Let R be a normed domain with field of fractions k, and let M be a normed R-Mackey functor on a finite group G. Let $U_1, \cdots U_n$*

and $U'_1, \cdots U'_m$ be subgroups of G for which there exists an epimorphism of $k[G]$-modules

$$\Phi\colon \bigoplus_i k[G/U_i] \to \bigoplus_j k[G/U'_j].$$

Then there is a R-linear map

$$\phi\colon \bigoplus_{i,j} M(U_i)^{U_i\backslash G/U'_j} \to \bigoplus_j M(U'_j)$$

such that the base change $\phi \otimes k$ is surjective and such that ϕ has operator norm bounded by

$$\max\{1, \max\{|[U'_i : gU_jg^{-1} \cap U'_i]| \text{ for } g \in G, i = 1, \cdots m, \text{ and } j = 1, \cdots, n\}\}.$$

Proof. We can decompose the morphism Φ in $\Phi = \sum_{i=1}^n \Phi_i$ with $\Phi_i\colon k[G/U_i] \to \bigoplus_j k[G/U'_j]$.

Then, if we denote by π_k the projection $\bigoplus_j k[G/U'_j] \to k[G/U'_k]$, with $1 \leq l \leq m$, then for all i, we have $\Phi_i = \sum_{j=1}^m \Phi_{i,j}$ with $\Phi_{i,j} = \pi_j \circ \Phi_i$. Hence $\Phi = \sum_{i,j} \Phi_{i,j}$ with $\Phi_{i,j}\colon k[G/U_i] \to k[G/U'_j]$.

Then, for every pair (i, j), $\Phi_{i,j}$ is the morphism associated to an element $\sum_k U_i g_{i,j,k} U_j$ of $k[U_i\backslash G/U_j]$ by the isomorphism of proposition 2.3. So by theorem 3.4, we have

$$\phi = \sum_{i,j} T_{\sum_k U_i g_{i,j,k} U_j}\colon \bigoplus_{i,j} M(U_i)^{U_i\backslash G/U'_j} \to \bigoplus_j M(U'_j).$$

And the bound on the operator norm is a direct result of lemma 3.15.

□

Example 3.17. Let V be a $\mathbb{Z}[G]$-module, equipped with a G-invariant euclidean inner product. For every $H < G$, denote by $M(H) = V^H$ the set of points in V fixed by the action of H.

Then M is a Mackey functor with

- for $H < G$ and for $g \in G$, $c_{g,H}\colon M(H) \to M({}^gH), x \mapsto g \cdot x$,
- for $H < J < G$, $\mathrm{Res}^H_J\colon M(H) \to M(J), x \mapsto x$,
- also for for $H < J < G$, $\mathrm{Ind}^H_J\colon M(J) \to M(H), x \mapsto \sum_{h \in H/J} h \cdot x$.

In addition, M is normed, using the restriction of the euclidean norm to V^H.

Proof. First let us prove that M is a Mackey functor. The axioms of triviality, transitivity and G-equivariance are immediate to verify.

For all $H < G$ and $U, J \leq H$, and for all $x \in M(J)$, we have

$$\mathrm{Ind}_U^H \circ \mathrm{Res}_J^H(x) = \sum_{u \in U/H} u \cdot x$$

and

$$\sum_{h \in U\backslash H/J} \mathrm{Ind}_{U\cap {}^hJ}^U \circ \mathrm{Res}_{U\cap {}^hJ}^{{}^hJ} \circ c_{h,J}(x) = \sum_{h \in U\backslash H/J} \mathrm{Ind}_{U\cap {}^hJ}^U (h{\cdot}x) = \sum_{h \in U\backslash H/J} \sum_{u \in U\cap {}^hJ/U} (uh){\cdot}x$$

So we have indeed $\mathrm{Ind}_U^H \circ \mathrm{Res}_J^H(x) = \sum_{u \in U/H} u \cdot x$, so the Mackey formula stands.

Then, let us prove that M is normed.

- Since V has a norm derived from the euclidean inner product, it is a semi-normed $\mathbb{Z}$-module, and then for all $H < G$, $M(H) = V^H$ is a semi-normed $\mathbb{Z}$-module, with the norm inherited from V.
- For every $J < H < G$ and for every $g \in G$, it is clear that $c_{g,H}$ and Res_J^H are isometries.
- For every $H < J < G$ and for every $x \in M(J) = V^J$, we have $||\mathrm{Ind}_J^H(x)|| = ||\sum_{h \in H/K} h \cdot x|| \leq \sum_{h \in H/J} ||h \cdot x|| = |[J : H]| \cdot ||x||$. So the operator norm of Ind_J^H is bounded by $\max\{1, |[J : H]|\}$.

□

Example 3.18. Let K be a Galois extension of $\mathbb{Q}$, and let G be its Galois group. Then K is a semi-normed $\mathbb{Z}$-module with the normed induced by the Minkowski scalar product (see definition 3.8). If $H < G$, we will denote by $M(H)$ the subfield of K fixed by H. With these notations, M is a normed Mackey functor, with:

- For $H < G$ and $g \in G$, $c_{g,H} : x \mapsto g \cdot x$
- For $H < J < G$, $\mathrm{Res}_J^H : M(H) \to M(J), x \mapsto x$

- Also for $H < J < G$, $\mathrm{Ind}_J^H : M(J) \to M(H), x \mapsto \sum_{h \in H/J} hx$

This is simply a particular case of example 3.17.

By applying theorem 3.16 and example 3.18 to the particular case of a so called *Gassmann triple*, i.e. an isomorphism of the form $\mathbb{Q}[G/H] \simeq \mathbb{Q}[G/H']$, we can recover [48, theorem 1]. In the article [1], in preparation, we plan to study other examples of normed Mackey functors. In particular, we will develop an analogy of the number field case (example 3.18) to curves over functions fields. We will also study the case of Sunada isospectral manifolds (see [47]).

4 Norm relations

Suppose K/F is a Galois extension of number fields, of Galois group G. In [7], the authors studied a type of relation in $R[G]$, where R is a commutative ring, called *norm relation*. They then derive from such relations an inductive algorithm to compute the class group or the groups of S-units of K by induction, reducing the problem to a similar problem on some auxiliary subfields.

In section 4.1, we will define norm relations as in [7], and give some of their important properties. We will call them "classical" norm relations, as opposed to "generalised" norm relations, that we shall define and study in section 4.2.

In all of this chapter, G will denote a finite group.

4.1 Classical norm relation

This section will be largely based on [7].

Definition 4.1. Let H be a subgroup of G. We call the element $N_H = \sum_{h\in H} h \in \mathbb{Z}[G]$ the *norm element* of H.

Definition 4.2. Let $\mathcal{H}$ be a set a subgroups of G and R a commutative ring. A *norm relation over R with respect to $\mathcal{H}$* is an equality in $R[G]$ of the form

$$1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$$

where $a_i, b_i \in R[G]$, $H_i \in \mathcal{H}$, and $H_i \neq 1$.

Note that the H_i can appear with repetitions in the formula.

Example 4.3. The symmetric group S_3 admits a norm relation over $\mathbb{Q}$ with respect to $\mathcal{H} = \{\langle(1,2,3)\rangle, \langle(2,3)\rangle\}$. Indeed, one can check that

$$\begin{aligned} 1 = &- N_{\langle 2,3\rangle}((1,2,3) + 2\cdot(1,3)) + (1,2)N_{\langle 2,3\rangle}((2,3) + 2\cdot(1,2,3)) \\ &+ N_{\langle(1,2,3)}(2,3,4). \end{aligned}$$

In [22], our approach was to propose a more general type of relations (which we will study in section 4.2), and then generalise some of the main results in [7]. Let us recall here some of the properties of classical norm relations proven in [7], that we will adapt to generalised norm relation in section 4.2.

Proposition 4.4 (Proposition 2.10 of [7]). *Let $\mathcal{H}$ be a set of non trivial subgroups of G. Then the following are equivalent.*

- *There exists a norm relation in G over $\mathbb{Q}$ with respect to $\mathcal{H}$.*
- *We have $\langle N_H; H \in \mathcal{H} \rangle_{\mathbb{Q}[G]} = \mathbb{Q}[G]$ as a two sided ideal.*
- *For every simple $\mathbb{Q}[G]$-module V, there exists $H \in \mathcal{H}$ such that $V^H \neq \{0\}$.*
- *For every simple $\overline{\mathbb{Q}}[G]$-module V, there exists $H \in \mathcal{H}$ such that $V^H \neq \{0\}$.*
- *For every simple $\mathbb{C}[G]$-module V, there exists $H \in \mathcal{H}$ such that $V^H \neq \{0\}$.*

Now let us consider a relation in $\mathbb{Z}[G]$ of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i \tag{1}$$

with $H_i < G$, $a_i, b_i \in \mathbb{Z}[G]$ and $d \in \mathbb{Z}_{>0}$. That is to say a norm relation over $\mathbb{Q}$ where we multiplied each side by an adequate integer d to get a relation in $\mathbb{Z}[G]$.

In order to state proposition 4.7, we first need the following definitions:

Definition 4.5. Let R be a commutative ring. The *annihilator* of a subset S of an R-module M is $\mathrm{Ann}(S) = \{r \in R; \forall x \in S, rx = 0\}$.

Definition 4.6. The *exponent* of a $\mathbb{Z}$-module is the positive generator of the group of annihilators.

Proposition 4.7 (Proposition 3.1 of [7]). *Let M be a $\mathbb{Z}[G]$-module. If G admits a relation of the form (1), then the exponent of the quotient*

$$M / \sum_{i=1}^{\ell} a_i M^{H_i}$$

is finite and divides d.

Proposition 4.7 is quite general since it works for any finite group G and any $\mathbb{Z}[G]$-module M. For our purposes, we want to apply it to the context of number fields. That will be done with corollary 4.10. However, to state it, we first need to define S-units, and saturation.

Let $K/\mathbb{Q}$ be a Galois extension of number fields, of Galois group G.

Definition 4.8. Let S be a G-stable set of non zero prime ideals in the ring of integers $\mathbb{Z}_K$ of K. The group $\mathbb{Z}_{K,S}^\times$ of *S-units* of K is the subgroup of $K^\times$ defined by

$$\mathbb{Z}_{K,S}^\times = \{x \in K^\times ; v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}$$

where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation.

If L is a subfield of K, then we will define the S-units of L to be $\mathbb{Z}_{L,S}^\times = \mathbb{Z}_{L,S'}^\times$ with $S' = \{L \cap \mathfrak{p} | \mathfrak{p} \in S\}$.

With this definition, the multiplicative group $\mathbb{Z}_{K,S}^\times$ is a $\mathbb{Z}[G]$-submodule of $K^\times$, and for every subgroup $H < G$, we have $(\mathbb{Z}_{K,S}^\times)^H = \mathbb{Z}_{K^H,S}^\times$.

Definition 4.9. Let V be a finitely generated subgroup of $K^\times$, and let d be a positive integer. The *d-saturation* of V is the smallest subgroup $W \subset K^\times$ such that $V \subset W$ and $K^\times/W$ is d-torsion free. This is equivalent to adding to V all possible d^i-th roots in $K^\times$, for all $i \in \mathbb{Z}_{\geq 1}$.

Similarly, the *saturation* of V is the smallest subgroup $W \subset K^\times$ such that $V \subset W$ and $K^\times/W$ is torsion free.

In particular, the group $\mathbb{Z}_{K,S}$ is saturated.

When V is a $\mathbb{Q}[G]$-module and $a \in \mathbb{Q}[G]$, we will denote by V^a the image of V by the action of a.

Corollary 4.10 (Corollary 3.4 of [7])**.** *If G admits a norm relation of the form (1), then the exponent of the quotient*

$$\mathbb{Z}_{K,S}^\times / (\mathbb{Z}_{K^{H_1},S}^\times)^{a_1} \cdots (\mathbb{Z}_{K^{H_\ell},S}^\times)^{a_\ell}$$

is finite and divides d. In particular, the group $\mathbb{Z}_{K,S}^\times$ of S-units of K equals the d-saturation of the $\mathbb{Z}[G]$-module generated by $(\mathbb{Z}_{K^{H_1},S}^\times) \cdots (\mathbb{Z}_{K^{H_\ell},S}^\times)$.

This corollary is the cornerstone of an algorithm described in [7] to compute inductively the group of S-units of number fields. See section 5.1.

4.2 Generalised norm relations

Now, let us give a generalisation of definition 4.2, and see how the properties in section 4.1 can be adapted to this new definition.

Definition 4.11. Let H be a subgroup of G, $\mathcal{J}$ a set a subgroups of G and R a commutative ring. A *generalised norm relation over R with respect to H and $\mathcal{J}$* is an equality in $R[G]$ of the form

$$N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$$

where $a_i, b_i \in R[G]$, $J_i \in \mathcal{J}$, and $J_i \neq 1$.

Remark 4.12.

- Clearly, with the notations above, a classical norm relation is a generalised norm relation where H is the trivial subgroup.
- If a finite group G admits a generalised norm relation over a commutative ring R with respect to $H < G$ and $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ with $J_i < G$, let $\tilde{J}_1$ be a subgroup of G conjugate to J_1. Then G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and $\tilde{\mathcal{J}} = \{\tilde{J}_1, J_2, \cdots, J_\ell\}$.
- With the same notations, let $J_{\ell+1}$ be any other subgroup of G, then G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}_2 = \{J_1, \cdots, J_\ell, J_{\ell+1}\}$.

Example 4.13. Let $G = S_4$ seen as the group of permutations of the set $\{1,2,3,4\}$, and let $H = \langle (1,2),(3,4)\rangle \simeq C_2 \times C_2$.

If we take $J_1 = \langle (1,4)(2,3),(1,3)(2,4),(3,4)\rangle \simeq D_8$ and $J_2 = \langle (3,4),(2,4,3)\rangle \simeq S_3$, then, one can check that we have a relation

$$2N_H = a_1 N_{J_1} b_1 + a_2 N_{J_2} b_2$$

with $a_1 = -1_G$, $a_2 = 1_G + (1,2)$, $b_1 = (2,3,4) + (2,4)$ and $b_2 = (3,4) + (1,2,4,3)$.

The following proposition will give us some equivalent definitions of generalised norm relations. It is very similar to proposition 4.4 in the case of classical norm relations.

Proposition 4.14. *Let H be a subgroup of G, and $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ a set of non trivial subgroups of G. Then the following assertions are equivalent:*

1. *There exists a surjective morphism of* $\mathbb{Q}[G]$*-modules*

$$\phi\colon \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$$

where for all i, $n_i \in \mathbb{Z}_{>0}$.

2. *If* $e_1, \ldots, e_r$ *are the central primitive idempotent elements of* $\mathbb{Q}[G]$*, then for all* $1 \leq i \leq r$*, if* $e_i N_H \neq 0$*, there exists* $J \in \mathcal{J}$ *such that* $e_i N_J \neq 0$.

3. *For all simple* $\mathbb{Q}[G]$*-module* V*, if* $V^H \neq 0$*, there exists* $J \in \mathcal{J}$ *such that* $V^J \neq 0$.

4. *For all simple* $\overline{\mathbb{Q}}[G]$*-module* V*, if* $V^H \neq 0$*, there exists* $J \in \mathcal{J}$ *such that* $V^J \neq 0$.

5. *For all simple* $\mathbb{C}[G]$*-module* V*, if* $V^H \neq 0$*, there exists* $J \in \mathcal{J}$ *such that* $V^J \neq 0$.

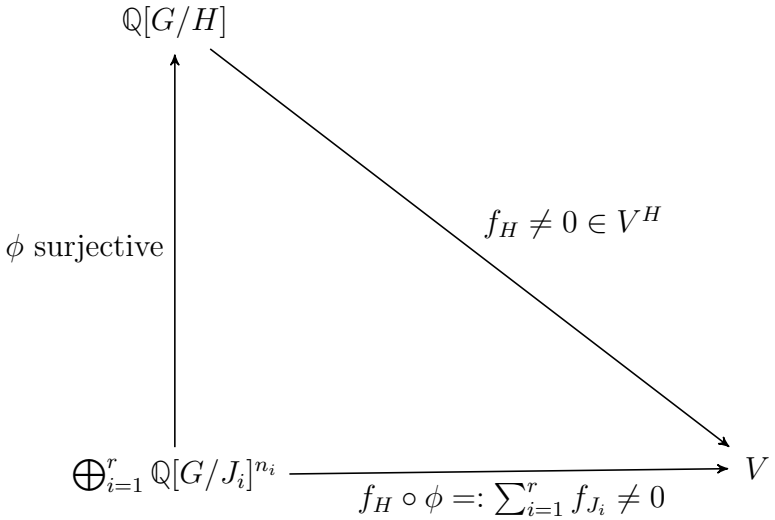
6. *The norm element* N_H *is in the two sided ideal* $\langle N_J : J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$.

7. *The group* G *admits a generalised norm relation over* $\mathbb{Q}$ *with respect to* H *and* $\mathcal{J}$.

Proof.

- $1 \Rightarrow 3$. We know there is an isomorphism of R-modules between V^H and $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/H], V)$.

  Likewise, for all i, V^{J_i} is isomorphic to $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/J_i], V)$. Suppose 1, then we have the following diagram, where f_H is an element of V^H seen as an element of $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/H], V)$, and the f_{J_i} are elements of $\mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/J_i], V)$.



So $\sum_{i=1}^r f_{J_i}$ is non zero, so at least one of the f_{J_i} is non zero, hence the conclusion.

- $2 \Leftrightarrow 3$. Let V_i be the simple $\mathbb{Q}[G]$-module (unique up to isomorphism) such that $e_i V_i \neq 0$ then $\mathbb{Q}[G]/(1-e_i)$ acts faithfully on V_i. So $e_i N_H = 0$ if and only if $N_H \cdot V_i = 0$, so if and only if $(\frac{1}{|H|} N_H) \cdot V_i = 0$ which is equivalent to $V_i^H = 0$.

- $3 \Rightarrow 1$. Suppose 3, then let $V = \mathbb{Q}[G/H]$. Then V is a $\mathbb{Q}[G]$-module, and V can decompose as $V = \bigoplus_k V_k$, where the V_k are simple. For all k, let $f_k \colon V \to V_k$ the projection. It can be seen as an element of V_k^H by 2.1. Then there exists a non zero element of $V_k^{J_i}$ for some i, by lemma 3. So we have a nonzero morphism $\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]^{n_i} \to V_k$ so it is surjective because V_k is simple. Hence the conclusion by putting together all the k.

- $3 \Rightarrow 4$. Suppose 3, let W be a simple $\overline{\mathbb{Q}}[G]$-module. W is isomorphic to a submodule of $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, with V a simple $\mathbb{Q}[G]$-module. Then we have $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^k W_j$, where the W_j are simple $\overline{\mathbb{Q}}[G]$-modules. So W is isomorphic to one of the W_j. What's more, the W_j are pairwise Galois conjugate, so $\dim_{\overline{\mathbb{Q}}} W_j^H = \dim_{\overline{\mathbb{Q}}} W_1^H$ for all j. So if W^H is non zero, V^H is also non zero. So, by 3, there exists $J \in \mathcal{J}$ such that V^J is non zero. Hence $W^J \neq 0$.

- $4 \Rightarrow 5$. The simple $\mathbb{C}[G]$-modules are exactly the $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$, where V is a simple $\overline{\mathbb{Q}}[G]$-module. The conclusion follows.

- $5 \Rightarrow 4$. Suppose 5, let V a simple $\overline{\mathbb{Q}}[G]$-module. If $V^H \neq 0$, then $(V \otimes_{\overline{\mathbb{Q}}} \mathbb{C})^H \neq 0$. So, by 4., there exists $J \in \mathcal{J}$ such that $(V \otimes_{\overline{\mathbb{Q}}} \mathbb{C})^J \neq 0$. Hence $V^J \neq 0$.

- $4 \Rightarrow 3$. Suppose 4, let V a simple $\mathbb{Q}[G]$-module such that $V^H \neq 0$. Consider $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^{k} W_j$. We know that $W_j^H \neq 0$ for all j. So there exists $J \in \mathcal{J}$ such that $W_1^J \neq 0$. So $V^J \neq 0$.

- $3 \Leftrightarrow 6$. Let I be a two-sided ideal of $\mathbb{Q}[G]$. We have $I = \sum_{i=1}^{r} e_i I$. What's more, there is an isomorphic projection of $e_i I$ in a two sided ideal of the algebra $\mathbb{Q}[G]/(1-e_i)$, which is simple. So $e_i I$ is either zero, or $e_i \mathbb{Q}[G]$. By applying this result to $I = \langle N_J : J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$, we find the equivalence.

- $6 \Leftrightarrow 7$. This equivalence comes directly from the definition of a generalised norm relation.

□

We will want to apply the concept of generalised norm relations to solve some algorithmic problem in the context of number fields. For convenience, let us define a notion of generalised norm relations between number fields:

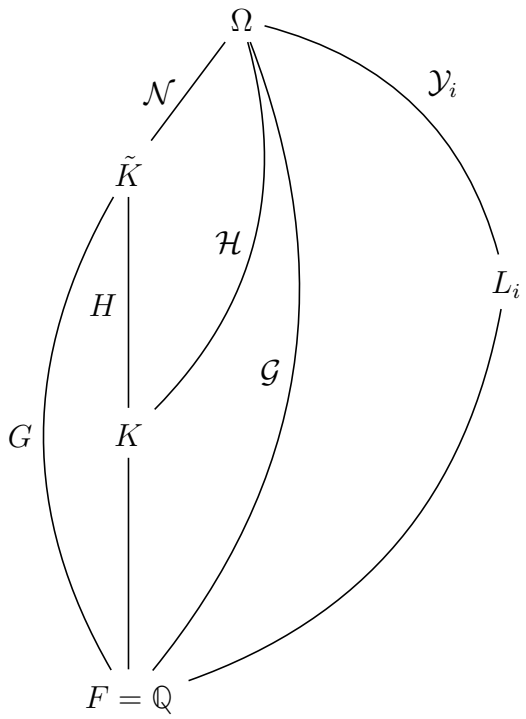
Definition 4.15. Let $K, L_1, \cdots, L_\ell$ be number fields. Let Ω be a Galois extension of $\mathbb{Q}$ containing K and all the L_i, and let $\mathcal{G}$ its Galois group. We denote by $\mathcal{H}$ the subgroup of $\mathcal{G}$ fixing K, and by $\mathcal{Y}_i$ the ones fixing the L_i respectively. Then we say there is a generalised norm relation between K and the L_i if there is a generalised norm relation over $\mathbb{Q}$ with respect to $\mathcal{H}$ and the $\mathcal{Y}_i$.

Example 4.16. There is a generalised norm relation between the number field K defined by $f(x) = x^6 - 6x^4 + 9x^2 + 23$ and the number fields L_1, L_2 respectively defined by $g_1(x) = x^3 - 9x - 27$ and $g_2(x) = x^2 + 207$. Indeed, $K/\mathbb{Q}$ is a Galois extension of Galois group $G = S_3$, and L_1, L_2 are the subgroups fixed respectively by $\mathcal{Y}_1 = \langle (2,3) \rangle$ and $\mathcal{Y}_2 = \langle (1,2,3) \rangle$, and G admits a classical norm relation over $\mathbb{Q}$ with respect to $\mathcal{J} = \{\mathcal{Y}_1, \mathcal{Y}_2\}$ (see example 4.3), which can be seen as a generalised norm relation with respect to $\mathcal{H} = 1$ and $\mathcal{J}$.

Suppose there is a generalised norm relation between some number fields K and $L_1, \cdots, L_\ell$. In chapter 5, we will describe some algorithms to compute the class group or the group of S-units of K inductively, by reducing the problem to the same computation in the auxiliary fields $L_1, \cdots, L_\ell$. But this method is only interesting when the L_i are of degree smaller than the degree of G.

Definition 4.17. We will say a generalised norm relation between a number field K and some other number fields $L_1, \cdots, L_\ell$ is *useful* if the degrees of all the L_i are smaller than the degree of K. Similarly, if G admits a generalised norm relation over $\mathbb{Q}$ with respect to $H < G$ and a set of subgroups $\mathcal{J} = \{J_1, \cdots, J_\ell\}$, then we will say the relation is *useful* if the orders of all the J_i are larger than the order of H.

Theorem 4.18. *Suppose there is a generalised norm relation between a number field K and some L_i that are not necessarily contained in the Galois closure $\tilde{K}$ of K. Denote by Ω a Galois extension of $\mathbb{Q}$ of Galois group $\mathcal{G}$ containing $\tilde{K}$ and all the L_i. Let $\mathcal{N}, \mathcal{H}$ and the $\mathcal{Y}_i$ be the subgroups of $\mathcal{G}$ fixing $\tilde{K}, K$ and the L_i as in the diagram below.*



Then there is also a generalized norm relation between K and some M_i that are contained in $\tilde{K}$.

Proof. We have $\mathcal{N} = \bigcap_{g\in\mathcal{G}} g\mathcal{H}g^{-1}$. What's more, $\mathcal{N}$ is normal in $\mathcal{G}$ and $G = \mathcal{G}/\mathcal{N}$ and $H = \mathcal{H}/\mathcal{N}$. Since there is a generalised norm relation between the L_i and K, there exists a relation of the form $N_{\mathcal{H}} = \sum_i a_i N_{\mathcal{Y}_i} b_i \in \mathbb{Q}[G]$. Consider the projection

$$\pi\colon \mathbb{Q}[\mathcal{G}] \to \mathbb{Q}[\mathcal{G}/\mathcal{N}] = \mathbb{Q}[G], \sum_i \lambda_i g_i \mapsto \sum_i \lambda_i \overline{g}_i.$$

This map π is a surjective morphism of $\mathbb{Q}$-algebras. Composing the relation by π we get

$$\pi(N_{\mathcal{H}}) = |\mathcal{N}|N_H = \sum_i \pi(a_i)\pi(N_{\mathcal{Y}_i})\pi(b_i)$$

and

$$\pi(N_{\mathcal{Y}_i}) = |\mathcal{N} \cap \mathcal{Y}_i| N_{\mathcal{Y}_i/(\mathcal{N}\cap\mathcal{Y}_i)}.$$

So there is a generalised norm relation between K and the $M_i = \Omega^{\mathcal{Y}_i/\mathcal{N}} \subseteq \tilde{K}$. Note that if for some i, $\mathcal{Y}_i \subset \mathcal{N}$, then $\tilde{K} \subset L_i$, and therefore the relation was not useful.

□

Theorem 4.18 will be helpful in particular when we will want a method to look for all generalised norm relations involving a number field (see section 4.5): we know we will only have to look at subfields of the Galois closure.

Now, in the rest of the section, let us prove some characterizations of generalised norm relations, with Hecke operators.

Lemma 4.19. *Let V be a $R[G]$-module, with $\frac{1}{|H|} \in R$, and $\phi\colon V \to R[G/H]$ a surjective morphism of $R[G]$-modules. There exists a preimage of $1H$ by ϕ that is in V^H.*

Proof. Since ϕ is surjective, there exists $v \in V$ such that $\phi(v) = 1H$. Now consider the element $v' = \frac{1}{|H|}\sum_{h\in H} h \cdot v$.

Then, clearly, $v' \in V^H$, and $\phi(v') = \frac{1}{|H|}\sum_{h\in H}\phi(h\cdot v) = \frac{1}{|H|}\sum_{h\in H} h \cdot \phi(v) = \frac{1}{|H|}\sum_{h\in H} h\cdot 1H = 1H$.

□

Proposition 4.20. *We have a generalised norm relation, given by a surjection*

$$\phi\colon \bigoplus_i \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H],$$

(where the J_i are not necessarily distinct) if and only if there exist $\mu_{i,h}$ and $\lambda_{i,k}$ elements of $\mathbb{Q}$, and $\delta_{i,h}$ and $g_{i,k}$ elements of G such that

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i,$$

where the equality takes place in in $(\bigoplus_i \mathbb{Q}[G/J_i])^H$.

Proof. Suppose there exists $\phi\colon \bigoplus_i \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$ surjective. Let us consider $\bigoplus_i \sum_k \lambda_{i,k} g_{i,k} J_i$ a preimage of $1H$. By lemma 4.19, we can suppose $\bigoplus_i \sum_k \lambda_{i,k} g_{i,k} J_i$ is in $(\bigoplus_i \mathbb{Q}[G/J_i])^H$

Let us write $\phi = \bigoplus_i \phi_i$ with $\phi_i\colon \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$. Then we have

$$1H = \sum_i \phi_i(\sum_k \lambda_{i,k} g_{i,k} J_i).$$

Then, by writing $\phi_i = \sum_h \mu_h T_{J_i \delta_{i,h} H} = T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H}$, we can obtain

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i$$

□

Considering the action of Hecke operators on the module of S-units, we then obtain the following corollary:

Corollary 4.21. *Let S be set of non-zero prime ideals of $\mathcal{O}_K$. If there is a generalised norm relation between K and the auxiliary fields K_i, then the map*

$$\Phi\colon \bigoplus_{i=1}^{\ell} \bigoplus_{C \in \mathrm{Compos}(K_i, K)} \mathcal{O}_{K_j,S}^{\times} \to \mathcal{O}_{K,S}^{\times}$$

$$\bigoplus_{i=1}^{\ell} \bigoplus_{C \in \mathrm{Compos}(K_i, K)} \mathfrak{a}_{i,C} \mapsto \sum_{i=1}^{\ell} \sum_{C \in \mathrm{Compos}(K_i, K)} C \cdot \mathfrak{a}_{i,C}$$

has an image of finite index.

Theorem 4.22. *If $L_1, \cdots, L_\ell$ are number fields, defined by the polynomials $f_1, \cdots, f_\ell$, and if we denote by R_i the set of roots of f_i in $\mathbb{C}$, then $K = \mathbb{Q}(\alpha)$ admits a* generalised norm relation with respect to $L_1, \cdots, L_\ell$, *if and only if there is a relation of the form*

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in Compo(K, L_i)} \sum_{\beta \in R_i} a_{i,C,\beta} C \cdot \beta$$

where the coefficients $a_{i,C,\beta}$ are in $\mathbb{Q}$.

Proof. This theorem is a rephrasing of proposition 4.20 using the isomorphisms of part 2.2. □

4.3 Optimal coefficient

In [7], the authors define the notion of denominator of a norm relation in the following way:

Definition 4.23 (Definition 2.15 of [7])**.**

- Let G be a finite group, and let $\mathcal{H}$ be a set of non-trivial subgroups of G. Then the *optimal denominator $d(\mathcal{H})$ relative to $\mathcal{H}$* is the unique non negative integer such that

$$d(\mathcal{H})\mathbb{Z} = \mathbb{Z} \cap \langle N_H | H \in \mathcal{H} \rangle_{\mathbb{Z}[G]}.$$

- Let $1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$ be a classical norm relation with $H_i \in \mathcal{H}$, then the least common denominator of the coefficients of the a_i and b_i is called the **denominator** of the relation.

That way, given a finite group G and $\mathcal{H}$ a set of non-trivial subgroups, there exists a norm relation over $\mathbb{Q}$ if and only if $d(\mathcal{H}) \neq 0$. In that case, $d(\mathcal{H})$ divides the denominator of the relation, and there exists a relation with denominator $d(\mathcal{H})$.

Then, in [7, Theorem 2.20], they prove that if $d(\mathcal{H})$ is positive, then it divides $|G|$, which is later useful to study the time complexity of some algorithms (see [7, Theorem 4.18]).

While generalizing the definition of optimal denominator for the context of generalised norm relations has some interest (see section 4.4), we will

prefer to define another similar notion, that fits more naturally with the Hecke operators point of view of generalised norm relations.

Definition 4.24. Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. If there is a norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}$, we define the *optimal coefficient* $c(\mathcal{J}, H)$ to be the smallest positive integer such that there exists an injective morphism of $\mathbb{Z}[G]$-module $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$ with $n_i \in \mathbb{Z}_{\geq 0}$ for all i, and a morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ such that $\phi \circ \psi = c(\mathcal{J}, H) \cdot \mathrm{id}$.

To prove that the optimal coefficient is well defined, we start by giving a more general proposition.

Proposition 4.25. *Let Γ be a finite group, and let $\mathcal{H}_1, \cdots, \mathcal{H}_r, \mathcal{Y}_1, \cdots, \mathcal{Y}_s$ be some subgroups of Γ. Let $M = \bigoplus_i \mathbb{Q}[\Gamma/\mathcal{H}_i]$ and $N = \bigoplus_j \mathbb{Q}[\Gamma/\mathcal{Y}_j]$.*

1. *If there exists a surjective morphism of $\mathbb{Q}[\Gamma]$-modules*

$$\Phi\colon M \to N,$$

then there is an injective morphism of $\mathbb{Q}[\Gamma]$-modules

$$\Psi\colon N \to M$$

such that $\Psi \circ \Phi = \mathrm{id}_N$.

2. *Similarly, If there exists an injective morphism of $\mathbb{Q}[\Gamma]$-modules*

$$\Psi\colon N \to M,$$

then there is a surjective morphism of $\mathbb{Q}[\Gamma]$-modules

$$\Phi\colon M \to N$$

such that $\Psi \circ \Phi = \mathrm{id}_N$.

Proof. Let us prove 1. Since $\mathbb{Q}[\Gamma]$ is a semi-simple algebra, this means we can write the decomposition in simple modules. Up to isomorphism, $N = \bigoplus_{j=1}^n W_j$ and $M = \bigoplus_{j=1}^n W_j \oplus \bigoplus_{k=1}^m V_k$, where the W_j and the V_k are simple, and Φ is the projection. Then Ψ is the natural injection $\bigoplus_{j=1}^n W_j \to \bigoplus_{j=1}^n W_j \oplus \bigoplus_{k=1}^m V_k$.

The proof of 2 is similar.

□

Proposition 4.26. *With the notations of the definition above, $c(\mathcal{J}, H)$ is well defined.*

Proof. Since there is a norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}$, there is a surjective $\mathbb{Q}[G]$-module morphism $\bigoplus_i \mathbb{Q}[G/J_i]^{n_i} \to \mathbb{Q}[G/H]$.

Consider an injection Ψ as in proposition 4.25, let c be the LCM of the denominators of all coefficients of all the $\Psi(gH)$ for $gH \in G/H$. Then $c \cdot \Psi$ induces an injective morphism of $\mathbb{Z}[G]$-modules $\mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$. With the same reasoning, we can construct a morphism of $\mathbb{Z}[G]$-modules $\Phi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ whose image is of finite index in $\mathbb{Z}[G/H]$. And then $\Psi \circ \Phi$ is a multiple of $\mathrm{id}_{\mathbb{Z}[G/H]}$. Hence the conclusion.

□

We now prove that the optimal coefficient is also smallest for the divisibility relation.

Proposition 4.27. *If c is a positive integer such that there exists ϕ and ψ as in definition 4.24 such that $\phi \circ \psi = c \cdot \mathrm{id}_{\mathbb{Z}[G/H]}$, then $c(\mathcal{J}, H) \mid c$.*

Proof. Consider the group

$$E = \langle t_2 \circ t_1 | n_i \in \mathbb{Z}_{\geq 1} \forall i, t_1 \in A_{1,(n_i)_i}, t_2 \in A_{2,(n_i)_i} \rangle_{\mathbb{Z}} \cap \mathbb{Z}\,\mathrm{id}_{\mathbb{Z}[G/H]},$$

where

$$A_{1,(n_i)_i} = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \bigoplus_i \mathbb{Z}[G/J_i]^{n_i})$$

and

$$A_{2,(n_i)_i} = \mathrm{Hom}_{\mathbb{Z}[G]}(\bigoplus_i \mathbb{Z}[G/J_i]^{n_i}, \mathbb{Z}[G/H]).$$

Then E is a subgroup of $\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H])$ contained in $\mathbb{Z}\,\mathrm{id}$, so E is of the form $a\mathbb{Z}\,\mathrm{id}$ with $a \in \mathbb{Z}_{\geq 0}$. And by definition, $a = c(\mathcal{J}, H)$. By construction, $c \cdot \mathrm{id}$ is in E, hence $c(\mathcal{J}, H) \mid c$.

□

Theorem 4.28. *With the notations of Definition 4.24, we have $c(\mathcal{J}, H) \mid |G|^2$.*

Proof. Let p be a prime number. Let $\mathcal{O}$ be a maximal order of $\mathbb{Q}_p[G]$ containing $\mathbb{Z}_p[G]$. By [16, 27.1, proposition] we have $\mathcal{O} \subset \frac{1}{|G|}\mathbb{Z}_p[G]$.

Consider $M_H = \mathcal{O} \cdot \mathbb{Z}_p[G/H] \subset \mathbb{Q}_p[G/H]$. Then M_H is an $\mathcal{O}$-module, and we have $\mathbb{Z}_p[G/H] \subset M_H \subset \frac{1}{|G|}\mathbb{Z}_p[G]$. Similarly, for all i, we write $M_{J_i} = \mathcal{O} \cdot \mathbb{Z}_p[G/J_i]$.

Let $e_1, \cdots, e_r$ be central primitive idempotents of $\mathbb{Q}_p[G]$ contained in $\mathcal{O}$, which exist since $\mathcal{O}$ is a maximal order. For all $1 \leq i \leq r$, there is a isomorphism $\alpha\colon \mathcal{O}/(1-e_i) \to M_n(\Lambda)$, where $\Lambda = \Lambda_i$ is the maximal order of a division algebra D over $\mathbb{Q}_p$ (see [42, theorem 17.3]). And α can be extended to $\mathcal{O}$ with the projection $\mathcal{O} \to \mathcal{O}/(1-e_i)$.

We have $M_n(\Lambda) \subset M_n(D)$ and $M_n(D)$ acts on D^n, which is the only simple $M_n(D)$-module up to isomorphism.

So $e_i M_H \otimes \mathbb{Q}_p \cong D^{na}$ with $a \in \mathbb{Z}_{\geq 1}$, since $e_i M_H \otimes \mathbb{Q}_p$ is a is a $M_n(D)$-module. Similarly, $e_i \bigoplus_i M_{J_i}^{n_i} \otimes \mathbb{Q}_p \cong D^{nb}$, and thus $e_i M_H \cong \Lambda^{na}$ and $e_i \bigoplus_i M_{J_i}^{n_i} \cong \Lambda^{nb}$.

What's more, we have a surjective morphism of $\mathbb{Q}_p[G]$-modules from $e_i \bigoplus_i M_{J_i}^{n_i} \otimes \mathbb{Q}_p = \bigoplus_i \mathbb{Q}_p[G/J_i]$ to $e_i M_H \otimes \mathbb{Q}_p = \mathbb{Q}_p[G/H]$, which means that $a \leq b$.

Let us fix an injective morphism of $\mathcal{O}$-modules $i\colon \Lambda^{na} \to \Lambda^{nb}$. Let s be a surjective morphism of $\mathcal{O}$-modules $\Lambda^{nb} \to \Lambda^{na}$, such that for all $x \in \Lambda^{na}$, $s \circ i(x) = x$.

That gives us, an injection of $\mathcal{O}$-modules $\tilde{\psi}\colon e_i M_H \to e_i \bigoplus_i M_{J_i}^{n_i}$, and a surjection $\tilde{\phi}\colon \bigoplus_i M_{J_i}^{n_i} \to M_H$.

Let us denote $\psi = |G|\tilde{\psi}$ and $\phi = |G|\tilde{\phi}$. That way, ψ induces an injective morphism $\mathbb{Z}_p[G/H] \to \bigoplus_i \mathbb{Z}_p[G/J_i]^{n_i}$ and ϕ a morphism $\bigoplus_i \mathbb{Z}_p[G/J_i]^{n_i} \to \mathbb{Z}_p[G/H]$ with image of finite index in $\mathbb{Z}_p[G/H]$. And we have $\phi \circ \psi = |G|^2 \,\mathrm{id}$.

By doing the same reasoning over all e_i and by putting together every prime p, we obtain the claimed result.

□

4.4 Norm relation over finite fields

In this thesis, we will mostly apply generalised norm relations to compute invariants of number fields (class groups or S-units groups, see chapter 5). This is why we mainly study generalised norm relations over $\mathbb{Q}$ or over $\mathbb{Z}$. However, for future research, it would be interesting to study generalised norm relations over finite fields, and this is what we begin to do in this section.

For this context, we find it more convenient to use a straightforward gen-

eralisation of optimal denominator (see definition 4.23 or [7, definition 2.15]) rather than the notion of optimal coefficient.

Definition 4.29. Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. We define the optimal denominator $d(\mathcal{J}, H)$ to be the unique non negative integer such that

$$d(\mathcal{J}, H)\mathbb{Z}N_H = \mathbb{Z}N_H \cap \langle N_{J_i} | 1 \leq i \leq \ell \rangle_{\mathbb{Z}[G]}.$$

That way, we have $d(\mathcal{J}, H) > 0$ if and only if there exists a generalised norm relation.

We also have a way to control the size of the optimal denominator:

Proposition 4.30. *Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. If $d(\mathcal{J}, H) > 0$, then $d(\mathcal{J}, H)$ divides $|G|^3$.*

The proof is very similar to that of theorem 4.28.

Proposition 4.31. *Let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. Let J be the Jacobson radical of $\mathbb{F}_p[G]$. Then the following are equivalent:*

1. *$p \nmid d(\mathcal{J}, H)$*
2. *There exists an extended norm relation over $\mathbb{F}_p$ with respect to $\mathcal{J}$ and H.*
3. *There exists an identity in $\mathbb{F}_p[G]/J$ of the form $N_H = \sum_i a_i N_{J_i} b_i$, with $a_i, b_i \in \mathbb{F}_p[G]/J$.*
4. *For every simple $\mathbb{F}_p[G]$ module V, if $N_H V \neq 0$, there exists $J_i \in \mathcal{J}$ such that $N_{J_i} V \neq 0$.*
5. *For every simple $\overline{\mathbb{F}_p}[G]$ module V, if $N_H V \neq 0$, there exists $J_i \in \mathcal{J}$ such that $N_{J_i} V \neq 0$.*

This is an adaptation of [7, proposition 2.18] to generalised norm relations. The proofs are very similar.

- It is clear that 1 implies 2. Conversely, assume that

$$N_H = \sum_i \overline{a_i} N_{J_i} \overline{b_i}$$

is a generalised norm relation over $\mathbb{F}_p$. Pick arbitrary lifts a_i, b_i of $\overline{a_i}, \overline{b_i}$, and let

$$\delta N_H = \sum_i a_i N_{J_i} b_i.$$

We have $N_{\mathbb{Z}[G]/\mathbb{Z}}(\delta) \equiv N_{\mathbb{F}_p[G]/\mathbb{F}_p}(1) \equiv 1 \mod p$, which is nonzero. Therefore the norm is nonzero, the element δ is invertible in $\mathbb{Q}[G]$,and the denominator d of δ^{-1} is coprime to p. Hence the relation

$$dN_H = \sum_i (d\delta^{-1} a_i) N_{J_i} b_i$$

with $d \in \mathbb{Z}$ coprime to p, and $(d\delta^{-1} a_i) \in \mathbb{Z}[G]$. Therefore, $p \nmid d(\mathcal{J}, H)$.

- It is clear that 2 implies 3. Conversely, assume that

$$N_H = \sum_i \overline{a_i} N_{J_i} \overline{b_i}$$

holds in $\mathbb{F}_p[G]/J$. Pick arbitrary lifts $a_i, b_i \in \mathbb{F}_p[G]$ of $\overline{a_i}, \overline{b_i}$, and let

$$\delta N_H = \sum_i a_i N_{J_i} b_i.$$

We have $\delta \equiv 1 \mod J$. Since 1 is invertible and J is a nilpotent two-sided ideal, this implies that δ is invertible. We therefore have the relation

$$N_H = \sum_i \delta^{-1} a_i N_{J_i} b_i$$

in $\mathbb{F}_p[G]$. So 3 implies 2.

- The proof of the equivalence between 3 and 4 is identical to that of proposition 4.14, by considering the central primitive idempotent of the semi-simple algebra $\mathbb{F}_p[G]/J$.

- The proof of the equivalence between 4 and 5 is identical to that of proposition 4.14.

4.5 Looking for generalised norm relations

Given a finite group G and a subgroup H, we do not have a simple criterion to determine whether or not there exists a set of subgroups $\mathcal{J}$ such that G admits a generalised norm relation with respect to H and $\mathcal{J}$. However, if we provide G, H and $\mathcal{J}$, we do have algorithms to check whether or not there is a generalised norm relation.

Therefore, when we only have G and H, we can enumerate all the subgroups of G and add them to a set $\mathcal{J}$ and check when (or if) $\mathcal{J}$ works.

We know we only have to enumerate the subgroups up to conjugacy. Moreover, if we are looking for useful norm relations, then we only have to enumerate the subgroups of G of order larger than the order of H.

Algorithm 4.32.
input: A finite group G, a subgroup H, and set of subgroups $\mathcal{J} = \{J_1, \cdots, J_\ell\}$.
output: A boolean indicating whether there is a generalised norm relation.

- Compute the central primitive idempotent elements $e_1, \cdots, e_r$ of the group algebra $\mathbb{Q}[G]$.
- For all $e \in \{e_1, \cdots, e_r\}$:
  - if $eN_H \neq 0$:
    - compute eN_J for all $J \in \mathcal{J}$,
    - if for some $J \in \mathcal{J}$, we have $eN_J \neq 0$, then skip directely to the next $e \in \{e_1, \cdots, e_r\}$,
    - if for all $J \in \mathcal{J}$, $eN_J = 0$, then return False.
- Return True

The correctness of algorithm 4.32 is an immediate result of 2 in proposition 4.14.

Remark 4.33.

- The software Sagemath ([18]) has a function to directly compute the central primitive idempotent elements of the group algebra $\mathbb{Q}[G]$.

- Suppose we have G and H and we are looking for a set $\mathcal{J}$ of subgroups such that there is a generalised norm relation. Then, rather than enumerating candidate sets $\mathcal{J}$ and using algorithm 4.32 for every candidate, it is more efficient to first compute the list E of every central primitive idempotent elements e_i of $\mathbb{Q}[G]$ such that $e_i N_H \neq 0$, then enumerate every proper subgroups J_j of G larger than H (from the largest to the smallest, and up to conjugacy), and for every J_j, remove from E all the e_i such that $e_i N_{J_j} \neq 0$. When the list E is empty, return the list of all enumerated J_j that decreased the size of E. If E is not empty after the enumeration, then there are no useful generalised norm relations.

We can also adapt algorithm 4.32 to obtain a very similar algorithm, this time based on 5 of proposition 4.14. For all irreducible character χ of G and for all $H < G$, let us denote by $\mathrm{Res}_H \chi$ the restriction to H of χ, and $\mathbb{1}$ the character of the trivial representation. Recall that if χ is the character associated to a simple $\mathbb{C}[G]$-module V, then we have $\dim(V^H) = \langle \mathbb{1}, \mathrm{Res}_H \chi \rangle = \frac{1}{|H|} \sum_{h \in H} \chi(h)$.

The software Sagemath also has a function to directly compute a character table of G.

Algorithm 4.34.
input: A finite group G, a subgroup H, and set of subgroups $\mathcal{J} = \{J_1, \cdots, J_\ell\}$.
output: A boolean indicating whether there is a generalised norm relation.

- Compute all irreducible characters $\chi_1, \cdots, \chi_r$ of G.
- for every $\chi \in \{\chi_1, \cdots, \chi_r\}$:
  - if $\langle \mathbb{1}, \mathrm{Res}_H \chi \rangle_H \neq 0$,
    - compute $\langle \mathbb{1}, \mathrm{Res}_J \chi \rangle_J$ for all $J \in \mathcal{J}$,
    - if for some $J \in \mathcal{J}$, we have $\langle \mathbb{1}, \mathrm{Res}_J \chi \rangle_J \neq 0$, then skip directly to the next $e \in \{e_1, \cdots, e_r\}$,
    - if for all $J \in \mathcal{J}$, $\langle \mathbb{1}, \mathrm{Res}_J \chi \rangle_J = 0$, then return False.
- Return True.

Remark 4.35. A more straightforward method would be to determine whether N_H is in the two sided ideal $\langle N_J | J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$.

According to proposition 4.30, this problem would be equivalent to finding whether $|G|^3 N_H$ is in $\langle N_J | J \in \mathcal{J} \rangle_{\mathbb{Z}[G]}$.

Since

$$\begin{aligned}\langle N_J | J \in \mathcal{J} \rangle_{\mathbb{Z}[G]} &= \langle gN_Jh | J \in \mathcal{J}, (g,h) \in G^2 \rangle_{\mathbb{Z}} \\ &= \langle gN_Jh; J \in \mathcal{J}, g \in G, h \in G/J \rangle_{\mathbb{Z}},\end{aligned}$$

this is a linear system over $\mathbb{Z}$. Note that it is more efficient for computational complexity to view it as a system over $\mathbb{F}_p$ with p a prime number that does not divide $|G|$. However, in practice this method is still much slower than algorithms 4.32 or 4.34, and only works for small examples.

Now suppose that we have a number field K and a family of number fields (K_i). To determine whether there is a generalised norm relation between K and the K_i, we could compute a Galois closure of K and the K_i, and the Galois group, and then apply algorithms 4.32 or 4.34. However, computing a Galois group is very costly.

Using the theorem 4.22, we can find an algorithm that is polynomial in the size of the input, and also determines the coefficients of the relation if it exists.

Algorithm 4.36.

input: A number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields given by the minimal polynomial f of α with $K = \mathbb{Q}(\alpha)$, and the minimal polynomials f_i of the β_i, with $K_i = \mathbb{Q}(\beta_i)$.
output: A boolean indicating whether there is a generalised norm relation, and if so, a formula of the form

$$1H = \sum_i T_{\sum_h \mu_{i,h} J_i \delta_{i,h} H} \sum_k \lambda_{i,k} g_{i,k} J_i$$

in $\mathbb{Z}[G/H]$.

- For all i, list all compositums of K and K_i.

  If $f_i = p_1 \cdots p_r \in K[X]$, then the compositums are the $K[X]/(p_j)$, with ι_K the inclusion, and $\iota_{L_i} \colon \beta_i \mapsto X \mod p_j$.

- For all i, and for all $\sigma \in \mathrm{Hom}(L_i, \mathbb{C})$ and for every compositum $\mathcal{C}$, compute $\mathcal{C} \cdot \sigma \in \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$.

- By linear algebra in $\mathbb{Q}[G/H] = \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$, find a linear combination of these element that equals $1H$ (if such a combination exists).

Theorem 4.37. *This algorithm is correct and its complexity is polynomial in the size of the input.*

Proof. The correctness of the algorithm follows from theorem 4.22.

For the complexity, we have to check that every step of the algorithm works in polynomial time.

- Listing all the compositums boils down to a problem of factorisation of polynomials in $K[X]$, which is polynomial thanks to the LLL algorithm (see [33]). The number of compositums to list is at most $\sum_{j=1}^{\ell} \deg(K_j)$.
- Given a complex embedding σ of a field K_j, and a compositum $\mathcal{C}$ of K and K_j, computing $\mathcal{C} \cdot \sigma$ is in $\mathcal{O}(\deg(K_j) \times \deg(K))$. And the number of times such a computation occurs is at most $\sum_j \deg(K_j) \times |\operatorname{Compos}(K, K_j)|$. What's more, the size of $\mathcal{C} \cdot \sigma$ is polynomial in the size of the input.

□

4.6 Comparing classical and generalised norm relations

In this section, we will discuss the relevance of studying generalised norm relation instead of classical norm relation.

Suppose we have a number field K, Galois over $\mathbb{Q}$, of Galois group G, and some K^{H_i} where G admits a classical norm relation over $\mathbb{Q}$ with respect to the H_i. Then, the article [7] describes an algorithm to compute the class group of K by induction, by reducing the problem to the computation of the class groups of the K^{H_i}.

Similarly, if we have a number field $\tilde{K}$, Galois over $\mathbb{Q}$, of Galois group G, a number field $K = \tilde{K}^H$ and some $\tilde{K}^{J_i}$ where G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and the J_i, then we will see in chapter 5 some algorithm to compute the class group of K by induction, by reducing the problem to the computation of the class groups of the $\tilde{K}^{J_i}$.

What's more, a generalised norm relation of a group G with respect to $H < G$ and a set of subgroups $\mathcal{J}$ can come directly from a classical norm relation in G (see fact 4.38) or in a quotient of G (see proposition 4.40).

Therefore, in order to justify the relevance of our generalisation of norm relations, we need to produce some examples where the methods in chapter 5 allows us to compute the class groups more efficiently than classical norm relations.

Fact 4.38. If there is a classical relation $1 = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$ for some finite group G and some set $\mathcal{J}$ of subgroups of G, then for any subgroup H, we can construct a generalised norm relation with respect to H and $\mathcal{J}$, simply by multiplying both sides of the classical relation by N_H.

Example 4.39. The alternating group $G = A_4$ admits a classical norm relation over $\mathbb{Q}$ with respect to $\mathcal{H} = \{C_2 \times C_2, C_3\}$. Indeed, if we see A_4 as a subgroup of the group of permutations of the set $\{1,2,3,4\}$, let $J_1 = \langle (1,2),(3,4)\rangle \simeq C_2 \times C_2$, and $J_2 = \langle (2,3,4)\rangle \simeq C_3$. Then we have the relation

$$\begin{aligned} 4 \cdot 1_G = {} & 1_G \cdot N_{J_1} \cdot (2(1,2)(3,4) + (1,2,3) + (1,4,2)) \\ & + 1_G \cdot N_{J_2} \cdot ((2,3,4) - (1,4,2)) \\ & - (1,2)(3,4) \cdot N_{J_2} \cdot ((2,3,4) + 2(1,4,2) + (1,3)(2,4)) \\ & + (1,2,3) \cdot N_{J_2} \cdot ((1,3)(2,4) - (1,4,2)). \end{aligned}$$

Then, let us take $H = \langle (1,2)\rangle \simeq C_2$. By multiplying both sides of this relation by N_H (either on the right or on the left), we get a generalised norm relation with respect to H and $\{J_1, J_2\}$. And this new relation is still useful, since H is of order lower than the orders of J_1 and J_2.

Therefore, if $\tilde{K}$ is a number field, Galois over $\mathbb{Q}$, of Galois group G, and if we have $K = \tilde{K}^H$, $K_1 = \tilde{K}^{J_1}$ and $K_2 = \tilde{K}^{J_2}$, then we will be able to compute the class group of the field K, of degree 6, by reducing the problem to the fields K_1 and K_2, of degree respectively 3 and 4. But the same result could have been obtained using only classical norm relations.

Proposition 4.40. *Let G be a finite group, $H, J_1, \cdots, J_\ell$ subgroups of G. Let N be a normal subgroup of G contained in H. Denote by π the projection from G to G/N. Then G admits a generalised norm relation with respect to H and $J_1, \cdots, J_\ell$ if and only if G/N admits a generalised norm relation with respect to $\pi(H)$ and $\pi(J_1), \cdots, \pi(J_\ell)$.*

Proof. Suppose G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and $J_1, \cdots, J_\ell$, of the form $N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$.

Let $\Pi\colon \mathbb{Q}[G] \to \mathbb{Q}[G/N], \sum_i \lambda_i g_i \mapsto \sum_i \lambda_i \pi(g_i)$. Then Π is a surjective morphism of $\mathbb{Q}[G]$-modules. And we have $\Pi(N_H) = |N| N_{H/N}$, and $\Pi(N_{Ji}) =$

$|N\cap J_i|N_{J_i/(N\cap J_i)}$. Then, if we compose the relation by Π, we get a generalised norm relation of G/N with respect to $\pi(H)$ and $\pi(J_1),\cdots,\pi(J_\ell)$.

Now suppose G/N admits a generalised norm relation with respect to $\pi(H)$ and $\pi(J_1),\cdots,\pi(J_\ell)$. So there is a surjective morphism

$$\phi\colon \bigoplus_{i=1}^{\ell} \mathbb{Q}[\pi(G)/\pi(J_i)] \to \mathbb{Q}[\pi(G)/\pi(H)].$$

So $\phi\circ\Pi$ is a surjective morphism from $\bigoplus_{i=1}^{\ell}\mathbb{Q}[G/J_i]$ to $\mathbb{Q}[\pi(G)/\pi(H)]$. And since $N\subset H\subset G$, we have $\pi(G)/\pi(H)\simeq G/H$. Thus, we have a surjective morphism from $\bigoplus_{i=1}^{\ell}\mathbb{Q}[G/J_i]$ to $\mathbb{Q}[G/H]$.

□

It is important to note however that some generalised norm relations do not come from a classical norm relation in a subgroup or in a quotient.

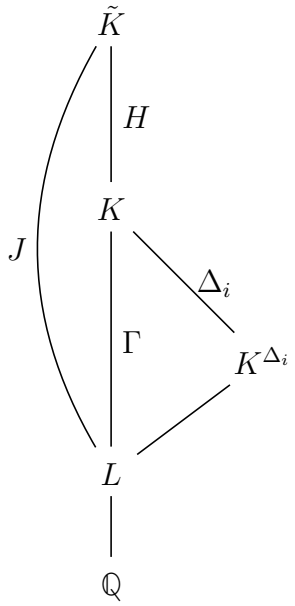
Example 4.41. For example, the symmetric group S_4 admits a norm relation over $\mathbb{Q}$ with respect to $H=C_2\times C_2$, and $\mathcal{J}=\{D_8,S_3\}$ (see example 4.13).

This generalised norm relation does not come from a classical norm relation because we can check that S_4 does not have a norm relation with respect to $\mathcal{J}$. It does not come from a quotient either because the largest normal subgroup of S_4 contained in H is trivial. One can check that it is not a linear combination of classical norm relations in G and in subquotients of G either.

See the appendix for more examples of generalised norm relations that do not come from classical norm relations, and that are more useful than classical norm relations, in a sense that we will define.

However, even when a generalised norm relation in $\mathbb{Q}[G]$ does not come from a classical norm relation in a quotient of G, it can still come from a classical norm relation in a quotient of a subgroup of G.

Indeed, let K be a non Galois extension of $\mathbb{Q}$. Denote by $\tilde{K}$ its Galois closure, G its Galois group and $H<G$ such that $K=\tilde{K}^H$. Suppose there is a subfield L such that $L\subset K\subset\tilde{K}$. Denote by J the subgroup of G such that $\tilde{K}^J=L$. Suppose also that H is normal in J, and $\Gamma=J/H$ admits a classical norm relation with respect to some subgroups Δ_i, as in the figure below.



Then, by proposition 4.40, since there is a classical norm relation in $\mathbb{Q}[\Gamma]$, J admits a generalised norm relation with respect to H and some lifts of the Δ_i, which can be seen as a relation in $\mathbb{Q}[G]$ since $J < G$.

Example 4.42. Let $G = \mathrm{GL}(2,3)$, and $H = C_3$. Then G admits a generalised norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J} = \{S_3, C_6\}$.

However, H is normal in $D_{12} < G$, and there is a classical norm relation in $D_{12}/H \simeq C_2 \times C_2$. We can check that this relation gives (by proposition 4.40) a generalised norm relation of D_{12} over $\mathbb{Q}$ with respect to $\mathcal{J} = \{S_3, C_6\}$, which in turn causes the relation with G, by fact 4.38.

Note also that if G admits a generalised normed relation with respect to a subgroup H and some auxiliary fields, then if H' is another subgroup containing H, then there is also a generalised norm relation with respect to H'. That means that if a field K admits a generalised norm relation with respect to some auxiliary fields L_i, then so do all of its subfields. The following algorithm is useful to find examples where generalised norm relation allow us to compute class groups more efficiently than classical norm relations in any subgroups or quotients.

Algorithm 4.43. input: A finite group G.

output: For all subgroup H of G, the smallest $n \in \mathbb{Z}$ such that for all Galois extension $\tilde{K}/\mathbb{Q}$, the class group of $\tilde{K}^H$ can be computed from the class groups of fields of degree less than n using classical norm relations.

- $L_J \leftarrow$ All subgroups of G up to conjugation
- $M \leftarrow$ List of the $\frac{|G|}{|J|}$ for all J in L_J. *The entries of M represent the degrees of the $\tilde{K}^J$. The goal will be to explore all classical norm relations in all quotients of G and update the entries of M to represent the maximum degree of the fields one has to study in order to compute the class group of $\tilde{K}^J$.*
- $M_2 \leftarrow$ An empty list
- WHILE $M_2 \neq M$
  - $M_2 \leftarrow M$
  - FOR i from 1 to $\#L_J$
    - $H \leftarrow L_J[i]$
    - FOR j from $i+1$ to $\#L_J$
      - $J \leftarrow L_J[j]$
      - Check if H is conjugate to a normal subgroup of J. If not, go directly to the next J.
      - Look for a classical norm relation in J/H that minimizes the entries of M corresponding to the subgroups involved.
      - If such a relation is found, update the entries of M accordingly. The entry corresponding to $\tilde{K}^H$ but also those corresponding to its subfields or all the fields isomorphic to those.

Example 4.44. Let $G = C_3 \times \mathrm{PSL}(3,2)$, and $H = S_3 < G$, (up to conjugacy, there is only one copy of S_3 in G). Suppose we have $\tilde{K}$ a Galois extension of $\mathbb{Q}$ of Galois group G. Then $K = \tilde{K}^H$ is a field of degree 84. To compute the class group of K, we can verify that there are no classical norm relations in any quotients or subgroups of G that allows us to recursively reduce the problem to fields of degree less than 84. However, there exists a generalised norm relation that allows us to reduce the problem to four fields of respective degree 24, 21, 8 and 3. Moreover, this generalised norm relation does not come from a subgroup or from a quotient of G.

Remark 4.45. As explained in [7, theorem 2.11], the groups that do not admit classical norm relations are the ones with a fixed point free unitary representation. In all the examples that we enumerated (see appendix), we could not find any generalised norm relations in these groups either, except the ones coming from classical norm relations in quotients. We do not know if this is true in general or if counterexamples are simply larger.

In the rest of this section, we will see that if we have an example of a useful generalised norm relation for a finite group G, we can build infinitely many other examples, simply by taking the same relation in $C_p \times G$, for any prime p that does not divide $|G|$.

Definition 4.46. Let G be a group that admits a generalised norm relation with respect to $H < G$ and a set a subgroups $\mathcal{J} = \{J_1 \cdots J_\ell\}$. We say that the relation is *optimal* if it is a relation that maximizes the quotient $\frac{|J_i|}{|H|}$, where J_i is the smallest group in $\mathcal{J}$.

Remark 4.47. With the notations of the previous definition, if $\tilde{K}/\mathbb{Q}$ is a Galois extension of Galois group G, then the quotient $\frac{|J_i|}{|H|}$ is the quotient of the degree of $\tilde{K}^H$ by the degree of $\tilde{K}^{J_i}$.

Lemma 4.48. *For all subgroup K' of G', either K' is of the form $1 \times K$ with $K < G$, or it is of the form $C_p \times K$ with $K < G$.*

Proof. Suppose K' contains an element $i \times g \in G' = C_p \times G$ with $i \neq 1$. Let n be the order of g in G. Then, since $\gcd(n, p) = 1$, the subgroup K' contains all the $(kn)i \times 1_G$ with k in $\mathbb{Z}_{>0}$. So $C_p \times 1_G$ is contained in G'. So it is easy to check that the projection of K' on G is indeed a subgroup of G. □

Proposition 4.49. *Let G be a group that admits a generalised norm relation with respect to $H < G$ and a set a subgroups $\mathcal{J} = \{J_1 \cdots J_\ell\}$. Suppose this generalised norm relation is optimal. Let p be a prime number that does not divide $|G|$. Then $C_p \times G$ admits an optimal generalised norm relation with respect to $1 \times H$ and $\mathcal{J}_2 = \{1 \times J_1, \cdots, 1 \times J_\ell\}$.*

Proof. Let $G' = C_p \times G$. Let ρ' be an irreducible representation of G'. Then $\rho' = \chi \otimes \rho$, with χ a character of C_p and ρ an irreducible representation of G.

Let K a subgroup of G. Then $(\rho')^{1\times K} = \rho^K$ and $(\rho')^{C_p \times K} = \chi^{C_p} \otimes \rho^K$. So $(\rho')^{C_p \times K} \neq 0$ if and only if χ is trivial and $\rho^K \neq 0$.

Since G admits a generalised norm relation with respect to H and $\mathcal{J}$, then for every irreducible representation ρ of G, if $\rho^H \neq 0$, there exists $J \in \mathcal{J}$ such that $\rho^J \neq 0$. Let $\rho' = \chi \otimes \rho$ be an irreducible representation of G'. Then it is easy to check that if $(\rho')^{1\times H} \neq 0$, there exists $J \in \mathcal{J}$ such that $(\rho')^{1\times J} \neq 0$. So G' admits a generalised norm relation with respect to $1 \times H$ and $\{1 \times J_1, \cdots, 1 \times J_\ell\}$.

Now let us prove that this relation is optimal. Suppose G has a better generalised norm relation with respect to $\tilde{H}' < G'$ and $\{\tilde{J_1}', \ldots, \tilde{J_m}'\}$. Let $\tilde{H}, \tilde{J}_1, \cdots, \tilde{J}_m < G$ the projections of $\tilde{H}'$ and of the $\tilde{J_i}'$ onto G. Then, using the same method as before, it is easy to check that G admits a generalised norm relation with respect to $\tilde{H}$ and the $\tilde{J}_i$, and that this norm relation is better than the first one, which is a contradiction.

□

Remark 4.50. Similarely, if G is a group that admits an optimal generalised norm relation with respect to $H < G$ and a set a subgroups $\mathcal{J} = \{J_1 \cdots J_\ell\}$, and if G' is another group, such that $|G|$ and $|G'|$ are coprime, then we can show that $G' \times G$ also admits a generalised norm relation with respect to $1 \times H$ and $\mathcal{J}_2 = \{1 \times J_1, \cdots, 1 \times J_\ell\}$. However, this generalised norm relation is not optimal a priori.

5 Computing class groups

The goal of this chapter is to use the properties of generalised norm relations, studied in chapter 4, to obtain inductive methods to compute the class groups of some number fields, in analogy with the methods described in [7] using classical norm relations.

5.1 Algorithms using S-units

In [7], the authors give applications of classical norm relations to obtaining relations between the arithmetic invariants of subfields of a Galois extension of number fields. The arithmetic invariants that we will be interested about here are S-units (see definition 4.8) and class groups.

Note that if we are able to compute the S-units of a number field K for every set S of prime ideals, then we can also compute its class group. This is the content of lemma 5.1 and proposition 5.2.

Lemma 5.1. *Let S be a finite set of prime ideals that generates the class group $\mathrm{Cl}(K)$ of a number field K. Consider the map*

$$\phi : \mathcal{O}_{K,S}^{\times} \to \mathbb{Z}^{|S|}, \alpha \mapsto (v_{\mathfrak{p}}(\alpha))_{\mathfrak{p}\in S}.$$

Then the sequence

$$\mathcal{O}_{K,S}^{\times} \xrightarrow{\phi} \mathbb{Z}^{|S|} \xrightarrow{\psi} \mathrm{Cl}(K) \to 0$$

is exact, where $\psi((v_{\mathfrak{p}})_{\mathfrak{p}\in S}) = \left[\prod_{\mathfrak{p}\in S} \mathfrak{p}^{v_{\mathfrak{p}}}\right]$.

In particular, $\mathrm{Cl}(K)$ is isomorphic to the cokernel of ϕ.

Proposition 5.2. *Let K be a number field. Assume the generalised Riemann hypothesis, then the set $S = \{\mathfrak{p} | N(\mathfrak{p}) \leq 12 \cdot \log(|\Delta_K|)^2\}$ generates the class group of K.*

Proof. See [3]. □

As in section 4.1, let us consider a relation of the form

$$d = \sum_{i=1}^{\ell} a_i N_{H_i} b_i \tag{2}$$

with $H_i < G$, $a_i, b_i \in \mathbb{Z}[G]$ and $d \in \mathbb{Z}_{>0}$.

In [7], the authors describe an algorithm ([7, algorithm 4.16]) such that, if there exists a relation of the form (2), then, on input of

- a number field K,
- an injection $G \to \mathrm{Aut}(K)$,
- a finite G-stable set S of prime ideals of K,
- for each $H \in \mathcal{H}$, a basis of the group of S-units of the subfield fixed by H,

the algorithm returns a $\mathbb{Z}$-basis of the group of S-units of K. What's more, the algorithm is deterministic and of time complexity polynomial in the size of the input. The proof of correctness relies on corollary 4.10.

Therefore, in order to compute the class groups of number fields with generalised norm relations, we will find a generalisation of proposition 4.7 and of corollary 4.10, and then we will use it to derive an algorithm similar to [7, algorithm 4.16].

Let K be a number field, let $\tilde{K}$ be its Galois closure and G the Galois group of $\tilde{K}$. Let $H < G$ be the subgroup such that $K = \tilde{K}^H$. Suppose there is a relation in $\mathbb{Z}[G]$ of the form

$$dN_H = \sum_i a_i N_{J_i} b_i \tag{3}$$

with $J_i < G$, $a_i, b_i \in \mathbb{Z}[G]$ and $d \in \mathbb{Z}_{>0}$ that comes from a generalised norm relation over $\mathbb{Q}$ where we multiply each side by an adequate integer d to get a relation in $\mathbb{Z}[G]$. (The integer d is actually the optimal denominator $d(\mathcal{J}, H)$, see definition 4.29.)

Proposition 5.3. *Let M be a $\mathbb{Z}[G]$-module. If G admits a relation of the form (3), then the exponent of the quotient $M^H/(N_H \cdot (\sum_i a_i M^{J_i}))$ is finite and divides $|H|^2 d$.*

Proof. Let $m \in M^H$. We have $N_H m = |H|m$, so $dN_H m = d|H|m$, hence $(\sum_i a_i N_{J_i} b_i)m = d|H|m$.

But $(\sum_i a_i N_{J_i} b_i)m = \sum_i a_i N_{J_i}(b_i m)$. And for all i, we have $N_{J_i}(b_i m) \in M^{J_i}$. So $d|H|m \in (\sum_i a_i M^{J_i})$.

Multiplying by N_H on the left, we get $d|H|^2 m \in N_H(\sum_i a_i M^{J_i})$. And we have $N_H(\sum_i a_i M^{J_i}) \subset M^H$. Hence the conclusion. □

Corollary 5.4. *With the same hypothesis as proposition 5.3, if we define $\alpha_i = N_H \cdot a_i$ for all i, then the exponent of the quotient*

$$\mathcal{O}^\times_{\tilde{K}^H,S}/((\mathcal{O}^\times_{\tilde{K}^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{\tilde{K}^{J_\ell},S})^{\alpha_\ell})$$

is finite and divides $|H|^2 d$.

In particular, the group $\mathcal{O}^\times_{\tilde{K}^H,S}$ is the $(|H|^2 d)$-saturation of the group

$$((\mathcal{O}^\times_{\tilde{K}^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{\tilde{K}^{J_\ell},S})^{\alpha_\ell}).$$

Proposition 5.5. *Suppose we have a relation of the form (3), and let M be a $\mathbb{Z}[G]$-module. Consider the maps*

$$\phi_M : M^H \to \bigoplus_{i=1}^{\ell} M^{J_i}, m \mapsto (N_{J_i} b_i m)_{1 \leq i \leq l}$$

and

$$\psi_M : \bigoplus_{i=1}^{\ell} M^{J_i} \to M^H, (m_i)_{1 \leq i \leq l} \mapsto N_H(\sum_{i=1}^{\ell} a_i m_i).$$

Then $\phi_M \otimes \mathbb{Q}$ is injective, and $\psi_M \otimes \mathbb{Q}$ is surjective.

Proof. Let us show that $\psi_M \circ \phi_M : M^H \to M^H = d|H| \cdot \mathrm{id}$.

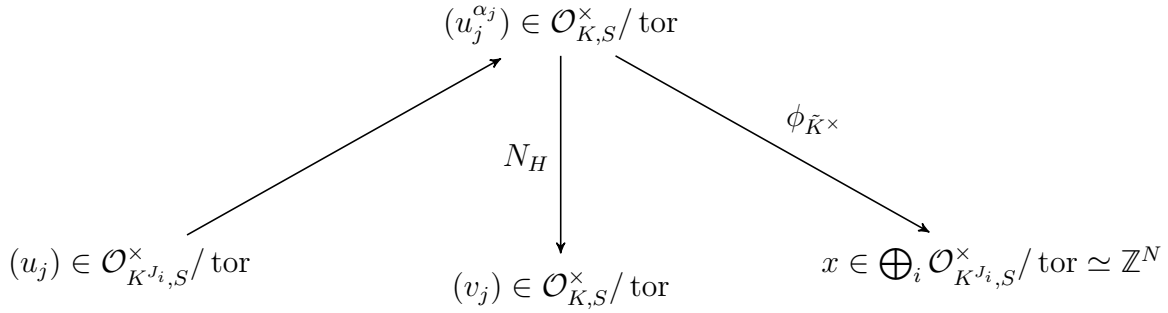
Indeed, let $m \in M^H$. Then $\psi \circ \phi(m) = N_H \sum_{i=1}^{\ell} a_i N_{J_i} b_i m = d N_H^2 m$. But we have $N_H^2 = |H| N_H$, and $N_H m = |H| m$ since $m \in M^H$. So $\psi \circ \phi(m) = d|H|^2 m$.

Hence the conclusion, since $d|H|^2 m$ is invertible in $\mathbb{Q}$. □

In the rest of the section, if V is an abelian group, V/tor will denote the group V modulo its torsion subgroup.

Note that for every i, $\mathcal{O}^\times_{\tilde{K}^{J_i},S}/\operatorname{tor}$ is isomorphic to $\mathbb{Z}^{n_i}$ where n_i is the rank of $\mathcal{O}^\times_{\tilde{K}^{J_i},S}/\operatorname{tor}$.

If we have a basis (u_j) of $\mathcal{O}^\times_{\tilde{K}^{J_i},S}/\operatorname{tor}$ for an integer $1 \leq i \leq \ell$, we can then send it in $\mathcal{O}^\times_{K,S}/\operatorname{tor}$ and also in $\mathbb{Z}^N$, with $N = \sum_{i=1}^{\ell} n_i$ via the maps that are described in the following diagram.



Algorithm 5.6. input: The groups G, H, and J_i for all i, the coefficients of the relation 3, and a basis $(u_{i,j})_j$ of $\mathcal{O}_{K^{J_i},S}^\times/\operatorname{tor}$ for all $1 \leq i \leq \ell$.
output: A basis of $V = ((\mathcal{O}_{K^{J_1},S}^\times)^{\alpha_1} \cdots (\mathcal{O}_{K^{J_\ell},S}^\times)^{\alpha_\ell})$, with $\alpha_i = N_H \cdot a_i$ for all i.

- For every $1 \leq i \leq \ell$, compute $(u_{i,j}^{\alpha_i}) \in \mathcal{O}_{K,S}^\times/\operatorname{tor}$.
- For every $1 \leq i \leq \ell$, compute $(v_{j,i} = N_H(u_{i,j}^{\alpha_i})) \in \mathcal{O}_{K,S}^\times/\operatorname{tor}$ and $x_i \in \mathbb{Z}^N$ as in the previous diagram.
- Create a matrix $M \in \mathcal{M}_{\ell,N}(\mathbb{Z})$ where the columns are the x_i.
- Apply an algorithm to obtain the Hermite normal form of M.
- Apply the same transformations to the $(v_{i,j})$, and output the result.

Algorithm 5.7. input: A number field K, its Galois closure $\tilde{K}$ and its Galois group G, $H < G$ such that $K = \tilde{K}^H$, a set of subgroups $\mathcal{J} = \{J_1, \cdots, J_\ell\}$, the coefficients of a relation of the form (3), and a G-stable set S of non-zero prime ideals of $\mathcal{O}_K$.
output: A basis of $\mathcal{O}_{K,S}^\times$.

- For every element J_i of $\mathcal{J}$, compute a basis of $\mathcal{O}_{K^{J_i},S}^\times$, with Buchmann's algorithm.
- With algorithm 5.6, compute a basis of $V = ((\mathcal{O}_{K^{J_1},S}^\times)^{\alpha_1} \cdots (\mathcal{O}_{K^{J_\ell},S}^\times)^{\alpha_\ell})$, with $\alpha_i = N_H(a_i)$ for all i.
- Output a basis of the d-saturation of V.

Proposition 5.8. *Algorithm 5.7 is correct.*

Proof. The correctness of the algorithm is a direct result of corollary 5.4 □

The main issue with algorithm 5.7 is that it requires to know the Galois group of the number field K of which we want to compute the group of S-units. In practice, when we only have a polynomial defining K, computing G is very costly. In that regard, algorithms 5.9 and 5.12 are more efficient.

Algorithm 5.9. input: A number field K and a set of number fields $\{K_j\}$, each given by an irreducible polynomial in $\mathbb{Q}[X]$ and such that K admits a generalised norm relation with respect to the K_j, a set S of prime numbers, and for each j a $\mathbb{Z}$-basis B_j of $\mathcal{O}_{K_j,S}^{\times}$.

output: A $\mathbb{Z}$-basis of $\mathcal{O}_{K,S}^{\times}$.

1. Compute $\pi_1, \cdots, \pi_k$ all the prime divisors of $n!$ where n is the degree of K (ie all the primes up to n). Let $r_i = 2v_{\pi_i}(n!)$.
2. For all j, compute all the compositums of K and K_j (up to isomorphism).
3. Compute the set B of images of every element of the B_j by every compositum of K and K_j.
4. Compute the subgroup $V \subset \mathcal{O}_{K,S}^{\times}$ generated by B.
5. For every i:
   - $V_i \leftarrow V$
   - $V_i \leftarrow \langle V_i, (x_1)^{\frac{1}{\pi_i}}, \cdots, (x_m)^{\frac{1}{\pi_i}} \rangle$ where $(\overline{x_i})$ is a basis of $(V_i \cap (K^{\times})^{\pi_i})/V_i^{\pi_i}$. (See [7, corollary 4.13])
   - Reduce the basis of V_i as in [36, lemma 7.1].
6. $V \leftarrow V_1 \cdots V_k$
7. Return a basis of V.

Note that to use this algorithm, we need to know that there exists a generalised norm relation, but we do not need to know the coefficients of the relations.

Theorem 5.10. *Algorithm 5.9 is correct. If we assume the generalized Riemann Hypothesis (GRH) then its complexity is polynomial in the size of the input.*

Proof. First, let us prove the correctness. Let G be the Galois group of K, let H the subgroup fixing K and for every i, let J_i the subgroup fixing K_i. Since there is a generalised norm relation, we know that there exists an integer c, a morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i] \to \mathbb{Z}[G/H]$ such that $\phi\otimes\mathbb{Q}$ is surjective, and an injective morphism of $\mathbb{Z}[G]$-modules $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]$, such that $\phi\circ\psi = c\cdot\mathrm{id}$ (by proposition 4.26).

Therefore, by proposition 3.5, for any cohomological Mackey functor M, there is a morphism $\phi_M\colon \bigoplus_{i=1}^m M(J_i) \to M(H)$, and a morphism $\psi_M\colon M(H) \to \bigoplus_{i=1}^m M(J_i)$ such that $\phi\circ\psi = c\cdot\mathrm{id}$. Consider $M(H) = \mathcal{O}_{\tilde{K}^H,S}$ and $M(J_i) = \mathcal{O}_{\tilde{K}^{J_i},S}$. Since $\phi\circ\psi = c\cdot\mathrm{id}$, the c-saturation of the image of ϕ is indeed $\mathcal{O}_{\tilde{K}^H,S}$. And by theorem 4.28, c divides $|G|^2$. Now, we know by remark 3.6 that ϕ_M can be expressed as a sum of elements of $J_i\backslash G/H$, and since, by proposition 2.17, these can be seen as elements of $\mathrm{Compos}(K_i, K)$, this proves the correctness.

Then let us prove the complexity. To compute all the π_i in step 1, we can use a sieve method, which is polynomial in n where n is the degree of K. Therefore, step 1 takes polynomial time.

As seen before, for every j, computing all the compositums of K and K_j takes polynomial time. What's more, the number and the size of the compositums obtained are also polynomial. So step 2 is also polynomial.

The size of the image of an element $x \in K_j$ by a compositum $\mathcal{C}$ is also polynomial, since the map induced by $\mathcal{C}$ is the composition of the injection $K_j \to C$ and the norm $C \to K$. So step 3 is polynomial.

For step 4 as well as step 7, one can deduce a basis from a generating set of the groups involved in polynomial time. The algorithms of [27] provide a basis of the relations between the generators, and the Hermite normal form [29] allows us to obtain a basis of the group in polynomial time.

The saturation in step 5 is performed as many times as the number of primes dividing $(n!)^2$, counted with multiplicity, according to theorem 4.28. That number is polynomial in n, since the number of different primes in the decomposition of $(n!)^2$ is at most n, and for every prime p, $v_p(n!) \leq \frac{\log(n!)}{\log(2)} = \mathcal{O}(n\log(n))$.

Moreover, for every prime dividing $(n!)^2$, counted with multiplicity, the saturation can be done in polynomial time, if we assume GRH. This is [7,

corollary 4.13].

□

5.2 Algorithms for direct computation

Now, let us present an algorithm that computes the class group directly, without computing the group of S-units first.

Remark 5.11. Assuming GRH, the paper [5] gives a polynomial time method to approximate, the residue κ_K of the Dedekind zeta function $\zeta_K(s)$ at $s = 1$ of a number field K, from the discriminant Δ_K and the norm of prime ideals of K.

Algorithm 5.12 is an alternative to algorithm 5.9, which is more efficient in practice but not provably polynomial-time.

Algorithm 5.12. input: A number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields, such that K admits a generalised norm relation with respect to $K_1, \cdots K_\ell$. We know the minimal polynomial f of α with $K = \mathbb{Q}(\alpha)$, and the minimal polynomials f_i of the β_i, with $L_i = \mathbb{Q}(\beta_i)$.

output: The structure of the class group of K

1. For every K_j, compute every compositums of K and K_j.
2. Compute $HR_K = h_K \operatorname{Reg}_K$ using the approximation method in [5]. An approximation up to a factor 1.5 is enough.
3. Initialize T a set of prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) = 1 \mod d$, where $d = \deg(K)^2$.

   The primes in T will be used to detect d-th powers.
4. Initialize a set of prime numbers $S_\mathbb{Q}$, and compute the set S of prime ideals of K above the primes in $S_\mathbb{Q}$.

   We hope that S will generate the class group.
5. For all K_j, let S_j be the set of prime ideals of K_j above all primes p in $S_\mathbb{Q}$, and compute a set U_j of generators of the group of S_j units of K_j.
6. For each j, for each $\mathfrak{p}$ in S_j, compute the vector $V_{j,\mathfrak{p}}$ of valuations of every element of U_j at $\mathfrak{p}$.

7. Compute the matrix of a map Φ, that sends all the ideals above all the primes in S_j to their image by every compositum. Apply this matrix to every $V_{j,\mathfrak{p}}$, then concatenate all the vectors to obtain a matrix M.

8. Apply the action of every compositum to every generator of the U_j then compute the discrete logarithms in $\mathbb{F}_\mathfrak{p}$ of for every p in T. Concatenate all the vectors of discrete logarithms to obtain a matrix N.

9. Concatenate the matrix M and N and compute the kernel R modulo d of this matrix.

   We hope to obtain a basis of the d-saturation of the images in K of the S_j-units of the K_j by the actions of every compositum.

10. Compute the Smith normal form of the concatenation of M and a basis of R.

    If T and S are large enough, that should give us the structure of $\mathrm{Cl}(K)$.

11. Compute the regulator of the group of units of K obtained by the d-saturation of images of the units of the K_j by the actions of every compositum. Multiply it with the class number to obtain a new HR product, that we will denote by $H\tilde{R}_K$. If the approximation for HR_K is up to a factor 1.5, then the regulator should be calculated with precision up to a factor $\frac{4}{3}$.

12. Check if the HR product corresponds to the one in step 3. If not, increase the size of T and $S_\mathbb{Q}$ and go back to step 5.

Theorem 5.13. *If this algorithm terminates, then it is correct.*

Proof. By proposition 4.26, there exists an injective morphism of $\mathbb{Z}[G]$-module $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$ with $n_i \in \mathbb{Z}_{>0}$ for all i, and a morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ such that the image of ϕ has finite index in $\mathbb{Z}[G/H]$ and $\phi \circ \psi = c(\mathcal{J}, H) \cdot \mathrm{id}$. Then, we can use proposition 3.5, with the Mackey functor M defined by $M(H) = \mathbb{Z}^\times_{\tilde{K}^H,S}$ and $M(J_i) = \mathbb{Z}^\times_{\tilde{K}^{J_i},S}$. This proves that the algorithm finds indeed all the S-units in K.

Then, if the verification of the HR product is correct, it means the S-units are enough to generate the class group. The crucial observation is that the approximation errors due to the choice of T and S cannot compensate. If T is not large enough and the algorithm incorrectly assumes an element

to be a d-th power, then $H\tilde{R}_K$ will be a divisor of its expected value. The same will happen if S is not large enough to generate the class group. □

Remark 5.14. Suppose we have a number field $K = \tilde{K}^H$ and a family $(K_i = \tilde{K}^{J_i})$ of number fields, such that K admits a generalised norm relation with respect to $K_1, \ldots, K_\ell$. If we want to compute the class group of K using algorithm 5.12, we could expect the most expensive step to be the computation of the S_j-units in all the K_j, since it is the only step whose computation is not polynomial in the size of the input. However, in practice, when we try to apply this method to reasonable size examples, the most expensive step is often the computation of the images of the ideals in the S_j by the compositums.

In some cases, computing the images of the morphisms associated with compositums can be facilitated by the following proposition.

Proposition 5.15. *Let $K = \tilde{K}^H$ and $L = \tilde{K}^J$, and let (C, ι_K, ι_L) be a compositum of K and L, where ι_L is the inclusion. Suppose we have fixed an embedding $\tilde{K} \to \mathbb{C}$, so $\mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$ and $\mathbb{Q}[\mathrm{Hom}(L, \mathbb{C})]$ canonically have a structure of $\mathbb{Q}[G]$-modules. Let F be the intersection $F = \iota_K(K) \cap L$, and suppose that $C = \iota_K(K) \otimes_F L$. Denote by ϕ the morphism of $\mathbb{Q}[G]$-modules*

$$\phi \colon \mathbb{Q}[\mathrm{Hom}(L, \mathbb{C})] \to \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$$

associated with the compositum (C, ι_K, ι_L) by proposition 2.19. Then, for any $\tau \in \mathrm{Hom}(L, \mathbb{C})$, we have

$$\phi(\tau) = \sum_{\substack{\sigma \in \mathrm{Hom}(K, \mathbb{C}) \\ \sigma \circ \iota_K^{-1}\big|_F = \tau\big|_F}} \sigma$$

(where $\sigma \circ \iota_K^{-1}\big|_F$ and $\tau\big|_F$ denote the restrictions of $\sigma \circ \iota_K^{-1}$ and τ to F).

To prove the proposition 5.15, we will need the following lemma:

Lemma 5.16. *With the notations of proposition 5.15, let α be the primitive element such that $\iota_K(K) = F(\alpha)$. Then we have $C = L(\alpha)$.*

Proof. Since L is included in C, and since α is in $\iota_K(K) \subset C$, we have $L(\alpha) \subset C$.

By definition, the field C is spanned by L and $\iota_K(K)$. We have of course $L \subset L(\alpha)$, and all elements of $\iota_K(K)$ can be written in the form $\sum_i x_i \alpha^i$, with $x_i \in F \subset L$ and $\alpha^i \in L(\alpha)$. So $\iota_K(K) \subset L(\alpha)$, hence $C \subset L(\alpha)$. □

Now let us prove proposition 5.15.

Proof. By proposition 2.23, for all $\tau \in \mathrm{Hom}(L, \mathbb{C})$, we have

$$\phi(\tau) = \sum_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} |E_{\sigma,\tau}| \cdot \sigma \tag{4}$$

with $E_{\sigma,\tau} = \{f \in \mathrm{Hom}(C, \mathbb{C}) | \sigma = f \circ \iota_K \text{ and } \tau = f \circ \iota_L\}$.

Let $\tau \in \mathrm{Hom}(L, \mathbb{C})$, $\sigma \in \mathrm{Hom}(K, \mathbb{C})$, and let $\tilde{\sigma} = \sigma \circ \iota_K^{-1} \in \mathrm{Hom}(\iota_K(K), \mathbb{C})$.

Let us show that $\tilde{\sigma} = \tau$ when restricted to $F = \iota_K(K) \cap L$ if and only if there exists $f \in \mathrm{Hom}(C, \mathbb{C})$ such that $\sigma = f \circ \iota_K$ and $\tau = f \circ \iota_L$, and that in this case, the f is unique.

Suppose that $\tilde{\sigma} = \tau$ when restricted to F. Then, since we have $C = \iota_K(K) \otimes_F L$, we can take $f \in \mathrm{Hom}(C, \mathbb{C})$ such that $f = \tau$ when restricted to L (ie $\tau = f \circ \iota_L$) . Let α be as in lemma 5.16. Then we have $\sigma = f \circ \iota_K$ if and only if $f(\alpha) = \tilde{\sigma}(\alpha)$. And by lemma 5.16, we know that f is uniquely determined by its restriction to L and by the image of α.

Conversely, suppose there is a $f \in \mathrm{Hom}(C, \mathbb{C})$ such that $\sigma = f \circ \iota_K$ and $\tau = f \circ \iota_L$. Then, for every x in $\iota_K(K) \cap L$, we have $\tilde{\sigma}(x) = \tau(x) = f(x)$. So $\tilde{\sigma} = \tau$ when restricted to $F = \iota_K(K) \cap L$.

With this result, the formula 4 gives us the conclusion.

□

5.3 Examples

Example 5.17. The group $G = S_5$ admits a generalised norm relation with respect to $H = S_3 < G$ and $\mathcal{J} = \{A_4, D_{12}, C_5 \rtimes C_4\}$. We can check that this relation does not come from a classical norm relation in a subgroup or a quotient. There are two non conjugate copies of S_3 in S_5. For H we have to take the one with no fixed point.

If we choose a Galois extension $\tilde{K}/\mathbb{Q}$ of Galois group G, then $K = \tilde{K}^H$ is of degree 20, and we can compute its class group inductively, by reducing the problem to three fields of respective degree 10, 10 and 6.

By choosing $\tilde{K}$ such that K has a big discriminant, we can obtain examples where the recursive method is more efficient to compute the class group of K than the pre-existing methods. For example, consider the polynomial $p(x) = x^5 + 91x^4 + 7x^3 - 11x^2 - x + 1$ and define $\tilde{K}$ to be the splitting field of $p(x)$. Then $\tilde{K}$ has Galois group S_5, and $K = \tilde{K}^{S_3}$ is a number field of degree 20 and of discriminant $2^{28} \cdot 383^{10} \cdot 4723^{10} \cdot 23831^{10} \simeq 6 \cdot 10^{114}$. On

Pari/GP [40], the function to compute $\mathrm{Cl}(K)$ was not able to finish in three days, whereas with the method of generalised norm relations, implemented also in Pari/GP, we obtained the result in less than nine hours (CPU time). The result is $\mathrm{Cl}(K) = C_4 \times C_2^4$.

Example 5.18. The group $G = A_5$ admits a generalised norm relation with respect to $H = C_2 \times C_2 < G$ and $\mathcal{J} = \{A_4, D_{10}\}$. We can check that this relation does not come from a classical norm relation in a quotient.

If we choose a Galois extension $\tilde{K}/\mathbb{Q}$ of Galois group G, then $K = \tilde{K}^H$ is of degree 15, and we can compute its class group inductively, by reducing the problem to two fields of respective degree 6 and 5. However, the method with classical norm relations also applies here, but with that method, the largest field we would need to consider is of degree 12.

To create a bigger example, since $7 \nmid |A_5|$, we can consider the generalised norm relation of $G' = C_7 \times A_5$ with respect to $H = C_2 \times C_2 < G$ and $\mathcal{J} = \{A_4, D_{10}\}$. That way, we can compute the class group of a field of degree 105 by reducing the problem to two fields of respective degree 42 and 35, whereas with classical norm relations, we would have reduced the problem to a field of degree 84.

For example, consider the polynomial $f(x) = x^6 - 2x^5 + 3x^4 - 4x^3 + 2x^2 - 2x - 1$. Define $\tilde{L}$ to be the splitting field of $f(x)$. Then $\tilde{L}$ has Galois group A_5. The splitting field $\tilde{M}$ of the polynomial $g(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$ has Galois group C_7. Up to isomorphism, there is only one compositum $\tilde{K}$ of $\tilde{L}$ and $\tilde{M}$. What's more, $\tilde{K}/\mathbb{Q}$ is Galois and its Galois group is $G = C_7 \times A_5$. Denote by K the subfield of $\tilde{K}$ fixed by $H = C_2 \times C_2$, which is a field of degree 105 and of discriminant $2^{126} \cdot 29^{90} \cdot 67^{42} \simeq 1.7 \cdot 10^{246}$. With the method involving only classical norm relation, we can compute $\mathrm{Cl}(K)$, but we have to compute the class group of some subfields, the largest of which is $F = \tilde{K}^{C_5}$, of degree 84 and of discriminant $2^{126} \cdot 29^{72} \cdot 67^{42} \simeq 8 \cdot 10^{219}$. On Pari/GP, the function to compute $\mathrm{Cl}(F)$ was not able to finish in over 5 months, whereas with our implementation of the method of generalised norm relations, we computed $\mathrm{Cl}(K)$ in about 5 days (CPU time). The result is $\mathrm{Cl}(K) = 1$. And the regulator of K is approximately $\mathrm{Reg}_K = 2.656 \cdot 10^{83}$.

6 An application of generalised norm relations to Leopoldt's conjecture

In this chapter we apply our notion of generalised norm relations to the study of Leopoldt's conjecture. We will need some results about local fields, in this chapter and in the next one, which can be found for example in [43]. Let p be a prime number, and K a number field of degree d, and let r_1, r_2 be the number of real and pairs of complex embeddings of K. Let $\epsilon_1, \cdots, \epsilon_{r_1+r_2-1}$ be a basis of the group $U(K)$ of units of $\mathbb{Z}_K^\times$. Fix an algebraic closure $\tilde{\mathbb{Q}}_p$ of the field $\mathbb{Q}_p$ of p-adic numbers, and denote by $\mathbb{C}_p$ the completion of $\tilde{\mathbb{Q}}_p$ by the p-adic absolute value. We call $\mathbb{C}_p$ the field of *p-adic complex numbers*. There is a uniquely defined p-adic logarithm $\log_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$ (see [chapter II, (5.4)][38]). Let $\sigma_1, \cdots, \sigma_d$ be the elements of $\mathrm{Hom}(K, \mathbb{C}_p)$. Let us recall the following definition.

Definition 6.1. The *regulator matrix* of K at p is defined by

$$\mathcal{R}_p(\epsilon_1, \cdots, \epsilon_{r_1+r_2-1}) = \begin{pmatrix} \log_p \sigma_1(\epsilon_1) & \cdots & \log_p \sigma_d(\epsilon_1) \\ \vdots & \ddots & \vdots \\ \log_p \sigma_1(\epsilon_{r_1+r_2-1}) & \cdots & \log_p \sigma_d(\epsilon_{r_1+r_2-1}). \end{pmatrix}$$

and the *p-adic regulator rank* of K is $r_p(K) = \mathrm{rank}\, \mathcal{R}_p(\epsilon_1, \cdots, \epsilon_{r_1+r_2-1})$. It is independent of the choice of the basis $(\epsilon_1, \cdots, \epsilon_{r_1+r_2-1})$ and of the ordering of the σ_i.

Then Leopoldt's conjecture can be stated as follows (see [39, chapter 10.3.5]).

Conjecture 6.2. For every number field K and every prime number p, the p-adic regulator rank $r_p(K)$ is equal to $r_1 + r_2 - 1$.

Leopoldt's conjecture has many equivalent formulations (see [39, Theorem 10.3.6]), and has connections in particular with Galois cohomology and with Iwasawa theory (see [39, Chapters 10 and 11]).

Here, we will be interested in the following equivalent formulation of Leopoldt's conjecture, which is also the one used in [23].

Let $S_p(K)$ be the set of places of K above p, and for every $w \in S_p(K)$, let U_{K_w} and $U^1_{K_w}$ be respectively the group of units and the subgroup of principal units of K_w (i.e. the units congruent to 1 modulo the maximal ideal).

Let us consider the diagonal embedding $\mathbb{Z}_K^\times \hookrightarrow \prod_{w\in S_p(K)} U_{K_w}$.
Taking the p-adic completion, we get an homomorphism

$$\lambda_{K,p}\colon \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_K^\times \to \prod_{w\in S_p(K)} U^1_{K_w}$$

Then Leopoldt's conjecture can be stated as follows:

Conjecture 6.3. For every number field K and for every prime number p, the homomorphism $\lambda_{K,p}$ is injective.

Definition 6.4. Let K be a number field, and p a prime number.

- We denote by $\mathrm{Leo}(K,p)$ Leopoldt's conjecture at K and p: we say that $\mathrm{Leo}(K,p)$ holds if $\lambda_{K,p}$ is injective.
- The *Leopoldt kernel* $\mathcal{L}(K,p)$ is the kernel of the map

$$\Lambda_{K,p} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \lambda_{K,p}\colon \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathbb{Z}_K^\times \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \prod_{w\in S_p(K)} U^1_{K_w}.$$

- The *Leopoldt defect* $\delta(K,p)$ is defined to be $\dim_{\mathbb{Q}_p} \mathcal{L}(K,p)$.

With that definition, we have that $\mathrm{Leo}(K,p)$ is equivalent to $\delta(K,p) = 0$.

Lemma 6.5 (lemma 2.2 of [23])**.** *Let L/K be a Galois extension of number fields, of Galois group G, and let p be a prime number. Then $\mathcal{L}(L,p)$ is a $\mathbb{Q}_p[G]$-module, and for any subgroup $H \leq G$, we have $\mathcal{L}(L,p)^H = \mathcal{L}(L^H,p)$.*

Proof. This is [23, lemma 2.2] □

In the rest of the chapter, we will see that some results in [23] using classical normed relations can be generalised.

Definition 6.6 and proposition 6.7 will be very close to what we have already seen in section 4.2, but rephrased to better fit the notations of [23].

Definition 6.6. In this chapter, if G is a finite group, $H < G$ a subgroup, and K a field of characteristic zero, then we will denote by f_H the idempotent element of the algebra $K[G]$ defined by $f_H = \frac{N_H}{|H|} = \frac{\sum_{h\in H} h}{|H|}$.

With this definition, we can state the following proposition, which is an extension of [23, Proposition 4.4].

Proposition 6.7. *Let G be a finite group and suppose that G has a generalised norm relation with respect to a subgroup $\Gamma < G$, and a set of subgroups $\mathcal{H}$. Let M be a $K[G]$-module. If $f_H M = 0$ for every non trivial $H \in \mathcal{H}$, then $f_\Gamma M = 0$*

Proof. This is a rephrasing of proposition 4.14, part 2. □

Corollary 6.8. *Let G be a finite group and suppose that G has a generalised norm relation with respect to a subgroup $\Gamma < G$, and a set of subgroups $\mathcal{H}$. Let $\mathcal{I} \subseteq \mathcal{H}$ be such that $1 \notin \mathcal{I}$ and for every $H \in \mathcal{H}$, there exists $I \in \mathcal{I}$ and $g \in G$ such that $gIg^{-1} \leq H$. Let M be a $K[G]$-module. If $f_I M = 0$ for every $I \in \mathcal{I}$, then $f_\Gamma M = 0$.*

This corollary is an adaptation of [23, corollary 4.5]. It is not exactly a generalisation since the converse that was true for classical norm relations is no longer true. The proofs are very similar.

Proof. Suppose that $f_I M = 0$ for every $I \in \mathcal{I}$.

If $H \in \mathcal{H}$, with $H \neq 1$ and $g \in G$, there is $I \in \mathcal{I}$ such that $gIg^{-1} \leq H$. Then we have $g f_I g^{-1} = f_{gIg^{-1}}$, and

$$f_H = \left(\frac{1}{[H : gIg^{-1}]} \sum_{h \in H/gIg^{-1}} h \right) g f_I g^{-1}.$$

Then, for all $x \in M$, we have $f_I g^{-1} x \in f_I M = 0$, so $f_H M = 0$. Therefore, $f_H M = 0$ for all $H \in \mathcal{H}$ with $H \neq 1$, and so, by proposition 6.7, we have $f_\Gamma M = 0$.

□

Proposition 6.9. *Let L/K be a Galois extension of number fields, and let G be its Galois group. Suppose that G has a generalised norm relation with respect to a subgroup $\Gamma < G$, and a set of subgroups $\mathcal{H}$. Let $\mathcal{I} \subseteq \mathcal{H}$ be such that $1 \notin \mathcal{I}$ and for every $H \in \mathcal{H}$, there exists $I \in \mathcal{I}$ and $g \in G$ such that $gIg^{-1} \leq H$. Let p be a prime number. If $\mathrm{Leo}(L^I, p)$ holds for every $I \in \mathcal{I}$, then $\mathrm{Leo}(L^\Gamma, p)$ holds.*

Proof. This follows directly from corollary 6.8 and lemma 6.5. □

Example 6.10. We saw in example 4.13 that the group $G = S_4$ admits a generalised norm relation over $\mathbb{Q}$ with respect to $H = C_2 \times C_2$ and $\mathcal{J} = \{D_8, S_3\}$. That means that for every Galois extension $\tilde{K}/\mathbb{Q}$ of Galois group $G = S_4$, and for p a prime number, if H is a subgroup of G isomorphic to $C_2 \times C_2$ and $J_1, J_2 < G$ are isomorphic to D_8 and S_3, if $\mathrm{Leo}(\tilde{K}^{J_1}, p)$ and $\mathrm{Leo}(\tilde{K}^{J_2}, p)$ both hold, then $\mathrm{Leo}(\tilde{K}^{H}, p)$ also holds.

We could use proposition 6.9 to find new examples of number fields F and primes p such that $\mathrm{Leo}(F, p)$ holds.

Until now, we were only interested in generalised norm relations where the auxiliary fields are of the lowest possible degree, so their class groups or their groups of S-units would be easier to compute a priori. However, to find examples where Leopoldt's conjecture holds, the most useful relations would be those where we know that Leopoldt's conjecture holds for every auxiliary fields.

To find such auxiliary fields, one can use for example the following result, by Ax and Brumer:

Theorem 6.11 ([2], [12])**.** *Let K be a finite abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field. Then* $\mathrm{Leo}(K, p)$ *holds for every prime number p.*

In [23], the authors also prove that Leopoldt's conjecture holds for certain primes for an infinite family of totally real S_3-extensions of $\mathbb{Q}$ (see [23, theorem 6.12]) or for an infinite family of totally real D_8-extensions of $\mathbb{Q}$ (see [23, corollary 6.17]).

7 Computing Selmer groups

In this chapter, we will present an algorithmic method to compute Selmer groups of finite Galois modules. We will use the following definition of a Selmer group.

Let K be a number field, $\overline{K}$ its algebraic closure, and $\mathcal{G}$ (or $\mathcal{G}_K$) its absolute Galois group. Let M be a left $\mathcal{G}$-module. Given a finite place v of K, let G_v denote the decomposition group of K at v, and I_v the inertia group. Then,

- a *local condition* at v is a subgroup $L_v \subset H^1(G_v, M)$,
- the *unramified condition* is the subgroup

$$H^1_{un}(G_v, M) = \ker\left\{H^1(G_v, M) \to H^1(I_v, M)\right\},$$

- a *Selmer system* for M is a set $\mathcal{L}$ of local conditions L_v at every finite place v of K, such that all but finitely many of the L_v are the unramified condition,
- given a Selmer system $\mathcal{L}$, the *Selmer group* attached to $\mathcal{L}$ is the subgroup of $H^1(\mathcal{G}_K, M)$ given by

$$\mathrm{Sel}_{\mathcal{L}} = \ker\left\{H^1(\mathcal{G}_K, M) \to \prod_v \frac{H^1(G_v, M)}{L_v}\right\}.$$

Note that this definition of Selmer group is restricted to subgroups of the first cohomology group $H^1(\mathcal{G}_K, M)$, but we can give a similar definition for Selmer groups that would be subgroups of other cohomology groups. For future research, it might be interesting to try and adapt the method presented in this chapter to be able to compute Selmer groups contained in $H^2(\mathcal{G}_K, M)$.

Some methods already exist to compute Selmer groups. For Selmer groups of elliptic curves, Bruin lists some of these algorithms in [11, section 5.4] and gives a geometric interpretation, and we can also mention some more recent articles, like the article [34] by Maistret and Shukla. The method presented here is more general, since it allows one to compute Selmer groups in general and not only Selmer groups of elliptic curves. For future work, we think it would be interesting to compare the time complexity of all the existing methods.

In all of the chapter, K will be a field of characteristic zero. We will denote by $\overline{K}$ its algebraic closure and by $\mathcal{G}$ the Galois group $\mathrm{Gal}(\overline{K}/K)$.

All modules will be left modules.

When R is a ring and M, N are left R-modules, we will denote by $\mathrm{Hom}_R(M,N)$ the group of R-module homomorphisms from M to N.

If M is a $\mathcal{G}$-module, we will denote by $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, \overline{K}^\times)$ the dual module of M, where $\overline{K}^\times$ is viewed as an abelian group.

In a finite field extension L/F, we will denote by $N_{L/F}(x)$ the norm of $x \in L$.

Unless specified otherwise, the group laws of cohomology groups will always be denoted multiplicatively.

7.1 Finding a resolution with Hecke operators

In all of the chapter, M will be a finite Galois module.

Let G be the image of the action $\mathcal{G} \to \mathrm{Aut}(M)$. It is isomorphic to a finite quotient of $\mathcal{G}$. Note that the action of $\mathcal{G}$ over M can be factorized to be seen as an action of G over M.

Remark 7.1. If $\mathcal{N}$ denotes the kernel of the action $\mathcal{G} \to \mathrm{Aut}(M)$, then G is the Galois group of the Galois extension $\overline{K}^{\mathcal{N}}/K$.

Suppose we have $\mathbb{Z}[G]$-modules P_i for every integer i, that are permutation modules, as well as some morphisms of G-modules s and d_i^* such that the sequence

$$\cdots \xrightarrow{d_2^*} P_2 \xrightarrow{d_1^*} P_1 \xrightarrow{d_0^*} P_0 \xrightarrow{s} M^* \to 0$$

is exact, where M^* is the dual module of M.

We will see in section 7.3 that we can always find such an exact sequence, and we will give an algorithm (algorithm 7.18) to compute such P_i and d_i^* up to any integer i.

For this method, we will only need to compute such sequences up to P_2. We will denote by (5) an exact sequence of the form

$$P_2 \xrightarrow{d_1^*} P_1 \xrightarrow{d_0^*} P_0 \xrightarrow{s} M^* \to 0. \tag{5}$$

Lemma 7.2. *The functor $P \mapsto P^* = \mathrm{Hom}_{\mathbb{Z}}(P, \overline{K}^\times)$, from the category of $\mathcal{G}$-modules that are finitely generated $\mathbb{Z}$-modules to the category of $\mathcal{G}$-modules, is exact.*

Proof. It is enough to prove that $P \mapsto P^*$ is exact as a functor from the category of $\mathbb{Z}$-modules to the category of $\mathbb{Z}$-modules.

Since $\overline{K}^\times$ is divisible, it is injective as a $\mathbb{Z}$-module. Therefore, the functor $P \mapsto P^* = \mathrm{Hom}_{\mathbb{Z}}(P, \overline{K}^\times)$ is exact. □

Once we obtain an exact sequence of the form (5), by lemma 7.2, we can take the dual and get an exact sequence of the form

$$0 \to M \to I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} I_2 \tag{6}$$

where $I_i = P_i^*$ for all i.

Consider an exact sequence of the form (6) obtained with the construction described above. The modules P_0, P_1, P_2 are permutations modules. In the rest of the section, let us write $P_i = \bigoplus_j \mathbb{Z}[G/H_{i,j}]$ for $i \in \{1,2,3\}$, and for every pair (i,j), let us define $L_{i,j} := \overline{K}^{H_{i,j}}$.

Proposition 7.3. *With the above notations, for $i \in \{1,2,3\}$, we have*

$$I_i = \bigoplus_j \mathrm{Ind}_{\mathcal{G}/\mathcal{G}_{L_{i,j}}} \overline{K}^\times = \bigoplus_j \overline{L_{i,j}}^\times$$

where $\mathcal{G}_{L_{i,j}}$ is the absolute Galois group of $L_{i,j}$. Moreover, we have

$$I_i^{\mathcal{G}} = I_i^G = \bigoplus_j L_{i,j}^\times.$$

Proof. See [49, Section 3.12, Example 19]. □

The morphisms $d_0 \colon I_0 \to I_1$ and $d_1 \colon I_1 \to I_2$ induce morphisms respectively from I_0^G to I_1^G and from I_1^G to I_2^G, that we will denote by d_0^G and d_1^G.

Proposition 7.4. *With the above notations, we have*

$$H^1(\mathcal{G}, M) = \frac{\mathrm{Ker}(d_1^G \colon I_1^G \to I_2^G)}{\mathrm{Im}(d_0^G \colon I_0^G \to I_1^G)}.$$

Proof. Let $J \subset I_1$ be the image of d_0. Then we have a short exact sequence

$$0 \to M \to I_0 \xrightarrow{d_0} J \to 0.$$

The associated long exact sequence starts with

$$0 \to M^{\mathcal{G}} \to I_0^{\mathcal{G}} \xrightarrow{d_0} J \to H^1(\mathcal{G}, M) \to H^1(\mathcal{G}, I_0)$$

and $H^1(\mathcal{G}, I_0) = \bigoplus_j H^1(G_{L_{0,j}}, \overline{L}_{0,j}^{\times})$ by Shapiro's lemma, and $H^1(G_{L_{0,j}}, \overline{L}_{0,j}^{\times}) = 0$ by Hilbert 90th theorem.

This last exact sequence allows us to deduce that

$$H^1(\mathcal{G}, M) = \frac{J^G}{\mathrm{Im}(d_0^G \colon I_0^G \to I_1^G)}. \tag{7}$$

What's more, by definition of J, we also have an exact sequence

$$0 \to J \to I_1 \xrightarrow{d_1} I_2,$$

hence the exact sequence

$$0 \to J^G \to I_1^G \xrightarrow{d_1} I_2^G,$$

from which we can deduce that

$$J^G = \mathrm{Ker}(d_1^G \colon I_1^G \to I_2^G).$$

Combining that result with 7, we get

$$H^1(\mathcal{G}, M) = \frac{\mathrm{Ker}(d_1^G \colon I_1^G \to I_2^G)}{\mathrm{Im}(d_0^G \colon I_0^G \to I_1^G)}.$$

□

Remark 7.5. If the modules I_i were injective, proposition 7.4 would be trivial, but this is not usually the case. For example, for all i, j, we have $H^2(\mathcal{G}, \mathrm{Res}_{L_{i,j}/K} \overline{K}^{\times}) = H^2(\mathcal{G}, \overline{L_{i,j}}^{\times})$ which is the Brauer group of $L_{i,j}$, which is usually non trivial.

Proposition 7.6. *For every subgroup $\mathcal{H} < \mathcal{G}_K$, the map*

$$\mathrm{Res} : H^1(\mathcal{G}_K, M) \to H^1(\mathcal{H}, M)$$

is the natural restriction

$$H^1(\mathcal{G}, M) = \frac{\mathrm{Ker}(d_1^{\mathcal{G}} \colon I_1^{\mathcal{G}} \to I_2^{\mathcal{G}})}{\mathrm{Im}(d_0^{\mathcal{G}} \colon I_0^{\mathcal{G}} \to I_1^{\mathcal{G}})} \to H^1(\mathcal{H}, M) = \frac{\mathrm{Ker}(d_1^{\mathcal{H}} \colon I_1^{\mathcal{H}} \to I_2^{\mathcal{H}})}{\mathrm{Im}(d_0^{\mathcal{H}} \colon I_0^{\mathcal{H}} \to I_1^{\mathcal{H}})}.$$

Proof. Let $J \subset I_1$ be the image of d_0. Then we have a short exact sequence

$$0 \to M \to I_0 \xrightarrow{d_0} J \to 0.$$

The associated long exact sequence starts with

$$0 \to M^{\mathcal{G}} \to I_0^{\mathcal{G}} \to J_1^{\mathcal{G}} \to H^1(\mathcal{G}, M).$$

We can then apply the restriction map to obtain

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M^{\mathcal{G}} & \longrightarrow & I_0^{\mathcal{G}} & \longrightarrow & J_1^{\mathcal{G}} & \longrightarrow & H^1(\mathcal{G}, M) \\ & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ 0 & \longrightarrow & M^{\mathcal{H}} & \longrightarrow & I_0^{\mathcal{H}} & \longrightarrow & J_1^{\mathcal{H}} & \longrightarrow & H^1(\mathcal{H}, M) \end{array}$$

Moreover, for every field F such that $K \subset F$, and for all i, we have $I_i^{\mathcal{G}} = L_i^\times$ and $I_i^{\mathrm{Gal}(\overline{F}/F)} = (L_i \otimes_K F)^\times$. So $I_i^{\mathcal{H}} = \overline{L_i}^{\mathcal{H}}$, hence the conclusion. □

7.2 A remarkable Selmer group

Let M be a finite Galois module, suppose that we have the Galois modules I_0, I_1, I_2 and the morphisms of G-modules d_0 and d_1 obtained as in section 7.1, such that the sequence

$$0 \to M \to I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} I_2$$

is exact. By proposition 7.4, we have

$$H^1(\mathcal{G}, M) = \frac{\mathrm{Ker}(d_1^G \colon I_1^G \to I_2^G)}{\mathrm{Im}(d_0^G \colon I_0^G \to I_1^G)}.$$

where for all $i \in \{0, 1, 2\}$, I_i^G is of the form $\bigoplus_j L_{i,j}^\times$ and the $L_{i,j}$ are intermediate fields between K and $\overline{K}$.

In the rest of the section, we will denote by L_i the étale algebra $\prod_j L_{i,j}$. We will allow ourself to extend to étale algebras the notions of class groups and S-unit groups.

Definition 7.7. Let S be a set of prime numbers. Let us define the group $H^1_S(\mathcal{G}, M) := \frac{\mathrm{Ker}(d_1^G \colon \bigoplus_j \mathbb{Z}^\times_{L_{1,j},S} \to \bigoplus_j \mathbb{Z}^\times_{L_{2,j},S})}{\mathrm{Im}(d_0^G \colon \bigoplus_j \mathbb{Z}^\times_{L_{0,j},S} \to \bigoplus_j \mathbb{Z}^\times_{L_{1,j},S})}$.

By theorem 2.24, the images of S-units by d_1^G and d_0^G are S-units, so the group $H^1_S(\mathcal{G}, M)$ is well defined.

When the context is clear, we will also allow ourself to write H^1 and H^1_S instead of $H^1(\mathcal{G}, M)$ and $H^1_S(\mathcal{G}, M)$.

The goal of this section will be to prove that $H^1_S(\mathcal{G}, M)$ is a Selmer group. We will use the following notations:

- $Z^1 := \mathrm{Ker}(d_1^G \colon I_1^G \to I_2^G)$
- $B^1 := \mathrm{Im}(d_0^G \colon I_0^G \to I_1^G)$
- $Z^1_S := \mathrm{Ker}(d_1^G \colon \bigoplus_j \mathbb{Z}^\times_{L_{1,j},S} \to \bigoplus_j \mathbb{Z}^\times_{L_{2,j},S})$
- $B^1_S := \mathrm{Im}(d_0^G \colon \bigoplus_j \mathbb{Z}^\times_{L_{0,j},S} \to \bigoplus_j \mathbb{Z}^\times_{L_{1,j},S})$.

Proposition 7.8. *We have an injection $H^1_S(\mathcal{G}, M) \hookrightarrow H^1(\mathcal{G}, M)$.*

Proof. We have trivially $Z^1_S \subset Z^1$. So in order to prove the proposition, it is enough to show that $B^1 \cap \mathbb{Z}^\times_{L_1,S} \subset B^1_S$. In other words, we need to show that if an element y in the image of d_0^G is an S-unit, then there exists an S-unit x in $I_0^G = L_0^\times$ such that $d_0^G(x) = y$.

If we take the tensor product of the exact sequence (6) with $\mathbb{Q}$, we obtain

$$0 \to I_0 \otimes \mathbb{Q} \xrightarrow{d_0} I_1 \otimes \mathbb{Q} \xrightarrow{d_1} I_2 \otimes \mathbb{Q}$$

because M is finite, so that $M \otimes \mathbb{Q} = 0$.

Then, by proposition 4.25 applied to P_0 and P_1, there exists a surjective morphism of G-modules $f \colon I_1 \to I_0$ such that $f \circ d_0 = k \cdot \mathrm{id}$.

Now, let y be an element of $B^1 \cap \mathbb{Z}^\times_{L_1,S}$. Since x is in B^1, there exists $x \in L_0^\times$ such that $d_0^G(x) = y$. So $s \circ d_0^G(x) = k \cdot x$ (or x^k in multiplicative notation). But $d_0^G(x) = y$ is an S-unit, so its image by f is also an S-unit by 2.4. Hence $k \cdot x$ is an S-unit. And since $\mathbb{Z}^\times_{S,L_0}$ is saturated as a subgroup of $L_0^\times$, that means x is also an S-unit.

So y is the image of an S-unit by d_0^G, ie $y \in B^1_S$. Hence $B^1_S \subset B^1 \cap \mathbb{Z}^\times_{L_1,S}$. □

Definition 7.9. In the rest of the section, if v is a finite place of K, we will use the following notations:

- $Z^1_{\text{units},v} = \text{Ker}(\mathbb{Z}^\times_{L_1,v} \xrightarrow{d_1} \mathbb{Z}^\times_{L_2,v})$,
- $B^1_{\text{units},v} = \text{Im}(\mathbb{Z}^\times_{L_0,v} \xrightarrow{d_0} \mathbb{Z}^\times_{L_1,v})$,
- $H^1_{\text{units},v} = \frac{Z^1_{\text{units},v}}{B^1_{\text{units},v}}$,
- K_v^{ur} the largest unramified extension of K_v, and $I_{K_v} = \text{Gal}(\overline{K_v}/K_v^{\text{ur}})$ the inertia group, and $\mathcal{G}_{K_v} = \text{Gal}(\overline{K_v}/K)$.
- $Z^1_{\text{ram},v} = \text{Ker}((L_0 \otimes K_v^{\text{ur}})^\times \xrightarrow{d_1} (L_1 \otimes K_v^{\text{ur}})^\times)$,
- $B^1_{\text{ram},v} = \text{Im}((L_1 \otimes K_v^{\text{ur}})^\times \xrightarrow{d_0} (L_2 \otimes K_v^{\text{ur}})^\times)$,
- $H^1_{\text{ram},v} = \frac{Z^1_{\text{ram},v}}{B^1_{\text{ram},v}}$.

When the context is clear, we will allow ourself to write H^1_{ram}, Z^1_{ram} and B^1_{ram}.

For every place v of K, we also write:

- $Z^1_v = \text{Ker}(L^\times_{1,v} \xrightarrow{d_{1,v}} L^\times_{2,v})$
- $B^1_v = \text{Im}(L^\times_{0,v} \xrightarrow{d_{0,v}} L^\times_{1,v})$
- $H^1_v = \frac{Z^1_v}{B^1_v}$.

where $d_{0,v}$ and $d_{1,v}$ are defined respectively by the two following commutative diagrams

$$\begin{array}{ccc} L_0^\times & \xrightarrow{d_0} & L_1^\times \\ (\star)\ \downarrow & & \downarrow \\ L_{0,v}^\times & \xrightarrow[d_{0,v}]{} & L_{1,v}^\times \end{array} \qquad \begin{array}{ccc} L_1^\times & \xrightarrow{d_1} & L_2^\times \\ (\star\star)\ \downarrow & & \downarrow \\ L_{1,v}^\times & \xrightarrow[d_{1,v}]{} & L_{2,v}^\times \end{array}$$

Proposition 7.10. *For every place v of K, we have*

$$\mathrm{Res}_v(H^1(G,M)) \subseteq \frac{Z_v^1}{B_v^1}$$

where Res_v *denotes the restriction map from* $H^1(\mathcal{G},M)$ *to* $H^1(\mathcal{G}_v,M)$.

Proof. Let $\overline{x}$ be a class in $H^1(G,M)$ and let x be a representative of $\overline{x}$ modulo B_1, and x_v the localisation of x at v.

Since the diagram $(\star\star)$ commutes and $d_1(x)=0$, we have $d_{1,v}(x_v)=0$. So $x_v \in Z_v^1$.

If x_2 is another representative of $\overline{x}$, then $x_2 = x+b$ with $b \in B^1$. When we take the localisation at v, we get $x_{2,v} = x_v + b_v$, and since the diagram $(\star)$ commutes, we have $b_v \in B_v^1$. Hence $\mathrm{Res}_v(\overline{x}) \in \frac{Z_v^1}{B_v^1}$.

□

Proposition 7.11. *With the notations of definition 7.9, we have* $H_v^1 = H^1(\mathcal{G}_{K_v},M)$ *and* $H^1_{\mathrm{ram}} = H^1(I_{K_v},M)$.

Proof. We can do the same construction as in section 7.1, with K_v (respectively K_v^{ur}) instead of K. The same resolution

$$0 \to M \to I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} I_2$$

also works in these cases, since the I_i are also both $\mathcal{G}_{K_v}$-modules and I_{K_v} modules. Moreover, for all i, we have $I_i^{\mathcal{G}_{K_v}} = L_{i,v}^\times$ and $I_i^{I_{K_v}} = (L_i \otimes K_v^{\mathrm{ur}})^\times$. Hence the conclusion. □

Note that, by proposition 7.6, the map $\mathrm{Res}_v : H^1(\mathcal{G}_K,M) \to H_{1,v}$ is the natural restriction $\frac{Z_1}{B_1} \to \frac{Z_{1,v}}{B_{1,v}}$.

Lemma 7.12. *Let $v \notin S$ be a place of K, then we have*

$$\mathrm{Res}_v(H_S^1(\mathcal{G},M)) \subseteq H^1_{\mathrm{units},v}.$$

Proof. Let v be a place not in S. Let $\overline{x}$ be a class in H_S^1, $x \in Z_S^1$ a representative of $\overline{x}$, and x_v the localisation of x at v. Since $v \notin S$, we have $x_v \in \mathbb{Z}_{L_1,v}^\times$. And since the diagram $(\star\star)$ commutes, we have $x_v \in Z_v^1$. So $x_v \in \mathrm{Ker}(\mathbb{Z}_{L_1,v}^\times \xrightarrow{d_{1,v}} L_{2,v}^\times)$. And if $x_2 = x \cdot b$ is another representative of $\overline{x}$, with $b \in B_S^1$, then it is easy to check that $b_v \in \mathrm{Im}(\mathbb{Z}_{L_0,v}^\times \to \mathbb{Z}_{L_1,v}^\times)$. Hence $\mathrm{Res}_v(\overline{x}) \in H_{\mathrm{units},v}$.

□

Proposition 7.13. *If S is a set of primes such that the class group $\mathrm{Cl}(L_0)$ is spanned by ideals above all primes in S, then we have*

$$H^1_S = \{x \in H^1 \mid \forall v \notin S, \mathrm{Res}_v(x) \in H^1_{\mathrm{units},v}\}.$$

Proof. By lemma 7.12, we already have the inclusion $H^1_S \subseteq \{x \in H^1 \mid \forall v \notin S, \mathrm{Res}_v(x) \in H^1_{\mathrm{units},v}\}$.

Now, let $\overline{x}$ be a class in $H^1(\mathcal{G}, M)$ such that for all place $v \notin S$, we have $\mathrm{Res}_v(x) \in H^1_{\mathrm{units},v}$. By definition, for all v, there exists z_v in $L_{0,v}^\times$ such that $\mathrm{Res}_v(x) \cdot d_{0,v}(z_v) \in \mathbb{Z}^\times_{L_1,v}$.

We want to show that there exists $z \in L_0^\times$ such that for all $v \notin S$, $z \cdot z_v^{-1} \in \mathbb{Z}^\times_{L_0,v}$. This problem is equivalent to taking a fractional ideal $\mathfrak{a}$ of L_0, and deciding whether there exists $\mathfrak{p}$ a product of prime ideals in S such that $\mathfrak{ap}$ is principal. But since S spans the class group of L_0, we know it is possible.

□

Proposition 7.14. *For every place v of K such that v does not divide $|M|$, we have $H^1_{\mathrm{units},v} = \mathrm{Ker}(\mathrm{Res}\colon H^1 \to H^1_{\mathrm{ram}})$.*

Proof. First let us show the inclusion $H^1_{\mathrm{units},v} \subseteq \mathrm{Ker}(\mathrm{Res}\colon H^1 \to H^1_{\mathrm{ram}})$.

We have the following diagram:

$$\begin{array}{ccccc}
(\mathcal{O}_{L_0} \otimes \mathcal{O}_{K_v^{\mathrm{ur}}})^\times & \xrightarrow{d_0} & (\mathcal{O}_{L_1} \otimes \mathcal{O}_{K_v^{\mathrm{ur}}})^\times & \xrightarrow{d_1} & (\mathcal{O}_{L_2} \otimes \mathcal{O}_{K_v^{\mathrm{ur}}})^\times \\
\downarrow i & & \downarrow i & & \downarrow i \\
(L_0 \otimes K_v^{\mathrm{ur}})^\times & \xrightarrow{d_0} & (L_1 \otimes K_v^{\mathrm{ur}})^\times & \xrightarrow{d_1} & (L_2 \otimes K_v^{\mathrm{ur}})^\times \\
\downarrow \mathrm{val} & & \downarrow \mathrm{val} & & \downarrow \mathrm{val} \\
\mathbb{Z}^{\mathrm{Hom}(L_0, K_v^{\mathrm{ur}})} & \xrightarrow{d_0} & \mathbb{Z}^{\mathrm{Hom}(L_1, K_v^{\mathrm{ur}})} & \xrightarrow{d_1} & \mathbb{Z}^{\mathrm{Hom}(L_2, K_v^{\mathrm{ur}})}
\end{array}$$

where the three vertical sequences are exact, and where val denotes the valuation morphisms. What's more, the morphism $d_0\colon \mathbb{Z}^{\mathrm{Hom}(L_0, K_v^{\mathrm{ur}})} \to \mathbb{Z}^{\mathrm{Hom}(L_1, K_v^{\mathrm{ur}})}$ is injective because the kernel of $d_0\colon (L_0 \otimes K_v^{\mathrm{ur}})^\times \to (L_1 \otimes K_v^{\mathrm{ur}})^\times$ is torsion, so its image under val is 0.

Let $x \in Z^1_{\mathrm{units}} \subset \mathcal{O}^\times_{L_1}$. That is to say $d_1(x) = 1 \in \mathcal{O}^\times_{L_2}$. We want to show that $\mathrm{Res}(x) = x \otimes 1 \in (L_1 \otimes K_v^{\mathrm{ur}})^\times$ is in $B^1_{\mathrm{ram}} = d_0((L_0 \otimes K_v^{\mathrm{ur}})^\times)$.

Let N be an integer such that the module M is annihilated by N, and such that N does not divide the characteristic of the residue field of $\mathcal{O}_K$. Then H^1_{ram} is N-torsion.

So there exists $y \in (L_0 \otimes K_v^{\text{ur}})^\times$ such that $\text{Res}(x)^N = d_0(y)$.

Since $x \in \mathcal{O}_{L_1}^\times$, then $\text{val}(\text{Res}(x)) = 0$, so $\text{val}(y) = 0$, so $y \in (\mathcal{O}_{L_0}^\times \otimes \mathcal{O}_{K_v^{\text{ur}}}^\times)^\times$. And $(\mathcal{O}_{L_0}^\times \otimes \mathcal{O}_{K_v^{\text{ur}}}^\times)^\times$ is N-divisible, so there exists $z \in (\mathcal{O}_{L_0}^\times \otimes \mathcal{O}_{K_v^{\text{ur}}}^\times)^\times$ such that $z^N = y$.

Hence $d_0(z)^N = d_0(y) = x^N$. This proves that $d_0(z) = \zeta_N x$, with ζ_N a N-th root of unity.

Now let us prove that for the N-th roots of unity, $\text{Im}(d_0) = \text{Ker}(d_1)$, which would imply the conclusion.

With the notation of section 7.1, we have an exact sequence

$$P_2 \xrightarrow{d_1^*} P_1 \xrightarrow{d_0^*} P_0 \xrightarrow{s} M^* \to 0.$$

Consider the modules $P_2' = \text{Im}(d_1^*)$ and $P_0' = \text{Im}(d_0^*)$. Then, by definition, we have the short exact sequence

$$0 \to P_2' \to P_1 \to P_0' \to 0.$$

By properties of Tor functors (see for example [14, chapter VI]), and because the modules P_1, P_0', P_2' are N-torsion free, we have the short exact sequence

$$0 \to P_2'/N \to P_1/N \to P_0'/N \to 0.$$

By taking the dual, we then get precisely that $\text{Im}(d_0) = \text{Ker}(d_1)$ for the N-th roots of unity, because for every i, we have $(P_i/N)^* = I_i[N]$, and $I_i[N]$ is the set of N-th roots of unity of $\overline{L_i}$.

Now let us show the second inclusion: $H^1_{\text{units},v} \supseteq \text{Ker}(\text{Res}\colon H^1 \to H^1_{\text{ram}})$.

Let x be an element of $\text{Ker}(\text{Res}\colon H^1 \to H^1_{\text{ram}})$, that is to say an element of $L_1^\times$ such that $\text{Res}(x) \in B^1_{\text{ram}}$. We want to show that there exists $z \in B^1$ such that $x \cdot z^{-1} \in \mathcal{O}_{L_1}^\times$.

As $\text{Res}(x)$ is in B^1_{ram}, there exists $y \in (L_0 \otimes K_v^{\text{ur}})^\times$ such that $d_0(\text{val}(y)) = \text{val}(\text{Res}(x))$. Besides, since x is in $L_1^\times$, then $\text{val}(\text{Res}(x))$ is invariant by the action of $\text{Gal}(K_v^{\text{ur}}/K)$.

So for all $g \in \text{Gal}(K_v^{\text{ur}}/K)$, $g \cdot d_0(\text{val}(y)) = d_0(\text{val}(y)) = d_0(g \cdot \text{val}(y))$. Since $d_0\colon \mathbb{Z}^{\text{Hom}(L_0, K_v^{\text{ur}})} \to \mathbb{Z}^{\text{Hom}(L_1, K_v^{\text{ur}})}$ is injective, that means $\text{val}(y)$ is also invariant by the action of $\text{Gal}(K_v^{\text{ur}}/K)$.

Therefore, $\mathrm{val}(y)$ is in $(\mathbb{Z}^{\mathrm{Hom}(L_0,K_v^{\mathrm{ur}})})^{(\mathrm{Gal}(K_v^{\mathrm{ur}}/K))}$, so there exists $z \in L_0^\times$ such that $\mathrm{val}(z) = \mathrm{val}(y)$.

And thus $\mathrm{val}(\mathrm{Res}(d_0(z))) = d_0(\mathrm{val}(z)) = d_0(\mathrm{val}(y)) = \mathrm{val}(\mathrm{Res}(x))$, hence $\mathrm{val}(\mathrm{Res}(d_0(z)x^{-1})) = 0$.

So, again by injectivity, $d_0(z) = x$, hence the conclusion.

□

Theorem 7.15. *If all prime ideals above S span $\mathrm{Cl}(L_0)$ and S contains all primes that divide $|M|$, then H^1_S is a Selmer group. More precisely, it is the Selmer group attached to the Selmer structure where all the conditions at places outside of S are unramified conditions and where there is no condition for the places in S.*

Proof. The theorem is a direct consequence of proposition 7.13 and proposition 7.14.

□

Remark 7.16. Since every Selmer group is contained in a H^1_S for some finite set of places S, this gives another proof that Selmer groups are finitely generated.

7.3 Algorithm and complexity

In this section, we will explain the algorithmic method to obtain a partial resolution of a finite Galois module M with permutation modules, as discussed in section 7.1 (See algorithm 7.18). Then, we will describe the algorithm to compute Selmer groups, (see algorithm 7.19) and discuss its complexity (see proposition 7.21).

But first, we have to explain how to represent in bits all the mathematical objects involved.

Let M be a finite Galois module, and G be the image of the action $\mathcal{G} \to \mathrm{Aut}(M)$. It is a finite group, so we can represent it as a subgroup of a permutation group. We can also suppose that we have a list $[g_1, \cdots, g_r]$ of generators.

Since M is a finite module, we can represent it as a list $[m_1, \cdots, m_s]$ of generators of M as an abelian group, and a list of relations, as well as a list of matrices giving the actions of the generators of G on the m_i.

We can represent a Selmer system $\mathcal{L}$, with a set of primes, indicating the places where the local conditions are not the unramified condition, a basis

of the local cohomology groups at these places and the generators of the subgroups in $\mathcal{L}$.

As for the Selmer group $\mathrm{Sel}_{\mathcal{L}}$, since it is a finitely generated group, we can represent it as a list of generators and a list of relations, or by its decomposition in cyclic factors, with the theorem of structure of finitely generated abelian groups.

Algorithm 7.17.

input: A finite group G and a finitely generated G-module N.
output: A permutation module P and a surjective morphism of G-modules $s\colon P \to N$.

- Let $(x_1, \cdots x_r)$ be a generating sequence of elements of N.
- For every element x in $\{x_1, \cdots, x_r\}$,
  - compute $H_x = \mathrm{Stab}_G(x)$ the stabilizer of x under the action of G.
  - Compute $f_x\colon \mathbb{Z}[G/H_x] \to N,\ 1 \cdot H_x \mapsto x$.
- Return $P = \bigoplus_{i=1}^{r} \mathbb{Z}[G/H_{x_i}]$ and $s = \sum_{i=1}^{r} f_{x_i}$.

Algorithm 7.18.
input: A finite Galois module M, of Galois group $\mathcal{G}$, and G the image of the action $\mathcal{G} \to \mathrm{Aut}(M)$.
output: Permutation modules P_i and morphisms of G-modules s and d_i^* such that the sequence

$$\cdots \xrightarrow{d_2^*} P_2 \xrightarrow{d_1^*} P_1 \xrightarrow{d_0^*} P_0 \xrightarrow{s} M^* \to 0$$

is exact.

1. Compute M^*, take $(x_1, \cdots, x_r)$ a finite generating sequence of elements of M^*.
2. Using algorithm 7.17, compute a permutation module P_0 as well as a surjective morphism of $\mathcal{G}$-module $s\colon P_0 \to M^*$
3. Compute the kernel K_0 of s.
4. Use algorithm 7.17 again, on K_0, to obtain P_1 and d_0^*.

5. Repeat the same process again to obtain all the P_i and the d_i^*.

Suppose we have a Selmer system $\mathcal{L}$, and we want to compute $\mathrm{Sel}_{\mathcal{L}}$, the Selmer group attached to $\mathcal{L}$ for M. Using the results in part 7.1 and 7.2, we deduce the following algorithm.

Algorithm 7.19.
input: A finite Galois module M, of Galois group $\mathcal{G}$, and G the image of the action $\mathcal{G} \to \mathrm{Aut}(M)$. A Selmer system $\mathcal{L}$.
output: The Selmer group $\mathrm{Sel}_{\mathcal{L}}$

- Use algorithm 7.18 to compute a resolution of M as in section 7.1.
- Let S be the smallest set of primes such that all conditions in $\mathcal{L}$ outside of S are the unramified condition and such that S spans the class group $\mathrm{Cl}(L_0)$ and S contains all the primes that divide $|M|$.
- Compute $H^1_S(G, M)$.
- Look for $\mathrm{Sel}_{\mathcal{L}}$ as a subgroup of the finitely generated group $H^1_S(G, M)$.

Theorem 7.20. *The algorithms 7.17, 7.18 and 7.19 are correct.*

Proof. The correctness of algorithms 7.17 and 7.18 are self explanatory, and the correctness of algorithm 7.19 is a consequence of theorem 7.15.

□

Proposition 7.21. *If we suppose that we have an oracle that can give us the S-units and the class group of any number fields, and another that can compute the fixed field of a subgroup of a Galois group, then the algorithm 7.19 has a time complexity polynomial in the size of the input and in $|M|$.*

Proof. First, let us prove that algorithm 7.18 has a time complexity polynomial in the size of M and G.

- If we have a finite G-module M given by a list of generators $[m_1, \cdots, m_s]$ and a list of matrices $[M_1, \cdots, M_r]$, as described above, then we can represent the dual module M^* by taking the inverse transpose of all the matrices, twisted by the cyclotomic character $\chi_{|M|}$.

Indeed, all elements of M are $|M|$-torsion, so $\mathrm{Hom}_{\mathbb{Z}}(M, \overline{K}^{\times}) = \mathrm{Hom}_{\mathbb{Z}}(M, \mu_{|M|})$ where $\mu_{|M|}$ is $\mathbb{Z}/|M|\mathbb{Z}$ as a $\mathcal{G}$-module where the action of $\mathcal{G}$ is given by the cyclotomic character $\chi_{|M|}$. So

$$\mathrm{Hom}_{\mathbb{Z}}(M, \overline{K}^{\times}) = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}/|M|\mathbb{Z}) \otimes \chi_{|M|},$$

and the dual module M^* is computed in polynomial time.

- We can compute the stabilizers $\mathrm{Stab}_G(x)$ in time polynomial in the size of M, using the method described in [30, Chapter 4.1].

- With the notations of section 7.1, the P_i are all free, finitely generated, $\mathbb{Z}$-modules, they can be represented as in [30, section 7.4.1].

  If $[g_1, \cdots, g_r]$ is a list of generators of G, let i be an integer, and let us fix $(p_{i,1}, \cdots, p_{i,d_i})$ be a $\mathbb{Z}$-basis of P_i. Then we can represent P_i as a list $[\alpha_1, \cdots, \alpha_r]$ where the α_j are the $(d_i \times d_i)$-matrices of the actions of the g_i on the basis $(p_{i,1}, \cdots, p_{i,d_i})$. So their size is still polynomial in the size of the input.

  And the morphisms of G-modules d_0 and d_1 can be represented as a list of co-sets, corresponding to their decompositions in Hecke operators (see fact 2.4) .

Once we apply algorithm 7.18, we obtain an exact sequence of the form

$$P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{s} M^* \to 0$$

and we represent d_0 and d_1 as a sum of cosets corresponding to Hecke operators. Then, with the notations of proposition 7.3, we can compute the number fields $L_{i,j} = \overline{K}^{H_{i,j}}$ thanks to the oracle.

Then, assuming the oracle gives us the S-units of all the $L_{i,j}$, with S easily accessible from the representation of the Selmer system $\mathcal{L}$ and from our oracle, computing the group $H^1_S(\mathcal{G}, M)$ boils down to computing the actions of Hecke operators on S-units, which takes polynomial time (see [22, Theorem 1.18]).

Finally, all there is left to do is to find a basis of $\mathrm{Sel}_{\mathcal{L}}$ as a subgroup of $H^1_S(G, M)$. This comes down to computing the kernel of the map

$$H^1_S(G, M) \to \prod_v \frac{H^1(G_v, M)}{L_v}.$$

□

Remark 7.22. To compute the fixed fields $L_{i,j} = \overline{K}^{H_{i,j}}$, one can use [24, algorithm 1]. However, we were unable to find a result in the literature about the complexity of this algorithm.

Conclusion

To conclude this thesis, let us sketch some possible continuations for our research.

- If G is a finite group, let $H, J_1, \cdots, J_\ell$ be non trivial subgroups of G, and let $\mathcal{J} = \{J_1, \cdots, J_\ell\}$. If there is a norm relation over $\mathbb{Q}$ with respect to H and $\mathcal{J}$. Then, by proposition 4.26, there exists an injective morphism of $\mathbb{Z}[G]$-module $\psi\colon \mathbb{Z}[G/H] \to \bigoplus_i \mathbb{Z}[G/J_i]^{n_i}$ with $n_i \in \mathbb{Z}_{\geq 0}$ for all i, and a morphism of $\mathbb{Z}[G]$-module $\phi\colon \bigoplus_i \mathbb{Z}[G/J_i]^{n_i} \to \mathbb{Z}[G/H]$ such that the image of ϕ has finite index in $\mathbb{Z}[G/H]$ and $\phi \circ \psi = c(\mathcal{J}, H) \cdot \mathrm{id}$. What's more, we have $c(\mathcal{J}, H) \big| |G|^2$. Then, by proposition 3.5, for every cohomological Mackey functor M, there exists $\phi_M\colon \bigoplus_{i=1}^m M(J_i) \to M(H)$ and $\psi_M\colon M(H) \to \bigoplus_{i=1}^m M(J_i)$ such that $\phi_M \circ \psi_M = c(\mathcal{J}, H) \cdot \mathrm{id}_{M(H)}$.

  In this thesis, we mainly use this result for the particular case where M is defined by $M(\Gamma) = \mathbb{Z}^\times_{\tilde{K}^\Gamma, S}$ for every $\Gamma < G$, for $\tilde{K}/\mathbb{Q}$ a Galois extension of number fields, of Galois group G, and for S a set of prime ideals of $\mathbb{Z}_{\tilde{K}}$. For further research, it would be interesting to look for other Mackey functors to apply this result to, and maybe find some algorithms similar to 5.9 to compute other objects inductively.

- Another open question would be to find a classification of all generalised norm relations, similar for example to the classification of Brauer relations given in [4].

- A very natural continuation to the research described in chapter 7 would be to actually implement algorithm 7.19. Moreover, the definition of Selmer groups can be extended to include not only subgroups of the first cohomology group H^1, but also all of the H^i. Although there would be some complications to overcome, one should be able to extend the method of chapter 7 to also compute Selmer groups in $H^2(G, M)$. We can also try to extend the method to be able to compute cup products, or other cohomological operations or pairings.

Appendix

The tables below give a list of norm relations in groups of order less than 720. For every row of the tables, G is a finite group, $\tilde{K}$ is a number field such that $\tilde{K}/\mathbb{Q}$ is a Galois extension of Galois group G. So the degree of $\tilde{K}$ is the order of G. We also have H a subgroup of G, and K is the number field defined by $K = \tilde{K}^H$. We define K_{J_1} to be the largest degree number field on which one would have to use Buchmann's algorithm, in order to compute $\mathrm{Cl}(K)$ using only classical norm relations, in any quotient of G. We can have $K_{J_1} = K$ when there are no relevant classical norm relations. Similarly, K_{J_2} is the largest degree number field on which one would have to use Buchmann's algorithm, in order to compute $\mathrm{Cl}(K)$ using generalised norm relations. The tables were obtained by enumerating every groups G of order n, for every n less than 720 (we skipped $n = 256, 384, 512, 576, 640$). Then for every G, we enumerated every subgroups H up to conjugacy classes, and computed the degrees of K_{J_1} and K_{J_2}. Here we display the examples where the degree of K_{J_2} is strictly lower than the degree of K_{J_1}.

Note that some rows can seem to be repeated. It can mean either that the group G differs between the two rows, but has the same structure description (which can happen in the case of a semi direct product for example), or that the subgroup H differs but has the same structure description (which can happen if G contains several copies of H that are not in the same conjugacy classe).

All of the calculation were done using sagemath (see [18]) and in particular the GAP library (see [26]).

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
S_4	24	$C_2 \times C_2$	6	6	4
A_5	60	$C_2 \times C_2$	15	12	6
A_5	60	S_3	10	10	6
$(S_3 \times S_3) \rtimes C_2$	72	D_8	9	9	6
$C_3 \times S_4$	72	$C_2 \times C_2$	18	18	12
$((C_4 \times C_2) \rtimes C_4) \rtimes C_3$	96	C_3	32	24	12
$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2$	96	$C_2 \times C_2 \times C_2$	12	6	4
$((C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2)$	108	S_3	18	18	9
S_5	120	$C_2 \times C_2$	30	15	10
S_5	120	S_3	20	20	10
S_5	120	D_8	15	15	10
S_5	120	D_{10}	12	12	10
$C_5 \times S_4$	120	$C_2 \times C_2$	30	30	20
$(C_2 \times (C_4 \rtimes C_4))_4$	128	C_2	64	16	8
$(C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	144	S_3	24	12	9
$(C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	144	D_8	18	18	9
$(C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	144	D_12	12	12	9
$S_3 \times S_4$	144	$C_2 \times C_2$	36	18	12
$S_3 \times S_4$	144	$C_2 \times C_2 \times C_2$	18	18	12
$S_3 \times S_4$	144	D_8	18	18	12
$(C_5 \times C_5) \rtimes S_3$	150	S_3	25	25	15
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes C_2$	162	S_3	27	18	9
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes C_2$	162	S_3	27	18	9
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes C_2$	162	S_3	27	18	9
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes C_2$	162	S_3	27	18	9
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes C_2$	162	S_3	27	18	9
$PSL(3,2)$	168	S_3	28	28	21
$PSL(3,2)$	168	C_7	24	24	21
$PSL(3,2)$	168	A_4	14	14	8
$PSL(3,2)$	168	A_4	14	14	8
$(C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3)$	168	A_4	14	14	8
$C_7 \times S_4$	168	$C_2 \times C_2$	42	42	28
$\mathrm{GL}(2,4)$	180	S_3	30	30	15
$\mathrm{GL}(2,4)$	180	D_{10}	18	18	15
$(C_4 \cdot (C_4 \times C_4))_3$	192	A_4	16	16	8
$C_2 \cdot (((C_4 \times C_4) \rtimes C_3) \rtimes C_2)$	192	C_3	64	48	24
$SL(2,3) \rtimes C_8$	192	C_3	64	32	24
$C_2 \times (((C_4 \times C_2) \rtimes C_4) \rtimes C_3)$	192	C_3	64	24	12
$((C_2 \times ((C_4 \times C_2) \rtimes C_2))_2)_3$	192	C_3	64	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_2	96	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_3	64	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_4	48	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_4	48	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	$C_2 \times C_2$	48	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_4	48	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_6	32	24	16
$(((C_4 \times C_2) \rtimes C_4)_2)_3$	192	C_6	32	24	16
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2) \rtimes C_2) \rtimes C_3$	192	A_4	16	16	8
$(((C_4 \times C_2 \times C_2) \rtimes C_2)_2) \rtimes C_3$	192	A_4	16	16	6
$(((C_4 \times C_2 \times C_2) \rtimes C_2)_2) \rtimes C_3$	192	A_4	16	16	8

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$(C_2 \times C_2) \cdot (C_2 \times S_4)$	192	C_3	64	32	24
$SL(2,3)_8$	192	C_3	64	32	24
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times C_2 \times C_2$	24	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times C_2 \times C_2$	24	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times C_2 \times C_2$	24	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	D_8	24	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	D_{12}	16	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times D_8$	12	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times D_8$	12	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times D_8$	12	12	8
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_3)_2$	192	$C_2 \times D_8$	12	12	8
$((C_4 \times Q_8) \rtimes C_2) \rtimes C_3$	192	C_3	64	48	24
$(Q_8 \times Q_8) \rtimes C_3$	192	C_3	64	32	24
$(((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2))_3)_2$	192	A_4	16	16	8
$((C_2 \times ((C_4 \times C_2) \rtimes C_2))_2) \rtimes C_3$	192	A_4	16	16	6
$((C_2 \times ((C_4 \times C_2) \rtimes C_2))_2) \rtimes C_3$	192	A_4	16	16	6
$((C_2 \times ((C_4 \times C_2) \rtimes C_2))_2) \rtimes C_3$	192	A_4	16	16	6
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	$C_2 \times C_2$	48	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	$C_2 \times C_2$	48	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	$C_2 \times C_2$	48	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	$C_2 \times C_2 \times C_2$	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$C_2 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	192	D_8	24	12	8
$(C_5 \times C_5) \rtimes D_8$	200	D_8	25	20	10
$((C_3 \times C_3) \rtimes C_3) \rtimes C_8$	216	S_3	36	36	27
$((C_3 \times C_3) \rtimes C_3) \rtimes Q_8$	216	S_3	36	36	27
$C_9 \times S_4$	216	$C_2 \times C_2$	54	54	36
$((C_3 \times C_3) \rtimes Q_8) \rtimes C_3$	216	$C_3 \times C_3$	24	12	9
$((C_3 \times C_3) \rtimes Q_8) \rtimes C_3$	216	$C_3 \times S_3$	12	12	9
$C_3 \times ((S_3 \times S_3) \rtimes C_2)$	216	D_8	27	24	12
$(C_3 \times C_3 \times C_3) \rtimes D_8$	216	$C_2 \times C_2$	54	24	12
$(C_3 \times C_3 \times C_3) \rtimes D_8$	216	C_6	36	24	12
$(C_3 \times C_3 \times C_3) \rtimes D_8$	216	D_8	27	24	12
$C_3 \times C_3 \times S_4$	216	$C_2 \times C_2$	54	18	12
$SL(2,5) \rtimes C_2$	240	C_5	48	48	40
$A_5 \rtimes C_4$	240	S_3	40	24	20
$C_2 \times S_5$	240	$C_2 \times C_2$	60	20	12
$C_2 \times S_5$	240	S_3	40	20	12
$C_2 \times S_5$	240	D_8	30	20	12
$C_2 \times S_5$	240	D_8	30	20	12
$C_2 \times S_5$	240	D_{12}	20	20	12
$C_2 \times S_5$	240	D_{12}	20	20	12
$D_{10} \times S_4$	240	$C_2 \times C_2$	60	30	20
$D_{10} \times S_4$	240	$C_2 \times C_2 \times C_2$	30	30	20

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$D_{10} \times S_4$	240	D_8	30	30	20
$C_{11} \times S_4$	264	$C_2 \times C_2$	66	66	44
$((C_2 2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes (C_3 \times C_3)$	288	$C_3 \times C_3$	32	32	24
$A_4 \times S_4$	288	$C_2 \times C_2$	72	18	16
$A_4 \times S_4$	288	$C_2 \times C_2 \times C_2$	36	18	16
$A_4 \times S_4$	288	D_8	36	18	16
$A_4 \times S_4$	288	$C_6 \times C_2$	24	18	16
$A_4 \times S_4$	288	$C_2 \times D_8$	18	18	16
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)_3$	288	$C_3 \times C_3$	32	24	18
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)_3$	288	$C_3 \times S_3$	16	16	12
$(A_4 \times A_4) \rtimes C_2$	288	$C_2 \times C_2 \times C_2$	36	18	12
$(A_4 \times A_4) \rtimes C_2$	288	$C_4 \times C_2$	36	18	12
$(A_4 \times A_4) \rtimes C_2$	288	D_{12}	24	18	12
$(A_4 \times A_4) \rtimes C_2$	288	D_{12}	24	18	12
$(A_4 \times A_4) \rtimes C_2$	288	$C_2 \times D_8$	18	18	12
$(A_4 \times A_4) \rtimes C_2$	288	$(C_3 \times C_3)_2$	16	16	12
$C_3 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	288	$C_2 \times C_2 \times C_2$	36	18	12
$(C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3)) \rtimes C_2$	288	$C_2 \times C_2$	72	18	12
$(C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3)) \rtimes C_2$	288	$C_2 \times C_2 \times C_2$	36	18	12
$(C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3)) \rtimes C_2$	288	$C_4 \times C_2$	36	18	12
$(C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3)) \rtimes C_2$	288	$C_4 \times C_2$	36	18	12
$(C_3 \times ((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3)) \rtimes C_2$	288	$C_4 \times C_2$	36	18	12
$(C_7 \times C_7) \rtimes S_3$	294	S_3	49	42	21
$C_5 \times A_5$	300	$C_2 \times C_2$	75	60	30
$C_5 \times A_5$	300	S_3	50	60	30
$(C_5 \times C_5) \rtimes D_{12}$	300	D_{12}	25	25	15
$C_1 3 \times S_4$	312	$C_2 \times C_2$	78	78	52
$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_4$	320	$C_2 \times C_2 \times C_2$	40	20	16
$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_4$	320	D_{10}	32	20	16
$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_4$	320	$(C_4 \times C_2) \rtimes C_2$	20	20	16
$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_4$	320	$C_2 \times D_8$	20	20	16
$((C_3 \times C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2)$	324	D_{12}	27	18	9
$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes (C_2 \times C_2)$	324	S_3	54	18	12
$((C_9 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2)$	324	S_3	54	54	27
$PSL(3,2) \rtimes C_2$	336	A_4	28	28	16
$PSL(3,2) \rtimes C_2$	336	D_{12}	28	28	21
$PSL(3,2) \rtimes C_2$	336	D_{14}	24	24	21
$C_2 \times PSL(3,2)$	336	$C_7 \rtimes C_3$	16	16	14
$C_2 \times ((C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3))$	336	$C_7 \rtimes C_3$	16	16	14
$D_{14} \times S_4$	336	$C_2 \times C_2$	84	42	28
$D_{14} \times S_4$	336	$C_2 \times C_2 \times C_2$	42	42	28
$D_{14} \times S_4$	336	D_8	42	42	28
A_6	360	$(C_3 \times C_3) \rtimes C_2$	20	20	10
A_6	360	S_4	15	15	10
A_6	360	S_4	15	15	10
$C_3 \times S_5$	360	S_3	60	60	30
$C_3 \times S_5$	360	D_{10}	36	36	30
$C_3 \rtimes S_5$	360	S_3	60	30	15
$C_3 \rtimes S_5$	360	D_{10}	36	18	15
$C_3 \rtimes S_5$	360	D_{12}	30	30	15

G	degree of $\check{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$C_3 \rtimes S_5$	360	$C_5 \rtimes C_4$	18	18	15
$A_5 \times S_3$	360	$C_2 \times C_2$	90	30	18
$A_5 \times S_3$	360	S_3	60	30	18
$A_5 \times S_3$	360	$C_2 \times C_2 \times C_2$	45	30	18
$A_5 \times S_3$	360	A_4	30	30	18
$A_5 \times S_3$	360	D_{12}	30	30	18
$C_6 \times A_5$	360	S_3	60	36	30
$C_6 \times A_5$	360	D_{10}	36	36	30
$C_5 \times ((S_3 \times S_3) \rtimes C_2)$	360	D_8	45	45	30
$(C_3 \times C_3) \rtimes ((C_{10} \times C_2) \rtimes C_2)$	360	$C_2 \times C_2$	90	45	30
$(C_3 \times C_3) \rtimes ((C_{10} \times C_2) \rtimes C_2)$	360	D_8	45	45	30
$C_{15} \times S_4$	360	$C_2 \times C_2$	90	90	60
$(C_5 \times C_5) \rtimes ((C_4 \times C_2)_2)$	400	$(C_4 \times C_2) \rtimes C_2$	25	20	10
$(C_{17} \times S_4$	408	$C_2 \times C_2$	102	102	68
$C_7 \times A_5$	420	$C_2 \times C_2$	105	84	42
$C_7 \times A_5$	420	S_3	70	70	42
$((C_3 \times C_3) \rtimes C_3) \rtimes \mathrm{QD}_{16}$	432	S_3	72	36	27
$((C_3 \times C_3) \rtimes C_3) \rtimes \mathrm{QD}_{16}$	432	D_{12}	36	36	27
$D_{18} \times S_4$	432	$C_2 \times C_2$	108	54	36
$D_{18} \times S_4$	432	$C_2 \times C_2 \times C_2$	54	54	36
$D_{18} \times S_4$	432	D_8	54	54	36
$C_2 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_8)$	432	S_3	72	72	54
$(((C_3 \times C_3) \rtimes Q_8) \rtimes C_3) \rtimes C_2$	432	$C_3 \times C_3$	48	24	18
$(((C_3 \times C_3) \rtimes Q_8) \rtimes C_3) \rtimes C_2$	432	$C_3 \times S_3$	24	24	18
$(((C_3 \times C_3) \rtimes Q_8) \rtimes C_3) \rtimes C_2$	432	$(C_3 \times C_3) \rtimes C_2$	24	12	9
$(((C_3 \times C_3) \rtimes Q_8) \rtimes C_3) \rtimes C_2$	432	$C_3 \times S_3$	24	24	18
$(((C_3 \times C_3) \rtimes Q_8) \rtimes C_3) \rtimes C_2$	432	$S_3 \times S_3$	12	12	9
$C_2 \times (((C_3 \times C_3) \rtimes Q_8) \rtimes C_3)$	432	$C_3 \times C_3$	48	24	18
$C_2 \times (((C_3 \times C_3) \rtimes Q_8) \rtimes C_3)$	432	$C_3 \times S_3$	24	24	18
$C_2 \times (((C_3 \times C_3) \rtimes Q_8) \rtimes C_3)$	432	$C_3 \times S_3$	24	24	18
$C_3 \times ((C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	432	D_8	54	48	24
$C_3 \times ((C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	432	QD_{16}	27	27	24
$(C_3 \times C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	432	D_8	54	27	24
$(C_3 \times C_3 \times C_3) \rtimes \mathrm{QD}_{16}$	432	QD_{16}	27	27	24
$((S_3 \times S_3) \rtimes C_2) \times S_3$	432	D_8	54	24	12
$((S_3 \times S_3) \rtimes C_2) \times S_3$	432	$C_2 \times D_8$	27	24	12
$C_3 \times S_3 \times S_4$	432	$C_2 \times C_2$	108	36	24
$C_3 \times S_3 \times S_4$	432	$C_2 \times C_2 \times C_2$	54	36	24
$C_3 \times S_3 \times S_4$	432	D_8	54	36	24
$C_3 \times S_3 \times S_4$	432	$C_6 \times C_2$	36	36	24
$((C_3 \times C_3) \rtimes C_2) \times S_4$	432	$C_2 \times C_2$	108	18	12
$((C_3 \times C_3) \rtimes C_2) \times S_4$	432	D_8	54	18	12
$((C_3 \times C_3) \rtimes C_2) \times S_4$	432	$C_2 \times C_2 \times C_2$	54	18	12
$C_3 \times ((C_5 \times C_5) \rtimes S_3)$	450	S_3	75	75	45
$C_{19} \times S_4$	456	$C_2 \times C_2$	114	114	76
$C_4 \rtimes S_5$	480	$C_2 \times C_2$	120	40	20
$C_4 \rtimes S_5$	480	S_3	80	40	20
$C_4 \rtimes S_5$	480	D_8	60	40	20
$C_4 \rtimes S_5$	480	D_8	60	40	20
$C_4 \rtimes S_5$	480	D_{12}	40	40	20

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$C_4 \rtimes S_5$	480	D_{12}	40	40	20
$A_5 \rtimes Q_8$	480	S_3	80	48	40
$SL(2,5) \rtimes (C_2 \times C_2)$	480	C_5	96	48	40
$SL(2,5) \rtimes (C_2 \times C_2)$	480	D_{10}	48	48	40
$C_2 \times (SL(2,5) \rtimes C_2)$	480	C_5	96	48	40
$C_2 \times (A_5 \rtimes C_4)$	480	S_3	80	24	20
$C_5 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	480	A_4	40	40	20
$C_5 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	480	A_4	40	40	20
$C_5 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	480	A_4	40	40	20
$C_2 \times C_2 \times S_5$	480	$C_2 \times C_2$	120	20	12
$C_2 \times C_2 \times S_5$	480	S_3	80	20	12
$C_2 \times C_2 \times S_5$	480	D_8	60	20	12
$C_2 \times C_2 \times S_5$	480	D_8	60	20	12
$C_2 \times C_2 \times S_5$	480	D_8	60	20	12
$C_2 \times C_2 \times S_5$	480	D_8	60	20	12
$C_2 \times C_2 \times S_5$	480	D_{12}	40	20	12
$C_2 \times C_2 \times S_5$	480	D_{12}	40	20	12
$C_2 \times C_2 \times S_5$	480	D_{12}	40	20	12
$C_2 \times C_2 \times S_5$	480	D_{12}	40	20	12
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_2) \rtimes C_3$	480	$C_2 \times C_2 \times C_2$	60	20	16
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_2) \rtimes C_3$	480	D_{10}	48	30	16
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_2) \rtimes C_3$	480	$C_2 \times D_8$	30	20	16
$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5) \rtimes C_2) \rtimes C_3$	480	$C_2 \times A_4$	20	20	16
$(C_5 \rtimes C_4) \times S_4$	480	$C_2 \times C_2$	120	30	20
$(C_5 \rtimes C_4) \times S_4$	480	D_8	60	30	20
$(C_5 \rtimes C_4) \times S_4$	480	$C_2 \times C_2 \times C_2$	60	30	20
$(C_5 \rtimes C_4) \times S_4$	480	$(C_4 \times C_2) \rtimes C_2$	30	30	20
$(C_5 \rtimes C_4) \times S_4$	480	$C_4 \times C_2 \times C_2$	30	30	20
$C_5 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_2 \times C_2 \times C_2$	60	30	20
$C_5 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_2 \times C_2$	120	30	20
$C_5 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_4 \times C_2$	60	30	20
$C_5 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_4 \times C_2$	60	30	20
$C_5 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_4 \times C_2$	60	30	20
$C_5 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	480	$C_2 \times C_2 \times C_2$	60	30	20
$(((C_9 \times C_3) \rtimes C_3) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_3 \times (C_9 \rtimes C_3)) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_3 \times (C_9 \rtimes C_3)) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_3 \times (C_9 \rtimes C_3)) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_3 \times (C_9 \rtimes C_3)) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_3 \cdot (C_3 \times C_3) \rtimes C_3) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$(((C_3 \times C_3 \times C_3) \rtimes C_3)_2$	486	S_3	81	54	27
$(((C_3 \times C_3 \times C_3) \rtimes C_3)_2$	486	S_3	81	54	27
$((C_9 \rtimes C_9) \rtimes C_3) \rtimes C_2$	486	S_3	81	54	27
$((C_5 \times C_5) \rtimes C_5) \rtimes (C_2 \times C_2)$	500	D_{10}	50	50	25
$((C_5 \times C_5) \rtimes C_5) \rtimes (C_2 \times C_2)$	500	D_{10}	50	50	25
$PSL(2,8)$	504	$C_2 \times C_2 \times C_2$	63	56	28
$PSL(2,8)$	504	D_{14}	36	36	28
$C_3 \times PSL(3,2)$	504	$C_2 \times C_2$	126	42	24
$C_3 \times PSL(3,2)$	504	$C_2 \times C_2$	126	42	24
$C_3 \times PSL(3,2)$	504	S_3	84	84	24

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$C_3 \times PSL(3,2)$	504	D_8	63	42	24
$C_3 \times PSL(3,2)$	504	A_4	42	42	24
$C_3 \times PSL(3,2)$	504	A_4	42	42	24
$C_3 \times PSL(3,2)$	504	A_4	42	42	24
$C_3 \times PSL(3,2)$	504	A_4	42	42	24
$(C_7 \rtimes C_3) \times S_4$	504	$C_2 \times C_2$	126	42	28
$(C_7 \rtimes C_3) \times S_4$	504	$C_6 \times C_2$	42	42	28
$C_7 \times ((S_3 \times S_3) \rtimes C_2)$	504	D_8	63	63	42
$(C_3 \times C_3) \rtimes ((C_{14} \times C_2)_2)$	504	$C_2 \times C_2$	126	84	42
$(C_3 \times C_3) \rtimes ((C_{14} \times C_2)_2)$	504	D_8	63	63	42
$C_{21} \times S_4$	504	$C_2 \times C_2$	126	126	84
$D_{22} \times S_4$	528	$C_2 \times C_2$	132	66	44
$D_{22} \times S_4$	528	$C_2 \times C_2 \times C_2$	66	66	44
$D_{22} \times S_4$	528	D_8	66	66	44
$C_9 \times A_5$	540	S_3	90	90	45
$C_9 \times A_5$	540	D_{10}	54	54	45
$C_5 \times (((C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2))$	540	S_3	90	90	45
$((C_3 \times C_3) \rtimes C_3) \rtimes D_{20}$	540	S_3	90	90	45
$C_3 \times C_3 \times A_5$	540	S_3	90	30	15
$C_3 \times C_3 \times A_5$	540	D_{10}	54	18	15
$C_{23} \times S_4$	552	$C_2 \times C_2$	138	138	92
$(C_7 \times C_7) \rtimes D_{12}$	588	D_{12}	49	42	21
$C_5 \rtimes S_5$	600	D_{12}	50	50	30
$A_5 \times D_{10}$	600	D_{12}	50	50	30
$(C_5 \times C_5) \rtimes (C_4 \times S_3)$	600	D_{12}	50	30	15
$D_{26} \times S_4$	624	$C_2 \times C_2$	156	78	52
$D_{26} \times S_4$	624	$C_2 \times C_2 \times C_2$	78	78	52
$D_{26} \times S_4$	624	D_8	78	78	52
$C_{27} \times S_4$	648	$C_2 \times C_2$	162	162	108
$(C_2 \times C_2 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)) \rtimes C_3$	648	S_3	108	54	36
$(C_2 \times C_2 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)) \rtimes C_3$	648	D_{12}	54	54	36
$(C_2 \times C_2 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)) \rtimes C_3$	648	D_{12}	54	54	36
$(C_2 \times C_2 \times (((C_3 \times C_3) \rtimes C_3) \rtimes C_2)) \rtimes C_3$	648	D_{12}	54	54	36
$C_3 \cdot (((C_3 \times C_3) \rtimes Q_8) \rtimes C_3)$	648	S_3	108	108	81
$(((C_3 \times C_3) \rtimes C_3) \rtimes Q_8) \rtimes C_3$	648	S_3	108	108	81
$(((C_3 \times C_3) \rtimes C_3) \rtimes Q_8) \rtimes C_3$	648	S_3	108	36	27
$(((C_3 \times C_3) \rtimes C_3) \rtimes Q_8) \rtimes C_3$	648	$C_3 \times S_3$	36	36	27
$(((C_3 \times C_3) \rtimes C_3) \rtimes Q_8) \rtimes C_3$	648	$C_3 \times S_3$	36	36	27
$(((C_3 \times C_3) \rtimes C_3) \rtimes Q_8) \rtimes C_3$	648	$C_3 \times S_3$	36	36	27
$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes Q_8$	648	S_3	108	36	27
$((C_9 \times C_3) \rtimes C_3) \rtimes C_8$	648	S_3	108	108	81
$C_9 \times ((S_3 \times S_3) \rtimes C_2)$	648	D_8	81	72	36
$(C_9 \times C_3 \times C_3) \rtimes D_8$	648	$C_2 \times C_2$	162	72	36
$(C_9 \times C_3 \times C_3) \rtimes D_8$	648	C_6	108	72	36
$(C_9 \times C_3 \times C_3) \rtimes D_8$	648	D_8	81	72	36
$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes D_8$	648	S_3	108	36	24
$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes D_8$	648	D_{12}	54	36	18
$(C_3 \times ((C_3 \times C_3) \rtimes C_3)) \rtimes D_8$	648	$C_3 \times S_3$	36	36	18
$C_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes Q_8)$	648	S_3	108	36	27
$((C_9 \times C_3) \rtimes C_3) \rtimes Q_8$	648	S_3	108	108	81

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$S_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2))$	648	S_3	108	36	18
$S_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2))$	648	D_{12}	54	36	18
$S_3 \times (((C_3 \times C_3) \rtimes C_3) \rtimes (C_2 \times C_2))$	648	$C_3 \times S_3$	36	36	18
$C_3 \times C_9 \times S_4$	648	$C_2 \times C_2$	162	54	36
$((C_3 \times C_3)_3) \times S_4$	648	$C_2 \times C_2$	162	54	36
$((C_3 \times C_3)_3) \times S_4$	648	$C_6 \times C_2$	54	54	36
$((C_3 \times C_3)_3) \times S_4$	648	$C_6 \times C_2$	54	54	36
$((C_3 \times C_3)_3) \times S_4$	648	$C_6 \times C_2$	54	54	36
$((C_3 \times C_3)_3) \times S_4$	648	$C_6 \times C_2$	54	54	36
$(C_9 \rtimes C_3) \times S_4$	648	$C_2 \times C_2$	162	54	36
$(C_9 \rtimes C_3) \times S_4$	648	$C_6 \times C_2$	54	54	36
$(((C_3 \times C_3) \rtimes C_3) \times A_4) \rtimes C_2$	648	D_{12}	54	54	36
$(((C_3 \times C_3) \rtimes C_3) \times A_4) \rtimes C_2$	648	D_{12}	54	54	36
$(((C_3 \times C_3) \rtimes C_3) \times A_4) \rtimes C_2$	648	D_{12}	54	54	36
$(((C_3 \times C_3) \rtimes C_3) \times A_4) \rtimes C_2$	648	D_{12}	54	54	36
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	D_{12}	54	36	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	$(C_3 \times C_3) \rtimes C_2$	36	36	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	D_{18}	36	36	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	D_{18}	36	36	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	S_4	27	27	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	D_{24}	27	27	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	D_{12}	54	36	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	$(C_6 \times C_2) \rtimes C_2$	27	27	18
$(((C_3 \times C_3 \times C_3) \rtimes (C_2 \times C_2)) \rtimes C_3) \rtimes C_2$	648	S_4	27	27	18
$(S_3 \times S_3 \times S_3) \rtimes C_3$	648	C_6	108	36	24
$(S_3 \times S_3 \times S_3) \rtimes C_3$	648	$C_2 \times C_2 \times C_2$	81	36	24
$(S_3 \times S_3 \times S_3) \rtimes C_3$	648	D_{12}	54	36	24
$(S_3 \times S_3 \times S_3) \rtimes C_3$	648	$C_2 \times A_4$	27	27	18
$C_3 \times C_3 \times ((S_3 \times S_3) \rtimes C_2)$	648	D_8	81	24	12
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	$C_2 \times C_2$	162	24	12
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	D_8	81	24	12
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	$C_3 \times S_3$	36	24	12
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	$C_3 \times S_3$	36	24	12
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	$C_3 \times C_3$	72	12	9
$(C_3 \times C_3 \times C_3 \times C_3) \rtimes D_8$	648	$(C_3 \times C_3)_2$	36	12	9
$C_3 \times C_3 \times C_3 \times S_4$	648	$C_2 \times C_2$	162	18	12
$C_{11} \times A_5$	660	$C_2 \times C_2$	165	132	66
$C_{11} \times A_5$	660	S_3	110	110	66
$C_7 \times (((C_4 \times C_2)_4) \rtimes C_3)$	672	C_3	224	168	84
$PSL(3,2) \rtimes C_4$	672	$C_7 \rtimes C_3$	32	32	28
$C_4 \times PSL(3,2)$	672	$C_7 \rtimes C_3$	32	32	28
$C_4 \times ((C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3))$	672	$C_7 \rtimes C_3$	32	32	14
$C_4 \times ((C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3))$	672	$C_2 \times A_4$	28	28	14
$C_7 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	672	A_4	56	56	28
$C_7 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	672	A_4	56	56	28
$C_7 \times (((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3)$	672	A_4	56	56	28
$C_2 \times (PSL(3,2) \rtimes C_2)$	672	S_4	28	28	16
$C_2 \times C_2 \times PSL(3,2)$	672	$C_7 \rtimes C_3$	32	16	14
$C_2 \times C_2 \times ((C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3))$	672	$C_7 \rtimes C_3$	32	16	14
$C_7 \times (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_2 \times C_2 \times C_2$	84	42	28

G	degree of $\check{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$C_7 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_2 \times C_2$	168	42	28
$C_7 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_4 \times C_2$	84	42	28
$C_7 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_4 \times C_2$	84	42	28
$C_7 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_4 \times C_2$	84	42	28
$C_7 \rtimes (((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2)$	672	$C_2 \times C_2 \times C_2$	84	42	28
$C_{29} \times S_4$	696	$C_2 \times C_2$	174	174	116
$A_5 \times (C_3 \rtimes C_4)$	720	S_3	120	72	60
$A_5 \times (C_3 \rtimes C_4)$	720	D_{10}	72	72	60
$C_{12} \times A_5$	720	S_3	120	72	60
$C_{12} \times A_5$	720	D_{10}	72	72	60
S_6	720	$C_3 \times C_3$	80	36	30
S_6	720	$C_3 \times S_3$	40	36	30
S_6	720	$C_3 \times S_3$	40	36	30
S_6	720	S_4	30	30	20
S_6	720	S_4	30	30	20
S_6	720	$S_3 \times S_3$	20	20	12
S_6	720	$S_3 \times S_3$	20	20	12
S_6	720	$C_2 \times S_4$	15	15	10
S_6	720	$C_2 \times S_4$	15	15	10
$A_6 \rtimes C_2$	720	D_8	90	72	60
$A_6 \rtimes C_2$	720	$C_3 \times C_3$	80	72	60
$A_6 \rtimes C_2$	720	D_{10}	72	72	60
$A_6 \rtimes C_2$	720	D_{16}	45	45	36
$A_6 \rtimes C_2$	720	$(C_3 \times C_3) \rtimes C_2$	40	40	20
$A_6 \rtimes C_2$	720	S_4	30	20	20
$A_6 \cdot C_2$	720	D_8	90	60	36
$A_6 \cdot C_2$	720	D_{10}	72	60	36
$A_6 \cdot C_2$	720	QD_{16}	45	45	36
$A_6 \cdot C_2$	720	S_4	30	30	20
$A_6 \cdot C_2$	720	$(C_3 \times C_3) \rtimes C_4$	20	20	12
$A_6 \cdot C_2$	720	$(C_3 \times C_3) \rtimes C_4$	20	20	12
$C_2 \times A_6$	720	$(C_3 \times C_3)$	80	40	30
$C_2 \times A_6$	720	$(C_3 \times C_3) \rtimes C_2$	40	40	30
$C_2 \times A_6$	720	S_4	30	30	20
$C_2 \times A_6$	720	S_4	30	30	20
$C_2 \times A_6$	720	$(C_3 \times C_3) \rtimes C_4$	20	20	12
$S_5 \times S_3$	720	S_3	120	60	30
$S_5 \times S_3$	720	D_{10}	72	60	30
$S_5 \times S_3$	720	D_{12}	60	60	30
$S_5 \times S_3$	720	D_{12}	60	60	30
$S_5 \times S_3$	720	D_{20}	36	36	30
$S_5 \times S_3$	720	$C_5 \rtimes C_4$	36	36	30
$A_5 \times A_4$	720	$C_2 \times C_2$	180	36	24
$A_5 \times A_4$	720	S_3	120	36	24
$A_5 \times A_4$	720	$C_2 \times C_2 \times C_2$	90	36	24
$A_5 \times A_4$	720	$C_6 \times C_2$	60	36	24
$A_5 \times A_4$	720	A_4	60	36	24
$A_5 \times A_4$	720	A_4	60	36	24
$A_5 \times A_4$	720	D_{12}	60	36	24
$A_5 \times A_4$	720	$C_3 \times S_3$	40	36	24

G	degree of $\check{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
$C_6 \times S_5$	720	$C_2 \times C_2$	180	60	36
$C_6 \times S_5$	720	S_3	120	60	36
$C_6 \times S_5$	720	D_8	90	60	36
$C_6 \times S_5$	720	D_8	90	60	36
$C_6 \times S_5$	720	D_{12}	60	60	36
$C_6 \times S_5$	720	D_{12}	60	60	36
$C_6 \times S_5$	720	A_4	60	60	36
$C_2 \times (A_5 \rtimes S_3)$	720	S_3	120	60	30
$C_2 \times (A_5 \rtimes S_3)$	720	D_{10}	72	60	30
$C_2 \times (A_5 \rtimes S_3)$	720	D_{12}	60	60	30
$C_2 \times (A_5 \rtimes S_3)$	720	D_{12}	60	60	30
$C_2 \times (A_5 \rtimes S_3)$	720	$C_5 \rtimes C_4$	36	36	30
$C_2 \times (A_5 \rtimes S_3)$	720	$C_5 \rtimes C_4$	36	36	30
$C_2 \times C_6 \times A_5$	720	S_3	120	36	30
$C_2 \times C_6 \times A_5$	720	D_{10}	72	36	30
$(C_3 \times C_3) \rtimes ((C_{10} \times C_2) \rtimes C_4)$	720	$C_2 \times C_2$	180	45	30
$(C_3 \times C_3) \rtimes ((C_{10} \times C_2) \rtimes C_4)$	720	$C_2 \times C_2 \times C_2$	90	45	30
$(C_3 \times C_3) \rtimes ((C_{10} \times C_2) \rtimes C_4)$	720	$(C_4 \times C_2) \rtimes C_2$	45	45	30
$C_5 \times ((C_3 \times C_3) \rtimes \mathrm{QD}_{16})$	720	S_3	120	60	45
$C_5 \times ((C_3 \times C_3) \rtimes \mathrm{QD}_{16})$	720	D_8	90	90	45
$C_5 \times ((C_3 \times C_3) \rtimes \mathrm{QD}_{16})$	720	D_{12}	60	60	45
$(C_3 \times C_3) \rtimes ((C_5 \rtimes Q_8) \rtimes C_2)$	720	S_3	120	60	45
$(C_3 \times C_3) \rtimes ((C_5 \rtimes Q_8) \rtimes C_2)$	720	D_{12}	60	60	45
$((S_3 \times S_3) \rtimes C_2) \times D_{10}$	720	$C_2 \times D_8$	45	45	30
$C_3 \times D_{10} \times S_4$	720	$C_2 \times C_2$	180	90	60
$C_3 \times D_{10} \times S_4$	720	$C_2 \times C_2 \times C_2$	90	90	60
$C_3 \times D_{10} \times S_4$	720	D_8	90	90	60
$C_5 \times S_3 \times S_4$	720	$C_2 \times C_2$	180	90	60
$C_5 \times S_3 \times S_4$	720	D_8	90	90	60
$C_5 \times S_3 \times S_4$	720	$C_2 \times C_2 \times C_2$	90	90	60
$D_{30} \times S_4$	720	$C_2 \times C_2$	180	90	60
$D_{30} \times S_4$	720	D_8	90	90	60
$D_{30} \times S_4$	720	$C_2 \times C_2 \times C_2$	90	90	60

We stopped our systematic research at groups of order 720 but we still tried some specific examples of greater order. In the table below, we display the examples where the group G is A_7, S_7, A_8 or S_8.

G	degree of $\tilde{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
A_7	2520	$(C_3 \times A_4) \rtimes C_2$	35	355	21
S_7	5040	S_4	210	105	70
S_7	5040	$C_2 \times C_2 \times S_3$	210	105	70
S_7	5040	$C_2 \times C_2 \times S_3$	210	126	84
S_7	5040	$C_2 \times A_4$	210	126	84
S_7	5040	$S_3 \times S_3$	140	126	70
S_7	5040	$S_3 \times S_3$	140	126	84
S_7	5040	$C_7 \rtimes C_6$	120	120	70
S_7	5040	$D_8 \times S_3$	105	105	70
S_7	5040	$C_2 \times S_4$	105	105	70
S_7	5040	$C_2 \times S_4$	105	105	70
S_7	5040	$(C_3 \times A_4)_2$	70	70	42
S_7	5040	$S_4 \times S_3$	35	35	30
A_8	20160	$C_2 \times C_2 \times C_2 \times C_2$	1260	210	168
A_8	20160	$(C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)$	630	315	168
A_8	20160	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2$	630	210	168
A_8	20160	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2$	630	210	168
A_8	20160	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2$	630	210	168
A_8	20160	$S_3 \times S_3$	560	336	168
A_8	20160	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3$	420	210	120
A_8	20160	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3$	420	210	120
A_8	20160	$C_2 \times C_2 \times A_4$	420	210	168
A_8	20160	$C_2 \times S_4$	420	336	168
A_8	20160	$C_2 \times S_4$	420	336	168
A_8	20160	$C_2 \times S_4$	420	336	168
A_8	20160	$C_2 \times S_4$	420	336	168
A_8	20160	$(C_2 \times C_2 \times C_2) \rtimes C_7$	360	336	168
A_8	20160	$(C_2 \times C_2 \times C_2) \rtimes C_7$	360	336	168
A_8	20160	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_2$	315	210	168
A_8	20160	$(S_3 \times S_3) \rtimes C_2$	280	280	168
A_8	20160	$(C_3 \times A_4) \rtimes C_2$	280	280	168
A_8	20160	$((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2)) \rtimes C_3$	210	210	120
A_8	20160	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2$	210	210	120
A_8	20160	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2) \rtimes C_3$	210	210	120
A_8	20160	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2$	210	210	120
A_8	20160	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2) \rtimes C_3$	210	210	120
A_8	20160	$(C_2 \times S_4) \rtimes C_2$	210	210	168
A_8	20160	S_5	168	168	120
A_8	20160	$PSL(3,2)$	120	120	105
A_8	20160	$\mathrm{GL}(2,4)$	112	112	70
A_8	20160	$(A_4 \times A_4) \rtimes C_2$	70	70	56
A_8	20160	$((A_4 \times A_4) \rtimes C_2) \rtimes C_2$	35	35	28
S_8	40320	$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3$	840	336	210
S_8	40320	$((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2)_2$	630	336	210
S_8	40320	$D_8 \times D_8$	630	336	210
S_8	40320	$(S_3 \times S_3)_2$	560	336	210
S_8	40320	$C_2 \times C_2 \times S_4$	420	210	168
S_8	40320	$((C_2 \times C_2 \times C_2 \times C_2)_2) \rtimes C_3$	420	336	210
S_8	40320	$((C_2 \times C_2 \times C_2 \times C_2)_3) \rtimes C_2$	420	336	210
S_8	40320	$C_2 \times C_2 \times S_4$	420	336	210

G	degree of $\check{K}$	H	degree of K	degree of K_{J_1}	degree of K_{J_2}
S_8	40320	$C_2 \times C_2 \times S_4$	420	336	210
S_8	40320	S_5	336	336	210
S_8	40320	$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_2) \rtimes C_2)_2$	315	315	210
S_8	40320	$A_4 \times A_4$	280	140	112
S_8	40320	$C_2 \times ((S_3 \times S_3) \rtimes C_2)$	280	280	210
S_8	40320	$S_4 \times S_3$	280	280	210
S_8	40320	$PSL(3,2)$	240	240	210
S_8	40320	$PSL(3,2)$	240	240	210
S_8	40320	$(C_2 \times C_2 \times C_2) \rtimes (C_7 \rtimes C_3)$	240	240	210
S_8	40320	$(((C_2 \times C_2 \times C_2) \rtimes (C_2 \times C_2) \rtimes C_3) \rtimes C_2$	210	210	168
S_8	40320	$S_4 \times D_8$	210	210	168
S_8	40320	$S_4 \times A_4$	140	140	112
S_8	40320	$(((C_2 \times C_2 \times C_2 \times C_2) \rtimes C_3) \rtimes C_2) \rtimes C_3$	140	140	112
S_8	40320	$PSL(3,2) \rtimes C_2$	120	120	112
S_8	40320	$A_5 \times S_3$	112	112	70
S_8	40320	$S_4 \times S_4$	70	70	56
S_8	40320	$((A_4 \times A_4) \rtimes C_2) \rtimes C_2$	70	70	56
S_8	40320	$(S_4 \times S_4) \rtimes C_2$	35	35	30

References

[1] Etienne Fabrice; Page Aurel and Vermeulen Floris. *Normed Mackey functors and applications*. In preparation. 2025.

[2] James Ax. "On the units of an algebraic number field". English. In: *Ill. J. Math.* 9 (1965), pp. 584–589. ISSN: 0019-2082.

[3] Eric Bach. "Explicit bounds for primality testing and related problems". In: *Mathematics of Computation* 55 (1990), pp. 355–380. URL: https://api.semanticscholar.org/CorpusID:31714069.

[4] Alex Bartel and Tim Dokchitser. "Brauer relations in finite groups". In: *Journal of the European Mathematical Society* 17.10 (Oct. 2015), pp. 2473–2512. ISSN: 1435-9863. DOI: 10.4171/jems/563. URL: http://dx.doi.org/10.4171/JEMS/563.

[5] Karim Belabas and Eduardo Friedman. "Computing the residue of the Dedekind zeta function". In: *Math. Comp.* 84.291 (2015), pp. 357–369. ISSN: 0025-5718,1088-6842. DOI: 10.1090/S0025-5718-2014-02843-3. URL: https://doi.org/10.1090/S0025-5718-2014-02843-3.

[6] Manjul Bhargava and Wei Ho. *On average sizes of Selmer groups and ranks in families of elliptic curves having marked points*. Preprint, arXiv:2207.03309 [math.NT] (2022). 2022. URL: https://arxiv.org/abs/2207.03309.

[7] Jean-François Biasse, Claus Fieker, Tommy Hofmann, and Aurel Page. "Norm relations and computational problems in number fields". English. In: *J. Lond. Math. Soc., II. Ser.* 105.4 (2022), pp. 2373–2414. ISSN: 0024-6107. DOI: 10.1112/jlms.12563.

[8] Spencer Bloch and Kazuya Kato. *L-functions and Tamagawa numbers of motives*. English. The Grothendieck Festschrift, Collect. Artic. in Honor of the 60th Birthday of A. Grothendieck. Vol. I, Prog. Math. 86, 333-400 (1990). 1990.

[9] Robert Boltje. "Class group relations from Burnside ring idempotents". English. In: *J. Number Theory* 66.2 (1997), pp. 291–305. ISSN: 0022-314X. DOI: 10.1006/jnth.1997.2165.

[10] Richard Brauer. "Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers". German. In: *Math. Nachr.* 4 (1951), pp. 158–174. ISSN: 0025-584X. DOI: 10.1002/mana.3210040116.

[11] Peter Bruin. *Extensions and torsors for finite group schemes*. 2022. arXiv: 2207.11289 [math.AG]. URL: https://arxiv.org/abs/2207.11289.

[12] Armand Brumer. "On the units of algebraic number fields". English. In: *Mathematika* 14 (1967), pp. 121–124. ISSN: 0025-5793. DOI: 10.1112/S0025579300003703.

[13] Johannes Buchmann. *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*. English. Sémin. Théor. Nombres, Paris/Fr. 1988-89, Prog. Math. 91, 27-41 (1990). 1990.

[14] Henri Cartan and Samuel Eilenberg. *Homological algebra.* English. Paperback ed. Princeton, NJ: Princeton University Press, 1999. ISBN: 0-691-04991-2.

[15] Henri Cohen. *Advanced topics in computational number theory*. English. Vol. 193. Grad. Texts Math. New York, NY: Springer, 2000. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0.

[16] Charles Curtis and Irving Reiner. *Methods of representation theory with applications to finite groups and orders. Volume 1.* English. Paperback edition. New York etc.: John Wiley &— Sons, 1990. ISBN: 0-471-52367-4.

[17] Harold Davenport. *Multiplicative number theory. Revised and with a preface by Hugh L. Montgomery.* English. 3rd ed. Vol. 74. Grad. Texts Math. New York, NY: Springer, 2000. ISBN: 0-387-95097-4.

[18] The Sage Developers, William Stein, David Joyner, David Kohel, John Cremona, and Burçin Eröcal. *SageMath, version 9.0*. 2020. URL: http://www.sagemath.org.

[19] Andreas Dress. *Contributions to the theory of induced representations*. English. Algebr. K-Theory II, Proc. Conf. Battelle Inst. 1972, Lect. Notes Math. 342, 183-240 (1973). 1973.

[20] Andreas Dress. *Notes on the theory of representations of finite groups. Part I: The Burnside ring of a finite group and some AGN-applications. With the aid of lecture notes, taken by Manfred Küchler*. English. Universität Bielefeld, Fakultät für Mathematik. 157, A 28, B 31 p. (1971). 1971.

[21] Fabrice Etienne. *An algorithm to compute Selmer groups via resolutions by permutations modules*. 2025. arXiv: 2504.13506 [cs.SC]. URL: https://arxiv.org/abs/2504.13506.

[22] Fabrice Etienne. *Computing class groups by induction with generalised norm relations*. 2025. arXiv: 2411.13124v2 [math.NT]. URL: https://arxiv.org/abs/2411.13124v2.

[23] Fabio Ferri and Henri Johnston. *Applications of representation theory and of explicit units to Leopoldt's conjecture*. 2023. arXiv: 2301.05700 [math.NT]. URL: https://arxiv.org/abs/2301.05700.

[24] Claus Fieker and Nicole Sutherland. *Constructions using Galois Theory*. 2022. arXiv: 2010.01281 [math.NT]. URL: https://arxiv.org/abs/2010.01281.

[25] Albrecht Fröhlich and Martin Taylor. *Algebraic number theory*. English. Vol. 27. Camb. Stud. Adv. Math. Cambridge (UK): Cambridge University Press, 1990. ISBN: 0-521-36664-X.

[26] *GAP – Groups, Algorithms, and Programming, Version 4.14.0*. The GAP Group. 2024. URL: %5Curl%7Bhttps://www.gap-system.org%7D.

[27] Guoqiang Ge. "Algorithms related to multiplicative representations of algebraic numbers, PhD thesis". In: *University of California, Berkeley* (1993).

[28] James Green. "Axiomatic representation threory for finite groups". English. In: *J. Pure Appl. Algebra* 1 (1971), pp. 41–77. ISSN: 0022-4049. DOI: 10.1016/0022-4049(71)90011-9.

[29] James Hafner and Kevin McCurley. "Asymptotically fast triangularization of matrices over rings". English. In: *Discrete algorithms. Proceedings of the 1st annual ACM-SIAM symposium, held January 22-24, 1990 in San Francisco, CA (USA)*. Philadelphia, PA (USA): SIAM, 1990, pp. 194–200. ISBN: 0-89871-251-3.

[30] Derek Holt, Bettina Eick, and Eamonn O'Brien. *Handbook of computational group theory.* English. Discrete Math. Appl. (Boca Raton). Boca Raton, FL: Chapman & Hall/CRC Press, 2005. ISBN: 1-58488-372-3.

[31] Victor Alecsandrovich Kolyvagin. "On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves". English. In: *Proceedings of the international congress of mathematicians (ICM), August 21–29, 1990, Kyoto, Japan. Volume I.* Tokyo etc.: Springer-Verlag, 1991, pp. 429–436. ISBN: 4-431-70047-1.

[32] Serge Lang. *Algebra.* English. 3rd revised ed. Vol. 211. Grad. Texts Math. New York, NY: Springer, 2002. ISBN: 0-387-95385-X.

[33] Arjen Lenstra, Hendrik jun. Lenstra, and László Lovász. "Factoring polynomials with rational coefficients". English. In: *Math. Ann.* 261 (1982), pp. 515–534. ISSN: 0025-5831. DOI: 10.1007/BF01457454. URL: https://eudml.org/doc/182903.

[34] Céline Maistret and Himanshu Shukla. *On the factorization of twisted L-values and* 11*-descents over C_5-number fields.* 2025. arXiv: 2501.09515 [math.NT]. URL: https://arxiv.org/abs/2501.09515.

[35] Barry Mazur. *Deforming Galois representations.* English. Galois groups over $\mathbb{Q}$, Proc. Workshop, Berkeley/CA (USA) 1987, Publ., Math. Sci. Res. Inst. 16, 385-437 (1989). 1989.

[36] Daniele Micciancio and Shafi Goldwasser. *Complexity of lattice problems. A cryptographic perspective.* English. Vol. 671. Kluwer Int. Ser. Eng. Comput. Sci. Boston, MA: Kluwer Academic Publishers, 2002. ISBN: 0-7923-7688-9.

[37] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers.* English. 3rd ed. Springer Monogr. Math. Berlin: Springer, 2004. ISBN: 3-540-21902-1.

[38] Jürgen Neukirch. *Algebraische Zahlentheorie.* German. Reprint of the 1992 original. Berlin: Springer, 2007. ISBN: 978-3-540-37547-0. DOI: 10.1007/978-3-540-37663-7.

[39] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields.* English. 2nd ed. Vol. 323. Grundlehren Math. Wiss. Berlin: Springer, 2008. ISBN: 978-3-540-37888-4.

[40] *PARI/GP version 2.15.4.* available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2023.

[41] Claudio Procesi. *Lie groups. An approach through invariants and representations.* English. Universitext. New York, NY: Springer, 2007. ISBN: 0-387-26040-4.

[42] Irving Reiner. *Maximal orders*. English. Reprint of the 1975 original. Vol. 28. Lond. Math. Soc. Monogr., New Ser. Oxford: Oxford University Press, 2003. ISBN: 0-19-852673-3.

[43] Jean-Pierre Serre. *Corps locaux*. French. 4th corrected ed. Paris: Hermann, Éditeurs des Sciences et des Arts, 2004. ISBN: 2-7056-1296-3.

[44] Jean-Pierre Serre. *Galois cohomology. Transl. from the French by Patrick Ion.* English. 2nd printing. Springer Monogr. Math. Berlin: Springer, 2002. ISBN: 3-540-42192-0.

[45] Jean-Pierre Serre. *Linear representations of finite groups. Translated from the French by Leonard L. Scott*. English. Vol. 42. Grad. Texts Math. Springer, Cham, 1977.

[46] Joseph Silverman. *The arithmetic of elliptic curves*. English. Vol. 106. Grad. Texts Math. Springer, Cham, 1986.

[47] Toshikazu Sunada. "Riemannian coverings and isospectral manifolds". English. In: *Ann. Math. (2)* 121 (1985), pp. 169–186. ISSN: 0003-486X. DOI: 10.2307/1971195.

[48] Floris Vermeulen. "Arithmetically equivalent number fields have approximately the same successive minima". English. In: *J. Number Theory* 249 (2023), pp. 119–130. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2023.02.011.

[49] Valentin Voskresenskiĭ. *Algebraic groups and their birational invariants. Transl. from the original Russsian manuscript by Boris Kunyavskii.* English. Rev. version of 'Algebraic tori', Nauka 1977. Vol. 179. Transl. Math. Monogr. Providence, RI: American Mathematical Society, 1998. ISBN: 0-8218-0905-9.

[50] Andrew Wiles. "Modular Elliptic Curves and Fermat's Last Theorem". In: *Annals of Mathematics* 141.3 (1995), pp. 443–551. ISSN: 0003486X, 19398980. URL: http://www.jstor.org/stable/2118559 (visited on 04/04/2025).

[51] Tomoyuki Yoshida. "On G-functors. II: Hecke operators and G-functors". English. In: *J. Math. Soc. Japan* 35 (1983), pp. 179–190. ISSN: 0025-5645. DOI: 10.2969/jmsj/03510179.