Mémoire de master

Fabrice Etienne

Notes

— Encadrant : Aurel Page.

— Référence :

— Jean-François Biasse, Claus Fieker, Tommy Hofmann et Aurel Page. “Norm relations and computational problems in number fields”. In : Journal of the London Mathematical Society (2022).

Table des matières

Remerciements

Je tiens tout d'abord à remercier l'Institut de Mathématiques de Bordeaux pour son accueil et particulièrement M. Aurel PAGE qui a encadré mon stage.

Introduction

Ce mémoire est le compte rendu du stage de trois mois que j'ai effectué entre début mars et début juin 2022 à l'Institut de Mathématiques de Bordeaux, sous la direction de M. Aurel PAGE.
Mon travail a été de comprendre l'article en référence, et d'en généraliser certains résultats.

Pour un groupe fini G, l'objet de l'article est d'abord d'étudier les propriétés des relations de normes dans l'algèbre de groupe $\mathbb{Q}[G]$, ainsi que les conditions d'existence de telles relations. Ensuite, l'article se place dans le cas où G est le groupe de Galois d'une extension galoisienne de corps de nombres K/F. L'article décrit alors des algorithmes utilisant les relations de normes dans $\mathbb{Q}[G]$ qui permettent de calculer des objets arithmétiques sur K, tels que le groupe des S-unités de $K^\times$, en se ramenant à des calculs sur des extensions de corps de degrés plus petits. En effet, la complexité des algorithmes existants qui permettent de calculer le groupe des S-unités de $K^\times$ dépend du degré de K, de sorte que la méthode décrite dans l'article permet d'accélérer les calculs dans certains cas.

Durant mon stage, j'ai essayé de trouver une généralisation des relations de normes, qui permette d'appliquer une méthode similaire pour calculer le groupe des S-unités de K même dans le cas où K/F n'est pas galoisienne.

La première partie consistera en des rappels sur la théorie de Galois, qui sont nécessaires pour comprendre aussi bien l'article que la suite du mémoire. Ensuite je résumerai les principaux résultats et définitions de l'article. Les deux parties suivantes exposeront des définitions et des résultats, respectivement sur les algèbres de Hecke et sur les compositums. Contrairement aux parties précédentes, les résultats seront démontrés, puisque ce sont des preuves que j'ai cherchées pendant mon stage pour me familiariser avec ces objets. Les résultats sur les algèbres de Hecke seront utiles pour la suite. Ceux sur les compositums n'apparaîtront pas dans la suite du mémoire, mais ils seront utiles pour essayer de reformuler le problème en termes de théorie des corps, sans théorie de Galois, de manière à pouvoir se passer des calculs de clotures galoisiennes qui augmentent la complexité de certains algorithmes décrits dans la suite du mémoire. C'est une piste de réflexion que je n'ai pas eu le temps de creuser durant mon stage, mais sur laquelle je compte revenir plus tard. Ensuite, dans la cinquième partie, je proposerai une généralisation

de la notion de relations de normes (définition 66), et j'étudierai des conditions nécessaires et suffisantes d'existence de telles relations généralisées (théorème 64). Enfin, dans la sixième partie, je décrirai des algorithmes permettant chercher des relations de normes étendues, et de s'en servir pour calculer le groupe des S-unités d'un corps de nombre.

1 Théorie de Galois

Dans cette partie, on rappelera des définitions et des résultats de résultats de théorie de Galois, qui seront essentiels pour comprendre la suite. Les résultats ne seront pas démontrés.

Dans toute la partie, F désignera un corps de nombre de caractéristique 0 et K une extension de F de degré fini. On notera $\mathrm{Aut}_F(K)$ l'ensemble des automorphismes de K dans K qui sont F-linéaires.

Définition 1 On notera $K^{\mathrm{Aut}_F(K)}$ l'ensemble des éléments de K fixés par l'action de $\mathrm{Aut}_F(K)$.

Définition 2 L'extension K/F est dite *galoisienne* si les conditions équivalentes suivantes sont vérifiées :

1. On a $F = K^{\mathrm{Aut}_F(K)}$.
2. On a $|\mathrm{Aut}_F(K)| = [K : F]$ le degré de l'extension.
3. Pour tout $g \in F[X]$ irréductible avec une racine dans K, g est scindé dans K.
4. Le corps K est le corps de décomposition d'un polynôme $f \in F[X]$ irréductible.
5. Le corps K est le corps de décomposition d'un polynôme $f \in F[X]$.

Exemple 3

— Soit $L_1 = \mathbb{Q}(\sqrt{2})$. L'extension $L_1/\mathbb{Q}$ est le corps de décomposition du polynôme $f(X) = X^2 - 2$. Donc cette extension est galoisienne.

— Soient p, q deux nombres premiers distincts, et $L_2 = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Alors $L_2/\mathbb{Q}$ est le corps de décomposition du polynôme $f(X) = (X^2 - p)(X^2 - q)$. Donc cette extension est galoisienne.

— Soit $L_3 = \mathbb{Q}(\sqrt[3]{2})$. Calculons tous les éléments de $\mathrm{Aut}_{\mathbb{Q}}(L_3)$.
La famille $(1, \sqrt[3]{2}, \sqrt[3]{2}^2)$ est une $\mathbb{Q}$-base de L_3. Soit $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \in L_3$.
Soit $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(L_3)$. Alors $\sigma(a) = a, \sigma(b) = b$ et $\sigma(c) = c$.
Donc $\sigma(\alpha) = a + b\sigma(\sqrt[3]{2}) + c\sigma(\sqrt[3]{2})^2$. Donc σ est entièrement déterminé par $\sigma(\sqrt[3]{2})$.
Mais on sait que $\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$. De plus, la seule solution de l'équation $x^3 = 2$ qui est dans L_3 est $\sqrt[3]{2}$. Donc $\sigma(\sigma(\sqrt[3]{2})) = \sigma(\sqrt[3]{2})$.

En conclusion, $\mathrm{Aut}_{\mathbb{Q}}(L_3)$ est réduit au singleton identité. Donc $L_3^{\mathrm{Aut}_{\mathbb{Q}}(L_3)} = L_3 \neq \mathbb{Q}$. Donc l'extension $L_2/\mathbb{Q}$ n'est pas galoisienne.

Définition 4 Si K/F est galoisienne, on note $Gal(K/F) = \mathrm{Aut}_F(K)$. On dit que c'est le *groupe de Galois* de l'extension.

Remarque 5 Si K/F est une extension galoisienne finie de groupe de galois G, on a $|G| = [K : F]$.

Proposition 6 Si on a $F = K(\alpha_1, \cdots, \alpha_n)$ où les α_i sont les racines d'un polynôme séparable $f \in K[X]$, alors les éléments de $\mathrm{Aut}_F(K)$ permutent les (α_i), ie G est isomorphe à un sous-groupe du groupe de permutations S_n. De plus, les éléments de $Aut_F(K)$ envoient chaque α_i sur l'un de ses conjugués, c'est à dire sur une racine du même facteur irréductible de f.

Exemple 7

— Soit $L_1 = \mathbb{Q}(\sqrt{2})$. $L_1 = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$, où $\sqrt{2}, -\sqrt{2}$ sont les racines du polynôme séparable $X^2 - 2$. Donc $Gal(L_1/\mathbb{Q})$ est isomorphe à un sous-groupe de S_2. Or on sait que son cardinal est $[L_1 : \mathbb{Q}] = 2$, donc $Gal(L_1/\mathbb{Q}) = S_2$.

— Soient p, q deux nombres premiers distincts, et $L_2 = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.
$L_2 = \mathbb{Q}(\sqrt{p}, -\sqrt{p}, \sqrt{q}, -\sqrt{q})$, où $(\sqrt{p}, -\sqrt{p}, \sqrt{q}, -\sqrt{q})$ sont les racines du polynôme séparable $(X^2 - p)(X^2 - q)$. Donc $Gal(L_2/\mathbb{Q})$ est un sous-groupe de S_4. On sait de plus que son cardinal est $[L_2 : \mathbb{Q}] = 4$.
Déterminons l'ensemble des éléments de $Aut_{\mathbb{Q}}(L_2)$. Soit $\sigma \in Aut_{\mathbb{Q}}(L_2)$.
Alors σ est entièrement déterminé par les valeurs de $\sigma(\sqrt{p})$ et $\sigma(\sqrt{q})$, qui doivent de plus être conjugués respectivement à $\sqrt{p}$ et à $\sqrt{q}$.
Il n'y a donc que quatre possibilités :

1. $\begin{cases} \sigma(\sqrt{p}) &= \sqrt{p} \\ \sigma(\sqrt{q}) &= \sqrt{q} \end{cases}$
2. $\begin{cases} \sigma(\sqrt{p}) &= -\sqrt{p} \\ \sigma(\sqrt{q}) &= \sqrt{q} \end{cases}$
3. $\begin{cases} \sigma(\sqrt{p}) &= \sqrt{p} \\ \sigma(\sqrt{q}) &= -\sqrt{q} \end{cases}$
4. $\begin{cases} \sigma(\sqrt{p}) &= -\sqrt{p} \\ \sigma(\sqrt{q}) &= -\sqrt{q}. \end{cases}$

Ces quatre possibilités correspondent aux quatre éléments $\sigma_1, \cdots, \sigma_4$ de $Aut_{\mathbb{Q}}(L_2)$.
Remarquons que chaque élément correspond à une permutation de l'ensemble $\{\sqrt{p}, -\sqrt{p}, \sqrt{q}, -\sqrt{q}\}$.

Par exemple σ_2 permute les éléments $\sqrt{p}$ et $-\sqrt{p}$.
En numérotant de 1 à 4 les éléments de cet ensemble, on obtient donc que
$Aut_{\mathbb{Q}}(L_2) = \mathrm{Gal}(L_2/\mathbb{Q})$ est isomorphe au sous-groupe de S_4 décrit par l'ensemble
$\{id, (1,2), (3,4), (1,2)(3,4)\}$.

Définition 8 On appelle *clôture galoisienne* de K/F la plus petite extension de corps $\tilde{K}/K$ telle que $\tilde{K}/F$ est galoisienne.

Exemple 9 Soit $L_3 = \mathbb{Q}(\sqrt[3]{2})$. On a déjà vu que $L_3/\mathbb{Q}$ n'est pas galoisienne.
Considérons le polynôme $f(X) = X^3 - 2$. On remarque que $f(X)$ est irréductible dans $\mathbb{Q}[X]$, mais qu'il a une racine dans L_3, donc dans la clôture galoisienne de L_3. Donc f est scindé dans la clôture galoisienne de L_3.
Donc $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$, avec $\zeta = e^{\frac{2i\pi}{3}}$, est inclu dans la clôture galoisienne de L_3.
Mais $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$ est le corps de décomposition de f, donc $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})/\mathbb{Q}$ est galoisienne.
Finalement, $\mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2})$ est la clôture galoisienne de L_3.

Théorème 10 (Théorème fondamental de la théorie de Galois)
Si K/F est galoisienne, de groupe de Galois G, il existe une bijection (qui renverse l'inclusion) entre

- Les corps intérmédiaires $F \subset L \subset K$
- Les sous-groupes $H < G$

donnée par

- $L \mapsto Aut_L(K)$
- $H \mapsto K^H$.

Proposition 11 Si K/F est galoisienne, de groupe de Galois G, soit $H < G$ et $L = K^H$. Alors L/F est galoisienne si et seulement si $H \triangleleft G$. On a alors $Gal(L/F) = G/H$.

Théorème 12 Si K/F est galoisienne, il existe $\lambda \in K$ tel que les $\sigma(\lambda)$ pour $\sigma \in \mathrm{Gal}(K/F)$ forment une F-base de K.

Théorème 13 Si K/F est galoisienne, et si L_1, L_2 sont des corps intermédiaires $F \subseteq L_1, L_2 \subseteq K$, et $\sigma : L_1 \to L_2$ un morphisme de corps F-linéaire,
alors σ s'étend en $\tilde{\sigma} : K \to K$ avec $\tilde{\sigma} \in \mathrm{Gal}(K/F)$.

2 Retours sur l'article

Cette partie a pour but de résumer les principaux résultats et définitions de l'article. Les résultats ne seront pas démontrés.

2.1 Relations de normes

Dans cette sous-partie, on considère G un groupe fini quelconque et $H < G$ un sous-groupe.

Définition 14 On appelle *élément norme* de H l'élément $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$.

Définition 15 Pour tout $\mathbb{Z}[G]-$module M, on note M^H l'ensemble des points de M qui sont fixés par l'action de tous les éléments de H.

Proposition 16 L'élément norme N_H vérifie les propriétés suivantes.

- Pour tout $\mathbb{Z}[G]-$module M et pour tout $x \in M$, on a $N_H x \in M^H$.
- On a $N_H^2 = |H| N_H$.
- Si R est un anneau commutatif dans lequel $|H|$ est inversible, $e = \frac{1}{|H|} N_H \in R[G]$ est idempotent, et pour tout $R[G]$-module M, $eM = N_H M = M^H$.

Définition 17 Soit $\mathcal{H}$ un ensemble de sous-groupes de G, et R un anneau commutatif. Une *relation de norme* sur R par rapport à $\mathcal{H}$ est une égalité dans $R[G]$ de la forme $1 = \sum_{i=1}^{l} a_i N_{H_i} b_i$ où les a_i et les b_i sont des éléments de $R[G]$ et les H_i sont des éléments de $\mathcal{H}$ différents du sous-groupe trivial.

Remarque 18 L'article définit et étudie également deux autres types de relations : les relations de Brauer et les relations de normes scalaires. Cependant, on ne mentionnera ici que les relations de normes, puisque ce sont celles que l'on se proposera de généraliser par la suite.

Proposition 19 Soit $\mathcal{H}$ un ensemble de sous-groupes non triviaux de G. Les assertions suivantes sont équivalentes.

- Il existe une relation de norme sur $\mathbb{Q}$ par rapport à $\mathcal{H}$.
- On a $\langle N_H ; H \in \mathcal{H} \rangle_{\mathbb{Q}[G]} = \mathbb{Q}[G]$ en tant qu'idéal bilatère.
- Pour tout $\mathbb{Q}[G]$-module simple V, il existe $H \in \mathcal{H}$ tel que $V^H \neq \{0\}$.
- Pour tout $\overline{Q}[G]$-module simple V (avec $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$), il existe $H \in \mathcal{H}$ tel que $V^H \neq \{0\}$.
- Pour tout $\mathbb{C}[G]$-module simple V, il existe $H \in \mathcal{H}$ tel que $V^H \neq \{0\}$.

2.2 Applications en arithmétique

Dans cette sous-section, on considère K/F une extension galoisienne de corps de nombres, de groupe de Galois G. On s'intéressera à des relations de la forme

$(*) : d = \sum_{i=1}^{l} a_i N_{H_i} b_i$
avec $d \in \mathbb{N}^*, a_i, b_i \in \mathbb{Z}[G], H_i < G$.

Remarque 20 L'existence d'une relation de la forme $(*)$ est équivalente à l'existence d'une relation de norme sur $\mathbb{Q}$ par rapport à $\mathcal{H} = \{H_1, \cdots, H_\ell\}$ (à répétitions près), quitte à multiplier les deux côtés de la relation de norme par le plus petit commun multiple des dénominateurs des coefficients.

Définition 21 Soit R un anneau commutatif. *L'annulateur* d'une partie S d'un R-module M est $Ann(S) = \{r \in R; \forall x \in S, rx = 0\}$.

Définition 22 *L'exposant* d'un $\mathbb{Z}$-module est le générateur du groupe des annulateurs.

Proposition 23 Soit M un $\mathbb{Z}[G]$-module. Si G admet une relation de la forme $(*)$, alors l'exposant du quotient $M/(\sum_{i=1}^{l} a_i M^{H_i})$ est fini et divise d.

Remarque 24 Le groupe $K^\times$ est naturellement muni d'une structure de $\mathbb{Z}[G]$-module.

Remarque 25 En l'appliquant au cas $M = K^\times$, la proposition 23 permet de faire le lien entre les corps K et K^{H_i} pour $H_i \in \mathcal{H}$. Or les corps K^{H_i} sont des extensions de $\mathbb{Q}$ de degrés inférieurs à $[K : \mathbb{Q}]$. Par conséquent, un certain nombre d'objets arithmétiques tels que le groupe des S-unités, l'anneau des entiers ou groupe des classes, sont plus faciles à calculer pour les K^{H_i} que pour K (dans le sens où la complexités des algorithmes connus permettant de calculer ces objets dépend fortement du degré du corps).
Dès lors, une idée fondamentale de l'article sera de trouver des algorithmes permettant d'utiliser la relation $(*)$ pour calculer des objets sur K en fonction d'objets sur les K^{H_i}.

Définition 26 Soit S une partie G-stable de l'ensemble des idéaux premiers non nuls de l'anneau des entiers $\mathcal{O}_K$. Le *groupe des S-unités* est le sous-groupe de $K^\times$ défini par
$\mathcal{O}_{K,S}^\times = \{x \in K^\times; v_\mathfrak{p}(x) = 0 \forall \mathfrak{p} \in S\}$ où $v_\mathfrak{p}$ est la valuation $\mathfrak{p}$-adique.

Notation Dans la suite, S désignera toujours une partie G-stable de l'ensemble des idéaux premiers non nuls de $\mathcal{O}_K$.

Définition 27 Soit V un sous-groupe de $K^\times$ de type fini, et soit $d \in \mathbb{N}^\times$. La *d-saturation* de V est le plus petit sous-groupe $W \subset K^\times$ tel que $V \subset W$ et $K^\times/W$ est sans d-torsion.
De même, la saturation de V est le plus petit sous-groupe $W \subset K^\times$ tel que $V \subset W$ et $K^\times/W$ est sans torsion.

Proposition 28 Le groupe des S-unités de K est saturé dans $K^\times$, i.e. tout élément dont une puissance non nulle est une S-unité de K est lui même une S-unité de K.

Corollaire 29 Si G admet une relation de la forme $(*)$, alors l'exposant du quotient $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K^{H_1},S}^\times)^{a_1}\cdots(\mathcal{O}_{K^{H_\ell},S}^\times)^{a_\ell}$ est fini et divise d. En particulier, le groupe $\mathcal{O}_{K,S}^\times$ est la d-saturation du groupe $V=(\mathcal{O}_{K^{H_1},S}^\times)^{a_1}\cdots(\mathcal{O}_{K^{H^\ell},S}^\times)^{a\ell}$.

La suite de l'article consiste à utiliser ce résultat pour créer un algorithme permettant de calculer $\mathcal{O}_{K,S}^\times$ en fonction des $\mathcal{O}_{K^{H_i},S}^\times$. L'idée générale de l'algorithme est la suivante.

Algorithme 30
entrée : Une extension de corps galoisienne K/F, de groupe de Galois G, qui admet une relation de la forme $(*)$.
sortie : Une base sur $\mathbb{Z}$ du groupe des S-unités de $K^\times$.

1. Pour chaque sous corps $K_i=K^{H_i}$, calculer une base du groupe des S-unités de $K_i^\times$.
2. Déterminer le groupe $V=(\mathcal{O}_{K_1,S}^\times)^{a_1}\cdots(\mathcal{O}_{K_l,S}^\times)^{a_l}$.
3. Calculer et renvoyer la d-saturation de V.

Remarque 31 L'article prouve des résultats similaires pour l'anneau des entiers de K ainsi que pour le groupe des classes de K, et propose aussi des algorithmes pour calculer ces objets, mais on se concentrera ici sur le cas du groupe des S-unités.

2.3 Saturation

Afin d'implémenter cet algorithme, il reste à étudier comment calculer algorithmiquement la d-saturation d'un sous-groupe V de $K^\times$ de type fini.

Lemme 32 Soit $V\subset K^\times$ de type fini, et soit d un entier natuurel non nul. Alors, les assertions suivantes sont vraies.

— La d-saturation de V contient la d-torsion de $K^\times$.
— Le groupe V est d-saturé si et seulement si il est p-saturé pour tout p premier divisant d.
— Pour tout p premier, le groupe V n'est pas p-saturé si et seulement si il existe $\alpha\in K^\times\backslash V$ tel que $\alpha^p\in V$. Dans ce cas, p divise l'indice $[\langle V,\alpha\rangle : V]$.
— Soit p premier tel que V contient la p-torsion de $K^\times$. Alors V est p-saturé si et seulement si $V\cap(K^\times)^p=V^p$.

Notation Dans la suite, pour tout idéal non nul $\mathfrak{p}$ de $\mathcal{O}_K$, on notera $K_\mathfrak{p}$ la complétion $\mathfrak{p}$-adique de K, $v_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique, et $k_\mathfrak{p}=\mathcal{O}_K/\mathfrak{p}=\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ le corps résiduel en $\mathfrak{p}$.

Proposition 33 Soit $c \in \mathbb{R}^{+*}$, $V < K^\times$ de type fini, p un nombre premier et d un entier naturel non nul. On pose $\chi_\mathfrak{p} : K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^d \to \mathbb{Z}/d\mathbb{Z} \times k_\mathfrak{p}^\times/(k_\mathfrak{p}^\times)^d, \overline{x} \mapsto (\overline{v}, \overline{x\overline{\omega}^{-v}})$, avec $v = v_\mathfrak{p}(x)$. Soit m la dimension de l'intersection $\bigcap_{p\notin\mathfrak{p}, N(\mathfrak{p})\leq c} \ker(\chi_p) \subseteq V/V^p$
et soient $\alpha_1, \cdots, \alpha_m$ tels que $(\overline{\alpha_1}, \cdots, \overline{\alpha_m})$ soit une $\mathbb{F}_p$-base de cette intersection.
Alors, les assertions suivantes sont vraies :

1. Si $m = 0$, alors V est p-saturé
2. Si V n'est pas p-saturé, alors si c est assez grand, il existe $1 \leq i \leq m$ tel que α_i est une puissance p-ième.
3. Si V est p-saturé, alors pour c suffisement grand, on a $m = 0$.

De cette proposition, on peut déduire l'algorithme suivant pour calculer la p-saturation d'un groupe $V \subset K^\times$:

Algorithme 34
entrée : Un sous-groupe $V < K^\times$ de type fini, et un nombre premier p
sortie : Vrai si V est p-saturé, sinon, un élément α tel que p divise $[\langle V, \alpha\rangle : V]$

1. Soit $c > 0$ une constante quelconque.
2. Déterminer $(\overline{\alpha_1}, \cdots, \overline{\alpha_m})$ une $\mathbb{F}_p$-base de $\bigcap_{p\notin\mathfrak{p}, N(\mathfrak{p})\leq c} \ker(\chi_p)$
3. Si $m = 0$, renvoyer Vrai
4. Si $m > 0$, tester si l'un des α_i est une puissance p-ième. Si il existe α tel que $\alpha^p = \alpha_i$, renvoyer α
5. Remplacer c par $2c$ et retourner à l'étape 2

Par la proposition 33, cet algorithme termine et est correct. En l'appliquant à tous les nombres premiers p qui divisent d, on peut ainsi calculer algorithmiquement la d-saturation de V.

Remarque 35 Même si l'algorithme 34 termine et est correct, le fait qu'il dépende du choix d'une constante c arbitraire n'est pas satisfaisant. On peut se demander s'il existe un choix de c qui permette d'optimiser la complexité dans le cas général. Le théorème suivant vise à répondre à cette question.

Théorème 36 Supposons correcte l'hypothèse de Riemann généralisée. Soit $d = p^r$ avec p premier et $r \in \mathbb{N}^\times$. Soit K un corps de nombre de degré n et $L = K(\zeta_d)$ (avec ζ_d une racine primitive d-ième de l'unité). Soit S un ensemble fini de premiers de K et $M_S = \prod_{\mathfrak{p}\in S} N(\mathfrak{p})$. Soit

$S_p = S \cup \{\mathfrak{p}|p\}$.
Soit $c_0 = 18d^2(2\log|\Delta_K| + 6n\log d + M_S)^2$.
Soit T l'ensemble des idéaux premiers $\mathfrak{p}$ de K tels que

- $\mathfrak{p} \notin S_p$
- $\mathfrak{p}$ a pour degré résiduel 1
- $N(\mathfrak{p}) = 1 \bmod d$
- $N(\mathfrak{p}) \leq c_0$.

Soit $\alpha \in K^\times$ tel que toutes les valuations $\mathfrak{p}$-adiques de α pour des $\mathfrak{p} \notin S$ soient divisibles par d et tel que pour tout $\mathfrak{p} \in T$, l'image de α dans $K_\mathfrak{p}^\times$ est une puissance d-ième.
Alors $\alpha \in (L^\times)^d$. De plus, si L/K est cyclique, alors $\alpha \in (K^\times)^d$.

Corollaire 37 En supposant correcte l'hypothèse de Riemann généralisée, soit un sous-groupe $V \subset K^\times$ et un entier d qui est soit 2 soit une puissance d'un nombre premier impair.
Alors, avec les mêmes notation que pour le théorème précédent, on a
$(V \cap (K^\times)^d)/v^d = \bigcap_{p \notin \mathfrak{p}, N(\mathfrak{p}) \leq c_0} \ker(\chi_p)$.

Les deux résultats précédents supposent l'hypothèse de Riemann généralisée, qui peut s'énoncer comme ceci :
Pour tout caractère de Dirichlet χ, si s est un nombre complexe tel que $L(\chi, s) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} = 0$, et si la partie partie réelle de s est strictement comprise entre 0 et 1, alors elle vaut en fait $\frac{1}{2}$.

L'objectif de ce mémoire est de trouver une généralisation de ces résultats, qui permette de calculer le groupe des S-unités d'une extension non galoisienne de $\mathbb{Q}$, en se ramenant à des extensions de degré plus petit, de manière similaire. Les deux prochaines sections établieront des définitions et des résultats préalables, sur la théorie de Galois, sur les algèbres de Hecke, puis sur les compositums, qui seront utiles pour la généralisation.

3 Algèbres de Hecke

Dans cette section, G est un groupe fini et R est un anneau commutatif. L'objectif est d'enoncer des résultats qui seront utiles par la suite.

Notation Etant donné un ensemble E fini quelconque, $R[E]$ désigne l'ensemble abstrait $\{\sum_{e \in E} x_e e; x_e \in R\}$.

Définition 38 Soit V un $R[G]$-module, et H un sous-groupe de G. On notera V^H l'ensemble des points fixes de V par l'action de H.

Proposition 39 Si H est un sous-groupe de G et V est un $R[G]$-module, alors $\mathrm{Hom}_{R[G]}(R[G/H], V)$ est isomorphe à V^H en tant que R-modules. En effet, l'application
$\Phi : \mathrm{Hom}_{R[G]}(R[G/H], V) \to V^H, \phi \mapsto \phi(1 \cdot H)$
est un isomorphisme de R-modules.

Preuve. On considère le morphisme $\Phi : \mathrm{Hom}_{R[G]}(R[G/H], V) \to V^H, \phi \mapsto \Phi(1.H)$.
Montrons d'abord que Φ est bien à valeurs dans V^H :
Soient $h \in H$, $\phi \in \mathrm{Hom}_{R[G]}(R[G/H], V)$.
Alors $h \cdot \phi(1 \cdot H) = \phi(h \cdot 1 \cdot H) = \phi(1 \cdot H)$.
(La première égalité découle du fait que ϕ est un $R[G]$-morphisme.)
Donc $\phi(1 \cdot H) = \Phi(\phi)$ est bien dans V^H.

De plus, ϕ est entièrement déterminé par $\phi(1 \cdot H)$ car $R[G/H]$ est engendré comme $R[G]$-module par $1 \cdot H$. Donc Φ est injectif.
Enfin, tout élément $x \in V^H$ a pour antécédent le morphisme $\phi : R[G/H] \to V$ défini par $\phi(g \cdot H) = g \cdot x$ pour tout $g \in G$. Et ϕ est bien défini, car pour tout $g' = gh$ avec $h \in H$, $g' \cdot x = g(h \cdot x) = g \cdot x$ car $x \in V^H$. Donc Φ est surjective.
Finalement, Φ est donc un isomorphisme.

□

Définition 40 Si K, H sont des sous-groupes de G, alors $K\backslash G/H$ est le quotient de G par la relation d'équivalence $\sim$, définie par $g_1 \sim g_2$ si et seulement si il existe $(k, h) \in K \times H$ tel que $g_1 = kg_2h$.

Proposition 41 Si H, K sont des sous-groupes de G, alors $R[G/H]^K \simeq R[K\backslash G/H]$ en tant que R-modules.

Preuve. Soit $\alpha = \sum_{g \in G/H} \alpha_g gH \in R[G/H]$. Alors, α est fixé par K si et seulement si, pour tout $k \in K$, $k.\alpha = \sum_{g \in G/H} \alpha_g (kg)H = \sum_{g' \in G/H} \alpha_{k^{-1}g'} g'H = \alpha$. Donc α est fixé par K si et seulement si $\alpha_{k^{-1}g} = \alpha_g$ pour tous $g \in G/H$, $k \in K$. Donc $R[G/H]^K \simeq \{ \sum_{g \in G/H} \alpha_g KgH \} = R[K\backslash G/H]$.

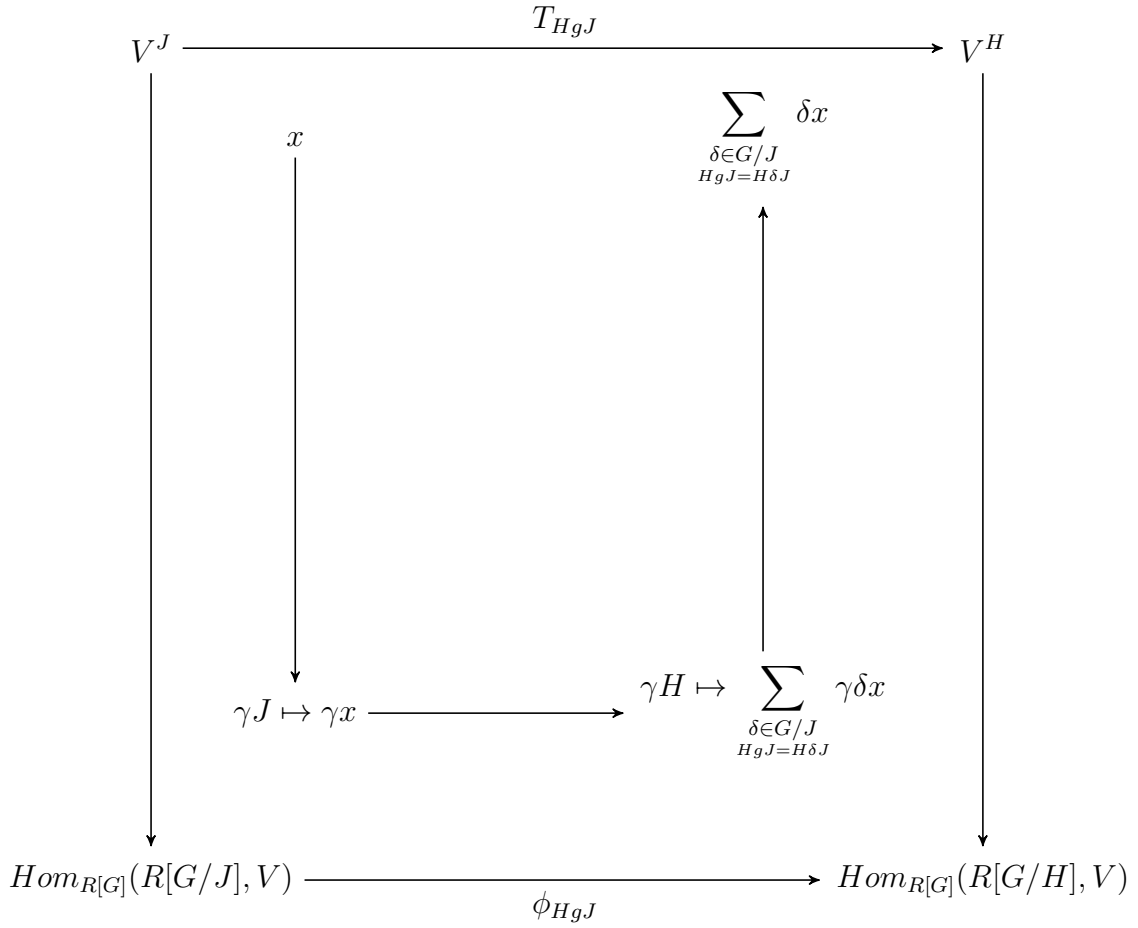
□

Proposition 42 Avec les notations précédentes, $R[K\backslash G/H] \simeq \mathrm{Hom}_{R[G]}(R[G/K], R[G/H])$.

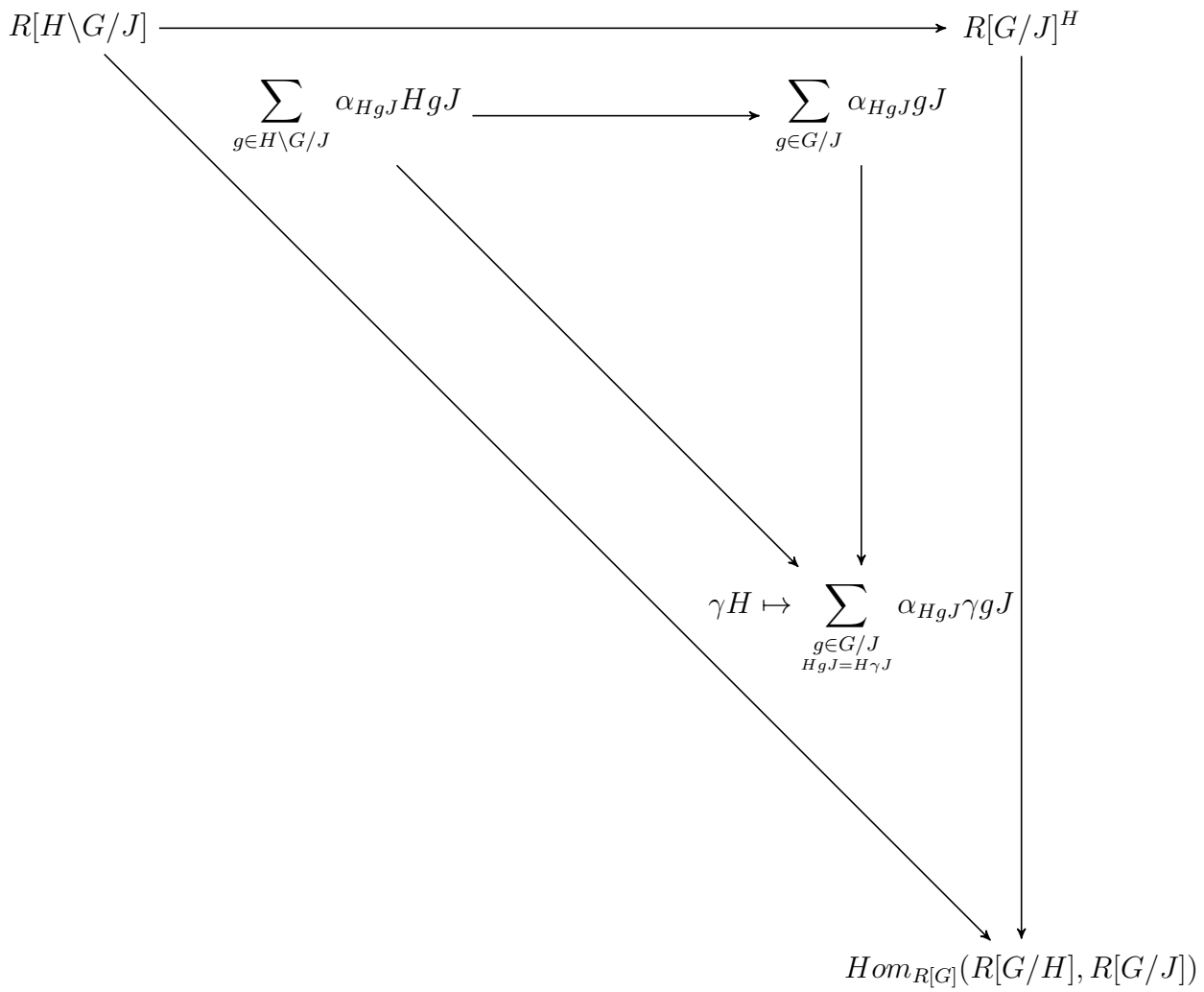
Preuve. $R[K\backslash G/H] \simeq R[G/H]^K$ par la proposition 41, et la proposition 39 avec $V = R[G/H]$ permet de conclure.

□

Remarque 43 Pour tout $R[G]$-module V, on peut donc voir chaque élément de $R[K\backslash G/H]$ comme un morphisme de R-modules de V^H dans V^K, donné par le diagramme ci dessous :



Où l'expression de ϕ_{HgJ} est obtenue en considérant le diagramme ci dessous.



Définition 44 On définit la multiplication dans $R[H\backslash G/H]$ comme héritée de la loi $\circ$ de $End_{R[G]}(R[G/H])$.

Proposition 45 $R[H\backslash G/H]$ est une algèbre sur R.

Preuve. Par la proposition 43, $R[H\backslash G/H] \simeq End_{R[G]}(R[G/H])$ qui est une algèbre sur R. □

Exemple 46 Posons $R = \mathbb{Q}$, $G = S_3$ et $H = \{id, (1,2)\}$.

- Il y a deux classes d'équivalences dans $H\backslash G/H$: $\{id, (1,2)\}$ et $\{(1,2,3), (1,3), (2,3), (2,3,1)\}$. En effet, $(1,2,3)(1,2) = (1,3)$, $(1,2)(1,2,3) = (2,3)$ et $(1,2)(1,2,3)(1,2) = (2,1,3)$. Donc $\mathbb{Q}[H\backslash G/H] = \{a(H1H) + b(H(1,3)H); (a,b) \in \mathbb{Q}^2\}$.
- Il y a trois classes d'équivalences dans G/H : $\{id, (1,2)\}$, $\{(1,2,3), (1,3)\}$ et $\{(2,1,3), (2,3)\}$. Par linéarité, un élément de $End_{R[G]}(R[G/H])$ est donc entièrement déterminé par les images de $1 \cdot id$ $1 \cdot (1,3)H$ et $1 \cdot (2,3)H$.
- Soit $x = a(HidH) + b(H(1,3)H)$ un élément de $\mathbb{Q}[H\backslash G/H]$. Par le deuxième diagramme de la remarque 44, x est associé à l'élément de $End_{R[G]}(R[G/H])$ qui envoie $\gamma H \in G/H$

sur

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

— On définit la loi + sur $\mathbb{Q}[H\backslash G/H]$ de manière naturelle par
$(a_1(HidH) + b_1(H(1,3)H)) + (a_2(HidH) + b_2(H(1,3)H))$
$= ((a_1 + a_2)(HidH) + (b_1 + b_2)(H(1,3)H))$,
et la loi $\cdot$ comme héritée de la loi $\circ$ sur $End_{R[G]}(R[G/H])$ par la correspondante décrite au point précédent. On a donc :

— $HidH \cdot HidH = HidH$

— $HidH \cdot H(1,3)H = H(1,3)H$

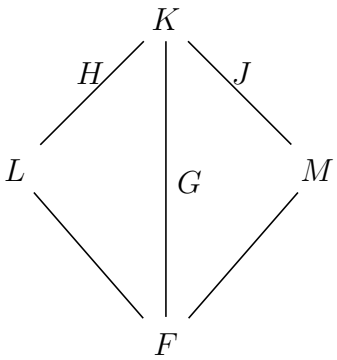
— $H(1,3)H \cdot HidH = H(1,3)H$

— $H(1,3)H$ est associé à $f : \gamma H \mapsto \begin{cases} 0 & \text{si} \quad H\gamma H = HidH \\ \gamma(1,3)H + \gamma(2,3)H & \text{si} \quad H\gamma H = H(1,3)H \end{cases}$,
si $\gamma \in \overline{(1,3)}$, alors $f(\gamma) = idH + (1,3)H$ donc $f^2(\gamma) = f(\gamma)$,
et de même, si $\gamma \in \overline{(2,3)}$, alors $f(\gamma) = (2,3)H + idH$ donc $f^2(\gamma) = f(\gamma)$,
d'où finalement $H(1,3)H \cdot H(1,3)H = H(1,3)H$.

Alors, $\mathbb{Q}[H\backslash G/H]$ est bien une algèbre.

4 Compositums

Dans cette section, K/F est une extension galoisienne de corps, de groupe de Galois G. Les corps L et M sont des extensions intermédiaires, de groupes de galois $H, J < G$.



Une grande partie de cette section (du lemme 47 à la proposition 56) est basée sur l'étude d'une partie d'un article en cours de préparation :
Bill Allombert et Aurel Page, Computing two-dimensional primitive Artin representations.

Lemme 47 L'ensemble fini $\mathrm{Hom}_{F-alg}(L,K)$ admet une action de G à gauche par post-composition. Cette action est transitive et le stabilisateur d'un élément ϕ de $\mathrm{Hom}_{F-alg}(L,K)$ est $\mathrm{Gal}(K/\phi(L)) \subset G$.

Preuve. Pour $g \in G$, $g.(\phi : x \mapsto \phi(x)) = (g \cdot \phi) : x \mapsto g \cdot \phi(x)$. Comme $G = \mathrm{Gal}(K/F)$, c'est bien une action de groupe.
Par définition, $\mathrm{Gal}(K/\phi(L))$ est le sous-groupe de G qui fixe $\phi(L)$ point par point, donc c'est bien le stabilisateur de ϕ pour cette action.
Prouvons maintenant que cette action est transitive. Par le théorème de l'élément primitif, il existe α tel que $L = F(\alpha)$. Soient ϕ, $\psi \in \mathrm{Hom}_{K-alg}(L,K)$. Par le théorème 13, il existe un isomorphisme qui envoie $\phi(\alpha)$ sur $\psi(\alpha)$ et qui laisse F invariant. Donc il existe $g \in G$ tel que $g \cdot \phi(\alpha) = \psi(\alpha)$.

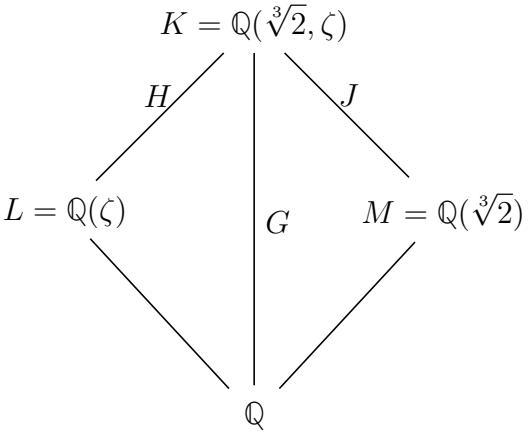
□

Remarque 48 En particulier, pour tout ϕ, l'application $G/H \to \mathrm{Hom}_{K-alg}(L,K), gH \mapsto g\phi$ est un isomorphisme de G-ensembles.

Théorème 49 rappel : propriété universelle du produit tensoriel d'algèbres
Pour tous $\phi : A \to C$ et $\psi : B \to C$ morphismes d'algèbres commutatives, il existe un unique morphisme $\rho : A \otimes_F B \to C$ tel que $\rho(a \otimes 1) = \phi(a)$ et $\rho(1 \otimes b) = \psi(b)$ pour tous $a \in A, b \in B$.

Définition 50 Un *compositum* de L et M est un triplet (C, ι_L, ι_M) où C/F est un corps, $\iota_L : L \to C$ et $\iota_M : M \to C$ des morphismes de F-algèbres, et où C est généré par $\iota_L(L)$ et $\iota_M(M)$.

Exemple 51 Considérons le shéma suivant, avec $\zeta := e^{\frac{2i\pi}{3}}$.



On a déjà vu dans un précédent exemple que $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$ est une extension galoisienne, car $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ est le corps de décomposition du polynôme séparable $X^3 - 2 \in \mathbb{Q}[X]$.

Posons $\iota_{1,L} : L \to \mathbb{Q}(\sqrt[3]{2})$ l'inclusion et $\iota_{1,M} : M \to \mathbb{Q}(\sqrt[3]{2})$ l'inclusion. Alors il est clair que $\mathbb{Q}(\sqrt[3]{2})$ est engendré par $\iota_{1,L}(L)$ et $\iota_{1,M}(M)$, donc $(K, \iota_{1,L}, \iota_{1,M})$ est un compositum de L et M.

Définition 52 m Un *morphisme de compositums* (C, ι_L, ι_M) et (C', ι'_L, ι'_M) est un morphisme de corps F-linéaire $f : C \to C'$ tel que $\iota'_L = f \circ \iota_L$ et $\iota'_M = f \circ \iota_M$.
On notera $\sim$ la relation d'isomorphie entre compositums.

Lemme 53 Les compositums de L et M, à isomorphisme près, forment un ensemble fini. Il y a une bijection entre cet ensemble et les quotients de $L \otimes_F M$. Pour $f : L \otimes_F M \to C$ surjective, le compositum associé est (C, ι_L, ι_M) et $\iota_L = f \circ (id_L \otimes 1)$, $\iota_L = f \circ (id_M \otimes 1)$.
Tout compositum est isomorphe à un compositum dont le corps est contenu dans K.

Preuve. La deuxième assertion découle directement de la propriété universelle du produit tensoriel d'algèbres, en prenant $A = L$, $B = M$, $C = C$, et $(\phi, \psi) = (\iota_L, \iota_C)$
Comme $L \otimes_F M$ est de dimension finie sur F, par le point précédent, l'ensemble des compositums de L et M à isomorphisme près est fini.
Enfin, il reste à montrer la dernière assertion.
Notons $L = F[X]/(f(X))$ avec $f(X) \in F[X]$ irréductible.
Alors $L \otimes_F M = F[X]/(f(X)) \otimes_F M = M[X]/(f(X))$.
Notons $f(X) = \prod_i f_i(X)$ la décomposition de $f(X)$ en facteurs irréductibles en tant que polynôme dans $M[X]$. On a alors $L \otimes_F M = \prod_i M[X]/(f_i(X))$.
De plus, on sait que les f_i sont scindés dans $L[X]$, donc dans $K[X]$, donc pour tout i, $M[X]/(f_i(X)) \subset K$ à isomorphisme près, car K contient M et K contient un corps de décomposition des f_i. D'où la conclusion.

□

Définition 54 Sous les hypothèses du lemme précédent, on note $Compos(L, M)$ l'ensemble des compositums de L et M dont le corps sous-jacent est contenu dans K.

Lemme 55 L'application $H : \mathrm{Hom}_{F-alg}(L, K) \to Compos(L, M), \phi \mapsto (\phi(L).M, \phi, incl_{M/K}$ induit une bijection de $J \backslash \mathrm{Hom}_{F-alg}(L, K)$ dans $Compos(L, M)/\sim$.

Preuve. Soit $\phi \in \mathrm{Hom}_{F-alg}(L, K)$. La multiplication par $g \in J$ induit un isomorphisme $(\phi(L).M, \phi, incl_{M/K}) \to (g.\phi(L).M, g.\phi, g.incl_{M/K})$. Comme $g \in J$, on sait que g fixe M point par point, donc $g.incl_{M/K} = incl_{M/K}$. On trouve donc que l'isomorphisme induit par g est de la forme $H(\phi) \to H(g.\phi)$.
Montrons l'injectivité de l'application induite par H : Soient $\phi, \phi' \in \mathrm{Hom}_{F-alg}(L, K)$, et soit $f : \phi(L).M \to \phi'(L).M$ un isomorphisme de compositums. Alors $f \circ incl_{K/M} = incl_{K/M}$. Et

f est l'identité sur M, donc f peut s'étendre en un isomorphisme $g \in J$. Comme f est un morphisme de compositums, $g\phi = \phi'$, donc $\phi \sim \phi'$.
Montrons maintenant la surjectivité de l'application induite par H : Par le lemme précédent, chaque compositum dans $Compos(L, M)$ est isomorphe à un compositum où $\iota_M = incl_{M/K}$. Soit $\iota_L : L \to K$ un F-morphisme, $\iota_L(L) \subset K$ donc on peut choisir $\phi = \iota_L$.

□

Proposition 56 L'application $J\backslash G/H \to Compos(L, M)/\sim, JgH \mapsto (gL.M, l \mapsto gl.1_M, incl_{M/K})$ est une bijection.

Preuve. Cette proposition découle directement des lemmes précédents.

□

Définition 57 Dans une extension finie de corps K/F, la *norme* d'un élément x est le déterminant de l'application multiplication à gauche par x sur K, vu comme un F-espace vectoriel. On la note $N_{K/F}(x)$.

Remarque 58 Avec les hypothèses précédentes sur les corps K et L, et pour $x \in K^\times$, on a

— $N_{K/\mathbb{Q}}(x) := \prod_{g \in G} g \cdot x = (\sum_{g \in G} g) \cdot x = N_G \cdot x$
— $N_{K/L}(x) = N_H \cdot x$
— pour $x \in L^\times$, $N_{L/\mathbb{Q}}(x) = \prod_{g \in G/H} g \cdot x$.

Notation Pour tout $R[G]$-module V, tout compositum $\mathcal{C} = (C, \iota_L, \iota_M)$ de L et M, peut être vu comme un élément de $J\backslash G/H$, via la bijection de la proposition 56. On a vu de plus que tout élément de JgH peut être vu comme une application de V^J dans V^H. On notera cette application $x \mapsto \mathcal{C} \cdot x$.

Théorème 59 Pour tout $R[G]$-module V et tout compositum $\mathcal{C} = (C, \iota_L, \iota_M)$ de L et M, on a :
$\forall x \in V^J, \mathcal{C}.x = N_{C/M}(\iota_L(x))$.

Lemme 60 Avec les notations précédentes, le corps fixé par $H \cap (gJg^{-1}) < G$ est le corps C.

Preuve. (preuve du lemme)

Notons $\tilde{L}$ le corps fixé par gJg^{-1}. Pour tout $\tilde{\ell} \in \tilde{L}$, pour tout $j \in J$, $g \circ j \circ g^{-1}(\tilde{\ell}) = \tilde{\ell}$, donc $j \circ g^{-1}(\tilde{\ell}) = g^{-1}(\tilde{\ell})$, donc j fixe $g^{-1}(\tilde{L})$, donc $g^{-1}(\tilde{L}) = L$, l'autre inclusion vient du fait que J et $g^{-1}Jg$ ont le même cardinal, donc fixent un corps de même indice. Donc $\tilde{L} = g(L) = \iota_L(L)$.

Notons maintenant $\tilde{C}$ le corps fixé par $H \cap (gJg^{-1})$.
Tous les éléments de M et de $\iota_L(L)$ sont dans $\tilde{C}$, donc leur sous-corps engendré C est inclu dans $\tilde{C}$.
Pour montrer l'autre inclusion, notons N le sous-groupe de G qui fixe C. Alors N est inclu dans H et dans gJg^{-1} donc dans leur intersection, donc $\tilde{C} \subset C$.

□

Preuve. (preuve du théorème) Soit $\mathcal{C} = (C, \iota_L, \iota_M)$ un compositum de L et M. On a vu que $\mathcal{C} = (gL.M, l \mapsto gl.1_M, incl_{K/M})$ pour un unique $JgH \in J\backslash G/H$.
Alors $\mathcal{C}.x = \prod_{\delta \in HgJ/J} \delta x = \prod_{\substack{\delta \in G/J \\ HgJ = H\delta J}} \delta x$
On veut faire un changement de variable de la forme $\delta = hg$. Pour $h, h' \in H$ on a $hgJ = h'gJ$, si et seulement si il existe $j \in J$ tel que $h = h'(gjg^{-1})$, donc si et seulement si $\overline{h} = \overline{h'}$ dans $H/(H \cap (gJg^{-1}))$.
Donc $\mathcal{C}.x = \prod_{h \in H/(H \cap (gJg^{-1}))} hgx$

En injectant le résultat du lemme dans la formule $\mathcal{C}.x = \prod_{h \in H/(H \cap (gJg^{-1}))} hgx$, on obtient finalement $\mathcal{C}.x = N_{C/M}(\iota_L(x))$.

□

5 Généralisation des relations de normes

Soit G un groupe fini. On commence par montrer une condition nécessaire et suffisante pour l'existence d'une relation de norme sur $\mathbb{Q}$ par rapport à un ensemble $\mathcal{H}$ de sous-groupes. On s'en inspirera ensuite pour trouver une généralisation.

Proposition 61 Si $\mathcal{H}$ est un ensemble de sous-groupes de G, alors il existe une relation de norme sur $\mathbb{Q}$ par rapport à $\mathcal{H}$ si et seulement si il existe un morphisme surjectif de G-modules $\sum_{H \in \mathcal{H}} \mathbb{Q}[G/H]^{m_H} \to \mathbb{Q}[G]$, avec $(m_H)_{H \in \mathcal{H}}$ des entiers naturels.

Preuve. Supposons tout d'abord l'existence d'une relation de norme de la forme $1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$, avec $\mathcal{H} = \{H_1, \cdots, H_\ell\}$. Posons $\phi : \sum_{i=1}^{\ell} \mathbb{Q}[G/H_i] \to \mathbb{Q}[G], (x_1, \cdots, x_\ell) \mapsto \sum_{i=1}^{\ell} a_i N_{H_i} x_i$, où mH_i.
ϕ est bien un morphisme de G-modules, et comme $1 = \sum_{i=1}^{\ell} a_i N_{H_i} b_i$, ϕ prend la valeur 1 en $(b_1, \cdots, b_\ell)$. Donc ϕ est bien surjectif.
Réciproquement, supposons qu'il existe $\phi : \sum_{i=1}^{\ell} \mathbb{Q}[G/H_i]^{m_{H_i}} \to \mathbb{Q}[G]$ un morphisme surjectif

de G-modules. On peut décomposer ϕ de la manière suivante : pour tout $x = (x_1, \cdots, x_\ell) \in \sum_{i=1}^{\ell} \mathbb{Q}[G/H_i]^{m_{H_i}}$, on a $\phi(x) = \sum_{i=1}^{\ell} \phi_i(x_i)$, avec pour tout i, $\phi_i : \mathbb{Q}[G/H_i] \to \mathbb{Q}[G]$. Alors, pour tout i, ϕ_i est aussi un morphisme de G-module. Par conséquent, pour tout $g \in G$, pour tout $1 \leq i \leq l$, et pour tout $x_i \in \mathbb{Q}[G/H_i]$, $g \cdot \phi_i(x) = \phi_i(g \cdot x)$.
En particulier, pour $h \in H_i$, $h \cdot \phi_i(gH_i) = \phi_i(h \cdot gH_i) = \phi_i(ghH_i) = \phi_i(gH_i)$.
Donc $\phi_i(G/H_i) \subset \mathbb{Q}[G]^{H_i} = N_{H_i} \cdot \mathbb{Q}[G]$.

Enfin, comme ϕ est surjective, et l'image de ϕ est contenu dans $\sum_{i=1}^{\ell} \mathbb{Q}[G] N_{H_i} \mathbb{Q}[G]$,

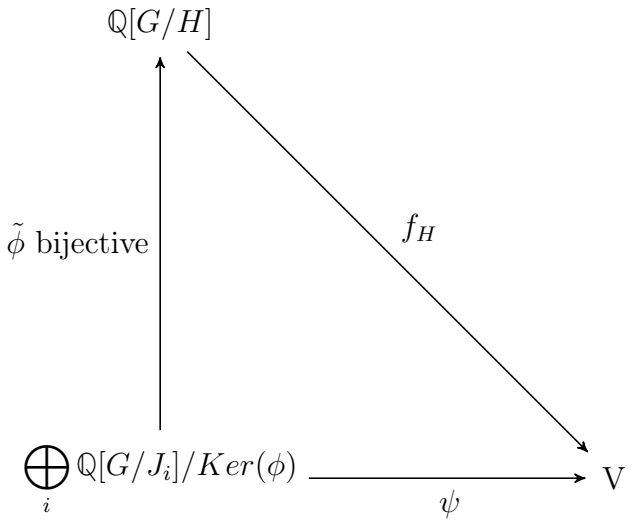
on a $\mathbb{Q}[G] = \sum_{i=1}^{\ell} \mathbb{Q}[G] N_{H_i} \mathbb{Q}[G]$,
d'où l'existence d'une relation de norme sur $\mathbb{Q}$ par rapport à $\mathcal{H}$.

□

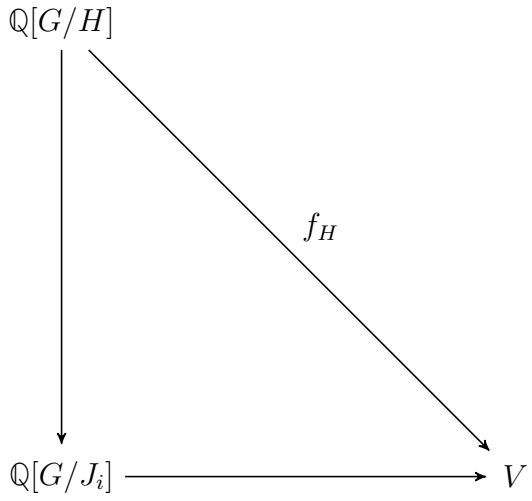
Théorème 62 Soient H et $J_1, \cdots, J_\ell$ des sous-groupes de G. On note $\mathcal{J} = \{J_i\}$ Les deux assertions suivantes sont équivalentes.

1. Il existe un morphisme de $\mathbb{Q}[G]$-modules surjectif $\phi : \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$.
2. Pour tout $\mathbb{Q}[G]$-module V, V^H est le sous $\mathbb{Q}[H\backslash G/H]$-module de V^H engendré par les images de tous les V^J par l'action des $\mathbb{Q}[H\backslash G/J]$ avec $J \in \mathcal{J}$.

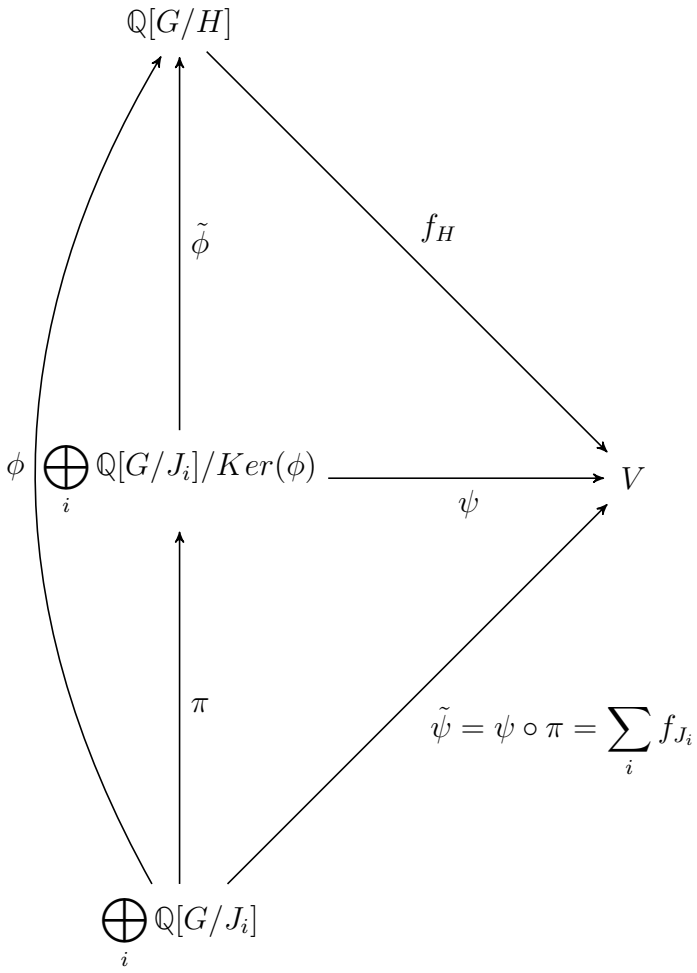
Preuve. — Preuve du sens direct :
Si on a $\phi : \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$, on note $\phi = \sum_{i=1}^{\ell} \phi_i$ avec $\phi_i : \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$. Soit V un $\mathbb{Q}[G]$-module et soit $f_H \in V^H \simeq \mathrm{Hom}_{\mathbb{Q}[G]}(\mathbb{Q}[G/H], V)$ (par la proposition 39). On pose $\tilde{\phi} : \left(\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i] \right) / Ker(\phi) \xrightarrow{\sim} \mathbb{Q}[G/H]$. Pour tout $x = (x_1, \cdots, x_\ell) \in \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]$, on peut poser
$\psi(x) := f_H \circ \tilde{\phi}(x) \in \mathrm{Hom}_{\mathbb{Q}[G]}(\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i])/Ker(\phi), V)$. On a alors $f_H = \psi \circ \tilde{\phi}^{-1}$.



On veut écrire f_H comme une combinaison linéaire en $\mathbb{Q}[H\backslash G/H] = End(\mathbb{Q}[G/H], \mathbb{Q}[G/H])$ de fonctions f_{H,J_i} qui admettent une décomposition de la forme

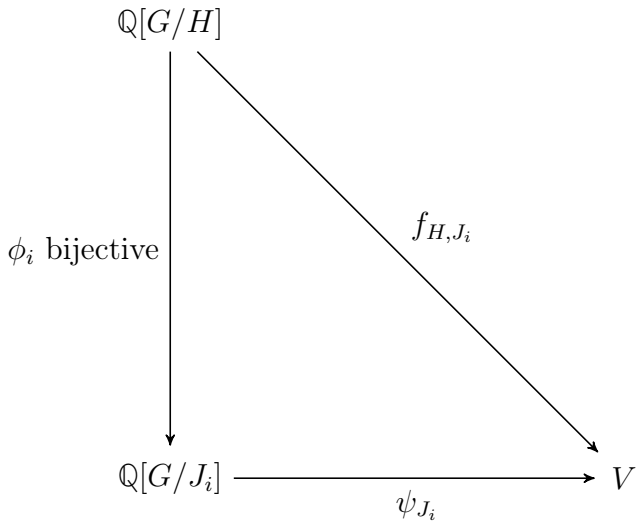


Pour cela, on considère le diagramme suivant : (où π est la projection canonique de $\bigoplus_i \mathbb{Q}[G/J_i]$ vers $\bigoplus_i \mathbb{Q}[G/J_i]/Ker(\phi)$, qui est surjective)



Comme $\tilde{\phi}^{-1}$ est un morphisme de $\mathbb{Q}[G]$-modules sur $(\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i])/Ker(\phi)$, on peut le prolonger en un morphisme de $\mathbb{Q}[G]$-modules sur $\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]$.

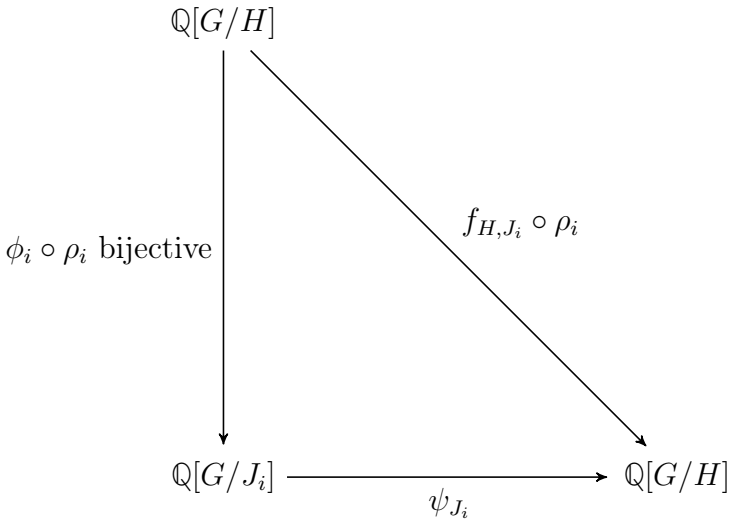
— Preuve du sens indirect :
Si l'assertion 2 est vérifiée, alors pour tout $\mathbb{Q}[G]$-module V, et pour tout $f_H \in V^H$, on peut écrire $f_H = \sum_i a_i H g_i H f_{H,J_i}$ avec $a_i \in \mathbb{Q}[G], g_i \in G$, et où f_{H,J_i} se décompose selon le diagramme suivant :



On veut alors construire $\phi : \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$ un morphisme surjectif.

Posons $V = \mathbb{Q}[G/H]$ et $f_H = id : V \to V$.

Les $a_i H g_i H$ correspondent d'après la proposition 42 à des éléments de $\mathrm{Hom}(\mathbb{Q}[G/H], \mathbb{Q}[G/H])$, qu'on notera ρ_i. On a donc le diagramme ci dessous :



On a alors $\sum_i \psi_{J_i} \circ \phi_i \circ \rho_i = id$. Donc $\sum_i \psi_{J_i}$ est surjectif.

On a donc bien un morphisme surjectif de $\bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i]$ dans $\mathbb{Q}[G/H]$.

□

La propriété consistant en l'existence d'un morphisme $\phi : \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$ paraît prometteuse car elle ressemble beaucoup à la caractérisation des relations de normes donnée en proposition 61. Cherchons d'autres propositions équivalentes.

Pour ce faire, nous admettrons le lemme suivant :

Lemme 63 Soient K et L des sous corps de $\mathbb{C}$, avec $K \subset L$. Alors :

— Pour tout $K[G]$-module V, et $H \leq G$, $\dim_K(V^H) = \dim_L(V \otimes_K L)^H$. Donc $V^H \neq 0$ si et seulement si $V \otimes_K L)^H \neq 0$.

— Tout $L[G]$-module simple est isomorphe à un sous-module de $V \times_K L$ pour V un $K[G]$-module.

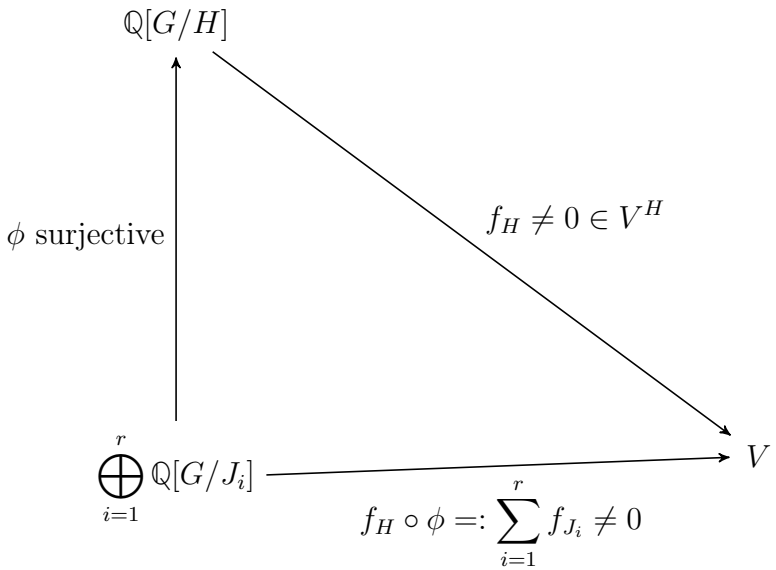
Théorème 64 Soient H et $J_1, \cdots, J_\ell$ des sous-groupes de G. On note $\mathcal{J} = \{J_i\}$. Les assertions suivantes sont équivalentes.

1. Il existe un morphisme de $\mathbb{Q}[G]$-modules surjectif $\phi : \bigoplus_{i=1}^{\ell} \mathbb{Q}[G/J] \to \mathbb{Q}[G/H]$.
2. Pour tout $\mathbb{Q}[G]$-module V simple, si $V^H \neq 0$, alors il existe $J \in \mathcal{J}$ tel que $V^J \neq 0$.
3. En notant $e_1, \cdots, e_r$ les éléments centraux primitifs idempotents de $\mathbb{Q}[G]$, pour tout $1 \leq i \leq r$, si $e_i N_H \neq 0$, alors l existe $J \in \mathcal{J}$ tel que $e_i N_J \neq 0$.
4. Pour tout $\overline{\mathbb{Q}}[G]$-module V simple, si $V^H \neq 0$, alors il existe $J \in \mathcal{J}$ tel que $V^J \neq 0$.
5. Pour tout $\mathbb{C}[G]$-module V simple, si $V^H \neq 0$, alors il existe $J \in \mathcal{J}$ tel que $V^J \neq 0$.
6. La norme N_H est dans l'idéal bilatère $\langle N_J; J \in \mathcal{J} \rangle_{\mathbb{Q}[G]}$.

Preuve. — Preuve que 1. $\Rightarrow$ 2.

On sait qu'il y a un isomorphisme entre les éléments de V^H et ceux de $Hom_{\mathbb{Q}[G]alg}(\mathbb{Q}[G/H], V)$, et de même entre les éléments de V^{J_i} et ceux de $Hom_{\mathbb{Q}[G]alg}(\mathbb{Q}[G/J_i], V)$ pour tout i.

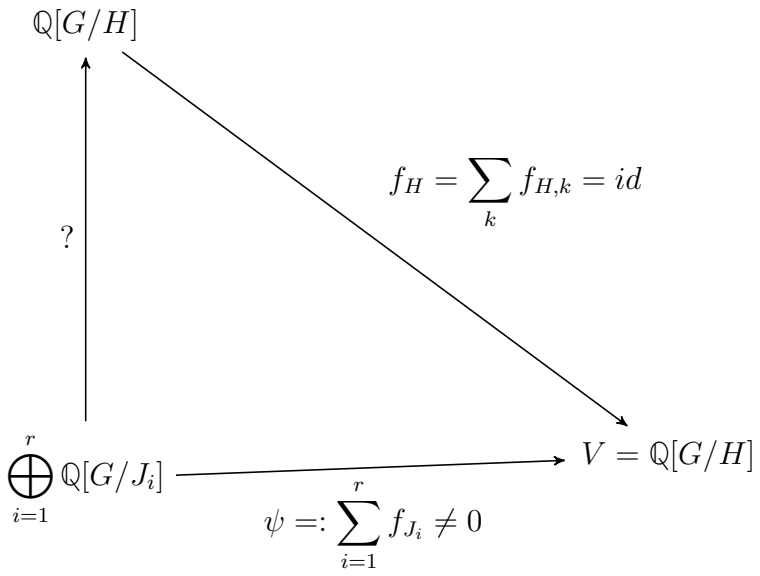
Si 1. est vraie, on a le diagramme ci dessous :



Donc $\sum_{i=1}^{r} f_{J_i}$ est non nulle, donc au moins l'un des f_{J_i} est non nul, ce qui permet de conclure.

— Preuve que 2. $\Leftrightarrow$ 3. :
Si on pose V_i le $\mathbb{Q}[G]$-module simple (unique à isomorphisme près) tel que $e_i V_i \neq 0$, alors $\mathbb{Q}[G]/(1-e_i)$ agit fidèlement sur V_i, donc $e_i N_H = 0$ si et seulement si $N_H \cdot V_i = 0$, donc si et seulement si $(\frac{1}{|H|} N_H) \cdot V_i = 0$ ce qui est équivalent à $V_i^H = 0$.

— Preuve que 2. $\Rightarrow$ 1. :
On suppose que 2. est vérifiée. Soit $V = \mathbb{Q}[G/H]$. Alors V est un $\mathbb{Q}[G]$-module et V se décompose en $V = \bigoplus_k V_k$ où les V_k sont simples. Pour tout k, on pose $f_{H,k} = id : V_k \to V_k \in V_k^H$. On a alors le diagramme suivant :



Comme V est simple et ψ est non nul, ψ est surjectif. Donc on a bien un morphisme surjectif $\bigoplus_{i=1}^{r} \mathbb{Q}[G/J_i] \to V = \mathbb{Q}[G/H]$, d'où la conclusion.

— Preuve que 3. $\Leftarrow$ 4.
On suppose 3. Soit W un $\overline{\mathbb{Q}}[G]$-module simple. W est isomorphe à un sous-module de $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ avec V un $\mathbb{Q}[G]$-module simple. On a $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^{k} W_j$ où les W_j sont des $\overline{\mathbb{Q}}[G]$-modules simples. W est donc isomorphe à l'un des W_j. De plus, les W_j sont conjugués galoisiens deux à deux. Donc $dim_{\overline{\mathbb{Q}}} W_j^H = dim_{\overline{\mathbb{Q}}} W_1^H$ pour tout j. Donc, si W^H est non nul, V^H est non nul. Donc, par 3., il existe $J \in \mathcal{J}$ tel que V^J est non nul. Par ce qui précéde, on a alors $W^J \neq 0$.

— Preuve que 4. $\Rightarrow$ 5.
Par le lemme 63, les $\mathbb{C}[G]$-modules simples sont exactement les $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$ où V est un $\overline{\mathbb{Q}}[G]$-module simple. Il en résulte immédiatement que 4. $\Rightarrow$ 5.

— Preuve que 5. $\Rightarrow$ 4.
On supose 5., soit V un $\overline{\mathbb{Q}}[G]$-module simple. Si $V^H \neq 0$, alors $(V \times_{\overline{\mathbb{Q}}} \mathbb{C})^H \neq 0$. Donc, par

4., il existe $J \in \mathcal{J}$ tel que $(V \otimes_{\overline{\mathbb{Q}}} \mathbb{C})^J \neq 0$, donc $V^J \neq 0$.

— Preuve que 4. $\Rightarrow$ 3.
On suppose 4., soit V un $\mathbb{Q}[G]$-module simple tel que $V^H \neq 0$.
On pose $V \times_{\mathbb{Q}} \overline{\mathbb{Q}} \simeq \bigoplus_{j=1}^{k} W_j$. On a vu que $W_j^H \neq 0$ pour tout j.
Donc il existe $J \in \mathcal{J}$ tel que $W_1^J \neq 0$.
Donc, par le lemme précédent, $V^J \neq 0$.

— Preuve que 3. $\Leftrightarrow$ 6.
Pour tout idéal bilatère I de $\mathbb{Q}[G]$, on a $I = \sum_{i=1}^{r} e_i I$. De plus, $e_i I$ se projette de manière isomorphe dans un idéal bilatère de l'algèbre $\mathbb{Q}[G]/(1-e_i)$ qui est simple. Donc $e_i I$ vaut soit $e_i\mathbb{Q}[G]$, soit zéro. En appliquant ce résultat à $I = \langle N_J; J \in \mathcal{J}\rangle_{\mathbb{Q}[G]}$, on trouve bien l'équivalence voulue.

□

Remarque 65 La sixième assertion peut se reformuler de la manière suivante :
il existe $(a_i)_{1\leq i\leq \ell}, (b_i)_{1\leq i\leq \ell}$ des éléments de $\mathbb{Q}[G]$ tels que $N_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$.
De cette manière, il apparaît clairement que les assertions précédentes définissent bien une généralisation des relations de normes.

Définition 66 Avec les mêmes notations que dans le théorème 64, si ces assertions sont vérifiées, on dira que G admet une *relation de norme étendue* sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$.

6 Algorithmique

6.1 Recherche de relations de normes étendues

Dans un premier temps, on cherche à trouver un algorithme qui étant donné G un groupe fini, $H < G$ et $\mathcal{J}$ un ensemble de sous-groupes de G, renvoie vrai si et seulement si G admet une relation de norme étendue par rapport à H et $\mathcal{J}$. Pour cela, plusieurs méthodes sont possibles.

Remarque 67 Le langage de programmation que j'ai utilisé pour implémenter tous les algorithmes décrits dans ce mémoire est SageMaths.

6.1.1 Méthode de l'idéal bilatère

Cette méthode utilise le fait que G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$ si et seulement si dN_H est dans l'idéal bilatère $\langle N_J; J \in \mathcal{J}\rangle_{\mathbb{Z}[G]}$, pour un entier naturel d non nul, à savoir la caractérisation 6. du théorème 64.

Notons $W := \langle N_J; J \in \mathcal{J} \rangle_{\mathbb{Z}[G]} = \langle gN_Jh; J \in \mathcal{J}, (g,h) \in G^2 \rangle_{\mathbb{Z}}$
$= \langle gN_Jh; J \in \mathcal{J}, g \in G, h \in G/J \rangle_{\mathbb{Z}}$.
Notons $(g_iN_{J_i}h_i)_{1 \leq i \leq n}$ la famille ordonnée des éléments de $\{gN_Jh; J \in \mathcal{J}, g \in G, h \in G/J\}$. Alors, pour $d \in \mathbb{N}^*$, $dN_H \in W$ si et seulement si il existe une famille $(a_i)_{1 \leq i \leq n}$ d'entiers tels que $dN_H = \sum_i a_i g_i N_{J_i} h_i$.
En remplaçant dans cette expression les N_{J_i} par $\sum_{j \in J_i} j$, puis en développant, on trouve alors $dN_H = \sum_{g \in G} \alpha_g g$, où les α_g sont des entiers, qui sont l'unique résultat d'un système d'équation en les a_i.
En numérotant les éléments de G de telle sorte que les éléments numérotés de 1 à $|H|$ soient les éléments de H, l'équation $dN_H = \sum_{g \in G} \alpha_g g$ peut s'écrire sous forme matricielle :

$$\begin{pmatrix} \alpha_{g_1} & & & \\ & \alpha_{g_2} & & \\ & & \ddots & \\ & & & \alpha_{g_{|G|}} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} d \\ \vdots \\ d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Finalement, G admet une relation de norme étendue sur $\mathbb{Z}$ par rapport à H et $\mathcal{J}$ si et seulement si il existe $(a_i)_{1 \leq i \leq n}$ tel que les α_g correspondants valent d si $g \in H$ et 0 sinon.
D'où l'algorithme ci-dessous :

Algorithme 68
entrée : Un groupe G, un sous-groupe H et un ensemble de sous-groupes $\mathcal{J}$.
sortie : Vrai si et seulement si G admet une relation de norme étendue sur $\mathbb{Z}$ par rapport à H et $\mathcal{J}$.

1. Créer des variables $(a_i)_{1 \leq i \leq n}$ où n est le cardinal de $\{gN_Jh; J \in \mathcal{J}, g \in G, h \in G/J\}$.
2. Développer la somme $\sum_i a_i g_i N_{J_i} h_i$ pour obtenir une somme de la forme $\sum_{g \in G} \alpha_g g$, où l'on sait exprimer les α_g comme des sommes de a_i.
3. Ecrire l'équation $dN_H = \sum_{g \in G} \alpha_g g$ comme un système d'équations sur les a_i.
4. retourner Vrai si ce système a une solution dans $\mathbb{Z}^n$, Faux sinon.

L'avantage de cette méthode est qu'elle permet aussi de calculer les coefficients de la relation de norme étendue.

Remarque 69 Le langage Sagemath propose une fonction pour déterminer si un système

donné, écrit sous forme matricielle, admet des solutions dans $\mathbb{Z}$. C'est pourquoi l'étape 4 n'est pas plus détaillée.

6.1.2 Méthode des éléments centraux primitifs idempotents.

Cette méthode utilise le fait que G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$ si et seulement si, en notant $e_1, \cdots, e_r$ les éléments centraux primitifs idempotents de $\mathbb{Q}[G]$, si pour un i quelconque $e_i N_H \neq 0$, alors il existe $J \in \mathcal{J}$ tel que $e_i N_J \neq 0$, à savoir la caractérisation 3. du théorème 64.

Remarque 70 Le langage Sagemath propose une fonction permettant de calculer directement les éléments centraux primitifs idempotents de $\mathbb{Q}[G]$.

Algorithme 71
entrée : Un groupe G, un sous-groupe H et un ensemble de sous-groupes $\mathcal{J}$.
sortie : Vrai si et seulement si G admet une relation de norme étendue sur $\mathbb{Z}$ par rapport à H et $\mathcal{J}$.

- Calculer $e_1, \cdots, e_r$ les éléments centraux primitifs idempotents de $\mathbb{Q}[G]$
- Pout tout $e \in \{e_1, \cdots, e_r\}$
  - Si $eN_H \neq 0$:
    - Calculer eN_J pour tout $J \in \mathcal{J}$.
    - Si $eN_J = 0$ pour tout J, renvoyer Faux.
- renvoyer Vrai.

Cette méthode est plus rapide que la précédente. L'étape qui prend le plus de temps est le calcul des éléments centraux primitifs idempotents.

6.1.3 Méthode des caractères

Cette méthode utilise le fait que G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$ si et seulement si, pour tout $\mathbb{C}[G]$-module V simple, si $V^H \neq \{0\}$, alors il existe $J \in \mathcal{J}$ tel que $V^J \neq 0$, à savoir la caractérisation 5. du théorème 64.
Un $\mathbb{C}[G]$-module simple V peut être vu, à isomorphisme près, comme un $\mathbb{C}^n$, avec $n = |G|$, sur lequel G agit. Donc il peut être vu comme une représentation $\rho_V : G \to GL_n(\mathbb{C})$.
Par conséquent, à chaque $\mathbb{C}[G]$-module simple V, on peut associer un caractère irréductible $\chi_V : G \to \mathbb{C}, g \mapsto tr(\rho_V(g))$. Et réciproquement, à chaque caractère irréductible, on peut associer un $\mathbb{C}[G]$-module simple.

Remarque 72 Avec les notations précédentes, pour tout $\mathbb{C}[G]$-module simple V, pour tout sous-groupe $H < G$, en notant $\mathbb{1}$ le caractère de la représentation triviale, et $res_H\chi$ la restriction à H d'un caractère χ, on a $|V^H| =< \mathbb{1}, res_H\chi_V >_H = \frac{1}{|H|}\sum_{h\in H}\chi_V(h)$.

On en déduit l'algorithme ci-dessous.

Algorithme 73
entrée : Un groupe G, un sous-groupe H et un ensemble de sous-groupes $\mathcal{J}$.
sortie : Vrai si et seulement si G admet une relation de norme étendue sur $\mathbb{Z}$ par rapport à H et $\mathcal{J}$.

- Calculer $\chi_1, \cdots, \chi_r$ les caractères irréductibles de G.
- Pout tout $\chi \in \{\chi_1, \cdots, \chi_r\}$
  - Si $< \mathbb{1}, res_H\chi_V >_H \neq 0$:
    - Calculer $< \mathbb{1}, res_J\chi_V >_J$ pour tout $J \in \mathcal{J}$.
    - Si $< \mathbb{1}, res_J\chi_V >_J = 0$ pour tout J, renvoyer Faux.
- renvoyer Vrai.

Remarque 74 Le langage Sagemath propose une fonction permettant de calculer directement la table de caractère du groupe G. Elle est en outre plus rapide que celle qui calcule les éléments centraux primitifs idempotents de $\mathbb{Q}[G]$.

6.1.4 Recherche de relation de normes

On cherche à présent un algorithme qui, étant donnés un groupe G et $H < G$ un sous-groupe, détermine si il existe un ensemble $\mathcal{J}$ de sous-groupes de G tel que G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$.

Remarque 75 On cherchera uniquement les relations de normes étendues avec tous les éléments de $\mathcal{J}$ de cardinal supérieur à celui de H. En effet, dans la suite, on se placera dans le cas où G est le groupe de Galois d'une extension de corps $K/\mathbb{Q}$, et on cherchera à utiliser la relation de norme pour calculer le groupe des S-unités de K^H en se ramenant à ceux des K^{J_i}. On veut donc que pour tout i, $[K^{J_i} : \mathbb{Q}] < [K^H : \mathbb{Q}]$.
Par ailleurs, pour tout $H < G$, G admet trivialement une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J} := \{H\}$.

Lemme 76 Si G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J} = \{J_1, \cdots, J_l\}$, soit $\tilde{J}_1$ un sous-groupe de G conjugué à J_1. Alors G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\tilde{\mathcal{J}} = \{\tilde{J}_1, J_2, \cdots, J_l\}$.

Preuve. Si G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J} = \{J_1, \cdots, J_l\}$, soit $\tilde{J}_1 = g^{-1}J_1 g$ avec $g \in G$. Alors, il existe un morphisme surjectif de $\mathbb{Q}[G]$-modules $\phi : \bigoplus_{i=1}^{l} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$.
De plus, comme J_1 et $\tilde{J}_1$ sont conjugués, il existe un isomorphisme de $\mathbb{Q}[G]$-modules de $\mathbb{Q}[G/J_1]$ dans $\mathbb{Q}[G/\tilde{J}_1]$.
Donc il existe $\tilde{\phi}$ un morphisme surjectif de $\mathbb{Q}[G]$-modules de $\mathbb{Q}[G/\tilde{J}_1] \oplus \bigoplus_{i=2}^{l} \mathbb{Q}[G/J_i]$ dans $\mathbb{Q}[G/H]$.
D'où la conclusion.

□

Lemme 77 Si G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J} = \{J_1, \cdots, J_l\}$, soit J_{l+1} un sous-groupe de G, alors G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J} = \{J_1, \cdots, J_l, J_{l+1}\}$,

Preuve. Supposons qu'il existe un morphisme surjectif de $\mathbb{Q}[G]$-modules $\phi : \bigoplus_{i=1}^{l} \mathbb{Q}[G/J_i] \to \mathbb{Q}[G/H]$. La projection naturelle $\pi : \bigoplus_{i=1}^{l+1} \mathbb{Q}[G/J_i] \to \bigoplus_{i=1}^{l} \mathbb{Q}[G/J_i]$ est un morphisme surjectif de $\mathbb{Q}[G]$-modules, donc $\tilde{\phi} := \phi \circ \pi$ est un morphisme surjectif de $\mathbb{Q}[G]$-modules de $\bigoplus_{i=1}^{l+1} \mathbb{Q}[G/J_i]$ dans $\mathbb{Q}[G/H]$. D'où la conclusion.

□

Algorithme 78

Entrée : G un groupe fini, $H < G$ un sous-groupe.
Sortie : $\mathcal{J}$ un ensemble de sous-groupes de G de cardinaux supérieurs à $|H|$, tel que G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$, et Faux si un tel $\mathcal{J}$ n'existe pas.

- Calculer une liste L des sous-groupes de G, à conjugaison près.
- Créer $\mathcal{J}$ une liste vide
- Pour J dans L de cardinal supérieur à celui de H :
  - ajouter J dans $\mathcal{J}$
  - si G admet une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$, renvoyer J.
- Renvoyer Faux.

Remarque 79 Comme l'objectif est de considérer le cas où G est le groupe de Galois d'une extension de corps $K/\mathbb{Q}$, et d'utiliser la relation de norme étendue pour faire le lien entre K^H et les K^{J_i}, on a intérêt à ce que les J_i soient le plus grand possible, afin de se rammener à des

corps de degrés le plus petit possible.
Dans le cas où l'algorithme renvoie un ensemble $\mathcal{J}$ de sous-goupes de G, cet ensemble peut ne pas être optimal, dans le sens où un autre ensemble $\mathcal{J}'$ pourrait convenir également, et contenir moins d'éléments, ou des éléments plus gros. Il y a deux manière d'améliorer ça.

— On peut parcourir les sous-groupes dans L du plus grand au plus petit, afin d'ajouter en priorité les plus grands.

— Une fois que l'algorithme renvoie un ensemble $\mathcal{J}$, on peut vérifier si un sous-ensemble de $\mathcal{J}$ convient également.

Exemple 80 En prenant $G = S_4$, et $H = \langle (2,4,3) \rangle$, alors G admet une raltion de norme étendue par rapport à H et $\mathcal{J} = \{J_1, J_2, J_3, J_4\}$, avec

— $J_1 = \langle (1,4)(2,3), (1,3)(2,4), (2,4,3), (3,4) \rangle$

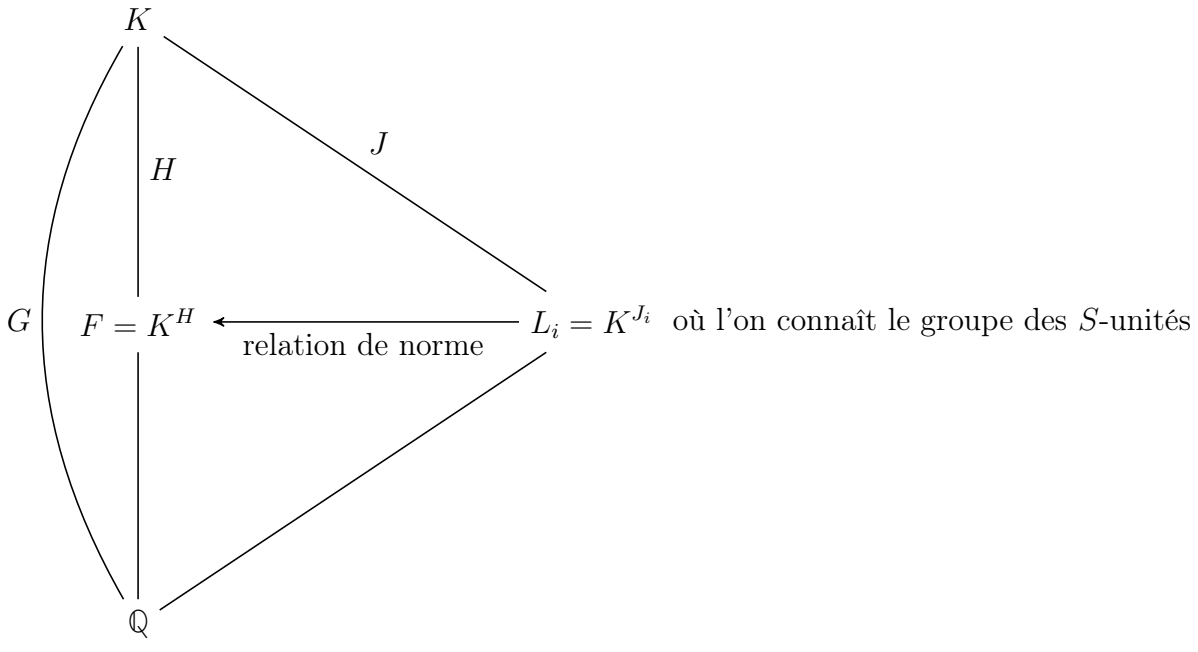
— $J_2 = \langle (1,4)(2,3), (1,3)(2,4), (2,4,3) \rangle$

— $J_3 = \langle (3,4), (2,4,3) \rangle$

— $J_4 = \langle (1,3,2,4), (1,2)(3,4) \rangle$.

6.2 Calcul du groupe des S-unités

Soit $F/\mathbb{Q}$ un corps de nombre, K sa clôture galoisienne, et G le groupe de Galois de $K/\mathbb{Q}$. Soit $H < G$ tel que $F = K^H$. Supposons que G vérifie une relation de norme étendue sur $\mathbb{Q}$ par rapport à H et $\mathcal{J}$, où $\mathcal{J}$ est un ensemble de sous-groupes de G. Soit S un ensemble G-stable d'idéaux premiers non nuls de l'anneau des entiers $\mathcal{O}_K$. Le but de cette sous-section est de trouver un algorithme qui calcule le groupe des S-unités de $F = K^H$ à partir des groupes des S-unités des K^{J_i} pour $J_i \in \mathcal{J}$, en utilisant la relation de norme.



Remarque 81 Le calcul de la clôture galoisienne K et du groupe de Galois G associé peut prendre un certain temps en pratique. Une solution serait de ré-exprimer le problème en termes de pure théorie des corps, sans théorie de Galois, en utilisant la notion de compositum. C'est un problème sur lequel je n'ai pas eu le temps de réfléchir pendant mon stage, mais sur lequel je compte revenir.

6.2.1 Résultats préliminaires

Théorème 82 On suppose que $dN_H = \sum_i a_i N_{J_i} b_i$, avec $d \in \mathbb{N}^*$ et $a_i, b_i \in \mathbb{Z}[G]$. Alors l'exposant du quotient $M^H/(N_H \cdot (\sum_i a_i M^{J_i}))$ est fini et divise $|H|^2 d$.

Preuve. Soit $m \in M^H$. On a $N_H m = |H|m$,
donc $dN_H m = d|H|m$,
donc $(\sum_i a_i N_{J_i} b_i)m = d|H|m$.
Or $(\sum_i a_i N_{J_i} b_i)m = \sum_i a_i N_{J_i}(b_i m)$. Et pour tout i, $N_{J_i}(b_i m) \in M^{J_i}$.
Donc $d|H|m \in (\sum_i a_i M^{J_i})$.
Mais on n'a pas $(\sum_i a_i M^{J_i}) \subset M^H$ en général, donc le quotient $M^H/(\sum_i a_i M^{J_i})$ n'a pas de sens.
Cependant, en composant à gauche par N_H, on obtient $d|H|^2 m \in N_H(\sum_i a_i M^{J_i})$. Et on a bien $N_H(\sum_i a_i M^{J_i}) \subset M^H$. D'où la conclusion.

□

Ce théorème est l'analogue de la proposition 23, pour les relations de normes étendues. Il permet de faire le lien lien entre les corps K^H et K^{J_i}.

Corollaire 83 Avec les mêmes hypothèses que le théorème 83, en notant $\alpha_i = N_H(a_i)$ pour tout i, l'exposant du quotient $\mathcal{O}^\times_{K^H,S}/((\mathcal{O}^\times_{K^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{K^{J_\ell},S})^{\alpha_l})$ est fini et divise $|H|^2 d$.
En particulier, le groupe $\mathcal{O}^\times_{K^H,S}$ est la $(|H|^2 d)$-saturation du groupe
$((\mathcal{O}^\times_{K^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{K^{J_l},S})^{\alpha_l})$.

Notation Dans la suite, on désignera par V le groupe $((\mathcal{O}^\times_{K^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{K^{J_l},S})^{\alpha_\ell})$, avec les notation du corollaire précédent.

6.2.2 Calcul d'une base du groupe V

Dans cette sous section, on s'intéressera au problème intermédiaire suivant : on cherche un algorithme qui, étant données des bases de chaque groupe $\mathcal{O}^\times_{K^{J_i},S}$, renvoie une base de V.

Dans toute cette partie, on supposera qu'on a une relation de la forme $dN_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$, avec $d \in \mathbb{N}^*$ et $a_i, b_i \in \mathbb{Z}[G]$.

Définition 84 Soit M un $\mathbb{Z}[G]$-module. On définit les fonctions

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

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

Proposition 85 Pour tout $\mathbb{Z}[G]$-module M, les deux affirmations suivantes sont vraies.

— L'application $\phi_M \otimes \mathbb{Q}$ est injective.

— L'application $\psi_M \otimes \mathbb{Q}$ est surjective.

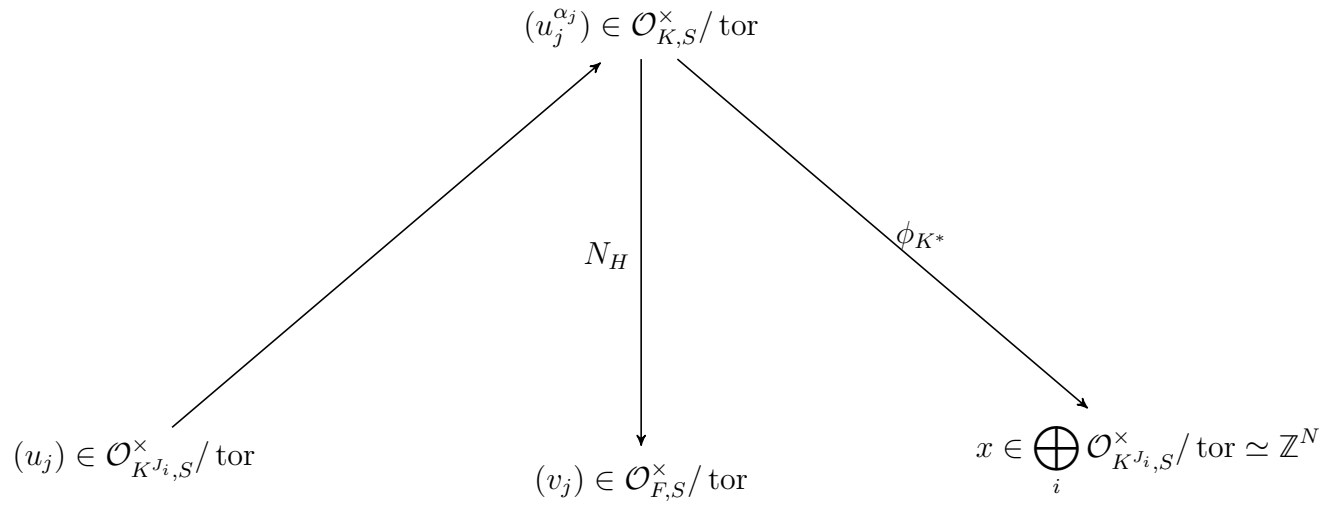
Preuve. On remarque que $\psi_M \circ \phi_M : M^H \to M^H = d|H|Id$.
En effet, soit $m =\in M^H$. Alors $\psi \circ \phi(m) = N_H \sum_{i=1}^{\ell} a_i N_{J_i} b_i m = dN_H^2 m$. Or $N_H^2 = |H| N_H$ et $N_H m = |H| m$ car $m \in M^H$, donc $\psi \circ \phi(m) = d|H|^2 m$. De plus, $|H|^2 d$ est inversible dans $\mathbb{Q}$, d'où la conclusion.

□

Notation Dans la suite, pour tout groupe V, on désignera par V/tor le groupe V quotienté par sa torsion.

Remarque 86 Pour tout i, $\mathcal{O}^{\times}_{K^{J_i},S}/\operatorname{tor}$ est isomorphe à $\mathbb{Z}^n$ avec n un entier naturel correspondant au cardinal d'une base.

On peut donc, à partir d'une base d'un $\mathcal{O}^{\times}_{K^{J_i},S}/\operatorname{tor}$, la projeter à la fois dans $\mathcal{O}^{\times}_{F,S}$ et dans $\mathbb{Z}^N$, avec N la somme des cardinaux des bases de tous les $\mathcal{O}^{\times}_{K^{J_i},S}$. Cette projection se fait via le diagramme suivant :



Algorithme 87
Entrée : une base $(u_{j,i})$ de $\mathcal{O}^\times_{K^{J_i},S}/\operatorname{tor}$ pour $1 \leq i \leq l$.
Sortie : une base de $V = ((\mathcal{O}^\times_{K^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{K^{J_l},S})^{\alpha_l})$

- Pour tout $1 \leq j \leq \ell$, calculer $u_j^{\alpha_j} \in \mathcal{O}^\times_{K,S}/\operatorname{tor}$
- Pour tout $1 \leq i \leq \ell$, calculer $(v_{j,i}) \in \mathcal{O}^\times_{F,S}/\operatorname{tor}$ et $x_i \in \mathbb{Z}^N$ comme dans le diagramme précédent.
- Créer une matrice M de taille (l, N) dont les colonnes sont les (x_i)
- Appliquer un algorithme pour mettre M sous forme normale de Hermite, en retenant les étapes de l'algorithme.
- Appliquer les mêmes transformations à la famille des $(v_{i,j})$, et renvoyer le résultat.

La famille des $(v_{j,i})$ est une famille génératrice de V par construction, et la mise sous forme normale de Hermite en fait une base, donc l'algorithme est correct.

6.2.3 Algorithme

Dans cette cette sous partie, on décrira un algorithme qui calcule le groupe des S-unités de F en s'appuyant sur les résultats des deux sous-parties précédentes.

Algorithme 88
Entrée : F une extension finie de $\mathbb{Q}$, $K/\mathbb{Q}$ l'extension galoisienne de $F/\mathbb{Q}$ et G son groupe de galois, $H < G$ tel que $F = K^H$, $\mathcal{J} = \{J_1, \cdots, J_\ell\}$ un ensemble de sous-groupes de G, d un entier naturel non nul, et $(a_i), (b_i) \in \mathbb{Z}[G]$ tels que $dN_H = \sum_{i=1}^{\ell} a_i N_{J_i} b_i$, S un ensemble G-stable d'idéaux premiers non nuls de l'anneau des entiers de F.
Sortie : Une base du groupe des S-unités de $F^\times$.

- Pour chaque élément J_i de $\mathcal{J}$, calculer une base du groupe des S-unités de K^{J_i}.
- Calculer une base du groupe V, comme dans la sous-partie précédente.
- Renvoyer une base de la d-saturation de V.

Cet algorithme est correct par le corollaire 83.

Conclusion

On a donc bien trouvé une généralisation de la notion de relation de norme, et utilisé ce résultat pour obtenir un algorithme permettant de calculer le groupe des S-unités de $K^\times$ pour $K/\mathbb{Q}$ une extension pas forcément galoisienne. Cependant, il reste encore à implémenter cet algorithme dans un langage plus adapté que Sagemath, par exemple Pari/GP. Il faut aussi réfléchir à optimiser sa complexité en temps et en espace de calcul. De plus, comme signalé plus haut, on peut réfléchir à une reformulation du problème qui permette de se passer du calcul d'une cloture galoisienne.