Corps de classes, formes modulaires, et formalisation

Filippo Alberto Edoardo Nuccio Mortarino Majno Di Capriglio

▶ **To cite this version:**

Filippo Alberto Edoardo Nuccio Mortarino Majno Di Capriglio. Corps de classes, formes modulaires, et formalisation. Théorie des nombres [math.NT]. Université Jean Monnet Saint-Étienne, 2023. ujm-04198760

HAL Id: ujm-04198760
https://ujm.hal.science/ujm-04198760

Submitted on 8 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License

Université Jean Monnet Saint-Étienne

École Doctorale de l'Université Jean Monnet Saint-Étienne

HABILITATION À DIRIGER DES RECHERCHES

Corps de classes, formes modulaires, et formalisation

par Filippo A. E. Nuccio Mortarino Majno di Capriglio

Maître de conférences, Université Jean Monnet Saint-Étienne

Rapporteurs

Kevin Buzzard	*Professor, Imperial College London*
Antoine Chambert-Loir	*Professeur, Université Paris Cité*
Cornelius Greither	*Professor i.R., Universität der Bundeswehr München*

Soutenance publique le 25 septembre 2023, devant le jury composé de

Kevin Buzzard	*Professor, Imperial College London*
Antoine Chambert-Loir	*Professeur, Université Paris Cité*
Cornelius Greither	*Professor i.R., Universität der Bundeswehr München*
Assia Mahboubi	*Directrice de recherche, INRIA*
Sophie Morel	*Directrice de recherche, C. N. R. S. – ENS de Lyon*
Xavier Roblot	*Maître de conférences HDR, Université Claude Bernard Lyon*

Corps de classes, formes modulaires, et formalisation

par Filippo A. E. Nuccio Mortarino Majno di Capriglio

Cette œuvre est sous licence Creative Commons CC BY-SA 4.0. Pour consulter une copie de la licence, visitez https://creativecommons.org/licenses/by-sa/4.0/deed.fr.

Filippo A. E. Nuccio Mortarino Majno di Capriglio
Université Jean Monnet Saint-Étienne
Institut Camille Jordan UMR 5208
23, rue du docteur Paul Michelon
F-42023, Saint-Étienne, France
filippo.nuccio@univ-st-etienne.fr
https://perso.univ-st-etienne.fr/nf51454h/

וַהֲיִינוּ דְּאָמַר רַבִּי חֲנִינָא: הַרְבֵּה לָמַדְתִּי מֵרַבּוֹתַי
וּמֵחֲבֵירַי יוֹתֵר מֵרַבּוֹתַי וּמִתַּלְמִדַי יוֹתֵר מִכּוּלָּן

תלמוד בבלי, תענית ז ע"א

Et voici ce que dit Rabbi Hanina : j'ai beaucoup appris de mes maîtres, et plus encore que de mes maîtres j'ai appris de mes copains. Mais ceux dont j'ai le plus appris, ce sont mes étudiants.

Talmud babylonien, traité Taanit, 7a

Table des matières

Introduction

Ce mémoire présente une synthèse des travaux de recherche que j'ai effectués depuis ma thèse soutenue en 2009. Les objets étudiés sont principalement de nature arithmétique et une partie de mes travaux concerne la formalisation de tels concepts dans l'assistant de preuve `lean-3`.

Sur la période 2009–2019 mes intérêts ont évolué à partir de l'argument de ma thèse, qui portait sur la théorie d'Iwasawa des corps de nombres totalement réels. Le fil conducteur du Chapitre II est la théorie d'Iwasawa, soit pour le groupe de classes au §II.1, soit pour les courbes elliptiques et les formes modulaires aux §§II.2–II.4.

Le Chapitre I présente deux travaux traitant les propriétés arithmétiques des extensions diédrales de corps de nombres. Le premier, décrit au §I.1 étudie une formule pour les nombres de classes dans de telles extensions ; le deuxième, objet du §I.2, analyse des phénomènes de congruence pour les représentations modulaires diédrales en lien avec les formes modulaires CM.

Depuis 2019 ma recherche s'est recentrée autour de la formalisation mathématique par ordinateur, et plus particulièrement dans l'assistant de preuve `lean-3`. Le Chapitre III est dédié à cet argument. Au §III.1 je présente un travail de formalisation des propriétés de base des anneaux de Dedekind et de la finitude du groupe de classes d'idéaux pour les corps globaux. Le §III.2 est consacré au *Liquid Tensor Experiment*, un travail qui répond au défi lancé par Scholze de formaliser un des ses résultat, obtenu avec Clausen, sur les espaces vectoriels liquides. Mes projets de recherche futurs s'inscrivent aussi dans la thématique de la formalisation, et je les illustre brièvement au §III.3.

Je ne m'aventure pas dans l'exercice périlleux de mentionner toutes les personnes auxquelles je dois ma gratitude. Je mesure la chance d'avoir croisé le chemin de tant d'amis, de collègues, de membres de ma famille. Je ferai de mon mieux pour leur exprimer ma reconnaissance personnellement. À cause de son caractère collectif, cela ne sera probablement pas possible avec la communauté `mathlib`, et je tiens donc à en remercier ici tous ses membres pour leur accueil, leur support, leurs enseignements.

Saint-Étienne, 6 juin 2023

I

Arithmétique des extensions diédrales

Ce chapitre regroupe des résultats portant sur les propriétés arithmétiques des extensions diédrales de corps de nombres. Au §I.1 je discute une formule qui relie les nombres de classes des sous-corps d'une extension diédrale ; au §I.2 j'étudie des phénomènes de congruence modulo un premier p entre une forme modulaire dont la représentation galoisienne modulo p est diédrale, et une forme à multiplication complexe.

Travaux présentés :

[CN20] L. Caputo & F. A. E. Nuccio Mortarino Majno di Capriglio – « Class number formula for dihedral extensions », *Glasgow Mathematical Journal* **62** (2020), no. 2, p. 323–353.

[BN18] N. Billerey & F. A. E. Nuccio Mortarino Majno di Capriglio – « Représentations galoisiennes diédrales et formes à multiplication complexe », *Journal de théorie des nombres de Bordeaux* **30** (2018), no. 2, p. 651–670.

I.1 Formule de nombre des classes pour extensions diédrales

avec L. Caputo

Étant donné un corps de nombres k, notons $\mathcal{C}\ell_k$ son groupe de classes et $h_k = |\mathcal{C}\ell_k|$ son nombre de classes. Pour une extension L/k, il est naturel de chercher à relier les nombres h_L et h_k, mais l'exemple des corps quadratiques montre qu'une formule universelle ne dépendant que de la structure galoisienne de L/k ne peut pas exister. Mentionnons à ce propos le théorème de Montgomery–Weinberg (voir [MW77]) qui établit l'existence d'une constante $c > 0$ telle que

$$h_{\mathbb{Q}(\sqrt{d})} > c\sqrt{d}\,\frac{\log\log d}{\log d}$$

pour une infinité de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$.

D'autre part, un célèbre résultat dû à Chevalley donne une relation entre nombres de classes dans une extension *cyclique* en termes cohomologiques :

Théorème (Formule des classes ambiges de Chevalley, voir [Lan90, Lemma 4.1]). *Soit k un corps de nombres et soit L/k une extension finie cyclique, de groupe $G = \mathrm{Gal}(L/k)$. Alors*

$$|\mathcal{C}\ell_L^G| = \frac{h_k \cdot e(L/k)}{[L:k]\big(\mathcal{O}_k^\times : \mathrm{N}_{L/k}L^\times \cap \mathcal{O}_k^\times\big)} \tag{I.1.1}$$

où $\mathcal{C}\ell_L^G$ dénote le sous-groupe des classes fixées par l'action de G, et $e(L/k) = \prod_{\mathfrak{p}} e(\mathfrak{p})$ est le produit des tous les indices de ramification.

Bien que l'exemple des groupes cycliques puisse paraître archétypique, il est en réalité quelque peu particulier. En effet, Brauer montra en 1947 que toute représentation d'un groupe fini G peut se décomposer en tant que combinaison linéaire *entière* (ou « virtuelle ») de représentations induites de sous-groupes cycliques. L'application qu'il avait en vue, et qui est importante pour nous, est le théorème suivant :

Théorème ([Bra51, Satz 1 et équation (12)]). *Soit $L/\mathbb{Q}$ une extension galoisienne à groupe de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$. Pour toute extensions intermédiaire $\mathbb{Q} \subseteq K \subseteq L$ notons $\mathcal{R}_K$* (resp. *w_K*) *le régulateur* (resp. *le nombre de racines de l'unité*) *de K. Il existe alors une relation*

$$\prod_H (h_{L^H})^{a_H} = \prod_H \left(\frac{w_{L^H}}{\mathcal{R}_{L^H}}\right)^{a_H} \tag{I.1.2}$$

pour H parcourant les sous-groupes cycliques *de G, et où les $a_H \in \mathbb{Z}$ sont des entiers. Si G n'est pas cyclique, une telle relation existe avec les a_H non tous nuls.*

La preuve du théorème de Brauer est de nature analytique. Elle repose sur le théorème mentionné précédemment portant sur les représentations virtuelles, qui permet de décomposer la représentation régulière comme combinaison linéaire à coefficients entiers de représentations induites de sous-groupes cycliques — les entiers $a_H \in \mathbb{Z}$ étant précisément les coefficients apparaissant dans une telle décomposition. Lorsque G est lui-même cyclique, il peut arriver que la seule relation soit la triviale, avec $a_H = 0$ pour tout H ; mais la définition même des coefficients a_H montre que si G n'est pas cyclique, il existe toujours une relation non-triviale. Une fois cette décomposition virtuelle obtenue, le formalisme des fonctions L d'Artin, conjointement à la formule pour le résidu de la fonction zêta d'un corps de nombre (voir [Tat67a, Main Theorem 4.4.1]), donne (I.1.2). Cela a, comme conséquence, l'apparition des facteurs transcendants $\mathcal{R}_{L^H}$ dans le membre de droite de (I.1.2), alors que le membre de gauche est évidemment rationnel ; en outre, pour appliquer la formule dans des cas explicites il est nécessaire de calculer les coefficients a_H — ce qui peut s'avérer, en général, impossible.

Lorsque le groupe de Galois $G = \mathrm{Gal}(L/k)$ qui apparaît dans le théorème de Brauer est diédral, le valeurs a_H et les contributions des régulateurs ont été explicitées en termes d'indices d'unités (ce qui est naturel, au vu de la définition du régulateur) dans certains cas. Halter-Koch dans [HK77] et Moser dans [Mos79] ont analysé le cas d'une extension diédrale $L/\mathbb{Q}$ de degré $2p$, où p est un premier impaire. En s'appuyant sur le résultat de Brauer et en explicitant le rapport des régulateurs, ils ont montré que dans ce cadre on a

$$\frac{h_L}{h_F h_K^2} = \big(\mathcal{O}_L^\times : \mathcal{O}_K^\times \mathcal{O}_{K'}^\times \mathcal{O}_F^\times\big) p^{-r} \tag{I.1.3}$$

où $K/\mathbb{Q}, K'/\mathbb{Q}$ sont deux sous-corps (conjugués) de degré p contenus dans L ; où $F/\mathbb{Q}$ est l'unique sous-extension quadratique contenue dans L ; et où r vaut 1 lorsque F est imaginaire, et vaut 2 lorsque F est réelle.

Ce genre d'analyse devient impraticable dès lors que le corps de base k n'est plus le corps $\mathbb{Q}$ des rationnels, et donc lorsque le groupe $\mathcal{O}_k^\times$ est plus compliqué que $\mathbb{Z}^\times = \{\pm 1\}$. Néanmoins, certaines généralisations partielles du résultat de Halter-Koch et Moser ont été proposées : nous nous contentons ici de mentionner le travail [Jau81b] où le corps de base k peut être soit $\mathbb{Q}$ soit un corps quadratique imaginaire (donc, toujours avec groupe d'unités fini), et l'ordre du groupe diédral peut être $2p^s$ pour p premier et $s \geqslant 1$; ou encore le travail [Lem05] de Lemmermeyer, qui montre (I.1.3) pour k quelconque, mais seulement pour extensions L/k d'ordre $2p$ et sous certaines hypothèses de ramification, hypothèses qui ont été levées dans le travail [Bar12] de Bartel.

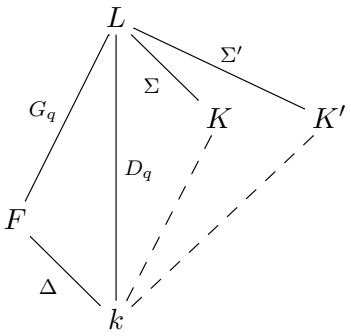
Le point de départ du travail [CN20] est l'observation que la formule des classes ambiges de Chevalley (I.1.1) admet une démonstration purement cohomologique, qui repose seulement sur la théorie du corps de classes (voir par exemple la preuve donnée dans [Lan90, Lemma 4.1]). Notre idée dans le cas diédral est d'étudier l'action du groupe quotient d'ordre 2 sur les groupes de cohomologie du sous-groupe distingué maximal, qui est abélien et auquel la théorie du corps de classes s'applique. Afin de détailler le résultat principal, fixons les notations suivantes :

Notation I.1.1. Soit $q \geqslant 3$ un nombre impair : notons D_q le groupe diédral d'ordre $2q$, dont nous fixons une présentation

$$D_q = \langle \sigma, \rho \,\big|\, \sigma^2 = \rho^q = 1, \sigma\rho = \rho^{-1}\sigma \rangle.$$

Le sous-groupe distingué d'ordre q est noté $G_q = \langle \rho \rangle$ et $\Delta = D_q/G_q$ dénote le quotient d'ordre 2 ; aussi, posons $\Sigma = \langle \sigma \rangle$ et $\Sigma' = \langle \sigma\rho \rangle$. Étant donnée une extension L/k avec un isomorphisme $\mathrm{Gal}(L/k) \cong D_q$ (qu'on considère choisi une fois pour toutes), notons F le sous-corps fixé par G_q et par K (*resp.* par K') le sous-corps fixé par Σ (*resp.* par Σ').

Le contexte galoisien est illustré dans le schéma suivant :



Étant donné un D_q-module B uniquement 2-divisible[1], le quotient Δ agit de façon fidèle sur les groupes de cohomologie de Tate $\widehat{H}^i(G_q, B)$: écrivons $\widehat{H}^i(G_q, B)^\pm$ pour le sous-module propre de valeur propre ± 1. Un argument de suite spectrale de Hochschild–Serre permet d'obtenir le résultat suivant :

1. Autrement dit, tel que la multiplication $\cdot 2 \colon B \to B$ est un isomorphisme.

Proposition I.1.2 ([CN20, Proposition 2.1]). *Soit B un D_q-module uniquement 2-divisible. Pour tout $i \in \mathbb{Z}$, le morphisme de restriction induit un isomorphisme*

$$\widehat{H}^i(D_q, B) \cong \widehat{H}^i(G_q, B)^+.$$

De plus, l'isomorphisme de périodicité de Tate $\widehat{H}^i(G_q, B) \cong \widehat{H}^{i+2}(G_q, B)$ (provenant de la cyclicité de G) anti-commute à l'action de Δ : on obtient, pour tout $i \in \mathbb{Z}$, des isomorphismes

$$\widehat{H}^i(G_q, B)^- \cong \widehat{H}^{i+2}(G_q, B)^+ \cong \widehat{H}^{i+2}(D_q, B)$$
$$\widehat{H}^i(G_q, B)^+ \cong \widehat{H}^{i+2}(G_q, B)^- \cong \widehat{H}^i(D_q, B).$$

Nous appliquons la Proposition I.1.2 aux différents modules qui apparaissent dans le diagramme commutatif suivant, dont les colonnes et les lignes sont exactes :

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{O}_L^\times[\frac{1}{2}] & \longrightarrow & L^\times[\frac{1}{2}] & \longrightarrow & \mathrm{PrId}_L[\frac{1}{2}] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathbb{I}_L[\frac{1}{2}] & \longrightarrow & \mathbb{A}_L^\times[\frac{1}{2}] & \longrightarrow & \mathrm{Id}_L[\frac{1}{2}] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Q_L[\frac{1}{2}] & \longrightarrow & \mathcal{C}_L[\frac{1}{2}] & \longrightarrow & \mathscr{C}\ell_L[\frac{1}{2}] & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array} \tag{I.1.4}$$

Dans (I.1.4) nous avons noté $\mathrm{PrId}_\bullet$ le groupe des idéaux fractionnaires principaux non-nuls, $\mathrm{Id}_\bullet$ le groupe des idéaux fractionnaires non-nuls, $\mathbb{A}_\bullet^\times$ le groupe des idèles et $\mathbb{I}_\bullet$ le groupe des idèles dont les composantes sont des unités à toute place finie : le groupe $Q_\bullet$ est défini comme le quotient $\mathbb{I}_\bullet/\mathcal{O}_\bullet^\times$. La cohomologie d'un groupe de Galois *abélien* à coefficient dans tout module apparaissant dans (I.1.4) est contrôlée par la théorie du corps de classes (voir [Tat67b]), et en appliquant la Proposition I.1.2 nous obtenons le

Théorème I.1.3 ([CN20, Theorem 3.14]). *Soit L/k une extension de corps de nombres à groupe de Galois D_q. Alors*

$$\frac{h_L h_k^2}{h_F h_K^2} = \frac{|\widehat{H}^0(D_q, \mathcal{O}_L^\times \otimes \mathbb{Z}[\frac{1}{2}])|}{|\widehat{H}^{-1}(D_q, \mathcal{O}_L^\times \otimes \mathbb{Z}[\frac{1}{2}])|} = \frac{|\widehat{H}^0(D_q, \mathcal{O}_L^\times)|}{|\widehat{H}^{-1}(D_q, \mathcal{O}_L^\times)|} \cdot \frac{|\widehat{H}^{-1}(\Sigma, \mathcal{O}_L^\times)|}{|\widehat{H}^0(\Sigma, \mathcal{O}_L^\times)|}.$$

Remarque I.1.4. Le membre de droite dans le théorème est un « quotient de Herbrand diédral », ainsi que la formule du Théorème I.1.3 est à rapprocher du résultat classique (voir [Tat67b, preuve du Theorem 8.3]) établissant que le quotient de Herbrand des unités dans une extension *cyclique* de degré n vaut n^{-1} (donc, il ne contient aucune information sur les nombres de classes) : nous interprétons ceci comme une manifestation algébrique de la particularité du cas cyclique déjà mentionnée à propos des résultats de Brauer.

Dans la formule du Théorème I.1.3 aucun facteur transcendent n'apparaît, et il est très aisé de traduire les quotients des ordres des groupes de cohomologie en termes d'indices d'unités. Nous nous contentons de mentionner ici les deux corollaires suivants (valables dans le même contexte que celui du Théorème I.1.3), où on note $v_\ell(-)$ la valuation ℓ-adique pour tout premier ℓ :

Corollaire I.1.5 ([CN20, Corollary 3.15]). *Pour tout nombre premier ℓ et pour tout corps $M \in \{k, F\}$ écrivons*

$$\beta_M(q) = \begin{cases} 0 & \text{si } M \text{ ne contient aucune racine } q\text{-ième de l'unité ;} \\ 1 & \text{sinon.} \end{cases}$$

On a alors les bornes suivantes

$$-av_\ell(q) \leqslant v_\ell\left(\frac{h_L h_k^2}{h_F h_K^2}\right) \leqslant bv_\ell(q)$$

où $a = \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_F^\times) + \beta_F(q) + 1$ et $b = \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times) + \beta_k(q)$. En particulier, si F est totalement réel de degré $[F : \mathbb{Q}] = 2d$, alors

$$-2dv_\ell(q) \leqslant v_\ell\left(\frac{h_L h_k^2}{h_F h_K^2}\right) \leqslant (d-1)v_\ell(q).$$

Corollaire I.1.6 ([CN20, Corollary 3.18]). *Supposons que F soit un corps CM[2] de degré $[F : \mathbb{Q}] = 2d$ et que k soit son sous-corps totalement réel maximal. Soit s l'ordre du quotient $\left((\mathcal{O}_K^\times)^q \cap \mathcal{O}_k^\times\right)/(\mathcal{O}_k^\times)^q$ et supposons que F ne contienne pas de racine q-ièmes de l'unité. Alors, pour tout nombre premier ℓ, on a*

$$-v_\ell(q) - v_\ell(s) \leqslant v_\ell\left(\frac{h_L h_k^2}{h_F h_K^2}\right) \leqslant (d-1)v_\ell(q).$$

I.2 Représentations galoisiennes diédrales et formes CM

avec N. Billerey

Afin d'introduire les résultats contenus dans [BN18], nous allons fixer quelque notation qui sera également utile dans les sections suivantes. Faisons le choix d'un corps algébriquement clos $\bar{\mathbb{Q}}$ qui contiendra toutes les extensions algébriques de $\mathbb{Q}$ qui apparaitront dans la suite ; pour une telle extension K, écrivons $\mathcal{G}_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ pour son groupe de Galois absolu. Des clôtures algébriques $\overline{\mathbb{F}_p}$ et $\overline{\mathbb{Q}_p}$ seront également fixées pour tout premier p.

Pour tout corps topologique E (les cas où E est une extension finie de $\mathbb{Q}_p$, muni de sa topologie p-adique ; et les cas $E = \mathbb{F}_q$ ou $E = \overline{\mathbb{F}_p}$, munis de la topologie discrète, seront les principaux) nous appelons *représentation galoisienne* tout homomorphisme continu $\rho\colon \mathcal{G}_{\mathbb{Q}} \to \mathrm{GL}_2(E)$; lorsque $E \subseteq \overline{\mathbb{F}_p}$ pour un certain premier p, nous dirons que la représentation galoisienne est *modulaire* (*modulo* p).

2. Nous rappelons qu'un corps de nombres est dit CM s'il est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel.

Définition I.2.1. Une représentation galoisienne modulaire $\rho\colon \mathcal{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ est dite diédrale si l'image de sa projectivisée $\mathbf{P}\rho\colon \mathcal{G}_{\mathbb{Q}} \to \mathrm{PGL}_2(\overline{\mathbb{F}_p})$ est isomorphe au groupe diédral D_n pour un certain $n \geqslant 3$ (nous gardons les Notation I.1.1 pour ce qui concerne les groupes diédraux et leurs sous-groupes). À toute représentation modulaire diédrale on peut associer un corps quadratique, noté K, qui est le sous-corps de $\overline{\mathbb{Q}}$ fixé par le noyau du caractère

$$\mathcal{G}_{\mathbb{Q}} \xrightarrow{\mathbf{P}\rho} D_n \longrightarrow \Delta$$

où on a encore noté $\mathbf{P}\rho$ la composition de $\mathbf{P}\rho$ avec un isomorphisme choisi $\operatorname{Im}\mathbf{P}\rho \cong D_n$.

Le point de départ de plusieurs études présentées dans ce mémoire est l'énoncé suivant, dû à Deligne[3] :

Théorème (voir [DS74, Théorème 6.1]). *Soit $f \in M_k\big(\Gamma_0(N), \varepsilon\big)$ une forme modulaire de poids $k \geqslant 2$, niveau N et caractère ε. Supposons qu'elle ne soit pas identiquement nulle et qu'elle soit fonction propre des T_ℓ pour $\ell \nmid N$, avec pour valeurs propres la collection $\{a_\ell\}$. Soit L une extension finie de $\mathbb{Q}$ contenant les a_ℓ et les valeurs $\varepsilon(\ell)$. Soit finalement $\mathfrak{p}$ une place finie de L, de caractéristique résiduelle p, et soit $L_{\mathfrak{p}}$ le complété de L en $\mathfrak{p}$. Il existe une représentation galoisienne semi-simple*

$$\rho_{f,\mathfrak{p}}\colon \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(L_{\mathfrak{p}}),$$

unique à isomorphisme près, qui est non-ramifiée en dehors de Np et telle que, pour tout premier $\ell \nmid Np$,

$$\operatorname{Tr}\big(\rho_{f,\mathfrak{p}}\operatorname{Frob}_{\mathcal{G}_{\mathbb{Q}}}(\ell)\big) = a_\ell \qquad \textit{et} \qquad \det\big(\rho_{f,\mathfrak{p}}\operatorname{Frob}_{\mathcal{G}_{\mathbb{Q}}}(\ell)\big) = \varepsilon(\ell)\ell^{k-1}.$$

Les valeurs propres d'une forme f comme dans l'énoncé du théorème précédent sont des entiers algébriques, ce qui montre qu'elle est une forme $\mathfrak{p}$-entière pour tout $\mathfrak{p}$, au sens de [DS74, §6.6]. On a donc le théorème suivant :

Théorème ([DS74, Théorème 6.7]). *Avec les notations et hypothèses du théorème précédent, supposons en plus que les valeurs propres $\{a_\ell\}$ ne soient pas toutes nulles modulo $\mathfrak{p}$. Dénotons par $\mathbb{F}_f$ le sous-corps de $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_{L_{\mathfrak{p}}}/\mathfrak{p}$ engendré par les $a_\ell \pmod{\mathfrak{p}}$ et par les valeurs $\varepsilon(\ell) \pmod{\mathfrak{p}}$, pour $\ell \nmid Np$. Il existe une représentation galoisienne modulaire semi-simple*

$$\overline{\rho_{f,\mathfrak{p}}}\colon \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_f),$$

qui est non-ramifiée en dehors de Np et telle que, pour tout premier $\ell \nmid Np$,

$$\operatorname{Tr}\big(\overline{\rho_{f,\mathfrak{p}}}\operatorname{Frob}_{\mathcal{G}_{\mathbb{Q}}}(\ell)\big) \equiv a_\ell \pmod{\mathfrak{p}} \quad \textit{et} \quad \det\big(\overline{\rho_{f,\mathfrak{p}}}\operatorname{Frob}_{\mathcal{G}_{\mathbb{Q}}}(\ell)\big) \equiv \varepsilon(\ell)\ell^{k-1} \pmod{\mathfrak{p}}.$$

Remarque I.2.2. Comme la notation le suggère, la représentation $\overline{\rho_{f,\mathfrak{p}}}$ peut être réalisée en choisissant d'abord un $\mathcal{O}_{L_{\mathfrak{p}}}$-réseau dans l'espace de la représentation $\rho_{f,\mathfrak{p}}$, puis en le réduisant modulo $\mathfrak{p}$; et, finalement, en semi-simplifiant.

3. Dans l'introduction de [DS74], écrit cinq ans après la parution de [Del68], on lit : « Signalons que nous avons utilisé en un point essentiel (§6, th. 6.1) des résultats démontrés par l'un de nous (P. Deligne), mais dont aucune démonstration complète n'a encore été publiée ; en attendant une telle publication (ainsi que celle du SGA5, dont ils dépendent), nous demandons au lecteur de bien vouloir les admettre. ». Ainsi, nous préférons renvoyer à [DS74, Théorème 6.1] plutôt qu'à [Del68]. Que les instruments illustrés au chapitre III permettent une vérification formelle de ces résultats à court terme est probablement optimiste.

Observons maintenant qu'à différence de $\rho_{f,\mathfrak{p}}$, qui est déterminée par la collection $\{a_\ell\}$, la représentation modulaire $\rho_{f,\mathfrak{p}}$ ne dépend que de la collection $\{a_\ell \pmod{\mathfrak{p}}\}$. En particulier, si $f \in M_k\big(\Gamma_0(N),\varepsilon\big)$ et $f' \in M_{k'}\big(\Gamma_0(N'),\varepsilon'\big)$ sont deux formes modulaires qui satisfont aux hypothèses du théorème, et telles que pour un certain premier $\mathfrak{p}$ de caractéristique résiduelle p on a les congruences

$$a_\ell \equiv a'_\ell \pmod{\mathfrak{p}} \qquad \text{et} \qquad \varepsilon(\ell) \equiv \varepsilon'(\ell) \pmod{\mathfrak{p}} \tag{I.2.1}$$

pour tout $\ell \nmid Np$, alors $\overline{\rho_{f,\mathfrak{p}}} = \overline{\rho_{f',\mathfrak{p}}}$. La question que nous abordons dans [BN18] est motivée par l'observation précédente, dans l'optique de comprendre quelles formes modulaires donnent lieu à une représentation modulaire fixée. Avant de préciser la question, nous aurons besoin de la définition suivante :

Définition I.2.3. Soit ν un caractère de Dirichlet non-trivial. Une forme parabolique nouvelle $f \in S_k^{\mathrm{new}}\big(\Gamma_0(N),\varepsilon\big)$ est dite à multiplication complexe (ou CM) par ν si on l'égalité

$$a_\ell = \nu(\ell)a_\ell$$

pour un ensemble de premiers de densité 1. Si c'est le cas, ν est un caractère impair d'ordre 2, de sorte que $\bar{\mathbb{Q}}^{(\operatorname{Ker}\nu)} = K$ est quadratique imaginaire (voir [Rib77, §3, Remarks] pour la première propriété, et [Rib77, Proposition 4.4 et Théorème 4.5] pour la deuxième). On dit aussi que f a multiplication complexe par le corps K.

Un argument de représentations de groupes finis (voir [Rib77, Proposition 4.4]) montre que si f est une forme nouvelle qui a CM par un corps quadratique imaginaire K, la restriction $\rho_{f\,|\mathcal{G}_K}$ a image abélienne, et en fait la représentation ρ_f est l'induite de $\mathcal{G}_K$ à $\mathcal{G}_\mathbb{Q}$ d'un caractère. Pour tout premier $\mathfrak{p}$, ces propriétés se transportent à la représentation modulaire $\overline{\rho_{f,\mathfrak{p}}}$ de sorte que, une fois pris le quotient par le centre, l'image est un groupe diédral. Avec les notations introduites précédemment, on vient d'obtenir la

Proposition. *Soit $f \in S_k^{\mathrm{new}}\big(\Gamma_0(N),\varepsilon\big)$ une forme parabolique nouvelle qui a CM par le corps K. Alors la représentation modulaire $\overline{\rho_{f,\mathfrak{p}}}$ est diédrale.*

On voit donc qu'avoir multiplication complexe, qui est un prédicat sur la forme « en caractéristique 0 », a comme conséquence d'être diédrale, ce qui est une propriété « résiduelle » de la représentation modulaire. D'ailleurs, il arrive parfois qu'une forme modulaire *qui n'a pas de multiplication complexe* ait une représentation modulaire qui, à certains premiers $\mathfrak{p}$, est diédrale. C'est le cas, par exemple, de la représentation ρ_Δ associée à la forme parabolique « de Ramanujan »

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots \in S_{12}^{\mathrm{new}}\big(\Gamma_0(1)\big) :$$

elle n'est pas CM mais la représentation $\overline{\rho_{\Delta,23}}$ est diédrale. Un autre exemple est fourni par la courbe elliptique

$$\mathsf{E} : Y^2 + Y = X^3 - X^2 - 18507X - 989382$$

notée 65533.a1 dans [LMF13] : elle (ou la forme f_E qui lui est associée) n'a pas de multiplication complexe, pourtant $\overline{\rho_{f_\mathsf{E},7}}$ est diédrale. Notre objectif est d'« expliquer » ces phénomènes par des congruences, au sens suivant : si une forme f n'a pas CM mais

est congrue, modulo $\mathfrak{p}$, à une autre forme g qui a CM, la représentation modulaire $\overline{\rho_{f,\mathfrak{p}}}$ coïncide avec $\overline{\rho_{g,\mathfrak{p}}}$ et sera forcément diédrale. Il est donc naturel de comprendre si le fait que la représentation associée à une forme *sans multiplication complexe* se réduise, modulo un premier $\mathfrak{p}$, à une représentation diédrale est toujours dû à une congruence $f \equiv g^{\mathrm{CM}} \pmod{\mathfrak{p}}$ pour une forme g^{CM} convenable qui a CM.

La réponse que nous donnons dans [BN18, Théorème 1.1] est positive. Il devient alors intéressant de comprendre si la forme g^{CM} est unique et, sinon, d'établir l'existence de choix « optimaux » pour de telles formes CM. Cette optimalité s'exprime en termes du poids $k(\pi)$, du caractère $\varepsilon(\pi)$ et du niveau $N(\pi)$ associés par Serre à une représentation galoisienne modulaire π. Nous ne rappelons pas la définition de ces objets ici, en renvoyant plutôt a [Ser87, §2 et §1.3] pour les deux premiers ; le niveau $N(\pi)$ est simplement la partie première à p du conducteur de Artin de π (voir *ibid.* §1.2).

Le résultat que nous obtenons est le suivant :

Théorème I.2.4 ([BN18, Théorème 1.1]). *Soit π une représentation galoisienne modulaire diédrale modulo p. Avec les notations précédentes, on suppose* :

a) *K est quadratique imaginaire* ;

b) *$2 \leq k(\pi) \leq p-1$ et $p \geqslant 5$.*

Alors π provient d'une forme nouvelle g^{CM} à multiplication complexe par le corps K, de poids $k(\pi)$ et de niveau

$$N' = \begin{cases} N(\pi) & \text{si } p \text{ est non ramifié dans } K \text{ ;} \\ p^2 N(\pi) & \text{si } p \text{ est ramifié dans } K. \end{cases}$$

De plus, on a les propriétés suivantes :

1. *si p est ramifié dans K, alors $p \in \{2k(\pi)-1,\ 2k(\pi)-3\}$;*
2. *si $\varepsilon(\pi)$ est trivial, alors la forme à multiplication complexe peut être choisie de caractère trivial et de niveau divisant N'.*

La démonstration du Théorème I.2.4 repose principalement sur la théorie du corps de classes pour le corps quadratique imaginaire K, qui permet de construire, en partant de π, un Größencharakter aux propriétés galoisiennes convenables (voir [BN18, Proposition 2.1]). En appliquant une construction classique due à Hecke et à Shimura (voir [Hec59, p. 717], [Shi71, Lemma 3] et [Shi72, p. 138]) on obtient une série qui est le développement de Fourier d'une forme à multiplication complexe g^{CM}.

Un corollaire du Théorème I.2.4, appliqué à $\overline{\rho_{f,\mathfrak{p}}}$, est le critère de congruence énonce auparavant :

Corollaire I.2.5. *Soit $f \in S_k^{\mathrm{new}}\big(\Gamma_0(N), \varepsilon\big)$ une forme parabolique nouvelle de poids $k \geqslant 2$ et soit $\mathfrak{p}$ un premier du corps des coefficients de f tel que $\overline{\rho_{f,\mathfrak{p}}}$ est diédrale. Soit p la caractéristique résiduelle de $\mathfrak{p}$ et supposons $p \geqslant 5$ ainsi que $p \nmid N$. Il existe alors une forme à multiplication complexe $g^{\mathrm{CM}} \in S_{k'}^{\mathrm{new}}\big(\Gamma_0(N'), \varepsilon'\big)$, où le poids k', le niveau N' et le caractère ε' peuvent être choisis comme dans le Théorème I.2.4, et une extension $\mathfrak{P}$ de $\mathfrak{p}$ à $\bar{\mathbb{Q}}$, telle que $f \equiv g^{\mathrm{CM}} \pmod{\mathfrak{P}}$.*

Démonstration. Le corps K associé à $\overline{\rho_{f,\mathfrak{p}}}$ est imaginaire : cela provient du fait que la représentation $\rho_{f,\mathfrak{p}}$ est toujours impaire, et que $p \neq 2$. Il reste à montrer les inégalités $2 \leqslant k(\overline{\rho_{f,\mathfrak{p}}}) \leqslant p-1$. Pour les obtenir, observons que [Kat73, Theorem 1.7.1] nous assure

que la forme modulaire $\overline{f}$ à coefficients dans $\overline{\mathbb{F}_p}$ est encore du même poids k que la forme f de départ. En outre, $\overline{\rho_{f,\mathfrak{p}}}$ coïncide avec la représentation $\rho_{\overline{f}}$ et on peut lui appliquer les théorèmes [Edi92, Theorem 2.5 ou Theorem 2.6] (selon que la forme soit ordinaire ou non) : on déduit le résultat voulu sur le poids de Serre par définition de ce dernier (voir [Ser87, §2]). □

En appliquant le Corollaire I.2.5 à la forme Δ et au premier 23, nous trouvons une forme $g^{\mathrm{CM}} \in S_{12}\big(\Gamma_0(23^2)\big)$ telle que $\Delta \equiv g^{\mathrm{CM}} \pmod{\mathfrak{p}_{23}}$ où $\mathfrak{p}_{23}$ est l'unique premier de $\mathcal{O}_L$ ramifié au-dessus de 23 : ici, L est le corps de coefficients de g^{CM}, de polynôme minimal $X^3 - 6X - 3$ (pour les détails, voir le fichier `DeltaMod23.gp` disponible sur la page de [BN18]). On peut en outre montrer que le niveau est optimal : en effet, il n'existe pas de forme à multiplication complexe de poids 12 et de niveau 1 ou 23 qui soit congrue à Δ modulo 23.

En spécialisant le Corollaire I.2.5 en poids $k = 2$ nous obtenons l'application suivante concernant les variétés abéliennes de type GL_2 (nous renvoyons à [Rib92] pour les généralités) :

Corollaire I.2.6 ([BN18, Corollaire 1.3]). *Soit $\mathsf{A}/\mathbb{Q}$ une variété abélienne de type GL_2 de conducteur N_{A} et $\mathfrak{p}$ une place finie de $E = \mathrm{End}_{\mathbb{Q}}(\mathsf{A}) \otimes \mathbb{Q}$ au-dessus du premier $p \geqslant 5$ ne divisant pas N_{A}. On suppose que l'image de $\overline{\rho_{\mathsf{A},\mathfrak{p}}}$ est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$. Alors, $\overline{\rho_{\mathsf{A},\mathfrak{p}}}$ provient d'une forme nouvelle à multiplication complexe de poids 2 et de niveau $N(\overline{\rho_{\mathsf{A},\mathfrak{p}}})$ (divisant N_{A}) qui, de plus, est de caractère trivial lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbb{Q}$.*

Le Corollaire I.2.6 est une généralisation en dimension quelconque de [Che02, Theorem 1.6], valable pour les courbes elliptiques. Il avait essentiellement déjà été obtenu par Nualart [Nua11, Theorem 1] et justifie [GP12, Remark4.4].

II

Théorie d'Iwasawa

Je rassemble dans ce chapitre certains résultats en théorie d'Iwasawa : pour les groupes de classes dans des « fausses » $\mathbb{Z}_p$-extension de type diédral au §II.1 ; pour la représentation galoisienne associée à une courbe elliptique aux §§II.2–II.3 ; et pour les familles de formes modulaires non-ordinaires au §II.4. Les aspects abordés relèvent du côté « algébrique » de la théorie d'Iwasawa et il ne sera pas question de fonctions L p-adiques dans ce chapitre.

Travaux présentés :

[CN22] L. Caputo & F. A. E. Nuccio Mortarino Majno di Capriglio – « Cohomology of normic systems and fake $\mathbb{Z}_p$-extensions » (2021), https://arxiv.org/abs/0807.1135.

[NS23] F. A. E. Nuccio Mortarino Majno di Capriglio & Sujatha R. – « Residual supersingular Iwasawa theory and signed Iwasawa invariants », *Rend. Semin. Mat. Univ. Padova* (2023), no. 149, p. 83–129.

[KNS24] D. Kundu, F. A. E. Nuccio Mortarino Majno di Capriglio & Sujatha R. – « Structure of fine Selmer groups in abelian p-adic Lie extensions », *Osaka J. Math.* **61** (2024), no. 1, à paraître – https://hal-cnrs.archives-ouvertes.fr/hal-03769801.

[NOR23] F. A. E. Nuccio Mortarino Majno di Capriglio, T. Ochiai & J. Ray – « A formal model of Coleman families and applications to Iwasawa invariants », *Ann. Math. Québec* (2023), à paraître – https://cnrs.hal.science/hal-03355637v3.

II.1 Cohomologie des systèmes normiques et fausses $\mathbb{Z}_p$-extensions

avec L. Caputo

Iwasawa prouva en 1958 dans [Iwa58] — et puis en forme plus générale et structurée dans [Iwa73a], en s'appuyant sur [Ser60] — le célèbre théorème suivant, dans lequel nous gardons les notations introduites au §I.1 :

Théorème (Iwasawa). *Soit L un corps de nombres et soit p un nombre premier. Étant donnée une chaine d'extensions galoisiennes*

$$L = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \cdots \subseteq L_\infty = \bigcup_{n\geqslant 0} L_n \tag{II.1.1}$$

telle que $[L_n : L_{n-1}] = p$ pour tout $n \geqslant 1$ et $\mathrm{Gal}(L_\infty/L) \cong \mathbb{Z}_p$, il existe trois entiers $\mu, \lambda \in \mathbb{Z}_{\geqslant 0}$ et $\nu \in \mathbb{Z}$ tels que

$$v_p(h_{L_n}) = \mu p^n + \lambda n + \nu \qquad \text{pour tout } n \gg 0. \tag{II.1.2}$$

On voit donc que la croissance du p-sous-groupe de Sylow du groupe de classes dans une extensions à groupe de Galois $\mathbb{Z}_p$ est contrôlée par une formule explicite qui comporte une partie exponentielle, une partie linéaire, et une partie constante. Bien que dans le premier travail [Iwa58] la formule n'eût été prouvée que pour $L = \mathbb{Q}(\mu_p)$ avec $L_n = \mathbb{Q}(\mu_{p^{n+1}})$ (pour p impair) — où μ_{p^m} dénote le groupe des racines p^m-ièmes de l'unité dans $\bar{\mathbb{Q}}$ — aucune hypothèse n'est en fait nécessaire ni sur le corps de base ni sur la définition explicite des corps L_n. Afin de considérer des contextes plus généraux, fixons une définition : une tour d'extensions comme dans (II.1.1) est appelée une $\mathbb{Z}_p$-extension ; par correspondance de Galois, pour tout $m \geqslant n \geqslant 0$ l'extension L_m/L_n est en fait galoisienne, à groupe de Galois cyclique d'ordre p^{m-n}, et on a $[L_n : L] = p^n$ pour tout $n \geqslant 0$. Il est facile de montrer que le corps $\mathbb{Q}$ des rationnels ne possède qu'une unique $\mathbb{Z}_p$-extension pour tout premier p : lorsque p est impair, on prend [1] pour $\mathbb{Q}_n$ le sous-corps (totalement réel) du corps cyclotomique $\mathbb{Q}(\mu_{p^{n+1}})$ qui est fixé par le sous-groupe d'ordre $(p-1)$ de $\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}) = \left(\mathbb{Z}/p^{n+1}\right)^\times \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/p^n$; lorsque $p = 2$ on prend pour $\mathbb{Q}_n$ le sous-corps totalement réel maximal (qui est d'indice 2) de $\mathbb{Q}(\mu_{2^{n+2}})$. Cette extension est la $\mathbb{Z}_p$-extension *cyclotomique* de $\mathbb{Q}$, notée $\mathbb{Q}_{\mathrm{cyc}} = \bigcup_n \mathbb{Q}_n$: tout corps de nombres L possède donc une extension cyclotomique L_{cyc} pour chaque p, définie par $L_n = L\mathbb{Q}_n$ et telle que $L_{\mathrm{cyc}} = L\mathbb{Q}_{\mathrm{cyc}}$. Un argument facile de théorie du corps de classes globale montre par ailleurs qu'un corps de nombres qui admet r_2 paires de plongements complexes conjugués possède au moins $(r_2 + 1)$ $\mathbb{Z}_p$-extensions linéairement indépendantes, mais l'extension cyclotomique joue un rôle particulier. En effet, Iwasawa lui-même proposa une conjecture remarquable, inspirée du comportement des points rationnels de la jacobienne d'une courbe sur un corps fini le long de l'unique $\mathbb{Z}_p$-extension de celui-ci :

Conjecture $\mu = 0$ d'Iwasawa. *Pour tout nombre premier p et tout corps de nombres L, l'invariant μ qui apparaît dans la formule (II.1.2) s'annule pour $L_\infty = L_{\mathrm{cyc}}$.*

Cette conjecture est un théorème dû à Ferrero et Washington (voir [FW79]) dans le cas où le corps L est une extension abélienne [2]. Il est par ailleurs bien connu qu'elle est fausse en dehors du cadre cyclotomique, comme montré déjà par Iwasawa dans [Iwa73b].

La stratégie déployée par Iwasawa pour démontrer la formule (II.1.2) est de nature algébrique. Pour la détailler, nous aurons besoin de la définition suivante :

1. Le conflit de notation entre le symbole $\mathbb{Q}_n$ qui indique le n-ième étage de la tour p-cyclotomique de $\mathbb{Q}$ et le symbole $\mathbb{Q}_p$ pour indiquer le corps des nombres p-adique est courant en théorie d'Iwasawa et ne pose normalement aucun problème : nous nous y conformons.
2. On entend par ceci que $L/\mathbb{Q}$ est galoisienne et $\mathrm{Gal}(L/\mathbb{Q})$ est abélien.

Définition II.1.1. Soit Γ un groupe profini : son algèbre d'Iwasawa est le complété

$$\Lambda(\Gamma) = \varprojlim_N \mathbb{Z}_p[\Gamma/N]$$

pour N parcourant les sous-groupes distingués d'indice fini de Γ, munie de la topologie de la limite projective, où la topologie sur chaque $\mathbb{Z}_p[\Gamma/N]$ est celle p-adique. Pour tout sous-groupe d'indice fini N, l'idéal d'augmentation $\mathfrak{I}_N$ est le noyau

$$\mathfrak{I}_N = \mathrm{Ker}\big(\Lambda(\Gamma) \longrightarrow \mathbb{Z}_p[\Gamma/N]\big).$$

On peut montrer que lorsque $\Gamma \cong \mathbb{Z}_p$, l'algèbre $\Lambda(\Gamma)$ est un anneau local régulier de dimension de Krull égale à 2 : en particulier, le seul idéal premier de hauteur supérieure ou égale à 2 est l'idéal maximal $\mathfrak{m}$ et donc les modules pseudo-nuls (au sens de [Bou06, Chapitre VII, §4, no. 4, Définition 2]) sont finis car $\Lambda(\Gamma)/\mathfrak{m} \cong \mathbb{F}_p$. Le théorème de structure (voir [Bou06, Chapitre VII, §4, no. 4, Théorèmes 4 et 5]) assure que tout $\Lambda(\Gamma)$-module M de type fini intervient dans une suite exacte

$$0 \longrightarrow K \longrightarrow M \longrightarrow \Lambda(\Gamma)^r \oplus \bigoplus_{i=1}^{s} \Lambda(\Gamma)/\mathfrak{r}_i^{a_i} \oplus \bigoplus_{i=1}^{e} \Lambda(\Gamma)/p^{b_i} \longrightarrow K' \longrightarrow 0 \tag{II.1.3}$$

où $r = \mathrm{rk}_{\Lambda(\Gamma)} M \geqslant 0$, $a_i, b_i \geqslant 1$; où les $\mathfrak{r}_i \subseteq \Lambda(\Gamma)$ sont des idéaux premiers principaux de hauteur 1 différents de $p\Lambda(\Gamma)$, donc tels que $(p, \mathfrak{r}_i)$ est d'indice fini dans $\Lambda(\Gamma)$; et où K, K' sont des modules pseudo-nuls, donc finis. En particulier, chaque $\Lambda(\Gamma)/\mathfrak{r}_i$ est un $\mathbb{Z}_p$-module libre de rang d_i, de sorte que $\mathrm{rk}_{\mathbb{Z}_p} \Lambda(\Gamma)/\mathfrak{r}_i^{a_i} = a_i d_i$. Supposons maintenant que le $\Lambda(\Gamma)$-module de type fini M soit en plus de torsion : dans (II.1.3) on a alors $r = 0$ et les invariants d'Iwasawa de M sont définis par les formules

$$\lambda_M = \sum_{i=1}^{s} a_i d_i \qquad \text{et} \qquad \mu_M = \sum_{i=1}^{e} b_i.$$

Leur rôle provient de l'observation suivante : si pour tous les idéaux $\mathfrak{r}_i$ qui interviennent dans (II.1.3) et tout idéal d'augmentation $\mathfrak{I}_{\Gamma_{\mathrm{cyc}}^{p^n}} = \mathfrak{I}_n$ ($n \geqslant 0$), l'idéal $(\mathfrak{r}_i, \mathfrak{I}_n)$ est d'indice fini dans $\Lambda(\Gamma)$, il existe une constante ν_M telle que

$$\Big|\bigoplus_{i=1}^{n} \Lambda(\Gamma)/(\mathfrak{r}_i^{a_i}, \mathfrak{I}_n)\Big| = p^{\lambda_M n + \nu_M}$$

et

$$\Big|\bigoplus_{i=1}^{e} \Lambda(\Gamma)/(p^{b_i}, \mathfrak{I}_n)\Big| = p^{\mu_M p^n}.$$

Si donc on demande au module de type fini et de torsion M que tous les idéaux $(\mathrm{Ann}_{\Lambda(\Gamma)}(M), \mathfrak{I}_n)$ soient d'indice fini pour $n \geqslant 0$, on obtient — grâce à la finitude de K et de K' dans (II.1.3) — l'estimation

$$|M/\mathfrak{I}_n M| = p^{\mu_M p^n + \lambda_M n + \nu}. \tag{II.1.4}$$

La preuve donnée par Iwasawa de la formule (II.1.2) consiste à chercher un $\Lambda(\Gamma)$-module X_L qui satisfait aux conditions suivantes :

a) X_L est de type fini et de torsion ;

b) l'indice de $(\mathrm{Ann}_{\Lambda(\Gamma)}(X_L), \mathfrak{I}_n)$ dans $\Lambda(\Gamma)$ est fini pour tout $n \geqslant 0$;

c) pour $n \gg 0$ on a un isomorphisme $X_L/\mathfrak{I}_n X_L \cong \mathcal{C}\ell_{L_n} \otimes \mathbb{Z}_p$.

Grâce à l'argument précédent, l'existence d'un tel module entraînerait directement la formule (II.1.2). Le module considéré par Iwasawa est

$$X_L = \varprojlim_n \left(\mathcal{C}\ell_{L_n} \otimes \mathbb{Z}_p\right)$$

où la limite projective est prise par rapport aux normes $\mathrm{N}_{L_m/L_n} : \mathcal{C}\ell_{L_m} \to \mathcal{C}\ell_{L_n}$. Le fait que X_L soit un $\Lambda(\Gamma)$-module est immédiat car chaque $\mathcal{C}\ell_{L_n} \otimes \mathbb{Z}_p$ est un $\mathbb{Z}_p[\mathrm{Gal}(L_n/L)]$-module, et il est facile de voir qu'il est de type fini ; qu'il soit de torsion est déjà plus fin, et provient de la théorie du corps de classes globale. Les points b) et c) sont *faux* en général, mais un petit argument de dévissage (détaillé, par exemple, dans [Ser60, §§4–6]) permet néanmoins de conclure.

Fixons désormais un premier impair $p \geqslant 3$. Dans le travail [CN22] nous considérons une variation prodiédrale et non galoisienne d'une $\mathbb{Z}_p$-extension, dans le but de généraliser la formule (II.1.2) au delà du cas galoisien. La définition de départ est la suivante :

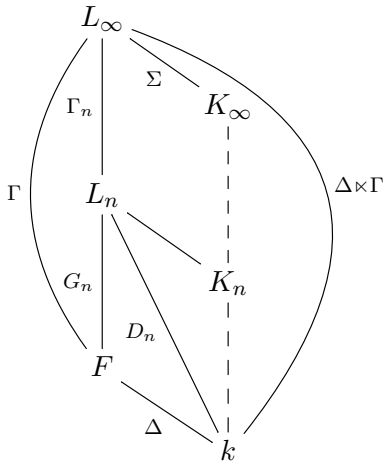
Définition II.1.2 ([CN22, Definition 4.1]). Soit F un corps de nombres et soit L_∞/F une $\mathbb{Z}_p$-extension. Supposons qu'il existe un sous-corps $k \subseteq F$ tel que, pour tout $n \geqslant 0$, L_n/k est une extension galoisienne à groupe de Galois diédral D_{p^n} d'ordre $2p^n$. Pour $n \geqslant 0$, soit K_n un sous-corps de L_n d'indice 2, choisi de façon à que $K_{n-1} \subseteq K_n$ pour tout $n \geqslant 1$, et soit $K_\infty = \bigcup K_n$. L'extension $K_\infty/K_0 = k$ est dite fausse $\mathbb{Z}_p$-extension de type diédral [3], et le corps F est l'extension quadratique normalisante de K_∞/k.

Remarque II.1.3. Les fausses $\mathbb{Z}_p$-extension de type diédral apparaissent naturellement dans le cadre des corps CM. On peut en effet montrer que le sous-corps totalement réel maximal F^+ d'un corps CM F admet au moins [4] r_2 fausses $\mathbb{Z}_p$-extensions, où r_2 dénote comme précédemment le nombre de paires de plongements complexes conjugués de F. Un exemple particulièrement explicite est fourni par les corps quadratiques imaginaires, qui sont des corps CM dont le sous-corps totalement réel maximal est $\mathbb{Q}$. Un tel corps quadratique imaginaire F admet une unique $\mathbb{Z}_p$-extension F_{anti} qui est galoisienne mais non abélienne sur $\mathbb{Q}$: on l'appelle la $\mathbb{Z}_p$-extension anticyclotomique de F. Pour une telle extension, on peut choisir $k = \mathbb{Q}$ dans la Définition II.1.2 pour obtenir une fausse $\mathbb{Z}_p$-extension de type diédral de $\mathbb{Q}$, ce qui fournit une infinité d'exemples de telles extensions.

Plaçons-nous dans le contexte de la Définition II.1.2 : soit $\Gamma = \mathrm{Gal}(L_\infty/F)$ et écrivons Γ_n pour le sous-groupe Γ^{p^n} ; adaptons les Notations I.1.1 en remplaçant les indices p^n par l'indice n, par simplicité, donc en dénotant D_n (*resp.* G_n) le groupe D_{p^n} (*resp.* G_{p^n}).

3. Nous traduisons ainsi l'expression *fake $\mathbb{Z}_p$-extension of dihedral type* de [CN22].
4. Et en fait *exactement*, si la conjecture de Leopoldt (qui sera rappelée sous peu) est vraie pour F.

On obtient alors le diagramme suivant de corps :



(II.1.5)

Les extensions K_m/K_n ne sont pas galoisiennes pour $m \geqslant n \geqslant 0$ et les techniques esquissées plus haut de théorie d'Iwasawa ne s'appliquent pas pour obtenir une formule de croissance du nombre de classes dans l'extension K_∞/k : par exemple, la limite

$$X_{\text{fake}} = \varprojlim \mathcal{C}\ell_{K_n} \otimes \mathbb{Z}_p$$

n'est pas un $\Lambda(\Gamma)$-module. Afin d'obtenir une telle formule, nous nous appuyons plutôt sur les résultats du §I.1 qui relient les ordres $|\mathcal{C}\ell_{K_n} \otimes \mathbb{Z}_p|$ aux ordres $|\mathcal{C}\ell_{L_n} \otimes \mathbb{Z}_p|$, pour lesquels la formule (II.1.2) est disponible.

En prenant les valuations p-adiques dans le Théorème I.1.3 on voit que les valuations p-adiques des nombres de classes dans (II.1.5) sont reliées, pour tout $n \geqslant 0$, par la formule

$$2v_p(h_{K_n}) = v_p(h_{L_n}) + 2v_p(h_k) - v_p(h_F) + v_p\big(|\widehat{H}^{-1}(D_n, \mathcal{O}_{L_n}^\times)|\big) - v_p\big(|\widehat{H}^0(D_n, \mathcal{O}_{L_n}^\times)|\big);$$

en la combinant avec la formule (II.1.2) on obtient l'existence de trois invariants $\mu_{\text{Iw}}, \lambda_{\text{Iw}}, \nu_{\text{Iw}}$ tels que, pour tout $n \gg 0$,

$$2v_p(h_{K_n}) = \mu_{\text{Iw}} p^n + \lambda_{\text{Iw}} n + \nu_{\text{Iw}} + v_p\big(|\widehat{H}^{-1}(D_n, \mathcal{O}_{L_n}^\times)|\big) - v_p\big(|\widehat{H}^0(D_n, \mathcal{O}_{L_n}^\times)|\big) \tag{II.1.6}$$

(on a intégré les constantes $2v_p(h_k)$ et $-v_p(h_F)$ dans le terme ν_{Iw}). Le problème devient donc celui d'établir une formule asymptotique pour l'ordre des groupes de cohomologie $\widehat{H}^{-1}(D_n, \mathcal{O}_{L_n}^\times)$ et $\widehat{H}^0(D_n, \mathcal{O}_{L_n}^\times)$ lorsque $n \to \infty$. Observons à nouveau que ces groupes ne sont pas munis d'une structure de G_n-module non-triviale et donc les techniques algébriques usuelles en théorie d'Iwasawa, qui suggèrent d'étudier le comportement d'une suite de groupes finis en les réalisant comme quotients d'un $\Lambda(\Gamma)$-module, ne s'appliquent pas.

La contribution principale du travail [CN22] est la définition d'un cadre catégorique convenable où une étude asymptotique de groupes finis puisse être menée. Le point de départ est l'observation que les groupes de cohomologie $\widehat{H}^{-1}(D_n, \mathcal{O}_{L_n}^\times)$ et $\widehat{H}^0(D_n, \mathcal{O}_{L_n}^\times)$ constituent, pour $n \geqslant 0$, à la fois un système inductif par rapport à des morphismes d'inflation et un système projectif par rapport à des morphismes induits par les normes.

Comme l'absence d'une action galoisienne ne permet pas de récupérer, pour n donné, le groupe $\widehat{H}^i(D_n, \mathcal{O}_{L_n}^\times)$ $(i = 0, -1)$ seulement à partir de la connaissance des limites

$$\varinjlim \widehat{H}^i(D_n, \mathcal{O}_{L_n}^\times) \qquad \text{ou} \qquad \varprojlim \widehat{H}^i(D_n, \mathcal{O}_{L_n}^\times),$$

il est nécessaire de travailler avec des *systèmes doubles* plutôt que de passer aux limites. Le désavantage devient alors que travailler « à groupes finis près » (la notion algébrique qui correspond à l'aspect « asymptotique » de la formule (II.1.6)) n'a plus aucun sens, du moment que chaque groupe de ces systèmes est fini et est donc « trivial à un groupe fini près ».

Pour pallier ce problème, nous définissons une catégorie $\mathbf{DS}_\Gamma^{\text{co.f.}-\text{g.}}$ formée de « systèmes doubles de groupes finis » avec une condition de finitude sur leurs limites inductives et montrons que pour $M_n \in \{\mathcal{O}_{L_n}^\times \otimes \mathbb{Z}_p, L_n^\times \otimes \mathbb{Z}_p, \mathbb{I}_{L_n} \otimes \mathbb{Z}_p, \mathbb{A}_{L_n}^\times \otimes \mathbb{Z}_p, \mathcal{C}_{L_n} \otimes \mathbb{Z}_p\}$ (avec les notations fixées dans (II.1.5)), les systèmes $\left(\widehat{H}^i(D_n, M_n)\right)_{n \geqslant 0}$, pour tout $i \in \mathbb{Z}$, sont des objets de cette catégorie. Le résultat principal de notre travail est la définition d'une sous-catégorie épaisse $\mathbf{B}_\Gamma^{\text{co.f.}-\text{g.}} \subseteq \mathbf{DS}_\Gamma^{\text{co.f.}-\text{g.}}$ par rapport à laquelle on peut considérer la catégorie quotient $\mathbf{DS}_\Gamma^{\text{co.f.}-\text{g.}}/\mathbf{B}_\Gamma^{\text{co.f.}-\text{g.}}$. Nous montrons que cette catégorie quotient est l'endroit naturel où traduire en termes algébriques les calculs asymptotiques du cardinal de groupes finis ; de plus, comme il s'agit d'une catégorie abélienne, nous disposons des techniques standard d'algèbre homologique. Nous obtenons, simplement par applications successives du lemme du serpent dans cette catégorie quotient, une formule « à la Iwasawa » qui contrôle la croissance des groupes de cohomologie de Tate des modules galoisiens apparaissant dans (II.1.5). En combinant ce résultat avec (II.1.6), nous obtenons le

Théorème II.1.4 ([CN22, Theorem 4.6 et Corollary 4.8]). *Soit K_∞/k une fausse $\mathbb{Z}_p$-extension de type diédral. Il existe trois constantes $\mu_{\text{fake}}, \nu_{\text{fake}} \in \mathbb{Z}[\frac{1}{2}], \lambda_{\text{fake}} \in \mathbb{Z}$ telles que*

$$v_p(h_{K_n}) = \mu_{\text{fake}} p^n + \lambda_{\text{fake}} n + \nu_{\text{fake}} \qquad \textit{pour tout } n \gg 0. \tag{II.1.7}$$

En outre, l'invariant λ_{fake} est encadré par les inégalités

$$\frac{\lambda_{\text{Iw}} + a}{2} \geqslant \lambda_{\text{fake}} \geqslant \frac{\lambda_{\text{Iw}} - b}{2}$$

où λ_{Iw} est l'invariant d'Iwasawa associé à la $\mathbb{Z}_p$-extension L_∞/F et a, b sont définis comme dans le Corollaire I.1.5.

Un tel résultat n'est pas entièrement nouveau. Dans le cas particulier où $F/\mathbb{Q}$ est galoisienne telle que $\text{Gal}(F/\mathbb{Q})$ est abélien d'exposant divisant $(p-1)$, et où $L_\infty/\mathbb{Q}$ est aussi galoisienne, le Théorème II.1.4 est un cas particulier de [Jau81a, Théorème 3]. Toutefois, a notre connaissance, notre travail est la première étude systématique de la croissance des groupes de cohomologie de Tate généraux dans les $\mathbb{Z}_p$-extensions.

Dans certains cas particuliers, nous pouvons améliorer les inégalités sur les invariants qui apparaissent dans (II.1.7). Pour énoncer ce résultat nous aurons besoin de la conjecture suivante :

Conjecture de Leopoldt. *Soit E un corps de nombres et soit r_2 le nombre de paires de plongements complexes conjugués de E. Le nombre de $\mathbb{Z}_p$-extensions linéairement indépendantes de E est égal à $r_2 + 1$. En particulier, tout corps totalement réel ne possède qu'une unique $\mathbb{Z}_p$-extension, qui est sa $\mathbb{Z}_p$-extensions cyclotomique.*

L'autre conjecture qui apparaît dans le corollaire suivant est la Conjecture de Gross : comme elle ne jouera aucun rôle dans le reste du mémoire, nous préférons renvoyer à [Gro81, Conjecture 1.15 and (1.21)] pour son énoncé précis. Nous nous contentons de mentionner que tant la Conjecture de Leopoldt que la Conjecture de Gross sont établies pour les corps abéliens (tels les corps quadratiques, par exemple).

Corollaire II.1.5 ([CN22, Corollary 4.14 et 4.18]). *Si F est un corps quadratique imaginaire et $L_\infty = F_{\mathrm{anti}}$ est sa $\mathbb{Z}_p$-extension anticyclotomique (voir* Remarque II.1.3*), on a*

$$\lambda_{\mathrm{fake}} = \begin{cases} \frac{\lambda_{\mathrm{Iw}}+1}{2} & \text{si } p \text{ est décomposé dans } F/\mathbb{Q}; \\ \\ \frac{\lambda_{\mathrm{Iw}}}{2} & \text{si } p \text{ n'est pas décomposé dans } F/\mathbb{Q}; \end{cases}$$

en particulier, λ_{Iw} est impair si p est décomposé dans $F/\mathbb{Q}$, et est pair sinon.

Plus généralement, soit F un corps CM de degré $[F:\mathbb{Q}] = 2d$. Supposons que $k = F^+$ soit son sous-corps totalement réel maximal, que p soit complètement décomposé dans $F/\mathbb{Q}$ et que $L_\infty/\mathbb{Q}$ soit galoisienne. Alors

$$\lambda_{\mathrm{fake}} \geqslant \frac{\lambda_{\mathrm{Iw}} + 1 - d}{2}.$$

Si, de plus, les conjectures de Leopoldt et de Gross sont vraies pour F, alors

$$\lambda_{\mathrm{fake}} \geqslant \frac{\lambda_{\mathrm{Iw}} + 2 - d}{2}.$$

Le résultat de parité pour l'invariant d'Iwasawa classique dans la $\mathbb{Z}_p$-extension anticyclotomique d'un corps quadratique imaginaire avait déjà été obtenu par Gillard dans [Gil76, Théorème 2 et Théorème 1–Corollaire] et par Carroll–Kisilevsky dans [CK82, Theorem 5]. Dans le même travail, ces derniers auteurs ont aussi prouvé une généralisation du Corollaire II.1.5 au delà du cas prodiédral mais seulement lorsque $\mathrm{Gal}(F/\mathbb{Q})$ est abélien d'exposant divisant $(p-1)$.

II.2 Théorie d'Iwasawa résiduelle et invariants d'Iwasawa signés

avec Sujatha R.

Dans cette section nous fixons un corps de nombres $L/\mathbb{Q}$ ainsi qu'un nombre premier impair $p \geqslant 3$. Étant donnée une courbe elliptique E/L, nous allons nous intéresser à la théorie d'Iwasawa cyclotomique de la représentation galoisienne p-adique attachée à E. On fait l'hypothèse de travail suivante :

La courbe elliptique E/L a bonne réduction à toute place de L divisant p.

Soit L_{cyc}/L la $\mathbb{Z}_p$-extension cyclotomique de L et notons L_n, pour $n \in \mathbb{N} \cup \{\mathrm{cyc}\}$, les sous-corps intermédiaires de $L_{\mathrm{cyc}}/L = L_0$. Le groupe de Galois $\mathrm{Gal}(L_{\mathrm{cyc}}/L)$ sera noté Γ_{cyc}. Comme au §I.2, on considère fixées des clôtures algébriques à la fois du corps $\mathbb{Q}$ et des différents corps p-adiques $\mathbb{Q}_p$, ce qui nous permet de dénoter sans ambiguïté par $\mathcal{G}_F$ le groupe de Galois absolu de tout corps F qu'on sera amené à considérer ; par simplicité on écrira $H^i(F,V)$ pour le i-ème groupe de cohomologie du groupe profini

$\mathcal{G}_F$ à coefficients dans un $\mathcal{G}_F$-module discret V. Étant donné un groupe abélien A et un entier n, indiquons par $A[n]$ les éléments de A de n-torsion,

$$A[n] = \{a \in A \text{ tels que } n \cdot a = 0\}.$$

Par petit abus de notation, nous écrirons $\mathsf{E}[p^k]$ et E, respectivement, pour dénoter les modules galoisiens $\mathsf{E}[p^k](\bar{\mathbb{Q}})$ et $\mathsf{E}(\bar{\mathbb{Q}})$.

Pour tout $n \geqslant 0$, et tout $k \geqslant 1$, considérons le groupe de Selmer associé à $\mathsf{E}[p^k]$:

$$\mathrm{Sel}(\mathsf{E}[p^k]/L_n) = \mathrm{Ker}\Big(H^1(L_n, \mathsf{E}[p^k]) \longrightarrow \bigoplus_v H^1(L_{n,v}, \mathsf{E})[p^\infty]\Big) \tag{II.2.1}$$

(pour v parcourant toutes les places non-archimédiennes de L_n). En partant de cette définition, on peut construire

(A) le groupe $\mathrm{Sel}(\mathsf{E}[p^\infty]/L_n)$, en prenant la limite inductive sur k des groupes définis dans (II.2.1), par rapport aux morphismes induits par $\mathsf{E}[p^k] \hookrightarrow \mathsf{E}[p^{k+1}]$;

(B) le groupe $\mathrm{Sel}(\mathsf{E}[p^k]/L_{\mathrm{cyc}})$, en prenant la limite inductive sur n des groupes définis dans (II.2.1), par rapport aux applications de restriction ;

(C) le dual de Pontryagin $\mathfrak{X}(\mathsf{E}[p^k]/L_n) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}(\mathsf{E}[p^k]/L_n), \mathbb{Q}_p/\mathbb{Z}_p)$, défini pour tout $n \in \mathbb{N} \cup \{\mathrm{cyc}\}$ et tout $1 \leqslant k \leqslant \infty$.

Nous renvoyons à l'article [Gre99] et à l'ouvrage [CS10] pour les généralités sur la cohomologie galoisienne des courbes elliptiques, notamment à [Gre99, Chapter 2] et à [CS10, Chapter 1].

Les groupes $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ jouent un rôle analogue au module X_L défini au §II.1 : en premier lieu, ils sont munis d'une structure de $\Lambda(\Gamma_{\mathrm{cyc}})$-modules et, en tant que tels, ils sont de type fini (voir [CS10, Lemma 2.4]). Leur structure est plus délicate, et on a le théorème suivant (sous l'hypothèse toujours en vigueur que la courbe ait bonne réduction au-dessus de p) :

Théorème (Mazur [Maz72], voir aussi [CS10, Theorem 2.6 et Theorem 2.7]). *Le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ est de torsion si et seulement si la réduction de E/L est ordinaire à toute place de L divisant p.*

Il suit du théorème de Mazur ci-dessus que, lorsque la réduction de E/L est ordinaire à toute place p-adique, le théorème de structure pour les $\Lambda(\Gamma_{\mathrm{cyc}})$-modules mentionné au §II.1 s'applique et on peut associer à $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ deux invariants d'Iwasawa $\mu_{\mathsf{E}/L}$ et $\lambda_{\mathsf{E}/L}$. Tout comme dans (II.1.4), ces invariants apparaissent dans une formule asymptotique qui contrôle la croissance de l'ordre du groupe de Tate–Shafarevich : dans le cas ordinaire et en supposant que $Ш(\mathsf{E}/L_n)[p^\infty]$ soit fini pour tout n, on a

$$v_p\big(|Ш(\mathsf{E}/L_n)|\big) = \mu_{\mathsf{E}/L} p^n + \lambda_{\mathsf{E}/L} n + \nu_{\mathsf{E}/L} \qquad \text{pour tout } n \gg 0 \tag{II.2.2}$$

pour un entier $\nu_{\mathsf{E}/L}$ indépendant de n (voir [Gre99, Theorem 1.10]). En outre, le fait que $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ soit un module de torsion donne un sens à la définition de sa *série caractéristique* et une Conjecture Principale reliant cette série caractéristique à une fonction L p-adique peut être formulée : nous n'aurons pas l'occasion de discuter ni de fonctions L p-adiques associées aux courbes elliptiques, ni de la Conjecture Principale, et nous renvoyons à [MSD74] et à [MTT86] pour une discussion détaillée.

Concentrons-nous maintenant sur le cas où la réduction de E/L est *supersingulière* à certaines places p-adiques dans L. Le théorème de Mazur cité précédemment montre que le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ n'est pas de torsion et l'approche classique pour en étudier la théorie d'Iwasawa à travers le théorème de structure pour les $\Lambda(\Gamma_{\mathrm{cyc}})$-modules n'est plus adaptée. Pour pallier ce problème, Kobayashi définit dans [Kob03] (en s'appuyant, entre autre, sur les travaux de Perrin-Riou, voir [PR93]) des variants « signés » du groupe de Selmer (et de son dual), dans le cas où $L = \mathbb{Q}$. Pour tout $n \in \mathbb{N} \cup \{\mathrm{cyc}\}$ il définit deux sous-$\Lambda(\Gamma_{\mathrm{cyc}})$-modules

$$\mathrm{Sel}^+(\mathsf{E}[p^\infty]/\mathbb{Q}_n) \subseteq \mathrm{Sel}(\mathsf{E}[p^\infty]/\mathbb{Q}_n) \qquad \text{et} \qquad \mathrm{Sel}^-(\mathsf{E}[p^\infty]/\mathbb{Q}_n) \subseteq \mathrm{Sel}(\mathsf{E}[p^\infty]/\mathbb{Q}_n) \tag{II.2.3}$$

ainsi que, au niveau infini, leurs duaux de Pontryagin, en analogie avec la définition du module $\mathfrak{X}(\mathsf{E}[p^\infty]/\mathbb{Q}_{\mathrm{cyc}})$:

$$\mathfrak{X}^\pm(\mathsf{E}[p^\infty]/\mathbb{Q}_{\mathrm{cyc}}) = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{Sel}^\pm(\mathsf{E}[p^\infty]/\mathbb{Q}_{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

L'avantage de cette approche est que ces groupes signés sont des $\Lambda(\Gamma_{\mathrm{cyc}})$-modules *de torsion*, et par conséquent des invariants $\mu^\pm_{\mathsf{E}/\mathbb{Q}}$ et $\lambda^\pm_{\mathsf{E}/\mathbb{Q}}$ peuvent être définis. Que ces groupes signés aient une signification arithmétique est témoigné par le fait qu'une formule analogue à (II.2.2) peut être établie[5], notamment $v_p\big(|Ш(\mathsf{E}/\mathbb{Q}_n)|\big) = e_n$ où (voir [Kob03, Theorem 1.4])

$$\begin{aligned} e_n = &\sum_{m=0}^{[\frac{n-2}{2}]} p^{n-1-2m} - \left[\frac{n}{2}\right] + \left[\frac{n}{2}\right]\lambda^+_{\mathsf{E}/\mathbb{Q}} + \left[\frac{n+1}{2}\right]\lambda^-_{\mathsf{E}/\mathbb{Q}} - n\cdot \mathrm{rk}_{\mathbb{Z}}\,\mathsf{E}(\mathbb{Q}_{\mathrm{cyc}}) \\ &+ \sum_{m=1}^{[\frac{n}{2}]} \phi(p^{2m})\mu^+_{\mathsf{E}/\mathbb{Q}} + \sum_{m=1}^{[\frac{n+1}{2}]} \phi(p^{2m-1})\mu^-_{\mathsf{E}/\mathbb{Q}} + \nu_{\mathsf{E}/\mathbb{Q}} \qquad \text{pour tout } n \gg 0. \end{aligned} \tag{II.2.4}$$

De plus, le travail [Pol03] montre que la fonction L p-adique $L_p(\mathsf{E}/\mathbb{Q}, s)$ d'une courbe elliptique à réduction supersingulière peut se décomposer comme une somme

$$L_p(\mathsf{E}/\mathbb{Q}, s) = L_p^+(\mathsf{E}/\mathbb{Q}, s)\cdot \log^+(s) + L_p^-(\mathsf{E}/\mathbb{Q}, s)\cdot \log^-(s),$$

où les deux séries $\log^\pm \in \mathbb{Q}_p(\!(T)\!)$ ont une croissance logarithmique au bord du disque unitaire dans $\mathbb{C}_p$, et les $L_p^\pm(\mathsf{E}/\mathbb{Q}, s)$ sont des séries de puissances dans $\mathbb{Z}_p[\![T]\!]$. La Conjecture Principale de la théorie d'Iwasawa de $\mathsf{E}/\mathbb{Q}$ prédit alors que les éléments $L_p^\pm(\mathsf{E}/\mathbb{Q}, s)$ engendrent les idéaux caractéristiques de $\mathfrak{X}^\pm(\mathsf{E}[p^\infty]/\mathbb{Q}_{\mathrm{cyc}})$ tout en interpolant les valeurs spéciales de la fonction L complexe $L(\mathsf{E}/\mathbb{Q}, s)$, ce qui appuie la valeur arithmétique des groupes de Selmer signés $\mathrm{Sel}^\pm(\mathsf{E}[p^\infty]/\mathbb{Q}_n)$.

La question que nous abordons dans le travail [NS23] est celle de l'invariance des groupes de Selmer signés (ou, au moins, des leurs invariants d'Iwasawa) par congruences. L'observation de départ est la suivante : on a vu dans (II.1.3) que tout $\Lambda(\Gamma_{\mathrm{cyc}})$-module M de type fini et de torsion admet un morphisme

$$M \longrightarrow \bigoplus_{i=1}^{s} \Lambda(\Gamma_{\mathrm{cyc}})/\mathfrak{r}_i^{a_i} \oplus \bigoplus_{i=1}^{e} \Lambda(\Gamma_{\mathrm{cyc}})/p^{b_i} \qquad (\text{avec } a_i, b_i \geqslant 1) \tag{II.1.3}$$

5. Sous l'hypothèse que tous les groupes de Tate–Shafarevich soient finis, évidemment.

à noyau et conoyau finis et que ceci donne lieu à la définition des invariants μ_M, λ_M. On voit facilement que λ_M est le $\mathbb{Z}_p$-rang du quotient de M par son sous-groupe de p^∞-torsion, et que e (le nombre de composantes de p-torsion dans (II.1.3)) est le rang du quotient M/pM en tant que module sur l'algèbre quotient $\Lambda(\Gamma_{\mathrm{cyc}})/p$: en particulier, M/pM est de $\big(\Lambda(\Gamma_{\mathrm{cyc}})/p\big)$-torsion (ou, de façon équivalente, M/pM est *fini*), si et seulement si $e = \mu_M = 0$. De plus, pour un module M sans $\Lambda(\Gamma_{\mathrm{cyc}})$-sous-modules finis non-triviaux (donc tel que tout morphisme comme dans (II.1.3) est en fait *injectif*) et tel que $\mu_M = 0$, l'invariant λ_M coïncide avec la dimension sur $\mathbb{F}_p$ de M/pM.

Une conséquence de cette discussion est que si M et N sont deux $\Lambda(\Gamma_{\mathrm{cyc}})$-modules (de type fini et) de torsion tels que $M/p \cong N/p$, alors

$$\mu_M = 0 \iff \mu_N = 0\,; \tag{II.2.5}$$

et, sous (II.2.5), si ni M ni N n'ont aucun sous-$\Lambda(\Gamma_{\mathrm{cyc}})$-module fini non-trivial, alors

$$\lambda_M = \lambda_N. \tag{II.2.6}$$

L'intérêt de ce qui précède dans le contexte de la théorie d'Iwasawa des courbes elliptiques s'appuie sur les résultats suivants, que nous résumons dans un énoncé unique par commodité, en renvoyant à [Gre99, Proposition 4.14], à [Kim13, Theorem 1.1] et à [KO18, Theorem 4.8] pour les détails ainsi que pour les hypothèses précises :

Théorème (Mazur, Greenberg, Kim, Kitajima–Otsuki). *Le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathfrak{X}(\mathsf{E}/L_{\mathrm{cyc}})$ n'a pas de sous-modules finis non-triviaux lorsque E a bonne réduction ordinaire aux places p-adiques ; dans le cas supersingulier, le même résultat reste vrai en remplaçant $\mathfrak{X}(\mathsf{E}/L_{\mathrm{cyc}})$ par $\mathfrak{X}^{\pm}(\mathsf{E}/L_{\mathrm{cyc}})$.*

En combinant (II.2.5)–(II.2.6) avec le théorème précédent, il est naturel de se poser les questions suivantes :

(A) est-ce que l'annulation de l'invariant $\mu_{\mathsf{E}/L}$ (*resp.* d'un des invariants $\mu^{\pm}_{\mathsf{E}/L}$) dans le cas ordinaire (*resp.* dans le cas supersingulier) ne dépend que de la classe d'isomorphisme de $\mathsf{E}[p]$?

(B) est-il vrai que si deux courbes elliptiques $\mathsf{E}_1, \mathsf{E}_2$ vérifient $\mathsf{E}_1[p] \cong \mathsf{E}_2[p]$, (éventuellement sous l'hypothèse que les invariants $\mu^*_{\mathsf{E}_i/L}$ s'annulent), alors $\lambda^*_{\mathsf{E}_1/L} = \lambda^*_{\mathsf{E}_2/L}$, où $*$ est le symbole vide lorsque la réduction est ordinaire et $* \in \{+,-\}$ lorsque la réduction est supersingulière ?

(C) lorsque la réponse au point (B) est négative, est-il au moins possible de donner une *formule* qui relie $\lambda^*_{\mathsf{E}_1/L}$ et $\lambda^*_{\mathsf{E}_2/L}$ pour deux courbes elliptiques telles que $\mathsf{E}_1[p] \cong \mathsf{E}_2[p]$, (éventuellement sous l'hypothèse que les invariants $\mu^*_{\mathsf{E}_i/L}$ s'annulent) ?

Greenberg et Vatsal ont abordé les problèmes (A)–(C) dans le cas de réduction ordinaire. Leur résultat est le suivant [6]

Théorème (Greenberg–Vatsal, voir [GV00, Theorem 1.4 et Theorem 1.5]). *Dans le cas* ordinaire*, la réponse au point (A) est « oui ». La réponse au point (B) est « non » : il existe une famille explicite infinie de courbes elliptiques E_i (pour $i \in \mathbb{Q}\setminus\{$ ensemble fini$\}$) telles que*

$$\mathsf{E}_i[5] \cong \mathsf{A}[5]$$

6. Une hypothèse technique est requise dans [GV00], mais nous la passons sous silence ici, en renvoyant au travail original pour les détails.

où A *est la courbe elliptique* $\mathsf{A}\colon y^2 = x^3 + x - 10$ (*qui est* 5*-ordinaire*) *mais telles que les* λ_{E_i} *sont non-bornés* (*voir* [GV00, p. 22]). *La réponse au point* (C) *est « oui », et une formule explicite est donnée dans* [GV00, (9)].

Le but de notre travail [NS23] est d'aborder les questions (A)–(C) dans le contexte supersingulier. Pour ce faire, il est commode de donner une autre définition de groupe de Selmer, équivalente à (II.2.1), en termes d'applications de Kummer : pour tout $n \geqslant 0$ et toute place v de L_n, considérons le morphisme κ_v, limite pour $k \to \infty$ des morphismes de bord induits par la multiplication par p^k :

$$\kappa_v\colon \mathsf{E}(L_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(L_{n,v}, \mathsf{E}[p^\infty])$$

On peut montrer que le noyau $\mathrm{Ker}\Big(H^1(L_{n,v}, \mathsf{E}[p^k]) \to H^1(L_{n,v}, \mathsf{E})\Big)$ coïncide avec $\mathrm{Im}(\kappa_v)$, et par conséquent

$$\mathrm{Sel}(\mathsf{E}/L_n) = \Big\{ c \in H^1(L_n, \mathsf{E}[p^\infty]) \text{ telles que } \mathrm{res}^{L_n}_{L_{n,v}}\, c \in \mathrm{Im}(\kappa_v) \text{ pour toute place } v \Big\}.$$

En ce sens, on peut interpréter les classes de cohomologie qui sont dans le groupe de Selmer comme « provenant d'un point local à toute place ». La première étape de l'étude dans [NS23] est la généralisation, pour tout choix d'un vecteur $\ddagger \in \{+,-\}^{S_{\mathrm{ss}}}$ (où S_{ss} est l'ensemble des places p-adiques de L où la réduction de E est supersingulière), de la définition du groupe de Selmer signé de Kobayashi : pour l'introduire, soit $\mathfrak{p}$ une place supersingulière pour E/L, fixons $t \geqslant 1$ et soit $\pm$ le signe $\ddagger_{\mathfrak{p}} \in \{+,-\}$. On dispose alors d'un morphisme de Kummer

$$\kappa_{\mathfrak{p}}^{p^t,\pm}\colon \mathsf{E}^{\pm}_{\mathfrak{p}}(L_{n,\mathfrak{p}})/p^t\mathsf{E}^{\pm}_{\mathfrak{p}}(L_{n,\mathfrak{p}}) \longrightarrow H^1(L_{n,\mathfrak{p}}, \mathsf{E}[p^t]) \tag{II.2.7}$$

où $\mathsf{E}^{\pm}_{\mathfrak{p}}$ est la composante « signée » des points locaux de la courbe E : nous renvoyons à [NS23, Definition 3.2 et Lemma 3.4], inspirés de [Kob03, Definition 3.13 et Lemma 8.17], pour les détails. Posons $\kappa_{\mathfrak{p}}^{p^\infty,\pm} = \varinjlim_t \kappa_{\mathfrak{p}}^{p^t,\pm}$. Le groupe de Selmer multi-signé est alors la limite inductive, par rapport aux morphismes de restriction,

$$\begin{aligned}\mathrm{Sel}^{\ddagger}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}}) = \varinjlim_{L \subseteq L_n \subset L_{\mathrm{cyc}}} \mathrm{Ker}\Big(H^1(\mathcal{G}^S_{L_n}, \mathsf{E}[p^\infty]) \longrightarrow \\ \bigoplus_{\mathfrak{l} \in S_{\mathrm{bad}} \cup S_{\mathrm{ord}}} H^1(L_{n,\mathfrak{l}}, \mathsf{E})[p^\infty] \oplus \bigoplus_{\mathfrak{p} \in S_{\mathrm{ss}}} H^1(L_{n,\mathfrak{p}}, \mathsf{E}[p^\infty])/\operatorname{Im} \kappa_{\mathfrak{p}}^{p^\infty,\ddagger_{\mathfrak{p}}}\Big).\end{aligned} \tag{II.2.8}$$

Dans (II.2.8) le symbole S_{bad} dénote l'ensemble fini des places de L où E a mauvaise réduction et S_{ord} dénote l'ensemble des places *au-dessus de* p où elle a bonne réduction ordinaire : finalement, S est la réunion $S = S_{\mathrm{bad}} \cup S_{\mathrm{ord}} \cup S_{\mathrm{ss}}$ et $\mathcal{G}^S_L = \mathrm{Gal}(L^S/L)$ est le groupe de Galois de l'extension maximale de L non-ramifiée en dehors de S. On note $\mathfrak{X}^{\ddagger}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ le dual de Pontryagin de $\mathrm{Sel}^{\ddagger}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$.

La deuxième étape consiste à définir les équivalents *résiduels*[7] des groupes ci-dessus : afin d'utiliser les techniques introduites dans [CS05b], on veut que les groupes résiduels soient en rapport avec les groupes de Selmer *fins* définis *ibid.* (et qui feront l'objet des §§II.3–II.4). Sans rentrer dans trop de détails, nous nous contentons ici de remarquer que les démonstrations reposent sur la théorie des groupes p-divisibles, à

7. Appelés groupes de Selmer signés résiduels *fins* dans [NS23].

travers le travail [CG96], et il n'est pas suffisant de se borner au cas $t = 1$ dans (II.2.7) afin de pour bâtir une théorie « résiduelle » (voir [NS23, Remark 3.5] pour une discussion approfondie). La définition appropriée sera la suivante :

$$\begin{aligned}\mathcal{R}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}}) = \varinjlim_{L\subseteq L_n\subset L_{\mathrm{cyc}}} \mathrm{Ker}\Big(H^1(\mathcal{G}^S_{L_n},\mathsf{E}[p]) \longrightarrow \bigoplus_{\mathfrak{l}\in S_{\mathrm{bad}}} H^1(L_{n,\mathfrak{l}},\mathsf{E}[p])\oplus \\ \bigoplus_{\mathfrak{q}\in S_{\mathrm{ord}}} H^1(L_{n,\mathfrak{q}},\widetilde{\mathsf{E}}_{\mathfrak{q}}[p])\oplus \bigoplus_{\mathfrak{p}\in S_{\mathrm{ss}}} H^1(L_{n,\mathfrak{p}},\mathsf{E}[p])/\operatorname{Im}\kappa_{\mathfrak{p}}^{p,\ddagger_{\mathfrak{p}}}\Big)\end{aligned} \tag{II.2.9}$$

où $\widetilde{\mathsf{E}}_{\mathfrak{q}}$ dénote la réduction de E modulo le premier $\mathfrak{q}$ de réduction ordinaire. Comme la notation $\mathcal{R}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}})$ le suggère, ces groupes de Selmer ne dépendent que de la classe d'isomorphisme de la représentation $\mathsf{E}[p]$ (voir [NS23, Corollary 4.3]), et il y a une injection de $\big(\Lambda(\Gamma_{\mathrm{cyc}})/p\big)$-modules discrets

$$\mathcal{R}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}}) \hookrightarrow \mathrm{Sel}^{\ddagger}(\mathsf{E}[p^{\infty}]/L_{\mathrm{cyc}})[p]$$

à conoyau fini (voir [NS23, Corollary 4.6]). On note enfin $\mathcal{Y}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}})$ le dual de Pontryagin de $\mathcal{R}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}})$.

Afin d'énoncer notre premier résultat, introduisons l'hypothèse suivante (toujours en supposant que E/L ait bonne réduction à toute place de L divisant p) :

(Hyp 1)

a) S_{ss} est non-vide ;

b) tous les premiers $\mathfrak{p}_1,\dots,\mathfrak{p}_d$ dans S_{ss} sont totalement décomposés dans $L/\mathbb{Q}$, donc $L_{\mathfrak{p}_i}\cong\mathbb{Q}_p$ pour tout $1\leqslant i\leqslant d$;

c) $1+p-|\widetilde{\mathsf{E}}(\mathbb{F}_{\mathfrak{p}_i})| = 0$, où $\mathbb{F}_{\mathfrak{p}_i}$ est le corps résiduel de $\mathfrak{p}_i$ et $\widetilde{\mathsf{E}}$ dénote la réduction de E modulo n'importe quel premier $\mathfrak{p}_1,\dots,\mathfrak{p}_d$ de réduction supersingulière (ces réductions étant toutes isomorphes) ;

d) l'indice de ramification $e(\mathfrak{p})$ dans l'extension $L/\mathbb{Q}$ de tout premier $\mathfrak{p}\in S_{\mathrm{ord}}$ où E a bonne réduction ordinaire est au plus égal à $p-1$.

Théorème II.2.1 ([NS23, Theorem 4.15]). *Soient E_1 et E_2 deux courbes elliptiques définies sur L, qui satisfont l'hypothèse (Hyp 1) et telles que $\mathsf{E}_1[p]\cong\mathsf{E}_2[p]$ en tant que représentations galoisiennes. Alors, les ensembles S^1_{ss} et S^2_{ss} des premiers supersinguliers pour E_1 et E_2 coïncident : soit S_{ss} cet ensemble. Étant donné un vecteur $\ddagger\in\{+,-\}^{S_{\mathrm{ss}}}$, supposons que les modules $\mathfrak{X}^{\ddagger}(\mathsf{E}_i[p^{\infty}]/L_{\mathrm{cyc}})$ soient de $\Lambda(\Gamma_{\mathrm{cyc}})$-torsion (pour $i=1,2$) et notons $\mu^{\ddagger}_{\mathsf{E}_i}$ les invariants d'Iwasawa correspondants. Alors*

$$\mu^{\ddagger}_{\mathsf{E}_1}=0 \Longleftrightarrow \mu^{\ddagger}_{\mathsf{E}_2}=0 \tag{II.2.10}$$

Remarque II.2.2. Comme mentionné plus haut, dans le cas particulier où $L=\mathbb{Q}$, les modules $\mathfrak{X}^{\pm}(\mathsf{E}_i[p^{\infty}]/\mathbb{Q}_{\mathrm{cyc}})$ sont de type fini grâce aux travaux de Kobayashi. Pour des critères de finitude dans le cas général, nous renvoyons à [KO18].

L'application principale du théorème précédent est la suivante :

Théorème II.2.3 ([NS23, Theorem 4.20]). *Soient E_1 et E_2 deux courbes elliptiques définies sur L et satisfaisant aux hypothèses du Théorème II.2.1, et soit $\ddagger\in\{+,-\}^{S_{\mathrm{ss}}}$. Supposons*

que $\mu^{\ddagger}_{\mathsf{E}_1} = 0$ *(ou que* $\mu^{\ddagger}_{\mathsf{E}_2} = 0$*, ce qui est équivalent grâce à* (II.2.10)*) et que les modules* $\mathfrak{X}^{\ddagger}(\mathsf{E}_i[p^\infty]/L_{\mathrm{cyc}})$ *n'aient pas de* $\Lambda(\Gamma_{\mathrm{cyc}})$*-sous-modules non-triviaux, pour* $i = 1, 2$*. Alors*

$$\lambda^{\ddagger}_{\mathsf{E}_i} = \rho^{\ddagger} + \delta_{\mathsf{E}_i} \tag{II.2.11}$$

où

$$\rho^{\ddagger} = \dim_{\mathbb{F}_q} \mathcal{Y}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}})$$

ne dépend que de la représentation résiduelle $\mathsf{E}_1[p] \cong \mathsf{E}_2[p]$*, et* $\delta_{\mathsf{E}_i} \in \mathbb{Z}_{\geqslant 0}$ *est un terme correctif explicite — défini dans [NS23, Definition 4.5] — qui est borné par*

$$2 \cdot \Big|\{\textit{places de } L_{\mathrm{cyc}} \textit{ au-dessus de } S_{\mathrm{bad}} \cup S_{\mathrm{ord}}\}\Big|.$$

Dans [NS23, §5] nous proposons des exemples numériques de familles de courbes satisfaisant aux conditions du Théorème II.2.3 et nous en calculons les invariants d'Iwasawa grâce à la formule (II.2.11)

II.3 Groupes de Selmer fins, extensions de Lie p-adiques abéliennes et Conjecture de Greenberg Généralisée

avec D. Kundu et Sujatha R.

Fixons un corps de nombres L et une courbe elliptique E/L, qui aura bonne réduction en dehors d' un ensemble fini S_{bad} de places de L. Étant donné un premier impair p, nous écrivons S_p pour l'ensemble des places p-adiques de L.

Nous avons vu au §II.2 que pour tout premier p tel que $S_p \cap S_{\mathrm{bad}} = \emptyset$, le module $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ n'est de torsion sur l'algèbre d'Iwasawa $\Lambda(\Gamma_{\mathrm{cyc}})$ du groupe de Galois cyclotomique $\Gamma_{\mathrm{cyc}} = \mathrm{Gal}(L_{\mathrm{cyc}}/L)$ que lorsque la réduction en p est ordinaire. Alors qu'au §II.2 nous avons pallié ce problème en nous intéressant aux groupes de Selmer (multi)-signés, dans cette section et dans la suivante nous allons travailler avec les groupes de Selmer *fins*, dont les groupes $\mathcal{R}^{\ddagger}(\mathsf{E}[p]/L_{\mathrm{cyc}})$ introduits dans (II.2.9) sont une version « résiduelle » modulo p. Ces variants des groupes de Selmer usuels ont été introduits par plusieurs auteurs, citons notamment Perrin-Riou dans son article [PR93], mais c'est surtout à partir du travail [CS05b] de Coates et Sujatha qu'ils ont été étudiés de façon systématique en théorie d'Iwasawa, même au delà du cas cyclotomique. Nous renvoyons aux références mentionnées dans [CS05b, §3] pour un historique des résultats obtenus qui les concernent : leur rôle central pour l'analyse de l'arithmétique cyclotomique d'une courbe elliptique a été étudié par Wuthrich dans sa thèse (voir en particulier [Wut07, Corollary 6.3]).

Afin de décrire le cadre non-cyclotomique, et parfois non-abélien, de la théorie d'Iwasawa pour E/L, nous aurons besoin de la définition suivante :

Définition II.3.1. Soit p un premier impair et soit S un ensemble de places de L contenant S_p. Une extension L_∞/L est S-admissible si

i) le groupe de Galois $\mathrm{Gal}(L_\infty/L)$ est un groupe de Lie p-adique sans éléments d'ordre p ;

ii) l'extension cyclotomique L_{cyc} est contenue dans L_∞ ;

iii) l'extension L_∞ est contenue dans L^S, donc elle est non-ramifiée en dehors de S.

Pour tout corps de nombres $F \supseteq L$ et tout premier $p \notin S_{\mathrm{bad}}$, le groupe de Selmer fin de la représentation $\mathsf{E}[p^\infty]$ est le noyau

$$\mathscr{R}(\mathsf{E}[p^\infty]/F) = \mathrm{Ker}\Big(H^1(\mathcal{G}_F^S, \mathsf{E}[p^\infty]) \longrightarrow \bigoplus_{v\in S} H^1(F_v, \mathsf{E}[p^\infty])\Big), \tag{II.3.1}$$

où $S = S_p \cup S_{\mathrm{bad}}$. Un argument classique montre qu'il est indépendant de S. Étant donnée une extension S-admissible L_∞/L, en passant aux limites inductives sur les sous-extensions $L \subseteq F \subseteq L_\infty$, on peut définir le groupe $\mathscr{R}(\mathsf{E}[p^\infty]/L_\infty)$, comme détaillé dans [KNS24, §2.3]. Les duaux de Pontryagin des groupes $\mathscr{R}(\mathsf{E}[p^\infty]/F)$ seront notés $\mathfrak{Y}(\mathsf{E}[p^\infty]/F)$; pour toute extension S-admissible L_∞/L le groupe $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_\infty)$ est muni d'une structure de module sur l'algèbre d'Iwasawa $\Lambda(\Gamma_\infty)$ du groupe $\Gamma_\infty = \mathrm{Gal}(L_\infty/L)$, et il est facile de montrer qu'en tant que tel il est de type fini. Le premier résultat qui joue un rôle majeur dans notre étude est le suivant :

Théorème ([CS05b, Lemma 3.1]). *Avec les notations introduites ci-dessus, soit p un premier impair tel que $S_p \cap S_{\mathrm{bad}} = \emptyset$ et soit L_∞/L une extension de Lie p-adique qui est S-admissible. Écrivons $\Gamma_\infty = \mathrm{Gal}(L_\infty/L)$. Le $\Lambda(\Gamma_\infty)$-module $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_\infty)$ est de torsion si et seulement si $H^2(\mathrm{Gal}(L^S/L_\infty), \mathsf{E}[p^\infty]) = 0$.*

Afin d'introduire la perspective générale derrière le travail [KNS24], il est opportun de discuter l'hypothèse d'annulation du groupe de cohomologie galoisienne qui apparaît dans le théorème ci-dessus. Nous l'isolons sous la forme suivante :

Conjecture de Leopoldt faible pour E. $H^2(\mathrm{Gal}(L^S/L_\infty), \mathsf{E}[p^\infty]) = 0$.

Son nom provient de l'analogie entre la représentation de torsion $\mathsf{E}[p^\infty] = \varinjlim \mathsf{E}[p^n]$ et la représentation $\mathbb{Q}_p/\mathbb{Z}_p(1) = \varinjlim \mu_{p^n}$, en ayant en vue la

Conjecture de Leopoldt faible. $H^2(\mathrm{Gal}(L^S/L_\infty), \mathbb{Q}_p/\mathbb{Z}_p(1)) = 0$.

Le rapport avec la Conjecture de Leopoldt, dont la Conjecture de Leopoldt faible est un affaiblissement, provient de [NSW08, Theorem 10.3.6] : celui-ci montre que la Conjecture de Leopoldt est équivalente à l'annulation $H^2(\mathcal{G}_L^S, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, pour le groupe de Galois $\mathcal{G}_L^S$ tout entier, plutôt que seulement pour son sous-groupe $\mathrm{Gal}(L^S/L_\infty)$ qui apparaît dans la Conjecture de Leopoldt faible — observons qu'il y a un isomorphisme $\mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Q}_p/\mathbb{Z}_p(1)$ en tant que représentations de $\mathrm{Gal}(L^S/L_\infty)$ grâce à la condition ii) de la Définition II.3.1. Dans le cas de l'extension cyclotomique $L_\infty = L_{\mathrm{cyc}}/L$, la Conjecture de Leopoldt faible est un théorème, dû à Iwasawa et Greenberg (voir [NSW08, Theorem 10.3.25]) ; sa version pour les courbes elliptiques, toujours dans le cas où $L_\infty = L_{\mathrm{cyc}}$, a été étudiée par Schneider, qui en a montré plusieurs critères de validité dans [Sch85]. Dans le cas où $L = \mathbb{Q}$ elle a été démontrée par Kato (voir [Kat04, Theorem 12.4]) ; pour $L/\mathbb{Q}$ abélien, et sous les hypothèses que E/L ait réduction supersingulière en p et que $\mathsf{E}(L)[p] \neq 0$, c'est un théorème de Schneider (voir [Sch85, Theorem 5]) ; pour L quelconque, un argument de suite spectrale de Hochshild–Serre, combiné avec [CS10, Proposition 1.9], montre qu'elle est vraie dès lors que $\mathrm{Sel}(\mathsf{E}/L)$ est fini.

L'idée que certaines propriétés cohomologiques de la représentation $\mathbb{Q}_p/\mathbb{Z}_p(1)$ (ou de μ_p) soient en fait générales et donc valables aussi pour $\mathsf{E}[p^\infty]$ (ou pour $\mathsf{E}[p]$) est un thème récurrent en théorie d'Iwasawa, et probablement la « Conjecture Principale de

Mazur » qui généralise au cas des courbes elliptiques (ordinaires) la Conjecture Principale classique — originairement énoncée pour $\mathbb{Q}_p/\mathbb{Z}_p(1)$ — rentre aussi dans ce cadre. Sous cette perspective, Coates et Sujatha ont introduit deux conjectures dans [CS05b] dont la première généralise la Conjecture $\mu = 0$ d'Iwasawa :

Conjecture A. *Le groupe* $H^2(\mathrm{Gal}(L^S/L_{\mathrm{cyc}}), \mathsf{E}[p])$ *est réduit à* 0.

Que cette conjecture soit étroitement liée à la Conjecture $\mu = 0$ d'Iwasawa est détaillé dans [CS05b, Theorem 3.4] où l'on démontre qu'elles sont en fait équivalentes lorsque $\mathsf{E}[p](L) = \mathsf{E}[p](\bar{\mathbb{Q}})$. En outre, [NS23, Proposition 4.8] montre qu'elle entraîne la Conjecture de Leopoldt faible pour E, ce qui met en évidence son importance dans l'étude de la théorie d'Iwasawa de E. Le premier résultat que nous obtenons est le suivant :

Théorème II.3.2 ([KNS24, Theorem 3.1]). *Supposons que* E/L *soit le changement de base* $(\mathsf{E}/\mathbb{Q}) \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(L)$ *d'une courbe elliptique rationnelle et faisons l'hypothèse que les groupes* $\mathsf{E}(L)$ *et* $Ш(\mathsf{E}/L)$ *soient finis. Lorsque* E *a multiplication complexe par un corps quadratique imaginaire* K*, supposons en plus que la clôture galoisienne* L^c *contienne* K*. Alors la Conjecture A est vraie pour un ensemble infini de nombres premiers ordinaires, de densité supérieure ou égale à* $\frac{1}{[L^c:\mathbb{Q}]}$.

La démonstration du théorème consiste à produire une infinité de premiers p (de la densité prescrite) qui sont ordinaires pour $\mathsf{E}/\mathbb{Q}$ et tels que la série caractéristique p-adique $f_p(T) \in \mathbb{Z}_p[\![T]\!]$ associée à $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ est une unité. Ceci entraîne à son tour que $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ est fini, car le théorème de Mazur rappelé au §II.2 (valable grâce à l'hypothèse que les premiers soient ordinaires) garantit qu'il s'agit d'un module de $\Lambda(\Gamma_{\mathrm{cyc}})$-torsion ; il sera d'ailleurs trivial, car (voir à nouveau le §II.2) il ne contient pas de sous-$\Lambda(\Gamma_{\mathrm{cyc}})$-modules finis non-triviaux. Finalement, $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}}) = 0$ force $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}}) = 0$, et la Conjecture A suit. Le point délicat dans la construction de nombres premiers ordinaires tels que la série caractéristique correspondante est triviale est un théorème de Murty (voir [Mur97]) qui contraint les premiers anomaux à former un ensemble de densité 0 : ce théorème n'étant valide que pour les courbes elliptiques modulaires, nous avons rajouté l'hypothèse que E provienne d'une courbe rationnelle. Un autre ingrédient essentiel pour la démonstration est le théorème [Mer96, Théorème] de Merel qui garantit une borne sur la taille du sous-groupe de torsion de $\mathsf{E}(L)$, borne qui ne dépend que de $[L : \mathbb{Q}]$.

En ce qui concerne les cas supersingulier, une adaptation de la démonstration du théorème précédent donne le

Théorème II.3.3 ([KNS24, Theorem 3.3]). *Soit* $\mathsf{E}/\mathbb{Q}$ *une courbe elliptique et supposons que* $\mathrm{Sel}(\mathsf{E}[p^\infty]/L)$ *soit fini. Alors la Conjecture A pour* E/L *est vraie pour presque tous les premiers de* L *où* E *a réduction supersingulière.*

La différence principale par rapport à la démonstration du Théorème II.3.2 consiste à remplacer le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathfrak{X}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ par les groupes signés $\mathfrak{X}^{\pm}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ introduits au §II.2.

L'énoncé de la Conjecture A peut être généralisé à toute extension S-admissible L_∞/L, et cette généralisation est tout particulièrement pertinente dans le programme, initié par Coates dans [Coa99] et poursuivi avec ses collaborateurs, de la théorie d'Iwasawa non-commutative. Cette généralisation a à nouveau été introduite dans le travail [CS05b] et prend la forme suivante :

Conjecture B. *Soit L_∞/L une extension qui est S-admissible et telle que son groupe de Galois $\Gamma_\infty = \mathrm{Gal}(L_\infty/L)$ soit de dimension*[8] *supérieure ou égale à 2. Alors la Conjecture A est vraie, et le groupe $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_\infty)$ est un $\Lambda(\Gamma_\infty)$-module pseudo-nul, c'est-à-dire que*

$$\mathrm{Ext}^1_{\Lambda(\Gamma_\infty)}\big(M, \Lambda(\Gamma_\infty)\big) = 0.$$

Remarque. Dans le cas (abélien) de dimension 1, tel celui du groupe Γ_{cyc}, la condition d'être pseudo-nul est équivalente à être fini (voir [NSW08, V, §1, Remarks to Definition 5.1.4]).

Bien que la perspective d'étendre les résultats, surtout ceux de caractère cohomologique, de la représentation $\mathbb{Q}_p/\mathbb{Z}_p(1)$ à la représentation $\mathsf{E}[p^\infty]$ soit intéressante en général, dans le cadre de la multiplication complexe elle devient considérablement plus naturelle : historiquement, d'ailleurs, le travail [CS05a] a été la première étude consacrée aux questions posées dans [CS05b], et s'est justement focalisée sur le contexte CM. Comme il l'a déjà été discuté au §I.2, la théorie de la multiplication complexe est étroitement liée à la théorie du corps de classes pour les corps quadratiques imaginaires et dans la deuxième partie du travail [KNS24] nous étudions la Conjecture B — et donc, en particulier, la Conjecture A — dans ce cas.

Un premier résultat dans cette direction est le suivant :

Théorème II.3.4 ([KNS24, Theorem 4.6]). *Étant donnés un corps quadratique imaginaire K et un premier $p \geqslant 5$ décomposé dans $K/\mathbb{Q}$, soient L un corps de nombres contenant K et E/L une courbe elliptique avec CM par $\mathcal{O}_K$. Supposons que E/L ait bonne réduction aux places dans S_p et que le groupe de Galois $\mathrm{Gal}(L(\mathsf{E}[p^\infty])/L)$ soit isomorphe à $\mathbb{Z}_p^2$. Si le groupe $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ est fini, alors la Conjecture B est vraie.*

La démonstration du théorème repose essentiellement sur les techniques d'algèbre homologique de [CS10], surtout dans la forme développée dans [NS23], et sur le théorème de structure des algèbres d'Iwasawa. Plus précisément, notons Γ_∞ le groupe $\mathrm{Gal}(L(\mathsf{E}[p^\infty])/L)$ et soit $H \subseteq \Gamma_\infty$ le sous-groupe $H = \mathrm{Gal}(L(\mathsf{E}[p^\infty])/L_{\mathrm{cyc}})$. Une étude de descente galoisienne de $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_\infty)_H$ à $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_{\mathrm{cyc}})$ combinée avec la « descente parfaite pour les groupes de Selmer » démontrée par Perrin-Riou (voir [PR81, Lemme 1.1(i) et Lemme 1.3]) permet de montrer que, sous les hypothèses du théorème, les coinvariants $\mathfrak{Y}(\mathsf{E}[p^\infty]/L_\infty)_H$ sont finis. Après, en nous appuyant sur le théorème de structure, nous montrons que pour tout $\Lambda(\Gamma_\infty)$-module M de type fini qui est aussi de type fini sur $\Lambda(H)$, si les coinvariants M_H sont finis, alors M est $\Lambda(\Gamma_\infty)$-pseudo-nul. En combinant les deux arguments, la Conjecture B suit.

Comme l'énoncé du Théorème II.3.4 le manifeste, le contexte CM assure que les groupes de Galois en jeu sont abéliens et de dimension supérieure à 1. Il se pose donc la question de clarifier les liens entre la Conjecture B et une conjecture en théorie d'Iwasawa classique « pour les corps de classes », due à Greenberg (voir [Gre01, Conjecture 3.5]), portant sur la taille de certains groupes de Galois abéliens non-ramifiés. Il s'agit de la

Conjecture de Greenberg Généralisée. *Notons $\widetilde{L}$ le composé de toutes les $\mathbb{Z}_p$-extensions de L, et soit $\mathcal{L}/\widetilde{L}$ l'extension pro-p abélienne non-ramifiée maximale de $\widetilde{L}$. Le groupe*

$$\mathrm{Gal}(\mathcal{L}/\widetilde{L})$$

8. La dimension dont il est question dans la Conjecture B est celle de Γ_∞ en tant que groupe de Lie p-adique.

est pseudo-nul en tant que module sur l'algèbre d'Iwasawa du groupe de Galois $\mathrm{Gal}(\widetilde{L}/L)$.

Dans le théorème suivant nous montrons que la Conjecture B pour les courbes CM est liée à la Conjecture de Greenberg Généralisée pour le corps de classes du corps de multiplication complexe. Avant d'énoncer le théorème, rappelons qu'un résultat classique de Deuring (voir [Deu52, §1]) établit qu'une courbe elliptique $\mathsf{E}/\overline{\mathbb{Q}}$ avec multiplication complexe par un ordre $\mathcal{O}$ dans un corps quadratique imaginaire K peut toujours être définie sur le corps de classes de Hilbert H_K de K.

Théorème II.3.5 ([KNS24, Theorem 5.4]). *Supposons que le premier $p \geqslant 5$ soit non-ramifié dans le corps quadratique imaginaire K, et que $H_K \cap \widetilde{K} = K$, où $\widetilde{K}$ est le composé de toutes les $\mathbb{Z}_p$-extensions de K. S'il existe une courbe elliptique E/H_K avec CM par $\mathcal{O}_K$ telle que la Conjecture B est vraie pour l'extension $H_K(\mathsf{E}[p^\infty])/H_K$, alors la Conjecture de Greenberg Généralisée est vraie pour le corps H_K.*

Nous nous contentons ici de mentionner que la démonstration du théorème s'appuie de façon cruciale sur les résultats [Ban07, Theorem 12] et [Kle16, Theorem 3.1-(i)], qui sont en quelque sorte complémentaires : alors que le théorème de Bandini est un lemme de « relèvement » de pseudo-nullité d'un quotient d'une algèbre d'Iwasawa à l'algèbre toute entière, celui de Kleine permet de « descendre » cette propriété le long d'extensions finies. Dans le deux cas, le contexte est celui d'algèbres d'Iwasawa pour groupes de Galois qui sont libres et de type fini sur $\mathbb{Z}_p$, et ne se généralisent pas directement au contexte des courbes elliptiques sans multiplication complexe.

II.4 Modèles entiers pour familles de Coleman et variations des invariants d'Iwasawa

avec T. Ochiai et J. Ray

Soit $p \geqslant 3$ un nombre premier et soit $N \geqslant 1$ un entier premier à p. Depuis les travaux de Hida dans les années ′80 (voir [Hid86] et les références *ibid.*), il est devenu apparent que certaines représentations galoisiennes p-adiques d'origine géométrique apparaissent naturellement « en familles ». En analogie avec l'étude du §II.2, ces familles se laissent classifier en deux types : les familles ordinaires (aussi appelées « familles de Hida ») et les familles non-ordinaires, qui généralisent en poids quelconque le cas des courbes elliptiques surpersingulières. Dans [Col96, Col97b, Col97a] et [CM98] Coleman et Coleman–Mazur ont introduit des objets géométriques, à savoir des variétés analytiques p-adiques, qui « contiennent » les familles non-ordinaires comme sous-espaces. Ces variétés sont connues, en français, sous le nom de « Variétés de Hecke » (*eigenvarieties* dans la terminologie anglo-saxonne) : nous renvoyons au travail [Buz07] de Buzzard pour une systématisation et une généralisation de la construction de Coleman–Mazur pour un poids modéré N quelconque ; ainsi qu'au travail [Bel12], par Bellaïche, pour une construction différente basée sur l'interpolation des symboles modulaires. Tout comme aux §§II.1–II.3 la perspective qui nous intéresse est celle de la théorie d'Iwasawa. Le point de départ est, comme discuté au §I.2, la possibilité d'associer à toute forme modulaire une représentation continue de $\mathcal{G}_{\mathbb{Q}}$: dans le contexte des formes ordinaires, Hida attacha à toute forme modulaire *ordinaire*

$f \in S_k\big(\Gamma_1(Np^\infty)\big)$ de poids k et niveau[9] $\Gamma_1(Np^\infty)$ une représentation continue

$$\Pi_{f,\mathrm{ord}} \colon \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{T}) \tag{II.4.1}$$

où $\mathbf{T}$ est une algèbre finie et plate sur $\mathbb{Z}_p[\![T]\!]$, avec une propriété « d'interpolation ». Cette dernière peut s'exprimer comme suit : il existe dans $\mathrm{Spec}(\mathbf{T})$ une famille $\{P_k\}$ d'idéaux premiers, indexés par les entiers supérieurs ou égaux a 2 tels que, pour tout $k \in \mathbb{Z}_{\geqslant 2}$, il y a un isomorphisme

$$\Pi_{f,\mathrm{ord}}/P_k \cong \rho_k \tag{II.4.2}$$

en tant que représentations de $\mathcal{G}_{\mathbb{Q}}$, où ρ_k est la représentation associée par Deligne à une certaine forme parabolique de poids k et niveau $\Gamma_1(Np^\infty)$, essentiellement unique et qui est congrue[10] modulo p à la forme f de départ : en particulier, $f_k = f$.

Des résultats similaires sont valables pour les familles de Coleman. De telles représentations « en familles » ont été construites dans les travaux cités de Coleman, de Coleman–Mazur, de Buzzard et de Bellaïche. Tout comme dans le cadre ordinaire, ces représentations permettent de retrouver, aux points classiques, la représentation p-adique de Deligne. Afin d'énoncer cette propriété, fixons quelque notation : notons $\mathscr{X}_N$ la variété de Hecke réduite pour GL_2 associée au niveau modéré N (voir [CM98] ou [Buz07]). Cet espace analytique p-adique est muni d'une projection $\pi\colon \mathscr{X}_N \to \mathscr{W}_N$ sur l'espace des poids $\mathscr{W}_N$, lui-même isomorphe à une réunion finie disjointe de boules analytiques p-adiques ouvertes. Pour toute extension complète $E/\mathbb{Q}_p$, les points $x \in \mathscr{X}_N(E)$ correspondent bijectivement aux formes modulaires p-adiques surconvergentes (voir [Buz07, Corollary 6.2], où le rayon de surconvergence ainsi que le niveau exacte et le Nebentypus sont précisés), définies sur E, qui sont vecteurs propres pour les opérateurs de Hecke et telles que la valeur propre $a_p(f)$ pour U_p est non-nulle : de plus, le poids d'une forme f_x correspondant à $x \in \mathscr{X}_N(E)$ est précisément $\pi(x)$. Fixons maintenant un rationnel non-négatif $\alpha \in \mathbb{Q}_{\geqslant 0}$: on peut alors considérer le sous-espace $\mathscr{C}_\alpha$ des points x tels que la valeurs propre $a_p(f_x)$ pour l'opérateur U_p a valuation égale à α. C'est cet espace qui généralise l'objet géométrique $\mathrm{Spec}(\mathbf{T})$, lui-même isomorphe (après un processus d'analytification) à $\mathscr{C}_0$: la condition d'être ordinaire correspond en effet à demander que la valeur propre pour U_p soit une unité p-adique, ou encore que sa valuation soit égale à 0. C'est en ces termes que la construction de Coleman–Mazur généralise[11] celle de Hida au delà du cas ordinaire. L'interpolation énoncée dans (II.4.2) prend ici la forme suivante (pour plus de détails voir, par exemple, [NOR23, §§2–3]) : il existe un sous-espace *affinoïde* $\mathscr{W}_N^* \subseteq \mathscr{W}_N$ et un sous-ensemble $\mathscr{Z} \subseteq \mathscr{W}_N^*(\mathbb{C}_p)$, lui-même en bijection avec $\mathbb{Z}_{\geqslant \alpha+1}$, tels que :

1. la restriction à $\mathscr{C}_\alpha \subseteq \mathscr{X}_N$ de la projection π définit un isomorphisme de l'intersection $\pi^{-1}(\mathscr{W}_N^*) \cap \mathscr{C}_\alpha \subseteq \mathscr{C}_\alpha$ avec $\mathscr{W}_N^*$;

9. Dans la première partie de cette section, nous faisons le choix de travailler avec le sous-groupe de congruences Γ_1 plutôt que Γ_0 pour éviter les discussions relatives aux Nebentypen, bien que la théorie permette un contrôle parfait de la variation du Nebentypus dans les familles. Aussi, la notation $\Gamma_1(Np^\infty)$ indique que la forme est de niveau $\Gamma_1(Np^r)$ pour un entier $r \geqslant 1$ que nous ne tâchons pas de spécifier.

10. Pour la notion de congruence entre représentations, nous renvoyons au §I.2.

11. Nous n'énonçons pas ici l'équivalent pour les familles de Coleman du fait que, lorsqu'on part d'une forme de poids k, l'élément de poids égal à k de la famille de Coleman associée à f est précisément la forme f de départ. Sous les hypothèses du Théorème II.4.1, on verra que cette propriété est satisfaite mais en général il faudrait introduire le concept de p-stabilisation, qui est trivial dans le cas ordinaire, et nous renvoyons à [Bel12, §2.2.2] pour une discussion approfondie.

2. étant donné $k \in \mathbb{Z}_{\geqslant \alpha+1} \overset{1:1}{\longleftrightarrow} \mathscr{Z}$, notons encore — par un petit abus de notation (anodin, grâce au point précédent) — par k l'unique point de $\mathscr{C}_\alpha$ d'image $k \in \mathscr{Z}$ à travers π. La forme modulaire p-adique surconvergente f_k est alors *classique* de poids k, c'est-à-dire qu'elle appartient à $S_k\big(\Gamma_1(Np^\infty)\big)$;
3. en écrivant $\mathscr{A}$ pour l'algèbre de Tate des fonctions analytiques sur $\mathscr{W}_N^*$ (ou sur le sous-espace $\pi^{-1}(\mathscr{W}_N^*) \cap \mathscr{C}_\alpha \subseteq \mathscr{C}_\alpha$, ce qui est équivalent grâce au point 1.), il existe une représentation galoisienne continue

$$\Pi_\alpha \colon \mathcal{G}_{\mathbb{Q}}^S \longrightarrow \mathrm{GL}_2(\mathscr{A}), \tag{II.4.3}$$

qui se spécialise (au sens de (II.4.2)) en tout point $k \in \mathscr{Z}$ à la représentation de Deligne associée à la forme classique f_k.

Une différence cruciale entre la construction originale de Hida par rapport à celle de Coleman–Mazur est dans le type d'anneau de coefficients : alors que dans (II.4.1) $\mathbf{T}$ est une algèbre finie et plate sur $\mathbb{Z}_p[\![T]\!]$, donc en particulier semi-locale et complète par rapport à la topologie de ses idéaux maximaux, dans (II.4.3) $\mathscr{A}$ est une algèbre de Banach, complète par rapport à la norme p-adique mais avec une infinité d'idéaux maximaux. Il ne s'agit donc pas d'un objet de la catégorie usuelle où l'on peut appliquer les techniques de la théorie d'Iwasawa, et la première partie de [NOR23] est consacrée à la construction d'une représentation 2-dimensionnelle sur une algèbre de séries formelles $\mathbf{A}$ finie sur $\mathbb{Z}_p[\![T]\!]$: plus précisément, nous montrons le

Théorème II.4.1 ([NOR23, Theorem 4.3]). *Fixons deux entiers $k_0 \in \mathbb{Z}_{\geqslant 2}$ et $0 \leqslant i < p-1$, un rationnel $\alpha \in \mathbb{Q}_{\geqslant 0}$ et un caractère $\varepsilon \colon \mathbb{Z}/(N)^\times \to \mathbb{C}^\times$. Écrivons ω pour le caractère de Teichmüller. Soit $f \in S_{k_0}\big(\Gamma_0(Np^\infty), \varepsilon\omega^{(i-k_0)}\big)$ une forme parabolique propre, normalisée, nouvelle en dehors de p, telle que la valuation p-adique du p-ème coefficient de Fourier satisfait $v_p\big(a_p(f)\big) = \alpha$; lorsque $i = 0$ supposons de plus que $a_p^2 \neq \varepsilon(p)p^{k_0-1}$. Il existe alors un rayon $r \in p^{\mathbb{Q}}$, et une représentation continue*

$$\boldsymbol{\rho}_{k_0,\alpha} \colon \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{A})$$

à coefficients dans l'algèbre $\mathbf{A}$ des séries formelles convergentes dans la boule analytique fermée $\mathscr{B}[k_0, r]$ (et coefficients dans une extension finie de $\mathbb{Q}_p$) avec les propriétés suivantes :

1. *étant donné $k \in \mathscr{B}[k_0, r](\mathbb{C}_p) \cap \mathbb{Z}$, notons $P_k \in \mathrm{Spec}(\mathbf{A})$ l'idéal premier noyau de l'évaluation au point k ; alors, pour tout $k \in \mathscr{B}[k_0, r](\mathbb{C}_p) \cap \mathbb{Z}_{>\alpha+1}$, il existe une forme parabolique $f_k \in S_k\big(\Gamma_1(Np^\infty)\big)$, propre pour les opérateurs de Hecke, nouvelle en dehors de p, satisfaisant $v_p\big(a_p(f_k)\big) = \alpha$ et telle que la représentation $\boldsymbol{\rho}_{k_0,\alpha}/P_k$ est isomorphe à la représentation ρ_{f_k} attachée à f_k ;*
2. *pour $k = k_0$, on a $f_{k_0} = f$.*

La démonstration du théorème repose essentiellement sur la technique, introduite par Wiles dans [Wil88] et reprise par Hida dans [Hid93], des pseudo-représentations. Cette technique utilise de façon cruciale la continuité par rapport à la topologie $\mathfrak{m}$-adique, où $\mathfrak{m}$ est l'idéal maximal de $\mathbf{A}$, de certaines fonctions

$$A, D \colon \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathbf{A}$$

et

$$\Xi\colon \mathcal{G}_{\mathbb{Q}} \times \mathcal{G}_{\mathbb{Q}} \longrightarrow \mathbf{A}\,:$$

nous renvoyons à [NOR23, §4] pour les détails. Il y a lieu d'observer ici qu'une autre définition d'une représentation galoisienne à valeurs dans une algèbre locale, telle $\boldsymbol{\rho}_{k_0,\alpha}$, a été proposée par Loeffler–Zerbes dans [LZ16]. Dans leur travail la représentation apparaît dans la cohomologie de certains faisceaux sur la courbe modulaire, définis dans [AIS15], et de ce fait la généralisation à formes modulaires pour des groupes autres que GL_2 est moins immédiate qu'avec notre construction.

L'application principale que nous proposons du Théorème II.4.1 est une généralisation des résultats de Emerton–Pollack–Weston [EPW06] au delà du cas ordinaire, dans le même esprit que la généralisation décrite au §II.2 du travail [GV00] de Greenberg–Vatsal. Le contexte du travail [EPW06] est celui de la théorie de Hida, telle que nous l'avons brièvement présentée précédemment. Étant donnée une forme modulaire ordinaire $f \in S_k\big(\Gamma_1(Np^\infty)\big)$, soit $\Pi_{f,\mathrm{ord}}$ la représentation définie dans (II.4.1). Une définition de groupe de Selmer, analogue à celle décrite au §II.2 pour les courbes elliptiques, peut se faire pour la représentation ρ_k associée à une forme modulaire de n'importe quel poids. On associe donc à toute forme f_k de la famille, et à toute extension finie $L/\mathbb{Q}$, un groupe de Selmer $\mathrm{Sel}(\rho_f/L) = \mathrm{Sel}(f/L)$ qui donne lieu, par passage à la limite inductive et au dual de Pontryagin, à un module $\mathfrak{X}(f/\mathbb{Q}_{\mathrm{cyc}})$ sur l'algèbre d'Iwasawa $\Lambda(\Gamma_{\mathrm{cyc}})$. L'analogue en poids supérieur du travail [Maz72] de Mazur mentionné au §II.2 dans le cas des courbes elliptiques a été obtenu par Kato (voir [Kat04, Chapter III]) ; on sait donc que le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathfrak{X}(f/\mathbb{Q}_{\mathrm{cyc}})$ est toujours de type fini, et qu'il est de torsion si et seulement si la forme f est ordinaire. Par conséquent, dans le cas des familles de Hida, tous les $\Lambda(\Gamma_{\mathrm{cyc}})$-modules $\mathfrak{X}(f_k/\mathbb{Q}_{\mathrm{cyc}})$ sont de torsion et on peut leur associer deux invariants λ_{f_k} et μ_{f_k}, comme décrit aux §§II.1–II.2.

Or, comme mentionné dans (II.4.2), toutes les représentations ρ_k obtenues par réduction de $\Pi_{f,\mathrm{ord}}$ modulo les idéaux premiers « classiques » sont congrues modulo p : on peut donc regarder la collection des représentations $\{\rho_k\}_{k\geqslant 2}$ comme une famille de déformations en caractéristique 0, et poids différents, de la même représentation $\overline{\rho}$. Il est donc naturel de se poser la même question qui était à la base du travail [NS23], notamment de savoir quelles propriétés arithmétiques (p-adiques) dépendent seulement de la réduction $\overline{\rho}$, et sont donc constantes dans la famille de Hida fixée. Le résultat principal obtenu par Emerton–Pollack–Weston peut se résumer ainsi :

Théorème ([EPW06, Theorem 4.3.3 et Theorem 4.3.4]). *L'invariant μ_f associé à la forme ordinaire f est nul si et seulement si il en est ainsi pour toute autre forme f_k de la famille*[12]*. Lorsque cette annulation a lieu, les invariants λ_{f_k} sont constants dans la famille.*

Dans l'optique de généraliser ce théorème aux familles de Coleman on se heurte immédiatement au problème que le $\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathrm{Sel}(f/\mathbb{Q}_{\mathrm{cyc}})$ n'est pas de torsion lorsque la forme f n'est pas ordinaire, tout comme au §II.2 ; en particulier, les invariants μ_f et λ_f ne peuvent pas être définis. Plutôt qu'étudier la variation en famille des invariants « signés » $\mu_{f_k}^{\pm}$ et $\lambda_{f_k}^{\pm}$ – qui sont la généralisation en poids supérieurs de ceux qui

12. Dans *loc. cit.* les auteurs ont affaire à des familles de Hida qui peuvent contenir plusieurs composantes, bien qu'en nombre fini, et le théorème ci-dessus n'est valable que composante-par-composante. Nous négligeons ce détail technique dans notre texte.

apparaissent dans (II.2.4), et qui ont été définis par Hatley–Lei dans [HL19] — nous faisons le choix d'étudier la variation en famille des invariants associés aux groupes de Selmer fins, introduits au §II.3.

Plaçons-nous dans le contexte du Théorème II.4.1, et faisons l'hypothèse que la représentation résiduelle $\overline{\boldsymbol{\rho}_{k_0,\alpha}}$, restreinte à $\mathcal{G}_{\mathbb{Q}_p}$, soit irréductible. Nous montrons alors (voir [NOR23, Theorem 6.3]) l'existence d'un $\mathbf{A}$-module $\mathbf{Y}(\boldsymbol{\rho}_{k_0,\alpha})$, défini au-dessus de la boule $\mathscr{B}[k_0, r]$, et de certains isomorphismes de spécialisation

$$s_k \colon \mathbf{Y}(\boldsymbol{\rho}_{k_0,\alpha})/P_k \cong \mathfrak{Y}(f_k/\mathbb{Q}_{\mathrm{cyc}}), \tag{II.4.4}$$

définis en dehors d'un nombre fini de points exceptionnels dans $\mathbb{Z}_{\geqslant \alpha+1}$; dans (II.4.4), les groupes $\mathfrak{Y}(f_k/\mathbb{Q}_{\mathrm{cyc}})$ sont les duaux des groupes de Selmer fins, tels que nous les avons définis au §II.3 (en remplaçant la représentation $\mathsf{E}[p^\infty]$ par ρ_{f_k}, comme précédemment). Le module $\mathbf{Y}(\boldsymbol{\rho}_{k_0,\alpha})$ se trouve muni, par construction, d'une action du groupe Γ_{cyc}, ce qui fait que les isomorphismes (II.4.4) sont en fait des isomorphismes en tant que $\Lambda(\Gamma_{\mathrm{cyc}})$-modules. Le résultat principal que nous obtenons est le suivant [13] :

Théorème II.4.2 ([NOR23, Theorem 7.1 et Theorem 7.3]). *Avec les mêmes notations introduites dans le Théorème II.4.1, supposons que la représentation $\overline{\boldsymbol{\rho}_{k_0,\alpha}}$, restreinte à $\mathcal{G}_{\mathbb{Q}_p}$ soit irréductible. Alors*

1. *Les conditions suivantes sont équivalentes :*
   - 1-a) *le $\mathbf{A}\widehat{\otimes_{\mathbb{Z}_p}}\Lambda(\Gamma_{\mathrm{cyc}})$-module $\mathbf{Y}(\boldsymbol{\rho}_{k_0,\alpha})$ est de type fini en tant que $\mathbf{A}$-module ;*
   - 1-b) *l'invariant d'Iwasawa fin $\mu_{f_k}^{\mathrm{fin}}$ attaché au groupe $\mathfrak{Y}(f_k/\mathbb{Q}_{\mathrm{cyc}})$ est nul pour toute forme f_k dans la famille de Coleman ;*
   - 1-c) *il existe une forme f_k dans la famille de Coleman pour laquelle l'invariant d'Iwasawa fin $\mu_{f_k}^{\mathrm{fin}}$ attaché au groupe $\mathfrak{Y}(f_k/\mathbb{Q}_{\mathrm{cyc}})$ est nul.*
2. *Si une des propriétés équivalentes 1-a)–1-c) ci-dessus est satisfaite, alors les invariants d'Iwasawa $\lambda_{f_k}^{\mathrm{fin}}$ attachés aux groupes de Selmer fins dans la famille de Coleman sont tous égaux, sauf pour un nombre fini de poids exceptionnels.*

Le Théorème II.4.2 est l'équivalent du résultat de Emerton–Pollack–Weston cité plus haut, parce que 1-a) est une condition globale sur la famille, sous laquelle tous les invariants $\mu_{f_k}^{\mathrm{fin}}$ s'annulent. Il s'agit d'ailleurs d'une condition qui est un analogue « en dimension supérieure » (analogie qui émerge dans la démonstration) de la condition mentionnée au §II.2 d'annulation de l'invariant μ pour un $\Lambda(\Gamma_{\mathrm{cyc}})$-module M de torsion, pour lequel on a l'équivalence

$$\mu_M = 0 \iff M \text{ est de type fini sur } \mathbb{Z}_p$$

(voir la discussion qui précède (II.2.5)). La démonstration du Théorème II.4.2 consiste en une généralisation des arguments de [EPW06], en remplaçant la condition d'ordinarité par la constance de la valuation p-adique α de la valeur propre $a_p(f_x)$ dans la famille de Coleman. Une fois de plus, travailler avec des $\mathbf{A}$-modules plutôt qu'avec des $\mathscr{A}$-modules permet d'adapter les arguments *ibid.*, en remplaçant les groupes de Selmer usuels par leurs équivalents fins afin de s'assurer que leurs limites projectives soient encore de torsion sur $\Lambda(\Gamma_{\mathrm{cyc}})$. Nous renvoyons à [NOR23, §7] pour les détails.

13. Dans [NOR23] les résultats sont énoncés pour la représentation duale $\boldsymbol{\rho}_{k_0,\alpha}^\star$: le passage entre les deux formulations étant classique, nous faisons le choix d'énoncer le théorème pour $\boldsymbol{\rho}_{k_0,\alpha}$ par simplicité.

III

Les projets de formalisation en `lean-3`

Pour terminer ce mémoire, je présente deux travaux de formalisation mathématique, qui ont été implémentés dans l'assistant de preuve `lean-3`[1] en s'appuyant sur la bibliothèque `mathlib` (voir le site [DeM23] ainsi que l'article [Mat20] pour une description détaillée du logiciel et de la librairie), suivis d'une perspective sur mes projets de recherche futurs.

L'idée d'exploiter la fiabilité des ordinateurs lors de l'exécution d'un programme pour valider des preuves d'énoncés mathématiques est ancienne, et remonte au moins aux expériences menées sur `Automath` par de Bruijn autour de 1967. Depuis, le domaine de la vérification de preuve assistée par ordinateur s'est développé en plusieurs directions et a donné lieu à différentes thématiques de recherche. Toutefois, c'est à partir du début du XXIème siècle que la vérification de preuve par ordinateur a pris un nouvel essor, par exemple avec la formalisation de la conjecture de Kepler par Hales et ses collaborateurs (voir [HAB+17]), en combinant les assistants de preuve `Isabelle` et `HOL-Light`. Autres projets remarquables de formalisation ont été ceux de Gonthier sur le théorème des quatre couleurs (datant de 2008, mais dont le rapport officiel n'est apparu qu'en 2023 dans [Gon23]), celui du théorème de Feit–Thompson par Gonthier et ses collaborateurs (voir [GAA+13]) et, plus récemment, le théorème d'Abel–Ruffini par Bernard, Cohen, Mahboubi et Strub (voir [BCMS21]) ; ces résultats ont été formalisés dans l'assistant de preuve `Coq`. Dans une direction un peu différente, la communauté mathématique travaillant dans l'assistant de preuve `lean-3` développe depuis quelques années la bibliothèque unifiée `mathlib`, dans le but de disposer de suffisamment de résultats fondamentaux pour pouvoir formaliser les résultats mathématiques les plus

1. Cet assistant de preuve est en train d'évoluer, avec sa librairie, à la nouvelle version `lean-4` (voir [DeM23]). Malheureusement, `lean-4` ne sera pas compatible avec `lean-3` et un travail collaboratif est en train d'être mené afin de porter la librairie `mathlib` de l'ancienne à la nouvelle version. En ce sens, les travaux illustrés ici peuvent paraître obsolètes mais, au moins en ce qui concerne le travail décrit au §III.1, il en existe une version portée en `lean-4`. Dans le cadre d'un mémoire d'HDR il m'a semblé plus opportun de décrire les travaux tels qu'ils ont été effectués originairement, et je me bornerai donc à `lean-3` dans ce chapitre.

récents : mentionnons à titre d'exemples la formalisation par Buzzard, Commelin et Massot de la définition d'espace perfectoïde (voir [BCM20]) et, tout récemment, l'aboutissement du *Liquid Tensor Experiment* (voir [Sch22] et [Mat22]), dont il sera question au §III.2.

L'activité de formalisation consiste en large mesure à s'assurer que le processus de traduction du langage mathématique courant au langage de programmation soit *fidèle* et *efficace*. Il doit être fidèle pour que les preuves validées correspondent effectivement aux énoncés mathématiques auxquels on s'intéresse ; et efficace pour que les techniques et les stratégies développées dans la pratique mathématique s'avèrent utiles aussi lors de la pratique de formalisation.

Tous les assistants de preuve cités plus haut ont une architecture commune : le choix d'un langage formel dans lequel exprimer les énoncés mathématiques (souvent différent de la théorie des ensembles) ; un programme très petit — dont l'exactitude peut idéalement être vérifiée indépendamment du reste de la structure informatique — appelé « noyau » ; et un programme d'interface entre le noyau et l'utilisateur. C'est à ce dernier niveau qui se joue l'équilibre entre la verbosité nécessaire pour écrire tout énoncé directement dans le langage machine (tâche quasiment impossible) et la communication informelle qui guide l'intuition des mathématiciens ; bien que le choix du programme d'interface soit cruciale dans l'expérience de l'utilisateur, il est important de souligner que la correction des preuves formalisées repose seulement sur le noyau, d'où la nécessité qu'il soit petit et facilement vérifiable. Pour un excellent survol de ces architectures communes je suggère la lecture de l'article [Mah14] de Mahboubi ; pour un texte complet je renvoie à sa thèse d'habilitation [Mah21]. Le système formel sous-jacent à `lean-3` est une théorie des types dépendants basée sur le calcul des constructions inductives. Je renvoie à [NG14, Chapters 5 and 6] pour les définition principales de la théorie des types dépendants et pour les fondements du calcul des constructions inductives, et à [Car19] pour l'équicohérence entre la théorie des types de `lean-3` et le système ZFC+ (ZFC avec l'hypothèse de l'existence de n cardinaux inaccessibles pour tout $n < \omega$).

Outre l'assistant de preuve lui-même, l'autre ingrédient essentiel est une bibliothèque des résultats déjà formalisés. L'effort de formalisation, en effet, n'a un sens que dans la mesure où il s'inspire du procès progressif usuel en mathématiques, où chaque théorème repose sur les précédents et constitue une brique sur laquelle s'appuieront les suivants. La construction d'une bibliothèque cohérente et les choix inhérents à sa structure sont donc fondamentaux et souvent spécifiques à chaque communauté travaillant dans un assistant de preuve. Pour `lean-3`, la bibliothèque en question est `mathlib` (maintenue à l'adresse [Mat23] et décrite dans [Mat20]). Dans les projets qui suivent, `mathlib` a été à la fois source de notions basiques et cible des résultats formalisés, qui l'ont intégrée dans les mois qui ont suivi la conclusion du travail. Il faut mentionner aussi que d'autres vastes bibliothèques de mathématiques formalisées existent, mais un travail systématique de comparaison dépasse les objectifs de ce travail. Je renvoie à l'ouvrage [MT22] pour une description de la bibliothèque *Mathematical Components*, développée en `Coq`, et au projet *Archive of Formal Proofs* (voir [AFP]) pour la collection des résultats formalisés en `Isabelle`.

Travaux présentés :

[BDNN21] A. Baanen, S. R. Dahmen, A. Narayanan & F. A. E. Nuccio Mortarino Majno di

Capriglio – « A Formalization of Dedekind Domains and Class Groups of Global Fields » dans *12th International Conference on Interactive Theorem Proving 2021*, vol. 193, 2021, p. 5 :1–5 :19.

[BDNN22] A. Baanen, S. R. Dahmen, A. Narayanan & F. A. E. Nuccio Mortarino Majno di Capriglio – « A Formalization of Dedekind domains and class groups of global fields » , *J. Automat. Reason.* **66** (2022), no. 4, p. 611–637.

[CTB+22] J. Commelin, A. Topaz, R. Barton, A. Best, R. Brasca, K. Buzzard, Y. Dillies, F. van Doorn, F. Glöckle, M. Himmel, H. Macbeth, P. Massot, B. Mehta, S. Morrison, F. A. E. Nuccio Mortarino Majno di Capriglio, J. Riou, D. Testa & A. Yang – « Liquid Tensor Experiment », https://github.com/leanprover-community/lean-liquid/, `commit` 92f188b, 2022.

III.1 Anneaux de Dedekind et groupes de classes

avec A. Baanen, S. R. Dahmen et Ashvni N.

Tout comme au §I.1 et au §II.1, l'objet d'étude principal de cette section est le groupe de classes $\mathcal{C}\ell_K$ (et, surtout, sa finitude) d'un corps de nombres ou, plus généralement, d'un corps global K, mais cette fois-ci du point de vue de la formalisation.

Le résultat principal qu'on a formalisé, contenant l'énoncé que le groupe de classes d'un corps global L est fini, se présente sous la forme suivante[2] :

```
definition class_group.fintype_of_admissible_of_finite {R : Type*} {S : Type*}
(K : Type*) (L : Type*) [euclidean_domain R] [comm_ring S] [is_domain S]
[field K] [field L] [algebra R K] [algebra K L] [is_fraction_ring R K]
[finite_dimensional K L] [is_separable K L] [algRL : algebra R L]
[is_scalar_tower R K L] [algebra R S] [algebra S L]
[ist : is_scalar_tower R S L] [iic : is_integral_closure S R L]
{abv : absolute_value R ℤ} (adm : abv.is_admissible) [infinite R]]
[decidable_eq R] : fintype (class_group S)
```

Extrait de code 1 – Finitude du groupe de classes

L'extrait de code 1 est représentatif de l'interaction homme-machine typique de la formalisation en `lean-3`. On se propose de le discuter en détail en l'employant en guise de guide pour illustrer plusieurs spécificités du processus de formalisation, certains choix qu'on a été amené à faire, ainsi que pour définir la notion de « stathme admissible » sur laquelle notre démonstration repose.

La première différence évidente avec la formulation mathématique est que la finitude du groupe de classes est ici une *définition*, alors qu'il semblerait naturelle de s'attendre à un *théorème*. Cela provient de la façon que `lean-3` a d'interpréter la notion de finitude pour, disons, un ensemble (pour un groupe, ou une autre structure, le discours serait analogue) : déjà, au vu de la discussion dans le préambule du chapitre, il est naturel de se concentrer sur la notion de type fini, plutôt que d'ensemble fini. Toutefois, à différence de la perspective usuelle, un type fini n'est pas un type qui jouit

2. Depuis la conclusion du projet, et la parution des articles [BDNN21] et [BDNN22], la totalité du code produit a intégré la bibliothèque `mathlib`. Ce processus nous a amenés à modifier certaines déclarations pour les rendre compatibles avec l'évolution de `mathlib`, et c'est sous cette forme que nous les présentons.

d'une certaine propriété, mais plutôt[3] *un couple* `(X, h)` constituée d'un type `X : Type*` et d'un terme `h : P` de type `P : Prop` ; le terme `h` doit être interprété comme une preuve de l'énoncé (représenté par `P`) que `X` est en bijection avec une certaine liste (sans éléments dupliqués, et à permutations près) de termes de `X`. Comme, par définition, les listes sont finies, la proposition `P` correspond à l'énoncé que `X` est fini, et `h` en est une preuve, ou un « témoin de vérité ». C'est en ce sens que la finitude du groupe de classe s'interprète comme la *définition* d'un couple `(class_group S, h)` constituant un type fini.

Avant de discuter plus en détail les autres ingrédients qui apparaissent dans l'extrait de code 1, concentrons-nous sur la notion de stathme admissible[4]. Au fait, notre projet de formaliser le résultat de Dirichlet sur la finitude du groupe de classes s'est — dès le départ — heurté à la question du choix de la démonstration à suivre. La plus habituelle (voir, par exemple, [Sam67, §4.2, Théorème 2]) repose sur la théorie de Minkowski des réseaux dans les espaces euclidiens, et sur la possibilité de plonger tout corps de nombres dans un espace euclidien convenable. Lorsque le corps est une extension finie de $\mathbb{F}_p(T)$ un tel plongement n'existe évidemment pas et une stratégie différente est déployée (voir, par exemple, [Ros02, Lemma 5.6]), en s'appuyant sur le théorème de Riemann–Roch et sur le fait qu'il n'existe qu'un nombre fini de polynômes de degré borné dans $\mathbb{F}_p[T]$. Néanmoins, nombre d'ingrédients qui interviennent dans les démonstrations coïncident dans les deux cas et ceci, conjointement à la nécessité d'éviter la duplication du code, nous a poussés à chercher une démonstration commune. Ni le souhait d'une telle uniformité ni la stratégie déployée sont vraiment nouveaux, et nous renvoyons à [Sta21] pour une autre démarche, similaire à la nôtre, ainsi que pour un historique des approches présentes dans la littérature. La définition sur laquelle s'appuie notre théorème est la suivante :

Définition III.1.1. Soit A un anneau euclidien et soit $v\colon A \to \mathbb{N}$ un stathme euclidien (voir [Bou07, Chap. VII, Exercices, §1, exerc. 7]). Le stathme est dit admissible s'il existe une fonction $\mathrm{card}\colon \mathbb{R}_{>0} \to \mathbb{N}$ telle que pour tout $\varepsilon > 0$, pour tout $a \in A \setminus \{0\}$ et pour tout sous-ensemble fini $X \subseteq A$, il existe une partition

$$X = \bigcup_{i \in I} X_i$$

indexée par un ensemble fini I de cardinal borné par $\mathrm{card}(\varepsilon)$, telle que pour tout $i \in I$

$$x, x' \in X_i \Longrightarrow v\big((x \mod a) - (x' \mod a)\big) < \varepsilon \cdot v(a).$$

L'idée sous-jacente à la définition est qu'elle assure l'existence de représentants des classes d'équivalence modulo b qui sont suffisamment proches entre eux. En particulier, tant le stathme $v(n) = |n|$ sur $\mathbb{Z}$ que le stathme $v(F) = p^{\deg F}$ sur $\mathbb{F}_p[T]$ sont admissibles. Le théorème qu'on montre est le suivant :

Théorème III.1.2 ([BDNN21]). *Soit R un anneau euclidien muni d'un stathme admissible v et soit S la clôture intégrale de R dans une extension finie L de $K = \mathrm{Frac}(R)$. Le groupe de classes d'idéaux de S est alors fini.*

3. La définition de `mathlib` d'un `fintype` n'est pas exactement celle que nous présentons ici, car elle repose sur la notion de `finset` : nous faisons le choix de cette simplification dans le but de présenter la notion de `structure` sans trop alourdir la discussion.

4. La définition originale, en anglais, est celle de *admissible absolute value*.

Pour montrer le théorème, on observe que l'admissibilité du stathme v entraîne l'existence d'un ensemble fini $\Theta \subseteq R \setminus \{0\}$ tel que pour tout $x, x' \in S$ avec $x' \neq 0$, il existe $z \in S$ et $\theta \in \Theta$ tels que

$$v\big(\mathrm{N}_{L/K}(\theta x - z x')\big) < v\big(\mathrm{N}_{L/K} x'\big). \tag{III.1.1}$$

Une conséquence de (III.1.1) est le fait que toute classe dans $\mathcal{C}\ell_L$ contient un idéal *entier* J tel que

$$\prod_{\theta \in \Theta} \theta \in J,$$

et comme il n'existe qu'un nombre fini d'idéaux entiers contenant un élément non-nul fixé, la finitude énoncée est démontrée.

Revenons maintenant à l'analyse de l'extrait de code 1. Le contenu mathématique est précisément celui du Théorème III.1.2. Néanmoins, on voit que les quatre objets `R, S,K` et `L` sont d'abord introduits simplement en tant que types (dans un univers convenable, d'où le `*` dans les déclarations `Type*`), auxquels on rajoute des hypothèses, telles `[euclidean_domain R]`, ou `[is_scalar_tower R K L]` ou `{abv : admissible_value R ℤ }` : clairement, elles correspondent aux hypothèses du théorème. L'idée de « faire une hypothèse » se traduit en `lean-3` par le rajout d'un terme (typé, en général) au contexte — autrement dit, l'extrait de code 1 définit un terme de type `fintype (class_group S)`, à savoir `class_group.fintype_of_admissible_of_finite`, *dans le contexte* où `R,S,K,L` sont dans `Type*`, où l'on a fixé des termes respectivement de type `[field K]` et `[field L]` ; et aussi un terme `algRL` de type `[algebra R L]`, un autre de type `[is_scalar_tower R K L]`, etc. Le fait que ces types apparaissent entre des crochets `[` et `]` déclare que le type en question est d'une certaine *classe*, concept crucial pour la gestion des hiérarchies des constructions mathématiques dans `mathlib`[5]. Sans rentrer dans les détails (pour lesquels on renvoie par exemple à [Mat20, §4]), nous nous contentons ici de mentionner que l'emploi des classes donne lieu à des inférences analogues aux aspects « automatiques » de la hiérarchie mathématique : tout comme un corps est automatiquement un anneau et un groupe (additif), à chaque terme de type `field K` (ce qui représente une structure de corps sur le type `K`) correspondent automatiquement un terme de type `ring K` et un terme de type `add_group K`, qui représentent les structures d'anneau (*resp.* de groupe additif) héritées de celle de corps. La conséquence et que si `lean-3` doit appliquer un résultat qui est valable dans les groupes additifs (par exemple, le lemme `sub_self {G : Type*} [add_group G] : ∀ (a : G), a - a = 0`) il pourra l'appliquer aux éléments de K puisque il aura inféré l'existence d'un terme de type `add_group K` à partit du terme de type `field K`. D'autres hypothèses apparaissent dans des parenthèses rondes `(` et `)` ou des accolades `{` et `}` : la différence entre elles est trop technique pour être analysée ici (voir [Mat20, §4.2] pour une discussion), et nous allons les considérer équivalentes. À nouveau, ces hypothèses sont présentées comme des termes de types convenables : par exemple, les hypothèses du Théorème III.1.2 que R soit euclidien — donc, muni d'un stathme — et que ce stathme soit admissible, correspondent à l'apparition, dans le contexte de l'extrait de code 1, des termes `{abv : absolute_value R ℤ }` (donc, `abv` est le stathme) ainsi que `(adm : abv.is_admissible)`.

La liste des hypothèses peut paraître redondante. Par exemple, le terme `algRL` qui apparaît dans la déclaration `[algRL : algebra R L]` représente le fait que, dans notre

5. Ce concept est en fait commun à plusieurs assistants de preuve, comme `Coq` (voir [SvdW11]) ou `Isabelle` (voir [HW07]).

contexte, L est muni d'une structure de R-algèbre, ce qui semble évident. Le problème est qu'à priori il pourrait y avoir plusieurs structures de R-algèbre sur L (par exemple, lorsque R admet des automorphismes non-triviaux, ce qui est le cas lorsqu'on remplace l'anneau $\mathbb{F}_p[T]$ par $\mathbb{F}_q[T]$ avec $q = p^a$ pour $a > 1$) : ceci est normalement passé sous silence dans un texte mathématique — en considérant qu'il existe une structure « préférentielle », ou « naturelle » — mais doit être spécifié lorsqu'on travaille avec un assistant de preuve.

Un discours analogue concerne le concept de « corps des fractions ». Pour le discuter, examinons l'extrait de code suivant, toujours issu de [BDNN21] :

```
theorem is_dedekind_domain_iff (A : Type*) [comm_ring A] [is_domain A]
(K : Type*) [field K] [algebra A K] [is_fraction_ring A K] :
is_dedekind_domain A ↔ is_noetherian_ring A ∧ ring.dimension_le_one A ∧
∀ {x : K} is_integral A x → (∃ (y : A), ⇑(algebra_map A K) y = x)
```

Extrait de code 2 – Indépendance du corps des fractions choisi

À première vue, l'extrait de code 2 semblerait être la *définition* d'un anneau de Dedekind. En réalité, il s'agit de l'énoncé que la propriété d'être de Dedekind est indépendante de la construction de K : il suffit qu'il satisfasse à la condition d'être *un* corps des fractions (ici rendue par l'existence d'un terme de type `is_fraction_ring A K`) pour pouvoir y tester la propriété d'être « intégralement clos » apparaissant dans la définition d'anneau de Dedekind. Il s'agit ici d'un phénomène typique du processus de formalisation, et auquel on a été confronté également dans notre choix de la définition de corps de nombres : souvent, un objet est défini par une propriété universelle et aucune construction « préférentielle » n'existe, ce qui rend nécessaire de vérifier que les propriétés dont il jouit ne dépendent pas de la présentation choisie. Dans le cas du corps des fractions, bien qu'une réalisation explicite en tant que localisé au monoïde des éléments non-nuls existe, elle n'est pas l'unique construction possible. Considérons par exemple la situation où A est un anneau de Dedekind, disons de corps des fractions K, défini comme le localisé $S_A^{-1}A$ pour $S_A = A \setminus \{0\}$; soit $P \in K[X]$ un polynôme irréductible et posons $L = K[X]/P$, puis définissons B comme la clôture intégrale de A dans L. Dans ce contexte, on sait que B est un anneau de Dedekind dont le corps des fractions $S_B^{-1}B$ (pour $S_B = B \setminus \{0\}$) est *isomorphe* à L, sans lui être *égal*. Il est donc important de vérifier que la propriété d'être intégralement clos qui apparaît dans la définition d'anneau de Dedekind est en fait indépendante du choix d'une représentation explicite d'un corps des fractions.

La discussion précédente nous permet d'aborder l'autre contribution principale du travail [BDNN21], à savoir la formalisation en `lean-3` de la définition d'anneau de Dedekind. Il est bien connu (voir, par exemple, [Bou07, Chap. VII, §2, no. 2, Théorème 1]) que les propriétés suivantes d'un anneau commutatif A sont équivalentes :

DD1) A est un anneau intègre noethérien, intégralement clos et de dimension de Krull égale à 1 ;

DD2) A est un anneau intègre noethérien tel que toute localisation $A_{\mathfrak{P}}$ à un idéal premier non nul $\mathfrak{P}$ est un anneau de valuation discrète ;

DD3) A est un anneau intègre tel que tout idéal fractionnaire non-nul dans son corps des fractions est inversible.

Elles ont été formalisées dans les formes suivantes (dans chacune, le contexte est celui d'un anneau commutatif intègre A, formalisé comme expliqué pour l'extrait de code 1, avec les déclarations `{A : Type*} [comm_ring A] [is_domain A]`) :

DD1) La première définition, analogue de DD1), est une `structure`, car elle contient trois champs, et a l'attribut `class` pour activer l'algorithme d'inférence automatique :

```
@[class] structure is_dedekind_domain  : Prop
is_noetherian_ring : is_noetherian_ring A
dimension_le_one : ring.dimension_le_one A
is_integrally_closed : is_integrally_closed A
```

DD2) La deuxième définition, analogue de DD2) est une `structure` et porte un autre nom parce qu'elle définit en effet un type différent (toujours dans `Prop`) :

```
structure is_dedekind_domain_dvr : Prop
is_noetherian_ring : is_noetherian_ring A
is_dvr_at_nonzero_prime : ∀ (P : ideal A), P ≠ ⊥ → ∀ (ᾰ : P.is_prime),
    discrete_valuation_ring (localization.at_prime P)
```

Le résultat suivant montre que la première propriété entraîne en fait la deuxième :

```
theorem is_dedekind_domain.is_dedekind_domain_dvr [is_dedekind_domain A] :
is_dedekind_domain_dvr A
```

Dans le contexte `{A : Type*} [comm_ring A] [is_domain A]`, s'il existe un terme de type `is_dedekind_domain A`, nécessairement unique à cause de l'axiome de *proof irrelevance* (donc, si la propriété d'être de Dedekind est satisfaite), alors[6] le théorème fournit aussi un (unique) terme de type `is_dedekind_domain_dvr A`.

DD3) La dernière définition, analogue de DD3), est une `definition` et définit un type dans `Prop`. Le `theorem is_dedekind_domain_inv.is_dedekind_domain` montre que cette dernière propriété entraîne la première, comme précédemment[7] :

```
definition is_dedekind_domain_inv : Prop :=
∀ (I : fractional_ideal (non_zero_divisors A) (fraction_ring A)),
I ≠ ⊥ → I * I⁻¹ = 1
```

Les trois extraits de code apparaissant dans DD1)–DD3) sont plutôt proches des définitions « usuelles » qu'on pourrait trouver dans un texte mathématique. Il y a néanmoins certaines différences, que nous nous proposons de discuter dans ce qui suit, toujours afin de décrire le processus de formalisation.

Dans DD2), la propriété `is_dvr_at_nonzero_prime` demande que pour tout idéal $\mathfrak{P}$ non nul, *et pour toute hypothèse* $\breve{\alpha}$ que cet idéal est premier, la localisation $A_{\mathfrak{P}}$ soit un anneau de valuation discrète. On voit que la propriété d'être « non nul » se présente sous la forme `P ≠ ⊥` : ici, $\bot$ dénote l'élément minimal de l'ensemble partiellement ordonné des idéaux de A. L'apparence de ce concept témoigne de l'approche de `mathlib` vis-à-vis des idéaux d'un anneau : ils sont définis comme les sous-modules du A-module A et la collection des sous-A-modules d'un A-module M est munie d'une structure d'ensemble partiellement ordonné (par inclusion), dont l'élément minimal est le sous-module $\bot = \{0\} \subseteq M$ et l'élément maximal est $\top = M \subseteq M$. L'avantage de regarder la

6. L'autre implication doit encore être formalisée dans `mathlib`.
7. À nouveau, l'implication inverse n'a pas encore été formalisée dans `mathlib`.

collection des sous-modules, ou des idéaux, comme un ensemble partiellement ordonné provient de la considération suivante : un idéal de A, dans `mathlib`, n'est pas défini comme un *sous-ensemble* de A stable par rapport aux opérations usuelles ; plutôt, il est une `structure` définie par quatre champs

```
I.val : set A
I.add_mem : ∀ {a b : M}, a ∈ I.val → b ∈ I.val → a + b ∈ I.val : Prop
I.zero_mem : 0 ∈ I.val : Prop
I.smul_mem : ∀ (c : R) {x : M}, x ∈ I.val → c • x ∈ I.val : Prop
```

Le premier champs correspond à l'ensemble sous-jacent à l'idéal, et les trois suivants aux propriétés satisfaites par I. Donc, se donner trois idéaux $I, J, K \subseteq A$ revient à se donner trois termes `I=(I.val,I.add_mem,I.zero_mem,I.smul_mem)`, `J=(J.val, J.add_mem,J.zero_mem,J.smul_mem)` et `K=(K.val,K.add_mem,J.zero_mem,K.smul_mem)` de type `ideal A`. Il suit que la somme $I + J$ n'est pas seulement définie en termes des ensembles `I.val` et `J.val` sous-jacents à `I` et `J`, mais par un quadruplet[8]

```
(I+J).val = {x+y : x ∈ I.val, y ∈ J.val} : set A
(I+J).add_mem = ... : Prop
(I+J).zero_mem = 0 ∈ (I+J).val : Prop
(I+J).smul_mem = ... : Prop
```

Supposons maintenant de vouloir montrer l'associativité de la somme d'idéaux, donc l'égalité $(I + J) + K = I + (J + K)$: traduite sous la forme `(I+J) + K = I + (J + K)` elle devient l'égalité entre deux quadruplets, aux détails éminemment rébarbatifs et lointains de la pratique mathématique usuelle. Or, la somme $I + J$ de deux idéaux est le plus petit idéal contenant I et J et réalise donc la borne supérieure `I ⊔ J` par rapport à l'ordre d'inclusion dans l'ensemble partiellement ordonné des idéaux de A. Une fois établi que `ideal A` est muni d'une telle structure, l'énoncé en vue se traduit sous la forme `(I ⊔ J) ⊔ K = I ⊔ (J ⊔ K)`. Cette égalité n'est rien d'autre que l'associativité de l'opération de « prendre la borne supérieure » dans un ensemble partiellement ordonné, fait complètement général et indépendant de la théorie des idéaux ; la preuve ne prend donc qu'une ligne :

```
lemma ideal.add_assoc {I J K : ideal A} : (I + J) + K = I + (J + K) :=
begin
  exact sup_assoc,--goals accomplished
end
```

Pour revenir aux anneaux de Dedekind, la décision a été prise — après discussion avec la communauté `mathlib` — d'utiliser comme définition celle d'anneau commutatif noethérien intègre, de dimension de Krull inférieure ou égale à 1 et intégralement clos dans son (ou dans un de ses…) corps des fractions, donc celle qui apparaît dans DD1). Il s'agit en effet du critère le plus facile à vérifier et qui permet le plus aisément de montrer que des anneaux satisfaisant certaines propriétés sont en fait de Dedekind : c'est le cas, par exemple, de l'anneau d'entiers d'une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$. D'autre part, la démonstration que tout idéal fractionnaire se factorise de façon unique en produit de puissances (entières) d'idéaux premiers est d'abord obtenue pour les anneaux qui satisfont `is_dedekind_domain_inv`, et « transférée » aux an-

8. Afin de ne pas alourdir le manuscrit, on ne donne pas les détails des termes `(I+J).add_mem` ou `(I+J).smul_mem`.

neaux de Dedekind grâce à `is_dedekind_domain_inv.is_dedekind_domain`. Finalement, `is_dedekind_domain_dvr` est évidemment très pratique afin de formaliser dans `mathlib` que les localisés des anneaux de Dedekind à leurs idéaux maximaux sont encore de Dedekind.

Nous clôturons cette section en mentionnant quelques projets qui se sont basés sur notre travail. En premier lieu, Best, Brasca, Rodriguez et Birkbeck sont en train de formaliser dans [BBBR23], en s'appuyant sur `mathlib`, la démonstration du théorème de Fermat pour les premiers réguliers. Rappelons qu'un nombre premier p est dit *régulier* lorsque $p \nmid h_{\mathbb{Q}(\mu_p)}$. Évidemment, à la fois les propriétés de base du corps de nombres $\mathbb{Q}(\mu_p)$ — par exemple, le fait que son anneau d'entiers soit de Dedekind — et la finitude du groupe $\mathcal{C}\ell_{\mathbb{Q}(\mu_p)}$ sont nécessaires, ne serait-ce que pour énoncer le résultat. Un autre projet qui a utilisé de façon cruciale les propriétés des anneaux de Dedekind est le travail [deF22], où de Frutos-Fernández formalise la définition et les propriétés principales de l'anneau des adèles et du groupe des idèles d'un corps global : la formalisation s'appuie sur [BDNN22], entre autre car la première partie du travail est consacrée à la définition de la valuation adique associée à un idéal maximal d'un anneau de Dedekind. Finalement, mentionnons le travail [AX23] où Angdinata et Xu ont formalisé la définition d'une loi de groupe (abélien) sur les points rationnels d'une courbe elliptique définie sur un corps F. Il est bien connu que définir une addition sur ces points n'est pas compliqué, mais que la démonstration qu'une telle opération est *associative* est épineuse : la stratégie principale dans [AX23] est de définir une fonction injective `to_class : W(F) ↪ class_group S` de l'ensemble `W(F)` des solutions F-rationnelles à une équation de Weierstraß qui définit la courbe elliptique, vers le groupe de classes d'idéaux d'un anneau de Dedekind `S` convenable. Ils montrent ensuite que `to_class` commute avec les additions définies sur `W(F)` et sur `class_group S`, respectivement : l'associativité souhaitée suit, grâce à l'injectivité de `to_class` (et au fait que la loi de groupe sur `class_group S` est associative).

Comme tout projet visant à intégrer `mathlib`, il est compliqué de donner une estimation précise du nombre de lignes de code « propres » à notre travail. Un calcul grossier nous restitue une valeur d'environs 5000 lignes de code rajoutées à `mathlib` en lien direct avec les anneaux de Dedekind et le groupe de classes, et d'environs 2500 lignes de codes inhérentes à des notions mathématiques plus primitives.

III.2 Le *Liquid Tensor Experiment*

avec J. Commelin, A. Topaz *et al.*

Lorsque Scholze proposa[9] le *Liquid Tensor Experiment*, une équipe de collaborateurs de la bibliothèque `mathlib` s'attaqua à la formalisation du [CS19a, Theorem 6.5], sous la forme du [Sch22, Theorem 1.1]. Bientôt il devint clair que le projet pouvait se décomposer naturellement en deux parties, la première ayant pour objectif la formalisation de [CS19a, Theorem 9.4] et la deuxième visant à déduire [Sch22, Theorem 1.1] du résultat principal de la première partie. Cette première partie s'acheva en exactement six mois (voir [Sch21a]) et la deuxième environs un an après (voir [Mat22]). Dans les

9. Initialement, le *Liquid Tensor Exeriment* fut proposé sous forme de billet dans le blog de Buzzard à l'adresse https://xenaproject.wordpress.com/2020/12/05/liquid-tensor-experiment/. Dans notre texte, nous nous référons à l'article [Sch22] qui reprend le billet sous forme d'article de revue.

références citées, il est évident que le rôle joué par Commelin et Topaz est tout particulier. Je fais donc le choix d'illustrer brièvement les mathématiques dont il est question dans le *Liquid Tensor Experiment* et de décrire après mes apports au projet [CTB+22] : en aucun cas il ne sera question de mettre sur un plan d'égalité les contributions de Commelin et Topaz avec les miennes.

Bien que les applications de la théorie des espaces vectoriels liquides (ou, plutôt, des modules sur les anneaux condensés analytiques) que Clausen et Scholze ont en vue soient principalement orientées vers la géométrie algébrique (voir [CS22]), je vais me concentrer sur les aspects en lien avec l'analyse fonctionnelle. Le point de départ est l'observation, bien classique, que l'analyse fonctionnelle et l'algèbre homologique interagissent assez mal entre elles. En premier lieu, les espaces vectoriels topologiques ne forment pas une catégorie abélienne : dénotons par $\mathbb{R}^\delta$ l'ensemble des réels muni de la topologie discrète, vu comme espace vectoriel réel, et par $\mathbb{R}$ le même espace muni de la topologie euclidienne. Alors, l'identité (ensembliste)

$$\mathrm{id}\colon \mathbb{R}^\delta \longrightarrow \mathbb{R} \tag{III.2.1}$$

est clairement linéaire et continue, à noyau et conoyau triviaux, mais n'est pas un isomorphisme d'espaces vectoriels topologiques. Dans le même esprit, considérons la catégorie Ban des espaces de Banach, avec applications linéaires continues comme morphismes : il ne s'agit pas d'une catégorie abélienne et elle n'est pas stable par extensions. En effet, d'une part, il est facile de construire des applications linéaires continues $T\colon V \to W$ entre $\mathbb{R}$-espaces de Banach dont l'image n'est pas fermée (ni complète, donc), et donc telle que la formule

$$V/\operatorname{Ker} T \cong \operatorname{Im} T$$

n'est pas valable, contrairement à ce qui se passe dans toute catégorie abélienne. D'autre part, Ribe a construit dans [Rib79] un espace vectoriel complet et métrisable F qui n'est pas localement convexe (en particulier, il n'est pas un espace de Banach) mais qui apparaît dans une suite exacte courte

$$0 \longrightarrow \mathbb{R} \longrightarrow F \longrightarrow \ell^1(\mathbb{R}) \longrightarrow 0, \tag{III.2.2}$$

ce qui montre que Ban n'est pas stable par extensions. Aussi, il n'y a pas un choix unique de produit tensoriel dans Ban : étant donnés $V, W \in \mathsf{Ban}$ il existe (au moins) deux définitions de produit tensoriel complété, le produit tensoriel projectif $V \otimes_\pi W \in \mathsf{Ban}$ et le produit tensoriel injectif $V \otimes_\varepsilon W \in \mathsf{Ban}$: en général, il s'agit d'espaces non-isomorphes, et chacun est « naturel » selon le point de vue qu'on prend pour la notion de « naturalité ».

Le formalisme des espaces condensés, introduit initialement dans [CS19b], définit un premier cadre où la topologie et l'algèbre homologique interagissent bien, mais celui-ci doit être raffinée afin de prendre en compte la notion de complétude caractéristique des espaces apparaissant en analyse fonctionnelle. Nous allons décrire le premier cadre, suivi par le raffinement en question. Commençons par la

Définition III.2.1. Un groupe abélien condensé est un faisceau en groupes abéliens sur le site proétale du singleton $\{*\}$: en d'autres mots, il s'agit d'un foncteur contravariant

$$\mathcal{G}\colon \mathsf{ProFin} \longrightarrow \mathsf{Ab}$$

de la catégorie des ensembles profinis[10] vers la catégorie des groupes abéliens, satisfaisant les conditions de faisceau :

i) $\mathcal{G}(\emptyset) = \{*\}$ et pour tout couple d'ensembles profinis S_1, S_2, la fonction

$$\mathcal{G}(S_1 \sqcup S_2) \longrightarrow \mathcal{G}(S_1) \times \mathcal{G}(S_2)$$

est bijective ;

ii) pour toute surjection $S' \to S$ d'ensembles profinis, la fonction

$$\mathcal{G}(S) \longrightarrow \{x \in \mathcal{G}(S') \big| p_1^*(x) = p_2^*(x) \in \mathcal{G}(S' \times_S S')\}$$

est bijective, où $p_1, p_2 \colon S' \times_S S' \to S'$ sont les deux projections.

Il est prouvé dans [CS19b, Theorem 2.2] que les groupes abéliens condensés forment une catégorie abélienne qui satisfait aux axiomes AB3–AB6 et AB3*–AB4* de [Gro57] : elle est stable par limites et colimites ; les produits, les sommes directes et les colimites filtrantes sont exactes ; et les colimites filtrantes commutent avec les produits. Elle est en plus munie d'un ensemble de générateurs projectifs compacts, ainsi que d'un produit tensoriel qui la rend symétrique monoïdale ; on la note $\mathsf{Cond}(\mathsf{Ab})$. Ce qui la rend particulièrement intéressante pour notre étude est l'existence d'un foncteur fidèle

$$\mathsf{AbTop} \longrightarrow \mathsf{Cond}(\mathsf{Ab})$$

qui envoie tout groupe abélien topologique G sur le groupe condensé $\underline{G} \colon S \mapsto \mathrm{Cont}(S, G)$, foncteur qui est en plus *plein* lorsqu'on le restreint aux groupes abéliens topologiques compactement engendrés. On peut donc regarder $\mathsf{Cond}(\mathsf{Ab})$ comme un élargissement de la catégorie des groupes abéliens topologiques qui a de bonnes propriétés algébriques.

L'étape suivante consiste à remplacer les groupes abéliens topologiques par les $\mathbb{R}$-espaces vectoriels topologiques : on obtient la catégorie $\mathsf{Mod}_{\underline{\mathbb{R}}}$ des modules (en groupes abéliens condensés) sur $\underline{\mathbb{R}}$, où $\underline{\mathbb{R}}$ dénote l'image de $\mathbb{R}$ dans la catégorie des anneaux condensés. Néanmoins, si l'objectif est d'avoir à disposition une théorie homologique capable de contrôler l'analyse fonctionnelle, cette catégorie est un choix trop grossier : aucun analogue des propriétés métriques, ni de complétude, n'a été introduit. Pour résoudre ce problème, Clausen–Sholze définissent une sous-catégorie de $\mathsf{Mod}_{\underline{\mathbb{R}}}$ convenable, en s'appuyant sur le théorème suivant ; nous n'avons volontairement pas encore donné la définition de structure analytique, afin d'en motiver l'introduction *à partir* de ce résultat.

Théorème III.2.2 ([CS19b, Proposition 7.5]). *Soit $(\mathcal{A}, \mathcal{F}_\mathcal{A})$ une structure analytique sur un anneau condensé $\mathcal{A}$. La sous-catégorie pleine $\mathsf{An}_\mathcal{A} \subseteq \mathsf{Mod}_\mathcal{A}$ formée des $\mathcal{A}$-modules M tels que, pour tout ensemble extrêmement discontinu*[11] *S, la fonction*

$$\mathrm{Hom}_\mathcal{A}(\mathcal{F}_\mathcal{A}[S], M) \longrightarrow M(S)$$

10. Il faut mentionner ici que la catégorie des ensembles profinis n'est pas petite. On va négliger cet aspect dans notre exposition, mais observons que lors du processus de formalisation les choix d'univers ont joué un rôle important.

11. C'est ainsi que Bourbaki traduit dans [Bou71, Chapitre I, Exercices, §11, exerc. 21] le terme *extremally disconnected*, qui est celui employé par Clausen–Scholze. Je remercie Sophie Morel pour la référence bibliographique.

est un isomorphisme, est une catégorie abélienne stable par limites, colimites et extensions (extensions dans $\mathsf{Cond}(\mathsf{Ab})$*). Les objets* $\mathcal{F}_{\mathcal{A}}(S)$*, pour* S *extrêmement discontinu, forment une famille de générateurs projectifs compacts. Le foncteur d'inclusion admet un adjoint à gauche*

$$\mathsf{Mod}_{\mathcal{A}} \longrightarrow \mathsf{An}_{\mathcal{A}} \colon M \longmapsto M \otimes_{\mathcal{A}} \mathcal{F}_{\mathcal{A}} \tag{III.2.3}$$

qui est la seule extension de $\mathcal{A}(S) \mapsto \mathcal{F}_{\mathcal{A}}(S)$ *préservant les colimites. Lorsque* $\mathcal{A}$ *est commutatif, il existe un unique produit tensoriel* $- \otimes_{\mathcal{A}^{\mathsf{An}}} -$ *rendant le foncteur dans* (III.2.3) *symétrique monoïdal.*

Le théorème précédent[12] suggère une solution naturelle au problème de trouver un cadre homologique convenable pour l'analyse fonctionnelle : montrer que l'anneau condensé $\underline{\mathbb{R}}$ est muni d'une structure analytique et prouver que la catégorie $\mathsf{An}_{\underline{\mathbb{R}}}$ produite dans le Théorème III.2.2 contient Ban comme sous-catégorie pleine et fidèle, et qu'en plus le produit tensoriel $- \otimes_{\underline{\mathbb{R}}^{\mathsf{An}}} -$ interagit bien avec $- \otimes_{\pi} -$ et $- \otimes_{\varepsilon} -$.

Avant de continuer, nous devons au lecteur la

Définition III.2.3 ([CS19b, Definition 7.1]). Soit $\mathcal{A}$ un anneau condensé. Une structure d'anneau pré-analytique sur $\mathcal{A}$ est la donnée d'un foncteur

$$\mathcal{F}_{\mathcal{A}} \colon \{\text{ensembles extrêmement discontinus}\} \longrightarrow \mathsf{Mod}_{\mathcal{A}}$$

à valeur dans les $\mathcal{A}$-modules (en groupes abéliens condensés), qui envoie les réunions disjointes finies sur les produits finis, avec une transformation naturelle $S \mapsto \mathcal{F}_{\mathcal{A}}(S)$.

La structure pré-analytique est dite analytique si pour tout couple d'ensembles I, J, toutes collections d'ensembles extrêmement discontinus $\{T_i\}_{i\in I}, \{T'_j\}_{j\in J}$ et tout morphisme de $\mathcal{A}$-modules

$$f \colon \bigoplus_{i\in I} \mathcal{F}_{\mathcal{A}}(T_i) \longrightarrow \bigoplus_{j\in J} \mathcal{F}_{\mathcal{A}}(T'_j)$$

de noyau $\mathcal{K}$, il y a un isomorphisme

$$\mathbf{R}\underline{\mathrm{Hom}}_{\mathcal{A}}(\mathcal{F}_{\mathcal{A}}(S), \mathcal{K}) \xrightarrow{\cong} \mathbf{R}\underline{\mathrm{Hom}}_{\mathcal{A}}(\mathcal{A}(S), \mathcal{K}) \tag{III.2.4}$$

pour tout ensemble extrêmement discontinu S.

Notons que, dans la Définition III.2.3, rien n'impose que la structure d'anneau analytique sur un anneau condensé $\mathcal{A}$ soit unique. En effet, la construction de [CS19a, §6] produit une infinité de structures d'anneau analytique sur $\underline{\mathbb{R}}$, indexées par $p \in]0, 1]$. Nous allons maintenant les décrire.

Fixons un réel $0 < p \leqslant 1$. Afin de donner une structure analytique sur $\underline{\mathbb{R}}$ il faut tout d'abord se donner un foncteur (nous remplaçons la notation $\mathcal{F}_{\underline{\mathbb{R}}}$ par $\mathscr{M}_{<p}$, en cohérence avec [CS19a])

$$\mathscr{M}_{<p} \colon \{\text{ensembles extrêmement discontinus}\} \longrightarrow \mathsf{Mod}_{\underline{\mathbb{R}}}.$$

Pour le définir, soit $p' < p$ et soit S un ensemble profini, dont nous choisissons une présentation $S = \varprojlim_i S_i$, avec les S_i finis : posons

$$\mathscr{M}_{p'}(S) = \bigcup_{c\geqslant 0} \varprojlim_i \mathbb{R}[S_i]_{\ell^{p'}\leqslant c},$$

12. La [CS19b, Proposition 7.5] contient aussi une deuxième partie relative à la version dérivée de l'inclusion $\mathsf{An}_{\mathcal{A}} \subseteq \mathsf{Mod}_{\mathcal{A}}$, mais nous ne la discutons pas dans ce texte.

où $\mathbb{R}[S_i]_{\ell^{p'}\leqslant c}$ est le sous-espace de $\mathbb{R}[S_i]$ formé des vecteurs $v=(v_s)$ tels que $\sum_s |v_s|^{p'}\leqslant c$. La valeur du foncteur $\mathscr{M}_{<p}$ sur S est alors la limite inductive

$$\mathscr{M}_{<p}(S)=\varinjlim_{p'<p}\mathscr{M}_{p'}(S). \tag{III.2.5}$$

On vérifie sans trop de difficulté que les conditions de commutation aux réunions disjointes finies de la Définition III.2.3 sont satisfaites. Ce qui rend ces espaces intéressants est qu'ils jouissent d'une propriété universelle de prolongement des fonctions continues : en effet, pour tout espace condensé $V\in\mathsf{Mod}_{\underline{\mathbb{R}}}$ et toute fonction continue $f\colon S\to V$ définie sur un ensemble profini S, il existe une unique extension

$$\tilde{f}\colon \mathscr{M}_{<p}(S)\longrightarrow V \tag{III.2.6}$$

qui est un morphisme de $\underline{\mathbb{R}}$-espaces condensés. En quelque sorte, donc, ils jouent le rôle « d'objet libre sur S » dans la catégorie $\mathsf{Mod}_{\underline{\mathbb{R}}}$, mais avec une condition de croissance contrôlée par p. Cette analogie est d'ailleurs la clé pour montrer que la structure pré-analytique qu'on vient de définir sur $\underline{\mathbb{R}}$ est analytique : en effet, demander l'existence de l'isomorphisme (III.2.4) revient à demander que les $\mathscr{M}_{<p}(S)$ coïncident avec les objets libres $\underline{\mathbb{R}}[S]$ au moins dans la catégorie dérivée (et pour S extrêmement discontinu). Une réduction esquissée dans [CS19a, p. 36] réduit (III.2.4) à montrer le[13]

Théorème III.2.4. *Soient $0<p'<p\leqslant 1$ deux réels, soit S un ensemble profini et soit V un $\mathbb{R}$-espace vectoriel topologique qui est un p-espace de Banach (vu comme objet de $\mathsf{Mod}_{\underline{\mathbb{R}}}$). Alors*

$$\mathrm{Ext}^i_{\mathsf{Cond(Ab)}}(\mathscr{M}_{p'}(S),V)=0$$

pour tout $i\geqslant 1$.

La démonstration du Théorème III.2.4 était l'objectif principal du projet [CTB+22]. Une fois démontré, il donne une structure analytique (qui dépend de p) sur $\underline{\mathbb{R}}$, et le Théorème III.2.2 produit une catégorie abélienne, stable par extensions, et symétrique monoïdale, dénoté Liq_p, dont les objets sont les « espaces vectoriels p-liquides ». Elle reçoit un foncteur plein et fidèle

$$\underline{\cdot}\colon \mathsf{Ban}\longrightarrow \mathsf{Liq}_p,$$

qui s'étend à tous les $\mathbb{R}$-espaces vectoriels topologiques, et tel que pour tout couple d'espaces nucléaires V,W on a $\underline{V\otimes_\pi W}\cong \underline{V}\otimes_{\mathsf{Liq}_p}\underline{W}$. Elle constitue donc un cadre convenable pour exploiter les techniques d'algèbre homologique en analyse fonctionnelle, au moins pour les espaces de Banach : la même chose reste d'ailleurs vraie en remplaçant Ban par Ban_p, la catégorie des p-espaces de Banach, pour tout $0<p\leqslant 1$.

La construction de la catégorie Liq_p met en évidence l'importance de la définition d'une structure d'anneau analytique sur $\underline{\mathbb{R}}$, à travers le Théorème III.2.4 : c'est à ce niveau que se situe mon apport à [CTB+22]. Comme discuté à [CS19a, p. 36], la définition en question repose sur une technique plutôt inusuelle, à savoir un mélange de structures profinies et de structures continues réelles. En effet, les briques fondamentales de la théorie des espaces condensés sont les ensembles profinis (et même ceux extrêmement discontinus), et afin de calculer les foncteurs dérivés qui apparaissent dans le

13. Un survol sur les définitions de base des p-espaces de Banach se trouve au §III.3.3.

Théorème III.2.4 il faut trouver des résolution projectives d'espaces vectoriels réels *par des ensembles profinis !* Pour ce faire, Clausen–Scholze s'appuient sur la suite exacte apparaissant dans [CS19a, p. 44], dont la formalisation prend la forme suivante :

```
theorem θ_φ_exact {S : Fintype} (r p : ℝ≥0) [hr : r < 1] [hr' : 0 < r]
(h_rp : r = 2^(-p)) (F : 𝓛 r S ) (hF : θ r p F = 0) : ∃ G, φ G = F :=
```

Extrait de code 3 – L'exactitude de la suite exacte de spécialisation

Afin de décrire le contenu de l'extrait de code 3, introduisons un peu de notation. Soit `S : Fintype` un ensemble fini et `r < 1` un réel non négatif : on dénote par $\mathscr{L}$ `r S` l'anneau des « mesures de Laurent d'ordre `r` sur `S` », qui est la `structure` suivante :

```
structure 𝓛 (r : ℝ≥0) (S : Fintype) :=
(to_fun   : S → ℤ → ℤ)
(summable : ∀ s : S, summable (λ n ,|to_fun s n| * r ^ n))
```

Il s'agit donc des collections finies (indexées par `S`) des séries de Laurent $\mathtt{f_s} \in \mathbb{Z}(\!(T)\!)$ qui donnent lieu à des séries de puissances absolument convergentes sur le disque fermé de rayon `r`. Maintenant, on peut considérer l'équivalent réel de $\mathscr{L}$, où l'on fixe un réel non négatif `p < 1` (pour l'instant, `r` et `p` n'ont pas de rapport) : il est donné par la

```
definition 𝓜 (p : ℝ≥0) (S : Fintype) := S ⟶ ℝ
```

Ceci n'est rien d'autre que l'espace vectoriel $\mathbb{R}^{\mathtt{S}} = (\mathtt{S} \to \mathbb{R})$ muni de la norme ℓ^p définie par $\|\mathtt{F}\| = \sum$ `s ,| F s | ^ p`. Définissons alors le morphisme θ `r p` : $\mathscr{L}$ `r S` $\to$ $\mathscr{M}$ `p S` comme l'évaluation en $\left(\frac{1}{2}\right)$:

```
definition θ (r p : ℝ≥0) (S : Fintype) : (𝓛 r S) ⟶ 𝓜 p S :=
  λ F s, tsum (λ n, (F s n) * (1/2) ^ n)
```

Observons que, lorsque `S = {*}`, l'anneau des mesures de Laurent se réduit aux séries de Laurent avec une condition de convergence et l'espace $\mathscr{M}$ `p {*}` n'est rien d'autre que $\mathbb{R}$ (avec une valeur absolue renormalisée). Le premier résultat formalisé a été la preuve que tout nombre réel $x \in \mathbb{R}$ admet une « expansion $\left(\frac{1}{2}\right)$-adique » à coefficient entiers (chose qui entraîne facilement le même résultat pour `S` fini quelconque) :

```
lemma θ_surjective  (r p : ℝ≥0) (x : ℝ) [hr : r < 1] : ∃ (F : 𝓛 r {*}),
 (θ r p {*}) F = x :=
```

Outre la surjectivité de θ, il a été aussi question d'en étudier le noyau : il est clair que si une série de Laurent $f(T) \in \mathbb{Z}(\!(T)\!)$ est de la forme $f(T) = (2T-1)g(T)$ pour une autre série $g(T) \in \mathbb{Z}(\!(T)\!)$, alors $f\left(\frac{1}{2}\right) = 0$. Le point crucial a été de formaliser un résultat de Harbater (voir [Har84, Theorem 1.2 (b)]) qui montre que le noyau dans $\mathscr{L}$ `r {*}` de l'évaluation en $\left(\frac{1}{2}\right)$ est l'idéal principal engendré par $(2T-1)$: ce qui n'est pas évident est que diviser une série s'annulant en $\left(\frac{1}{2}\right)$ par $(2T-1)$ donne une série qui a encore les propriétés de convergence requises pour être un élément de $\mathscr{L}$ `r {*}` . Pour le formaliser, j'ai en premier lieu formalisé la multiplication par l'élément $(2T-1)$ (où les variables `r` et `S` sont désormais implicites), simplement en tant qu'opération sur les coefficients afin d'éviter de définir une `instance : has_mul` $\mathscr{L}$ `r S` de multiplication interne sur le groupe additif des mesures :

```
definition φ : 𝓛 r S ⟶ 𝓛 r S :=
λ F, shift (1) F - 2 • F
```

Ensuite, on peut définir un opérateur ψ: $\mathrm{Ker}(\mathrm{eval}_{1/2}) \to \mathscr{L}$ r S comme suit :

```
definition ψ (F : 𝓛 r S) (hF : θ r p F = 0) : 𝓛 r S :=
{ to_fun := λ s n, if F.d ⩽ n then
    ∑ l in range (n - F.d).nat_abs.succ, F s (n - 1 - l) * (2 ^ l)
    else 0,
  summable' := ...
```

Finalement, j'ai prouvé que, lorsque $r = 2^{(-p)}$, le noyau de l'évaluation coïncide bien avec l'image de φ, en montrant que toute mesure F telle que l'évaluation en $\left(\frac{1}{2}\right)$ vaut 0 est de la forme φG =(2T-1)G pour une mesure G convenable (en pratique, il s'agit de G = ψF) :

```
lemma θ_φ_split_exact (h_rp : r = 2^(-p)) (F : 𝓛 r S) (hF : θ r p F = 0) :
   φ(ψ F hF) = F :=
```

Extrait de code 4 – La détermination du noyau de θ, fonction d'évaluation en $\left(\frac{1}{2}\right)$

On peut maintenant revenir à l'extrait de code 3. L'énoncé du théorème *ibid.* est l'exactitude au milieu de la suite exacte

$$0 \longrightarrow \mathscr{L}\ \mathtt{r}\ \mathtt{S} \xrightarrow{\varphi} \mathscr{L}\ \mathtt{r}\ \mathtt{S} \xrightarrow{\theta\ \mathtt{r}\ \mathtt{p}\ \mathtt{S}} \mathscr{M}\ \mathtt{p}\ \mathtt{S} \longrightarrow 0 \tag{III.2.7}$$

pour tout 0 < p < 1 et pour r = 2^(-p). Alors que le terme h_rp dans l'extrait de code 4 était seulement une hypothèse technique, nécessaire lors de la formalisation à cause de la définition de mathlib de l'opérateur d'évaluation[14], dans (III.2.7) la relation entre r et p est censée garder trace des topologies en jeu. En effet, tels qu'on les a présentés jusqu'ici, les résultats précédents sont indépendants du choix de la norme ℓ^p sur l'espace des mesures $\mathscr{M}$ p S et il n'a pas été question de munir l'espace $\mathscr{L}$ r S d'aucune topologie. Néanmoins, (III.2.7) doit être regardée comme une suite exacte dans la catégorie CpAbNorSepFil des groupes compacts pseudo-normés séparés filtrés, dont les morphismes sont continus : c'est un ingrédient crucial pour mettre en relation les catégories Ban et $\mathsf{Mod}_{\underline{\mathbb{R}}}$, ainsi que $\mathsf{Mod}_{\underline{\mathbb{R}}}$ et $\mathsf{Mod}_{\underline{\mathbb{Z}(\!(\mathsf{T})\!)}}$. Il a donc fallu formaliser le résultat suivant :

```
theorem continuous_θ_c {S : Fintype} (r p c: ℝ≥0) [hr : r < 1] [hr' : 0 < r]
[hp : p < 1] [hp' : 0 < p] (H : r = 2 ^ (-p)) : continuous (θ_c r p S) :=
```

Extrait de code 5 – La continuité de θ

Ce qui est assez frappant dans l'extrait de code 5, et qui reflet l'extraordinaire originalité du travail de Clausen–Scholze, est la comparaison de deux topologies apparemment très différentes. On y voit apparaître une modification $\theta_{\mathtt{c}}$ de θ, qui dépend du paramètre c, paramètre qui joue un rôle essentiel dans la « topologie » de $\mathscr{L}$ r S . En effet, le domaine de θ est l'espace des mesures de Laurent, qui n'a pas une topologie naturelle. Il est toutefois muni d'une filtration croissante par des sous-espaces, indexés par $c \geqslant 0$, qui sont des espaces topologiques grâce à la présentation suivante : pour chaque valeur $c \in \mathbb{R}_{\geqslant 0}$ soit

$$\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c} = \left\{ \sum_{n\in\mathbb{Z}, s\in \mathtt{S}} a_{n,s} T^n[s] \;\middle|\; a_{n,s} \in \mathbb{Z} \ \text{ et } \sum_{n\in\mathbb{Z}, s\in \mathtt{S}} |a_{n,s}|\, \mathtt{r}^n \leqslant c \right\}$$

14. L'opérateur tsum qui apparaît dans la définition de θ restitue 0 lorsque son argument diverge, ce qui force toutes les séries qui ne convergent pas en (1/2) à être dans le noyau de θ.

l'espace des mesures dont la somme (pour tout $s \in \mathtt{S}$) est bornée par c. Chacun des espaces $\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c}$ est profini : en effet, pour tout sous-ensemble fini $A \subseteq \mathbb{Z}$, les mesures à coefficients dans A

$$\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c,A} = \left\{ \sum_{n\in\mathbb{Z},s\in\mathtt{S}} a_{n,s}T^n[s] \;\middle|\; a_{n,s} \in A \quad \text{et} \quad \sum_{n\in\mathbb{Z},s\in\mathtt{S}} |a_{n,s}|\,\mathtt{r}^n \leqslant c \right\}.$$

forment un ensemble fini, car $\mathbb{Z}$ est discret et car la condition de sommabilité dans la définition de $\mathscr{L}\ \mathtt{r}\ \mathtt{S}$ garantit qu'il n'y a qu'un nombre fini de coefficients non-nuls avec indice négatif — qu'il n'y ait qu'un nombre fini de coefficients non-nuls avec indice positif suit de la borne sur la norme. Comme

$$\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c} = \varprojlim_{A} \left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c,A},$$

on peut munir $\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c}$ de la topologie profinie. Cette famille de sous-espaces compacts donne lieu à une filtration croissante

$$\mathscr{L}\ \mathtt{r}\ \mathtt{S} = \bigcup_{c\geqslant 0} \left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c}.$$

De façon analogue on peut écrire le $\mathbb{R}$-espace vectoriel de dimension finie $\mathscr{M}\ \mathtt{p}\ \mathtt{S}$ comme la réunion filtrante des boules compactes de rayon (pour la normé ℓ^p) borné :

$$\mathscr{M}\ \mathtt{p}\ \mathtt{S} = \bigcup_{c\geqslant 0} \left(\mathscr{M}\ \mathtt{p}\ \mathtt{S}\right)_{\ell^p\leqslant c}.$$

En premier lieu, il a été question de montrer que θ est une « contraction », dans le sens qu'il existe une constante $0 < C < 1$ telle que l'image par θ de $\left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c}$ est contenue dans $\left(\mathscr{M}\ \mathtt{p}\ \mathtt{S}\right)_{\ell^p\leqslant Cc}$ pour tout c. La fonction

$$\theta_{\mathtt{c}} : \left(\mathscr{L}\ \mathtt{r}\ \mathtt{S}\right)_{\leqslant c} \longrightarrow \left(\mathscr{M}\ \mathtt{p}\ \mathtt{S}\right)_{\ell^p\leqslant Cc}$$

est la restriction de θ et l'extrait de code 5 est l'énoncé que cette fonction est continue. Que la topologie profinie du domaine de $\theta_{\mathtt{c}}$ et celle euclidienne de son codomaine puissent interagir et le faire de façon intéressante pour étudier des phénomènes d'analyse fonctionnelle s'est révélé plutôt surprenant (voir par exemple la discussion [Sch21b] sur *MathOverflow* initiée par Scholze).

Une fois que la « comparaison » entre structures profinies et structures réelles — sous la forme de la suite exacte (III.2.7) — est disponible, un argument de changement de base (voir [CS19a, Proposition 6.15]) permet de réduire le calcul des foncteurs dérivés dans le Théorème III.2.4 à son équivalent obtenu en remplaçant l'anneau analytique $(\mathbb{R}, \mathsf{Liq}_p)$ par l'anneau analytique $(\underline{\mathbb{Z}((T))}, \mathsf{Liq}_{\underline{\mathbb{Z}((T))},r})$. Ici, la condition d'être « liquide » pour un $\underline{\mathbb{Z}((T))}$-module est analogue à celle pour $\underline{\mathbb{R}}$, avec une modification convenable de la propriété universelle d'extension (III.2.6) (voir [CS19a, Theorem 6.10] pour plus de détails). Or, prouver l'équivalent pour l'anneau analytique $(\underline{\mathbb{Z}((T))}, \mathsf{Liq}_{\underline{\mathbb{Z}((T))},r})$ du Théorème III.2.4 était précisément l'objectif de la première partie du projet [CTB+22]. Dans le manuscrit original, il correspond au [CS19a, Theorem 9.4] et prend la forme suivante dans la formalisation :

```
theorem thm94 : ∀ m : ℕ, ∃ (k K : ℝ≥0) (hk : fact (1 ⩽ k)) (c₀ : ℝ≥0),
∀ (S : Profinite) (V : SemiNormedGroup.{u}) [normed_with_aut r V],
((BD.data.system κ r V r').obj (op $ of r' ((Lbar.functor.{0 0} r').obj S))).
   is_bounded_exact k K m c₀
```

Extrait de code 6 – L'objectif de la première partie du projet

Je ne rentrerai pas dans les détails de la définition du complexe de Breen–Deligne, ni du complexe de Commelin qui a été utilisé à sa place dans la formalisation et qui est derrière l'extrait de code 6. Je me contenterai de mentionner que ma contribution à la première partie du projet s'est concentrée sur la formalisation de certaines structures discrètes et du [CS19a, Lemme 9.7], formalisé sous la forme du

```
lemma lem97 [fintype ι] [module.finite ℤΛ] [module.free ℤΛ] (N : ℕ)
(hN : 0 < N) (l : ι → Λ) : ∃ A : finset (Λ →+ ℤ), ∀ x : Λ →+ ℤ, ∃ (x' ∈ A)
(y : Λ →+ ℤ), x = N • y + x' ∧ ∀ i, (0 ⩽ x' (l i) ∧ 0 ⩽ (x - x') (l i)) ∨
  (x' (l i) ⩽ 0 ∧ (x - x') (l i) ⩽ 0)
```

Pour une vision d'ensemble du projet, le *blueprint* [CCMS23] contient un texte interactif qui permet de faire le lien entre le manuscrit [CS19a] et le code qui constitue [CTB+22], ainsi que deux graphiques de dépendance de tous les résultats formalisés (un pour chaque partie du projet).

III.3 Perspectives de recherche

Mes perspectives de recherche à moyen terme sont centrées autour des enjeux de formalisation, dans la continuation des travaux discutés aux §§III.1–III.2. Je vais en illustrer trois, plus ou moins liées aux sujets traités précédemment.

III.3.1 Théorie du corps de classes

Après le travail [BDNN21], discuté au §III.1 et qui établit la finitude du groupe de classes d'un corps de nombres, plusieurs autres résultats de théorie algébrique des nombres ont intégré `mathlib`, ou sont en train de l'intégrer : de Frutos-Fernández a formalisé la théorie des valuations sur les anneaux de Dedekind et les définitions des adèles et des idèles d'un corps de nombres ; Roblot a formalisé le théorème des unités de Dirichlet ; les auteurs de [BBBR23] ont défini le discriminant d'une extension et les formules du discriminant des corps cyclotomiques ; Baanen, Best et Dahmen ont formalisé les solutions à nombreuses équations de Mordell en menant des calculs explicites de nombres de classes … L'étape fondamentale suivante semble être la formalisation de la théorie du corps de classes. Il s'agit d'un projet que nous avons entamé avec de Frutos-Fernández, et qui se décompose naturellement en deux parties : commencer par formaliser la théorie du corps de classes locale, et après s'appuyer sur celle-ci pour formaliser la théorie globale.

Plusieurs formulations existent de la théorie locale, et les travaux récents de Livingston, qui a formalisé la théorie de la cohomologie des groupes, nous ont convaincus que l'approche la plus adaptée est celle cohomologique. La première étape consistera dans la formalisation des résultats de base des anneaux de valuation discrète et des

extensions des corps locaux[15] : existence d'une unique extension non-ramifiée pour tout degré donné, isomorphisme de son groupe de Galois avec le groupe de Galois de l'extension des corps résiduels, polynômes d'Eisenstein des extensions ramifiées, description des normes d'unités dans les extensions totalement ramifiées et dans celles non-ramifiées. Une fois ces fondamentaux établis, la deuxième étape sera purement cohomologique : d'abord, il faudra étendre le travail de Livingston pour définir la cohomologie de Tate pour les groupes finis. On passera après à démontrer l'isomorphisme $H^2(K, K^\times) \cong \mathbb{Q}/\mathbb{Z}$ pour tout corps local K, et ensuite à formaliser la définition et les propriété des « formations de classes » (voir [Ser68, Chapitre XI]), en démontrant au passage le théorème de Tate–Nakayama sous la forme de [Ser68, Chapitre IX, §8, Théorème 13] : une conséquence sera l'isomorphisme de Tate

$$\widehat{H}^n(G_{X/Y}, \mathbb{Z}) \cong \widehat{H}^{n+2}(G_{X/Y}, \mathcal{A}_X) \qquad \text{pour tout } n \in \mathbb{Z}$$

où $G_{X/Y} = G_Y/G_X$ est le groupe « relatif » dans une formation de classes $(G_\bullet, \mathcal{A}_\bullet)$. Déjà à ce stade on pourra prouver l'existence de la classe fondamentale canonique $u_{E/K} \in \widehat{H}^2(E/K, E^\times)$ pour toute extension finie E/K de corps locaux ainsi que (grâce au travail de de Frutos-Fernández qui a formalisé le groupe de classes d'idèles) l'existence de la classe fondamentale $u_{F/L} \in \widehat{H}^2(F/L, \mathcal{C}_F)$ pour toute extension finie F/L de corps de nombres. L'isomorphisme entre le groupe de Galois d'une extension abélienne E/K de corps locaux (*resp.* une extension abélienne F/L de corps de nombres) et le quotient $K^\times/\mathrm{N}_{E/K}E^\times$ (*resp.* le quotient $\mathcal{C}_L/\mathrm{N}_{F/L}\mathcal{C}_F$) suivra. Une fois ces résultats établis, on pourra se consacrer aux théorèmes d'existence, mais à moyen terme le projet esquissé ci-dessus constitue déjà une perspective de travail qui sera riche de développements et d'applications.

III.3.2 La suite spectrale de Serre

La situation actuelle de la théorie homotopique dans `mathlib` n'est pas au même stade de maturité que celui d'autres domaines. Étant donné un espace topologique pointé (X, x_0), la définition du premier groupe d'homotopie $\pi_1(X, x_0)$ a été formalisée, mais la structure de groupe sur les $\pi_n(X, x_0)$ (pour $n \geqslant 2$) ne l'a pas encore été (les ensembles sous-jacents sont toutefois définis dans `mathlib`). Une autre notion qui n'a pas encore été formalisée est celle du revêtement universel, ni plus généralement celle de fibration de Serre. Néanmoins, à la fois les généralités concernant la topologie de la convergence compacte et de l'espace des lacets ont été formalisées, ce qui rend naturel l'objectif de définir la structure de groupe sur $\pi_n(X, x_0)$ et le formalisme galoisien du revêtement universel. Une fois cette étape achevée, il faudra pousser la formalisation jusqu'à l'existence au moins de la suite exacte longue d'homotopie pour une fibration de Serre.

Bien évidemment, à long terme, l'objectif serait la suite spectrale de Serre pour une fibration, de tant plus que la théorie de l'homologie singulière est en train d'être développée et sera probablement disponible dans `mathlib`. Un projet à moyen terme qui serait intéressant en soi est la démonstration des résultats principaux sur l'homotopie et l'homologie des H-espaces — notion que j'ai récemment formalisée et qui a intégré `mathlib` — et plus particulièrement des espaces de lacets, notamment le fait que leur π_1

15. Un corps local, pour nous, sera une extensions finie soit de $\mathbb{Q}_p$ soit de $\mathbb{F}_p(\!(T)\!)$, pour un certain premier p.

est toujours abélien. On aurait alors tous les ingrédients pour formaliser le [Ser51, Chapitre V] et donc aussi certains premiers résultats sur les groupes d'homotopie des sphères. Une fois la suite spectrale (notion que Riou a déjà développée en `lean-3`, et qu'il est en train d'adapter à `lean-4` pour qu'elle intègre `mathlib`) à disposition, nombre de résultats de [Ser51] sur les groupes d'homotopie des sphères pourront être formalisés.

III.3.3 Extensions de p-espaces de Banach

Soit $0 < p \leqslant 1$ un paramètre réel. Je ne rappelle pas la définition précise de p-espace de Banach (je renvoie, par exemple, à [CS19a, Definition 6.1]), et je me contente de mentionner qu'il s'agit d'espaces vectoriels topologiques réels munis d'une norme archimédienne telle que $\|\alpha v\| = |\alpha|^p \|v\|$ pour tout $\alpha \in \mathbb{R}$ et tout vecteur v. En particulier, un 1-espace de Banach n'est rien d'autre qu'un espace de Banach, et il y a une inclusion $\mathsf{Ban}_p \subseteq \mathsf{Ban}_{p'}$ pour tout $p' \leqslant p$: on a donc $\mathsf{Ban} \subseteq \mathsf{Ban}_p$ pour tout $0 < p \leqslant 1$.

Bien que dans la présentation au §III.2 les p-espaces de Banach ne soient apparus que marginalement, ils jouent un rôle important dans la théorie des espaces liquides. L'extension de Ribe (III.2.2) montre que le problème d'extension dans Ban n'est pas trivial, et sa découverte provient d'une étude plus générale sur la stabilité par extension des propriétés métriques, ou analytiques, de certains espaces. Le travail de Ribe montre que la propriété d'être « localement convexe » n'est pas stable par extension, mais un résultat remarquable de Kalton prouve la chose plus précise suivante (voir [Kal78, Theorem 3.5]) : si dans une suite exacte (avec morphismes linéaires et continus)

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0$$

de $\mathbb{R}$-espaces vectoriels topologiques, Y est un p-espace de Banach pour un certain $p \leqslant 1$ et Z est un p'-espace de Banach pour un $p' < p$, alors X est lui-même un p'-espace de Banach : que l'inégalité $p' < p$ soit stricte est d'ailleurs à la base du « contrexemple » de Ribe. Une autre façon de mentionner ce résultat est que toute extension de deux p-espaces de Banach est automatiquement un p'-espace de Banach pour tout $p' < p$. Il se pose donc le problème de réinterpréter ce genre de résultats sur les extensions de p'-espaces de Banach par des p-espaces de Banach en termes de la catégorie Liq_p, au vu de l'existence du foncteur $\mathsf{Ban}_p \hookrightarrow \mathsf{Liq}_p$. Surtout, comme je l'ai illustré au §III.2, l'étape cruciale du projet [CTB+22] a été de montrer le Théorème III.2.4 sur l'annulation des groupes Ext^i, qui classifient les suites exactes à $(i+2)$ termes. Le cas $i = 1$ est donc l'énoncé précédent tiré de [Kal78] et il semble naturel d'étudier, par exemple pour $i = 2$, quelles informations peut-on dégager du Théorème III.2.4 (mais où les Ext sont calculés dans $\mathsf{Cond}(\mathsf{Ab})$) sur les extensions à 4 termes de p-espaces de Banach. Malheureusement, il n'est pas clair si la totalité de [CTB+22] intégrera `mathlib`, surtout dans sa nouvelle version en `lean-4`, et le premier objectif de ce projet serait de transférer dans `mathlib` les résultats sur les p-espaces de Banach qui ont été formalisés pour [CTB+22]. En deuxième lieu, il faudra formaliser les résultats de Kalton dans [Kal78] et de Ribe dans [Rib79]. Finalement, on pourra étudier en détail le cas $i = 2$ pour en déduire des conséquences sur les 4-extensions de p-espaces de Banach. Comme l'application principale des espaces condensés que Clausen–Scholze sont en train de développer dans [CS22] est orientée vers la géométrie algébrique, l'ambition de ce projet de formalisation sera de révéler des applications nouvelles de la théorie des espaces liquides, dans une direction plus spécifiquement analytique.

Bibliographie

[AFP] AFP – « The Archive of Formal Proofs », https://www.isa-afp.org.

[AIS15] F. Andreatta, A. Iovita & G. Stevens – « Overconvergent Eichler–Shimura isomorphisms », *J. Inst. Math. Jussieu* **14** (2015), no. 2, p. 221–274.

[AX23] D. K. Angdinata & J. Xu – « An Elementary Formal Proof of the Group Law on Weierstrass Elliptic Curves in any Characteristic », 2023, https://arxiv.org/abs/2302.10640.

[BDNN21] A. Baanen, S. R. Dahmen, A. Narayanan & F. A. E. Nuccio Mortarino Majno di Capriglio – « A Formalization of Dedekind Domains and Class Groups of Global Fields », dans *12th International Conference on Interactive Theorem Proving 2021*, vol. 193, 2021, p. 5 :1–5 :19.

[BDNN22] — , « A formalization of Dedekind domains and class groups of global fields », *J. Automat. Reason.* **66** (2022), no. 4, p. 611–637.

[Ban07] A. Bandini – « Greenberg's conjecture and capitulation in $\mathbb{Z}_p^d$-extensions », *J. Number Theory* **122** (2007), no. 1, p. 121–134.

[Bar12] A. Bartel – « On Brauer–Kuroda type relations of S-class numbers in dihedral extensions », *J. Reine Angew. Math.* **668** (2012), p. 211–244.

[Bel12] J. Bellaïche – « Critical p-adic L-functions », *Invent. Math.* **189** (2012), no. 1, p. 1–60.

[BCMS21] S. Bernard, C. Cohen, A. Mahboubi & P.-Y. Strub – « Unsolvability of the Quintic Formalized in Dependent Type Theory », dans *ITP 2021 - 12th International Conference on Interactive Theorem Proving* (Rome / Virtual, Italy), 2021.

[BBBR23] A. Best, C. Birkbeck, R. Brasca & E. Rodriguez – « Fermat's last theorem for regular primes », https://github.com/leanprover-community/flt-regular, `commit` 6062f95, 2023.

[BN18] N. Billerey & F. A. E. Nuccio Mortarino Majno di Capriglio – « Représentations galoisiennes diédrales et formes à multiplication complexe », *Journal de théorie des nombres de Bordeaux* **30** (2018), no. 2, p. 651–670.

[Bou71] N. Bourbaki – *Éléments de mathématique. Topologie générale. Chapitres 1 à 4*, Hermann, Paris, 1971.

[Bou06] — , *Éléments de mathématique. Algèbre commutative. Chapitres 5 à 7*, Springer, Berlin, 2006.

[Bou07] — , *Éléments de mathématique. Algèbre. Chapitres 4 à 7*, Springer, Berlin, 2007.

[Bra51] R. Brauer – « Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers », *Math. Nachr.* **4** (1951), p. 158–174.

[Buz07] K. Buzzard – « Eigenvarieties », dans *L-functions and Galois representations*, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, p. 59–120.

[BCM20] K. Buzzard, J. Commelin & P. Massot – « Formalising Perfectoid Spaces », dans *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (New York, NY, USA), CPP 2020, Association for Computing Machinery, 2020, p. 299–312.

[CN20] L. Caputo & F. A. E. Nuccio Mortarino Majno di Capriglio – « Class number formula for dihedral extensions », *Glasgow Mathematical Journal* **62** (2020), no. 2, p. 323–353.

[CN22] — , « Cohomology of normic systems and fake $\mathbb{Z}_p$-extensions », 2022, https://arxiv.org/abs/0807.1135.

[Car19] M. Carneiro – *The Type Theory of Lean*, Mémoire, https://ub.com/digama0/lean-type-theory/releases, 2019.

[CK82] J. E. Carroll & H. H. Kisilevsky – « On Iwasawa's λ-invariant for certain $\mathbf{Z}_l$-extensions », *Acta Arith.* **40** (1981/82), no. 1, p. 1–8.

[Che02] I. Chen – « Surjectivity of mod l representations attached to elliptic curves and congruence primes », *Canad. Math. Bull.* **45** (2002), no. 3, p. 337–348.

[CCMS23] D. Clausen, J. Commelin, P. Massot & P. Scholze – « Liquid Tensor Experiment », https://leanprover-community.github.io/liquid/, `commit` bf9cef2, 2023.

[CS19a] D. Clausen & P. Scholze – « Lectures on Analytic Geometry », disponible à l'adresse https://www.math.uni-bonn.de/people/scholze/Analytic.pdf, 2019.

[CS19b] — , « Lectures on Condensed Mathematics », disponible à l'adresse https://www.math.uni-bonn.de/people/scholze/Condensed.pdf, 2019.

[CS22] — , « Condensed Mathematics and Complex Geometry », disponible à l'adresse https://people.mpim-bonn.mpg.de/scholze/Complex.pdf, 2022.

[Coa99] J. Coates – « Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication », dans *Arithmetic theory of elliptic curves* (*Cetraro, 1997*), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, p. 1–50.

[CG96] J. Coates & R. Greenberg – « Kummer theory for abelian varieties over local fields », *Invent. Math.* **124** (1996), no. 1-3, p. 129–174.

[CS05a] J. Coates & Sujatha R. – « Fine Selmer groups for elliptic curves with complex multiplication », dans *Algebra and number theory*, Hindustan Book Agency, Delhi, 2005, p. 327–337.

[CS05b] — , « Fine Selmer groups of elliptic curves over p-adic Lie extensions », *Math. Ann.* **331** (2005), no. 4, p. 809–839.

[CS10] — , *Galois cohomology of elliptic curves*, second ed., Narosa Publishing House, New Delhi, 2010.

[Col96] R. F. Coleman – « Classical and overconvergent modular forms », *Invent. Math.* **124** (1996), no. 1-3, p. 215–241.

[Col97a] — , « Classical and overconvergent modular forms of higher level », *J. Théor. Nombres Bordeaux* **9** (1997), no. 2, p. 395–403.

[Col97b] — , « p-adic Banach spaces and families of modular forms », *Invent. Math.* **127** (1997), no. 3, p. 417–479.

[CM98] R. F. Coleman & B. Mazur – « The eigencurve », dans *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, vol. 254, Cambridge Univ. Press, Cambridge, 1998, p. 1–113.

[CTB+22] J. Commelin, A. Topaz, R. Barton, A. Best, R. Brasca, K. Buzzard, Y. Dillies, F. van Doorn, F. Glöckle, M. Himmel, H. Macbeth, P. Massot, B. Mehta, S. Morrison, F. A. E. Nuccio Mortarino Majno di Capriglio, J. Riou, D. Testa & A. Yang – « Liquid Tensor Experiment », https://github.com/leanprover-community/lean-liquid/, `commit` 92f188b, 2022.

[deF22] M. I. de Frutos-Fernández – « Formalizing the Ring of Adèles of a Global Field », dans *13th International Conference on Interactive Theorem Proving (ITP 2022)* (Dagstuhl, Germany), J. Andronick & L. de Moura, éds., Leibniz International Proceedings in Informatics (LIPIcs), vol. 237, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, p. 14 :1–14 :18.

[Del68] P. Deligne – « Formes modulaires et représentations l-adiques », no. 355, 1968, p. 139–172.

[DS74] P. Deligne & J.-P. Serre – « Formes modulaires de poids 1 », *Ann. Sci. Ecole Norm. Sup. (4)* 7 (1974), p. 507–530 (1975).

[DeM23] L. De Moura – « The LEAN Theorem Prover », https://github.com/leanprover-community/lean/, `commit` 367b387, 2023.

[DeM23] — , « The LEAN Theorem Prover », https://leanprover.github.io/, `commit` 367b387, 2023.

[Deu52] M. Deuring – « Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper », *Math. Ann.* **124** (1952), p. 393–426.

[Edi92] B. Edixhoven – « The weight in Serre's conjectures on modular forms », *Invent. Math.* **109** (1992), no. 3, p. 563–594.

[EPW06] M. Emerton, R. Pollack & T. Weston – « Variation of Iwasawa invariants in Hida families », *Invent. Math.* **163** (2006), no. 3, p. 523–580.

[FW79] B. Ferrero & L. C. Washington – « The Iwasawa invariant μ_p vanishes for abelian number fields », *Ann. of Math. (2)* **109** (1979), no. 2, p. 377–395.

[GP12] E. Ghate & P. Parent – « On uniform large Galois images for modular abelian varieties », *Bull. Lond. Math. Soc.* **44** (2012), no. 6, p. 1169–1181.

[Gil76] R. Gillard – « Remarques sur certaines extensions prodiédrales de corps de nombres », *C. R. Acad. Sci. Paris Sér. A-B* **282** (1976), no. 1, p. Ai, A13–A15.

[Gon23] G. Gonthier – « A computer-checked proof of the Four Color Theorem », Tech. report, Inria, 2023.

[GAA+13] G. Gonthier, A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. Le Roux, A. Mahboubi, R. O'Connor, S. O. Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi & L. Théry – « A machine-checked proof of the odd order theorem », dans *Proceedings of the 4th International Conference on Interactive Theorem Proving* (Berlin, Heidelberg), ITP'13, Springer-Verlag, 2013, p. 163–179.

[Gre99] R. Greenberg – « Iwasawa theory for elliptic curves », dans *Arithmetic theory of elliptic curves* (*Cetraro, 1997*), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, p. 51–144.

[Gre01] — , « Iwasawa theory – past and present », dans *Class field theory – its centenary and prospect. Proceedings of the 7th MSJ International Research Institute of the Mathematical Society of Japan, Tokyo, Japan, June 3–12, 1998*, Tokyo : Mathematical Society of Japan, 2001, p. 335–385.

[GV00] R. Greenberg & V. Vatsal – « On the Iwasawa invariants of elliptic curves », *Invent. Math.* **142** (2000), no. 1, p. 17–63.

[Gro81] B. H. Gross – « p-adic L-series at $s = 0$ », *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, p. 979–994 (1982).

[Gro57] A. Grothendieck – « Sur quelques points d'algèbre homologique », *Tôhoku Math. J.* (2) **9** (1957), p. 119–221.

[HW07] F. Haftmann & M. Wenzel – « Constructive type classes in Isabelle », dans *Types for Proofs and Programs* (Berlin, Heidelberg), T. Altenkirch & C. McBride, éds., Springer Berlin Heidelberg, 2007, p. 160–174.

[HAB+17] T. Hales, M. Adams, G. Bauer, T. D. Dang, J. Harrison, L. T. Hoang, C. Kaliszyk, V. Magron, S. McLaughlin, T. T. Nguyen, Q. T. Nguyen, T. Nipkow, S. Obua, J. Pleso, J. Rute, A. Solovyev, T. H. A. Ta, N. T. Tran, T. D. Trieu, J. Urban, K. Vu & R. Sumkeller – « A formal proof of the Kepler Conjecture », *Forum of Mathematics, Pi* **5** (2017), p. e2.

[HK77] F. Halter-Koch – « Einheiten und Divisorenklassen in Galois'schen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl l », *Acta Arith.* **33** (1977), no. 4, p. 355–364.

[Har84] D. Harbater – « Convergent arithmetic power series », *Amer. J. Math.* **106** (1984), p. 801–846.

[HL19] J. Hatley & A. Lei – « Arithmetic properties of signed Selmer groups at non-ordinary primes », *Annales de l'Institut Fourier* **69** (2019), no. 3, p. 1259–1294.

[Hec59] E. Hecke – *Mathematische Werke*, Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen, Vandenhoeck & Ruprecht, Göttingen, 1959.

[Hid86] H. Hida – « Galois representations into $GL(2, \mathbf{Z}_p[[X]])$ attached to ordinary cusp forms », *Invent. Math.* **85** (1986), no. 3, p. 545–613.

[Hid93] — , *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts, vol. 26, Cambridge University Press, Cambridge, 1993.

[Iwa58] K. Iwasawa – « On some invariants of cyclotomic fields », *Amer. J. Math. 80 (1958), 773-783 ; erratum* **81** (1958), p. 280.

[Iwa73a] — , « On $\mathbf{Z}_l$-extensions of algebraic number fields », *Ann. of Math. (2)* **98** (1973), p. 246–326.

[Iwa73b] — , « On the μ-invariants of $\mathbb{Z}_\ell$-extensions », dans *Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki*, Kinokuniya, Tokyo, 1973, p. 1–11.

[Jau81a] J.-F. Jaulent – « Théorie d'Iwasawa des tours métabeliennes », dans *Seminar on Number Theory, 1980–1981* (*Talence, 1980–1981*), Univ. Bordeaux I, Talence, 1981, p. Exp. No. 21, 16.

[Jau81b] — , « Unités et classes dans les extensions métabéliennes de degré nl^s sur un corps de nombres algébriques », *Ann. Inst. Fourier* (*Grenoble*) **31** (1981), no. 1, 39–62.

[Kal78] N. J. Kalton – « The three space problem for locally bounded F-spaces », *Compositio Mathematica* **37** (1978), no. 3, p. 243–276.

[Kat04] K. Kato – « p-adic Hodge theory and values of zeta functions of modular forms », *Astérisque* (2004), no. 295, p. ix, 117–290.

[Kat73] N. M. Katz – « p-adic properties of modular schemes and modular forms », dans *Modular functions of one variable, III* (*Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972*), Springer, Berlin, 1973, p. 69–190. Lecture Notes in Mathematics, Vol. 350.

[Kim13] B. D. Kim – « The plus/minus Selmer groups for supersingular primes », *J. Aust. Math. Soc.* **95** (2013), no. 2, p. 189–200.

[KO18] T. Kitajima & R. Otsuki – « On the Plus and the Minus Selmer Groups for Elliptic Curves at Supersingular Primes », *Tokyo J. Math.* **41** (2018), no. 1, p. 273–303.

[Kle16] S. Kleine – « Relative extensions of number fields and Greenberg's generalised conjecture », *Acta Arith.* **174** (2016), no. 4, p. 367–392.

[Kob03] S. Kobayashi – « Iwasawa theory for elliptic curves at supersingular primes », *Invent. Math.* **152** (2003), no. 1, p. 1–36.

[KNS24] D. Kundu, F. A. E. Nuccio Mortarino Majno di Capriglio & Sujatha R. – « Structure of fine Selmer groups in abelian p-adic Lie extensions », *Osaka J. Math.* **61** (2024), no. 1, à paraître – https://hal-cnrs.archives-ouvertes.fr/hal-03769801.

[Lan90] S. Lang – *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin.

[Lem05] F. Lemmermeyer – « Class groups of dihedral extensions », *Math. Nachr.* **278** (2005), no. 6, p. 679–691.

[LZ16] D. Loeffler & S. L. Zerbes – « Rankin–Eisenstein classes in Coleman families », *Res. Math. Sci.* **3** (2016), No. 29.

[LMF13] LMFDB Collaboration – « The L-functions and Modular Forms Database », http://www.lmfdb.org, 2013.

[Mah14] A. Mahboubi – « Un ordinateur pour vérifier les preuves mathématiques », Images des Mathématiques, 2014, https://images.math.cnrs.fr/Un-ordinateur-pour-verifier-les-preuves-mathematiques?lang=fr.

[Mah21] — , « Machine-checked computer-aided mathematics », Habilitation à diriger des recherches, Université de Nantes (UN), Nantes, FRA., 2021.

[MT22] A. Mahboubi & E. Tassi – *Mathematical Components*, Zenodo, https://doi.org/10.5281/zenodo.7118596, 2022.

[Mat20] Mathlib community – « The Lean Mathematical Library », dans *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (New York, NY, USA), CPP 2020, Association for Computing Machinery, 2020, p. 367–381.

[Mat22] — , « Completion of the Liquid Tensor Experiment », Lean Community blog https://leanprover-community.github.io/blog/posts/lte-final/, `commit` b2ff996, 2022.

[Mat23] — , « Lean mathlib », https://github.com/leanprover-community/mathlib, `commit` 36938f7, 2023.

[Maz72] B. Mazur – « Rational points of abelian varieties with values in towers of number fields », *Invent. Math.* **18** (1972), p. 183–266.

[MSD74] B. Mazur & P. Swinnerton-Dyer – « Arithmetic of Weil curves », *Invent. Math.* **25** (1974), p. 1–61.

[MTT86] B. Mazur, J. Tate & J. Teitelbaum – « On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer », *Invent. Math.* **84** (1986), no. 1, p. 1–48.

[Mer96] L. Merel – « Bornes pour la torsion des courbes elliptiques sur les corps de nombres », *Invent. Math.* **124** (1996), no. 1-3, p. 437–449.

[MW77] H. L. Montgomery & P. J. Weinberger – « Real quadratic fields with large class number », *Math. Ann.* **225** (1977), no. 2, p. 173–176.

[Mos79] N. Moser – « Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbf{Q}$ », *Abh. Math. Sem. Univ. Hamburg* **48** (1979), p. 54–75.

[Mur97] V. K. Murty – « Modular forms and the Chebotarev density theorem. II », dans *Analytic number theory* (*Kyoto, 1996*), London Math. Soc. Lecture Note Ser., vol. 247, Cambridge Univ. Press, Cambridge, 1997, p. 287–308.

[NG14] R. Nederpelt & H. Geuvers – *Type Theory and Formal Proof. An Introduction*, Cambridge University Press, Cambridge, 2014.

[NSW08] J. Neukirch, A. Schmidt & K. Wingberg – *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008.

[Nua11] J. Nualart – « Minimal lifts of dihedral 2-dimensional Galois representations », *Bull. Braz. Math. Soc. (N.S.)* **42** (2011), no. 3, p. 359–371.

[NOR23] F. A. E. Nuccio Mortarino Majno di Capriglio, T. Ochiai & J. Ray – « A formal model of Coleman families and applications to Iwasawa invariants », *Ann. Math. Québec* (2023), à paraître – https://cnrs.hal.science/hal-03355637v3.

[NS23] F. A. E. Nuccio Mortarino Majno di Capriglio & Sujatha R. – « Residual supersingular Iwasawa theory and signed Iwasawa invariants », *Rend. Semin. Mat. Univ. Padova* (2023), no. 149, p. 83–129.

[PR81] B. Perrin-Riou – « Groupe de Selmer d'une courbe elliptique à multiplication complexe », *Compositio Math.* **43** (1981), no. 3, p. 387–417.

[PR93] — , « Fonctions L p-adiques d'une courbe elliptique et points rationnels », *Ann. Inst. Fourier* (*Grenoble*) **43** (1993), no. 4, p. 945–995.

[Pol03] R. Pollack – « On the p-adic L-function of a modular form at a supersingular prime », *Duke Math. J.* **118** (2003), no. 3, p. 523–558.

[Rib79] M. Ribe – « Examples for the nonlocally convex three space problem », *Proc. Amer. Math. Soc.* **73** (1979), no. 3, p. 351–355.

[Rib77] K. A. Ribet – « Galois representations attached to eigenforms with Nebentypus », dans *Modular functions of one variable, V* (*Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976*), Springer, Berlin, 1977, p. 17–51. Lecture Notes in Math., Vol. 601.

[Rib92] — , « Abelian varieties over $\mathbf{Q}$ and modular forms », dans *Algebra and topology 1992 (Taejŏn)*, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, p. 53–79.

[Ros02] M. Rosen – *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Sam67] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[Sch85] P. Schneider – « p-adic height pairings. II », *Invent. Math.* **79** (1985), no. 2, p. 329–374.

[Sch21a] P. Scholze – « Half a year of the Liquid Tensor Experiment : Amazing developments », Xena Project Blog https://xenaproject.wordpress.com/2021/06/05/half-a-year-of-the-liquid-tensor-experiment-amazing-developments/, 2021.

[Sch21b] — , « Nonconvexity and discretization », MathOverflow, https://mathoverflow.net/q/386796, 2021, (page consultée le 4 juin 2023).

[Sch22] — , « Liquid Tensor Experiment », *Experimental Mathematics* **31** (2022), no. 2, p. 349–354.

[Ser51] J.-P. Serre – « Homologie singulière des espaces fibrés. Applications », *Ann. of Math.* (2) **54** (1951), p. 425–505.

[Ser60] — , « Classes des corps cyclotomiques », dans *Séminaire Bourbaki : années 1958/59 – 1959/60, exposés 169-204*, Séminaire Bourbaki, no. 5, Société mathématique de France, 1960, p. 83–93.

[Ser68] — , *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser87] — , « Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ », *Duke Math. J.* **54** (1987), no. 1, p. 179–230.

[SvdW11] B. Spitters & E. van der Weegen – « Type classes for mathematics in type theory », *Mathematical Structures in Computer Science* **21** (2011), no. 4, p. 795–825.

[Shi71] G. Shimura – « On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields », *Nagoya Math. J.* **43** (1971), p. 199–208.

[Shi72] — , « Class fields over real quadratic fields and Hecke operators », *Ann. of Math.* (2) **95** (1972), p. 130–190.

[Sta21] A. Stasinski – « A uniform proof of the finiteness of the class group of a global field », *The American Mathematical Monthly* **128** (2021), no. 3, p. 239–249.

[Tat67a] J. T. Tate – « Fourier analysis in number fields, and Hecke's zeta-functions », dans *Algebraic Number Theory* (*Proc. Instructional Conf., Brighton, 1965*), Thompson, Washington, D.C., 1967, p. 305–347.

[Tat67b] — , « Global class field theory », dans *Algebraic Number Theory* (*Proc. Instructional Conf., Brighton, 1965*), Thompson, Washington, D.C., 1967, p. 162–203.

[Wil88] A. Wiles – « On ordinary λ-adic representations associated to modular forms », *Invent. Math.* **94** (1988), no. 3, p. 529–573.

[Wut07] C. Wuthrich – « Iwasawa theory of the fine Selmer group », *J. Algebraic Geom.* **16** (2007), no. 1, p. 83–108.