Université Mohammed Premier
Faculté des Sciences
Département de Mathématiques
Oujda

Master

Théorie des Nombres, Cryptographie et Systèmes de Sécurité

Première Année

Semestre : 2

Titre

Théorie du corps de classes I

Notes préparées par le Professeur
Abdelkader Zekhnini

Année Universitaire : 2019/2020. Version 1

La théorie du corps de classes a une réputation de difficulté qui est en partie justifiée. Mais il faut faire une distinction : il n'est peut-être pas en effet dans la science de théorie où tout à la fois les démonstrations soient aussi ardues, et les résultats d'une aussi parfaite simplicité et d'une aussi grande puissance.

Jacques Herbrand (1908-1931).

L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques K peuvent être déterminées par des éléments tirés de la connaissance de K lui-même ; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement.

Chevalley 1940.

Table des matières

Remerciements

Nous tenons à remercier tous les collègues et amis qui ont contribués à la réalisation de ce cours, surtout le professeur M. C. Ismaili, qui m'a permis d'utiliser le fichier Tex de l'un de ses cours de Master, et mon étudiant M. M. Chems-Eddin.

Références

Nous commençons par donner une liste de livres que nous croyons important pour les débutants souhaitant étudier la théorie algébrique des nombres.
La bibliographie suivante mentionne quelques références classiques que nous croyons pertinents (mais pas complets), ces livres sont importants pour étudier la théorie des corps de classes et les thèmes sur lesquels est basée (pour d'autres livres voir la fin de ces notes).

- Pour les nombres p-adiques voir : F.Q. Gouvea, p-adic Numbers : An Introduction. Springer Verlag, 1993.
- Pour la théorie de corps de classes voir : G. J. Janusz, *Algebraic Number Fields*, Graduate Studies in Mathematics, volume 7, USA, Second Edition (1996). C'est la base de ces notes, il est particulièrement convivial pour une première lecture, voir aussi [9, 10], tandis que le livre de G. Gras, *Class Field Theory.* Springer Verlag, 2003, est une bonne référence pour une lecture plus approfondie,
- Pour la théorie algébrique des nombres [3, 11, 7, 8, 5] sont des bonnes références.

Introduction

0.1 Définition de la théorie du corps de classe

La théorie du corps de classe est la description des extensions abéliennes des corps globaux et des corps locaux. La nomination "corps de classe" fait référence à une extension de corps satisfaisant une propriété technique historiquement liée aux groupes de classes d'idéaux. La théorie du corps de classe est donc une branche majeure de la théorie algébrique des nombres qui a pour but la classification des extensions abéliennes, c'est-à-dire les extensions galoisiennes et de groupe de Galois abélien, d'un corps commutatif donné. Plus précisément, il s'agit de décrire et de construire ces extensions en termes de propriétés arithmétiques du corps de base lui-même.

Cette théorie tire son origine de la preuve de la réciprocité quadratique par Gauss à la fin du 18-ème siècle. Ces idées ont été développées au cours du siècle suivant, donnant lieu à un ensemble de conjectures de Hilbert qui ont ensuite été prouvées par Takagi et Artin, la plupart des résultats centraux ont été démontrés dans la période s'étendant entre 1900 et 1950. Ces conjectures et leurs preuves constituent l'essentiel de la théorie du corps de classe. La théorie a été nommée ainsi en rapport avec les idées, conjectures et résultats de ses débuts, tel que le corps de classe de Hilbert, et s'organisa vers 1930.

De nos jours, le terme "la théorie du corps de classe" est généralement utilisé comme synonyme de l'étude de toutes les extensions abéliennes des corps de nombres algébriques (et plus généralement des corps globaux), mais aussi des corps de nombres p-adiques (et plus généralement des corps locaux).

Une autre ligne importante est la recherche de générateurs explicites pour les corps de classes de corps de nombres algébriques, c'est-à-dire de générateurs donnés par les valeurs de fonctions transcendantes. C'est le "Kronecker Jugendtraum" (rêve de jeunesse de Kronecker). Il n'est encore réalisé que pour de rares cas, notamment celui du corps des rationnels (théorème de Kronecker-Weber, où les générateurs sont des racines de l'unité, c'est-à-dire des valeurs de la fonction exponentielle), et des corps quadratiques imaginaires (cas des corps à multiplication complexe, où les générateurs sont des valeurs de fonctions elliptiques).

Parmi les résultats majeurs, on trouve celui qui indique que, étant donné un corps de nombres k, notons par K l'extension maximale abélienne non ramifiée de k (cette extension est dite **corps de classe de Hilbert de** k), le groupe de Galois de K sur k est canoniquement isomorphe au groupe de classes d'idéaux de k. Cet énoncé peut être généralisé par la loi de

réciprocité d'Artin, écrivant $\mathrm{Cl}(k)$ pour le groupe de classes d'idéaux de k et prenons L une extension abélienne finie de k, cette loi donne un isomorphisme canonique :

$$\theta_{L/k} : \mathrm{Cl}(k)/N_{L/k}(\mathrm{Cl}(L)) \longrightarrow Gal(L/k),$$

où $N_{L/k}$ désigne la norme de L à k. Cette isomorphisme est appelé après **l'application de réciprocité**. Le théorème d'existence indique que l'application de réciprocité peut être utilisée pour effectuer une bijection entre l'ensemble des extensions abéliennes de k et l'ensemble des sous-groupes fermés d'indices finis de $\mathrm{Cl}(k)$.

Une méthode standard pour développer la théorie du corps de classe globale, depuis les années 1930, consiste à développer la théorie du corps de classe locale, qui décrit les extensions abéliennes des corps locaux, puis à l'utiliser pour construire la théorie du corps de classe globale. Cela a été fait pour la première fois par Artin et Tate en utilisant la théorie de la cohomologie des groupes, et en particulier en développant la notion de formation de classes. Plus tard, Neukirch a trouvé une preuve des principales affirmations de la théorie des corps de classes globaux sans utiliser les idées cohomologiques.

Le programme de Langlands (c'est un domaine de recherche actif et fertile en conjectures de grande portée et influentes. Ce programme souhaite relier la théorie des nombres aux représentations de certains groupes (la géométrie), il a été proposé par Robert Langlands (1967, 1970)) propose une approche pour généraliser la théorie des corps de classes aux extensions non abéliennes. Cette généralisation est encore principalement conjecturale. Pour les corps de nombres, la théorie des corps et les résultats liés au théorème de la modularité sont les seuls cas connus.

Terminons cette section par dire que l'un des principaux théorèmes de la théorie du corps de classe affirme que les "corps de classes" ne sont que "les extensions abéliennes". Quand à Hilbert, il définit "le corps de classe" comme suit :

Une extension finie K d'un corps de nombres k est dite **corps de classe** de k si exactement les idéaux premiers principaux de l'anneau des entiers $\mathcal{O}_k$ de k se décomposent complètement dans K/k. Ce corps K porte actuellement son nom, et on l'appelle **le corps de classe de Hilbert** de k, et il est défini comme étant **l'extension maximale abélienne non ramifiée de** k.

0.2 Survol historique

La notion du **corps de classe** est généralement attribuée à Hilbert. Mais en réalité, Kronecker pensa avant à cette notion, et le terme est du à Weber, avant même l'apparition du papier fondamental de Hilbert. Kronecker, dans son article "Grundzüge einer arithmetischen theorie der algebraischen grössen" (1882), discuta ce qu'on appelle, dans la terminologie moderne, l'extension algébrique K d'un corps de nombres donné k telle que tous les idéaux de k devient principaux dans K. Par cette notion, Kronecker anticipa le théorème de l'idéal principal de la théorie du corps de classe, énoncé et dans des cas spéciaux prouvé par Hilbert.

Weber n'a cependant pas défini la notion du corps de classe sur cette base, une base qui, aujourd'hui, ne convient pas pour construire la théorie. Ce qu'il a postulé fait partie de la loi

de décomposition. Alors que Hilbert, dans sa définition, ne considérait que le cas des classes d'idéaux absolus. Hilbert a en fait donné deux définitions différentes d'un corps de classe. Après la preuve que les extensions cycliques non ramifiées K/k de degré premier ℓ ne peuvent exister que si le nombre de classe $h(k)$ est divisible par ℓ (Satz 94 dans le Zahlbericht de Hilbert), il dit simplement qu'il appellera de tels corps des corps de classe. Dans son travail sur la loi de réciprocité quadratique, il a proposé une définition plus précise :

Une extension finie K d'un corps de nombres k est dite un **corps de classe** de k si exactement **les idéaux principaux premiers de $\mathcal{O}_k$ se décomposent complètement** dans K/k.

Quand à Weber, il a donné sa définition en généralité, à savoir :

Soient k un corps de nombres et C/P_k un groupe de congruence de k. Une extension algébrique K/k est appelée **corps de class** associée à C/P_k, si exactement les idéaux premiers de k de degré d'inertie égal à 1 qui sont principaux (appartiennent à la classe principale P_k) se décomposent complètement dans K.

La théorie du corps de classe introduite par Weber, Kronecker, Hilbert et Furtwängler a été généralisée par Takagi en permettant aux extensions abéliennes d'être ramifiées. De plus, il a défini le corps de classe différemment :

K/k est appelé corps de classe associé au groupe de congruence C/P_k, si et seulement si l'égalité $[C : \mathrm{P}_k] = [K : k]$ est vraie.

Les principaux théorèmes de la théorie des corps de classe prouvés par Takagi, et basés sur cette définition, peuvent être résumés comme suit :

La relation du corps de classe établit une correspondance bijective entre tous les corps relativement abéliens K/k et tous les groupes de congruence C/P_k de k.

Donc pour Takagi un corps de class de k est une extension abélienne de k.

Trois thèmes de la théorie des nombres à la fin du XIXe siècle ont été à la base de la théorie du corps de classe : les relations entre les extensions abéliennes et les groupes de classes d'idéaux, les théorèmes de densité pour les nombres premiers (et les fonctions L) et les lois de réciprocité. La théorie du corps de classe s'est développée à partir de ces idées initiales à travers les travaux de Kronecker, Weber, Hilbert, Takagi, Artin, Hasse et Chevalley. Pour un historique détaillé sur le développement de la théorie du corps de classe, vous pouvez consulter [13], [14, 15, 16] et le début de la partie 2 de [17].

Dans la suite, une chronologie de la théorie du corps de classes (voir le site Wikipédia).

- 1801 Carl Friedrich Gauss démontre la loi de réciprocité quadratique.
- 1829 Niels Henrik Abel utilise des valeurs spéciales de la fonction lemniscate pour construire des extensions abéliennes de $\mathbb{Q}(i)$, une fonction lemniscate est une fonction ayant une courbe plane de la forme d'un 8.

- 1837 Théorème de Dirichlet sur les progressions arithmétiques.
- 1853 Leopold Kronecker announce le théorème de Kronecker–Weber.
- 1880 Kronecker présente son Jugendtraum (rêve de jeune) sur les extensions abéliennes des corps quadratiques imaginaires.
- 1886 Heinrich Martin Weber démontre le théorème de Kronecker–Weber (avec une petite faute).
- 1896 David Hilbert donne la première preuve complète du théorème de Kronecker-Weber.
- 1897 Weber introduit les groupes de classes de rayons et généralise les groupes de classes d'idéaux.
- 1897 Hilbert publie son Zahlbericht (rapport sur la théorie des nombres).
- 1897 Hilbert réécrit la loi de la réciprocité quadratique comme formule de produit pour le symbole Hilbert.
- 1897 Kurt Hensel introduit les nombres p-adiques.
- 1898 Hilbert conjecture l'existence et les propriétés du corps de classe de Hilbert au sens étroit, en les prouvant dans le cas particulier où le nombre de classes est 2.
- 1907 Philipp Furtwängler démontre l'existence et les propriétés de base du corps de classe de Hilbert.
- 1908 Weber définit le corps de classe d'un groupe de classe d'idéaux général.
- 1920 Teiji Takagi montre que les extensions abéliennes d'un corps de nombres sont exactement les corps de classes des groupes des classes d'idéaux.
- 1922 Le papier de Takagi sur les lois de réciprocité.
- 1923 Helmut Hasse a introduit le principe de Hasse (pour le cas particulier des formes quadratiques).
- 1923 Emil Artin conjecture sa loi de réciprocité.
- 1924 Artin introduit les fonctions L.
- 1926 Nikolai Chebotaryov prouve son théorème de densité.
- 1927 Artin prouve sa loi de réciprocité donnant un isomorphisme canonique entre les groupes de Galois et les groupes de classes d'idéaux.
- 1930 Furtwängler et Artin prouvent le théorème de l'idéal principale.
- 1930 Hasse introduit la théorie du corps de classe locale.
- 1931 Hasse prouve le théorème de la norme de Hasse.
- 1931 Hasse classifie les algèbres simples sur les corps locaux.
- 1931 Jacques Herbrand introduit le quotient d'Herbrand.
- 1931 Le théorème d'Albert–Brauer–Hasse–Noether montre le principe de Hasse pour les algèbres simples sur les corps globaux.
- 1933 Hasse classifie les algèbres simples sur les corps de nombres.
- 1934 Max Deuring et Emmy Noether développent la théorie du corps de classe en utilisant les algèbres.

- 1936 Claude Chevalley introduit les idèles.
- 1940 Chevalley utilise les idèles pour donner une preuve algébrique de la seconde inégalité pour les extensions abéliennes.
- 1948 Shianghao Wang prouve le théorème de Grunwald-Wang, corrigeant une erreur de Grunwald.
- 1950 La thèse de Tate utilise l'analyse dans les anneaux d'adèles pour étudier les fonctions zêta.
- 1951 André Weil introduit le groupe de Weil.
- 1952 Artin et Tate introduisent les formations de classes dans leurs notes sur la théorie du corps de classes.
- 1952 Gerhard Hochschild et Tadashi Nakayama introduisent la cohomologie de groupes dans la théorie du corps de classe.
- 1952 John Tate introduit le groupe de cohomologie de Tate.
- 1964 Evgeny Golod et Igor Shafarevich prouvent que la tour des corps de classes peut être infinie.
- 1965 Jonathan Lubin et Tate utilisent les lois de groupe formelle de Lubin-Tate pour construire des extensions abéliennes ramifiées des corps locaux.

0.3 Les résultats essentiels traités dans ce cours

Dans ces notes, nous allons étudier les notions ci-citées. Soient K un corps de nombres, $\mathbf{I}_K$ le groupe des idéaux fractionnaires de K et $\mathfrak{m}$ un module de K. Dans cette partie nous établirons les résultats suivants.

1. La cohomologie des groupes cycliques et le quotient d'Herbrand.
2. Des résultats pour préparer la seconde égalité.
3. Calcul d'un indice de norme.
4. L'égalité fondamentale pour les extensions cycliques L/K, c-à-d le nombre de classes $h_{\mathfrak{m}}(L/K) = \mathrm{Gal}(L/K)$.
5. Le théorème de la norme de Hasse ou le principe du local-globale : dans une extension cyclique L/K un élément de K est norme d'un élément de L si et seulement s'il est localement norme en tout premier (fini ou infini) de K. Résultat non vrai pour une extension abélienne en général.
6. La loi de réciprocité pour une extension cyclique L/K moyennant le résultat 1, c'est-à-dire l'application d'Artin réalise un isomorphisme entre les groupes $\mathbf{I}_K^{\mathfrak{m}}/N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$ et $\mathrm{Gal}(L/K)$.
7. La loi e réciprocité d'Artin : généralisation du résultat 6 au cas d'une extension abélienne moyennant le théorème de structure des groupes abéliens finis.
8. Généralisation du résultat 1 au cas d'une extension abélienne.
9. Le théorème de Kronecker-Weber : toute extension abélienne de $\mathbb{Q}$ est incluse dans une extension cyclotomique $\mathbb{Q}(e^{\frac{2i\pi}{n}})$, où $n \in \mathbb{N}$.

Chapitre 1

Rappels

1.1 Action d'un groupe sur un ensemble

La plupart des théories mathématiques étudient des objets constitués d'un ensemble E muni d'une structure : espace métrique, espace topologique, groupe, espace vectoriel,.... En général, l'ensemble G des applications bijectives de E sur lui-même, respectant cette structure, est alors stable par composition et l'application réciproque f^{-1} de tout $f \in G$ est élément de G. La composition des applications étant associative, G est un groupe d'élément neutre id_E. Plus exactement, G est un sous-groupe du groupe S_E des bijections de E sur E. Par exemple, les situations suivantes entrent dans ce schéma.

a. E est un espace métrique et G est l'ensemble des bijections de E sur E qui conservent la distance (G est le groupe des isométries de E sur E),

b. E est un espace topologique et G est l'ensemble des bijections de E sur E qui sont continues ainsi que leur réciproque (groupe des homéomorphismes de E sur E),

c. E est un groupe et G est l'ensemble des bijections f de E sur E qui préservent la structure de groupe, c'est-à-dire telles que $f(xy) = f(x)f(y)$ pour tous x, $y \in E$ (groupe $\mathrm{Aut}(E)$ des automorphismes du groupe E),

d. E est un espace vectoriel et G est l'ensemble des applications linéaires bijectives de E sur E (groupe $\mathrm{GL}(E)$ des automorphismes de l'espace vectoriel E),

e. E est un espace vectoriel euclidien et G est l'ensemble des applications linéaires isométriques de E sur E (groupe orthogonal $O(E)$ de E),

f. E est un espace vectoriel hermitien et G est l'ensemble des applications linéaires isométriques de E sur E (groupe unitaire $U(E)$ de E).

Les exemples d., e. et f. ci-dessus, sont particulièrement importants. En effet, on dispose sur E de tous les outils de l'algèbre linéaire pour étudier les éléments du groupe G : représentation matricielle de ses éléments, diagonalisation ou réduction des endomorphismes, etc.... Dans le passé, pour étudier un groupe donné, les mathématiciens ont pris l'habitude de le plonger dans l'un des trois derniers exemples cités. Cela s'appelle faire une représentation du groupe G. Ainsi, un groupe G opérant sur un ensemble E est le cadre naturel de nombreux groupes

classiques. C'est aussi un outil fondamental des mathématiques contemporaines. Précisons ce que l'on entend par ça.

Dans toute cette section, nous considérons G un groupe multiplicatif d'élément neutre 1 et E un ensemble non vide. L'ensemble des bijections de E sur E sera noté S_E et on l'appellera groupe des permutations ou groupe symétrique de E.

1.1.1 Définitions

Définition 1.1.1. Soient G un groupe, dont la loi est notée multiplicativement, d'élément neutre 1 et un ensemble E. On dit G opère sur l'ensemble E s'il existe une application

$$\begin{array}{rccc} \varphi: & G\times E & \longrightarrow & E \\ & (g,x) & \longmapsto & \varphi(g,x)=g\cdot x \end{array}$$

telle que $\forall g,h\in G,\ \forall x\in E,\ \begin{cases} g\cdot(h\cdot x) &= (gh)\cdot x \\ 1\cdot x &= x. \end{cases}$

On appelle G-ensemble tout ensemble muni d'une action de G.

Remarque 1.1.1. Une façon équivalente, plus abstraite, mais plus féconde, de définir une action du groupe G sur l'ensemble E se fait en donnant un morphisme de groupes, dit associé à l'action,

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & S_E \\ & g & \longmapsto & \varphi_g \end{array}$$

du groupe G dans le groupe symétrique S_E de l'ensemble E. Un tel morphisme est appelé une représentation du groupe G.

En effet, supposons que G opère sur E. Pour $g\in G$, l'application

$$\begin{array}{rccc} \varphi(g)=\varphi_g: & E & \longrightarrow & E \\ & x & \longmapsto & \varphi_g(x)=g.x \end{array}$$

est une bijection de E sur E, c'est-à-dire $\varphi_g\in S_E$. Car de $1.x=x$ pour tout $x\in E$, on déduit que $\varphi_1=id_E$ et avec $g.(g^{-1}.x)=(gg^{-1}).x=1.x=x$ et $g^{-1}(g.x)=x$, on déduit que $\varphi_g\circ\varphi_{g^{-1}}=\varphi_{g^{-1}}\circ\varphi_g=id_E$, ce qui signifie que $\varphi(g)=\varphi_g$ est bijective d'inverse $\varphi(g^{-1})=\varphi_{g^{-1}}$.

De plus avec $g.(g'.x)=(gg').x$, pour tous g, g', x, on déduit que

$$\varphi(gg')=\varphi_{gg'}=\varphi_g\circ\varphi_{g'}=\varphi(g)\circ\varphi(g'),$$

c'est-à-dire que l'application φ est un morphisme de groupes de G dans S_E. Le noyau de ce morphisme est le noyau de l'action de G sur E.

Réciproquement, un tel morphisme φ définit une action de G sur E de la manière suivante : $g\cdot x=(\varphi(g))(x)=\varphi_g(x)$ pour tous $g\in G,\ x\in E$.

Dans le cas où l'ensemble E est muni d'une structure supplémentaire (algébrique, topologique, géométrique, ...), on ne considère que les morphismes φ tels que $\varphi(g)$ préserve cette structure pour tout $g\in G$. Par exemple, si E est un espace vectoriel, on exige que φ soit à valeurs dans $GL(E)$.

Exemples 1.1.1.

1. On peut faire opérer un groupe G sur lui-même de plusieurs façons :
   i. par l'application dite : translation à gauche, $(g,h) \in G \times G \longmapsto g \cdot h = gh$.
   ii. par l'application dite : translation à droite, $(g,h) \in G \times G \longmapsto g \cdot h = hg^{-1}$.
   iii. par automorphismes intérieurs (on dit aussi G opère sur lui-même par conjugaison),
   $$(g,h) \in G \times G \longmapsto g \cdot h = ghg^{-1} \in G.$$
2. Un groupe G agit sur tout sous-groupe distingué H par conjugaisons :
   $$(g,h) \in G \times H \longmapsto g \cdot h = ghg^{-1} \in H.$$
3. Le groupe symétrique de E opère naturellement sur E par :
   $$\mathrm{S}_E \times E \longrightarrow E,\ (\sigma, x) \longmapsto \sigma \cdot x = \sigma(x).$$

1.1.2 Orbites, stabilisateurs et points fixes

Définition 1.1.2. Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble de E défini par : $O_x = \{g \cdot x, \quad g \in G\} = G \cdot x$ est appelé orbite de x sous l'action de G.

Remarque 1.1.2. On vérifie facilement que la relation définie sur E par :

$$xRy \text{ si, et seulement si, il existe } g \in G \text{ tel que } y = g \cdot x$$

est une relation d'équivalence sur E, car

- $x = 1 \cdot x$ donne la réflexivité,
- $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie, et
- $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité.

La relation R s'appelle la relation de conjugaison : les éléments x et y de E sont conjugués, s'il existe $g \in G$ tel que $g.x = y$. De plus la classe de $x \in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E :

$$E = \coprod_{x \in E} O_x.$$

Exemple 1.1.1.

- Pour l'action de $G = S_E$ sur E, il y a une seule orbite. En effet, pour tout $x \in E$ on a
$$O_x = \{\sigma.x = \sigma(x) \mid \sigma \in G\},$$
car pour tout $y \in E$, il existe $\sigma \in G$ tel que $y = \sigma(x)$, où σ est la transposition (xy) si $x \neq y$ et $\sigma = id_E$ si $x = y$.
- Pour l'action de G sur lui même par conjugaisons, les orbites sont appelée classes de conjugaison :
$$\forall h \in G,\ O_h = \{g.h = ghg^{-1} \mid g \in G\}.$$

G est abélien ssi $O_h = \{h\}$ pour tout $h \in G$.

Définition 1.1.3. Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble de G défini par : $G_x = \{g \in G \mid g \cdot x = x\}$ est appelé le stabilisateur de x sous l'action de G.

Lemme 1.1.1. *Pour tout $x \in E$, G_x est un sous-groupe de G, en général non normal.*

Preuve. Simple à vérifier. □

Remarque 1.1.3. Considérons un ensemble E non réduit à un point et l'action de $G = S_E$, $\sigma.x = \sigma(x)$. À chaque $\sigma \in G_x$, on associe la restriction σ' à $E - \{x\}$, ce qui définit un isomorphisme de G_x sur $S_{E-\{x\}}$.

Définition 1.1.4. Soit un élément g du groupe G. L'ensemble Fix_g des éléments de E invariants sous l'action de g est dit l'ensemble des points fixés par g :

$$\mathrm{Fix}_g = \{x \in E \mid g \cdot x = x\}.$$

1.1.3 Caractéristiques des actions de groupe

Définition 1.1.5. On dit que G agis trivialement sur E si pour tout $g \in G$ et tout $x \in E$, $g.x = x$.

Définition 1.1.6 (Action transitive)**.**
Une action est dite transitive si elle possède une et une seule orbite. Une action d'un groupe G sur un ensemble E est donc transitive si et seulement si E n'est pas vide et que deux éléments quelconques de E peuvent être envoyés l'un sur l'autre par l'action d'un élément du groupe :

$$\forall x, y \in E, \quad \exists g \in G \quad y = g \cdot x.$$

Définition 1.1.7 (Action libre)**.**
Une action est dite libre si tous les stabilisateurs sont réduits au neutre, autrement dit si tout élément différent du neutre agit sans point fixe :

$$\forall x \in E, \quad \mathrm{G}_x = \{1\}.$$

Définition 1.1.8 (Action fidèle)**.**
Une action est dite fidèle (on dit parfois aussi effective) si l'intersection de tous les stabilisateurs est réduite au neutre, autrement dit si seul le neutre fixe tous les points. Une action libre est fidèle. De façon équivalente, une action est fidèle si le morphisme

$$\begin{array}{rcccl} \varphi & : & G & \to & \mathrm{S}_E \\ & & g & \mapsto & \varphi_g : E \to E;\ x \mapsto \varphi_g(x) \end{array}$$

est injectif.

Définition 1.1.9 (Action simplement transitive)**.**
Une action est dite simplement transitive si elle est à la fois transitive et libre. Autrement dit,

deux éléments quelconques de l'ensemble E sont envoyés l'un sur l'autre par un et un seul élément du groupe :

$$\forall x, y \in E, \quad \exists! g \in G \quad y = g \cdot x.$$

Par exemple, l'action d'un groupe sur lui-même par translations à gauche (ou à droite) est simplement transitive.

Une action transitive d'un groupe fini G sur un ensemble E est simplement transitive si et seulement si G et E ont même cardinal.

1.1.4 Équation des classes

Proposition 1.1.1. *Soit G un groupe agissant sur un ensemble E. Soit x un élément de E. Alors, il existe une bijection entre l'orbite $O_x = G \cdot x$ de x et $(G/G_x)_g$, l'ensemble des classes à gauche de G modulo G_x (le stabilisateur de x). Donc* $\mathrm{card}(O_x) = [G : G_x]$.

Preuve. Soit application $\varphi : \begin{array}{ll} (G/G_x)_g & \longrightarrow O_x \\ \overline{g} = gG_x & \longmapsto g \cdot x \end{array}$ montrons que φ est une bijection.

D'abord, vérifions que φ est bien définie. Soit donc $g' \in G$ tel que $g'G_x = gG_x$, alors $g'^{-1}g \in G_x$. On en déduit donc $g'^{-1}g \cdot x = x$, d'où $g \cdot x = g' \cdot x$. Par suite l'application φ est bien définie.

Il est simple de voir que φ est surjective. Soit g, g' dans G tels que $\varphi(\overline{g}) = \varphi(\overline{g'})$, alors $g \cdot x = g' \cdot x$, alors $(g'^{-1}g) \cdot x = x$, et donc $(g'^{-1}g) \in G_x$. Ceci implique $gG_x = g'G_x$, donc φ est injective. Elle est par suite une bijection, ce qui prouve la proposition. □

Désignons par X un système de représentants des orbites c'est-à-dire

$$E = \coprod_{x \in X} O_x = \coprod_{x \in X} G \cdot x, \text{ (réunion disjointe)}$$

autrement dit X est un ensemble constitué d'un représentant de chaque orbite, alors on a le résultat suivant.

Théorème 1.1.1 (**Equation des classes**). *Soit G un groupe agissant sur un ensemble fini E. Alors, on a :*

$$\mathrm{card}(E) = \sum_{x \in X} [G : G_x].$$

Preuve. Soit $x \in X$. On utilise la proposition précédente, on a $\mathrm{card}(O_x) = [G : G_x]$. D'autre part, on sait $E = \coprod_{x \in X} O_x$, donc $\mathrm{card}(E) = \sum_{x \in X} \mathrm{card}(O_x)$, par suite $\mathrm{card}(E) = \sum_{x \in X} [G : G_x]$. □

Soit G un groupe fini ; on fait opérer G sur lui même par conjugaison. Donc pour un $x \in G$, on a le stabilisateur de x (dans ce cas, on dit aussi le centralisateur de x) est :

$$G_x = \{g \in G \mid g.x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\},$$

et l'orbite de x est :

$$O_x = G \cdot x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}.$$

Lemme 1.1.2. *Pour tout $x \in G$, on a $O_x = \{x\}$ si et seulement si $x \in Z(G)$, donc*

$$\text{card}(O_x) = 1 \text{ si et seulement si } x \in Z(G), \text{ c'est-à-dire, } [G : G_x] = 1 \Longleftrightarrow x \in Z(G).$$

Preuve. Remarquons d'abord que pour tout $x \in G$, $x \in O_x$, donc $\text{card}(O_x) = 1$ si et seulement si pour tout $g \in G$, on a $gxg^{-1} = x$ c'est-à-dire si et seulement si $x \in Z(G)$. □

Corollaire 1.1.1. *Soient G un groupe fini et $Z(G)$ son centre. On considère l'action de G sur lui même par conjugaison. Soit X l'ensemble constitué d'un représentant de chaque orbite. Alors, pour les x qui sont dans X, l'équation des classes devient :*

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : G_x].$$

Preuve. Comme pour tout $x \in Z(G)$, $O_x = \{x\}$ (lemme 5.2.1), alors pour les x qui sont dans X on a :

$$G = \bigcup_{x \in X} O_x = (\bigcup_{x \in Z(G)} O_x) \cup (\bigcup_{x \notin Z(G)} O_x) = Z(G) \cup (\bigcup_{x \notin Z(G)} O_x).$$

Par le théorème 1.1.1 on obtient

$$|G| = \sum_{x \in Z(G)} [G : G_x] + \sum_{x \in X \text{ et } x \notin Z(G)} [G : G_x] = |Z(G)| + \sum_{x \notin Z(G)} [G : G_x].$$

□

1.2 Notion de G-module

Cette section fait partie de la précédente, mais vu son importance nous la traitons séparément.

Définition 1.2.1. Soit G un groupe, dont la loi est notée multiplicativement, d'élément neutre 1. Un G-module est un groupe abélien A, dont la loi est notée additivement, sur lequel G agit de manière compatible avec la structure du groupe abélien sur A, c'est-à-dire A est menu d'une action

$$\varphi : G \times A \longrightarrow A \,;\, (g, a) \longmapsto g.a$$

telle que pour tout $g \in G$, l'application $\varphi_g : a \longmapsto g.a$ est un homomorphisme de groupes abéliens. On a donc les règles de calcul suivantes : pour tous $g, g' \in G$ et tous $a, a' \in A$

1. $g.(a + a') = g.a + g.a'$,
2. $g.(g'.a) = (gg').a$,

3. $1.a = a$.

Remarques 1.2.1.

1. Notons que φ_g est un automorphisme de A, de réciproque $\varphi_{g^{-1}}$. Si A est un groupe abélien, se donner une structure de G-module sur A revient à se donner un homomorphisme de groupes de G dans $(\mathrm{Aut}(A), \circ)$, où $\mathrm{Aut}(A)$ est l'ensemble des automorphismes du groupe abélien A.
2. Soient un groupe G et un anneau R, on définit **l'algèbre du groupe** G (Group Ring) et on note $R[G]$ comme étant l'ensemble des sommes formelles presque nulles (combinaisons linéaires)
$$\alpha = \sum_{g \in G} \alpha_g g,$$
où $\alpha_g \in R$ avec un nombre fini des α_g sont non nuls.
$R[G]$ est un groupe abélien libre admettant comme base les éléments de G menu d'une addition définie par :
$$\alpha + \beta = \left(\sum_{g \in G} \alpha_g g \right) + \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} (\alpha_g + \beta_g) g.$$
On définit aussi sur $R[G]$ une multiplication fourni par celle de G (le produit de convolution) par :
$$\alpha\beta = \left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{g' \in G} \beta_g g' \right) = \sum_{(g,g') \in G \times G} \alpha_g \beta_{g'} g g'.$$
On a les notes suivantes :
   a. On peut aussi définir le produit $\alpha\beta$ comme suit
$$\alpha\beta = \sum_{u \in G} C_u u, \quad \text{où } C_u = \sum_{(gg'=u} \alpha_g \beta_{g'}.$$
   b. $R[G]$ avec la somme et la multiplication définies en haut est un anneau, non commutatif si G n'est pas commutatif.
   c. Pour $\alpha = \sum_{g \in G} \alpha_g g$ dans $R[G]$ et $\lambda \in R$, on définit $\lambda\alpha = \sum_{g \in G} (\lambda \alpha_g) g$.
3. Se donner un G-module est équivaut à se donner un module sur l'anneau $R = \mathbb{Z}[G]$. En effet, si A est un module sur l'anneau R, on définit une structure de G-module sur A par $g.a = ga$ pour tout $(g, a) \in G \times A$; réciproquement si A est un G-module, on le munit d'une structure de module sur R en posant $(\sum_{g \in G} n_g g)x = \sum_{g \in G} n_g (g.x)$.

Définition 1.2.2. Un morphisme de G-modules (ou G-morphisme ou même application G-linéaire) $f : A \longrightarrow B$ est un morphisme de groupes abéliens qui commute aux opérations de G, i.e.
$$\text{pour tous } x, y \in A \text{ et tout } g \in G, \begin{cases} f(x+y) = f(x) + f(y) \\ f(g.x) = g.f(x). \end{cases}$$

Cela revient à dire que f est un morphisme de R-modules.

On définit de manière évidente les notions d'isomorphisme de G-modules, de sous G-module, etc.

Si A et B sont des G-modules, on note par $Hom_G(A,B)$ l'ensemble des G-morphismes de A dans B, c'est un groupe abélien pour l'addition, qui est aussi un sous-groupe du groupe $Hom_{\mathbb{Z}}(A,B)$ des morphismes de groupes abéliens de A dans B (non nécessairement compatible avec l'action de G).

Notons que $Hom_G(A,B)$ devient lui aussi un G-module avec les structures : pour tous φ, φ' de $Hom_G(A,B)$ et pour tous $a \in A$ et $g \in G$, on a

$$(\varphi+\varphi')(a) = \varphi(a)+\varphi'(a)$$
$$(g\varphi)(a) = g(\varphi(g^{-1}a)).$$

Définition 1.2.3. Soit G un groupe.

1. Un sous-module d'un G-module A est un sous-groupe B de A stable sous l'action de G, c'est-à-dire $g.b \in B$ pour tout $g \in G$ et $b \in B$.
2. Étant donné un sous-module B d'un G-module A, le module quotient A/B est le groupe quotient menu de l'action $g.(a+B) = g.a + B$.

Exemples 1.2.1.

1. Si on pose $G = \{\pm 1\}$ et $A = \mathbb{Z}$. Alors l'opération de G sur A définie par $g.x = gx$ fait de A un G-module.
2. Pour tout groupe abélien A, l'action triviale de G sur A fait de A un G-module.
3. Le groupe abélien $\mathbb{Z}[G]$ est muni d'une structure canonique de G-module via l'action à gauche de G sur lui-même par translation.
4. Soit A l'ensemble des formes quadratiques binaires $f(x,y) = ax^2 + 2bxy + cy^2$ avec a, b, c des entiers (une forme quadratique binaire est une forme quadratique, i.e un polynôme homogène de degré 2 en deux variables : $q(x,y) = \alpha x^2 + \beta xy + \gamma y^2$).
   Soit aussi $G = \mathrm{SL}_2(\mathbb{Z}) = \{M \in \mathcal{M}_2(\mathbb{Z}) |\ \det(M) = 1\}$ le groupe spécial linéaire (qui est un sous-groupe distingué du groupe linéaire $\mathrm{GL}_2(\mathbb{Z})$ de degré 2, puisqu' il est noyau de l'homomorphisme de groupes $f : \mathrm{GL}_2(\mathbb{Z}) \longrightarrow \mathbb{Z}^*,\ M \longmapsto \det(M)$). On définit une action de G sur A par :
   $$(M \cdot f)(x,y) = f((x,y)M^t) = f((x,y)\cdot \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}) = f(\alpha x + \beta y, \gamma x + \delta y),$$
   où $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ et $(x,y).M$ est une multiplication des matrices. Alors A est un G-module. En effet, on a :
   $$M.(N.(f(x,y)) = M.f((x,y)N^t) = f((x,y)N^tM^t) = f((x,y)(MN)^t) = (MN).f(x,y).$$
5. Soit L une extension finie galoisienne de groupe de Galois G d'un corps K. Alors les ensembles suivants sont des G-modules sous l'action de $G = \mathrm{Gal}(L/K)$:

$$L, \quad L^*, \quad I_L \quad \text{et} \quad Cl(L), \qquad \text{où } L^*, \quad I_L \quad \text{et} \quad Cl(L)$$

sont respectivement le groupe multiplicatif de L, le groupe des idéaux fractionnaires de L et le groupe de classes de L.

Définition 1.2.4. Soit H un sous-groupe d'un groupe G. Soit A un H-module. On définit un groupe abélien $I_G^H(A)$ comme étant l'ensemble des applications

$$f : G \longrightarrow A \text{ vérifiant}$$
$$f(hg) = h \cdot f(g) \text{ pour tous } g \in G,\ h \in H.$$

Ce groupe abélien est alors muni d'une structure de G-module via les formules :

$$(f + f')(g) = f(g) + f'(g) \text{ pour tout } g \in G,$$
$$(g.f)(g') = f(g'g) \text{ pour tous } g, g' \in G.$$

On dit que $I_G^H(A)$ est l'induit de H à G du H-module A.

En particulier si H est le sous-groupe trivial et A est un groupe abélien, on note simplement $I_G(A)$ l'induit correspondant, qu'on appelle G-module induit du groupe abélien A.

Définition 1.2.5. On dit qu'un G-module A est induit s'il existe un groupe abélien B tel que A soit isomorphe à $I_G(B)$.

Remarque 1.2.1. Si A est déjà muni d'une structure de G-module, alors $I_G(A)$ est isomorphe au G-module $\mathcal{F}(G, A)$ défini comme l'ensemble des applications de G dans A avec l'action $(g.f)(x) = g.f(g^{-1}.x)$; un isomorphisme est en effet donné par :

$$\begin{array}{rccl} \varphi & : & I_G(A) & \longrightarrow & \mathcal{F}(G, A) \\ & & f & \longmapsto & \varphi_f : G \longrightarrow A;\ g \longmapsto \varphi_f(g) = g.f(g^{-1}). \end{array}$$

1.3 Suites exactes

Définition 1.3.1. Une suite (finie ou infinie) de G-modules et de G-morphismes

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \cdots$$

est dite exacte si pour tout entier naturel n on a $\mathrm{Im}(f_n) = \ker(f_{n+1})$. Notons que $A_0, A_1, \ldots$ sont des G-modules et $f_0, f_1, \ldots$ des G-morphismes avec $f_n : A_n \to A_{n+1}$.

Remarques 1.3.1. Comme des cas simples, si 0 est le G-module trivial, alors

1. La suite $0 \to A_1 \xrightarrow{f} A_2$ est exacte si et seulement si f est injective.
2. La suite $A_2 \xrightarrow{g} A_3 \to 0$ est exacte si et seulement si g est surjective.
3. La suite $0 \to A_1 \xrightarrow{f} A_2 \to 0$ est exacte si et seulement si f est bijective.

Remarque 1.3.1.

1. La définition précédente définie les suites exactes infinies à droite, on peut de même définir les suites exactes infinies à gauche (qu'on peut indexées par $-\mathbb{N}$), ou infinies des deux côtés (indexées par $\mathbb{Z}$).
2. On peut aussi définir des suites exactes pour d'autres structures et morphismes de ces structures, par exemple des suites exactes de groupes, d'anneaux, d'algèbres, ect.

Exemple 1.3.1. Soient K un corps de nombres et $\mathcal{O}_K$ son anneau des entiers algébriques. Désignons par $\mathbf{I}_K$ Le groupe des idéaux fractionnaires de K. Soit le morphisme

$$i : K^* \longrightarrow \mathbf{I}_K;\ \alpha \longmapsto i(\alpha) = (\alpha) = \alpha\mathcal{O}_K,$$

où K^* est le groupe multiplicative de K, l'image de i est l'ensemble des idéaux fractionnaires principaux de K parfois noté $\mathbf{P}_K$. Le noyau de i est U_K, le groupe des unités de l'anneau $\mathcal{O}_K$, et son conoyau est le groupe de classes de K, noté C_K ou $\mathrm{Cl}(K)$. Alors la suite suivante est une suite exacte :

$$0 \to U_K \xrightarrow{i_c} K^* \xrightarrow{i} \mathbf{I}_K \xrightarrow{p_c} \mathrm{Cl}(K) \to 0,$$

i_c et p_c sont l'injection et la projection canoniques respectivement.

Parmi les suites exactes importantes est celle dite **suite exacte courte** :

Définition 1.3.2. Soient A, B et C des G-modules et f et g des G-morphismes. On appelle suite exacte courte toute suite exacte de la forme

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

Exemple 1.3.2. Soit i l'injection canonique de $n\mathbb{Z}$ dans $\mathbb{Z}$, $n \in \mathbb{N}$, et p la projection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, alors la suite suivante est une suite exacte courte :

$$0 \to n\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{p} \mathbb{Z}/n\mathbb{Z} \to 0.$$

Définition 1.3.3. Soit S la suite exacte courte $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$. Alors S est dite :

1. scindée à gauche s'il existe une rétraction de f, c'est-à-dire il existe un G-morphisme $f' : B \to A$ tel que $f'f = id_A$;
2. scindée à droite s'il existe une section de g, c'est-à-dire il existe un G- morphisme $g' : C \to B$ tel que $gg' = id_C$;
3. scindée en biproduit (à la fois somme et produit) s'il existe une réalisation par B du biproduit $A \oplus C$ pour laquelle f s'identifie à l'injection naturelle de A dans $A \oplus C$ et g à la projection naturelle de $A \oplus C$ dans C.

Dans le cas d'une catégorie abélienne, l'existence de ces trois scindages est équivalente et la suite exacte courte est alors dite scindée.

Exemple 1.3.3. Soit un entier $n > 2$, soit i l'inclusion du groupe alterné A_n dans le groupe symétrique S_n et ε la signature, la suite courte

$$0 \to A_n \xrightarrow{\iota} S_n \xrightarrow{\epsilon} \{-1, 1\} \to 0$$

est exacte et scindée à droite (par exemple, le morphisme de groupes envoyant -1 sur n'importe quelle transposition de S_n est une section de ε) mais pas à gauche (aucun sous-groupe d'ordre 2 de S_n n'est normal).

Remarque 1.3.2 (Lien avec l'homologie).
Soient $(A_n)_{n\in\mathbb{N}}$ des G-modules et $f_n : A_n \to A_{n+1}$ des G-morphismes. On dit que la suite

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \cdots$$

est un complexe différentiel si pour tout n, on a $f_{n+1} \circ f_n = 0$, autrement dit :

$$\mathrm{Im}(f_n) \subseteq \ker(f_{n+1}).$$

En particulier, toute suite exacte est un complexe différentiel. On peut aussi considérer des suites exactes de groupes, d'anneaux, d'espaces vectoriels, etc.

L'homologie d'un complexe différentiel est la mesure de son défaut d'exactitude. Plus précisément, le n-ième groupe d'homologie de $(A_n)_{n\in\mathbb{N}}$ est défini comme étant le groupe quotient

$$H_n = \ker(f_{n+1})/\mathrm{Im}(f_n).$$

La suite est exacte si tous ses groupes d'homologie sont triviaux.

L'homologie est utile en topologie et géométrie : on peut associer un complexe différentiel à tout espace topologique ou à toute variété différentielle. Le complexe associé à un espace topologique est un invariant topologique de l'espace, c'est-à-dire que deux espaces homéomorphes ont le même complexe différentiel associé. En particulier, deux espaces topologiques ayant des groupes d'homologie différents ne sont pas homéomorphes.

Le lemme suivant dit **lemme des cinq** permet d'établir l'injectivité et la surjectivité des G-morphismes (par fois on dit les flèches) dans les diagrammes commutatifs.

Lemme 1.3.1 (Lemme des cinq). *Soit un diagramme commutatif de G-modules à lignes exactes.*

$$\begin{array}{ccccccccc}
M_1 & \xrightarrow{a_1} & M_2 & \xrightarrow{a_2} & M_3 & \xrightarrow{a_3} & M_4 & \xrightarrow{a_4} & M_5 \\
\downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} \\
N_1 & \xrightarrow{b_1} & N_2 & \xrightarrow{b_2} & N_3 & \xrightarrow{b_3} & N_4 & \xrightarrow{b_4} & N_5
\end{array}$$

alors

1. *si f_1 est surjective et f_2, g_1 sont injectives, alors h est injective,*
2. *si g_2 est injective et f_2, g_1 sont surjectives, alors h est surjective, ces deux affirmations donnent la forme la plus utilisée suivante :*
3. *si f_1, f_2, g_1 et g_2 sont bijectives, alors h est bijective,*

Preuve. On commence par montrer l'injectivité de h.

Soit $x_3 \in M_3$. Si $h(x_3) = 0$, alors $g_1(a_3(x_3)) = b_3(h(x_3)) = 0$, donc $a_3(x_3) = 0$ car g_1 est injective. Comme les lignes horizontales sont des suites exactes, il existe $x_2 \in M_2$ tel que $x_3 = a_2(x_2)$. Soit $y_2 = f_2(x_2)$; on a $b_2(y_2) = h(x_3) = 0$, donc il existe $y_1 \in N_1$ tel que $f_2(x_2) = b_1(y_1)$. Mais f_1 est surjective, donc il existe $x_1 \in M_1$ tel que $y_1 = f_1(x_1)$. On a alors $x_3 = a_2(x_2 - a_1(x_1))$ (car $a_2 \circ a_1 = 0$) mais aussi

$$f_2(x_2 - a_1(x_1)) = f_2(x_2) - f_2(a_1(x_1)) = y_2 - b_1(f_1(x_1)) = 0.$$

Donc $x_2 - a_1(x_1) = 0$, car f_2 est injective, et $x_3 = 0$.

Montrons maintenant la surjectivité.

Soit $y_3 \in N_3$; il existe alors $x_4 \in M_4$ tel que $g_1(x_4) = b_3(y_3)$ par surjectivité de g_1. On a $g_2(a_4(x_4)) = b_4(g_1(x_4)) = b_4(b_3(y_3)) = 0$, donc $a_4(x_4) = 0$ car g_2 est injective. Comme les lignes horizontales sont des suites exactes, il existe $x_3 \in M_3$ tel que $a_3(x_3) = x_4$. On a alors : $b_3(y_3 - h(x_3)) = 0$ donc il existe $y_2 \in N_2$ tel que $y_3 - h(x_3) = b_2(y_2)$, puis par surjectivité de f_2, il existe $x_2 \in M_2$ tel que $f_2(x_2) = y_2$. On a alors $y_3 = h(x_3 + a_2(x_2))$ ce qui donne la surjectivité de la troisième flèche verticale. □

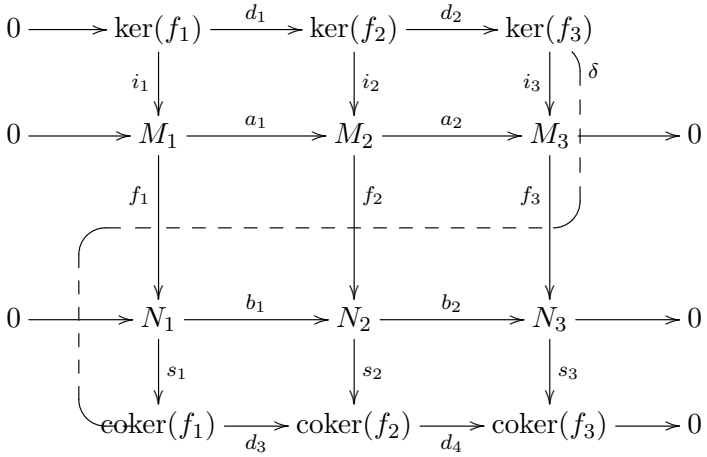
Ceci vaut non seulement pour les G-modules, mais aussi pour les groupes, les espaces vectoriels, les A-modules, etc.

Lemme 1.3.2 (**Lemme du serpent**). *Soit un diagramme commutatif de G-modules à lignes exactes.*

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{a_1} & M_2 & \xrightarrow{a_2} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{b_1} & N_2 & \xrightarrow{b_2} & N_3 & & \end{array}$$

Alors il existe un morphisme δ dit **de connexion** *de* $\ker(f_3)$ *dans* $\operatorname{coker}(f_1)$ *tel que la suite suivante liant les noyaux et les conoyaux de f_1, f_2 et f_3 soit exacte :*

$$0 \longrightarrow \ker(f_1) \longrightarrow \ker(f_2) \longrightarrow \ker(f_3) \xrightarrow{\delta} \operatorname{coker}(f_1) \longrightarrow \operatorname{coker}(f_2) \longrightarrow \operatorname{coker}(f_3) \longrightarrow 0.$$



Preuve. Les morphismes entre les noyaux et les morphismes entre les conoyaux sont induits de manière naturelle par les morphismes (horizontales) donnés par la commutativité du diagramme. L'exactitude des deux suites induites découle directement de l'exactitude des lignes du diagramme d'origine. L'énoncé important du lemme est qu'il existe un morphisme de connexion δ qui complète la suite exacte.

Le morphisme δ peut être construit de la manière suivante :

Choisissez un élément x dans $\ker f_3$ et regardons-le comme un élément de M_3. Comme a_2 est surjectif, il existe alors y dans M_2 avec $f_3(y) = x$. Par la commutativité du diagramme, nous avons $b_2(f_2(y)) = f_3(a_2(y)) = f_3(x) = 0$ (puisque x est dans le noyau de f_3), et donc $f_2(y)$ est dans le noyau de b_2. Puisque la ligne du bas est exacte, nous trouvons un élément z dans N_1 avec $b_1(z) = f_2(y)$. L'élément z est unique par l'injectivité de b_1. On définit alors $\delta(x) = z + Im(f_1)$. Il faut maintenant vérifier que δ est bien défini (c'est-à-dire que $\delta(x)$ ne dépend que de x et non du choix de y), qu'il s'agit d'un homomorphisme et que la longue suite résultante est en effet exacte. On peut vérifier régulièrement l'exactitude par la poursuite du diagramme (voir la preuve de [12, Lemme 9.1, page 159]) □

1.4 Groupe de classes de rayon

Soient K un corps de nombres et $\mathcal{O}_K$ son anneau des entiers algébriques. Notons par $\mathbf{I}_K$ Le groupe des idéaux fractionnaires de K, c'est un groupe abelien engendré par les premiers fini. Il existe une application naturelle

$$\begin{array}{rccl} i: & K^* & \longrightarrow & \mathbf{I}_K \\ & \alpha & \longmapsto & i(\alpha) = (\alpha) = \alpha\mathcal{O}_K, \end{array}$$

où K^* est le groupe multiplicative de K. Le noyau de i est U_K, le groupe des unités de l'anneau $\mathcal{O}_K$. La structure de U_K est bien connue par le théorème des unités de Dirichlet. Le conoyau de i, $\mathbf{I}_K/Im(i)$, est le groupe de classes de K, noté C_K ou $\mathrm{Cl}(K)$. Le groupe $\mathrm{Cl}(K)$ est fini et la suite suivante est exacte :

$$0 \to U_K \xrightarrow{i_c} K^* \xrightarrow{i} \mathbf{I}_K \xrightarrow{p_c} \mathrm{Cl}(K) \to 0,$$

i_c et p_c sont l'injection et la projection canoniques respectivement.

Rappelons que, pour un corps de nombres K, on définit un premier ou une place de K comme étant une classe d'équivalence d'une valuation non trivial sur K. Il existe deux types de premiers : les premiers finis qui peuvent être identifiés, via le théorème d'Ostrowski, aux idéaux premiers de $\mathcal{O}_K$, et les premiers infinis de K. Un premier infini réal peut être identifié à un plongement de K dans $\mathbb{R}$, et un premier infini complexe peut être identifié à une paire conjuguée de plongements de K dans $\mathbb{C}$. Nous utiliserons $\mathfrak{p}$ ou v pour désigner un nombre premier fini ou infini.

Définition 1.4.1. Un module de K est un produit formelle

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})},$$

où l'idéal $\mathfrak{p}$ parcourt tous les idéaux premiers finis ou infinis de K tel que l'exposant $m(\mathfrak{p}) \geq 0$, et $m(\mathfrak{p}) > 0$ uniquement pour un nombre fini de $\mathfrak{p}$. De plus si $\mathfrak{p}$ est un premier infini réel alors $m(\mathfrak{p}) = 0$ ou 1 et s'il est complexe $m(\mathfrak{p}) = 0$.

Remarques 1.4.1. 1. Quelques auteurs parlent du **diviseur** de K au lien du module de K.

2. Un module $\mathfrak{m}$ de K peut s'écrire sous la forme suivante :

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$$

où $\mathfrak{m}_\infty$ est un produit de premiers infinis réels (i.e., $\mathfrak{m}_\infty$ est un ensemble ou produit d'ensembles de plongements réels de K dans $\mathbb{C}$), et $\mathfrak{m}_0$ est un produit des puissances positives d'idéaux premiers finis, donc $\mathfrak{m}_0$ peut être identifié à un idéal de $\mathcal{O}_K$.

3. Dans la définition précédente $m(\mathfrak{p})$ désigne la valuation $\mathfrak{p}$-adique $v_\mathfrak{p}(\mathfrak{m})$.

Exemple 1.4.1. $\mathfrak{m} = (1)$, $\mathfrak{m} = \mathfrak{p}_\infty$, $\mathfrak{m} = (3)^2(5)^3(17)^4$ et $\mathfrak{m} = (5)^3(17)^4(19)^5\mathfrak{p}_\infty$ sont des modules de $\mathbb{Q}$.

Définition 1.4.2. Soient $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}$ et $\mathfrak{n} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ deux modules de K.

1. On dit que $\mathfrak{m}$ divise $\mathfrak{n}$, et on note $\mathfrak{m}|\mathfrak{n}$, si $m(\mathfrak{p}) \leq n(\mathfrak{p})$ pour tout $\mathfrak{p}$. Autrement dit, $\mathfrak{m}|\mathfrak{n} \iff \mathfrak{m}_0|\mathfrak{n}_0$ (i.e., $\mathfrak{n}_0 \subset \mathfrak{m}_0$) et $\mathfrak{m}_\infty \subset \mathfrak{n}_\infty$. En particulier, un premier $\mathfrak{p}$ divise $\mathfrak{m}$ si et seulement si $m(\mathfrak{p}) > 0$.
2. Si $\mathfrak{a}$ est un idéal fractionnaire non-nul de K, alors on dit que $\mathfrak{a}$ est premier à $\mathfrak{m}$ si $v_\mathfrak{p}(\mathfrak{a}) = 0$ pour tout $\mathfrak{p}|\mathfrak{m}_0$; ceci est équivalent à dire : $\mathfrak{a}$ est premier à $\mathfrak{m}$ si on peut écrire $\mathfrak{a} = \dfrac{\mathfrak{b}}{\mathfrak{c}}$ avec $\mathfrak{b}$ et $\mathfrak{c}$ deux idéaux entiers étrangers à $\mathfrak{m}_0$ (i.e. $\mathfrak{b} + \mathfrak{m}_0 = \mathcal{O}_K$ et $\mathfrak{c} + \mathfrak{m}_0 = \mathcal{O}_K$).
3. On dit qu'un élément $\alpha \in K^*$ est premier à $\mathfrak{m}$ si l'idéal principal $(\alpha) = \alpha\mathcal{O}_K$ est premier à $\mathfrak{m}$.

Remarque 1.4.1. Si $\mathfrak{a}$ n'est pas un idéal entier de $\mathcal{O}_K$, alors $\mathfrak{a}$ est premier à $\mathfrak{m}$ ne veut pas dire que $\mathfrak{a} + \mathfrak{m}_0 = \mathcal{O}_K$, puisque cette égalité implique que $\mathfrak{a} \subset \mathcal{O}_K$.

Lemme 1.4.1. *Soit $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}$ un module de K. L'ensemble des idéaux fractionnaires de K premiers à $\mathfrak{m}$ est un groupe, il sera noté par $\mathbf{I}_K^\mathfrak{m}$.*

Preuve. Simple à vérifier. □

Dans la suite, nous allons étendre la relation de congruence entre les éléments de $\mathcal{O}_K$ modulo un idéal à la notion de congruence entre les éléments de K^* modulo un module de K.

Définition 1.4.3.

1. Soit $\mathfrak{p}$ un idéal premier réel de K et soit $x \longmapsto x_\mathfrak{p}$ le plongement de x dans le complété $K_\mathfrak{p} = \mathbb{R}$, i.e. $x_\mathfrak{p}$ est l'image de x par le plongement associé à $\mathfrak{p}$. Soient α et β dans K^*, alors

$$\alpha \equiv^* \beta \pmod{\mathfrak{p}} \text{ si et seulement si } \alpha_\mathfrak{p},\ \beta_\mathfrak{p} \text{ ont le même signe,}$$

c'est-à-dire $(\frac{\alpha}{\beta})_\mathfrak{p} > 0$.

2. Soit $\mathfrak{p}$ un premier fini identifié à un idéal de $\mathcal{O}_K$. Soit n un entier positive, rappelons que dans le localisé $(\mathcal{O}_K)_\mathfrak{p}$ de $\mathcal{O}_K$ en $\mathfrak{p}$, les éléments $1 + \mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p}$ sont des unités et forment un sous-groupe du groupe des unités $U((\mathcal{O}_K)_\mathfrak{p})$ de $\mathcal{O}_K$ (c'est le noyau de l'homomorphisme

$U((\mathcal{O}_K)_\mathfrak{p}) \longrightarrow U\left((\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p}\right)$.
Soient deux éléments α et β dans K^*, on écrit

$$\alpha \equiv^* \beta \pmod{\mathfrak{p}^n}$$

pour dire que α et β sont dans la même classe d'équivalence $1+\mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p}$ (ce qui est équivalent à dire que $\alpha(1+\mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p}) = \beta(1+\mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p})$), i.e.
$\alpha \in \beta(1+\mathfrak{p}^n(\mathcal{O}_K)_\mathfrak{p})$. Autrement dit

$$\alpha \equiv^* \beta \pmod{\mathfrak{p}^n} \Longleftrightarrow \frac{\alpha}{\beta} \text{ est une unité de } (\mathcal{O}_K)_\mathfrak{p} \text{ et } v_\mathfrak{p}\left(\frac{\alpha}{\beta}-1\right) \geq n.$$

Définition 1.4.4 (Congruence multiplicative). Soit maintenant un module $\mathfrak{m}$ du corps K. Soient α et β dans K^*, alors on a :

$$\alpha \equiv^* \beta \pmod{\mathfrak{m}} \Longleftrightarrow \alpha \equiv^* \beta \pmod{\mathfrak{p}^{n(\mathfrak{p})}} \text{ pour tout } \mathfrak{p} \text{ de } K \text{ tel que } n(\mathfrak{p}) > 0.$$

Comme cas particulier, pour tout $\alpha \in K^*$ on a :

$$\alpha \equiv^* 1 \pmod{\mathfrak{m}} \Longleftrightarrow \begin{cases} v_\mathfrak{p}(\alpha-1) > n(\mathfrak{p}), \forall \mathfrak{p}|\mathfrak{m}_0 \text{ avec } v_\mathfrak{p}(\mathfrak{m}_0) = n(\mathfrak{p}) > 0, \\ \alpha_\mathfrak{p} > 0, \text{ pour chaque } \mathfrak{p} \text{ divisant } \mathfrak{m}_\infty. \end{cases}$$

Remarque 1.4.2. Notons qu'on vérifie simplement que la congruence modulo un module $\mathfrak{m}$ de K est compatible avec le produit mais ne l'est pas avec l'addition, puisque K^* n'est pas stable pour l'addition.

Définition 1.4.5. Soit $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ un module de K, de partie finie $\mathfrak{m}_0$ et de partie infinie $\mathfrak{m}_\infty$. On définit deux parties de K^* comme suit

$$K_\mathfrak{m} = \{\tfrac{a}{b} \mid a,\ b \in \mathcal{O}_K;\ \text{et les idéaux } (a),(b) \text{ sont premiers avec } \mathfrak{m}_0\}$$
$$K_{\mathfrak{m},1} = \{\alpha \in K_\mathfrak{m} \mid \alpha \equiv^* 1 \pmod{\mathfrak{m}}\}.$$

Remarque 1.4.3. Il faut noter que $K_\mathfrak{m}$ et $K_{\mathfrak{m},1}$ sont des sous-groupes de K^*, et que $K_\mathfrak{m}$ dépend uniquement des premiers finis divisant $\mathfrak{m}$ et non pas de leurs exposants. Tandis que le groupe $K_{\mathfrak{m},1}$ dépend des premiers finis et infinis divisant $\mathfrak{m}$ et aussi des exposants de ceux qui sont finis. Le groupe $K_{\mathfrak{m},1}$ est dit **le rayon modulo** $\mathfrak{m}$.

Notation. Soient $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ un module de K et S un ensemble contenant des premiers finis de $\mathcal{O}_K$. Rappelons que $\mathbf{I}_K^S$ désignera le groupe abélien libre engendré par les idéaux premiers de $\mathcal{O}_K$ n'appartenant pas à S. On notera aussi par $\mathbf{I}_K^\mathfrak{m}$ le groupe des idéaux engendrés par les idéaux premiers ne divisant pas $\mathfrak{m}_0$, $\mathbf{I}_K^\mathfrak{m}$ dépend des premiers finis divisant $\mathfrak{m}$ et non pas de leurs exposants.

Considérons aussi l'homomorphisme $i : K^* \longrightarrow \mathbf{I}_K^\mathfrak{m};\ \alpha \longmapsto i(\alpha) = (\alpha)$. i envoie $K_\mathfrak{m}$ et $K_{\mathfrak{m},1}$ dans $\mathbf{I}_K^\mathfrak{m}$. Notons que $i(K_{\mathfrak{m},1})$ est le groupe des idéaux fractionnaires de K qui sont engendrés par les éléments $\alpha \in K^*$ tels que $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$.

Définition 1.4.6. Soit un module $\mathfrak{m}$ de K. Le quotient $\mathbf{I}_K^\mathfrak{m}/i(K_{\mathfrak{m},1})$ est un groupe fini appelé le **groupe de classes de rayon** modulo $\mathfrak{m}$, on le note $\mathrm{Cl}_\mathfrak{m}(K)$. Les classes dans ce quotient sont dites les **classes de rayon** modulo $\mathfrak{m}$.

Exemple 1.4.2. Considérons le corps $K = \mathbb{Q}$.

1. Soit n un entier naturel non nul, soit le module $\mathfrak{m} = (n)$ l'idéal engendré par n. Alors le groupe $\mathbf{I}_K^{\mathfrak{m}}$ est constitué des idéaux premiers engendrés par les entiers rationnels premiers à n, d'où
$$\mathbf{I}_K^{\mathfrak{m}} \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$
Soit $(r) \in \mathbf{I}_K^{\mathfrak{m}}$, alors (r) est engendré par r et $-r$. Si $(r) \in i(K_{\mathfrak{m},1})$, alors on doit avoir $\pm r \equiv 1 \pmod{n}$, donc $r \equiv \pm 1 \pmod{n}$. D'où $i(K_{\mathfrak{m},1}) = \{\pm 1\}$, par suite
$$\mathrm{Cl}_{\mathfrak{m}}(K) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}/\{\pm 1\}.$$

2. Soit le module $\mathfrak{m} = (n)\mathfrak{p}_{\infty}$, où $\mathfrak{p}_{\infty}$ est le premier réal associé à la valeur absolue. Alors le groupe $\mathbf{I}_K^{\mathfrak{m}}$ est constitué des idéaux premiers engendrés par les entiers rationnels premiers à n, même dans ce cas on a :
$$\mathbf{I}_K^{\mathfrak{m}} \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$
Soit $(r) \in \mathbf{I}_K^{\mathfrak{m}}$, alors (r) est engendré par r et $-r$. Si $(r) \in i(K_{\mathfrak{m},1})$, alors nous devons être capable de prendre un générateur positive congruent à 1 mod n, donc on doit avoir $|r| \equiv 1 \pmod{n}$, car si $|r| \equiv \pm 1 \pmod{n}$, alors $(r) \notin i(K_{\mathfrak{m},1})$. D'où $i(K_{\mathfrak{m},1}) = \{1\}$, par suite
$$\mathrm{Cl}_{\mathfrak{m}}(K) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}/\{1\} \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Chapitre 2

Cohomologie des groupes cycliques

2.1 Les groupes cohomologiques H^0 et H^1

Soit $G = \langle \sigma \rangle$ un groupe cyclique d'ordre n, le générateur σ est fixe le long de cette section. Posons

$$\Delta = 1 - \sigma \qquad \text{et} \qquad N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}.$$

Pour un G-module A, Δ et N agissent, comme des endomorphismes de A, par les règles suivantes :
- si A est un groupe additif, alors

$$\Delta(a) = a - \sigma(a), \quad \text{et} \quad N(a) = a + \sigma(a) + \cdots + \sigma^{n-1}(a),$$

- si A est un groupe multiplicatif, alors

$$\Delta(a) = \tfrac{a}{\sigma(a)}, \quad \text{et} \quad N(a) = a\sigma(a)\cdots\sigma^{n-1}(a).$$

Notation. Pour faire apparaître le module sur lequel Δ et N agissent, nous noterons dans la suite Δ_A et N_A.

Remarques 2.1.1.

1. Si $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$ est le groupe de Galois d'une extension cyclique L/K, alors en prenant $A = \mathrm{Cl}(L)$, N est un endomorphisme sur $\mathrm{Cl}(L)$ appelé la norme algébrique. En général $N \neq N_{L/K}$, mais ces deux normes sont reliées par la relation suivante : $N = j \circ N_{L/K}$, où $j : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(L)$ est le transfert des classes idéaux.
2. Remarquez que si $A = L^*$ le groupe multiplicatif d'une extension cyclique L galoisienne d'un corps K de groupe de Galois G, alors $N = N_{L/K}$.

Lemme 2.1.1. *Indépendamment des modules les égalités suivantes sont toujours satisfaites :*

$$N\Delta = \Delta N = 0.$$

Par consequent, $Im(\Delta) \subset \ker(N)$ *et* $Im(N) \subset \ker(\Delta)$.

Preuve. On a $N\Delta = (1+\sigma+\sigma^2+\cdots+\sigma^{n-1})(1-\sigma)$
$= 1+\sigma+\sigma^2+\cdots+\sigma^{n-1}-\sigma-\sigma^2-\cdots-\sigma^{n-1}-\sigma^n$
$= 1-\sigma^n = 1-1 = 0.$
De même $\Delta N = 1-\sigma^n = 1-1 = 0$.
Donc pour $b \in Im(\Delta)$, il existe $a \in A$ tel que $b = \Delta(a)$, d'où $N(b) = N\Delta(a) = 0$, c-à-dire $b \in \ker(N)$, alors $Im(\Delta) \subset \ker(N)$. L'autre inclusion est prouvée de la même façon. □

Notons que l'égalité entre ces groupes n'est pas toujours réalisée, la différence est alors mesurée par la paire de groupes abéliens suivante.

Définition 2.1.1. Soit un G-module A, alors les groupes de cohomologie de A sont :

$$H^0(A) = \frac{\ker(\Delta_A)}{N(A)} \qquad \text{et} \qquad H^1(A) = \frac{\ker(N_A)}{\Delta(A)}.$$

Dans le résultat suivant, nous montrons qu'un G-morphisme induit un morphisme entre les groupes de cohomologie.

Proposition 2.1.1. *Soient A et B deux G-modules et $f : A \longrightarrow B$ un G-morphisme. Alors*

1. *f commute avec Δ et N,*
2. *$f(\ker(\Delta_A)) \subset \ker(\Delta_B)$ et $f(N(A)) \subset N(B)$,*
3. *il existe des applications f_i induites par f telles que f_i est un morphisme de $H^i(A)$ dans $H^i(B)$, pour $i = 0, 1$.*

Preuve. 1. Comme f est un G-module, alors pour tout $a \in A$,

$$\Delta f(a) = \Delta(f(a)) = f(a) - \sigma(f(a)) = f(a) - f(\sigma(a)) = f(a - \sigma(a)) = f\Delta(a),$$

donc $\Delta f = f\Delta$. De la même on montre que f commute avec N.
2. Par 1. on a pour tout $a \in \ker(\Delta_A)$:

$$\begin{aligned} \Delta_A(a) = 0 &\Longrightarrow f(\Delta_A(a)) = f(0) = 0 \\ &\Longrightarrow \Delta_B(f(a)) = 0 \\ &\Longrightarrow f(a) \in \ker(\Delta_B), \end{aligned}$$

Donc $f(\ker(\Delta_A)) \subset \ker(\Delta_B)$.
De même, pour tout $b \in N(A)$, il existe $a \in A$ tel que $b = N(a)$, donc

$$\begin{aligned} b = N(a) &\Longrightarrow f(b) = f(N(a)) \\ &\Longrightarrow f(b) = N(f(a)) \\ &\Longrightarrow f(b) \in N(B), \text{ car } f(a) \in B \Longrightarrow N(f(a)) \in N(B). \end{aligned}$$

$f(N(A)) \subset N(B)$.
3. Le point 2. permet de définir deux applications :

$$\begin{aligned} f_0 : H^0(A) = \frac{\ker(\Delta_A)}{N(A)} &\longrightarrow H^0(B) = \frac{\ker(\Delta_B)}{N(B)} \\ a + N(A) &\longmapsto f_0(a + N(A)) = f(a) + N(B) \end{aligned}$$

et

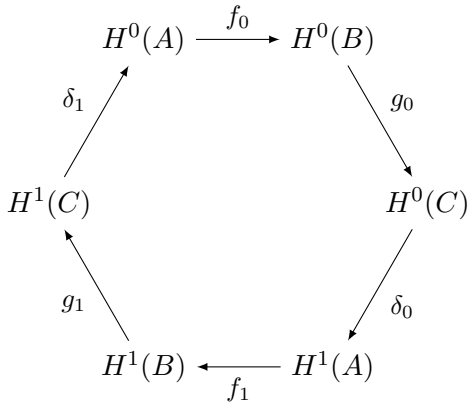
$$\begin{aligned} f_1 : H^1(A) = \frac{\ker(N_A)}{\Delta(A)} &\longrightarrow H^1(B) = \frac{\ker(N_B)}{\Delta(B)} \\ a + \Delta(A) &\longmapsto f_1(a + \Delta(A)) = f(a) + \Delta(B) \end{aligned}$$

□

Lemme 2.1.2 (L'hexagone exact)**.** *Soit une suite exacte de G-modules et de G-homomorphismes*

$$0 \longrightarrow A - \xrightarrow{f} B - \xrightarrow{g} C \longrightarrow 0.$$

Alors il existe des applications δ_0 et δ_1 telles que l'hexagone suivant soit exact en chaque groupe :



Preuve. Commençons d'abord par définir ce qu'on appelle **les homomorphismes de connection δ_0 et δ_1**. Une fois cela fait, la vérification de l'exactitude est un exercice élémentaire mais laborieux qui repose uniquement sur l'exactitude de la suite de départ. Ces détails sont laissés au soin du lecteur.

Soit $c \in \ker(\Delta_C)$, il existe donc $b \in B$ tel que $g(b) = c$, car g est surjective. On en déduit que $\Delta g(b) = g(\Delta b) = \Delta c = 0$, d'où $\Delta b \in \ker g = \operatorname{Im} f$. Il existe alors $a \in A$ tel que $f(a) = \Delta b$. L'égalité $Nf(a) = f(Na) = N\Delta b = 0$ montre que $Na \in \ker f = \{0\}$. Finalement $a \in \ker N$. L'application δ_0 est définie par l'équation :

$$\delta_0(c + N(C)) = a + \Delta(A)$$

et c'est une application de $H^0(C)$ vers $H^1(A)$. On doit montrer que δ_0 est bien définie. Supposons $c + N(C) = c' + N(C)$ et $g(b') = c'$. Alors $\Delta b' = f(a')$ et il faut vérifier que $a - a' \in \Delta A$. Il existe $b'' \in B$ tel que $c - c' = Ng(b'') = gN(b'')$. Nous avons maintenant $g(b - b' - N(b'')) = 0$, alors il existe $a'' \in A$ tel que $b - b' - N(b'') = f(a'')$. On en déduit que $\Delta b - \Delta b' = \Delta f(a'') = f(\Delta a'') = f(a - a')$. Comme f est injective, $a - a'$ est dans $\Delta(A)$. Ainsi, δ_0 est bien définie.

le fait que δ_0 est un homomorphisme découle directement du fait qu'à chaque étape des calculs précédents un élément a été choisi en utilisant les homomorphismes de la suite de départ.

L'application δ_1 est définie de façon analogue. Pour $c \in \ker(N_C)$ nous posons :

$$\delta_1(c + \Delta(C)) = a + N(A)$$

si $g(b) = c$ et $f(a) = Nb$. Le reste de la démonstration est laissé à titre d'exercice. □

2.2 Le quotient d'Herbrand

Définition 2.2.1. Soit A un G-module. Le quotient de Herbrand de A, sous la condition que $H^0(A)$ et $H^1(A)$ soient finis, est le rapport

$$q(A) = \frac{|H^1(A)|}{|H^0(A)|}.$$

On dira que le quotient de Herbrand $q(A)$ pour un G-module A est défini si $H^0(A)$ et $H^1(A)$ sont des groupes finis.

Lemme 2.2.1. *Soit $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ une suite exacte de G-modules. Si deux des trois objets $q(A)$, $q(B)$ et $q(C)$ sont définis, alors tous les quotients sont définis et $q(A)q(C) = q(B)$.*

Preuve. En utilisant le lemme de l'hexagone et en supposant que $q(A)$ et $q(B)$ sont définis, alors on trouve que :

$$|H^i(C)| = |\ker(\delta_i)||\mathrm{Im}\,\delta_i| = |\mathrm{Im}\,g_i||\mathrm{Im}\,\delta_i|.$$

Maintenant g_i est défini sur un groupe fini et $\mathrm{Im}\,\delta_i$ est contenu dans un groupe fini, d'où $q(C)$ est défini.

Il faut remarquer que :

$$|H^0(A)||H^0(C)||H^1(B)| = |H^1(A)||H^1(C)||H^0(B)|$$

car les deux quantités sont égales à :

$$|\ker(f_0)||\mathrm{Im}\,f_0||\ker(\delta_0)||\mathrm{Im}\,\delta_0||\ker(g_1)||\mathrm{Im}\,g_1|.$$

On en déduit donc que $q(A)q(C) = q(B)$.
Les autres cas se traitent de la même manière. □

Corollaire 2.2.1. *Si $A \subset B$ sont des G-modules et $C = B/A$ est fini, alors $q(A) = q(B)$ lorsque l'un des deux quotients est défini.*

Preuve. Le résultat découle du fait que $q(C) = 1$ lorsque C est un groupe fini. En effet, si tel est le cas pour C, alors :

$$q(C) = \frac{[\ker(N) : \mathrm{Im}\,(\Delta)]}{[\ker(\Delta) : \mathrm{Im}\,(N)]} = \frac{|\ker(N)||\mathrm{Im}\,(N)|}{|\ker(\Delta)||\mathrm{Im}\,(\Delta)|} = \frac{|C|}{|C|}.$$

D'où le résultat. □

Exemple 2.2.1 (Le quotient d'Herbrand d'un module de permutation)**.** Pour illustrer toutes ces idées, on considérera l'exemple suivant qu'on utilisera plus tard.

Soient d un diviseur quelconque de $n = |G|$ et R un domaine d'intégrité (anneau commutatif intègre) de caractéristique 0, et soit aussi :

$$A = \sum_{i}^{d} Ru_i$$

un R-module libre de rangs d et de générateurs les u_i. On suppose que G agit sur A en permutant les éléments de la base selon les règles suivantes :

$$\sigma(u_i) = \begin{cases} u_{i+1} & \text{si } i < d, \\ u_1 & \text{si } i = d. \end{cases}$$

Clairement σ^d engendre le sous-groupe qui agit comme l'identité sur A. On notera ce sous-groupe par $G_A = \langle \sigma^d \rangle$ qui est un sous-groupe d'indice d dans G. alors

Proposition 2.2.1. *Posons $m = nd$. Si R/mR est fini, alors $q(A)$ est bien défini et on a $q(A) = [R : mR]^{-1}$. En particulier si $R = \mathbb{Z}$, alors $q(A) = [\mathbb{Z} : m\mathbb{Z}]^{-1} = G_A^{-1}$.*

Preuve. En calculant les groupes impliqués dans la définition du quotient $q(A)$, on trouve :

a. $\ker N = \{\sum a_i u_i \mid \sum a_i = 0\}$,

b. $\operatorname{Im} \Delta = \ker N$,

c. $\ker \Delta = R(u_1 + \cdots + u_d)$,

d. $\operatorname{Im} N = mR(u_1 + \cdots + u_d)$.

On en déduit alors que $H^0(A) \simeq \mathbb{Z}/m\mathbb{Z}$ et $H^1(A) = 0$, d'où le résultat. □

Chapitre 3

Préparation pour la seconde inégalité

3.1 Rappel

Dans cette section, on suppose que l'extension de corps de nombres L/K est galoisienne de groupe de Galois cyclique $G = \langle \sigma \rangle$. Notons par $\mathcal{O}_k$ l'anneau des entiers d'un corps de nombres k.

Définition 3.1.1. Soit $\mathcal{P}$ un premier infini de K. On dit que $\mathcal{P}$ est ramifié dans L si $\mathcal{P}$ est réel sur K mais $\mathcal{P}$ s'étend à un premier complexe de L. Dans ce cas, on pose l'indice de ramification $e_{\mathcal{P}} = 2$ et formellement $f_{\mathcal{P}} = 1$. Pour les premiers $\mathcal{P}$ infinis non ramifiés on pose $e_{\mathcal{P}} = f_{\mathcal{P}} = 1$.

Soit $\mathfrak{m}$ un module de K contenant au moins tous les premiers (finis et infinis) de K qui se ramifient dans L. On rappelle q'un modules $\mathfrak{m}$ de K est un produit formel $\mathfrak{m} = \prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}$ pris sur tous les idéaux premiers de K avec $n_{\mathcal{P}}$ un entier positif qui est non nul uniquement pour un nombre fini de $\mathcal{P}$. De plus, $n_{\mathcal{P}} = 0$ ou 1 si $\mathcal{P}$ est un premier réel infini et $n_{\mathcal{P}} = 0$ si $\mathcal{P}$ est un premier complexe infini.

Rappelons que $\mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}$ est défini comme étant le sous-groupe du groupe des idéaux $\mathbf{I}_{\mathbf{K}}$ engendré par tous les idéaux premiers de K ne divisant pas $\mathfrak{m}$, de même $\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}$ est le groupe des idéaux fractionnaires de L dont la décomposition en idéaux premiers ne contient aucun idéal divisant $\mathfrak{m}$ avec un exposant non nul.

Chaque idéal premier $\mathcal{P}$ de K peut être vu comme un produit d'idéaux dans L. De cette façon, $\mathfrak{m}$ est aussi considéré comme un module de L. Ainsi, $\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}$ est parfaitement défini et c'est un G-module puisque si $\mathfrak{p}$ est un idéal premier de L ne divisant pas $\mathfrak{m}$, alors $\sigma(\mathfrak{p})$ ne divise pas $\mathfrak{m}$ non plus.

On commence par calculer certains groupes.

3.2 Calcul de certains groupes de cohomologie

Proposition 3.2.1. *Soit $\mathfrak{m}$ un module de K divisible par tous les premiers de K qui se ramifies dans L. Alors*

a. $H^0(L^*) = K^*/N(L^*)$.

b. $H^1(L^*) = 1$.

c. $H^0(\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}) = \mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}/N(\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}})$.

d. $H^1(\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}) = 1$.

Preuve.
a. Rappelons que $H^0(L^*) = \dfrac{\ker(\Delta_{L^*})}{N(L^*)}$, alors le résultat est immédiat puisque $\ker(\Delta_{L^*})$ est l'ensembles des éléments de L^* laissés fixes par G qui est K^*.
b. Montrer que $H^1(L^*) = 1$ consiste à redémontrer le théorème 90 de Hilbert.
c. De la même manière, un idéal fractionnaire $\mathcal{H} = \prod \mathfrak{P}_i$ de $\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}$ est laissé fixe par σ si et seulement si $\mathcal{H} \in \ker(\Delta_{\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}})$, c-à-d $\ker(\Delta_{\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}})$ est l'ensemble des idéaux fractionnaires $\mathcal{H}$ de $\mathbf{I}_{\mathbf{L}}^{\mathcal{M}}$ laissés fixes par G. Supposons que pour un premier $\mathfrak{P}$ de L on a $\mathfrak{P}^k$ divise $\mathcal{H}$, alors tous les $\sigma^i(\mathfrak{P})$ divisent $\mathcal{H}$ et donc la k-ème puissance du produit des distincts conjugués de $\mathfrak{P}$ divise $\mathcal{H}$. Maintenant si $\mathfrak{P} \cap K = P$, alors P ne divise pas $\mathfrak{m}$, donc P est non ramifié dans L. Ainsi, P est le produit des distincts conjugués de $\mathfrak{P}$, d'où $\mathcal{H} = \mathcal{H}_0 P^k$ avec $\mathcal{H}_0$ aussi fixe par G. Il s'ensuit de cette façon que $\mathcal{H} \in \mathbf{I}_{\mathbf{K}}^{\mathfrak{m}}$.
d. Il reste à prouver que $H^1(\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}) = 1$. Soit $\mathcal{H} \in \mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}$ avec $N(\mathcal{H}) = 1$. Soit $\mathfrak{P}_0^{a_0}$ la puissance exacte du premier $\mathfrak{P}_0$ qui apparaît dans $\mathcal{H}$. soit $\mathfrak{P}_i = \sigma^i(\mathfrak{P}_0)$ pour $1 \leq i \leq g-1$ et supposons $\sigma^g(\mathfrak{P}_0) = \mathfrak{P}_0$ avec g minimal. Soit $\mathfrak{P}_i^{a_i}$ la puissance de $\mathfrak{P}_i$ divisant $\mathcal{H}$. Posons :

$$\mathfrak{B} = \mathfrak{P}_0^{a_0}\mathfrak{P}_1^{a_0+a_1}\cdots\mathfrak{P}_{g-2}^{a_0+\cdots+a_{g-2}},$$

alors

$$\Delta\mathfrak{B} = \mathfrak{P}_0^{a_0}\mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_{g-2}^{a_{g-2}}\mathfrak{P}_{g-1}^{b},$$

où $b = -a_0 - \cdots - a_{g-2}$. Soit P tel que $N(\mathfrak{P}_0) = P^f$. Comme $N(\mathcal{H}) = 1$ et comme la P-partie de $N(\mathcal{H})$ doit provenir des termes $N(\mathfrak{P}_i)$, alors :

$$N(\prod \mathfrak{P}_i^{a_i}) = P^{f(a_0+\cdots+a_{g-1})} = 1.$$

On en déduit alors que $\sum a_i = 0$, d'où $b = a_{g-1}$. Par conséquent, $\Delta\mathfrak{B}$ est la contribution des $\mathfrak{P}_i$ dans l'écriture de $\mathcal{H}$ en produit de premiers de L. En procédant de la même manière avec les autres diviseurs premiers de $\mathcal{H}$, on arrive au fait que $\mathcal{H} = \Delta(\mathfrak{B}_1 \cdots \mathfrak{B}_r)$, c.-à.d. $\mathcal{H} \in \operatorname{Im}\Delta$, d'où $\ker N = \operatorname{Im}\Delta$, par suite $H^1(\mathbf{I}_{\mathbf{L}}^{\mathfrak{m}}) = 1$. □

3.3 Sur les S-unités

Nous allons définir dans cette sous-section certains G-modules et certains G-morphismes très utilisées dans la suite du cours. Soit toujours $\mathfrak{m}$ un module de K.

Commençons par l'homomorphisme $j_{\mathfrak{m}} : \mathbf{I_L} \to \mathbf{I_L^{\mathfrak{m}}}$ défini sur les premiers par :

$$j_{\mathfrak{m}}(\mathfrak{P}) = \begin{cases} \mathfrak{P}, & \mathfrak{P} \not| \mathfrak{m}, \\ 1, & \mathfrak{P} | \mathfrak{m}. \end{cases}$$

Évidemment, $j_{\mathfrak{m}}$ est surjective et envoie un idéal $\mathcal{H}$ sur la partie de $\mathcal{H}$ relativement première à $\mathfrak{m}$.

On rappelle que l'application $i : L^* \longrightarrow \mathbf{I_L}$ fait correspondre à un élément α de L^* l'idéal fractionnaire principal $(\alpha) = \alpha\mathcal{O}_{L^*}$ de $\mathbf{I_L}$ engendré par α. On notera par $f_{\mathfrak{m}}$ la composée $j_{\mathfrak{m}} o i = j_{\mathfrak{m}} i : L^* \to \mathbf{I_L^{\mathfrak{m}}}$.

Il faut noter que tous les groupes mentionnés sont des G-modules et les applications i, $j_{\mathfrak{m}}$ et $f_{\mathfrak{m}}$ sont des G-morphismes.

Notons par S l'ensemble des idéaux premiers de L qui divisent $\mathfrak{m}$, et soit $L^S = \ker f_{\mathfrak{m}}$. On peut facilement voir que :

$$L^S = \{\alpha \in L^* \mid i(\alpha) \text{ est divisible uniquement par des premiers de } S\}.$$

Dans le cas où $S \subseteq S_\infty$; l'ensemble des premiers infinis, L^S n'est rien d'autre que le groupe des unités de $\mathcal{O}_L$ l'anneau des entiers de L qu'on note $L^S = \mathbf{U}_L$. C'est pour cette raison qu'on dit que (pour tout S) L^S est le groupe des S-unités. En fait, L^S est l'ensemble des éléments qui sont des unités localement en dehors de S.

On va commencer par une série de calculs pour déterminer le quotient de Herbrand de plusieurs G-modules.

Lemme 3.3.1. *Si $q(\mathbf{U}_L)$ et $q(\ker(j_{\mathfrak{m}}))$ sont définis, alors $q(L^S) = q(\mathbf{U}_L)q(\ker(j_{\mathfrak{m}}))$.*

Preuve. L'équation $1 = f_{\mathfrak{m}}(L^S) = j_{\mathfrak{m}} i(L^S)$ donne naissance à une suite exacte :

$$1 \to i(L^S) \to \ker(j_{\mathfrak{m}}) \to C \to 1$$

pour un certain groupe C. En fait, C est fini puisque :

$$C \simeq \frac{\ker(j_{\mathfrak{m}})}{i(L^S)} \simeq \frac{\ker(j_{\mathfrak{m}})}{i(L^*) \cap \ker(j_{\mathfrak{m}})} \simeq \frac{i(L^*)\ker(j_{\mathfrak{m}})}{i(L^*)}$$

car $i(L^S) = \ker(j_{\mathfrak{m}}) \cap i(L^*)$ et le dernier sous-groupe quotient est un sous-groupe du groupe des classe d'idéaux de L qui est un groupe fini. Donc par le Lemme 2.2.1 et le Corollaire 2.2.1 (puisque $q(\ker(j_{\mathfrak{m}}))$ est défini) on a $q(i(L^S)) = q(\ker(j_{\mathfrak{m}}))$. Après, en utilisant la suite exacte

$$1 \to \mathbf{U}_L \to L^S \to i(L^S) \to 1$$

nous concluons que $q(L^S) = q(\mathbf{U}_L)q(\ker(j_{\mathfrak{m}}))$. □

3.4 Calcul des quotients de Herbrand de $\mathbf{U}_L$ et du groupe de S-unités

La prochaine tâche sera le calcul de $q(\mathbf{U}_L)$ et $q(\ker(j_{\mathfrak{m}}))$. Le premier quotient de Herbrand est calculé en trouvant un sous-groupe approprié d'indice fini dans $\mathbf{U}_L$ de telle sorte qu'on puisse appliquer le Corollaire 2.2.1. On suppose que L admet r premiers réels $\mathfrak{P}_1, ..., \mathfrak{P}_r$ et s premiers complexes $\mathfrak{P}_{r+1}, ..., \mathfrak{P}_{r+s}$. Le théorème suivant sera très utile pour le calcul des quotients de Herbrand précités.

Théorème 3.4.1. *Il existe des unités $w_1, ..., w_{r+s}$ dans $\mathbf{U}_L$ en correspondance biunivoque avec les premiers infinis de L tels que :*

a. *G permute de façon cyclique les w_i correspondant au premiers infinis $\mathfrak{P}_i$ qui sont au dessus d'un premier infini P de K.*

b. *$1 = \prod w_i$ est la seule relation entre les w_i.*

c. *Le sous-groupe W engendré par les w_i est d'indice fini dans $\mathbf{U}_L$.*

Preuve. Pour plus de détails et la démonstration voir J. Janusz pages 175-176. □

Le sous-groupe W est utile dans les calculs puisqu'on peut évaluer $q(W)$. On procède comme suit : pour chaque premier infini P de K et un premier $\mathfrak{P}$ de L au dessus de P, posons $d_P = [G : D_{\mathfrak{P}}]$ et

$$A_P = \sum_1^{d_P} \mathbb{Z} u_{i,P}.$$

C'est un $\mathbb{Z}$-module libre ayant d_P générateurs sur lesquels G agit de façon cyclique. Nous avons maintenant une suite exacte :

$$0 \longrightarrow \mathbb{Z} - \frac{g}{} \rightarrow \sum_{P|\infty} A_P - \frac{h}{} \rightarrow W \longrightarrow 0,$$

où $g(z) = z \sum_i \sum_P u_{i,P}$ et h est défini en envoyant les éléments de la base $u_{i,P}$ de façon surjective sur les unités w_i correspondant aux diviseurs premiers $\mathfrak{P}_i$ de P de telle sorte que h soit un G-homomorphisme. L'exactitude est en fait assurée par (b) du théorème précédent. Nous calculons :

$$q(W)q(\mathbb{Z}) = q(\sum A_P) = \prod q(A_P).$$

L'action de G sur $\mathbb{Z}$ est triviale et cela permet de voir que $q(\mathbb{Z}) = 1/|G|$ moyennant la Proposition 2.2.1. La même proposition donne $q(A_P) = |D_{\mathfrak{P}}|^{-1}$ si $\mathfrak{P}|P$. On peut facilement calculer le groupe $D_{\mathfrak{P}}$ puisque si P est un premier réel infini non ramifié, il se décompose complètement dans L, ce qui veut dire que $D_{\mathfrak{P}} = 1$. Lorsque P est ramifié $|D_{\mathfrak{P}}| = 2$. Il suffit maintenant juste de remarquer que $q(W) = q(\mathbf{U}_L)$ pour avoir le théorème suivant.

Théorème 3.4.2. *Soit r_0 le nombre des premiers infinis de K qui se ramifient dans L. Alors :*

$$q(\mathbf{U}_L) = \frac{[L : K]}{2^{r_0}}.$$

Pour compléter le calcul de $q(L^S)$ nous avons besoin de déterminer $q(\ker(j_{\mathfrak{m}}))$.

Le groupe $\ker(j_{\mathfrak{m}})$ est un groupe abélien puisque engendré par les premiers de S. Pour chaque premier $\mathfrak{p}$ de K avec $\mathfrak{p}$ divisible par les premiers de S, posons $I_{\mathfrak{p}}$ le sous-groupe de $\ker(j_{\mathfrak{m}})$ engendré par les diviseurs premiers de $\mathfrak{p}$ dans L. On a donc :

$$\ker(j_{\mathfrak{m}}) = \prod_{\mathfrak{p}} I_{\mathfrak{p}} \quad \text{et donc} \quad q(\ker(j_{\mathfrak{m}})) = \prod q(I_{\mathfrak{p}}).$$

Soit $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ et $N_{L/K}(\mathfrak{P}_i) = P^f$. On sait que G est agit de façon transitive sur les $\mathfrak{P}_i$, et on peut alors facilement vérifier moyennant la Proposition 2.2.1 que :

a. $\ker(N_{I_{\mathfrak{p}}}) = \{\prod \mathfrak{P}_i^{a_i} \mid \sum a_i = 0\}$,

b. $\mathrm{Im}\,(\Delta_{I_{\mathfrak{p}}}) = \ker(N_{I_{\mathfrak{p}}})$,

c. $\ker(\Delta_{\ker(N_{I_{\mathfrak{p}}})}) = \langle \mathfrak{D} \rangle$, $\mathfrak{D} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$,

d. $\mathrm{Im}\,(N_{I_{\mathfrak{p}}}) = \langle \mathfrak{p}^f \rangle = \langle \mathfrak{D}^{ef} \rangle$.

Ainsi, $q(I_{\mathfrak{p}}) = 1/ef = 1/e_{\mathfrak{p}} f_{\mathfrak{p}}$, et par suite $q(\ker(j_{\mathfrak{m}})) = \left(\prod_{\mathfrak{p}|\mathfrak{m}_0} e_{\mathfrak{p}} f_{\mathfrak{p}}\right)^{-1}$, où $\mathfrak{m}_0$ est la partie finie de $\mathfrak{m}$. Finalement, en appliquant le Lemme 3.3.1 et les calculs précédents on arrive au théorème suivant.

Théorème 3.4.3. *Soit S l'ensemble des premiers finis divisant le module $\mathfrak{m}$ de K. Supposons que $\mathfrak{m}$ est divisible par tous les premiers de K qui se ramifient dans L, alors*

$$q(L^S) = \frac{[L:K]}{\prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}},$$

où le produit est pris sur tous les premiers finis ou infinis divisant $\mathfrak{m}$.

Chapitre 4

Calcul d'un indice de norme

4.1 Définition d'un indice de norme

Comme précédemment, L/K sera une extension cyclique de groupe de Galois $G = \langle\sigma\rangle$. Pour un module $\mathfrak{m}$ de K on pose :

$$a(\mathfrak{m}) = [K^* : N(L^*)K_{\mathfrak{m},1}].$$

On rappelle que

$$K_{\mathfrak{m},1} = \{\alpha \in K_{\mathfrak{m}} \mid \alpha \equiv 1 \bmod \mathfrak{m}\},$$

où

$$K_{\mathfrak{m}} = \left\{ \frac{a}{b} \mid a, b \in \mathcal{O}_K,\ a\mathcal{O}_K \text{ et } b\mathcal{O}_K \text{ relativement premiers à } \mathfrak{m}_0 \right\}$$

et $\mathfrak{m}_0$ est la partie finie du module $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.

Notre but est d'évaluer l'indice $a(\mathfrak{m})$ au moins sous la condition que $\mathfrak{m}$ est divisible par tous les premiers de K qui se ramifient dans L et de plus les diviseurs premiers finis de $\mathfrak{m}$ ont des puissances suffisamment grandes.

Lemme 4.1.1. *Soient $\mathfrak{m}$ et $\mathfrak{n}$ deux modulus de K premiers entre eux, alors*

$$a(\mathfrak{mn}) = a(\mathfrak{m})a(\mathfrak{n}).$$

Preuve. Le théorème d'approximation implique que l'application

$$\alpha \longmapsto (\alpha K_{\mathfrak{m},1}, \alpha K_{\mathfrak{n},1})$$

induit un isomorphisme

$$\frac{K^*}{K_{\mathfrak{mn},1}} \to \frac{K^*}{K_{\mathfrak{m},1}} \times \frac{K^*}{K_{\mathfrak{n},1}}.$$

Cela induit un homomorphisme

$$\frac{K^*}{K_{\mathfrak{mn},1}} \to \frac{K^*}{N(L^*)K_{\mathfrak{m},1}} \times \frac{K^*}{N(L^*)K_{\mathfrak{n},1}}$$

qui est surjectif dans le produit direct. Le lemme sera établi si on prouve que le noyau de cette application est exactement $N(L^*)K_{\mathfrak{mn},1}/K_{\mathfrak{n},1}$.

Supposons que $\alpha K_{\mathfrak{mn},1}$ est dans le noyau. Il existe alors β_1 et β_2 dans L tels que :

$$\alpha \equiv N(\beta_1) \mod \mathfrak{m}, \quad \alpha \equiv N(\beta_2) \mod \mathfrak{n}.$$

En regardant $\mathfrak{m}$ et $\mathfrak{n}$ comme des modules de L, ils restent premiers entre eux et donc il existe une solution β dans L aux congruences :

$$\beta \equiv \beta_1 \mod \mathfrak{m}, \quad \beta \equiv \beta_2 \mod \mathfrak{n}.$$

On en déduit alors que :

$$N(\beta)N(\beta_1)^{-1} \in K \cap N_{L/K}(L_{\mathfrak{m},1})$$
$$N(\beta)N(\beta_2)^{-1} \in K \cap N_{L/K}(L_{\mathfrak{n},1}).$$

Dans la suite, nous montrons que $K \cap N_{L/K}(L_{\mathfrak{m},1}) \subseteq K_{\mathfrak{m},1}$. Soit $\mathfrak{p}^t$ la puissance de l'idéal premier $\mathfrak{p}$ de K divisant $\mathfrak{m}$ et soit $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ la factorisation de $\mathfrak{p}$ dans L. Si $\gamma = a/b$ est dans L avec a et b des entiers algébriques et $\gamma \equiv 1 \mod \mathfrak{m}$, alors :

$$a \equiv b \mod (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{te}.$$

Comme le produit $\mathfrak{P}_1 \cdots \mathfrak{P}_g$ est invariant par tout $\sigma \in G(L/K)$, nous avons :

$$\sigma(a) \equiv \sigma(b) \mod (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{te}$$

et donc

$$N_{L/K}(a) \equiv N_{L/K}(b) \mod (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{te}.$$

Ces normes sont dans K, alors les congruences peuvent être lues modulo $K \cap (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{te} = \mathfrak{p}^t$. On en déduit que $N_{L/K}(a) \equiv N_{L/K}(b)$ et donc que $N_{L/K}(\gamma) \equiv 1 \mod \mathfrak{p}^t$. Comme cela se produit pour chaque diviseur de $\mathfrak{m}$, on en déduit l'inclusion désirée.

Nous avons déjà $\alpha N_{L/K}(\beta_1)^{-1} \in K_{\mathfrak{m},1}$ et $\alpha N_{L/K}(\beta_2)^{-1} \in K_{\mathfrak{n},1}$, d'où :

$$\alpha N_{L/K}(\beta)^{-1} \in K_{\mathfrak{m},1} \cap K_{\mathfrak{n},1} = K_{\mathfrak{mn},1}.$$

Ce qui est suffisant pour prouver le lemme. □

Ce lemme réduit le calcul de $a(\mathfrak{m})$ au cas $\mathfrak{m} = \mathfrak{p}^n$ pour un premier $\mathfrak{p}$ et $n \geq 1$. Le cas $\mathfrak{p}$ premier infini est facile comme on va le voir à travers ce lemme.

Lemme 4.1.2. *Si $\mathfrak{p}$ est un premier infini de K alors $a(\mathfrak{p}) = e_{\mathfrak{p}}$ l'indice de ramification.*

Preuve. Supposons $\mathfrak{m} = \mathfrak{p}$ un premier réel infini ramifié dans L. Soient $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ les premiers (complexes) de L au dessus de $\mathfrak{p}$. Alors pour $\alpha \in L^*$,

$$N_{L/K}(\alpha) = \prod_i N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\alpha).$$

Comme $L_{\mathfrak{P}_i}$ est le corps des nombres complexes et $K_{\mathfrak{p}}$ le corps des nombres réel, toutes les normes dans le côté droit sont positives. Ainsi, $N(L^*) = K_{\mathfrak{m},1}$ et $K^*/K_{\mathfrak{m},1}$ est d'ordre 2. Le lecteur peut vérifier dans tous les autres cas que $[K^* : N(L^*)K_{\mathfrak{m},1}] = 1 = e_{\mathfrak{p}}$ comme demandé. □

Dans tout le reste du paragraphe, nous travaillons avec un premier fini et $\mathfrak{m} = \mathfrak{p}^n$. On note par $\mathfrak{P}$ un premier de L divisant $\mathfrak{p}$. On note aussi par $e_\mathfrak{p}$ respectivement $f_\mathfrak{p}$ l'indice de ramification et le degré résiduel de $\mathfrak{P}$ sur $\mathfrak{p}$.

Lemme 4.1.3.

a. $[K^* : N(L^*)K_{\mathfrak{m},1}] = f_P$;

b. $a(\mathfrak{m}) = f_P[K_\mathfrak{m} : (K_\mathfrak{m} \cap N(L^*))K_{\mathfrak{m},1}]$.

Preuve. Comme $\mathfrak{m} = \mathfrak{p}^n$ alors $K_\mathfrak{m}$ n'est rien d'autre que le groupe des unités de l'anneau de valuation discrète $A_\mathfrak{p}$ le localisé en $\mathfrak{p}$. Soit π un générateur de l'idéal maximal, donc tout élément de K^* peut s'écrire sous la forme $\pi^t u$ avec $u \in K_\mathfrak{m}$.

Nous savons que $N(\mathfrak{P}) = (\pi^f)$, et les éléments dans $N(L^*)$ auront donc la forme $\pi^{tr}w$ avec $w \in K_\mathfrak{m}$. On en déduit que :

$$K^*/K_\mathfrak{m}N(L^*) \simeq \langle\pi\rangle/\langle\pi^f\rangle$$

qui est d'ordre $f = f_\mathfrak{p}$ comme exigé par (a).

Une factorisation de $a(\mathfrak{m})$ peut être obtenue à partir des indices successifs des sous-groupes de la chaîne suivante :

$$K^* \supset N(L^*)K_\mathfrak{m} \supset N(L^*)K_{\mathfrak{m},1}.$$

Le premier indice est $f_\mathfrak{p}$ grâce à (a). Pour calculer le second indice dans (b) nous devons remarquer qu'il existe un isomorphisme naturel

$$\frac{K_\mathfrak{m}}{(K_\mathfrak{m} \cap N(L^*))K_{\mathfrak{m},1}} \simeq \frac{N(L^*)K_\mathfrak{m}}{N(L^*)K_{\mathfrak{m},1}}$$

induit par l'inclusion de $K_\mathfrak{m}$ dans $N(L^*)K_\mathfrak{m}$. □

La procédure à partir de ce point est d'exprimer ce dernier groupe sus-mentionné purement en termes locaux. Pour cela, nous avons besoin de notations additionnelles. Comme d'habitude, $K_\mathfrak{p}$ et $L_\mathfrak{P}$ désignent les complétés en les premiers $\mathfrak{p}$ et $\mathfrak{P}$. Soit $\mathbf{U}_\mathfrak{p}$ le groupe des unités dans l'anneau de valuation de $K_\mathfrak{p}$ et $\mathbf{U}_\mathfrak{P}$ le groupe des unités dans l'anneau de valuation de $L_\mathfrak{P}$. Les idéaux maximaux des anneaux de valuation seront notés simplement par $\mathfrak{p}$ et $\mathfrak{P}$. Pour chaque entier positif n on pose :

$$\mathbf{U}_\mathfrak{p}^{(n)} = 1 + \mathfrak{p}^n$$

qui est l'ensemble des unités dans $\mathbf{U}_\mathfrak{p}$ congrues à 1 modulo $\mathfrak{p}^n$. Enfin, nous noterons $N_\mathfrak{p}$ la norme de $L_\mathfrak{P}$ vers $K_\mathfrak{p}$.

Lemme 4.1.4. *Pour $\mathfrak{m} = \mathfrak{p}^n$ il existe un isomorphisme*

$$\frac{K_\mathfrak{m}}{(K_\mathfrak{m} \cap N(L^*))K_{\mathfrak{m},1}} \simeq \frac{\mathbf{U}_\mathfrak{p}}{N_\mathfrak{p}(\mathbf{U}_\mathfrak{P})\mathbf{U}_\mathfrak{p}^{(n)}}.$$

Preuve. Le groupe $\mathbf{U}_\mathfrak{p}/\mathbf{U}_\mathfrak{p}^{(n)}$ est l'image des unités dans $A_\mathfrak{p} = K_\mathfrak{m}$ et donc l'application

$$v : \ \alpha \mapsto \alpha N_\mathfrak{p}(\mathbf{U}_\mathfrak{P})\mathbf{U}_\mathfrak{p}^{(n)}$$

envoie $K_{\mathfrak{m}}$ de façon surjective sur le groupe donné et le noyau contient $K_{\mathfrak{m},1}$ puisque ce dernier est l'ensemble envoyé surjectivement sur $\mathbf{U}_{\mathfrak{p}}^{(n)}$. Maintenant, supposons que α est dans le noyau. Pour un certain $\beta \in \mathbf{U}_{\mathfrak{P}}$, nous avons $\alpha N_{\mathfrak{p}}(\beta)^{-1} \in \mathbf{U}_{\mathfrak{p}}^{(n)}$. Soient alors $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ tous les premiers de L au dessus de $\mathfrak{p}$. Il existe un élément $\gamma \in L$ tel que :

$$\begin{aligned} \gamma &\equiv \beta \mod {\mathfrak{P}_1}^{ne} \\ \gamma &\equiv 1 \mod {\mathfrak{P}_j}^{ne}, \ \ j \neq 1, \ \ e = e(\mathfrak{P}/P) \end{aligned}$$

Maintenant pour $\tau \in G(L/K)$ mais $\tau \notin D_{\mathfrak{P}}$ nous avons $\tau^{-1}(\mathfrak{P}) = \mathfrak{P}_j \neq \mathfrak{P}_1$ et donc :

$$\tau(\gamma) \equiv 1 \mod {\mathfrak{P}_1}^{ne}.$$

Si les $\tau_i D_{\mathfrak{P}}$ désignent les classes à gauche modulo $D_{\mathfrak{P}}$ dans G, alors :

$$N_{L/K}(\gamma) = \prod_i \prod_{\tau \in D_{\mathfrak{P}}} \tau_i \tau(\gamma) \equiv \prod_{\tau \in D_{\mathfrak{P}}} \tau(\gamma) \equiv N_{\mathfrak{p}}(\gamma) \mod \mathfrak{P}^{ne}.$$

Par conséquent, $N_{L/K}(\gamma) \equiv N_{\mathfrak{p}}(\beta) \mod \mathfrak{P}^{ne}$ et donc $\alpha \in N(\gamma) K_{\mathfrak{m},1}$. Comme $\alpha \in K_{\mathfrak{m}}$, nous voyons que $N(\gamma) \in (K_{\mathfrak{m}} \cap N(L^*)) K_{\mathfrak{m},1}$. Nous avons déjà vu que $K_{\mathfrak{m},1}$ est dans le noyau. Il est évident que les normes de L sont envoyées dans $N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})$, ce qui termine la démonstration. □

Le calcul de $a(\mathfrak{p}^n)$ est maintenant réduit à un problème d'unités dans les complétés. Cela s'effectuera en deux étapes et chacune d'elles nécessite un certain nombre de calculs préliminaires. On doit en gros montrer que $\mathbf{U}_{\mathfrak{p}}^{(n)} \subseteq N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})$ pour n suffisamment grand. Ensuite, le problème se réduira au calcul de l'indice $[\mathbf{U}_{\mathfrak{p}} : N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})]$ qui se fera en utilisant le quotient de Herbrand $q(\mathbf{U}_{\mathfrak{P}})$.

Nous travaillons maintenant uniquement dans les corps complétés $K_{\mathfrak{p}}$ et $L_{\mathfrak{P}}$.

Considérons les séries :

$$\exp(x) = \sum_0^\infty \frac{x^n}{n!},$$

$$\log(1+x) = \sum_1^\infty \frac{(-1)^{n+1} x^n}{n!}.$$

Cela sera utilisé pour x dans $L_{\mathfrak{P}}$ et $K_{\mathfrak{p}}$. Il est nécessaire de déterminer le domaine de convergence. Posons $v_{\mathfrak{P}}$ la valuation exponentielle. Une série infinie $\sum a_n x^n$ converge dans $L_{\mathfrak{P}}$ si et seulement si $v_{\mathfrak{P}}(a_n x^n) \to \infty$ lorsque $n \to \infty$.

Soit q l'entier premier dans $\mathfrak{P}$ et posons $e_0 = v_{\mathfrak{P}}(q)$. Supposons $n! = q^r t$ avec t et q premiers entre eux. Alors :

$$r = \left[\frac{n}{q}\right] + \left[\frac{n}{q^2}\right] + \cdots < n \sum_1^\infty q^{-i} = \frac{n}{q-1}.$$

Par conséquent, $v_{\mathfrak{P}}(\frac{x^n}{n!}) = n v_{\mathfrak{P}}(x) - v_{\mathfrak{P}}(n!) > n(v_{\mathfrak{P}}(x) - e_0/(q-1))$. On en déduit que $\exp(x)$ converge si $v_{\mathfrak{P}}(x) > e_0/(q-1)$.

De façon similaire, $v_{\mathfrak{P}}(x^n/n) = n(v_{\mathfrak{P}}(x) - v_{\mathfrak{P}}(n)/n)$, d'où $\log(1+x)$ converge chaque fois que $v_{\mathfrak{P}}(x) \geq 1$. Finalement, les deux relations familières :

$$\log \exp(x) = x, \quad \exp \log(1+x) = 1+x$$

peuvent être vérifiées formellement. Nous utiliserons les propriétés simultanément.

Proposition 4.1.1. *Pour n suffisamment grand, la fonction* log *donne un isomorphisme de $\mathbf{U}_{\mathfrak{p}}^{(n)}$ vers le groupe additif $\mathfrak{p}^n$.*

Preuve. Prendre n assez grand de telle sorte que $\exp(x)$ converge pour x dans $\mathfrak{p}^n$. Par conséquent, $\exp(x) = 1+x+\cdots$ est dans $\mathbf{U}_{\mathfrak{p}}^{(n)}$, et pour $1+y$ dans $\mathbf{U}_{\mathfrak{p}}^{(n)}$, $\log(1+y) = y+\cdots$ est dans $\mathfrak{p}^{(n)}$. De plus, ce sont des homomorphismes de groupes et sont inverses l'un de l'autre. □

Proposition 4.1.2. *Soit d un entier positif. Pour n suffisamment grand, tout élément de $\mathbf{U}_{\mathfrak{p}}^{(n)}$ est la d-ème puissance d'un élément dans $\mathbf{U}_{\mathfrak{p}}$. En particulier, avec $d = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ et n suffisamment grand, $\mathbf{U}_{\mathfrak{p}}^{(n)} \subseteq N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})$.*

Preuve. Si $v_{\mathfrak{P}}(d) = k$, on prend n assez grand pour que $\exp(x)$ converge pour x dans $\mathfrak{p}^{n-e_0 k}$. Prendre ensuite tout $1+x$ dans $\mathbf{U}_{\mathfrak{p}}^{(n)}$ et poser $y = \log(1+x)$. Alors y est dans $\mathfrak{p}^n$ et y/d est dans le domaine de convergence de exp. Lorsqu'on pose $z = \exp(y/d)$, alors $z \in \mathbf{U}_P$ et $z^d = 1+x$.

Pour prouver le dernier point de la proposition concernant les normes il suffit de remarquer que pour $u \in K_{\mathfrak{p}}$, $N_{\mathfrak{p}}(u) = u^d$, et donc toutes les d-èmes puissances sont normes En particulier, $\mathbf{U}_{\mathfrak{p}}^{(n)}$ est formé entièrement de normes. □

Corollaire 4.1.1. *Pour n suffisamment grand, nous avons :*

$$a(\mathfrak{p}^n) = f_{\mathfrak{p}}[\mathbf{U}_{\mathfrak{p}} : N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})].$$

L'indice restant ici est égal à $|H^0(\mathbf{U}_{\mathfrak{P}})|$ qui est égal à $q(\mathbf{U}_{\mathfrak{P}})^{-1}|H^1(\mathbf{U}_{\mathfrak{P}})|$. Nous allons calculer toutes ces quantités.

Lemme 4.1.5. $|H^1(\mathbf{U}_{\mathfrak{P}})| = e_{\mathfrak{p}} =$ *l'indice de ramification de* $\mathfrak{p}$.

Preuve. Par le théorème 90 de Hilbert, $\ker(N_{\mathbf{U}_{\mathfrak{P}}}) = \mathbf{U}_{\mathfrak{P}} \cap \Delta(L_{\mathfrak{P}}^*)$. Soit π un générateur de l'idéal $\mathfrak{P}$ de telle sorte que tout élément x dans $L_{\mathfrak{P}}$ soit de la forme $\pi^a u$ avec $u \in \mathbf{U}_{\mathfrak{P}}$. Soit σ un générateur de $D_{\mathfrak{P}} = \mathrm{Gal}(L_{\mathfrak{P}}/K_P)$. Alors $\sigma(\pi) = \pi w$ avec $w \in \mathbf{U}_{\mathfrak{P}}$, d'où $\Delta(x) = \pi^a u/\pi^a w'$ est dans $\mathbf{U}_{\mathfrak{P}}$. Par conséquent $\ker(N_{\mathbf{U}_{\mathfrak{P}}}) = \Delta(L_{\mathfrak{P}}^*)$. Ceci nous permet d'écrire :

$$H^1(\mathbf{U}_{\mathfrak{P}}) \simeq \Delta(L_{\mathfrak{P}}^*)/\Delta(\mathbf{U}_{\mathfrak{P}}) \simeq L_{\mathfrak{P}}^*/K_P^*\mathbf{U}_{\mathfrak{P}}$$

avec le dernier isomorphisme induit par l'application surjective $x \mapsto \Delta(x)$ de $L_{\mathfrak{P}}^*$ sur $\Delta(L_{\mathfrak{P}}^*)$.

Soit π_0 un générateur de $\mathfrak{p}$ tel que $\pi_0 = \pi^e u$ pour une certaine unité u et $e = e_{\mathfrak{p}}$. Alors :

$$L_{\mathfrak{P}}^* \simeq \langle \pi \rangle \times \mathbf{U}_{\mathfrak{P}},$$

$$K_{\mathfrak{p}}^*\mathbf{U}_{\mathfrak{P}} \simeq \langle \pi^e \rangle \times \mathbf{U}_{\mathfrak{P}}$$

et le quotient est donc d'ordre $e_{\mathfrak{p}}$ comme souhaité. □

Enfin, nous arrivons au dernier terme restant.

Lemme 4.1.6. $q(\mathbf{U}_{\mathfrak{P}}) = 1$.

Preuve. Le lemme 2.2.3 et le corollaire 2.2.1 seront utilisés fréquemment.

Pour tout entier positif n, le quotient $\mathbf{U}_{\mathfrak{P}}/\mathbf{U}_{\mathfrak{P}}^{(n)}$ est fini puisque le groupe des unités de l'anneau fini $B_{\mathfrak{P}}/\mathfrak{P}^n$. Ainsi, $q(\mathbf{U}_{\mathfrak{P}}) = q(\mathbf{U}_{\mathfrak{P}}^{(n)})$.

On prend n assez grand pour que la proposition 2.3.2 puisse être appliquée. Alors la fonction log donne un isomorphisme de $\mathbf{U}_{\mathfrak{P}}^{(n)}$ avec le groupe additif $\mathfrak{P}^n$. De plus, c'est un $D_{\mathfrak{P}}$-isomorphisme, d'où $q(\mathbf{U}_{\mathfrak{P}}^{(n)}) = q(\mathfrak{P}^n)$. Ce dernier quotient n'est rien d'autre que $q(B_{\mathfrak{P}})$ car $B_{\mathfrak{P}}/\mathfrak{P}^n$ est fini.

Ensuite, on applique le théorème de la base normale. Il existe un élément α dans $B_{\mathfrak{P}}$ tel que les distinctes images sous $D_{\mathfrak{P}}$ sont linéairement indépendantes sur $K_{\mathfrak{p}}$. Cela signifie que :

$$\mathfrak{M} = \sum_{\tau \in D_{\mathfrak{P}}} B_{\mathfrak{P}} \tau(\alpha)$$

est un $B_{\mathfrak{P}}$-module libre de même rang que $B_{\mathfrak{P}}$ sur $A_{\mathfrak{p}}$. Cela force $B_{\mathfrak{P}}/\mathfrak{M}$ à être fini et donc $q(B_{\mathfrak{P}}) = q(\mathfrak{M})$. Maintenant, $\mathfrak{M}$ est un module sur lequel $D_{\mathfrak{P}}$ agit en permutant les éléments de la base. On en déduit que $q(\mathfrak{M}) = 1$ (proposition 2.2.1) car aucun élément de $D_{\mathfrak{P}}$ n'agit de façon triviale (à part l'identité). □

Nous sommes maintenant en mesure de finir le problème de départ en combinant tous les résultats de cette section.

Théorème 4.1.1. *Soit* $\mathfrak{m}$ *un module du corps* K*. Si les premiers finis divisant* $\mathfrak{m}$ *ont des puissances suffisamment grandes, alors :*

$$a(\mathfrak{m}) = [K^* : N(L^*)K_{\mathfrak{m},1}] = \prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Au cours de l'établissement de ce résultat, certaines propriétés ne manquant pas d'intérêt ont été établies pour les extensions cycliques comme la proposition suivante :

Proposition 4.1.3. *Si* $\mathfrak{p}$ *est non ramifié alors tout élément dans* $\mathbf{U}_{\mathfrak{p}}$ *est norme d'un élément de* $\mathbf{U}_{\mathfrak{P}}$.

Preuve. En combinant les deux lemmes précédents on trouve que $H^0(\mathbf{U}_{\mathfrak{P}}) = 1$, donc $\mathbf{U}_{\mathfrak{p}} = N_{\mathfrak{p}}(\mathbf{U}_{\mathfrak{P}})$. □

Proposition 4.1.4. *Le quotient* $K^*/N_{\mathfrak{p}}(L_{\mathfrak{P}}^*)$ *est d'ordre* $[L_{\mathfrak{P}} : K_P]$.

Preuve. Nous avons l'inclusion de $D_{\mathfrak{P}}$-modules $\mathbf{U}_{\mathfrak{P}} \subseteq L_{\mathfrak{P}}^*$ de quotient $\langle \overline{\pi} \rangle$; le groupe cyclique infini engendré par l'image de l'élément premier π. Nous avons aussi le fait que $\langle \overline{\pi} \rangle$ est un $D_{\mathfrak{P}}$-module avec une action triviale.

Il s'en suit que $q(\langle \overline{\pi} \rangle) = |D_{\mathfrak{P}}|^{-1}$ et donc $q(L_{\mathfrak{P}}^*) = |D_{\mathfrak{P}}|^{-1}$ car $q(\mathbf{U}_{\mathfrak{P}}) = 1$. Il suffit ensuite d'utiliser la définition de q est le théorème 90 de Hilbert pour conclure que $H^0(L_{\mathfrak{P}}^*)$ est d'ordre $|D_{\mathfrak{P}}|$. □

Chapitre 5

L'égalité fondamentale pour les extensions cycliques

Soit toujours une extension cyclique L/K de groupe de Galois $G = Gal(L/K) = \langle\sigma\rangle$. On rappelle que l'application $j_{\mathfrak{m}} : \mathbf{I_L} \to \mathbf{I_L^{\mathfrak{m}}}$ défini sur les premiers par :

$$j_{\mathfrak{m}}(\mathfrak{P}) = \begin{cases} \mathfrak{P}, & \mathfrak{P} \not| \mathfrak{m}, \\ 1, & \mathfrak{P} | \mathfrak{m}, \end{cases}$$

et que l'application $i : L^* \longrightarrow \mathbf{I_L}$ fait correspondre à un élément α de L^* l'idéal fractionnaire principal $(\alpha) = \alpha\mathcal{O}_{L^*}$ de $\mathbf{I_L}$ engendré par α.

Pour un module $\mathfrak{m}$ de K, considérons le groupe

$$\mathrm{C}^{\mathfrak{m}} = \frac{\mathbf{I}_K^{\mathfrak{m}}}{N_{L/K}(\mathbf{I}_L^{\mathfrak{m}}) i(K_{\mathfrak{m},1})},$$

qui est un groupe fini, car il est l'image par une surjection d'un groupe fini [4, Corollaire 1.6 page 141], l'ordre de ce groupe sera noté $h_{\mathfrak{m}}(L/M)$. Le but de cette section est de montrer que cet ordre est $h_{\mathfrak{m}}(L/M) = [L : K]$ sous certaines conditions sur le module $\mathfrak{m}$ qui seront donnés après.

5.1 Résultats préliminaires

Soit S l'ensemble des premiers finis divisant $\mathfrak{m}$. Dans la section 3, nous avons définit l'ensemble L^S comme étant le noyau de l'application $f_{\mathfrak{m}} : L^* \longrightarrow \mathbf{I}_L^{\mathfrak{m}}$ reliant chaque élément de L^* avec l'idéal principal qu'il engendre en négligeant toutes les puissances des premiers de S de sa factorisation. Nous avons la suite exacte suivante :

$$1 \longrightarrow L^S \longrightarrow L^* \xrightarrow{f_{\mathfrak{m}}} \mathbf{I}_L^{\mathfrak{m}} \longrightarrow V \longrightarrow 1 \tag{5.1}$$

avec V est un groupe quotient convenable mettant la suite exacte. Nous déduisons donc les deux suites exactes courtes suivantes :

$$1 \longrightarrow L^S \xrightarrow{\gamma} L^* \xrightarrow{\alpha} f_{\mathfrak{m}}(L^*) \longrightarrow 1 \tag{5.2}$$

$$1 \longrightarrow f_{\mathfrak{m}}(L^*) \xrightarrow{\beta} \mathbf{I}_L^{\mathfrak{m}} \longrightarrow V \longrightarrow 1 \tag{5.3}$$

Nous calculerons donc les ordres des groupes de cohomologie et les quotients d'Herbrand des groupes des trois suites précédentes, pour dégager l'égalité fondamentale des extensions cycliques. Nous allons procéder par étape.

Pour un homomorphisme $h : A \longrightarrow B$, notons par $\mathrm{coker}(h)$ le conoyau de l'application h qui est $\frac{B}{Im(h)}$. Posons

$$\begin{aligned} P &= \{\alpha \in K^* \mid j_{\mathfrak{m}}(\alpha) \in N(\mathbf{I}_L^{\mathfrak{m}})\}, \\ Q &= \{\alpha \in K^* \mid j_{\mathfrak{m}}(\alpha) \in N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})\}. \end{aligned}$$

Utilisant les groupes de cohomologie dans la suite (**??**) pour construire le diagramme suivant :

$$\begin{array}{ccccccccc}
 & & & & \frac{N(L^*)K_{\mathfrak{m},1}}{N(L^*)} & \xrightarrow{f_0^*} & \frac{N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})}{N(\mathbf{I}_L^{\mathfrak{m}})} & \xrightarrow{p^*} & X \longrightarrow 1 \\
 & & & & \downarrow{\scriptstyle d_5} & & \downarrow{\scriptstyle d_6} & & \downarrow{\scriptstyle d_7} \\
\ker(f_0) = \frac{P}{N(L^*)} & \longrightarrow & \frac{K^*}{N(L^*)} & \xrightarrow{f_0} & \frac{\mathbf{I}_K^{\mathfrak{m}}}{N(\mathbf{I}_L^{\mathfrak{m}})} & \xrightarrow{p} & \mathrm{coker}(f_0) & \longrightarrow & 1 \\
\downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d_2} & & \downarrow{\scriptstyle d_3} & & \downarrow{\scriptstyle d_4} & & \\
\ker(g) = \frac{Q}{N(L^*)K_{\mathfrak{m},1}} & \longrightarrow & \frac{K^*}{N(L^*)K_{\mathfrak{m},1}} & \xrightarrow{g} & \frac{\mathbf{I}_K^{\mathfrak{m}}}{N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})} & \xrightarrow{p'} & \mathrm{coker}(g) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Dans ce diagramme, X est définit comme étant le noyau de d_4, l'application f_0^* est induite par f_0 et p^* est aussi induite par p qui est la projection canonique sur le conoyau de f_0. Les applications d_5, d_6 et d_7 sont des inclusions, d_1, d_2, d_3 sont des projections naturels ; d_4 est l'unique application qui du carré un carré commutatif, c'est-à-dire $d_4(p(x)) = p'(d_3(x))$. Les deux applications horizontales sans noms sont des inclusions.

Montrons que p^* est surjective. Soit $x \in X$, alors $d_4(d_7(x)) = 0$, donc $\exists u \in \frac{\mathbf{I}_K^{\mathfrak{m}}}{N(\mathbf{I}_L^{\mathfrak{m}})}$ vérifiant $p(u) = d_7(x)$ et par commutativité nous déduisons que $p'(d_3(u)) = 0$. D'où $\exists z \in \frac{K^*}{N(L^*)}$ tel que $g(d_2(z)) = d_3(u)$, il s'en suit que $u - f_0(z) \in \ker(d_3)$ ce qui implique l'existence d'un $w \in \frac{N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})}{N(\mathbf{I}_L^{\mathfrak{m}})}$ tel que $d_6(w) = u - f_0(z)$.Donc

$$d_7(p^*(w)) = p(d_6(w)) = p(u - f_0(z)) = d_7(x),$$

or d_7 est injective, alors $p^*(w) = x$, et par suite p^* est surjective. On peut facilement remarquer que $p^* f_0^* = 0$.

Maintenant nous montrons que f_0^* est aussi surjective. Pour $\alpha \in K_{\mathfrak{m},1}$, nous avons $j_{\mathfrak{m}}(\alpha) = i(\alpha)$ car (α) n'est divisible par aucun premier divisant $\mathfrak{m}$. Donc $f_0^*(K_{\mathfrak{m},1}) = i(K_{\mathfrak{m},1})$, ce qui est largement suffisant pour dire que f_0^* est surjective. Il s'en suit que $X = 0$ et que d_4 est injective puisque $X = \ker(d_4)$.

Une poursuite simple de diagramme, et utilisant le fait que d_3 et p' sont surjectives, montre que d_4 est aussi surjective. Il s'en suit que $\mathrm{coker}(f_0) \simeq \mathrm{coker}(g)$. C'est la première assertion du lemme suivant.

Lemme 5.1.1. *Soit* $n(\mathfrak{m}) = [K_{\mathfrak{m},1} \cap i^{-1}(N(\mathbf{I}_L^{\mathfrak{m}})) : K_{\mathfrak{m},1} \cap N(L^*)]$. *Les groupes* $\ker(f_0)$ *et* $\mathrm{coker}(f_0)$ *sont finis et vérifient les assertions suivantes :*

1. $\mathrm{coker}(f_0) \simeq \mathrm{coker}(g)$.
2. $|\ker(f_0)| = |\ker(g)| n(\mathfrak{m})$.

Preuve. Le diagramme précèdent montre que d_1 est surjective, donc $|\ker(g)| = \frac{|\ker(f_0)|}{|\ker(d_1)|}$. D'autre part, $\ker(d_1)$ est la partie de $\ker(f_0)$ incluse dans $\ker(g)$, donc

$$|\ker(g)||\ker(f_0) \cap \ker(d_2)| = |\ker(f_0)|\cdot$$

Soit $xN(L^*) \in \ker(f_0) \cap \ker(d_2)$, alors $xN(L^*) = yN(L^*)$ pour un certain $y \in K_{\mathfrak{m},1}$ et $j_{\mathfrak{m}}(y) \in N(\mathbf{I}_L^{\mathfrak{m}})$. Puisque $y \in K_{\mathfrak{m},1}$, alors $j_{\mathfrak{m}}(y) = i(y)$, c'est-à-dire $y \in K_{\mathfrak{m},1} \cap i^{-1}(N(\mathbf{I}_L^{\mathfrak{m}}))$. De plus, l'égalité $yN(L^*) = y'N(L^*)$ est vraie, avec $y' \in K_{\mathfrak{m},1}$, ssi y et y' sont dans la même classe d'équivalence modulo $K_{\mathfrak{m},1} \cap N(L^*)$. Ce qui donne que $|\ker(f_0) \cap \ker(d_2)| = n(\mathfrak{m})$, d'où le résultat. □

Dans la suite, nous calculerons les ordres $|\ker(f_0)|$ et $|\mathrm{coker}(f_0)|$ en fonction de $q(L^S)$ qui est déjà calculer au moins pour certains modules $\mathfrak{m}$. Pour cela, nous aurons besoin du lemme suivant.

Lemme 5.1.2. *Soit* f *un homomorphisme définit sur un groupe abélien* A. *Soit* B *un sous groupe de* A *d'indice fini. Alors*

$$[A : B] = [f(A) : f(B)][\ker(f) : B \cap \ker(f)].$$

Preuve. Par la tour $B \subset B.\ker(f) \subset A$, on peut facilement voir que

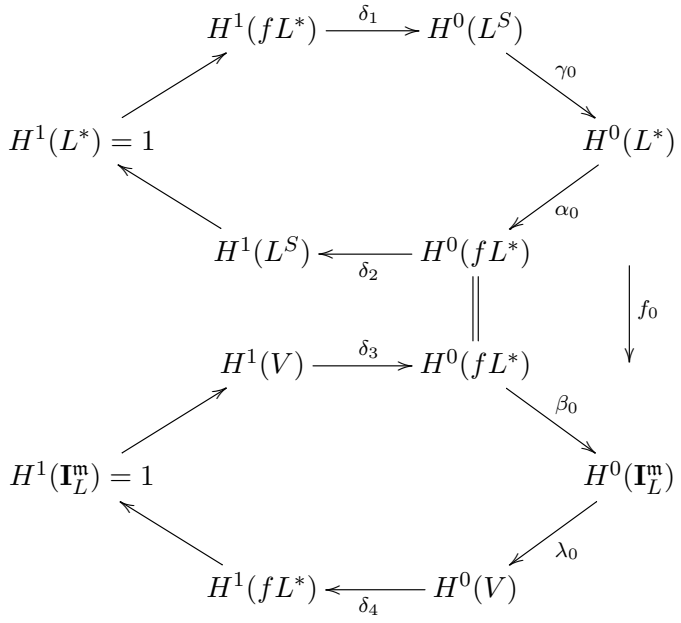
$$[A : B] = [A : B.\ker(f)][B.\ker(f) : B],$$

Par les théorèmes d'isomorphisme on a d'une part, $A/\ker(f) \simeq f(A)$ et, en considérant l'application $f : B \longrightarrow B$, $f(B) \simeq B/B \cap \ker(f) \simeq B.\ker(f)/\ker(f)$, alors

$$f(A)/f(B) \simeq (A/\ker(f))/(B.\ker(f)/\ker(f)) \simeq A/B.\ker(f),$$

d'autre part, $B.\ker(f)/B \simeq \ker(f)/B \cap \ker(f)$. Donc $[A : B.\ker(f)] = [f(A) : f(B)]$ et $[B.\ker(f) : B] = [\ker(f) : B \cap \ker(f)]$. D'où le lemme. □

Pour continuer, nous considérons les hexagones exactes suivantes dérivées des suites exactes (**??**) et (**??**). Notons que $H_1(L^*) = 1$ et $H^1(\mathbf{I}_L^{\mathfrak{m}}) = 1$ (voir Proposition 3.2.1). Pour simplification nous noterons $f = f_{\mathfrak{m}}$.



Lemme 5.1.3. 1. $\operatorname{coker}(f_0) = \dfrac{|H^0(V)|}{|H^1(f(L^*))|}\dfrac{|H^1(L^S)|}{[\ker(\beta_0) :\ \ker(\beta_0)\cap\ \operatorname{img}(\alpha_0)]}$,

2. $\ker(f_0) = |\ker(\beta_0)\cap\ \operatorname{img}(\alpha_0)|\dfrac{|H^0(L^S)|}{H^1(f(L^*))}$.

Preuve. L'exactitude des hexagones et la relation $f_0=\beta_0\alpha_0$ seront utilisés sans commentaire. Nous avons

$$|\operatorname{coker}(f_0)| = [H^0(\mathbf{I}_L^{\mathfrak{m}}) :\ \operatorname{img}(\beta_0\alpha_0)] = [H^0(\mathbf{I}_L^{\mathfrak{m}}) :\ \operatorname{img}(\beta_0)][\operatorname{img}(\beta_0) :\ \operatorname{img}(\beta_0\alpha_0)].$$

Appliquons maintenant le Lemme 5.1.2, pour $A=H^0(L^*)$ et $B=\operatorname{img}(\alpha_0)$, nous obtenons

$$[H^0(f(L^*)) :\ \operatorname{img}(\alpha_0)] = [\operatorname{img}(\beta_0) :\ \operatorname{img}(\beta_0\alpha_0)][\ker(\beta_0) :\ \ker(\beta_0)\cap\operatorname{img}(\alpha_0)].$$

Or $[H^0(f(L^*)) :\ \operatorname{img}(\alpha_0)] = |\operatorname{coker}(\alpha_0)|$ qui est égale à $|\operatorname{img}(\delta_2)| = |H^1(L^S)|$ et $[H^0(\mathbf{I}_L^{\mathfrak{m}}) :\ \operatorname{img}(\alpha_0)] = |\operatorname{coker}(\beta_0)|$ qui est égale à $|\operatorname{img}(\lambda_0)|$. De plus on a la relation

$$|H^0(V)| = |\operatorname{img}(\lambda_0)||\operatorname{img}(\delta_4)| = |\operatorname{img}(\lambda_0)||H^1(f(L^*))|.$$

Combinons ces résultats pour déduire le premier résultat.

Remarque 5.1.1. Notons que dans ce résultat, on peut remplacer $\ker(\beta_0)$ par $\operatorname{img}(\delta_3)$, et par suite $|\ker(\beta_0)| = |H^1(V)|$.

Montrons la deuxième assertion, pour cela rappelons d'abord que si

$$A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C$$

sont deux morphismes de groupes, alors $\ker(g\circ f)/\ker(f) \simeq \mathrm{img}(f)\cap\ker(g)$ (vous pouvez par exemple considérer le morphisme $h : \ker(g\circ f) \longrightarrow \mathrm{img}(f)\cap\ker(g);\ x \longmapsto f(x)$). Donc

$$\begin{aligned} |\ker(f_0)| &= |\ker(\beta_0\alpha_0)| = |\ker(\beta_0)\cap\mathrm{img}(\alpha_0)||\ker(\alpha_0)| \\ &= |\ker(\beta_0)\cap\mathrm{img}(\alpha_0)||\mathrm{img}(\gamma_0)| \\ &= |\ker(\beta_0)\cap\mathrm{img}(\alpha_0)|\frac{|H^0(L^S)|}{|H^1(f(L^*))|}. \end{aligned}$$

□

Lemme 5.1.4. *Le quotient d'Herbrand de L^S est donné par : $q(L^S) = \dfrac{|\mathrm{coker}(f_0)|}{|\ker(f_0)|}$.*

Preuve. Par le Lemme 5.1.3, on a :

$$\begin{aligned} \frac{|\mathrm{coker}(f_0)|}{|\ker(f_0)|} &= \frac{\dfrac{|H^0(V)|}{|H^1(f(L^*))|}\dfrac{|H^1(L^S)|}{[\ker(\beta_0):\ \ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)]}}{|\ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)|\dfrac{|H^0(L^S)|}{H^1(f(L^*))}} \\ &= \frac{q(L^S)|H^0(V)|}{[\ker(\beta_0):\ \ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)]|\ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)|} \\ &= \frac{q(L^S)|H^0(V)|}{\dfrac{|\ker(\beta_0)|}{|\ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)|}|\ker(\beta_0)\cap\ \mathrm{img}(\alpha_0)|} \\ &= \frac{q(L^S)|H^0(V)|}{|\ker(\beta_0)|} \\ &= \frac{q(L^S)}{q(V)} \qquad \text{car } |\ker(\beta_0)| = |H^1(V)|. \end{aligned}$$

Or V est un groupe fini car il est l'image homomorphique du groupe de classes de L. Donc $q(V) = 1$, d'où le résultat cherché. □

5.2 L'égalité fondamentale

Nous commençons par calculer l'ordre de $\mathrm{C}^{\mathfrak{m}}$ en fonction du noyau et du conoyau de l'application g, puis en fonction de $\mathrm{coker}(f_0)$ et de $\ker(f_0)$. Soit alors la suite suivante extraite du diagramme précédent

$$1 \longrightarrow\ \ker(g)\ \longrightarrow\ \frac{K^*}{N(L^*)K_{\mathfrak{m},1}} \xrightarrow{\ g\ } \mathrm{C}^{\mathfrak{m}} = \frac{\mathbf{I}_K^{\mathfrak{m}}}{N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})} \xrightarrow{\ p'\ } \mathrm{coker}(g)\ \longrightarrow 1$$

Nous avons, par le Théorème 4.1.1, que $a(\mathfrak{m}) = [K^* : N(L^*)K_{\mathfrak{m},1}] = \prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}}f_{\mathfrak{p}}$ sous la condition que les diviseurs premiers de $\mathfrak{m}$ ont des exposants suffisamment grands. Nous utiliserons ce nombre sous la même condition.

Lemme 5.2.1. *L'ordre de $\mathrm{C}^{\mathfrak{m}}$ est donné par $|\mathrm{C}^{\mathfrak{m}}| = |\mathrm{img}(g)||\mathrm{coker}(g)| = a(\mathfrak{m})\frac{|\mathrm{coker}(g)|}{|\ker(g)|}$*

Preuve. Il suffit d'utiliser l'exactitude de la suite précédente. □

Lemme 5.2.2. *L'ordre de* $\mathrm{C}^{\mathfrak{m}}$ *est donné aussi par*

$$h_{\mathfrak{m}}(L/K) = |\mathrm{C}^{\mathfrak{m}}| = a(\mathfrak{m})n(\mathfrak{m})\frac{|\mathrm{coker}(f_0)|}{|\ker(f_0)|} = a(\mathfrak{m})n(\mathfrak{m})q(L^S)\cdot$$

Preuve. Il suffit d'appliquer les Lemmes 5.1.1, 5.1.4 et 5.2.1. □

Maintenant nous pouvez énoncer le théorème principal de cette section.

Théorème 5.2.1 (**L'égalité fondamentale des extensions cycliques).** *Soit* L/K *une extension cyclique de corps de nombres, et soit* $\mathfrak{m}$ *un module de* K *divisible par tous les premiers ramifiés dans* L/K *avec des puissances suffisamment grandes, alors*

$$h_{\mathfrak{m}}(L/K) = |\mathrm{C}^{\mathfrak{m}}| = [L : K]\cdot$$

Preuve. Par le Lemme 5.2.2, on a $h_{\mathfrak{m}}(L/K) = |\mathrm{C}^{\mathfrak{m}}| = a(\mathfrak{m})n(\mathfrak{m})q(L^S)$. De plus, les suppositions faites sur $\mathfrak{m}$ impliquent que $a(\mathfrak{m}) = \prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}}f_{\mathfrak{p}}$ (Théorème 4.1.1) et que $q(L^S) = \dfrac{[L : K]}{\prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}}f_{\mathfrak{p}}}$ (Théorème 3.4.3). Donc $h_{\mathfrak{m}}(L/K) = |\mathrm{C}^{\mathfrak{m}}| = n(\mathfrak{m})[L : K]$. La première inégalité affirme que $h_{\mathfrak{m}}(L/K) \leq [L : K]$, on tire donc que $h_{\mathfrak{m}}(L/K) = |\mathrm{C}^{\mathfrak{m}}| = [L : K]$ et que $n(\mathfrak{m}) = 1$. □

Le résultat de ce théorème sera généralisé à n'importe quelle extension abélienne.
Comme $n(\mathfrak{m}) = [K_{\mathfrak{m},1} \cap i^{-1}(N(\mathbf{I}_L^{\mathfrak{m}})) : K_{\mathfrak{m},1} \cap N(L^*)]$, alors on a le corollaire suivant.

Corollaire 5.2.1. *Avec les même hypothèses que le théorème* 5.2.1*, on a :*

$$K_{\mathfrak{m},1} \cap i^{-1}(N(\mathbf{I}_L^{\mathfrak{m}})) = K_{\mathfrak{m},1} \cap N(L^*).$$

5.3 Théorème de la norme de Hasse

Le Corollaire 5.2.1 affirme que tout élément de $K_{\mathfrak{m},1}$, s'il engendre un idéal qui est norme d'un idéal de L, alors ce générateur est aussi norme. Résultat qui permet d'établir le théorème de Hasse ci-dessous. Donnons d'abord la définition suivante.

Définition 5.3.1. Un élément $\alpha \in K$ est dit norme localement en un premier $\mathfrak{p}$ de K si pour un certain premier $\mathfrak{P}$ de L au dessus de $\mathfrak{p}$, α est norme dans l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Théorème 5.3.1 (**Théorème de la norme de Hasse).** *Soit* L/K *une extension cyclique. Un élément de* K *est norme dans* L/K *si et seulement s'il est norme localement en tout premier de* K*.*

Preuve. C'est un calcule élémentaire pour savoir que si $a = N_{L/K}(b) \in K$ est norme d'un élément b de L, alors il est norme localement en tout premier $\mathfrak{p}$ de K, i.e. $a = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\gamma)$, où

$\gamma \in L_{\mathfrak{P}}$. Il suffit de prendre $\gamma = \Pi\tau_i(b)$, τ_i parcours un ensemble des classes d'équivalences du groupe de décomposition $G_{\mathfrak{P}}$.

La preuve de l'implication réciproque repose sur le théorème d'approximation. Soit $\alpha \in K$, avec α norme local dans l'extension en tout premier de K. Dans le but de montrer que α est norme globale dans L/K, c'est-à-dire il existe $\theta \in L$ tel que $N(\theta) = \alpha$, nous allons montrer que l'idéal fractionnaire (α) est norme puis par utilisation du théorème d'approximation et le fait que $n(\mathfrak{m}) = 1$, on tire que α est lui aussi norme dans L/K.

Soit $\mathfrak{p}^a$ la $\mathfrak{p}$-partie de (α), i.e. la plus grande puissance de $\mathfrak{p}$ dans la factorisation de (α), où $\mathfrak{p}$ est un premier de K, désignons par $\mathfrak{P}$ un premier de L au dessus de $\mathfrak{p}$. Soit $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$, alors $\mathfrak{p}^a$ est norme d'un idéal de L ssi f divise a puisque L/K est une extension galoisienne et tous les premiers de L au dessus de $\mathfrak{p}$ ont la même norme $\mathfrak{p}^f$. Vérifions que cette condition est valable pour (α). Soit $\beta \in L_{\mathfrak{P}}$ un élément satisfaisant $N_{\mathfrak{p}}(\beta) = \alpha$, et soient aussi $(\beta)_{\mathfrak{P}}$ l'idéal fractionnaire de $L_{\mathfrak{P}}$ engendré par β et $(\alpha)_{\mathfrak{p}}$ l'idéal fractionnaire de $K_{\mathfrak{p}}$ engendré par α). Alors $(\beta)_{\mathfrak{P}} = \mathfrak{P}^t$ pour un certain entier t et

$$(N_{\mathfrak{p}}(\beta))_{\mathfrak{p}} = N_{\mathfrak{p}}(\mathfrak{P}^t) = \mathfrak{p}^{ft} = (\alpha)_{\mathfrak{p}} = \mathfrak{p}^a.$$

Ce qui implique que f divise a et que (α) est norme d'un idéal de L.

Soit maintenant un module $\mathfrak{m}$ de K tel que $n(\mathfrak{m}) = 1$, ce module $\mathfrak{m}$ existe par le Corollaire 5.2.1. Posons $\mathfrak{m} = \prod \mathfrak{p}_i^{b_i}$, et notons, pour chaque i, par $\mathfrak{P}_i$ un idéal de L au dessus de $\mathfrak{p}_i$ et par $e_i = e(\mathfrak{P}_i/\mathfrak{p}_i)$ l'indice de ramification.

Il existe un élément $\beta_i \in L_{\mathfrak{P}_i}$ avec $\alpha = N_{\mathfrak{p}_i(\beta_i)}$ où $N_{\mathfrak{p}_i} = N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}_i}}$. Utilisant le théorème d'approximation dans L pour obtenir un élément $\gamma \in L$ satisfaisant pour chaque i

$$\begin{aligned} &\gamma \equiv^* \beta_i \pmod{\mathfrak{P}_i^{b_i e_i}} \\ &\gamma \equiv^* 1 \pmod{\mathfrak{P}^{b_i e_i}}, \quad \text{if } \mathfrak{P}|\mathfrak{p}, \mathfrak{P} \neq \mathfrak{P}_i. \end{aligned}$$

Pour $\sigma \in G(L/K)$ mais $\sigma \notin G(\mathfrak{P}_i)$, on peut avoir

$$\gamma \equiv^* 1 \pmod{\sigma^{-1}(\mathfrak{P}^{b_i e_i})} \text{ et } \sigma(\gamma) \equiv^* 1 \pmod{\mathfrak{P}^{b_i e_i}}.$$

Ceci implique que

$$N_{L/K}(\gamma) = \prod_{\tau_j} \prod_{\sigma \in G(\mathfrak{P}_i)} \tau_j\sigma(\gamma) \equiv^* \prod_{\sigma \in G(\mathfrak{P}_i)} \sigma(\gamma) = N_{\mathfrak{p}}(\gamma) \equiv^* N_{\mathfrak{P}}(\beta_i) \pmod{\mathfrak{P}_i^{b_i e_i}}.$$

Après combinaison ceci pour tous i, on voit facilement que

$$\alpha \equiv^* N_{L/K}(\gamma) \pmod{\mathfrak{m}},$$

par suite

$$\alpha N_{L/K}(\gamma)^{-1} \in K_{\mathfrak{m},1}.$$

Comme nous avons vu que $i(\alpha)$ est une norme d'un idéal, alors nous déduisons que

$$\alpha N_{L/K}(\gamma)^{-1} \in K_{\mathfrak{m},1} \cap i^{-1}(N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})).$$

Par le choix de $\mathfrak{m}$ tel que $n(\mathfrak{m}) = 1$, alors le groupe du droite est $K_{\mathfrak{m},1} \cap (N_{L/K}(L^*))$. Ce qui implique que $c = \alpha N_{L/K}(\gamma)^{-1} \in N(L^*)$, c-à-d, $c = \alpha N_{L/K}(\gamma)^{-1}$ est norme, et d'où α est aussi norme. □

Remarque 5.3.1. Le théorème de la norme de Hasse est parfois donné sous le nom du «principe local-global».

Notons aussi que ce résultat n'est pas valable dans une extension quelconque même dans le cas abélien, voir un contre exemple détaillé dans [6, page 360], un antre contre exemple est donné dans [4, page 190].

Chapitre 6

Théorème de Réciprocité

Pour une extension cyclique L/K et pour un module convenable $\mathfrak{m}$ de K, nous avons vu que l'indice du sous groupe $N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$ dans $\mathbf{I}_K^{\mathfrak{m}}$ est $[L : K]$. D'autre part, l'application d'Artin $\varphi_{L/K}$ envoie surjectivement $\mathbf{I}_K^{\mathfrak{m}}$ sur $Gal(L/K)$ et que $\ker(\varphi_{L/K})$ est d'indice $[L : K]$ dans $\mathbf{I}_K^{\mathfrak{m}}$. Donc les deux sous groupes $N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$ et $\ker(\varphi_{L/K})$ ont même indice dans $\mathbf{I}_K^{\mathfrak{m}}$. Notre but est de prouver que ces deux sous groupes sont identiques, une fois ce résultat établie, nous pouvons le généraliser aux extensions abéliennes.

Rappelons que l'application d'Artin est définie sur le groupe d'idéaux $\mathbf{I}_K^{\mathfrak{m}}$ tant que $\mathfrak{m}$ est divisible par tous les premiers de K ramifiés dans L. Donc $\ker(\varphi_{L/K}) \subset \mathbf{I}_K^{\mathfrak{m}}$.

6.1 Loi de réciprocité

Définition 6.1.1. Soit L/K une extension galoisienne de corps de nombres et soit $\mathfrak{m}$ un module de K. On dit qu'un triplet $(L, K, \mathfrak{m})$ vérifie la loi de réciprocité ou que la loi de réciprocité a lieu pour le triplet $(L, K, \mathfrak{m})$ si $Gal(L/K)$ est abélien et $\mathfrak{m}$ est un module de K satisfaisant $i(K_{\mathfrak{m},1}) \subset \ker(\varphi_{L/K})$.

Lemme 6.1.1. *Si le module $\mathfrak{m}$ de K est divisible par tous les premiers de K ramifiés dans L et si la loi de réciprocité a lieu pour le triplet $(L, K, \mathfrak{m})$, alors*

$$\ker(\varphi_{L/K}) = N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}).$$

Preuve. Par [4, Corollaire 3.2, Ch.III], on sait que $N(\mathbf{I}_L^{\mathfrak{m}}) \subset \ker(\varphi_{L/K})$, alors la loi de réciprocité implique que

$$N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1}) \subset \ker(\varphi_{L/K}) \subset \mathbf{I}_K^{\mathfrak{m}}.$$

D'autre part, la première inégalité (voir [4, Théorème 5.6, Ch. 4]) implique que l'indice de $N(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$ dans $\mathbf{I}_K^{\mathfrak{m}}$ est au plus égale à $[L : K]$, quant à l'indice de $\ker(\varphi_{L/K})$ dans $\mathbf{I}_K^{\mathfrak{m}}$ est exactement $[L : K]$. D'où l'égalité des deux sous groupes en question. □

Il existe plusieurs situations importantes où la loi de réciprocité est vérifiée, citons quelques cas :

Exemples 6.1.1 (Exemples des triplets qui vérifient la loi de réciprocité).

1. Si θ_m est une racine primitive m-ième et $\mathfrak{m}$ est le module $(m)p_\infty$ pour $\mathbb{Q}$, alors la loi de réciprocité a lieu pour le triplet $(\mathbb{Q}(\theta_m), \mathbb{Q}, \mathfrak{m})$, voir [4, Proposition 3.3, Ch. 3].
2. Si la loi de réciprocité est satisfaite pour un triplet $(L, K, \mathfrak{m})$ et E est une extension finie de K, alors la loi de réciprocité a lieu pour le triplet $(LE, E, \mathfrak{m})$, où $\mathfrak{m}$ est le module étendu à E.
   Soit $\alpha \in E_{\mathfrak{m},1}$, alors $N_{E/K}(\alpha) \in K_{\mathfrak{m},1}$. Donc par [4, Proposition 3.1, Ch. 3], on a $\varphi_{EL/E} = \varphi_{L/K} \circ N_{E/K}$, par suite
   $$\varphi_{EL/E}(\alpha) = \varphi_{L/K}(N_{E/K}(\alpha)) \in \varphi_{L/K}(i(K_{\mathfrak{m},1})) = 1.$$
   Ainsi $i(E_{\mathfrak{m},1}) \subset \ker(\varphi_{EL/E})$.
3. Si la loi de réciprocité est satisfaite pour un triplet $(L, K, \mathfrak{m})$ et si $\mathfrak{n}$ est un autre module de K, alors la loi de réciprocité est satisfaite pour le triplet $(L, K, \mathfrak{mn})$. Ceci est immédiat puisque $K_{\mathfrak{mn},1} \subset K_{\mathfrak{m},1}$.
4. Si θ_n est une racine primitive n-ième et $\mathfrak{m}$ un module de K divisible par $(n)p_\infty$ (module de $\mathbb{Q}$ regardé comme module de K par extension des scalaires), alors la loi de réciprocité a lieu pour le triplet $(K(\theta_n), K, \mathfrak{m})$. C'est une combinaison des trois dernières affirmations.
5. Si θ_n est une racine primitive n-ième, $\mathfrak{m}$ un module de K divisible par $(n)p_\infty$ et $K \subset E \subset K(\theta_n)$, alors la loi de réciprocité a lieu pour le triplet $(E, K, \mathfrak{m})$.
   Par la propriété de l'automorphisme de Frobenius donné par [4, Propriété 2.3, Ch. 3], on a $\varphi_{E/K} = \mathbf{res}\varphi_{K(\theta_n)/K}$, avec **res** désigne la restriction des automorphismes de $K(\theta_n)$ à E. Si $i(E_{\mathfrak{m},1} \subset \ker(\varphi_{K(\theta_n)/K})$, alors aussi $i(E_{\mathfrak{m},1} \subset \ker(\varphi_{E/K})$, par suite la loi a lieu pour le triplet $(E, K, \mathfrak{m})$.

Définition 6.1.2. Si θ_n est une racine de l'unité, alors l'extension $K(\theta_n)$ est dite extension cyclotomique de K. De même le corps $\mathbb{Q}(\theta_n)$ est dit corps cyclotomique.

Les extensions cyclotomiques jouent un rôle crucial dans la démonstration de la loi de réciprocité d'Artin. Nous aurons besoin de la construction des corps cyclotomiques ayant des propriétés convenables. Nous commençons par quelques lemmes techniques.

Lemme 6.1.2. *Soient a et r des entiers naturels ≥ 2 et q un entier premier. Alors il existe un premier p tel que a soit d'ordre q^r modulo p. Le lemme exprime que*

$$a^{q^r} \equiv 1 \pmod{p}.$$

Preuve. Soit le polynôme suivant :

$$g(X) = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + X + 1,$$

En posant $X^q = (Y+1)^q$, où $Y = X - 1$, on montre par la formule du binôme de Newton que

$$g(X) = \frac{\sum_{k=0}^{q} \mathrm{C}_q^k Y^k - 1}{Y} = \sum_{k=1}^{q} \mathrm{C}_q^k Y^{k-1} = \sum_{k=1}^{q} \mathrm{C}_q^k (X-1)^{k-1}.$$

Donc

$$\begin{aligned} g(X) &= X^{q-1} + X^{q-2} + \cdots + X + 1 \\ &= (X-1)^{q-1} + \mathbb{C}_q^{q-2}(X-1)^{q-3} + \cdots + \mathbb{C}_q^k(X-1)^{k-1} + \cdots + X - 1 + q. \end{aligned} \tag{6.1}$$

Notons que pour tout entier $n \geq 2$, $g(n) \geq 3$, alors $g(n)$ admet un diviseur premier. Désignons par p un diviseur premier de $g = g(a^{q^{r-1}})$.
Si p ne divise le dénominateur $a^{q^{r-1}} - 1$, alors p doit être le dernier entier satisfaisant

$$a^{q^r} \equiv 1 \pmod{p}.$$

Alors ce choix de ce premier convient.
Supposons que p divise $a^{q^{r-1}} - 1$, alors, par (**??**) et en on prenant $X = a^{q^{r-1}}$, on voit que $p = q$. Nous devons démontrer que g n'est pas une puissance de q, alors un autre choix de p peut être couvert par le premier cas.

Supposons que $q > 2$, alors chacun des termes suivants

$$(X-1)^{q-1}, \qquad \mathbb{C}_q^k(X-1)^{k-1};\ k \neq 1$$

est divisible par q^2 puisque q divise les coefficients binomiaux. Il s'ensuit par l'équation (**??**) que q^2 ne divise pas g, et comme aussi $a \geq 2$, alors $q \neq g$. D'où un autre choix convenable de p peut être fait.

Finalement, supposons que $q = 2$, alors

$$g = (a^{2^{r-1}} - 1) + 2 = a^{2^{r-1}} + 1.$$

IL est nécessaire de montrer que ceci n'est pas une puissance de 2. Clairement a ne peut pas être pair si g est une puissance de 2. Mais avec $a = 2k + 1$ impair, on voit que

$$g = a^{2^{r-1}} + 1 = (2k+1)^{2^{r-1}} + 1 \equiv 2 \pmod{4}.$$

Cependant $g \neq 2$ puisque $r - 1 \geq 1$ et par suite g n'est pas une puissance de 2. Donc tous les cas sont testés, d'où le lemme. □

Remarque 6.1.1.
- Deux éléments a et b d'un groupe abélien sont dits independents si $\langle a \rangle \cap \langle b \rangle = 1$.
- Deux entiers m et n premiers avec q sont dits independents modulo q s'ils sont independents comme éléments du groupe multiplicatif des entiers modulo q.

Lemme 6.1.3. *Soit $n = q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}$ la factorisation entière de n en nombres premiers distincts q_i, et soit un entier $a \geq 2$, alors il existe une infinité de nombres entiers m libres de carrés de la forme $m = p_1 p_2 \cdots p_s p'_1 p'_2 \cdots p'_s$ tels que l'ordre de a modulo m soit divisible par n. Il existe également un nombre entier b dont l'ordre modulo m est divisible par n et tel que a et b sont independents mod m (c-à-d, dans $(\mathbb{Z}/m\mathbb{Z})^\times$, on a $\langle a \rangle \cap \langle b \rangle = \{1\}$). De plus, le plus petit premier divisant m peut être choisi arbitrairement grand.*

Preuve. La démonstration est technique est repose sur le lemme précédent. □

Soit L/K une extension abélinne de corps den nombres. Nous essayerons maintenant de traduire les deux lemmes précédents en résultats des extensions cyclotomiques. Pour cela donnons un petit rappel sur les extensions cyclotomiques.

Remarques 6.1.1. Soit ζ une racine primitive n-ième de l'unité, $n \in \mathbb{N}^*$, donc ζ est d'ordre n, et elle est aussi une racine du n-ième polynôme cyclotomique Φ_n défini par

$$\Phi_n(X) = \prod_{0 \leq k < n,\ k \wedge n = 1} \left(X - e^{\frac{2ik\pi}{n}} \right),$$

où $k \wedge n = 1$ signifie que k et n sont premiers entre eux.

1. Si n divise un entier $m \in \mathbb{N}$, alors le n-ième corps cyclotomique $\mathbb{Q}(\zeta)$ est un sous-corps du m-ième.
2. L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est de degré $\varphi(n)$, où φ désigne la fonction indicatrice d'Euler.
3. L'extension cyclotomique est aussi le corps de décomposition du polynôme ϕ_n. Elle est donc galoisienne. Cela signifie que le plus petit corps contenant une racine du polynôme contient aussi toutes les racines du polynôme. Dire que ce corps est une extension galoisienne signifie deux choses : d'une part, les polynômes minimaux de ce corps n'ont pas de racines multiples (ce qui est toujours vrai pour les extensions sur les nombres rationnels) ; et d'autre part, tous les morphismes de ce corps dans les nombres complexes ont pour image le corps lui-même. Ce sont donc des automorphismes.
4. Cette extension est abélienne. En effet, son groupe de Galois (le groupe de ses automorphismes) est abélien, car isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 6.1.1. *Soit L/K une extension abélienne de corps den nombres de dimension $n = [L : K]$ et soit s un entier positif. Soit $\mathfrak{p}$ un premier de K non ramifié dans L. Alors il existe un entier positif m relativement premier à s et à $\mathfrak{p}$ vérifiant les assertions suivantes :*

1. *si θ_n est une racine primitive n-ième de l'unité et $E = K(\theta_n)$, alors l'ordre de $\varphi_{E/K}(\mathfrak{p})$ est divisible par n,*
2. *$L \cap E = K$,*
3. *il existe un automorphisme $\tau \in \mathrm{Gal}(E/K)$ dont l'ordre est divisible par n et que le groupe d'intersection $\langle \tau \rangle \cap \langle \varphi_{E/K}(\mathfrak{p}) \rangle = \{1\}$.*

Preuve. Posons $a = N_{K/\mathbb{Q}}(\mathfrak{p})$ et utilisant le Lemme 6.1.3. L'extension L possède un nombre fini de sous-extensions contenant K, il existe donc une racine M-ième de l'unité, θ_M, telle que $\mathbb{Q}(\theta_M)$ contient toutes les sous-extensions cyclotomiques contenues dans L. Dans le Lemme 6.1.2, on fait un choix de m de telle sorte que tous les diviseurs premiers de m soient supérieurs à Ms. Donc

$$\mathbb{Q}(\theta_M) \cap \mathbb{Q}(\theta_m) = \mathbb{Q} \quad \text{et donc } L \cap \mathbb{Q}(\theta_m) = \mathbb{Q}.$$

En prenant $E = K(\theta_m)$, alors l'assertion 2 est satisfaite.

Soit $\sigma = \varphi_{E/K}(\mathfrak{p})$, alors les propriétés définissant l'automorphisme de Frobenius assure que :

$$\sigma(\theta_m) = \theta_m^{N_{K/\mathbb{Q}}(\mathfrak{p})} = \theta_n^a,$$

par suite l'assertion 1 est vérifiée. Enfin, en prenant b comme dans le Lemme 6.1.3, l'automorphisme $\tau(\theta_m) = \theta_m^n$ de $\mathbb{Q}(\theta_m)$ admet un ordre divisible par $n$et il est independent avec σ. Comme $K \cap \mathbb{Q}(\theta_m) = \mathbb{Q}$, alors l'automorphisme se prolonge à un élément de $\mathrm{Gal}(E/K)$ avec le même ordre ; d'où l'assertion 3 est satisfaite, ce qui complete la preuve de la proposition. □

Nous arrivons maintenant au lemme technique suivant qui est nécessaire pour la démonstration du théorème de réciprocité.

Lemme 6.1.4 (**Lemme d'Artin**). *Soient L/K une extension cyclique de corps den nombres, s un entier positif et $\mathfrak{p}$ un premier de K non ramifié dans L. Alors il existe un entier positif m et une extension F de K satisfaisants les conditions suivantes :*

1. $L \cap F = K$,
2. $L \cap K(\theta_m) = K$, *où θ_m est une racine primitive m-ième de l'unité,*
3. $L(\theta_m) = F(\theta_m)$,
4. $\mathfrak{p}$ *se décompose complètement dans F.*

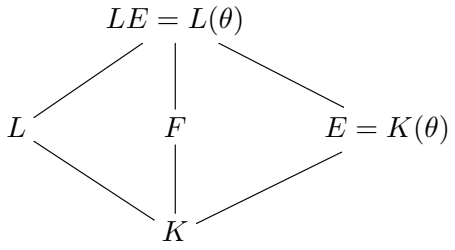
Preuve. Choisissons un entier positif m et une racine primitive m-ième de l'unité θ_m comme dans la Proposition précédente 6.1.1. Posons $\theta = \theta_m$ et $E = K(\theta)$, alors $L(\theta) = LE$ et $L \cap E = K$, d'où la deuxième assertion est vérifiée, et $\mathrm{Gal}(L(\theta)/K)$ admet la structure suivante :

$$\mathrm{Gal}(L(\theta)/K) = \mathrm{Gal}(L/K) \times \mathrm{Gal}(E/K).$$

Soit σ un générateur de $\mathrm{Gal}(L/K)$ et τ un élément choisi pour satisfaire la troisième assertion de la Proposition 6.1.1, c-à-d τ et $\varphi_{E/K}(\mathfrak{p})$ sont independents. Soit H le sous groupe engendré par

$$\sigma \times \tau \text{ et } \varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p}),$$

désignons par F le sous-corps de LE laissé fixe par H.



Par [4, Propriété 2.4], on sait que l'automorphisme de Frobenius vérifie la relation suivante :

$$\varphi_{LE/K}(\mathfrak{p}) = \varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p})$$

cet élément engendre le groupe de décomposition dans $\mathrm{Gal}(LE/K)$ d'un premier de LE au dessus de $\mathfrak{p}$, donc ce groupe est inclus dans H. L'automorphisme de Frobenius de $\mathfrak{p}$ pour l'extension F/K est l'identité puisque F est le corps fixe par H et l'automorphisme de Frobenius est donné par

$$\mathbf{res_F}\varphi_{LE/K}(\mathfrak{p}) = 1.$$

Ce qui implique que $\mathfrak{p}$ se décompose complètement dans F, ceci prouve la quatrième assertion.

Montrons que $F(\theta) = FE$ est le corps fixé par $H \cap Gal(L/K) \times 1$. Pour cela, nous allons montrer que si $(\rho \times \tau)^\mu(\varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p}))^\nu \in Gal(L/K) \times 1$, où μ et ν sont deux entiers, alors $(\rho \times \tau)^\mu(\varphi_{L/K}(\mathfrak{p}) \times \varphi_{E/K}(\mathfrak{p}))^\nu$ est l'identité. Comme $\langle\tau\rangle \cap \langle\varphi_{E/K}(\mathfrak{p})\rangle = \{1\}$, alors $\tau^\mu = 1$, ce qui montre que de plus que n divise μ, par suite $\sigma^\mu = 1$ car l'ordre de σ est $n = [L : K]$. On conclut donc que $\varphi_{E/K}(\mathfrak{p}))^\nu = 1$ et d'où n divise ν, et pa suite $\varphi_{L/K}(\mathfrak{p}))^\nu = 1$, et donc le seul élément dans l'intersection est l'identité, ce qui termine la preuve du troisième assertion. La preuve de la première assertion est immédiat par la définition de H. L'intersection $L \cap F$ est la partie de L fixée par H. Cependant la restriction de H à L contient $res_L(\sigma \times \tau) = \sigma$ qui engendre tout $Gal(L/K)$, d'où $L \cap F = K$. □

Maintenant, nous pouvons montrer la loi de réciprocité pour les extensions cycliques.

Théorème 6.1.1. *Soit L/K une extension cyclique à groupe de Galois G, et soit $\mathfrak{m}$ un module de K divisible par tous les premiers de K ramifiés dans L. On suppose que l'égalité fondamentale $h_\mathfrak{m}(L/K) = [L : K]$ est satisfaite. Alors le triplet $(L, K, \mathfrak{m})$ vérifie la loi de réciprocité.*

Preuve. Nous montrerons que $\ker(\varphi_{E/K}(\mathfrak{p})_{\mathbf{I}_K^\mathfrak{m}}) \subset i(K_{\mathfrak{m},1})N(\mathbf{I}_L^\mathfrak{m})$, alors l'égalité s'en déduira car ces deux groupes ont le même index $[L : K]$ dans $\mathbf{I}_K^\mathfrak{m}$.

Soit un idéal $\mathfrak{A}$ dans $\mathbf{I}_K^\mathfrak{m}$ pour lequel $\varphi_{E/K}(\mathfrak{A}) = 1$, factorisons $\mathfrak{A}$ comme suit :

$$\mathfrak{A} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$$

les premiers $\mathfrak{p}_i$ sont non ramifiés dans L car les ramifiés divisent $\mathfrak{m}$ et $\mathfrak{A}$ est premier à $\mathfrak{m}$ par choix. Le Lemme d'Artin pour chaque premier $\mathfrak{p}_i$ pour avoir pour chacun d'eux une racine d'unité θ_{m_i}tels que m_i sont relativement premiers deux à deux. Par le choix fait dans la Proposition 6.1.1, nous pouvons assurer que $K \cap \mathbb{Q}(\theta_{m_i}) = \mathbb{Q}$, d'où le groupe de Galois

$$G_i = \mathrm{Gal}(K(\theta_{m_i})/K) \simeq \mathrm{Gal}(\mathbb{Q}(\theta_{m_i})/\mathbb{Q}).$$

De plus le groupe de Galois de $L(\theta_{m_1}, \theta_{m_2}, \cdots, \theta_{m_r})$ sur K est le groupe produit direct

$$\mathcal{G} = \mathrm{Gal}(L(\theta_{m_1}, \theta_{m_2}, \cdots, \theta_{m_r})/K) = G \times G_1 \times \cdots G_r,$$

avec $G = \langle\sigma\rangle$. Soit τ_i l'élément choisi comme le Lemme d'Artin (utilisant $\mathfrak{p}_i$ à la place de $\mathfrak{p}$). Soit H_i le sous-groupe de $G \times G_i$ engendré par

$$\sigma \times \tau_i \text{ et } \varphi_{L/K}(\mathfrak{p}_i) \times \varphi_{K(\theta_{m_1})/K}(\mathfrak{p}_i).$$

On peut voir H_i comme un sous-groupe de $\mathcal{G}$ par le plongement trivial.

Soit F_i le sous corps $L(\theta_{m_1}, \theta_{m_2}, \cdots, \theta_{m_r})$ laissé fixe par $H_i \times \prod_{j \neq i} G_j$, posons $F = F_1F_2 \cdots F_r$, alors montrons que $L \cap F = K$ et $Gal(LF/F) = Gal(L/K)$.

Notons d'abord que, pour tout i, $Gal(LF/F_i)$ contient l'élément

$$\lambda = \sigma \times \tau_i \times \cdots \times \tau_r.$$

L'intersection des groupes $Gal(LF/F_i)$ fixe F et contient λ. Donc le corps L_capF est fixé par cet élément et par $1 \times \tau_i \times \cdots \times \tau_r$, d'où $L \cap F$ est fixé par σ puisque le sous corps de L fixé par σ est K, nous obtenons $L \cap F = K$. L'égalité $Gal(LF/F) = Gal(L/K)$ est vraie, car la restriction de $Gal(LF/F)$ à L définie un isomorphisme avec $Gal(L/K)$.

Considérons maintenant $\varphi_{L/K}(\mathfrak{p}_i^{a_i}) = \sigma^{d_i}$ pour un certain $d_i \geq 0$. Alors

$$\varphi_{L/K}(\mathfrak{A}) = \prod_i \sigma^{d_i} = 1.$$

Posons $d = \sum_{i=1}^{r} d_i$, alors on déduit que n divise d, où $n = [L : K] = |G|$. L'application d'Artin envoie surjectivement $\mathbf{I}_{\mathbf{F}}^{\mathfrak{m}'}$ sur $Gal(LF/F)$ pour un certain module $\mathfrak{m}'$ avec des exposants suffisamment grands et des diviseurs convenables. nous pouvons prendre $\mathfrak{m}'$ divisible par $\mathfrak{m}$ et par tous les entiers m_i. Il existe donc un idéal $\mathfrak{B}_0$ relativement premier à $\mathfrak{m}$ et à tous les entiers m_i tel que $\varphi_{LE/F}(\mathfrak{B}_0) = \sigma$.

Posons $N_{F/K}(\mathfrak{B}_0) = \mathfrak{B} \in \mathbf{I}_K^{\mathfrak{m}}$, or $\varphi_{L/K}(\mathfrak{B}) = \varphi_{L/K}(N_{F/K}(\mathfrak{B}_0)) = \varphi_{LF/F}(\mathfrak{B}_0) = \sigma$ (voir [4, Proposition 3.1]) puisque $\mathfrak{B}$ est norme d'un élément de F, il est aussi norme d'un élément de F_j. De plus, chaque $\mathfrak{p}_i$ se décompose complètement dans F_i, alors $\mathfrak{p}_i$ est norme d'un élément de F_i. Il existe donc un idéal $\mathcal{C}_i$ premier à $\mathfrak{m}$ et à tous les entiers m_i tel que

$$N_{F_i/K}(\mathfrak{C}_i) = \mathfrak{p}_i^{a_i}\mathfrak{B}^{-d_i}.$$

Maintenant nous avons

$$\varphi_{LF_i/F_i}(\mathfrak{C}_i) = \varphi_{L/K}(N_{F_i/K}(\mathfrak{C}_i)) = \varphi_{L/K}(\mathfrak{p}_i)^{a_i}\varphi_{L/K}(\mathfrak{B})^{-d_i} = \sigma^{d_i - d_i} = 1.$$

L'extension LF_i de F_i satisfait $F_i \subset LF_i \subset F_i(\theta_{m_i})$ voir Lemme d'Artin 6.1.4. D'après l'exemple 5 page 49, la loi de réciprocité a lieu pour le triplet $(LF_i, F_i, \mathfrak{m}'')$ autant que $\mathfrak{m}''$ est divisible par $(m_i)\mathfrak{p}_\infty$, le module de $\mathbb{Q}$ étendu à F_i. Par le choix de $\mathcal{C}_i$ premier à m_i et à $\mathfrak{m}$, alors on peut choisir $\mathfrak{m}''$ divisible par $\mathfrak{m}$ et que $\mathfrak{C}_i \in \mathbf{I}_{F_i}^{\mathfrak{m}''}$. Par la loi de réciprocité, il existe $\gamma_i \in F_i$, $\gamma_i \equiv^* 1 \pmod{\mathfrak{m}''}$, et un idéal $\mathcal{D}_i \in \mathbf{I}_{LF_i}^{\mathfrak{m}''}$ tels que

$$\mathfrak{C}_i = (\gamma_i)N_{LF_i/F_i}(\mathcal{D}_i).$$

Appliquons la norme dans K, on obtient :

$$\mathfrak{p}_i^{a_i}\mathfrak{B}^{-d_i} = (N_{F_i/K}(\gamma_i))N_{LF_i/K}(\mathfrak{D}_i).$$

Comme le module $\mathfrak{m}''$ est pris divisible par $\mathfrak{m}$, alors on a en plus $\alpha_i = N_{F_i/K}(\gamma_i) \in K_{\mathfrak{m},1}$. En prenant le produit sur tous les i, $1 \leq i \leq r$, on obtient

$$\mathfrak{A}\mathfrak{B}^{-d} = \prod_i \mathfrak{p}_i^{a_i}\mathfrak{B}^{-d_i} = \prod_i \alpha_i \prod_i N_{LF_i/K}(\mathfrak{D}_i).$$

Posons $\mathfrak{D}_i' = N_{LF_i/L}(\mathfrak{D}_i)$ qui est premier à $\mathfrak{m}$. Finalement, on a

$$\mathfrak{A} = \mathfrak{B}^d(\alpha_1\alpha_2\cdots\alpha_r)N_{L/K}(\mathfrak{D}_1'\mathfrak{D}_2'\cdots\mathfrak{D}_r').$$

Nous avons déjà mentionné que n divise d, alors $\mathfrak{B}^d$ est norme dans L/K, par suite $\mathfrak{A} \in i(K_{\mathfrak{m},1})N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$ comme prévu. □

Ce résultat délicat pour les extensions cycliques se généralise facilement aux extensions abéliennes moyennant le théorème de structure des groupes abéliens finis.

Théorème 6.1.2 (Théorème de la réciprocité d'Artin). *Soit L/K une extension abélienne de corps de nombres de groupe de Galois G, et soit $\mathfrak{m}$ un module de K divisible par tous les premiers de K ramifiés dans L. Si les exposants des premiers divisant $\mathfrak{m}$ sont suffisamment grands, alors l'application d'Artin $\varphi_{L/K}$ envoie surjectivement $\mathbf{I}_K^{\mathfrak{m}}$ sur G et que son noyau est* $\ker(\varphi_{L/K}) = i(K_{\mathfrak{m},1})N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$.

Preuve. Comme le groupe G est abélien, alors il s'écrit comme produit direct des sous-groupes cycliques C_i (c'est le théorème de structure des groupes abéliens finis)

$$G = C_1 \times C_2 \times \cdots \times C_s.$$

Soit H_j le produit direct de tous les sous-groupes cycliques C_i avec $1 \leq i \neq j \leq s$, donc $G = H_j \times C_j$. Soit E_j le sous corps de L laissé fixe par H_j, d'où par la théorie de Galois E_j est une extension cyclique de K de groupe de Galois C_j. Par suite il existe un module $\mathfrak{m}_j$ de K tel que la loi de réciprocité soit vérifiée pour le triplet $(E_j, K, \mathfrak{m}_j)$. Notons que tout premier de K ramifié dans E_j est aussi ramifié dans L. De plus $\mathfrak{m}_j$ peut être choisi de telle manière qu'il soit divisible seulement par les premiers ramifiés dans E_j et les exposants dans $\mathfrak{m}$ soient suffisamment grand pour que $\mathfrak{m}_j|\mathfrak{m}$. Donc la loi de réciprocité est vérifiée pour le triplet $(E_j, K, \mathfrak{m})$, ce qui implique que

$$i(K_{\mathfrak{m},1}) \subset \bigcap_j \ker(\varphi_{E_j/K}).$$

Pour tout idéal $\mathfrak{A} \in \mathbf{I}_K^{\mathfrak{m}}$, nous avons par [4, Propriété 2.4] sur l'automorphisme de Frobenius, $\varphi_{L/K}(\mathfrak{A})|_{E_j} = \varphi_{E_j/K}(\mathfrak{A})$. En particulier pour $\mathfrak{A} \in i(K_{\mathfrak{m},1})$ on trouve que

$$\varphi_{L/K}(\mathfrak{A})|_{E_j} = 1.$$

Mais $L = E_1E_2 \cdots E_s$, car le groupe qui laisse fixe tous les E_j est le groupe intersection de tous les H_j qui est trivial ; un automorphisme trivial sur tous les E_j est l'identité sur L tout entier. Ansi $i(K_{\mathfrak{m},1}) \subset \bigcap_j \ker(\varphi_{L/K})$ et que la loi de réciprocité a lieu pour $(L, K, \mathfrak{m})$; moyennant le Lemme 6.1.1 on obtient le résultat voulu à savoir
$\ker(\varphi_{L/K}) = N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$. □

6.2 Théorème de Kronecker-Weber

Comme illustration du profit et de la puissance du théorème de la réciprocité d'Artin, nous citons comme consequence le résultat suivant : le théorème de Kronecker-Weber qui classifie les extensions abéliennes du corps des rationnels $\mathbb{Q}$ comme sous-corps de certains corps cyclotomiques. Nous commençons par un théorème général.

Théorème 6.2.1. *Soient L/K une extension abélienne de corps de nombres et $\mathfrak{m}$ un module de K tels que la loi de réciprocité soit satisfaite pour le triplet $(L, K, \mathfrak{m})$. Si E est une extension galoisinne de K telle que $N_{E/K}(\mathbf{I}_E^{\mathfrak{m}}) \subset N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})$, alors $L \subset E$.*

Pour la preuve nous avons besoin du résultat suivant :

Lemme 6.2.1 ([4, Corollaire 5.5, Ch IV])**.** *Soient L_1 et L_2 deux extensions galoisiennes d'un corps de nombres K. Soit S_i, où $i = 1, 2$, l'ensemble des idéaux premiers de $\mathcal{O}_K$ qui se décomposent complètement dans L_i. Si $S_1 \subset S_2$ (sauf éventuellement pour un nombre fini d'idéaux), alors $L_2 \subset L_1$*

Preuve du théorème 6.2.1. À l'exception d'un nombre fini d'idéaux premiers divisant le module $\mathfrak{m}$, les idéaux premiers finis qui se décomposent complètement dans E appartiennent tous à $N_{E/K}(\mathbf{I}_E^{\mathfrak{m}})$. Ces derniers doivent aussi se décomposés complètement dans L puisque sont dans le noyau de l'application d'Artin $\varphi_{L/K}$, par suite le Lemme 6.2.1 implique que $L \subset K$. □

Théorème 6.2.2. *Un corps de nombres L est une extension abélienne de $\mathbb{Q}$ si et seulement si $L \subset \mathbb{Q}(\theta_m)$ pour une racine m-ième θ_m de l'unité.*

Preuve. Rappelons d'abord que toute extension cyclotomique $\mathbb{Q}(\theta)$ de $\mathbb{Q}$ est abélienne, alors le sens inverse est immédiat puisque tout sous-corps de $\mathbb{Q}(\theta)$ est aussi une extension abélienne de $\mathbb{Q}$.

Montrons maintenant le sens direct. Notons d'abord que la loi de réciprocité est vérifiée pour le triplet $(L, \mathbb{Q}, \mathfrak{m})$ pour un certain module $\mathfrak{m}$ de K. Soit m un entier positif, on peut supposer que $\mathfrak{m} = (m)p_\infty$. Soit θ_m une racine primitif m-ième de l'unité, posons $E = \mathbb{Q}(\theta_m)$; par les calculs dans la preuve de [4, Proposition 3.3, Chap III], on déduit que $i(\mathbb{Q}_{\mathfrak{m},1}) = \ker(\varphi_{E/\mathbb{Q}})$ et

$$i(\mathbb{Q}_{\mathfrak{m},1}) = i(\mathbb{Q}_{\mathfrak{m},1})N_{E/\mathbb{Q}}(\mathbf{I}_E^{\mathfrak{m}}) \subset \ker(\varphi_{L/K}) = i(\mathbb{Q}_{\mathfrak{m},1})N_{L/\mathbb{Q}}(\mathbf{I}_L^{\mathfrak{m}}).$$

Donc par le Théorème 6.2.1 on tire que $L \subset E$. □

Bibliographie

[1] F.Q. Gouvea, *p-adic Numbers : An Introduction.* Springer Verlag, 1993.

[2] G. Gras, *Class Field Theory.* Springer Verlag, 2003.

[3] D. Hilbert, *The theory of algebraic number fields,* Translated from germany by Iain T. Adamson, Springer-verlag berlin heidelberg (1998).

[4] G. J. Janusz, *Algebraic Number Fields,* Graduate Studies in Mathematics, volume 7, USA, Second Edition (1996).

[5] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields.* Springer-Verlag, NY, 1978.

[6] J. Cassels and A. Fröhlich, *Algebraic number theory.* Thompson Publ, Washington, 1967.

[7] A. Fröhlich and M.J. Taylor, *Algebraic number theory.* Cambridge University Press, Great Britain, 1991.

[8] H.P.F. Swinnerton-Dyer, A Brief Guide to Algebraic Number Theory. University Press of Cambridge, 2001.

[9] F. Lemmermeyer, *Class Field Towers,* September 7, (2010).

[10] J.S. Milne, *Class Field Theory* (*v*4.02), (2013), www.jmilne.org/math/.

[11] P. Samuel, *Théorie des nombres,* Collection Méthodes, éditions Hermann.

[12] Lang, Serge. *Algebra* (*Rev. 3. ed., corr. printing. ed.*) New York, NY, Springer, (2005).

[13] H. Hasse, *History of Class Field Theory,* in "Algebraic Number Theory", J. W. S. Cassels and A. Fröhlich, Academic Press, New York, (1967).

[14] S. Iyanaga, *The Theory of Numbers,* North-Holland, Amsterdam, 1975.

[15] S. Iyanaga, *Travaux de Claude Chevalley sur la théorie du corps de classes : Introduction, Japan. J. Math. 1 (2006), 25-85.*

[16] M. Katsuya, *The Establishment of the Takagi-Artin Class Field Theory,* in The Intersection of History and Mathematics, (C. Sasaki, M. Sugiura, J. W. Dauben ed.), Birkhauser, Boston, 1995, 109-128.

[17] S. Lang, *Algebraic Number Theory,* 2nd ed., Springer-Verlag, New York, 1994.