Modular Galois representations and linear forms in abelian logarithms

Baptiste Peaucelle

Université Clermont Auvergne
École Doctorale des Sciences Fondamentales
Laboratoire de Mathématiques Blaise Pascal (UMR 6620)

Thèse de doctorat
Discipline : Mathématiques

Représentations galoisiennes modulaires et formes linéaires de logarithmes abéliens

Présentée par Baptiste Peaucelle
Sous la direction de Nicolas Billerey et Éric Gaudron

Soutenue publiquement le vendredi 9 décembre 2022 devant le jury composé de

M. Sinnou David	PR à Sorbonne Université	Président
M. Gaël Rémond	DR à l'Institut Fourier	Rapporteur
M. Gabor Wiese	PR à l'Université du Luxembourg	Rapporteur
Mme. Sandra Rozensztajn	MCF à l'ENS de Lyon	Examinatrice
M. Samuele Anni	MCF Aix-Marseille Université	Examinateur
M. Nicolas Billerey	MCF à l'Université Clermont-Auvergne	Directeur
M. Éric Gaudron	PR à l'Université Clermont-Auvergne	Directeur

Remerciements

J'aimerais en tout premier lieu remercier mes deux directeurs de thèse – Nicolas et Éric. Je ne saurais dire à quel point je vous suis reconnaissant. Pour avoir accepté de m'encadrer en thèse, pour votre disponibilité, pour les innombrables heures que vous m'avez consacrées durant un peu plus de trois ans, pour toutes les questions (pas toujours pertinentes) auxquels vous avez répondu, pour votre soutien à la fois pendant les bons et les mauvais moments. Pour tout cela, sans quoi cet aboutissement ne serait pas là.

Merci aussi tout particulièrement à Gaël Rémond et Gabor Wiese qui ont accepté de lire et de rapporter cette thèse. J'admire leurs travaux et j'ai été très honoré qu'ils acceptent de relire mon travail. Merci également à Sinnou David, Sandra Rozensztajn, et Samuele Anni d'avoir accepté de faire partie de mon jury.

Cette thèse est l'aboutissement de ces trois dernières années mais aussi de mes 4 années à l'ENS **de** Lyon. 7 années à travailler (un peu) mais aussi et surtout 7 années de rencontres et d'amitiés, de personnes qui font ou ne font plus partie de ma vie mais qui ont un jour été dedans. J'aimerais toutes et tous vous remercier en oubliant sûrement des gens, des choses, et dans un désordre le plus complet.

Merci à ma famille, maman, papa, Anne-Laure, et Camille. Même si je sais que vous ne comprenez pas vraiment ce que je fais, je sais que vous êtes là.

Dans la catégorie vieux lyonnais, merci Angèle pour toutes les discussions (plus ou moins pertinentes) en amphi pour faire passer les cours parfois un peu longs, pour la danse, et pour tous les bons moments passés ensemble depuis maintenant un peu plus de 7 ans. Merci Alice (Best témoins !) pour la danse, la coloc, et pour m'aider à procrastiner dès que j'en ai besoin. Merci, à tout le groupe, Hugo, Émile, Colin, Clément, Adèle, Octave, Meven, Rédouane, Loïs, pour toutes les vacances, les soirées, les sorties, et les voyages improbables passés.

Dans la catégorie lyonnaises un peu moins vieilles, merci à toutes les membres de MSR. Merci Vinciane pour les expériences culinaires étonnement souvent réussies. J'ai arrêté de compter les thés froids laissés dans la coloc. Merci Flora pour les nombreux hébergements à Lyon, dans des situations parfois un peu critiques. Merci Marion pour ta bonne humeur toujours communicative et le temps un peu trop important passé à parler de départements français. Merci Sophia pour nous avoir supporté avec Marion parler de départements français. Merci Valentine, et surtout merci Moïra pour tout ce qui a été vécu ! J'aurais aimé que nous nous haîmes moins.

Dans la catégorie matheux clermontois, merci Tristan pour tous tes jeux de mots plus ou moins inspirés, pour les bières, planches, vins à l'Épicologue ou ailleurs (et toujours de manière raisonnable bien sûr), pour toutes les aberrations mathématiques écrites au tableau. Après cinq

mois à apprendre des départements, cours d'eau, chefs-lieux, blasons, et Rocamadour, j'espère que tu connais un peu plus la géographie française qu'avant. Je ne sais pas trop si je dois te mettre dans la catégorie lyonnaise et ou clermontoise, mais merci Caroline pour la coloc et le confinement passé en ta compagnie. Merci plus généralement à tous les thésards du labo, jeunes ou moins jeunes. Sophie, Arthur, Fernando, Léo, Émilien, Julian, Vincent, Sébastien, Damien, Franck, Athina, Valentin, Arnaud. Merci à tous les membres de l'équipe de théorie des nombres que j'ai pu côtoyer pendant 3 ans, Nicolas et Éric encore une fois mais aussi Richard, Marusia et François, et merci à tous les membres du labo, entre autres Abel, César, Simon, François, et Thierry.

Dans la catégorie musiciens clermontois, merci avant tout Guillaume. J'ai toujours passé d'excellents moments en ta compagnie, que ce soit à faire de la musique, ou autour d'un verre. J'ai beaucoup appris en discutant avec toi. Merci aussi à tous les musiciens de l'Orchestre et plus particulièrement au pupitre de saxophones. C'était toujours un plaisir de dire des bêtises pendant les répètes. J'espère de nouveau avoir l'occasion de jouer avec vous et au moins de venir vous écouter jouer.

Dans la catégorie lyonnais plus ou moins jeunes, merci à toutes les personnes qui sont encore à Lyon en ce moment et que j'ai retrouvées depuis un peu plus de 3 mois. Merci tout spécialement Élodie, c'est toujours un plaisir de discuter et de passer du temps avec toi. Merci à tous les gens que je croise à la Fanfare et à l'Orchestre, c'est toujours un plaisir pour moi de faire de la musique. Merci Colin pour la coloc et pour me poser des questions de maths dès que tu en as l'occasion. Peut-être qu'un jour on aura un plafond fonctionnel. Merci aux membres de l'UMPA, Robin et Swann pour les longs débats sur le TD, Raphaël pour rehausser mes compétences en algèbre commutative, et plus généralement à tous les membres de l'équipe de théorie des nombres que je croise régulièrement. Merci au Foyer et merci en vrac à tous les gens que j'ai beaucoup côtoyés ces derniers mois : Héloïse, Ella, Antonin, Yohann, Rémi, Sasha, Jean, Pauline, Isa, et j'en oublie très certainement.

Sans vous toutes et tous, je ne serais pas qui et où je suis aujourd'hui.

Contents

English introduction

In number theory, Diophantine equations have always motivated the search of new tools, new methods, and new theorems to resolve them. One of the most famous is with no doubt Fermat's last theorem. In the 1630s, Pierre de Fermat wrote that the equation

$$X^n + Y^n = Z^n \tag{0.1}$$

in non-zero integers had no solution (X, Y, Z) if n is greater than 2. In 1995 – almost four centuries – many mathematicians, and a lot of new tools later, Andrew Wiles brought the last piece of mathematics to solve Fermat's last theorem. This approach is now known as the modular method. It uses elliptic curves, modular forms, and their Galois representations, in order to prove that no solution to (0.1) can exist. Since Wiles' proof, this approach has been developed and generalised to be applied to other Diophantine equations. For example, in [Dar00], Darmon proposed an ambitious program in order to tackle generalised Fermat equations using abelian varieties of GL_2-type, Hilbert modular forms, and their Galois representations.

Another example of theory which can be applied to the resolution of Diophantine equations is the theory of linear forms in logarithms. Briefly, it deals with questions about linear independence of logarithms of algebraic numbers, and more generally of logarithms of rational points in commutative algebraic groups. An example of resolution of Diophantine equation in which this theory has played a key role is Catalan's conjecture. Catalan proposed in 1844 [Cat44] that the only integer solution to the equation

$$X^p - Y^q = 1$$

was $(p, q, X, Y) = (2, 3, 3, 2)$. This conjecture has been resolved 160 years later by Mihăilescu [Mih04] using among other things a bound coming from the theory of linear forms in logarithms of algebraic numbers. Another Diophantine tool that has been developed from the theory of linear forms in logarithms is the method of the elliptic logarithm. It was conceptualised by Stroeker and Tzanakis [ST94] and Gebel, Pethö, and Zimmer [GPZ94] in 1994, and a major step in the theory, done by David [Dav95], made possible the applicability of the method.

More recently, a work of Bugeaud, Mignotte, and Siksek [BMS06a] combined the forces of both the modular method, and results from the theory of linear forms in logarithms to prove Diophantine results about perfect powers in Fibonacci and Lucas sequences. They proved that the only Fibonacci and Lucas numbers that are integer powers are 0, 1, 8, and 144, and 1 and 4 respectively. Building on these ideas they manage to prove similar results in later articles [BMS06b; Bug+07; Bug+08].

The goal of this thesis is to bring new results on the modular forms and linear forms in logarithms sides. Our work focuses on giving explicit results. In particular, we describe several algorithms we have implemented in the number theory system PARI/GP. This manuscript is split in two parts. In the first one we work purely on the linear forms in logarithms side. We develop new, totally explicit theorems in the context of logarithms in abelian varieties over number fields. Our results are similar in nature to those of David [Dav95] for elliptic curves, and improve and generalise the work of [Gau06]. In the second part of the thesis, we go on the side of modular forms and their Galois representations. We again prove explicit and algorithmic results in the context of small images of residual Galois representations of modular forms. Our work generalises the one of Billerey and Dieulefait [BD14], and the one of Ribet [Rib75; Rib85] before them. We redirect the interested reader to chapters 1 and 8 for more details on the two parts of the thesis.

Introduction

En théorie des nombres, les équations diophantiennes ont toujours été un moteur dans la recherche de nouveaux outils, de nouvelles méthodes, et de nouveaux résultats pour les résoudre. Sans doute le plus célèbre exemple de telle équation est le Grand théorème de Fermat. Dans les années 1630, Pierre de Fermat écrivit dans la marge de son exemplaire d'*Arithmetica* de Diophante que l'équation

$$X^n + Y^n = Z^n \tag{0.2}$$

n'avait pas de solution entière non-nulle (X, Y, Z), si n est supérieur ou égal à 3. En 1995 – presque 4 siècles plus tard – et suite aux efforts de nombreux mathématiciens et au développement de nombreuses nouvelles mathématiques, Andrew Wiles apporta la dernière pierre à la démonstration du Grand théorème de Fermat. La stratégie de cette preuve est maintenant connue sous le nom de méthode modulaire. Elle utilise des courbes elliptiques, des formes modulaires, et leurs représentations galoisiennes pour démontrer qu'aucune solution non triviale à l'équation (0.2) n'existe. Depuis la preuve de Wiles, cette méthode a été approfondie et généralisée afin d'être appliquée à d'autres équations diophantiennes. En particulier, depuis [Dar00], Henri Darmon a développé un programme pour aborder les équations de Fermat généralisées en utilisant des variétés abéliennes de type GL_2, des formes modulaires de Hilbert, et leurs représentations galoisiennes.

Un autre exemple de mathématiques dont les progrès ont été appliquées dans le but de résoudre des équations diophantiennes est la théorie des formes linéaires de logarithmes. Cette théorie s'intéresse aux questions d'indépendance linéaire de logarithmes de nombres algébriques (et plus généralement aux logarithmes de points rationnels dans des groupes algébriques commutatifs). Un exemple célèbre d'équation diophantienne pour laquelle cette théorie a joué un rôle important est l'équation de Catalan. En 1844, Catalan proposa dans [Cat44] que la seule solution entière à l'équation

$$X^p - Y^q = 1$$

était $(p, q, X, Y) = (2, 3, 3, 2)$. Cette conjecture resta elle aussi ouverte durant de nombreuses années et c'est seulement en 2004 que Mihăilescu la démontra en utilisant, entre autres, la théorie des formes linéaires de logarithmes de nombres algébriques. Parmi les outils diophantiens développés à partir de la théorie des formes linéaires de logarithmes, on peut aussi citer la méthode du logarithme elliptique. Elle fut originellement imaginée d'une part par Stroeker et Tzanakis dans [ST94], et d'autre part par Gebel, Pethö, and Zimmer dans [GPZ94]. Les avancées majeures de David [Dav95] permirent à partir de 1995 à cette méthode d'être mise en œuvre.

Plus récemment, le travail commun de Bugeaud, Mignotte, et Siksek [BMS06a] combina les forces à la fois de la méthode modulaire et de la théorie des formes linéaires de logarithmes pour résoudre de nouveaux problèmes diophantiens concernant des puissances parfaites dans les suites de Fibonacci et de Lucas. Ils prouvèrent que les seuls nombres de la forme a^n avec a et n entiers sont 0, 1, 8 et 144 dans la suite de Fibonacci, et 1 et 4 dans la suite de Lucas. En réutilisant les idées de leur méthode, ils parvinrent à démontrer des résultats du même ordre dans leurs articles suivants [BMS06b ; Bug+07 ; Bug+08].

Le but de cette thèse est d'apporter de nouveaux résultats à la fois à la théorie des formes modulaires, et à celle des formes linéaires de logarithmes. Notre travail se concentre sur les aspects effectifs des deux théories. En particulier, nous développons plusieurs algorithmes que nous avons implémentés dans le logiciel de calcul formel PARI/GP. Le présent manuscrit est séparé en deux parties. La première traite uniquement de formes linéaires de logarithmes. Nous y prouvons de nouveaux résultats d'indépendance linéaires de logarithmes dans le contexte des variétés abéliennes. Nos résultats sont comparables à ceux de David [Dav95] pour les courbes elliptiques, et améliorent et généralisent ceux de Gaudron [Gau06]. La seconde partie s'intéresse aux formes modulaires et à leurs représentations galoisiennes résiduelles. Nous y prouvons des résultats explicites et algorithmiques de petite image résiduelle. Nous prolongeons le travail de Billerey et Dieulefait [BD14], et ceux de Ribet [Rib75 ; Rib85] avant eux. Nous renvoyons le lecteur intéressé aux chapitres 2 et 9 pour plus de détails sur les deux parties de la thèse.

References for the introduction

[BD14] Nicolas Billerey and Luis V. Dieulefait. "Explicit large image theorems for modular forms". In: *Journal of the London Mathematical Society. Second Series* 89.2 (2014), pp. 499–523. DOI: 10.1112/jlms/jdt072 (cited on pp. 10, 12).

[BMS06a] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. "Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers". In: *Annals of Mathematics. Second Series* 163.3 (2006), pp. 969–1018. DOI: 10.4007/annals.2006.163.969 (cited on pp. 9, 12).

[BMS06b] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. "Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation". In: *Compositio Mathematica* 142.1 (2006), pp. 31–62. DOI: 10.1112/S0010437X05001739 (cited on pp. 9, 12).

[Bug+07] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. "Perfect powers from products of terms in Lucas sequences". In: *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]* 611 (2007), pp. 109–129. DOI: 10.1515/CRELLE.2007.075 (cited on pp. 9, 12).

[Bug+08] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. "Fibonacci numbers at most one away from a perfect power". In: *Elemente der Mathematik* 63.2 (2008), pp. 65–75. DOI: 10.4171/EM/89 (cited on pp. 9, 12).

[Cat44] E. Catalan. "Note extraite d'une lettre adressée à l'éditeur par Mr. E. Catalan, Répétiteur à l'école polytechnique de Paris". In: *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]* 27 (1844), p. 192. DOI: 10.1515/crll.1844.27.192 (cited on pp. 9, 11).

[Dar00] Henri Darmon. "Rigid local systems, Hilbert modular forms, and Fermat's last theorem". In: *Duke Mathematical Journal* 102.3 (2000), pp. 413–449. DOI: 10.1215/S0012-7094-00-10233-5 (cited on pp. 9, 11).

[Dav95] Sinnou David. "Minorations de formes linéaires de logarithmes elliptiques". In: *Mémoires de la Société Mathématique de France. Nouvelle Série* 62 (1995), pp. iv+143 (cited on pp. 9–12).

[Gau06] Éric Gaudron. "Formes linéaires de logarithmes effectives sur les variétés abéliennes". In: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 39.5 (2006), pp. 699–773. DOI: 10.1016/j.ansens.2006.09.001 (cited on pp. 10, 12).

[GPZ94] J. Gebel, A. Pethö, and H. G. Zimmer. "Computing integral points on elliptic curves". In: *Acta Arithmetica* 68.2 (1994), pp. 171–192. DOI: 10.4064/aa-68-2-171-192 (cited on pp. 9, 11).

[Mih04] Preda Mihăilescu. "Primary cyclotomic units and a proof of Catalan's conjecture". In: *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]* 572 (2004), pp. 167–195. DOI: 10.1515/crll.2004.048 (cited on p. 9).

[Rib75] Kenneth A. Ribet. "On ℓ-adic representations attached to modular forms". In: *Inventiones Mathematicae* 28 (1975), pp. 245–275. DOI: 10.1007/BF01425561 (cited on pp. 10, 12).

[Rib85] Kenneth A. Ribet. "On l-adic representations attached to modular forms. II". In: *Glasgow Mathematical Journal* 27 (1985), pp. 185–194. DOI: 10.1017/S0017089500006170 (cited on pp. 10, 12).

[ST94] R. J. Stroeker and N. Tzanakis. "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms". In: *Acta Arithmetica* 67.2 (1994), pp. 177–196. DOI: 10.4064/aa-67-2-177-196 (cited on pp. 9, 11).

Part I

Linear forms in abelian logarithms

Chapter 1

English introduction

1.1 Linear forms in logarithms

In this part of the present manuscript we present our new results in the theory of linear forms in logarithms. A logarithm of an algebraic number α is any number $u \in \mathbb{C}$ such that $e^u = \alpha$. The theory of linear forms in logarithms is interested in linear relations between logarithms of algebraic numbers (and more generally between logarithms of points in commutative algebraic groups). One can pin down the starting point of the theory to the work of Lindemann [Lin82] and Weierstraß [Wei85] that proved one of the first result about linear independence of exponentials and logarithms of algebraic numbers. It states the following.

Theorem 1.1 (Lindemann–Weierstraß). *Let $\alpha_1, \dots, \alpha_n$ be distinct algebraic numbers. Then, the numbers $e^{\alpha_1}, \dots, e^{\alpha_n}$ are linearly independent over $\overline{\mathbb{Q}}$.*

Lindemann and Weierstraß' result proves the transcendence of any non-zero logarithm of an algebraic number α, because $e^{\log \alpha} - \alpha \cdot e^0 = 0$. As $i\pi$ is a logarithm of -1, it also establishes the transcendence of π. These results lead Hilbert to formulate its seventh problem in 1900 about the transcendence of algebraic powers of algebraic numbers.

Hilbert's seventh problem (1900). *Let α be an algebraic number different from 0 and 1, and let β be an irrational algebraic number. Write $\alpha = e^u$. The number $\alpha^\beta := e^{\beta u}$ is transcendental.*

This problem had soon be resolved independently by Gelfond and Schneider in 1934 and 1935 respectively and is now known as Gelfond–Schneider's theorem. For our interests, we can restate it as a problem about linear independence of logarithms of algebraic numbers. It is indeed equivalent to the following result.

Theorem 1.2 (Gelfond–Schneider [Gel34; Sch35]). *Let u_1, u_2 be two complex numbers such that e^{u_1} and e^{u_2} are algebraic. If u_1 and u_2 are linearly independent over $\mathbb{Q}$, they are linearly independent over $\overline{\mathbb{Q}}$.*

Until now, all these statements were qualitative results about linear independence of exponentials of algebraic numbers in the case of Lindemann–Weierstraß' theorem, and of logarithms in the case of Gelfond–Schneider's result. The next big step in the theory of linear forms in

logarithms had been made by Baker in 1966. He proved the first fully explicit quantitative statement about linear independence of logarithms of algebraic numbers. His theorem can be stated as follows.

Theorem 1.3 ([Bak66]). *Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers not 0 or 1, and let u_i be a logarithm of α_i. If $u_1, \dots, u_n$ are linearly independent over $\mathbb{Q}$, then $1, u_1, \dots, u_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

More precisely, for $d > 0$, there exists an effective constant C depending on $\alpha_1, \dots, \alpha_n$, and d such that for all algebraic numbers $\beta_1, \dots, \beta_n$ of degree at most d, we have

$$|\beta_1 u_1 + \cdots + \beta_n u_n| > C e^{-(n+2)\log H},$$

where H denotes the maximum of the heights of the β_i's.

To prove theorem 1.3 Baker developed what is now known as Baker's method. Our results will use a generalisation of this method in the context of abelian varieties. To better understand their nature, let us take a more general point of view on the theory.

Let G be a commutative algebraic group defined over a number field $k \subset \mathbb{C}$, and let $p \in G(\mathbb{C})$. The group $G(\mathbb{C})$ is a complex Lie group and its tangent space $t_G(\mathbb{C})$ is a complex vector space. A logarithm of p is a preimage $u \in t_G(\mathbb{C})$ by the exponential application $\exp_G : t_G(\mathbb{C}) \to G(\mathbb{C})$. Let W_0 be vector subspace of $t_G(\mathbb{C})$ defined over k (this means that W_0 can be described with linear equations with coefficients in k). The general theory of linear forms in logarithms mainly try to answer two questions:

1. Can u lie in W_0, and if yes for what reasons?
2. When $u \notin W_0$, can we give a lower-bound for the distance between u and W_0 in terms of G, u, and W_0?

The reason we still call this "linear forms in logarithms" can be seen in the following way. Consider a basis $(e_1, \dots, e_g)$ of $t_G(k)$, and a basis $(\varphi_1, \dots, \varphi_t)$ of the dual space $W_0^\perp$ of linear forms of $t_G(k)$ vanishing on W_0. Let us write $u = u_1 e_1 + \cdots + u_g e_g$ and $\varphi_i = a_{i,1} e_1^* + \cdots a_{i,g} e_g^*$. The distance $d(u, W_0)$ is then comparable to the quantity

$$\max_{1 \leqslant i \leqslant t} |u_1 a_{i,1} + \cdots u_g a_{i,g}|,$$

and the maps $(u_1, \dots, u_g) \mapsto a_{i,1} u_1 + \cdots + a_{i,g} u_g$ are linear forms in the coordinates of the logarithm u.

Historically, the most explored case of commutative algebraic group G has been the case of the group $G = \mathbb{G}_a \times \mathbb{G}_m^n$. In this context, we have $G(\mathbb{C}) = \mathbb{C} \times (\mathbb{C}^\times)^n$ and the exponential application is equal to $\mathrm{Id} \times \exp^n : (u_0, u_1, \dots, u_n) \mapsto (u_0, e^{u_1}, \dots, e^{u_n})$. If we take $u_0 = 0$, $u_1, \dots, u_n$ to be logarithms of elements of $\overline{\mathbb{Q}}$, and $W_0 := \ker(\beta_1 x_1 + \cdots + \beta_n x_n)$ a hyperplane, we recover Baker's question to find a lower-bound for the linear form

$$|\beta_1 u_1 + \cdots + \beta_n u_n|.$$

It also encompasses all previous results as Baker's theorem already generalises Lindemann–Weierstraß' and Gelfond–Schneider's theorems.

To question 1, the first general answer had been given by Wüstholz in 1989. His result states the obstruction to u to be rational is the tangent space of an algebraic subgroup of G.

Theorem 1.4 ([Wüs89]). *The smallest vector subspace of $t_G(\mathbb{C})$ defined over $\overline{\mathbb{Q}}$ that contains u is the tangent space of a connected algebraic subgroup $\widetilde{G}$ of G.*

In particular, if $u \in W_0$, then $W_0 \supseteq t_{\widetilde{G}}(\mathbb{C})$.

Although this statement is only qualitative, one can in fact give explicit upper-bounds for the degree of the subgroup $\widetilde{G}$. For example, a bound for the degree $\deg \widetilde{G}$ of a subgroup whose tangent space contains u appear in the work of David [Dav95, Théorème 2.1] in the case of G a product of elliptic curves over a number field.

Let us now look at question 2. Research about it can be divided in several categories. First, the general ones dealing with an arbitrary commutative algebraic group G over a number field. One can for example cite the results of Philippon and Waldschmidt in 1988 [PW88] and the ones of Gaudron in 2005 [Gau05]. Then, estimations for the linear group $\mathbb{G}_a \times \mathbb{G}_m^n$ – extending the work of Baker. See for example [Gau14]. Finally, – and this is the case we will be interested in – the case of G an elliptic curve and more generally an abelian variety. One of the most famous results in this case is the one of David [Dav95, Théorème 2.1]. For a product of elliptic curves $E_1 \times \cdots E_n$ defined over an arbitrary number field k, and $u_1, \dots, u_n$ such that $p_i := \exp_{E_i}(u_i) \in E_i(k)$, he gave a totally explicit lower bound for a linear form $\beta_0 + \beta_1 u_1 + \cdots \beta_n u_n$, with $(\beta_i)_i \in k^{n+1}$ under the assumption that the logarithm $(1, u_1, \dots, u_n)$ does not lie in the tangent space of an algebraic subgroup of $\mathbb{G}_a \times E_1 \times \cdots E_n$ of degree less than an explicit constant. By explicit in this context we mean a lower-bound depending on n, $[k : \mathbb{Q}]$, the Weil heights $h(\beta_i)$ of the coefficients of the linear form, the Néron–Tate heights $\widehat{h}(p_i)$ of the rationals points p_i, the heights $h(E_i)$ of the elliptic curves, the absolute values $|u_i|$ of the logarithms, and $\mathrm{Im}(\tau_i)$ with $\tau_i \in \mathbb{C}$ such that $E_i \cong \mathbb{C}^2/(\mathbb{Z} \oplus \mathbb{Z}\tau_i)$ and $\mathrm{Im}(\tau_i) > 0$. This theorem leads to the applicability of the so-called elliptic logarithm method, developed by independently by Stroeker and Tzanakis [ST94] and Gebel, Pethö, and Zimmer [GPZ94]. This method results to many Diophantine applications. See for example [SdW99; Tza02; KR18].

In the same vein of David's result, Gaudron [Gau06] proved a similar result in the context of abelian varieties defined over a number field. For a principally polarised abelian variety (A, L) defined over a number field k, a logarithm u such that $p := \exp_A(u) \in A(k)$, and a k-vector subspace W_0 of t_A of codimension t, he gave – under some technical assumption – an explicit lower-bound for the distance between u and W_0 in terms of the degree $[k : \mathbb{Q}]$, the Néron–Tate height $\widehat{h}_L(p)$ of p, the Faltings height of A, the norm $\|u\|$ relative the polarisation L, and the height of W_0. It was the first result of this kind in the level of generality. The results of this part of the thesis exactly fit in this framework.

1.2 Statement of results

Let A be an abelian variety of dimension g defined over a number field k. Let $\sigma : k \hookrightarrow \mathbb{C}$ be a complex embedding of k, and let L be a polarisation on A. The Riemann form of L_σ gives a Hermitian structure $\|\cdot\|_\sigma$ to the tangent space t_{A_σ}. Consider a vector subspace W_0 of t_{A_σ} defined over k. Let $p \in A(k)$ be k-rational point of A, and let $u \in t_{A_\sigma}$ be a logarithm of p,

that is $\exp_{A_\sigma}(u) = p$. Our goal in all this part of this manuscript is to give a lower-bound for the distance $d(u, W_{0,\sigma})$, assuming that it is not zero. We seek for an explicit bound, in terms of the classical invariants of our data such that the degree $[k : \mathbb{Q}]$ of the field of definition of A, the Faltings height $h_F(A)$ of A, the degree $\deg_L A$ of A relative to the polarisation L, the Néron–Tate height $\widehat{h}_L(p)$ of p, the norm $\|u\|_\sigma$ of u, or the height $h(W_0)$ of W_0 (this height will be defined precisely in chapter 4). We give two answers to this question: a first one under some assumption on the pair (A, u), and a second, unconditional one. A simplified version of our first lower-bound can be stated as follows.

Theorem 1.5 (theorem 4.3)**.** *Consider the above notations and define*

$$\log a := \max\left(\widehat{h}_L(p), \frac{\mathrm{e}^2\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right), \qquad \log b := \max(1, h(W_0)),$$

$$\textit{and } \mathfrak{a} \geqslant [k:\mathbb{Q}]\max\left(1, h_F(A), \log \mathrm{h}^0(A,L), \log[k:\mathbb{Q}], \log\log a\right).$$

If u does not lie in the tangent space of a proper subvariety of A, then

$$\log d(u, W_{0,\sigma}) \geqslant -C\mathfrak{a}^{1/t}\left(1 + [k:\mathbb{Q}]\mathfrak{a}\log a\right)^{g/t}\left(\mathfrak{a} + [k:\mathbb{Q}]\log b\right)(\deg_L A)^g,$$

with $C = (5(g+t))^{\frac{4(g+t+1)^2}{t}}$.

The method used to prove theorem 1.5 can be seen as a generalisation of Baker's method. However, we used all the most recent tools available in the literature, such as Hirata-Khono's reduction method, a new multiplicity lemma due to Nakamaye, and Chudnovsky's change of variables. Our result is totally explicit in the classical invariants of the abelian variety (A, L), the point p, the logarithm u, and the subspace W_0. It is very comparable to [Gau06, Théorème 1] in the case of a principally polarised abelian variety, but improves their constant c_1 from $(10(g+t))^{13\frac{(g+t)^2}{t}}$ to $(5(g+t))^{4\frac{(g+t+1)^2}{t}}$. Moreover, as Gaudron's result – and previously in the work of David and Hirata-Kohno [DH02, Theorem 1] – our result is linear in the parameter $\log b$, and is therefore optimal for this parameter. Looking at the hypothesis of the theorem, it is again similar to Gaudron's Théorème 1 hypothesis.

After proving theorem 1.5, we prove a more general result, removing its assumption on (A, u). A special case of this second main result goes as follows.

Theorem 1.6 (theorem 4.6)**.** *Consider the above notations and define*

$$M_A := \max\left(1, \log[k:\mathbb{Q}], h_F(A), \log^+\widehat{h}_L(p), \log\frac{\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right),$$

and $\log b := \max(1, h(W_0))$.

If $u \notin W_{0,\sigma}$, then

$$\log d(u, W_{0,\sigma}) \geqslant -C[k:\mathbb{Q}]^{(2g+1)(g+1)}M_A^{(g+1)^2}\max(M_A, \log b)\max\left(1, \widehat{h}_L(p), \frac{\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right)^{g^2+g},$$

with $C = (265000g)^{4g^3}$.

If $g = 1$, we have

$$\log d(u, W_\sigma) \geqslant -2 \cdot 10^{39} D^3 M_A^2 \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|_\sigma^2}{D}\right).$$

This result is the main novelty of this part of the manuscript, because it is the first one of this kind in the context of abelian varieties. Indeed, our result can be used without any restriction on the abelian variety A, and on the point u other than the fact that it does not lie in $W_{0,\sigma}$, which was not the case in [Gau06]. The proof of theorem 1.6 comes back to theorem 1.5 applied to the smallest abelian subvariety A_u which tangent space contains u. The heart of the proof is then to compare the invariants of the new setting to the ones of the original context of the theorem. It uses in a crucial way the work of Bosser and Gaudron [BG19], who proved a bound for the degree of A_u in terms of A, u, and p. We also use the recent Rémond [Rém22] who gave a new bound the Faltings height of any subvariety of A. As in theorem 1.5, the dependence in the height of the subspace W_0 is linear, and therefore optimal.

Chapitre 2

Introduction en français

2.1 Formes linéaires de logarithmes

Dans cette partie, nous présentons nos contributions à la théorie des formes linéaires de logarithmes. Un logarithme d'un nombre algébrique α, est n'importe quel nombre complexe $u \in \mathbb{C}$ tel que $e^u = \alpha$. La théorie des formes linéaires de logarithmes s'intéresse aux relations linéaires qui existent entre ces logarithmes (et plus généralement, aux logarithmes de points rationnels dans des groupes algébriques commutatifs). On peut retracer l'origine de cette théorie aux travaux de Lindemann [Lin82] d'une part, et de Weierstraß [Wei85] d'autre part, qui prouvèrent un des premiers résultats d'indépendance linéaire d'exponentielles et de logarithmes de nombres algébriques. Leur résultat est le suivant

Théorème 2.1 (Lindemann–Weierstraß)**.** *Soient $\alpha_1, \dots, \alpha_n$ des nombres algébriques distincts. Alors, les nombres $e^{\alpha_1}, \dots, e^{\alpha_n}$ sont linéairement indépendants sur le corps $\overline{\mathbb{Q}}$.*

Ce théorème prouve en particulier la transcendance de n'importe que logarithme non-nul d'un nombre algébrique α. En effet, la famille $(e^{\log \alpha}, e^0)$ est linéairement liée sur $\overline{\mathbb{Q}}$ car $e^{\log \alpha} - \alpha e^0 = 0$ et donc $\log \alpha$ ne peut être algébrique. Il découle aussi la transcendance de π car $i\pi$ est un logarithme de -1, et i est algébrique. Tous ces résultats menèrent Hilbert en 1900 à énoncer un problème de transcendance de puissances algébriques de nombres algébriques dans sa fameuse liste des 23. Son problème peut s'énoncer comme suit.

Septième problème de Hilbert (1900)**.** *Soit α un nombre algébrique différent de 0 et de 1, et soit β un nombre algébrique irrationnel. On note $\alpha = e^u$ avec $u \in \mathbb{C}$. Alors le nombre $\alpha^\beta := e^{\beta u}$ est transcendant.*

Ce problème fut rapidement résolu suite aux travaux indépendants de Gelfond [Gel34] et Schneider [Sch35] en 1934 et 1935 respectivement. Leur résultat est maintenant connu sous le nom de théorème de Gelfond–Schneider et peut être reformulé comme un problème d'indépendance linéaire entre des logarithmes de nombres algébriques. En effet, on peut montrer que le Septième problème de Hilbert est équivalent au résultat suivant.

Théorème 2.2 (Gelfond–Schneider [Gel34 ; Sch35])**.** *Soient u_1, u_2 deux nombres complexes tels que e^{u_1} et e^{u_2} sont algébriques. Si u_1 et u_2 sont linéairement indépendants sur $\mathbb{Q}$, alors ils le sont sur $\overline{\mathbb{Q}}$.*

Jusqu'à maintenant, tous les résultats que nous avons évoqués étaient des énoncés qualitatifs d'indépendance linéaire d'exponentielles de nombres algébriques dans le cas du théorème de Lindemann–Weierstraß, et de logarithmes de nombres algébriques dans le cas de Gelfond–Schneider. C'est à Baker que l'on doit une avancée majeure sur ces questions. En 1966, il prouva le premier résultat entièrement explicite d'indépendance linéaire de logarithmes. Une version de son théorème est la suivante.

Théorème 2.3 ([Bak66]). *Soient $\alpha_1, \dots, \alpha_n$ des nombres algébriques distincts de 0 ou 1, et soit u_i un logarithme de α_i. Si $u_1, \dots, u_n$ sont linéairement indépendants sur $\mathbb{Q}$, alors $1, u_1, \dots, u_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.*

Plus précisément, pour tout $d > 0$, il existe une constante effective C dépendant de $\alpha_1, \dots, \alpha_n$, et d telle que pour tous nombres algébriques $\beta_1, \dots, \beta_n$ de degré au plus d, on ait

$$|\beta_1 u_1 + \cdots + \beta_n u_n| > C e^{-(n+2)\log H},$$

où H désigne le maximum des hauteurs des β_i.

Pour démontrer le théorème 2.3 Baker développa une méthode maintenant connue sous le nom de méthode de Baker. Pour démontrer nos résultats nous utiliserons une généralisation de cette méthode dans le contexte des variétés abéliennes. Pour mieux comprendre la nature de ces résultats, nous allons prendre un point de vue plus général sur la théorie.

Soit G un groupe algébrique commutatif défini sur un corps de nombre $k \subset \mathbb{C}$, et soit $p \in G(\mathbb{C})$. Le groupe $G(\mathbb{C})$ est un groupe de Lie complexe et son espace tangent $t_G(\mathbb{C})$ est un espace vectoriel complexe. Un logarithme du point p est un antécédent de p par l'exponentielle de G, $\exp_G : t_G(\mathbb{C}) \to G(\mathbb{C})$. Soit W_0 un sous-espace de $t_G(\mathbb{C})$ défini sur k, c'est-à-dire que W_0 peut être décrit par des équations linéaires à coefficients dans k. La théorie des formes linéaires de logarithmes s'intéresse alors principalement aux deux questions suivantes :

1. Est-ce que u peut appartenir à l'espace W_0, et si oui pour quelles raisons ?

2. Quand u n'appartient pas à W_0, peut-on donner une borne inférieure pour la distance de u à W_0 en fonction du groupe G, du point u, et de W_0 ?

On peut expliquer pourquoi ces questions traitent toujours de « formes linéaires de logarithmes » de la façon suivante. Soit $(e_1, \dots, e_g)$ une base de $t_G(k)$, et soit $(\varphi_1, \dots, \varphi_t)$ une base de l'espace dual $W_0^\perp$ des formes linéaires sur $t_G(k)$ qui s'annulent sur W_0. On peut décomposer u en $u = u_1 e_1 + \cdots + u_g e_g$ et φ_i en $\varphi_i = a_{i,1} e_1^* + \cdots a_{i,g} e_g^*$. La distance $d(u, W_0)$ est alors comparable à

$$\max_{1 \leqslant i \leqslant t} |u_1 a_{i,1} + \cdots u_g a_{i,g}|,$$

et les applications $(u_1, \dots, u_g) \mapsto a_{i,1} u_1 + \cdots + a_{i,g} u_g$ sont des formes linéaires en les coordonnées du logarithme u.

Historiquement, le cas de groupe algébrique commutatif G le plus étudié a été le cas $G = \mathbb{G}_a \times \mathbb{G}_m^n$. Dans ce cas on a $G(\mathbb{C}) = \mathbb{C} \times (\mathbb{C}^\times)^n$ et l'exponentielle de G est l'application $\mathrm{Id} \times \exp^n$: $(u_0, u_1, \dots, u_n) \mapsto (u_0, e^{u_1}, \dots, e^{u_n})$. Si on prend $u_0 = 0$, $u_1, \dots, u_n$ des logarithmes d'éléments

de $\overline{\mathbb{Q}}$, et $W_0 := \ker(\beta_1 x_1 + \cdots + \beta_n x_n)$ un hyperplan, on retrouve le problème de Baker de minorer la forme linéaire

$$|\beta_1 u_1 + \cdots + \beta_n u_n|.$$

Ces questions englobent aussi tous les résultats antérieurs au théorème de Baker qui les généralisaient déjà.

La première réponse générale à la question 1 a été apportée par Wüstholz in 1989. Son résultat énonce que la seule obstruction à u d'être rationnel est l'espace tangent d'un sous-groupe algébrique de G.

Théorème 2.4 ([Wüs89]). *Le plus petit espace vectoriel de $t_G(\mathbb{C})$ défini sur $\overline{\mathbb{Q}}$ qui contient u est l'espace tangent d'un sous-groupe algébrique connexe $\widetilde{G}$ de G.*

En particulier, si $u \in W_0$, alors $W_0 \supseteq t_{\widetilde{G}}(\mathbb{C})$.

Malgré le fait que cet énoncé soit seulement qualitatif, on peut énoncer des bornes effectives sur le degré du sous-groupe $\widetilde{G}$. Par exemple, on peut trouver dans le travail de David [Dav95, Théorème 2.1], une borne sur le degré d'un sous-groupe dont l'espace tangent contient u dans le cas où G est un produit de courbes elliptiques définies sur un corps de nombres.

Intéressons-nous maintenant à la question 2. On peut découper les travaux sur ces questions en plusieurs catégories. Tout d'abord, les énoncés concernant un sous-groupe algébrique commutatif G arbitraire. On peut citer entre autres les travaux importants de Philippon et Waldschmidt de 1988 [PW88], et ceux de Gaudron de 2005 [Gau05]. Ensuite, les estimations pour le groupe linéaire $\mathbb{G}_a \times \mathbb{G}_m^n$ – qui généralisent les travaux de Baker. Voir par exemple le travail [Gau14]. Enfin, – et c'est le cas qui nous intéressera par la suite – le cas de G une courbe elliptique ou plus généralement une variété abélienne. L'un des résultats les plus connus sur ce sujet est celui de David [Dav95, Théorème 2.1]. Pour G un produit de courbes elliptiques $E_1 \times \cdots \times E_n$ toutes définies sur un même corps de nombres k, et des logarithmes $u_1, \ldots, u_n$ tels que $p_i := \exp_{E_i}(u_i) \in E_i(k)$, il donne une borne inférieure entièrement effective pour la forme linéaire $\beta_0 + \beta_1 u_1 + \cdots + \beta_n u_n$, avec $(\beta_i)_i \in k^{n+1}$, sous l'hypothèse que le logarithme $(1, u_1, \ldots, u_n)$ n'appartiennent pas à l'espace tangent d'un sous-groupe algébrique de $\mathbb{G}_a \times E_1 \times \cdots \times E_n$, de degré inférieur à une constante effective. Par effectif dans ce contexte, nous entendons une borne ne dépendant que n, du degré $[k : \mathbb{Q}]$, des hauteurs de Weil $h(\beta_i)$ des coefficients de la forme linéaire, des hauteurs de Néron–Tate $\widehat{h}(p_i)$ des points rationels p_i, des hauteurs de Faltings $h(E_i)$ des courbes elliptiques, de la valeur absolue $|u_i|$ des logarithmes, et enfin de $\mathrm{Im}(\tau_i)$ avec $\tau_i \in \mathbb{C}$ tel que $E_i \cong \mathbb{C}^2/(\mathbb{Z} \oplus \tau_i \mathbb{Z})$. Ce théorème mena à la mise en œuvre de la méthode du logarithme elliptique, imaginée indépendamment par Stroeker et Tzanakis [ST94], et Gebel, Pethö, et Zimmer [GPZ94]. Cette méthode déboucha sur de nombreux résultats diophantiens. Voir par exemple [SdW99 ; Tza02 ; KR18].

Dans la même lignée des résultats de David, Gaudron prouva en 2006 [Gau06] un résultat similaire dans le cadre des variétés abéliennes définies sur des corps de nombres. Pour une variété abélienne principalement polarisée (A, L) définie sur un corps de nombres k, un logarithme u d'un point rationnel $p \in A(k)$, et un sous-k-espace vectoriel W_0 de $t_{A(\mathbb{C})}$ de codimension t, Gaudron donne – sous certaines hypothèses techniques – une borne inférieure effective pour la distance de u à W_0 en fonction du degré $[k : \mathbb{Q}]$, de la hauteur de Néron–Tate $\widehat{h}_L(p)$ de p, de la hauteur de Faltings de A, de la norme $\|u\|$ relative à la polarisation L, et de la hauteur de W_0. Ce résultat

était à l'époque le premier résultat totalement explicite de ce genre, dans ce niveau de généralité. Les résultats de cette partie de la thèse s'intègrent dans ce contexte et généralisent les résultats de Gaudron.

2.2 Résultats

Soit A une variété abélienne de dimension g définie sur un corps de nombres k. Soit $\sigma : k \hookrightarrow \mathbb{C}$ un plongement complexe de k, et soit L une polarisation de A. La forme de Riemann de L_σ munit l'espace tangent t_{A_σ} d'une structure hermitienne $\|\cdot\|_\sigma$. Soit W_0 un sous-espace vectoriel k-rationnel de t_A. On considère enfin un point rationnel $p \in A(k)$ et un logarithme $u \in t_{A_\sigma}$ de p, c'est-à-dire tel que $\exp_{A_\sigma}(u) = p$. Notre but est de minorer la distance $d(u, W_{0,\sigma})$ relative à la structure hermitienne de t_{A_σ} donnée par L_σ. Nous cherchons une borne aussi explicite que possible, fonction des invariants algébriques et analytiques de nos données, tels que le degré $[k : \mathbb{Q}]$ du corps de définition de A, la hauteur de Faltings $h_F(A)$ de A, le degré $\deg_L A$ de A relatif à la polarisation L, la hauteur de Néron–Tate $\widehat{h}_L(p)$ du point p, la norme $\|u\|_\sigma$ de u, ou la hauteur $h(W_0)$ de W_0 (cette hauteur sera définie précisément dans le chapitre 4). Nous donnons deux minorations pour cette distance. Une première sous une hypothèse sur la paire (A, u), et une seconde totalement inconditionnelle. Un énoncé simplifié de notre premier résultat est le suivant.

Théorème 2.5 (Theorem 4.3)**.** *Avec les notations ci-dessus, définissons*

$$\log a := \max\left(\widehat{h}_L(p), \frac{\mathrm{e}^2\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right), \qquad \log b := \max(1, h(W_0)),$$

$$\textit{et } \mathfrak{a} \geqslant [k:\mathbb{Q}] \max\left(1, h_F(A), \log \mathrm{h}^0(A, L), \log[k:\mathbb{Q}], \log\log a\right).$$

Si u n'appartient à l'espace tangent d'aucune sous-variété stricte de A, alors

$$\log d(u, W_{0,\sigma}) \geqslant -C\mathfrak{a}^{1/t}\left(1 + [k:\mathbb{Q}]\mathfrak{a}\log a\right)^{g/t}\left(\mathfrak{a} + [k:\mathbb{Q}]\log b\right)(\deg_L A)^g,$$

avec $C = (5(g+t))^{\frac{4(g+t+1)^2}{t}}$.

La méthode utilisée pour prouver le théorème 2.5 peut être vue comme une généralisation de la méthode de Baker. Cependant, nous utilisons les outils les plus récents existant dans la littérature, tels que la méthode de réduction d'Hirata-Khono, un nouveau lemme de multiplicité dû à Nakamaye, ou le principe de changement de variables de Chudnovsky. Nos résultats sont totalement effectifs en les invariants classiques de la variété abélienne (A, L), du point p, du logarithme u, et du sous-espace W_0. Ils sont comparables au [Gau06, Théorème 1] dans le cas d'une variété abélienne principalement polarisée, mais améliorent leur constante c_1 de $(10(g+t))^{13\frac{(g+t)^2}{t}}$ à $(5(g+t))^{4\frac{(g+t+1)^2}{t}}$. De plus, comme chez Gaudron – et comme précédemment dans le travail de David et Hirata-Kohono [DH02, Theorem 1] – notre minoration est linéaire en $\log b$, et donc optimal pour ce paramètre. En comparant l'hypothèse de notre théorème et l'hypothèse du résultat [Gau06, Théorème 1], on peut voir qu'elles sont similaires.

Une fois le théorème 2.5 démontré, nous prouvons un second résultat plus général, supprimant l'hypothèse sur la paire (A, u). Un cas particulier de notre énoncé s'énonce de la manière suivante.

Théorème 2.6 (Theorem 4.6)**.** *Avec les notations ci-dessus, on définit*

$$M_A := \max\left(1, \log[k:\mathbb{Q}], h_F(A), \log^+ \widehat{h}_L(p), \log \frac{\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right),$$

et $\log b := \max(1, h(W_0))$.

Si $u \notin W_{0,\sigma}$ *et* $g \geqslant 2$*, alors*

$$\log d(u, W_{0,\sigma}) \geqslant -C[k:\mathbb{Q}]^{(2g+1)(g+1)} M_A^{(g+1)^2} \max(M_A, \log b) \max\left(1, \widehat{h}_L(p), \frac{\|u\|_\sigma^2}{[k:\mathbb{Q}]}\right)^{g^2+g},$$

avec $C = (265000g)^{4g^3}$.

Si $g = 1$*, on a*

$$\log d(u, W_\sigma) \geqslant -2 \cdot 10^{39} D^3 M_A^2 \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|_\sigma^2}{D}\right).$$

Ce résultat est la principale nouveauté de cette partie du manuscrit. C'est le premier résultat de ce type dans le cadre des variétés abéliennes. En effet, étant totalement inconditionnel, il peut être utilisé sans aucune restriction sur la variété abélienne A, ni sur logarithme u autre qu'il n'appartienne pas à l'espace $W_{0,\sigma}$, ce qui n'était par exemple pas le cas dans [Gau06]. La preuve du théorème 2.6 se base sur le théorème 2.5 appliqué à la plus petite sous-variété abélienne A_u dont l'espace tangent contient u. Le cœur de notre preuve est alors de comparer les invariants de nos nouvelles données, en fonction des données initiales. Cette partie de la preuve utilise de manière essentielle les travaux de Bosser et Gaudron [BG19] qui ont donné une majoration du degré de A_u en fonction de A, u, et p. Nous utilisons aussi les résultats récents de Rémond [Rém22] qui a donné une nouvelle borne pour la hauteur de Faltings d'une sous-variété de A. Comme pour le théorème 2.5, la dépendance en la hauteur du sous-espace W_0 est linéaire et ainsi optimale.

Chapter 3

Preliminaries

This chapter is devoted to introduce the tools we will use in this part of the thesis and their main properties. The content of this chapter is contain no original result and we will refer to the existing literature for further developments of these topics.

3.1 Hermitian adelic vector bundles

3.1.1 Definitions

We present here the main concepts of the theory of Hermitian adelic vector bundles. We restrict our exposition to Hermitian adelic vector bundles over the spectrum of the integer ring of a number field, even though a more general theory of adelic vector bundles over the spectrum of a number field exists. The content of this section comes essentially from [Gau08], [GR13], [Gau14, §3], and [Gau21]. We fix a number field k of degree D, and we write $\mathcal{O}_k$ for its ring of integers. For any place v of k, let k_v be the v-adic completion of k, and $\mathbb{C}_v$ be the v-adic completion of an algebraic closure of k.

Definition 3.1 ([Gau08, 3. Fibré vectoriel adélique])**.** *A Hermitian adelic fiber bundle $\overline{\mathcal{E}}$ over $\operatorname{Spec}\mathcal{O}_k$ is the data of a $\mathcal{O}_k$-projective module of finite type $\mathcal{E}$ together with, for every Archimedean place v of k, a norm $\|\cdot\|_v$ on the $\mathbb{C}_v$-vector space $E_v := \mathcal{E}\otimes_{\mathcal{O}_k}\mathbb{C}_v$ that is Euclidean if v is real, and Hermitian and invariant under complex conjugation if v is complex.*

Remark 3.2. *Any Hermitian adelic vector bundle $\overline{\mathcal{E}}$ over $\operatorname{Spec}\mathcal{O}_k$ naturally comes with an integral structure. Indeed, for a finite place v of k and $x\in E_v$, the quantity*

$$\|x\|_v := \inf\{|a|_v, a\in\mathbb{C}_v,\ \textit{such that } x\in a\cdot(E\otimes\mathcal{O}_{\mathbb{C}_v})\}$$

defines an ultrametric norm on E_v. Moreover, choosing a minimal spanning family $(e_1,\dots,e_n)$ of $\mathcal{E}$, we have for any $\lambda_1,\dots,\lambda_n\in\mathbb{C}_v$,

$$\left\|\sum_{i=1}^n \lambda_i e_i\right\|_v = \max_{1\leqslant i\leqslant n}|\lambda_i|_v.$$

The classical operations of linear algebra naturally transfer to Hermitian adelic vector bundles. We present below the main constructions we will use in the upcoming chapters.

Definition 3.3 ([Gau21, 2.2 Rigid Adelic Spaces]). *Let $\overline{\mathcal{E}}$ and $\overline{\mathcal{F}}$ be two Hermitian adelic vector bundles over* $\operatorname{Spec}\mathcal{O}_k$. *The following spaces are Hermitian adelic vector bundles over* $\operatorname{Spec}\mathcal{O}_k$.

- *The induced space $\overline{\mathcal{F}}$, for a submodule $\mathcal{F}$ of $\mathcal{E}$, with the induced norms.*

- *The Hermitian sum $\overline{\mathcal{E}\oplus\mathcal{F}}$ with norms $\|x\oplus y\|_v^2 := \|x\|_v^2 + \|y\|_v^2$, for all Archimedean place v and $x\oplus y\in E_v\oplus F_v$.*

- *The quotient $\overline{\mathcal{E}/\mathcal{F}}$, for a submodule $\mathcal{F}$, with the quotient norms defined by*

$$\|x+F_v\|_v := \inf\{\|y\|_v, x-y\in F_v\}, \quad \forall x\in E_v.$$

- *The tensor product $\overline{\mathcal{E}\otimes_{\mathcal{O}_k}\mathcal{F}}$ with the tensor norms constructed as follows. Let v be a Archimedean place of k. Let $(e_1,\dots,e_n)$, $(f_1,\dots,f_m)$ be orthonormal bases of E_v and F_v respectively. The norm of an element $x=\sum\limits_{i,j}\lambda_{i,j}e_i\otimes f_j$ of $(\mathcal{E}\otimes_{\mathcal{O}_k}\mathcal{F})_v = E_v\otimes_{\mathbb{C}_v}F_v$ is*

$$\|x\|_v^2 := \sum_{i,j}|\lambda_{i,j}|^2.$$

  This indeed defines a norm on $(\mathcal{E}\otimes_{\mathcal{O}_k}\mathcal{F})_v$ which is independent of the choice of the orthonormal bases.

- *The space $\overline{\operatorname{Hom}(\mathcal{E},\mathcal{F})}$ with the operator norms defined by*

$$\|f\|_v = \inf_{x\in E_v\setminus\{0\}}\frac{\|f(x)\|_v}{\|x\|_v}, \quad \forall f\in\operatorname{Hom}(E_v,F_v).$$

  In particular the dual space $\overline{\mathcal{E}^\vee}$ is a Hermitian adelic vector bundle.

- *For a positive integer i, the i-th symmetric power $\overline{\operatorname{Sym}^i(\mathcal{E})}$ of $\mathcal{E}$ with the quotient norm coming from the natural surjection $E_v^{\otimes i}\to\operatorname{Sym}^i(E_v)$. If $(e_1,\dots,e_n)$ is an orthonormal basis of E_v, then the family $(e_1^{i_1}\cdots e_n^{i_n})_{i_1+\cdots+i_n=i}$ is orthogonal and we have*

$$\|e_1^{i_1}\cdots e_n^{i_n}\|_v^2 = \frac{i!}{i_1!\cdots i_n!}.$$

- *For a positive integer i, the i-th exterior power $\overline{\wedge^i\mathcal{E}}$ of $\mathcal{E}$ with the quotient norms coming from the natural surjection $E_v^{\otimes i}\to\wedge^i E_v$. For i vectors $e_1,\dots,e_i$ in E_v, one has*

$$\|e_1\wedge\cdots\wedge e_i\|_v^2 = \det(\langle e_n,e_m\rangle_v)_{1\leqslant n,m\leqslant i},$$

  where $\langle\cdot,\cdot\rangle_v$ denotes the inner product on E_v associated to $\|\cdot\|_v$.

  In particular the determinant $\overline{\det\mathcal{E}} := \overline{\wedge^{\operatorname{rk}\mathcal{E}}\mathcal{E}}$ is a Hermitian adelic vector bundle.

3.1.2 Slopes and heights

Definition 3.4 ([Gau14, Définition 3.3]). *Let $\overline{\mathcal{E}}$ be a Hermitian adelic vector bundle over* $\operatorname{Spec}\mathcal{O}_k$.

- *If* $\operatorname{rk}\mathcal{E}=1$, *the (normalised) Arakelov degree of* $\overline{\mathcal{E}}$ *is defined as*

$$\widehat{\deg}_{\mathrm{n}}\,\overline{\mathcal{E}} := -\frac{1}{D}\sum_{v}[k_v:\mathbb{Q}_v]\log\|x\|_v,$$

  where the sum ranges over all places v of k (Archimedean or not), and x is any non-zero element of $\mathcal{E}$. This definition is independent of the choice of x.

- *If* $\operatorname{rk}\mathcal{E}\geqslant 1$, *the Arakelov degree of* $\overline{\mathcal{E}}$ *is the Arakelov degree of* $\overline{\det\mathcal{E}}$.

- *The height of* $\overline{\mathcal{E}}$ *is defined by* $h(\overline{\mathcal{E}}) := -\widehat{\deg}_{\mathrm{n}}\overline{\mathcal{E}}$.

- *The Arakelov slope* $\widehat{\mu}(\overline{\mathcal{E}})$ *of* $\overline{\mathcal{E}}$ *is the number*

$$\widehat{\mu}(\overline{\mathcal{E}}) := \frac{\widehat{\deg}_{\mathrm{n}}\,\overline{\mathcal{E}}}{\operatorname{rk}\mathcal{E}}.$$

- *Let* $x\in(\mathcal{E}\otimes_{\mathcal{O}_k}k)\setminus\{0\}$, *the Arakelov height of x is defined as*

$$\widehat{h}(x) := \frac{1}{D}\sum_{v}[k_v:\mathbb{Q}_v]\log\|x\|_v.$$

These notions nicely behave with respect to the constructions we gave in definition 3.3, as stated in the following proposition.

Proposition 3.5 ([Gau21, Proposition 5]). *Let $\overline{\mathcal{E}}$, $\overline{\mathcal{F}}$ be two Hermitian adelic vector bundles over* $\operatorname{Spec}\mathcal{O}_k$. *We have*

- $\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{E}\oplus\mathcal{F}}\right)=\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{E}}\right)+\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{F}}\right)$;
- *If $\mathcal{F}$ is a submodule of $\mathcal{E}$,* $\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{E}/\mathcal{F}}\right)=\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{E}}\right)-\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{F}}\right)$;
- $\widehat{\mu}\left(\overline{\mathcal{E}\otimes\mathcal{F}}\right)=\widehat{\mu}\left(\overline{\mathcal{E}}\right)+\widehat{\mu}\left(\overline{\mathcal{F}}\right)$;
- $\widehat{\mu}\left(\overline{\mathcal{E}^{\vee}}\right)=-\widehat{\mu}\left(\overline{\mathcal{E}}\right)$;
- *More generally* $\widehat{\mu}\left(\overline{\operatorname{Hom}(\mathcal{E},\mathcal{F})}\right)=\widehat{\mu}(\overline{\mathcal{E}})-\widehat{\mu}(\overline{\mathcal{F}})$;

Finally, for two submodules $\mathcal{F}$ and $\mathcal{G}$ of a Hermitian adelic vector bundle $\overline{\mathcal{E}}$ over $\operatorname{Spec}\mathcal{O}_k$, we can compare the degrees of $\overline{\mathcal{F}}$, $\overline{\mathcal{G}}$, $\overline{\mathcal{F}+\mathcal{G}}$ and $\overline{\mathcal{F}\cap\mathcal{G}}$.

Proposition 3.6 ([Gau21, Proposition 6]). *We have*

$$\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{F}}\right)+\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{G}}\right)\leqslant\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{F}+\mathcal{G}}\right)+\widehat{\deg}_{\mathrm{n}}\left(\overline{\mathcal{F}\cap\mathcal{G}}\right).$$

A natural way Hermitian adelic vector bundles arise is through ample invertible sheaves on schemes over $\operatorname{Spec}\mathcal{O}_k$.

Definition 3.7. *A Hermitian line bundle $\overline{\mathcal{L}}$ on a scheme $\mathcal{X}$ over* $\operatorname{Spec}\mathcal{O}_k$ *is an invertible sheaf $\mathcal{L}$ over $\mathcal{X}$ together with, for all $x \in \mathcal{X}(\mathcal{O}_k)$ and all Archimedean place v of k, a norm $\|\cdot\|_{x,v}$ on the fiber $(x^\star\mathcal{L})_v$ which is Euclidean if v is real, and Hermitian and invariant under complex conjugation if v is complex.*

Given a Hermitian line bundle $\overline{\mathcal{L}}$, on $\mathcal{X}/\operatorname{Spec}\mathcal{O}_k$, the $\mathcal{O}_k$-module $x^\star\mathcal{L}$ is thus given a structure of Hermitian adelic vector bundle of rank one. This leads to the following notion of height.

Definition 3.8. *Let $\overline{\mathcal{L}}$ be a Hermitian line bundle on a scheme $\mathcal{X}$ over* $\operatorname{Spec}\mathcal{O}_k$*, and let $x \in \mathcal{X}(\mathcal{O}_k)$. The height of x relative to $\mathcal{L}$ is defined as*

$$h_{\mathcal{L}}(x) := \widehat{\deg}_{\mathrm{n}}\left(\overline{x^\star\mathcal{L}}\right) = -\frac{1}{D}\sum_v [k_v : \mathbb{Q}_v] \log \|s(x)\|_{x,v},$$

where the sum ranges over all the places v of k, and s is a local section of $\mathcal{L}$ that does not vanish at x.

The final tool of Arakelov theory of Hermitian adelic vector bundles we will need is the maximal slope of a bundle. It is a fact that, for a Hermitian adelic vector bundle $\overline{\mathcal{E}}$, there is a constant $c(\overline{\mathcal{E}})$, depending only on $\overline{\mathcal{E}}$, such that for any submodule $\mathcal{F}$ of $\mathcal{E}$, we have

$$\widehat{\mu}(\overline{\mathcal{F}}) \leqslant c(\overline{\mathcal{E}}).$$

See [Gau08, Proposition 5.3] or [Gau21, Lemma 12] for a proof of this result. This legitimises the following definition.

Definition 3.9. *Let $\overline{\mathcal{E}}$ be a Hermitian adelic vector bundle over* $\operatorname{Spec}\mathcal{O}_k$*. The maximal slope of $\mathcal{E}$ is the real number*

$$\widehat{\mu}_{\max}(\overline{\mathcal{E}}) := \sup\left\{\widehat{\mu}(\overline{\mathcal{F}}),\ \mathcal{F} \text{ submodule of } \mathcal{E}\right\}.$$

A direct consequence of this definition is that the maximal slope of $\overline{\mathcal{E}}$ is always at least as big as the Arakelov degree of any line of $\mathcal{E}$. The opposite of the degree of a line being the height of one its non-zero elements, we get the following result.

Proposition 3.10. *Let $\overline{\mathcal{E}}$ be a Hermitian adelic vector bundle over* $\operatorname{Spec}\mathcal{O}_k$*. For any non-zero element x of $\mathcal{E} \otimes_{\mathcal{O}_k} k$, we have*

$$-\widehat{\mu}_{\max}(\overline{\mathcal{E}}) \leqslant \widehat{h}(x).$$

This seemingly trivial result will in fact play a key role in our study.

The maximal slope behaves less nicely with the natural operations on Hermitian adelic vector bundles than the Arakelov slope. We will still need estimates for the maximal slope of tensor products and symmetric powers. We have the following results.

Proposition 3.11 ([Gau08, Propriétés 5.7])**.** *Let $\overline{\mathcal{E}}$, $\overline{\mathcal{F}}$ be two Hermitian adelic fiber bundles over* $\operatorname{Spec}\mathcal{O}_k$ *with* $\operatorname{rk}\mathcal{F} = 1$*. We have*

$$\widehat{\mu}_{\max}(\overline{\mathcal{E}\otimes\mathcal{F}}) = \widehat{\mu}_{\max}(\overline{\mathcal{E}}) + \widehat{\mu}_{\max}(\overline{\mathcal{F}}).$$

Proposition 3.12 ([GR13, Proposition 8.4])**.** *Let $\overline{\mathcal{E}}$ be a Hermitian adelic fiber bundle over* $\operatorname{Spec}\mathcal{O}_k$*. For any positive integer ℓ, we have*

$$\widehat{\mu}_{\max}\left(\overline{\operatorname{Sym}^\ell\mathcal{E}}\right) \leqslant \ell\left(\widehat{\mu}_{\max}\left(\overline{\mathcal{E}}\right) + 2\log\operatorname{rk}\mathcal{E}\right).$$

3.2 Complex abelian varieties

In this section, we recall some of the theory of abelian varieties defined over the field of complex numbers. We will only scratch the surface of this very rich theory. For many more details on this subject, see [BL04].

3.2.1 Line bundles and factors of automorphy

Let A be an abelian variety over $\mathbb{C}$ and let t_A denotes the tangent space of A at 0_A. The group $A(\mathbb{C})$ of $\mathbb{C}$-points of A is naturally given the structure of a connected compact complex Lie group. This ensures (see [BL04, Lemma 1.1.1]) that $A(\mathbb{C})$ is a complex torus and comes with its exponential function

$$\exp_A : t_A \longrightarrow A(\mathbb{C}).$$

The map $\exp_A$ is surjective and its kernel denoted Ω_A is called the period lattice of A. In order to relate holomorphic function on t_A, and holomorphic line bundles on A, we define the notion of factor of automorphy on A.

Definition 3.13. *Let $Z^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$ denotes the group holomorphic maps $a : \Omega_A \times t_A \to \mathbb{C}^\times$ satisfying the cocycle relation*

$$a(\omega_1 + \omega_2, x) = a(\omega_1, \omega_2 + x)a(\omega_2, x), \quad \forall \omega_1, \omega_2 \in \Omega_A, \ \forall x \in t_A.$$

The elements of $Z^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$ are called factors of automorphy of A.

For any non-vanishing holomorphic function $g : t_A \to \mathbb{C}^\times$, the map $a_g : \Omega \times t_A \to \mathbb{C}^\times$ given by

$$a_0(\omega, x) = \frac{g(\omega + x)}{g(x)}$$

is a factor of automorphy. The group of such factors of automorphy is denoted $B^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$.

We let $H^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$ to be the group $Z^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))/B^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$.

Theorem 3.14 ([BL04, Proposition B.1])**.** *There is a group isomorphism between the Picard group $\mathrm{Pic}(A)$ of holomorphic line bundles on A and $H^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$.*

Sketch of proof. Let L be a holomorphic line bundle on A. One can pull back $L(\mathbb{C})$ by $\exp_A$ to get the holomorphic line bundle $\exp_A^\star L(\mathbb{C})$ on t_A. This bundle is necessarily trivial because there is no non-trivial holomorphic line bundle on a complex vector space (see [BL04, Lemma 2.1.1.]). Given a trivialisation $\alpha : \exp_A^\star L(\mathbb{C}) \to t_A \times \mathbb{C}$, we get the following diagram.

$$\begin{array}{ccccc} t_A \times \mathbb{C} & \xleftarrow{\alpha} & \exp_A^\star L(\mathbb{C}) & \xrightarrow{\exp_A^\star} & L(\mathbb{C}) \\ & \searrow & \downarrow & & \downarrow \\ & & t_A & \xrightarrow{\exp_A} & A(\mathbb{C}) \end{array}$$

The action of Ω_A on t_A by translation can be pulled back on $\exp_A^\star L(\mathbb{C})$, and then on $t_A \times \mathbb{C}$ using α. It can be shown that this action of Ω_A on $t_A \times \mathbb{C}$ is of the shape $\omega \cdot (x, z) = (x + \omega, a(\omega, x)z)$ for a factor of automorphy a which class in $H^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$ is independent of α.

Conversely, given a factor of automorphy a one can construct a holomorphic line bundle $L := (t_A \times \mathbb{C})/\Omega_A$ where Ω_A acts on $t_A \times \mathbb{C}$ by $\omega \cdot (x, z) = (\omega + x, a(\omega, x)z)$. One shows that this construction factors through $B^1(\Omega_A, H^0(\mathcal{O}^\star_{t_A}))$ and is the inverse of the previous construction. ■

From theorem 3.14, we can deduce a correspondence between sections of (A, L) and some holomorphic functions on t_A.

Theorem 3.15 ([BL04, Appendix B, p.574])**.** *Let L be a holomorphic line bundle on A and let a be a factor of automorphy corresponding to $L \in \mathrm{Pic}(A)$. Define the $\mathbb{C}$-vector space*

$$\Theta(a) := \left\{ \vartheta : t_A \to \mathbb{C} \;\middle|\; \begin{array}{l} \vartheta \text{ is holomorphic and} \\ \vartheta(x+\omega) = a(\omega, x)\vartheta(x), \ \forall (\omega, x) \in \Omega_A \times t_A \end{array} \right\}.$$

We have an isomorphism of $\mathbb{C}$-vector spaces $H^0(A, L) \cong \Theta(a)$.

Sketch of proof. Similarly to the proof of theorem 3.14, given a holomorphic line bundle L, its pull-back by $\exp_A$ is a trivial line bundle on t_A, and the choice of a trivialisation α give rise to the factor of automorphy a. Given a section $s \in H^0(A, L)$ of L, we then get the following diagram.

$$\begin{array}{ccccc} t_A \times \mathbb{C} & \xleftarrow{\alpha} & \exp_A^\star L(\mathbb{C}) & \xrightarrow{\exp_A^\star} & L(\mathbb{C}) \\ & \searrow & \downarrow \uparrow \exp_A^\star s & & \downarrow \uparrow s \\ & & t_A & \xrightarrow[\exp_A]{} & A(\mathbb{C}) \end{array}$$

From the definition of a, one see that we have $\alpha \circ \exp_A^\star s(x) = (x, \vartheta(x))$ for some holomorphic function ϑ satisfying $\vartheta(x + \omega) = a(\omega, x)\vartheta(x)$. This yields a map $H^0(A, L) \to \Theta(a)$ which can be shown to be an isomorphism. ■

3.2.2 The Riemann form of a line bundle

Let L be a holomorphic line bundle on A. It can be viewed as an element of the group $H^1(X, \mathcal{O}^\star_X)$. From the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_{A(\mathbb{C})} \xrightarrow{\exp(2i\pi\cdot)} \mathcal{O}^\star_{A(\mathbb{C})} \longrightarrow 0,$$

one gets a morphism $H^1(A, \mathcal{O}^\star_{A(\mathbb{C})}) \to H^2(A, \mathbb{Z})$. Define the Néron–Severi group $NS(A)$ to be the image of this morphism. The following theorem states that it corresponds to a class of Hermitian forms on t_A.

Theorem 3.16 ([BL04, Theorem 2.1.2, Proposition 2.1.6 and Lemma 2.1.7])**.** *There is an isomorphism between $NS(A)$ and the group of Hermitian forms $H : t_A \times t_A \to \mathbb{C}$ satisfying $\mathrm{Im}\, H(\Omega_A, \Omega_A) \subseteq \mathbb{Z}$.*

Given a holomorphic line bundle L over A, the Hermitian form H corresponding to the image of L in $NS(A)$ is called its Riemann form.

For our purposes, the interest of the Riemann form of a holomorphic line bundle L is twofold. It gives a canonical factor of automorphy corresponding to L, and it defines a hermitian structure on t_A.

Definition 3.17. *Let $H : t_A \times t_A \to \mathbb{C}$ be a Hermitian form such that $\operatorname{Im} H(\Omega_A, \Omega_A) \subseteq \mathbb{Z}$. A semi-character for H is a map $\chi : \Omega_A \to \mathbb{U}$ (where $\mathbb{U}$ is the group of complex numbers of module 1) satisfying $\chi(\omega_1 + \omega_2) = \chi(\omega_1)\chi(\omega_2)\exp(i\pi H(\omega_1, \omega_2))$.*

Theorem 3.18 ([BL04, 2.2])**.** *Let $H \in NS(A)$ and let χ be a semi-character for H. Let $a_{H,\chi}$ be the map defined by*

$$a_{H,\chi} : \left| \begin{array}{ccc} \Omega_A \times t_A & \longrightarrow & \mathbb{C}^\star \\ (\omega, x) & \longmapsto & \chi(\omega)\exp\left(\pi H(x,\omega) + \frac{\pi}{2}H(\omega,\omega)\right) \end{array} \right. .$$

The map $a_{H,\chi}$ is a factor of automorphy for A and the associated holomorphic line bundle $L(H,\chi)$ admits H as its Riemann form. Moreover, the mapping $(H,\chi) \mapsto L(H,\chi)$ is an isomorphism onto the group of holomorphic line bundles. Given L, the associated pair (H,χ) is called the Appel–Humbert data of L.

Remark 3.19. *For a holomorphic line bundle L, the factor of automorphy $a_{H,\chi}$ coming from the Appel–Humbert data of L is canonically attached to L. We will therefore usually denote by $\Theta(A,L)$ the space $\Theta(a_{L,\chi})$ of theorem 3.15.*

Consider now $\vartheta \in \Theta(A,L)$. Notice that the map

$$\begin{array}{ccc} t_A & \longrightarrow & \mathbb{C} \\ z & \longmapsto & |\vartheta(z)|\exp\left(-\frac{\pi}{2}H(z,z)\right) \end{array}$$

is invariant under translations by elements of Ω_A. Moreover, if L is ample then its Riemann form is a positive definite Hermitian form (see [BL04, Proposition 4.5.2.]). Hence, given $z \in t_A$ and $x := \exp_A(z)$, we can endow the fiber L_x with the Hermitian metric

$$\|s(x)\|_{L_x} := |\vartheta(z)|\exp\left(-\frac{\pi}{2}\|z\|_L^2\right), \quad \forall s \in H^0(A,L), \tag{3.1}$$

where $\vartheta \in \Theta(A,L)$ is the theta function associated to s by theorem 3.15, and $\|z\|_L := H(z,z)$. This definition is independent of the choice of the section s. This defines two norms on $H^0(A,L)$:

$$\|s\|_\infty := \sup_{x \in A(\mathbb{C})} \|s(x)\|_{L_x} \quad \text{and} \quad \|s\|_2^2 := \int_{A(\mathbb{C})} \|s(x)\|_{L_x}^2 \mathrm{d}x.$$

3.2.3 Injectivity diameter and covering radius

We conclude this section with two metric properties of complex abelian varieties: the injectivity diameter and the covering radius.

Definition 3.20. *Let (A,L) be a polarised complex abelian variety. The injectivity diameter $\rho(A,L)$ of (A,L) is the diameter of the biggest ball of t_A such that $\exp_A$ is injective, namely*

$$\rho(A,L) := \inf_{\omega \in \Omega_A \setminus \{0\}} \|\omega\|_L.$$

The covering radius $r(A, L)$ of (A, L) is the maximum distance of a point of t_A to the period lattice:

$$r(A, L) := \sup_{z \in t_A,\ \omega \in \Omega_A} \|z - \omega\|_L.$$

The injectivity diameter is a special case of minima associated to a lattice. It is the first minimum of Ω_A. In fact, the study of minima of a lattice allows one to compare $\rho(A, L)$ and $r(A, L)$.

Proposition 3.21 ([BG19, 3.11.1, p. 28])**.** *Let (A, L) be a polarised complex abelian variety of dimension g. We have*

$$r(A, L) \leqslant \frac{g\, \mathrm{h}^0(A, L)}{\rho(A_\sigma, L_\sigma)},$$

where $\mathrm{h}^0(A, L)$ denote the dimension of $H^0(A, L)$.

3.3 Abelian varieties over number fields

3.3.1 Faltings height

We recall the definition of the Faltings height of an abelian variety over a number field. For a reference, see for example [GR14b, 2.3 Hauteur de Faltings] . Notice however that the normalisation they choose for their Faltings height is slightly different from ours.

Let A be an abelian variety over a number field k. Let K/k be a finite extension such that A_K is semi-stable. We have a semi-stable model $\pi : \mathcal{A} \to \operatorname{Spec} \mathcal{O}_K$ of generic fiber A_K. Let $\varepsilon : \operatorname{Spec} \mathcal{O}_K \to \mathcal{A}$ be the zero section of π. We denote by $\Omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}$ the sheaf of first order differentials over $\mathcal{A}$, and by $\Omega^g_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K} = \det \Omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}$ its maximal exterior power. Define $\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}$ as the sheaf

$$\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K} := \varepsilon^\star \Omega^g_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}.$$

It is an invertible sheaf over $\operatorname{Spec} \mathcal{O}_K$ and for any embedding $\sigma : K \hookrightarrow \mathbb{C}$, the line bundle $\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K} \otimes_\sigma \mathbb{C} \cong H^0(\mathcal{A}_\sigma, \Omega^g_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K})$ can be given the following Hermitian structure:

$$\|s\|^2_{\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}, \sigma} = \frac{i^{g^2}}{2^g} \int_{\mathcal{A}_\sigma(\mathbb{C})} s \wedge \overline{s}, \quad \forall s \in H^0(\mathcal{A}_\sigma, \Omega^g_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}).$$

This gives a structure of Hermitian adelic vector bundle to $\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}$ over $\operatorname{Spec} \mathcal{O}_K$.

Definition 3.22. *The Faltings height $h_F(A)$ of A is the Arakelov degree of $\overline{\omega_{\mathcal{A}/\operatorname{Spec} \mathcal{O}_K}}$.*

Remark 3.23. *The Faltings height depends neither on the extension K/k, nor on the semi-stable model π.*

The Faltings height is not always positive, however Bost have proven the following lower bound for the Faltings height of an abelian variety.

Proposition 3.24 ([GR14b, Corollaire 8.4.])**.** *For any abelian variety A of dimension g over a number field, we have*

$$h_F(A) \geqslant -\frac{g}{2} \log(2\pi^2).$$

3.3.2 Moret-Bailly models

In order to apply the theory of Hermitian adelic vector bundle we exposed in section 3.1 to polarised abelian varieties defined over a number field, we need some integral structure associated to them. This was achieved by Moret-Bailly and Bost in [Mor85] and [Bos96a] thought the notion of Moret-Bailly models.

Definition 3.25. *Let (A, L) be a polarised abelian variety over a number field k, and let F be a finite subset of $A(\overline{k})$. A Moret-Bailly model $(\mathcal{A}, \overline{\mathcal{L}}, (\varepsilon_P)_{P\in F})$ of (A, L, F) over a number field K containing k is composed of*

- *a semi-stable group scheme $\pi : \mathcal{A} \to \operatorname{Spec} \mathcal{O}_K$ with generic fiber isomorphic to A_K;*
- *a Hermitian line bundle $\overline{\mathcal{L}}$ over $\mathcal{A}$ with generic fiber L_K, such that for any complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, the metric on $\mathcal{L} \otimes_\sigma \mathbb{C}$ coincides with the one coming from the Riemann form of $L \otimes_\sigma \mathbb{C}$;*
- *for any $P \in F$, a section $\varepsilon_P : \operatorname{Spec} \mathcal{O}_K \to \mathcal{A}$ of π, such that the corresponding geometric point $\varepsilon_{P,\overline{K}} \in \mathcal{A}\left(\overline{K}\right) \cong A\left(\overline{K}\right)$ coincides with P.*

The existence and properties of Moret-Bailly models have been studied by Bost in [Bos96a, §4.3]. We state his results.

Theorem 3.26 ([Bos96a, Theorem 4.10])**.** *Let (A, L) be a polarised abelian variety of dimension g over a number field k, and let F be a finite subset of $A(\overline{k})$.*

1. *There exists a finite extension K/k of k such that (A, L, F) admits a Moret-Bailly model over K.*
2. *For any Moret-Bailly model $(\mathcal{A}, \overline{\mathcal{L}}, (\varepsilon_P)_{P\in F})$ and any $P \in F$, the normalised height $\widehat{\deg}_{\mathrm{n}}\left(\overline{\varepsilon_P^\star \mathcal{L}}\right)$ coincide with the Néron–Tate height $\widehat{h}_L(P)$ of P.*
3. *If $(\mathcal{A}, \overline{\mathcal{L}}, (\varepsilon_P)_{P\in F})$ is a Moret-Bailly model of (A, L, F) over K, and K'/K is a finite extension of number fields, then $(\mathcal{A} \times_{\mathcal{O}_K} \mathcal{O}_{K'}, \overline{\mathcal{L} \times_{\mathcal{O}_K} \mathcal{O}_{K'}}, (\varepsilon_P \otimes_{\mathcal{O}_K} \mathcal{O}_{K'})_{P\in F})$ is a Moret-Bailly model of $(A_{K'}, L_{K'}, F)$ over K'. In other words, Moret-Bailly models are compatible with extension of scalars.*
4. *Let $(\mathcal{A}, \overline{\mathcal{L}}, (\varepsilon_P)_{P\in F})$ be a Moret-Bailly model of (A, L, F) over K. The space of global sections $H^0(A, L) \otimes_k K$ of (A_K, L_K) inherits a structure of Hermitian adelic vector bundle over $\operatorname{Spec} \mathcal{O}_K$ with $H^0(\mathcal{A}, \mathcal{L})$ as underlying space and the Hermitian structure coming from L as metrics at the Archimedean places of K. Its Arakelov slope is given by*

$$\widehat{\mu}\left(\overline{H^0(\mathcal{A}, \mathcal{L})}\right) = -\frac{1}{2} h_F(A) + \frac{1}{4} \log \mathrm{h}^0(A, L) - \frac{g}{4} \log(2\pi^2).$$

The existence of a Moret-Bailly model $(\mathcal{A}, \overline{\mathcal{L}}, \emptyset)$ over K of a polarised abelian variety $(A, L, \emptyset)$ also gives the tangent space t_{A_K} a structure of Hermitian adelic vector bundle over $\operatorname{Spec} \mathcal{O}_K$. Its underlying space is the tangent space at the origin $t_{\mathcal{A}}$ of $\mathcal{A}$ and the metrics at the Archimedean places are given by the metrics $\|\cdot\|_{L,\sigma}$. The Arakelov slope of $\overline{t_{\mathcal{A}}}$ has also been computed by Bost.

Proposition 3.27 ([Bos96b, Proposition D.1]). *Let (A, L) be a polarised abelian variety of dimension g over a number field k. Let $(\mathcal{A}, \overline{\mathcal{L}}, \emptyset)$ be a Moret-Bailly model of $(A, L, \emptyset)$ over K. The Arakelov slope of $\overline{t_{\mathcal{A}}}$ is equal to*

$$\widehat{\mu}\left(\overline{t_{\mathcal{A}}}\right) = -\frac{1}{g}\left(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A, L)\right).$$

To conclude on that topic, we give an estimation of the maximal slope of $\overline{t_{\mathcal{A}}}$ and $\overline{t^{\mathrm{v}}_{\mathcal{A}}}$ that has been computed by Gaudron.

Proposition 3.28 ([Gau19, Corollary 4.5 & p. 447]). *Let (A, L) be a polarised abelian variety of dimension g over a number field, and let $(\mathcal{A}, \overline{\mathcal{L}}, \emptyset)$ be Moret-Bailly model of $(A, L, \emptyset)$. We have*

$$\max\left(\widehat{\mu}_{\max}\left(\overline{t_{\mathcal{A}}}\right), 0\right) \leqslant 12 h_F(A) + 16 g \log(24g),$$

and

$$\widehat{\mu}_{\max}\left(\overline{t^{\mathrm{v}}_{\mathcal{A}}}\right) \leqslant (0.6g + 1)\left(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A, L)\right) + g^2 \log(10g).$$

3.4 Projective spaces

Besides abelian varieties, we will also deal with affine and projective spaces associated to a vector space or a module. Let us first recall how one can define an affine or projective scheme from a module.

Definition 3.29 ([Mum99, §4],[Har77, Proposition II.2.5]). *Let $\mathcal{E}$ be a module over a commutative ring R. We denote $\mathcal{E}^{\mathrm{v}} := \mathrm{Hom}_R(\mathcal{E}, R)$ the dual of $\mathcal{E}$.*

- *The affine group scheme $\mathbb{V}(\mathcal{E}^{\mathrm{v}})$ over $\operatorname{Spec} R$ associated to $\mathcal{E}$ is defined as*

$$\mathbb{V}(\mathcal{E}^{\mathrm{v}}) := \operatorname{Spec}\left(\operatorname{Sym} \mathcal{E}^{\mathrm{v}}\right).$$

  The scheme $\mathbb{V}(\mathcal{E}^{\mathrm{v}})$ represents the functor $S \mapsto \mathcal{E} \otimes_R S$.

- *The projective scheme $\mathbb{P}(\mathcal{E}^{\mathrm{v}})$ over $\operatorname{Spec} R$ associated to $\mathcal{E}$ is*

$$\mathbb{P}(\mathcal{E}^{\mathrm{v}}) := \operatorname{Proj}\left(\operatorname{Sym} \mathcal{E}^{\mathrm{v}}\right).$$

The Hermitian ample line bundles on projective spaces are very well known: they are the tensor powers of the canonical bundle $\mathcal{O}(1)$. We recall here a way to describe it.

Let R be a commutative ring and n be a positive integer. The tautological bundle $\mathcal{O}(-1)$ on $\mathbb{P}^n_R$ is defined as $\mathbb{A}^{n+1}_R \setminus \{0\}$ with the canonical map $(x_0, \dots, x_n) \mapsto [x_0 : \cdots : x_n]$. The fiber of a point $[x_0 : \cdots : x_n]$ is the line spanned by $(x_0, \dots, x_n)$. Taking the dual bundle, we get $\mathcal{O}(1)$.

Definition 3.30. *The line bundle $\mathcal{O}(1)$ on $\mathbb{P}^n_R$ is the dual of the tautological bundle $\mathcal{O}(-1)$. For a positive integer D, the line bundle $\mathcal{O}(D)$ is the D-th tensor power of $\mathcal{O}(1)$, that is $\mathcal{O}(D) := \mathcal{O}(1)^{\otimes D}$.*

The R-module of global sections $H^0(\mathbb{P}^n_R, \mathcal{O}(D))$ is isomorphic to the R-module of homogeneous polynomials $P \in R[X_0, \dots, X_n]$ of degree D.

Let k be a number field and write $\mathcal{O}_k$ its ring of integers. The line bundle $\mathcal{O}(-1)$ on $\mathbb{P}^n_{\mathcal{O}_k}$ has a natural structure of Hermitian adelic line bundle coming from the one of $\mathcal{O}_k^{n+1}$. Passing to the dual and the tensor power, we get such a structure on $\mathcal{O}(D)$. Let $\sigma : k \hookrightarrow \mathbb{C}$ be a complex embedding of k. For a section $s \in H^0(\mathbb{P}^n_k, \mathcal{O}(D))$ corresponding to a homogeneous polynomial $P \in k[X_0, \dots, X_n]$ of degree D, and a point $x := [x_0 : \cdots : x_n] \in \mathbb{P}^n_k$, the norm of $s(x)$ is given by

$$\|s(x)\|_{\mathrm{FS},\sigma} := \frac{|P(x_0, \dots, x_n)|_\sigma}{(|x_0|_\sigma^2 + \cdots + |x_n|_\sigma^2)^{D/2}}. \tag{3.2}$$

This is the so-called Fubini–Study metric of $\mathbb{P}^n_{k,\sigma}$. We can do the same construction for $\mathbb{E}$ with $\overline{\mathcal{E}}$ a general Hermitian adelic fiber bundle $\overline{\mathcal{E}}$ it comes with a Hermitian structure at the Archimedean places. We can then compute the Arakelov heights and slopes associated to this Hermitian adelic vector bundle structure. They are given in the following propositions.

Proposition 3.31 ([Bos91, 1.2. Degré arakelovien])**.** *Let k be a number field and let n be a positive integer. The height of a point $x := [x_0 : \cdots : x_n] \in \mathbb{P}^n_k$ relative to the line bundle $\mathcal{O}(1)$ is equal to*

$$h_{\mathcal{O}(1)}(x) = \frac{1}{2} \sum_{\sigma : k \hookrightarrow \mathbb{C}} \log \left(\sum_{i=0}^{n} |\sigma(x_i)|^2 \right) - \log \mathrm{Norm} \left(x_0 \mathcal{O}_k + \cdots + x_n \mathcal{O}_k \right),$$

where Norm *denotes the ideal norm on the group the fractional ideals of $\mathcal{O}_k$.*

Remark 3.32. *For $x := (x_1, \dots, x_n) \in k^n$, we denote by $h_{\mathcal{O}(1)}(x)$ the height of $[1 : x_1 : \cdots : x_n]$ relative to $\mathcal{O}(1)$. For any non-zero integer m and $x \in k^n$, we have*

$$h_{\mathrm{Weil}}(x) \leqslant h_{\mathcal{O}(1)}(x) \leqslant h_{\mathrm{Weil}}(x) + \frac{1}{2} \log(n+1) \quad \text{and} \quad h_{\mathcal{O}(1)}(mx) \leqslant h_{\mathcal{O}(1)}(x) + \log |m|,$$

where h_{Weil} the classical Weil logarithmic height on $\mathbb{P}^n_k$.

Proposition 3.33 ([Gau06, Proposition 4.2])**.** *Let D be a positive integer. Let k be a number field and let $\overline{\mathcal{E}}$ be a Hermitian adelic fiber bundle of dimension $N+1$ over* Spec $\mathcal{O}_k$*. The normalised Arakelov slope of $\overline{H^0(\mathbb{P}(\mathcal{E}), \mathcal{O}(D))}$ is equal to*

$$\widehat{\mu}\left(\overline{H^0(\mathbb{P}(\mathcal{E}), \mathcal{O}(D))}\right) = \frac{1}{2} \log \binom{N+D}{N} + D\widehat{\mu}(\overline{\mathcal{E}}) + \frac{1}{2} \log \gamma_{N,D},$$

where $\log \gamma_{N,D} := \frac{1}{\binom{N+D}{N}} \sum_{\substack{\tau \in \mathbb{N}^{N+1}, \\ |\tau| = D}} \log \frac{D!}{\tau_1! \cdots \tau_{N+1}!}$.

3.5 Comparison of norms

A compact complex variety with a Hermitian line bundle $(X, L, \|\cdot\|)$ is composed of the data of a compact complex variety X, together with line bundle L equipped for any $x \in X$ with a Hermitian norm $\|\cdot\|_x$ of the fiber L_x.

Given two compact complex varieties with a Hermitian line bundle $(X_1, L_1, \|\cdot\|_{X_1})$ and $(X_2, L_2, \|\cdot\|_{X_2})$, one can construct a new one $(X_1 \times X_2, L_1 \boxtimes L_2, \|\cdot\|_{X_1 \times X_2})$ in the following way.

The underlying variety is the product variety $X_1 \times X_2$. The line bundle one puts on $X_1 \times X_2$ is the external tensor product $L_1 \boxtimes L_2 := p_1^\star L_1 \otimes p_2^\star L_2$ (with p_i the projection $X_1 \times X_2 \to X_i$). For $(x_1, x_2) \in X_1 \times X_2$, the fiber $(L_1 \boxtimes L_2)_{(x_1,x_2)}$ is isomorphic to the tensor product of the fibers $(L_1)_{x_1} \otimes (L_2)_{x_2}$ which has a canonical Hermitian structure $\|\cdot\|_{X_1\times X_2}$ coming from the ones on $(L_1)_{x_1}$ and $(L_2)_{x_2}$. Notice that the group of global of $(X_1 \times X_2, L_1 \boxtimes L_2)$ is isomorphic to $H^0(X_1, L_1) \otimes H^0(X_2, L_2)$ by the Künneth formula (see [Kem93, Proposition 9.2.4]).

Let $(X, L, \|\cdot\|)$ be a compact complex variety with a Hermitian line bundle. We can define two metrics on the group of global sections $H^0(X, L)$ of (X, L). First, we have the sup norm given by

$$\forall s \in H^0(X, L), \quad \|s\|_\infty := \sup_{x\in X(\mathbb{C})} \|s(x)\|_x.$$

This is well-defined since X is compact. Next, the normalised measure $\mathrm{d}x$ on $X(\mathbb{C})$ induces a Hermitian metric on $H^0(X, L)$ given by

$$\forall s \in H^0(X, L), \quad \|s\|_2^2 := \int_{X(\mathbb{C})} \|s(x)\|_x^2 \mathrm{d}x.$$

We call this norm the L^2 norm on $H^0(X, L)$.

We would like to compare the sup norm and the L_2 norm for the compact complex varieties with a Hermitian line bundle we will be dealing with – namely (A, L) for a complex polarised abelian variety, and $(\mathbb{P}(E), \mathcal{O}(D))$ for a complex projective variety $\mathbb{P}(E)$. Let us define the ratio

$$R(X, L, \|\cdot\|) := \sup_{s\in H^0(X,L)\setminus\{0\}} \frac{\|s\|_\infty}{\|s\|_2}.$$

The following proposition shows that R is compatible with the notion of product defined above.

Proposition 3.34. *Let $(X_1, L_1, \|\cdot\|_{X_1})$, $(X_2, L_2, \|\cdot\|_{X_2})$ be two compact complex varieties with a Hermitian line bundle. We have*

$$R(X_1 \times X_2, L_1 \boxtimes L_2, \|\cdot\|_{X_1\times X_2}) = R(X_1, L_1, \|\cdot\|_{X_1}) R(X_2, L_2, \|\cdot\|_{X_2}).$$

Proof. Let us R, R_1, and R_2 for $R(X_1 \times X_2, L_1 \boxtimes L_2, \|\cdot\|_{X_1\times X_2})$, $R(X_1, L_1, \|\cdot\|_{X_1})$, and $R(X_2, L_2, \|\cdot\|_{X_2})$ respectively. For $(x_1, x_2) \in X_1 \times X_2$, we have

$$\|s_1(x_1)\|_{X_1,x_1}\|s_2(x_2)\|_{X_2,x_2} = \|(s_1 \otimes s_2)(x_1, x_2)\|_{X_1\times X_2,(x_1,x_2)} \leqslant R \cdot \|s_1 \otimes s_2\|_2 = R \cdot \|s_1\|_2\|s_2\|_2.$$

Taking the supremum over (x_1, x_2) we get $\|s_1\|_\infty\|s_2\|_\infty \leqslant R\cdot\|s_1\|_2\|s_2\|_2$ and therefore $R_1R_2 \leqslant R$.

Conversely, let $s \in H^0(X_1 \times X_2, L_1 \boxtimes L_2) \setminus \{0\}$. We can write $s = \sum_{i,j} s_{i,j} e_i \otimes f_j$ where $(e_i)_i$ and $(f_j)_j$ are orthonormal bases of $H^0(X_1, L_1)$ and $H^0(X_2, L_2)$. The L^2 norm of s is then equal to

$$\|s\|_2^2 = \sum_{i,j} |s_{i,j}|^2.$$

For any $(x_1, x_2) \in X_1 \times X_2$, we have

$$s(x_1, x_2) = \sum_{i,j} s_{i,j} e_i(x_1) \otimes f_j(x_2).$$

Let $e \in (L_1)_{x_1}$ be an element of norm 1. As $(L_1)_{x_1}$ is a one dimensional $\mathbb{C}$-vector space, for every i we can write $e_i(x_1) = \alpha_i e$ with $\alpha_i \in \mathbb{C}$ such that $|\alpha_i| = \|e_i(x_1)\|_{x_1}$. Therefore,

$$\begin{aligned}\|s(x_1,x_2)\|_{X_1\times X_2,(x_1,x_2)} &= \left\|e\otimes\sum_{i,j} s_{i,j}\alpha_i f_j(x_2)\right\|_{X_1\times X_2,(x_1,x_2)}\\ &= \left\|\sum_{i,j} s_{i,j}\alpha_i f_j(x_2)\right\|_{X_2,x_2}\\ &\leqslant R_2\left\|\sum_{i,j} s_{i,j}\alpha_i f_j\right\|_2.\end{aligned}$$

Notice now that $\left\|\sum_{i,j} s_{i,j}\alpha_i f_j\right\|_2^2 = \sum_j \left|\sum_i s_{i,j}\alpha_i\right|^2 = \sum_j \left\|\sum_i s_{i,j}e_i(x_1)\right\|_{X_1,x_1}^2$. We thus get

$$\|s(x_1,x_2)\|_{X_1\times X_2,(x_1,x_2)} \leqslant R_1R_2\sqrt{\sum_j\left\|\sum_i s_{i,j}e_i\right\|_2^2} \leqslant R_1R_2\sqrt{\sum_{i,j}|s_{i,j}|^2} = R_1R_2\|s\|_2.$$

Taking the supremum for $(x_1,x_2)\in X_1\times X_2$, we get the converse inequality $R\leqslant R_1R_2$. ■

We now state an upper-bound for $R(X,L,\|\cdot\|_X)$ in the two special cases we will be interested in: the case of complex polarised abelian varieties, and the case of complex projective spaces.

Proposition 3.35 ([Gau19, Theorem 3.2]). *Let (A,L) be a complex polarised abelian variety of dimension g. We have*

$$\sup_{s\in H^0(A,L)\setminus\{0\}}\frac{\|s\|_\infty}{\|s\|_2} \leqslant \mathrm{h}^0(A,L)^{1/2}\max\left(1,\frac{1}{\rho(A,L)}\right)^{g/2}(3.9g)^{g/2}.$$

Remark 3.36. *The constant 3.9 instead of the 5 in [Gau19, Theorem 3.2] is justified just before Remark 3.2.4 of [Gau19].*

Proposition 3.37 ([Gau06, Proposition 4.14]). *Let E be a complex vector space of dimension N, and let D be an integer. We have*

$$\sup_{s\in H^0(\mathbb{P}(E),\mathcal{O}(D))\setminus\{0\}}\frac{\|s\|_\infty}{\|s\|_2} = \binom{N+D-1}{N-1}^{1/2}.$$

3.6 Some combinatorial identities

To conclude this chapter, we prove here some combinatorial identities that will be useful in the rest of this part of the thesis.

For a tuple $\tau\in\mathbb{N}^n$, we will denote by

$$|\tau| := \tau_1+\cdots+\tau_n$$

the length of τ, and by

$$\tau! := \tau_1! \cdots \tau_n!,$$

the factorial of τ.

Lemma 3.38. *Let n, N_1 and N_2 be three non-negative integers. We have*

1. $\#\{\tau \in \mathbb{N}^n, |\tau| = N_1\} = \binom{N_1+n-1}{n-1}$;
2. $\#\{\tau \in \mathbb{N}^n, |\tau| \leqslant N_1\} = \binom{N_1+n}{n}$;
3. $\#\{\tau \in \mathbb{N}^n, |\tau| \leqslant N_1 \text{ and } \tau_n \leqslant N_2\} = \binom{N_1+n}{n} - \binom{N_1-N_2+n-1}{n}$.

Proof. 1. For any $N \geqslant 1$, let $S(N) := \{\tau \in \mathbb{N}^n, |\tau| = N\}$ and $S'(N) := \{\tau \in S(N), \tau_i \geqslant 1, \forall i\}$. The set $S'(N)$ is in one-to-one correspondence with the set of increasing maps from $\{1, \dots, n-1\}$ to $\{1, \dots, N-1\}$, a tuple τ corresponding to the map $i \mapsto \sum_{j=1}^{i} \tau_j$. This latter set has cardinality $\binom{N-1}{n-1}$.

   Notice now that $S(N)$ is in bijection with $S'(N+n)$ via the map $\tau \mapsto (\tau_i + 1)_i$. Applying the argument above with $N = N_3 + n$, allows us to conclude.

2. We have a bijection $\{\tau \in \mathbb{N}^n, |\tau| \leqslant N_1\} \to \left\{\tau' \in \mathbb{N}^{n+1}, |\tau'| = N_1\right\}$ sending τ to $(\tau, N_1 - |\tau|)$. The result then follows from the previous one.

3. We have a bijection between $\{\tau \in \mathbb{N}^n, |\tau| \leqslant N_1, \tau_n > N_2\}$ and $\{\tau \in \mathbb{N}^n, |\tau| \leqslant N_1 - N_2 - 1\}$ given by $\tau = (\tau', \tau_n) \mapsto (\tau', N_1 - |\tau|)$. The result then follows from the second one.

■

Lemma 3.39. *Let n, N_1, N_2 be three non-negative integers with $N_2 \leqslant N_1$. We have*

$$\binom{N_1+n}{n} - \binom{N_1-N_2+n-1}{n} \leqslant (N_2+1)(N_1+1)^{n-1}.$$

In particular with $N_2 = N_1$, we have $\binom{N_1+n}{n} \leqslant (N_1+1)^n$.

Proof. From lemma 3.38, the left-hand side is the cardinality of the set S of tuples $\tau \in \mathbb{N}^n$ such that $|\tau| \leqslant N_1$ and $\tau_n \leqslant N_2$. We have an injection of S into $\{0, \dots, N_1\}^{n-1} \times \{0, \dots, N_2\}$, and the result follows. ■

Chapter 4

The setup

4.1 Data

Let k be a number field of degree D over $\mathbb{Q}$. We fix an embedding $\sigma_0 : k \hookrightarrow \mathbb{C}$ of k into $\mathbb{C}$. Consider a polarised abelian variety (A, L) of dimension g, defined over k. Let p_A be a k-rational point of A and u_A a logarithm of p_A in $t_{A_{\sigma_0}}$, that is

$$\exp_{A_{\sigma_0}}(u_A) = p_A.$$

Let W_0 be a k-vector subspace of t_A of codimension $t \geqslant 1$ and define

$$G_0 := \mathbb{V}\left((t_A/W_0)^\vee\right)$$

the group scheme over $\operatorname{Spec} k$ associated to the vector space t_A/W_0 (see definition 3.29). Let p_0 be a k-rational point of G_0. We define the algebraic group G over k to be

$$G := G_0 \times_{\operatorname{Spec} k} A,$$

and we let $p := (p_0, p_A) \in G(k)$. The group $G_{\sigma_0}(\mathbb{C})$ has a structure of complex Lie group and an exponential map $\exp_{G_{\sigma_0}} = \mathrm{Id} \times \exp_{A_{\sigma_0}}$. Denote by $u := (u_0, u_A)$ the logarithm of p in $t_{G_{\sigma_0}(\mathbb{C})}$ coming from u_0 and u_A. Notice that the point u_0 correspond bijectively to the point p_0.

Consider the canonical projection $\lambda : t_A \to t_A/W_0$. We denote by W the graph of λ in $t_G = (t_A/W_0) \times t_A$, that is

$$W := \{(\lambda(x), x), x \in t_A)\} \subset t_G.$$

In order to consider ample line bundles attached to the group G, let $\overline{G}$ be the compactification of G defined by

$$\overline{G} := \operatorname{Proj} \operatorname{Sym}\left(k \oplus (t_A/W_0)^\vee\right) \times_{\operatorname{Spec} k} A = \mathbb{P}\left((k \oplus (t_A/W_0))^\vee\right) \times_{\operatorname{Spec} k} A.$$

We put the ample line bundle

$$M := \mathcal{O}(1) \boxtimes L$$

on $\overline{G}$.

For a complex embedding $\sigma : k \hookrightarrow \mathbb{C}$, we will denote by $\|\cdot\|_\sigma$ the Hermitian norm on t_{G_σ} defined as the Hermitian sum of the Fubini–Study metric on $t_{G_{0,\sigma}}$ induced by the quotient norm on t_A/W_0 and the one coming from L_σ on t_{A_σ}. For $x = (x_0, x_A) \in t_{G_\sigma}$ we have

$$\|x\|_\sigma^2 = \|x_0\|_{\mathrm{FS},\sigma}^2 + \|x_A\|_{L_\sigma}^2.$$

When there will be no ambiguity on the norm, we will also denote by $\|\cdot\|_\sigma$ the norms $\|\cdot\|_{\mathrm{FS},\sigma}$ and $\|\cdot\|_{L_\sigma}$.

Our goal is to find a lower-bound for the distance $d(u, W_{\sigma_0})$ in terms of the invariants of (A, L, p_A, u_A) on the one hand, and of (W_0, u_0) on the other hand. We group these invariants in three constants. Let $E \geqslant e$ be a real number. Define

$$\begin{aligned} \log a &:= \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|_{\sigma_0}^2 E^2}{D}\right), \quad \log b := \max\left(h_{\mathcal{O}(1)}(p_0), h(W_0)\right), \\ \text{and} \quad \mathfrak{a} &:= \left\lceil \frac{D}{\log E} \max\left(1, h_F(A), \log \mathrm{h}^0(A, L), \log \frac{D}{\log E}, \log\log a\right)\right\rceil, \end{aligned} \tag{4.1}$$

where $\lceil x \rceil$ denotes the ceiling of x. The numbers $\log a$ and $\log b$ measure the arithmetic complexity of the data relative to (p_A, u_A), and (p_0, W_0) respectively. The term $\mathfrak{a}$ considers the invariants related to (A, L). Beside these three quantities, another invariant related to A will naturally appear in the proofs and had already been considered in [GR14a]. Let y be the real number

$$y := \inf_{B \subsetneq A} \left(\frac{\deg_L B}{\deg_L A}\right)^{1/(\dim A - \dim B)},$$

where the infimum is taken over all the strict subvarieties B of A. It compares to the degree of (A, L) in the following way.

Proposition 4.1. *We have* $\dfrac{1}{\deg_L A} \leqslant y \leqslant \dfrac{1}{(\deg_L A)^{1/g}}$.

Proof. By definition of y we have

$$y \leqslant \left(\frac{\deg_L(0)}{\deg_L A}\right)^{1/(g-0)} = \frac{1}{(\deg_L A)^{1/g}}.$$

Moreover, we can bound from below $\deg_L B$ by 1 and then $\dfrac{1}{(\deg_L A)^{g-\dim B}}$ by $\dfrac{1}{\deg_L A}$. ∎

During the proof we will need a technical hypothesis on A and u_A in order to obtain our first result. From now on and until section 7.2, we assume the following.

Hypothesis 4.2. *For all embeddings $\sigma : \overline{k} \hookrightarrow \mathbb{C}$ dividing σ_0, and all strict abelian subvarieties B of A_σ, the tangent space of B_σ does not contain u_A.*

Under hypothesis 4.2 our result is the following.

Theorem 4.3. *Assume hypothesis 4.2. Then, we have*

$$\begin{aligned} \log d(u, W_{\sigma_0}) \geqslant -(5(g+t))^{\frac{4(g+t+1)^2}{t}} \mathfrak{a}^{1/t} \left(1 + \frac{D\mathfrak{a}\log a}{\log E}\right)^{g/t} \\ \times (\mathfrak{a}\log E + D\log b) \frac{1}{y^{1+g/t}(\deg_L A)^{1/t}}. \end{aligned}$$

Remark 4.4. *Notice that theorem 1.5 follows indeed from theorem 4.3 by taking* $E = \mathrm{e}$, $u_0 = 0$, *and bounding* $y^{-1-g/t}(\deg_L A)^{-1/t}$ *by* $(\deg_L A)^g$ *using proposition 4.1.*

This result compares to [Gau06, Corollaire 3.2] (taking $B = \{0\}$ in their result). Besides the better constant of g and t, our hypothesis 4.2 is weaker than their hypotheses (**1**) and (**2**).

Remark 4.5. *Hypothesis 4.2 implies that* u *does not lie in* W_{σ_0} *as a consequence of Wüstholz' analytic subgroup theorem 1.4. Indeed, if* $u \in W_{\sigma_0}$, *then there exists a connected algebraic subgroup* $\widetilde{G}$ *of* $G_{\overline{k}}$ *such that* $u \in t_{\widetilde{G}}(\mathbb{C}) \subseteq W_{\sigma_0}$. *We can decompose* $\widetilde{G}$ *as* $H_0 \times_{\operatorname{Spec}\overline{\mathbb{Q}}} B$ *with* H_0 *a subgroup of* G_0 *and* B *an abelian subvariety of* A. *We then get* $u_A \in t_B$ *and therefore* $B = A$ *because of hypothesis 4.2. It follows that* $t_{\widetilde{G}}(\mathbb{C}) = t_{H_0}(\mathbb{C}) \times t_A(\mathbb{C}) \subseteq W_{\sigma_0}$, *which is impossible.*

Once theorem 4.3 is proved, we shall reduce hypothesis 4.2 to the weakest hypothesis possible, namely that u_A does not belong to W_{0,σ_0}. This will be our second main result.

Theorem 4.6. *Let* A' *be the smallest abelian subvariety of* A_{σ_0} *such that* $u_A \in t_{A',\sigma_0}$. *Assume that* $u_A \notin W_{0,\sigma_0}$ *and that* $u_0 \in (t_{A'} + W_0)/W_0$. *Write*

$$M_A := \max\left(1, \log D, h_F(A), \log^+ \widehat{h}_L(p_A), \log \frac{\|u_A\|_{\sigma_0}^2}{D}\right),$$

and $\log b := \max\left(h_{\mathcal{O}(1)}(p_0), h(W_0)\right)$.

Let σ *be a place of* $\overline{k}$ *above* σ_0. *If* $g \geqslant 2$, *we have*

$$\log d(u, W_\sigma) \geqslant -(265000g)^{4g^3} D^{(2g+1)(g+1)} \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|_{\sigma_0}^2}{D}\right)^{g^2+g} M_A^{(g+1)^2} \max(M_A, \log b).$$

If $g = 1$, *we have*

$$\log d(u, W_\sigma) = \|u_0 - u_A\|_\sigma \geqslant -2 \cdot 10^{39} D^3 M_A^2 \max(M_A, h_{\mathcal{O}(1)}(p_0)) \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|_\sigma^2}{D}\right).$$

Remark 4.7. *We deduce theorem 1.6 from theorem 4.6 by taking* $u_0 = 0$.

The main achievement of this result is the absence of any supplementary hypothesis on the logarithm u_A. It is to our knowledge the first result of this kind.

4.2 Overview of the proof

We will now begin the proof of theorem 4.3. Let us describe its main steps and the tools we will be using. Our proof is an application of Baker's method, using the technique of the auxiliary section.

In a first time, we modify slightly our data in order to control the parameters of the problem. This is the use of the quantities D_0 and D_1 defined below in section 4.3. We then make use of a Siegel lemma due to Gaudron [Gau14, Lemme de Siegel approché absolu, p.24] in order to construct a section s of small height, and small derivatives at the multiples of the point p (see chapter 5). The choice of our constants, combined with a multiplicity lemma due to Nakamaye [Nak07, Theorem 1] ensure that the jet of the section s does not vanish at a controlled order and

at a controlled multiple of p. We then estimate the norm of this jet at every Archimedean and non-Archimedean place in chapter 6. The non-Archimedean estimates make use of a theorem of Gaudron based on Chudnovsky's change of variables [Gau06, Proposition 5.10]. The Archimedean estimates are split between the places that lie above σ_0, and the ones that do not. For the second ones, we use only elementary analysis. For the first ones, we make use of an interpolation lemma developed by Bosser and Gaudron [BG19, Proposition 2.1]. This is where the distance from u to W_σ appear, and is the most delicate part of the proof. Finally, in the last chapter 7 we combine all these estimates with the Siegel lemma of chapter 5, and an estimation of the maximal slope of the adelic bundle of jets to finally get our lower-bound for the distance.

4.3 Parameters

Let

$$C_0 = (5(g+t))^3 \quad \text{and} \quad C_1 = (5(g+t))^{2g+t}. \tag{4.2}$$

We define two real numbers $\widetilde{S}$ and $\widetilde{S}_1$ by

$$2\widetilde{S}+1 := C_0\mathfrak{a} \quad \text{and} \quad 2\widetilde{S}_1+1 := C_1(2\widetilde{S}+1) = C_0C_1\mathfrak{a}, \tag{4.3}$$

and $S := \lfloor \widetilde{S} \rfloor$, and $S_1 = \lfloor \widetilde{S}_1 \rfloor$. Let $\widetilde{T}_1$ be a positive real number. We put

$$\begin{aligned} \widetilde{D}_0 &:= \frac{y\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0\left((2\widetilde{S}_1+1)\log E + D(\log \widetilde{S}_1 + \log b)\right)} = \frac{y\widetilde{T}_1}{C_0C_1}\left(1+\frac{D(\log \widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E}\right)^{-1} \\ \text{and } \widetilde{D}_1 &:= \frac{y\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0\left((2\widetilde{S}_1+1)\log E + D\widetilde{S}_1^2\log a\right)} = \frac{y\widetilde{T}_1}{C_0C_1}\left(1+\frac{D\widetilde{S}_1^2\log a}{(2\widetilde{S}_1+1)\log E}\right)^{-1}. \end{aligned} \tag{4.4}$$

Remark 4.8. *These parameters will be used to control the quantities that will arise during the proofs and their shape has been motivated for that purpose. All the numbers with a capital T will represent some order of derivation, the numbers with a capital S, some number of multiples of our point p, and the numbers D_0 and D_1, some power of the line bundles $\mathcal{O}(1)$ and L.*

Let H be a connected subgroup scheme of G defined over $\overline{k}$. It decomposes as $H_0 \times_{\operatorname{Spec}\overline{k}} B$, where H_0 is a subgroup scheme of G_0 (in fact the group scheme associated to some vector subspace of $t_A/W_0 \otimes \overline{k}$), and B is an abelian subvariety of A, both defined over $\overline{k}$. Let g' be the dimension of B, t' be the dimension of H_0, and put $c_W(H) := \operatorname{codim}_{W_{\overline{k}}}(W_{\overline{k}} \cap t_H)$.

Lemma 4.9. *One has an exact sequence of vector spaces*

$$0 \longrightarrow \frac{W_{\overline{k}}}{t_H \cap W_{\overline{k}}} \xrightarrow{f} \frac{t_{G_{\overline{k}}}}{t_H} \xrightarrow{g} \frac{t_{G_{0,\overline{k}}}}{t_{H_0}+\lambda(t_B)} \longrightarrow 0$$

where $f(w+t_H\cap W_{\overline{k}}) = w+t_H$ and $g((x_0,x_A)+t_H) = x_0-\lambda(x_A)+(t_{H_0}+\lambda(t_B)$.

Proof. It is clear that f is injective, g is surjective, and that $\mathrm{Im}(f) \subseteq \ker(g)$. Let $(x_0, x_A) + t_H$ be in the kernel of g. This means that $x_0 - \lambda(x_A) \in t_{H_0} + \lambda(t_B)$. Therefore, there exist $y_0 \in t_{H_0}$ and $x_B \in t_B$ such that $x_0 = y_0 + \lambda(x_A + x_B)$, and thus

$$(x_0, x_A) + t_H = (\lambda(x_A + x_B), x_A + x_B) + t_H \in W_{\overline{k}} + t_H = \mathrm{Im}(f).$$

■

Corollary 4.10. *We have* $\max(g - g', t - t') \leqslant c_W(H) \leqslant g + t - (g' + t') = \mathrm{codim}_{G_{\overline{k}}}(H)$.

Moreover, if $W_{\overline{k}} + t_H = t_G$, *then* $c_W(H) = \mathrm{codim}_{G_{\overline{k}}} H$, *and if* $W_{\overline{k}} + t_H \neq t_G$, *then* $t - t' > 0$ *and* $g - g' > 0$.

Proof. From lemma 4.9 we have

$$c_W(H) = \mathrm{codim}_{G_{\overline{k}}} H - \dim\left(t_{G_{0,\overline{k}}}/(t_{H_0} + \lambda(t_B))\right).$$

Therefore, $c_W(H) \leqslant \dim G - \dim H = (g + t) - (g' + t')$. Moreover, from the surjections $t_{A_{\overline{k}}}/t_B \to t_{G_{0,\overline{k}}}/(t_{H_0} + \lambda(t_B))$, and $t_{G_{0,\overline{k}}}/t_{H_0} \to t_{G_{0,\overline{k}}}/(t_{H_0} + \lambda(t_B))$ it follows that

$$\dim\left(t_{G_{0,\overline{k}}}/(t_{H_0} + \lambda(t_B))\right) \leqslant \min(g - g', t - t').$$

For the second part of the corollary, notice that we have an isomorphism $W_{\overline{k}}/(t_H \cap W_{\overline{k}}) \cong (W_{\overline{k}} + t_H)/t_H$. Therefore, if $W_{\overline{k}} + t_H = t_{G_{\overline{k}}}$ then $W_{\overline{k}}/(t_H \cap W_{\overline{k}}) \cong t_{G_{\overline{k}}}/t_H$ and we have $c_W(H) = \mathrm{codim}_{G_{\overline{k}}}(H)$. Moreover, from lemma 4.9 we have $W_{\overline{k}} + t_H = t_{G_{\overline{k}}}$ if and only if $t_{G_{0,\overline{k}}} = t_{H_0} + \lambda(t_B)$. In particular, this is satisfied if either $t_{A_{\overline{k}}} = t_B$, or $t_{G_{0,\overline{k}}} = t_{H_0}$. ■

Corollary 4.10 implies that under the assumption $W_{\overline{k}} + t_H \neq t_{G_{\overline{k}}}$ we have $t - t' > 0$, and we can define

$$x(H) := \left(\#\left(\frac{\Gamma_p(S_1) + H}{H}\right) \frac{\widetilde{T}_1^{c_W(H)}}{2^g} \frac{\binom{g'+t'}{g'} \widetilde{D}_0^{t'} \widetilde{D}_1^{g'} \deg_L B}{\binom{g+t}{g} \widetilde{D}_0^{t} \widetilde{D}_1^{g} \deg_L A}\right)^{1/(t-t')}, \tag{4.5}$$

where $\Gamma_p(S_1) := \{np, -S_1 \leqslant n \leqslant S_1\}$.

Remark 4.11. *For two positive integers* n_0, n_1, *the degree of* H *relative to the line bundle* $\mathcal{O}(n_0) \boxtimes L^{\otimes n_1}$ *is equal to* $\binom{g'+t'}{g'} n_0^{t'} n_1^{g'} \deg_L B$. *As the parameters* $\widetilde{D}_0$ *and* $\widetilde{D}_1$ *are not integers in general, the term* $\frac{\binom{g'+t'}{g'} \widetilde{D}_0^{t'} \widetilde{D}_1^{g'} \deg_L B}{\binom{g+t}{g} \widetilde{D}_0^{t} \widetilde{D}_1^{g} \deg_L A}$ *that appear in the definition of* $x(H)$ *interpolates* $\frac{\deg_{\mathcal{O}(n_0) \boxtimes L^{\otimes n_1}} H}{\deg_{\mathcal{O}(n_0) \boxtimes L^{\otimes n_1}} G}$ *for non-integer values of* n_0 *and* n_1.

Remark 4.12. *The somewhat complicated shape of* $x(H)$ *will be motivated by the upcoming lemma 4.16. It will allow us to get rid of some subgroup of* G *that will measure the obstruction of sections to vanish up to a certain order.*

From the definition of $\widetilde{D}_0$ and $\widetilde{D}_1$, the quantity $\widetilde{T}_1^{(\mathrm{codim}_G(H) - c_W(H))/(t-t')} x(H)$ is independent of $\widetilde{T}_1$. We can therefore fix $\widetilde{T}_1$ such that $x(\{0\})$ is equal to 1. Notice indeed that we have

$W + t_{\{0\}} = W \neq t_G$, and that $x(\{0\})$ is thus well-defined. From the definition of $\widetilde{D}_0$, $\widetilde{D}_1$ and S_1, we have

$$\widetilde{T}_1 = \left(\frac{\#\Gamma_p(S_1)(C_0C_1)^{g+t}\left(1+\frac{\widetilde{S}_1^2 D\log a}{(2\widetilde{S}_1+1)\log E}\right)^g\left(1+\frac{D(\log \widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E}\right)^t}{2^g\binom{g+t}{g} y^{g+t}\deg_L A} \right)^{1/t}. \tag{4.6}$$

Let x be the infimum of the $x(H)$'s over all the subgroups H satisfying $W_{\overline{k}} + t_H \neq t_{G_{\overline{k}}}$, and fix a subgroup H satisfying $x(H) = x$. This is well-defined because $x(H)$ takes values in a finite set. From the definition of $\widetilde{T}_1$ we moreover have $x \leqslant x(\{0\}) = 1$. Along the proof we will need to distinguish two different cases depending on the cardinality of the group $\frac{\Gamma_p(S_1)+H}{H}$.

Definition 4.13. *We say that we are in the periodic case if $\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)$ is not maximal, that is less than $2S_1+1$. Otherwise, we say that we are in the non-periodic case.*

We finally define

$$\begin{aligned} T_1 &:= \lfloor \widetilde{T}_1 \rfloor, \quad T_0 := 2(g+t)T_1 - 1, \quad T_2 := \begin{cases} \left\lfloor \frac{\widetilde{T}_1}{C_1} \right\rfloor & \text{in the periodic case;} \\ T_0 & \text{in the non-periodic case,} \end{cases} \\ D_0 &:= \lfloor x\widetilde{D}_0 \rfloor, \quad D_1 := \lfloor \widetilde{D}_1 \rfloor, \quad S_0 := \begin{cases} (g+t)S_1 & \text{in the periodic case;} \\ S & \text{in the non-periodic case,} \end{cases} \end{aligned} \tag{4.7}$$

and we equip $\overline{G}$ with the line bundle $M(D_0, D_1) := \mathcal{O}(D_0) \boxtimes L^{\otimes D_1}$.

The following proposition contains a lot of inequalities we will be using constantly in the rest of the part. The proof is quite technical and uses intensively the definition (4.2), (4.3), (4.4), (4.5), (4.6), and (4.7).

Proposition 4.14. *The following inequalities hold.*

1. $\widetilde{T}_1 \geqslant (2(g+t))^{4g+2t+6} \geqslant 10^7$ *and* $T_2 \geqslant 1$;
2. $\widetilde{D}_0, \widetilde{D}_1 \leqslant \dfrac{y\widetilde{T}_1}{C_0C_1} \leqslant \dfrac{\widetilde{T}_1}{C_0C_1}$;
3. $D_1 \geqslant (2(g+t))^{2g+t+3}$ *and* $D_0 \geqslant (2(g+t))^3$;
4. $\dfrac{(2\widetilde{S}+1)\log E}{DC_0} \geqslant \max\left(1, \dfrac{\log E}{D}, h_F(A), \log \mathrm{h}^0(A,L), \log\dfrac{D}{\log E}, \log\log a, \log\|u_A\|_{\sigma_0}\right)$;
5. $\log \mathfrak{a} \leqslant \dfrac{2(2\widetilde{S}+1)\log E}{DC_0}$;
6. $\left(1+\|ES_1\lambda(u_A)\|_{\sigma_0}^2\right)^{D_0/2} \leqslant \exp\left(1.01\cdot\dfrac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\right)$;
7. $\log\widetilde{D}_0 \leqslant \dfrac{(2\widetilde{S}+1)\log E}{DC_0} \times \frac{7(g+t)^3}{t}$.

Proof. 1. For the lower bound of $\widetilde{T}_1$, we use its value (4.6). The quantities

$$1+\frac{\widetilde{S}_1^2 D\log a}{(2\widetilde{S}_1+1)\log E},\quad 1+\frac{D(\log\widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E},\quad \text{and}\quad \#\Gamma_p(S_1)$$

are bigger than or equal to 1. As a consequence

$$\widetilde{T}_1 \geqslant \left(\frac{(C_0C_1)^{g+t}}{2^g\binom{g+t}{g}y^{g+t}\deg_L A}\right)^{1/t}.$$

From proposition 4.1, we have $\frac{1}{y^{g+t}\deg_L A}\geqslant(\deg_L A)^{t/g}\geqslant 1$, and therefore

$$\widetilde{T}_1 \geqslant \left(\frac{(C_0C_1)^{g+t}}{2^g\binom{g+t}{g}}\right)^{1/t} \geqslant \left(\frac{(5(g+t))^{(g+t)(2g+t+3)}}{2^{2g+t}}\right)^{1/t} \geqslant (2(g+t))^{2(2g+t+3)}.$$

For the lower bound of T_2 we have $T_2\geqslant\left\lfloor\frac{\widetilde{T}_1}{C_1}\right\rfloor$. The previous lower for $\widetilde{T}_1$ being greater than the value of C_1, it leads to the wanted bound.

2. This is straightforward from the definition (4.4) of $\widetilde{D}_0$ and $\widetilde{D}_1$.

3. From the value (4.6) of $\widetilde{T}_1$ and the definition (4.4) of $\widetilde{D}_1$, we have

$$\widetilde{D}_1 = \left(\frac{\#\Gamma_p(S_1)(C_0C_1)^g\left(1+\frac{\widetilde{S}_1^2D\log a}{(2\widetilde{S}_1+1)\log E}\right)^{g-t}\left(1+\frac{D(\log\widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E}\right)^{t}}{2^g\binom{g+t}{t}y^g\deg_L A}\right)^{1/t}.$$

From proposition 4.1, we have $y^g\deg_L A\leqslant 1$. Bounding again

$$1+\frac{\widetilde{S}_1^2 D\log a}{(2\widetilde{S}_1+1)\log E},\quad 1+\frac{D(\log\widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E},\quad \text{and}\quad \#\Gamma_p(S_1)$$

by 1 leads to

$$\widetilde{D}_1 \geqslant \left(\frac{(C_0C_1)^g}{2^g\binom{g+t}{t}}\right)^{1/t} \geqslant \left(\frac{(5(g+t))^{g(2g+t+3)}}{2^{2g+t}}\right)^{1/t} \geqslant (2(g+t))^{2g+t+3}.$$

For the bound for D_0, let us compute the value of $x\widetilde{D}_0$:

$$\begin{aligned} x\widetilde{D}_0 &= \widetilde{D}_0\left(\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)\frac{\widetilde{T}_1^{c_W(H)}}{2^g}\frac{\binom{g'+t'}{g'}\widetilde{D}_0^{t'}\widetilde{D}_1^{g'}\deg_L B}{\binom{g+t}{g}\widetilde{D}_0^{t}\widetilde{D}_1^{g}\deg_L A}\right)^{1/(t-t')} \\ &= \left(\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)\frac{\widetilde{T}_1^{c_W(H)}}{\widetilde{D}_1^{g-g'}}\frac{\deg_L B}{\deg_L A}\frac{\binom{g'+t'}{g'}}{2^g\binom{g+t}{g}}\right)^{1/(t-t')}. \end{aligned}$$

We can bound from below the cardinality of $\frac{\Gamma_p(S_1)+H}{H}$ and $\binom{g'+t'}{g'}$ by 1. Furthermore, from the definition of y, we have $\frac{\deg_L B}{\deg_L A}\geqslant y^{g-g'}$. Therefore,

$$x\widetilde{D}_0 \geqslant \left(\frac{\widetilde{T}_1^{c_W(H)}y^{g-g'}}{\widetilde{D}_1^{g-g'}2^g\binom{g+t}{g}}\right)^{1/(t-t')} \geqslant \left(\frac{\widetilde{T}_1^{c_W(H)}y^{g-g'}}{\widetilde{D}_1^{g-g'}2^{2g+t}}\right)^{1/(t-t')}.$$

To conclude, from corollary 4.10 we have $c_W(H) \geqslant g - g' \geqslant 1$. Because $\widetilde{T}_1$ is greater than 1 we deduce that $\widetilde{T}_1^{c_W(H)} \geqslant \widetilde{T}_1^{g-g'}$. Using proposition 4.14.2 and the values of C_0 and C_1, we finally get

$$x\widetilde{D}_0 \geqslant \left(\frac{\widetilde{T}_1^{g-g'} y^{g-g'}}{\widetilde{D}_1^{g-g'} 2^{2g+t}}\right)^{1/(t-t')} \geqslant \left(\frac{(C_0C_1)^{g-g'}}{2^{2g+t}}\right)^{1/(t-t')} \geqslant \left(\frac{C_0C_1}{2^{2g+t}}\right)^{1/t} \geqslant (2(g+t))^3.$$

Applying the floor function on both sides gives $D_0 \geqslant (2(g+t))^3$.

4. From (4.1), we have

$$\mathfrak{a} \geqslant \max\left(1, \frac{D}{\log E} \max\left(1, h_F(A), \log \mathrm{h}^0(A, L), \log \frac{D}{\log E}, \log\log a\right)\right).$$

The announced lower bound for $\frac{(2\widetilde{S}+1)\log E}{DC_0} = \frac{\mathfrak{a}\log E}{D}$ is then clear except maybe for

$$\frac{(2\widetilde{S}+1)\log E}{DC_0} \geqslant \log \|u_A\|_{\sigma_0}.$$

On the one hand, from the value of $\log a$, we have $\frac{(2\widetilde{S}+1)\log E}{C_0 D} \geqslant \log \frac{\|u_A\|_{\sigma_0}^2 E^2}{D}$. On the other hand we have $\frac{(2\widetilde{S}+1)\log E}{C_0 D} \geqslant \log \frac{D}{\log E}$. Therefore,

$$\log \|u_A\|_{\sigma_0} = \frac{1}{2}\left(\log \frac{\|u_A\|_{\sigma_0}^2 E^2}{D} + \log \frac{D}{E^2}\right) \leqslant \frac{1}{2}\left(\frac{(2\widetilde{S}+1)\log E}{DC_0} + \frac{(2\widetilde{S}+1)\log E}{DC_0}\right).$$

5. We have $\frac{\mathfrak{a}\log E}{D} \geqslant \log \frac{D}{\log E}$, and therefore

$$\log \mathfrak{a} = \log \frac{\mathfrak{a}\log E}{D} + \log \frac{D}{\log E} \leqslant \frac{2\mathfrak{a}\log E}{D} = \frac{2(2\widetilde{S}+1)\log E}{DC_0}.$$

6. We have

$$\left(1 + \|ES_1\lambda(u_A)\|_{\sigma_0}^2\right)^{D_0/2} \leqslant \exp\left(D_0 \log^+ \|u_A\|_{\sigma_0} + D_0 \log E + D_0 \log S_1 + \frac{D_0}{2}\log(2)\right).$$

Using the previous estimates, we can bound D_0 by $\frac{\widetilde{T}_1}{C_0C_1}$, $\log^+ \|u_A\|_{\sigma_0}$, $\log E$, and 1 by $\frac{(2\widetilde{S}+1)\log E}{C_0}$, and $D_0 \log S_1$ by $\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}$ to get

$$\left(1 + \|ES_1\lambda(u_A)\|_{\sigma}^2\right)^{D_0/2} \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \left(\frac{2}{C_0C_1} + 1 + \frac{\log(2)}{2C_0C_1}\right)\right).$$

From the values of C_0 and C_1 we deduce the result.

7. From the values (4.4) and (4.6) of $\widetilde{D}_0$ and $\widetilde{T}_1$, we have

$$\widetilde{D}_0 = \left(\frac{\#\Gamma_p(S_1)(C_0C_1)^g\left(1 + \frac{\widetilde{S}_1^2 D}{(2\widetilde{S}_1+1)\log E}\log a\right)^g}{2^g\binom{g+t}{g} y^g \deg_L A}\right)^{1/t}.$$

As $\#\Gamma_p(S_1)$ is less than $C_0C_1\mathfrak{a}$, and $\frac{\widetilde{S}_1^2}{2\widetilde{S}_1+1}$ is bounded by $\frac{\widetilde{S}_1}{2} \leqslant \frac{C_0C_1\mathfrak{a}}{2}$, we have

$$\widetilde{D}_0 \leqslant \left(\frac{(C_0C_1)^{2g+1}}{2^{2g}\binom{g+t}{g}}\right)^{1/t} \left(1+\frac{D\log a}{\log E}\right)^{g/t} \frac{\mathfrak{a}^{(g+1)/t}}{(y^g \deg_L A)^{1/t}}.$$

To bound $\log \widetilde{D}_0$, we need to bound the logarithm of each term. Because $\log^+ \log a$, $\log^+ \frac{D}{\log E}$, and $\log 2$ are bounded by $\frac{(2\widetilde{S}+1)\log E}{DC_0}$, we have

$$\frac{g}{t}\log\left(1+\frac{D\log a}{\log E}\right) \leqslant \frac{g}{t}\left(\log^+\log a + \log^+\frac{D}{\log E} + \log 2\right) \leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0} \times \frac{3g}{t}.$$

To bound $\frac{g+1}{t}\log\mathfrak{a}$, we use the point 5 of the proof:

$$\frac{g+1}{t}\log\mathfrak{a} \leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0} \times \frac{2(g+1)}{t}.$$

Finally, because $y\deg_L A \geqslant 1$, we have $\frac{1}{y^g \deg_L A} \leqslant (\deg_L A)^{g-1}$. Hence,

$$\begin{aligned}\log\frac{1}{(y^g\deg_L A)^{1/t}} \leqslant \frac{g-1}{t}\log\deg_L A = \frac{g-1}{t}\log(g!) + \frac{g-1}{t}\log \mathrm{h}^0(A,L)\\ \leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0}\left(\frac{(g-1)^2}{t}\log g + \frac{g-1}{t}\right).\end{aligned}$$

We deduce that $\log\widetilde{D}_0$ is bounded by $c(g,t)\frac{(2\widetilde{S}+1)\log E}{DC_0}$, with

$$c(g,t) = \frac{1}{t}\log\left(\frac{(C_0C_1)^{2g+1}}{2^{2g}\binom{g+t}{g}}\right) + \frac{3g}{t} + \frac{2(g+1)}{t} + \frac{(g-1)^2}{t}\log g + \frac{g-1}{t}.$$

Recall that we have $C_0C_1 = (5(g+t))^{2g+t+3}$. Therefore, we get

$$\begin{aligned}\frac{tc(g,t)}{(g+t)^3} &\leqslant \frac{(2g+1)(2g+t+3)\log(5(g+t))}{(g+t)^3} + \frac{6g+1}{(g+t)^3} + \frac{(g-1)^2\log(g)}{(g+t)^3}\\ &\leqslant \underbrace{\frac{(2g+1)(2g+4)\log(5(g+1))}{(g+1)^3}}_{\leqslant\frac{3\cdot 6\cdot\log(10)}{8}} + \underbrace{\frac{6g+1}{(g+1)^3}}_{\leqslant\frac{7}{8}} + \underbrace{\frac{(g-1)^2\log(g)}{(g+1)^3}}_{\leqslant 0.5}\\ &\leqslant 7.\end{aligned}$$

We conclude that $\log\widetilde{D}_0 \leqslant \frac{7(g+t)^3}{t} \times \frac{(2\widetilde{S}+1)\log E}{DC_0}$.

■

Remark 4.15. *The inequalities 4.14.3 ensure that the line bundle $M(D_0,D_1)$ is in fact ample.*

Before we switch to the actual heart of the proof, we state a result that will ensure that the global sections of $(\overline{G}, M(D_0,D_1))$ will not vanish too many along W at some multiples of p. Such statement is known as a multiplicity lemma.

Lemma 4.16 (multiplicity lemma)**.** *Let $s \in H^0(\overline{G}, M(D_0, D_1)) \otimes \overline{k}$. If s_{σ_0} vanishes to order at least $(g+t)T_1 + 1$ at $\Gamma_p((g+t)S_1)$ along W_{σ_0}, then $s = 0$.*

In order to prove lemma 4.16 we use the following theorem of Nakamaye.

Theorem 4.17 ([Nak07, Theorem 1])**.** *Let G be a complex algebraic commutative group of dimension d. Let $\mathcal{L}$ be an ample line bundle on $\overline{G}$. Let $\Lambda \subseteq t_G$ be a non-zero vector subspace of the tangent space of G. Assume $T, S \geqslant 1$, let $0 \neq \sigma \in H^0(\overline{G}, \mathcal{L})$, and $p \in G(\mathbb{C})$. If σ vanishes at order at least $dT + 1$ along Λ at $\Gamma_p(dS)$, then there exists a proper connected subgroup G' of G such that*

$$T^{c_\Lambda(G')} \# \left(\frac{\Gamma_p(S) + G'}{G'} \right) \deg_{\mathcal{L}}(\overline{G'}) \leqslant \deg_{\mathcal{L}}(\overline{G}).$$

Proof of lemma 4.16. Let $s \in H^0(\overline{G}, M(D_0, D_1)) \otimes \overline{k}$ be non-zero and assume by contradiction that s_{σ_0} vanishes at order at least $(g+t)T_1 + 1$ at $\Gamma_p((g+t)S_1)$ along W_{σ_0}. From theorem 4.17, there exists a proper connected subgroup G'_{σ_0} of G_{σ_0} such that

$$T_1^{c_W(G'_{\sigma_0})} \# \left(\frac{\Gamma_p(S_1) + G'_{\sigma_0}}{G'_{\sigma_0}} \right) \deg_{M(D_0,D_1)_{\sigma_0}}(\overline{G'_{\sigma_0}}) \leqslant \deg_{M(D_0,D_1)_{\sigma_0}}(\overline{G_{\sigma_0}}). \tag{4.8}$$

The subgroup G'_{σ_0} comes from a subgroup G' defined on $\overline{k}$ and G' splits into $G'_0 \times_{\mathrm{Spec}_{\overline{k}}} C$ with G'_0 a subgroup scheme of G_0 of dimension t'' and C an abelian subvariety of A of dimension g''. We consider two possible cases:

1. If $t_{G'} + W_{\overline{k}} \neq t_{G_{\overline{k}}}$, then by the very definition of x, we have $x(G') \geqslant x$. We can express the degree of $\overline{G'}$ relative to the ample line bundle $M(D_0, D_1)_{\overline{k}}$ in terms of $\deg_L(C)$:

$$\begin{aligned}
\deg_{M(D_0,D_1)}(\overline{G'}) &= \dim(G')! \times \frac{\deg_{M(D_0,D_1)}(\overline{G'_0} \times_{\mathrm{Spec}_{\overline{k}}} C)}{\dim(G')!} \\
&= \dim(G')! \times \frac{\deg_{\mathcal{O}(D_0)}(\overline{G'_0})}{\dim(G'_0)!} \times \frac{\deg_{L^{\otimes D_1}}(C)}{\dim(C)!} \\
&= \binom{g''+t''}{g''} D_0^{t''} D_1^{g''} \deg_L(C).
\end{aligned}$$

   Replacing C by A, g'' by g, t'' by t, the same formula holds for the degree of $\overline{G}$ relative to $M(D_0, D_1)$. Therefore, using the definition (4.5) of $x(G')$, we have

$$\begin{aligned}
x(G')^{t-t''} &= \# \left(\frac{\Gamma_p(S_1) + G'}{G'} \right) \frac{\widetilde{T}_1^{c_W(G')}}{2^g} \frac{\binom{g''+t''}{g''} \widetilde{D}_0^{t''} \widetilde{D}_1^{g''} \deg_L(C)}{\binom{g+t}{g} \widetilde{D}_0^{t} \widetilde{D}_1^{g} \deg_L A} \\
&= \# \left(\frac{\Gamma_p(S_1) + G'}{G'} \right) T_1^{c_W(G')} \frac{\deg_{M(D_0,D_1)}(\overline{G'})}{\deg_{M(D_0,D_1)}(\overline{G})} \\
&\quad \times 2^{-g} \left(\frac{\widetilde{T}_1}{T_1} \right)^{c_W(G')} \left(\frac{D_0}{\widetilde{D}_0} \right)^{t-t''} \left(\frac{D_1}{\widetilde{D}_1} \right)^{g-g''}.
\end{aligned}$$

As $\widetilde{T}_1 \geqslant 2$, we can bound $\frac{\widetilde{T}_1}{T_1}$ by $\frac{3}{2}$. We also have $D_1 \leqslant \widetilde{D}_1$, $D_0 \leqslant x\widetilde{D}_0$, and $c_W(G') \leqslant g$. Therefore,

$$x(G')^{t-t''} \leqslant 2^{-g}\left(\frac{3}{2}\right)^g x^{t-t''} < x^{t-t''}.$$

This case is therefore impossible.

2. If $t_{G'} + W_{\overline{k}} = t_{G_{\overline{k}}}$. By corollary 4.10, we have $c_W(G') = g + t - (g'' + t'')$. Therefore,

$$\#\left(\frac{\Gamma_p(S_1) + G'}{G'}\right) T_1^{g+t-(g''+t'')} \frac{\binom{g''+t''}{g''} D_0^{t''} D_1^{g''} \deg_L(C)}{\binom{g+t}{g} D_0^t D_1^g \deg_L A} \leqslant 1.$$

However, the cardinality of $\frac{\Gamma_p(S_1)+G'}{G'}$ is positive, from proposition 4.14 the quotients $\frac{T_1}{D_0}$ and $\frac{T_1}{D_1}$ are both greater than or equal to $\frac{C_0C_1}{2y}$, and $\frac{\deg_L(C)}{\deg_L A} \geqslant y^{g-g''}$. We can further bound the binomial quotient:

$$\frac{\binom{g''+t''}{g''}}{\binom{g+t}{g}} = \frac{(g''+t'')!g!t!}{(g+t)!g''!t''!} \geqslant \frac{(g''+t'')!}{(g+t)!} = \frac{1}{(g+t)\cdots(g''+t''+1)} \geqslant \frac{1}{(g+t)^{g+t-(g''+t'')}}.$$

We then get

$$\begin{aligned}\#\left(\frac{\Gamma_p(S_1) + G'}{G'}\right) T_1^{g+t-(g''+t'')} \frac{\binom{g''+t''}{g''} D_0^{t''} D_1^{g''} \deg_L(C)}{\binom{g+t}{g} D_0^t D_1^g \deg_L A} &> \frac{1}{y^{t-t''}}\left(\frac{C_0C_1}{2(g+t)}\right)^{g+t-(g''+t'')} \\ &\geqslant 1.\end{aligned}$$

This case is thus also impossible and the section s has to be zero.

■

4.4 Adelic structures

In order to use the theory of Hermitian adelic vector bundles we introduced in section 3.1, we need to associate a structure of projective module to the k-vector space of global sections of $\left(\overline{G}, M(D_0, D_1)\right)$. First, consider a Moret-Bailly model $\left(\mathcal{A}, \overline{\mathcal{L}_{D_1}}, (\varepsilon_{mp_A})_{-(g+t)S_1 \leqslant m \leqslant (g+t)S_1}\right)$ defined over some finite extension K/k of the triplet $\left(A, L^{\otimes D_1}, (mp_A)_{-(g+t)S_1 \leqslant m \leqslant (g+t)S_1}\right)$ (see theorem 3.26). The space $H^0(\mathcal{A}, \mathcal{L}_{D_1})$ has a structure of Hermitian adelic vector bundle compatible with the Riemann form of $(A, L^{\otimes D_1})$, as well as the tangent space $t_{\mathcal{A}}$. Let $\mathcal{W}_0$ be the $\mathcal{O}_K$-submodule $t_{\mathcal{A}} \cap (W_0 \otimes_k K)$ coming from the vector space W_0 and define

$$\mathcal{G}_0 := \mathbb{V}\left((t_{\mathcal{A}}/\mathcal{W}_0)^\vee\right) \quad \text{and} \quad \mathcal{G} := \mathcal{G}_0 \times_{\operatorname{Spec}\mathcal{O}_K} \mathcal{A}.$$

The generic fibers of $\mathcal{G}_0$ and $\mathcal{G}$ are G_0 and G respectively. We now put the invertible sheaf

$$\mathcal{M}(D_0, D_1) := \mathcal{O}(D_0) \boxtimes \mathcal{L}_{D_1},$$

on the scheme $\overline{\mathcal{G}} := \mathbb{P}\left(\mathcal{O}_K \times_{\operatorname{Spec}\mathcal{O}_K} (t_{\mathcal{A}}/\mathcal{W}_0)^\vee\right) \times_{\operatorname{Spec}\mathcal{O}_K} \mathcal{A}$ over $\operatorname{Spec}\mathcal{O}_K$. It is equipped with Hermitian metrics at the Archimedean places of K obtained by Hermitian sum of the Fubini-Study metrics on $\mathcal{O}(D_0)$ coming from t_A and the cubist metrics on $\mathcal{L}_{D_1}$. The $\mathcal{O}_K$-module

$H^0\left(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1)\right)$ is locally free and following section 3.5, for a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, we have a Hermitian metric on $H^0\left(\overline{G}, \mathcal{M}(D_0, D_1)\right) \otimes_\sigma \mathbb{C} = H^0\left(\overline{G_\sigma}, M(D_0, D_1)_\sigma\right)$ given by

$$\|s\|_{2,\sigma}^2 = \int_{\overline{G_\sigma}(\mathbb{C})} \|s(x)\|_{x,\sigma}^2 \mathrm{d}x, \quad \forall s \in H^0\left(\overline{G_\sigma}, M(D_0, D_1)_\sigma\right).$$

This defined a Hermitian adelic vector bundle $\overline{H^0\left(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1)\right)}$, allowing us to use Arakelov theory with the sections of $(\overline{G}, M(D_0, D_1))$. Let us describe more precisely this Hermitian structure. There is a canonical way to attach a holomorphic function on t_{G_σ} to a section s. Indeed, we have an isomorphism $H^0\left(\overline{G_\sigma}, M(D_0, D_1)_\sigma\right) \cong H^0\left(A_\sigma, L_\sigma^{\otimes D_1}\right) \otimes H^0\left(\overline{G_{0,\sigma}}, \mathcal{O}(D_0)\right)$, and therefore s decomposes as

$$s = \sum_j s_{A,j} \otimes s_{0,j},$$

with $s_{A,j} \in H^0\left(A_\sigma, L_\sigma^{\otimes D_1}\right)$ and $s_{0,j} \in H^0\left(\overline{G_{0,\sigma}}, \mathcal{O}(D_0)\right)$. From theorem 3.15, the $s_{A,j}$'s correspond to holomorphic functions ϑ_j on t_{A_σ}, and from definition 3.30 the $s_{0,j}$'s correspond to homogeneous polynomials of degree at most D_0 on $\overline{G_{0,\sigma}}$. Embedding $t_{G_{0,\sigma}}$ in $\overline{G_{0,\sigma}}$ by sending x_0 to $[1 : x_0]$, the $s_{0,j}$'s correspond to polynomials P_j of degree at most D_0 on $t_{G_{0,\sigma}}$. Therefore, the section s corresponds to the function

$$s^\star := \sum_j \vartheta_j P_j. \tag{4.9}$$

Moreover, from (3.1) and (3.2), we get a structure of compact complex variety with a Hermitian line bundle on $(\overline{G}_\sigma, M(D_0, D_1)_\sigma)$ defined by

$$\|s([1 : x_0], x_A)\|_\sigma = |s^\star(z)| \frac{\exp\left(-\frac{\pi}{2} D_1 \|x_A\|_\sigma^2\right)}{(1 + \|x_0\|_\sigma^2)^{D_0/2}}, \qquad \forall (x_0, x_A) \in G_\sigma, \tag{4.10}$$

with $z \in t_{G_\sigma}$ such that $(x_0, x_A) = \exp_{G_\sigma}(z)$. In the following, we will also use a lot the sup norm

$$\|s\|_{\infty,\sigma} := \sup_{x \in \overline{G}_\sigma} \|s(x)\|_\sigma.$$

Applying the results of section 3.5, together with the values of our parameters we can compare the Hermitian norm and the sup-norm.

Lemma 4.18. *Let K'/k be a finite extension of k, let $\sigma : K' \hookrightarrow \mathbb{C}$ be a complex embedding of K', and let $s \in H^0(\overline{G}_\sigma, M(D_0, D_1)_\sigma)$. We have*

$$\|s\|_{\infty,\sigma} \leqslant \|s\|_{2,\sigma} D_1^{g/2} \binom{t + D_0}{t}^{1/2} \mathrm{h}^0(A, L)^{1/2} (3.9g)^{g/2} \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

In particular,

$$\|s\|_{\infty,\sigma} \leqslant \|s\|_{2,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S} + 1) \log E}{D C_0 C_1}\right) \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

Proof. The first result follows from propositions 3.34, 3.35 and 3.37. We then bound $D_1^{g/2}$ and $\binom{t+D_0}{t}^{1/2}$ using proposition 4.14. The function $x \mapsto \frac{\log x}{x}$ is decreasing for $x \geqslant \mathrm{e}$, and $D_1 \geqslant (2(g+t))^{2g+t+3} \geqslant \mathrm{e}$ from proposition 4.14.3. Therefore,

$$D_1^{g/2} = \exp\left(\frac{g}{2}\log D_1\right) \leqslant \exp\left(\underbrace{\frac{g}{2}\frac{(2g+t+3)\log(2(g+t))}{(2(g+t))^{2g+t+3}}}_{\leqslant 1/10} D_1\right) \leqslant \exp\left(\frac{\widetilde{T}_1}{10C_0C_1}\right).$$

Similarly, we have $\binom{t+D_0}{t}^{1/2} \leqslant (D_0+1)^{t/2}$ from lemma 3.39, and because the map $x \mapsto \frac{\log(x+1)}{x}$ is decreasing for $x \geqslant 0$, and $D_0 \geqslant (2(g+t))^3$ from proposition 4.14.3, we have

$$\binom{t+D_0}{t}^{1/2} \leqslant \exp\left(\frac{t}{2}\log(D_0+1)\right) \leqslant \exp\left(\underbrace{\frac{t}{2}\frac{3\log(2(g+t))}{(2(g+t))^3}}_{\leqslant 1/10} D_0\right) \leqslant \exp\left(\frac{\widetilde{T}_1}{10C_0C_1}\right).$$

Moreover, from proposition 4.14.4 we have $\mathrm{h}^0(A,L)^{1/2} \leqslant \exp\left(\frac{(2\widetilde{S}+1)\log E}{2DC_0}\right)$ and $\frac{(2\widetilde{S}+1)\log E}{DC_0} \geqslant 1$. Therefore,

$$\mathrm{h}^0(A,L)^{1/2}(3.9g)^{g/2} \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\left(\frac{1}{2\widetilde{T}_1} + \frac{g\log(3.9g)}{2\widetilde{T}_1}\right)\right).$$

From proposition 4.14.1, $2\widetilde{T}_1 \geqslant 2\cdot(2(g+t))^{4g+2t+6} \geqslant 10C_1(1+g\log(3.9g))$, and therefore

$$\begin{aligned}\|s\|_{\infty,\sigma} &\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\times\frac{3}{10C_1}\right)\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}\\ &\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1}\right)\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}.\end{aligned}$$

■

4.5 Autissier matrix lemma

Autissier matrix lemma [Aut13, Corollary 1.4] gives an upper-bound for the mean of the numbers $\frac{1}{\rho(A_\sigma,L_\sigma)^2}$ over all the complex embeddings of (A,L). The following result of [Gau19] is a direct application of it using the value $\varepsilon = 1 - \frac{6}{2.3\pi}$.

Proposition 4.19 ([Gau19, Matrix lemma, p. 443])**.** *Let (A,L) be a polarised abelian variety of dimension g over a number field k. We have*

$$\frac{1}{D}\sum_{\sigma:k\hookrightarrow\mathbb{C}}\frac{1}{\rho(A_\sigma,L_\sigma)^2} \leqslant (2.3+5.5g)\max\left(1, h_F(A)+\frac{1}{2}\log \mathrm{h}^0(A,L)\right).$$

The quantity we will have to bound during the proof is not the mean of $\left(\frac{1}{\rho(A_\sigma,L_\sigma)^2}\right)_\sigma$ by the mean of the positive part of the logarithm of it. In order to switch between these two means we have the following lemma is extracted from [BG19, Lemme 3.19].

Lemma 4.20. *Let $x_1, \dots, x_n$ be positive real numbers. We have*

$$\frac{1}{n}\sum_{i=1}^{n}\log^+(x_i) \leqslant \max\left(1, \log\left(\frac{1}{n}\sum_{i=1}^{n}x_i\right)\right).$$

Combining proposition 4.19 and lemma 4.20 we get the following.

Proposition 4.21. *Let K'/k be a finite extension of k. For any positive integer n, we have*

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log^+\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes n})} \leqslant \frac{1}{2}\max\left(1, \frac{(2\widetilde{S}+1)\log E}{DC_0}\times\left(1+\log\frac{9(g+t)}{n}\right)\right).$$

Proof. First notice that for any positive real number x, we have $\log^+ x = \frac{1}{2}\log^+ x^2$. Combining this with lemma 4.20 we get

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log^+\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes n})} \leqslant \frac{1}{2}\max\left(1, \log\left(\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes n})^2}\right)\right).$$

From the definition of the injectivity diameter we have $\rho(A_\sigma, L_\sigma^{\otimes n})^2 = n\rho(A_\sigma, L_\sigma)^2$. Applying proposition 4.19, we deduce that

$$\begin{aligned}\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log^+&\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes n})}\\ &\leqslant \frac{1}{2}\max\left(1, \log\left(\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\frac{1}{n\rho(A_\sigma, L_\sigma)^2}\right)\right)\\ &\leqslant \frac{1}{2}\max\left(1, \log^+\frac{(2.3+5.5g)\max\left(1, h_F(A)+\frac{1}{2}\log \mathrm{h}^0(A,L)\right)}{n}\right).\end{aligned}$$

From proposition 4.14.4, 1, $h_F(A)$, and $\log \mathrm{h}^0(A,L)$ are all bounded by $\frac{(2\widetilde{S}+1)\log E}{DC_0}$. Therefore,

$$\begin{aligned}\log\frac{(2.3+5.5g)\max\left(1, h_F(A)+\frac{1}{2}\log \mathrm{h}^0(A,L)\right)}{n} &\leqslant \log\left(\frac{(2\widetilde{S}+1)\log E}{DC_0}\times\frac{3(2.3+5.5g)}{2n}\right)\\ &\leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0}\left(1+\log\left(\frac{3(2.3+5.5g)}{2n}\right)\right).\end{aligned}$$

We conclude using the inequalities $\frac{3(2.3+5.5g)}{2} \leqslant 3.5+8.3g \leqslant 9(g+t)$. ∎

We will need proposition 4.21 for both $n=1$ and $n=D_1$. We state hereafter the results we will use during the proof.

Corollary 4.22. *Let K'/k be a finite extension of k and let $\sigma : K' \hookrightarrow \mathbb{C}$ be a complex embedding of K'. We have*

$$\log^+\frac{1}{\rho(A_\sigma, L_\sigma)} \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}\times(g+t),$$

and

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log^+\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\leqslant\frac{(2\widetilde{S}+1)\log E}{2DC_0}.$$

In particular

$$\log^+\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\leqslant\frac{(2\widetilde{S}+1)\log E}{2C_0}.$$

Proof. Because $\rho(A_\sigma,L_\sigma)$ depends only on $\sigma|_k$, we can bound $\log^+\frac{1}{\rho(A_\sigma,L_\sigma)}$ by $\sum_{\tau:k\hookrightarrow\mathbb{C}}\log^+\frac{1}{\rho(A_\tau,L_\tau)}$. Using proposition 4.21 with $n=1$, we get

$$\log^+\frac{1}{\rho(A_\sigma,L_\sigma)}\leqslant\frac{D}{2}\max\left(1,\frac{(2\widetilde{S}+1)\log E}{DC_0}\times(1+\log(9(g+t)))\right).$$

As $\frac{(2\widetilde{S}+1)\log E}{DC_0}\geqslant 1$, and $1+\log(9(g+t))\leqslant 1+9(g+t)\frac{\log(18)}{18}\leqslant 2(g+t)$, we deduce

$$\begin{aligned}\log^+\frac{1}{\rho(A_\sigma,L_\sigma)}&\leqslant\frac{D}{2}\max\left(1,\frac{(2\widetilde{S}+1)\log E}{DC_0}\times(1+\log(9(g+t)))\right)\\&\leqslant\frac{D}{2}\max\left(1,\frac{(2\widetilde{S}+1)\log E}{DC_0}\times 2(g+t)\right)\\&\leqslant\frac{(2\widetilde{S}+1)\log E}{C_0}\times(g+t).\end{aligned}$$

For the second result, we apply proposition 4.21 with $n=D_1$. From the lower-bound of proposition 4.14.3, we have $D_1\geqslant(2(g+t))^{2g+t+3}\geqslant 9(g+t)$. Therefore, because $\frac{(2\widetilde{S}+1)\log E}{DC_0}\geqslant 1$ from proposition 4.14.4, we have

$$\begin{aligned}\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log^+\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}&\leqslant\frac{1}{2}\max\left(1,\frac{(2\widetilde{S}+1)\log E}{DC_0}\times\Big(\underbrace{1+\log\frac{9(g+t)}{D_1}}_{\leqslant 1}\Big)\right)\\&\leqslant\frac{(2\widetilde{S}+1)\log E}{2DC_0}.\end{aligned}$$

■

Finally, we will also deal with means of functions involving the covering radii of (A,L). Using the previous results and proposition 3.21 we prove the result we will need.

Proposition 4.23.

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\leqslant\frac{2(2\widetilde{S}+1)\log E}{DC_0}$$

Proof. From proposition 3.21, we have $r(A_\sigma, L_\sigma) \leqslant \frac{g\,\mathrm{h}^0(A,L)}{\rho(A_\sigma,L_\sigma)}$. Using lemma 4.20 we have

$$\begin{aligned}
&\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\\
&\qquad\leqslant \frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi g\,\mathrm{h}^0(A,L)}{C_0C_1}\frac{1}{\rho(A_\sigma,L_\sigma)}+1\right)\\
&\qquad\leqslant \max\left(1,\log\left(\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\left(\frac{2\pi g\,\mathrm{h}^0(A,L)}{C_0C_1}\frac{1}{\rho(A_\sigma,L_\sigma)}+1\right)\right)\right).
\end{aligned}$$

From the convexity of the function $x\mapsto x^2$, the sum $\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\frac{1}{\rho(A_\sigma,L_\sigma)}$ is bounded by $\left(\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\frac{1}{\rho(A_\sigma,L_\sigma)^2}\right)^{1/2}$. Applying proposition 4.19, we get

$$\begin{aligned}
&\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\\
&\qquad\leqslant \max\left(1,\log\left(1+\frac{2\pi g\,\mathrm{h}^0(A,L)\sqrt{(2.3+5.5g)\max(1,h_F(A)+\frac{1}{2}\log\mathrm{h}^0(A,L))}}{C_0C_1}\right)\right).
\end{aligned}$$

Finally, from proposition 4.14.4, 1, $h_F(A)$, and $\log\mathrm{h}^0(A,L)$ are bounded by $\frac{(2\widetilde{S}+1)\log E}{C_0D}$. Using the values of C_0 and C_1, $\frac{2\pi g\sqrt{3(2.3+5.5g)}}{\sqrt{2}C_0C_1}$ is less than 1. It follows that

$$\begin{aligned}
&\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\\
&\leqslant \max\left(1,\log\left(1+\frac{2\pi g\,\mathrm{h}^0(A,L)\sqrt{(2.3+5.5g)\max(1,h_F(A)+\frac{1}{2}\log\mathrm{h}^0(A,L))}}{C_0C_1}\right)\right)\\
&\leqslant \max\left(1,\log\mathrm{h}^0(A,L)+\log\left(1+\frac{2\pi g\sqrt{2.3+5.5g}}{C_0C_1}\max(1,h_F(A)+\frac{1}{2}\log\mathrm{h}^0(A,L))^{1/2}\right)\right)\\
&\leqslant \max\left(1,\log\mathrm{h}^0(A,L)+\log\left(1+\sqrt{\frac{(2\widetilde{S}+1)\log E}{DC_0}}\times\underbrace{\frac{2\pi g\sqrt{3(2.3+5.5g)}}{\sqrt{2}C_0C_1}}_{\leqslant 1}\right)\right)\\
&\leqslant \max\left(1,\frac{(2\widetilde{S}+1)\log E}{DC_0}+\log\left(1+\sqrt{\frac{(2\widetilde{S}+1)\log E}{DC_0}}\right)\right)\\
&\leqslant \frac{2(2\widetilde{S}+1)\log E}{DC_0}.
\end{aligned}$$

■

Chapter 5

Siegel lemma

The goal of this chapter is to construct a section $s \in H^0(\overline{G}, M(D_0, D_1))$ of controlled height. More precisely, we want a section of small height with respect to the adelic Hermitian vector bundle structure of $\overline{H^0(\overline{G}, M(D_0, D_1))}$ defined in section 4.4, and with small derivatives at multiples of the point p. In order to do this, we define a twisted Hermitian metric on $\overline{H^0(\overline{G}, M(D_0, D_1))}$.

5.1 Adelic vector bundle of global sections

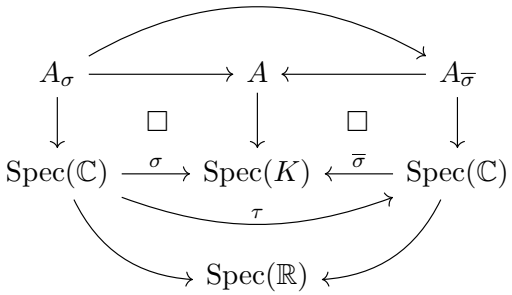
All along the proof we will be using a lot the theory of holomorphic functions over a complex vector space. Given a finite dimensional complex vector space V, a holomorphic function $f : V \to \mathbb{C}$, and a vector subspace W of V, the Taylor coefficients $\left(\frac{1}{\tau!} D^{\tau}_{\mathbf{w}} f(x)\right)_{\tau \in \mathbb{N}^g}$ of f at $x \in V$ along the basis $\mathbf{w} := (w_1, \dots, w_g)$ of W are the coefficients of the following Taylor expansion

$$f\left(x + \sum_{i=1}^{g} h_i w_i\right) = \sum_{\tau \in \mathbb{N}^g} \frac{1}{\tau!} D^{\tau}_{\mathbf{w}} f(x) h_1^{\tau_1} \cdots h_g^{\tau_g}, \quad \forall h_1, \dots, h_g \in \mathbb{C}.$$

The Taylor coefficients of a function are highly dependent of the chosen basis $\mathbf{w}$. We therefore need to fix a basis of W_σ for every embedding σ.

Let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding of K, where K is the field of definition of the group $\mathcal{G}$ (see section 4.4). We define a basis $\mathbf{w}_\sigma = (\mathbf{w}_{\sigma,1}, \dots, \mathbf{w}_{\sigma,g})$ of W_σ in the following way:

- **If σ divides neither σ_0 nor $\overline{\sigma_0}$**, we choose any orthonormal basis of W_σ.
- **If σ divides σ_0 and we are in the non-periodic case**, we again choose any orthonormal basis of W_σ.
- **If σ divides σ_0 and we are in the periodic case**, we first choose an orthonormal basis of $t_{H_\sigma} \cap W_\sigma$. We then complete it so that it is an orthonormal basis of W_σ with $\mathbf{w}_{\sigma,g}$ unitary and colinear to the orthogonal projection of $(\lambda(u_A), u_A)$ onto $(t_{H_\sigma} \cap W_\sigma)^{\perp}$. This is well-defined because of hypothesis 4.2. Indeed, we know that u_A does not lie inside t_{B_σ}. Thus, if $(\lambda(u_A), u_A)$ is contained in $t_{H_\sigma} \cap W_\sigma$, then in particular $u_A \in t_{B_\sigma}$.
- **If σ divides $\overline{\sigma_0}$**, we define $\mathbf{w}_\sigma$ to be the basis corresponding to $\mathbf{w}_{\overline{\sigma}}$ via the morphism $t_{G_\sigma} \to t_{G_{\overline{\sigma}}}$ induced by the complex conjugation. More precisely, the complex conjugation on $\mathbb{C}$ induces a morphism $\tau : \mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(\mathbb{C})$ that leads to the following diagram.



The arrow $A_\sigma \to A_{\overline{\sigma}}$ is an isomorphism of $\mathbb{R}$-schemes but not of $\mathbb{C}$-schemes. Taking the $\mathbb{C}$-points, we get an anti-linear isomorphism of real Lie groups $A_\sigma(\mathbb{C}) \to A_{\overline{\sigma}}(\mathbb{C})$, and we have the following result.

Proposition 5.1 ([GR14b, §2.6]). *The isomorphism $f : A_\sigma \to A_{\overline{\sigma}}$ lifts into an isomorphism $df : t_{A_\sigma} \to t_{A_{\overline{\sigma}}}$ such that $df(\Omega_{A_\sigma}) = \Omega_{A_{\overline{\sigma}}}$. It is an isometry with respect to the Hermitian metrics coming from L_σ and $L_{\overline{\sigma}}$.*

The isometry df then induces an isometry $df_0 : t_{G_{0,\sigma}} \to t_{G_{0,\overline{\sigma}}}$ that leads to the isometry $t_{G_\sigma} \to t_{G_{\overline{\sigma}}}$.

Remark 5.2. *Through this construction, many invariants are conserved. For example, we have $\rho(A_{\overline{\sigma}}, L_{\overline{\sigma}}) = \rho(A_\sigma, L_\sigma)$ and $r(A_{\overline{\sigma}}, L_{\overline{\sigma}}) = r(A_\sigma, L_\sigma)$. We will therefore usually prove results in the case $\sigma \mid \sigma_0$, the case $\sigma \mid \overline{\sigma_0}$ following from this construction.*

We now define a new adelic structure on the space $H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))$ that take into account the derivatives of the sections at the multiples of the point p.

Definition 5.3. *Define*

$$\Upsilon := \{(m, \tau) \in \mathbb{Z} \times \mathbb{N}^g, |m| \leqslant S_0,\ |\tau| \leqslant T_0,\ \text{and } \tau_g \leqslant T_2\}\,.$$

Recall that S_0, T_0, and T_2 have been defined after definition 4.13. For an embedding $\sigma : K \hookrightarrow \mathbb{C}$ of K extending σ_0 we define a linear map U_σ from $H^0(\overline{G}, M(D_0, D_1)) \otimes_\sigma \mathbb{C}$ to $\mathbb{C}^\Upsilon$ by

$$U_\sigma(s) := \left(\frac{1}{\tau!} D^\tau_{\mathbf{w}_\sigma} s^\star(mu) \frac{\exp\left(-\frac{\pi}{2} D_1 \|mu_A\|^2_\sigma\right)}{(1 + \|mu_0\|^2_\sigma)^{D_0/2}} \right)_{(m,\tau)\in\Upsilon},$$

where $s^\star$ is the holomorphic function of t_{G_σ} defined in (4.9). For $\sigma : k \hookrightarrow \mathbb{C}$ extending $\overline{\sigma_0}$, we define U_σ to be the corresponding linear map, as discussed in remark 5.2.

We finally twist the Hermitian adelic vector bundle structure on $\overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))}$ we defined in section 4.4. For $\alpha > 0$, we define for $\sigma : K \hookrightarrow \mathbb{C}$ and $s \in H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma)$,

$$\|s\|^2_{\alpha,\sigma} := \begin{cases} \|s\|^2_\sigma + \alpha^2 \|U_\sigma s\|^2_2 & \text{if } \sigma \text{ extends } \sigma_0 \text{ or } \overline{\sigma_0}; \\ \|s\|^2_\sigma & \text{otherwise.} \end{cases} \tag{5.1}$$

This define a Hermitian adelic structure on $\overline{H^0(\overline{G}, \mathcal{M}(D_0, D_1))}$. We will denote by h_α the height relative to this adelic bundle.

To construct the wanted section, we will use the following Siegel lemma applied to the vector bundles $\overline{H^0(\overline{G}, M(D_0, D_1))}$ and $\overline{\mathbb{C}^\Upsilon}$, together with the linear maps $(U_\sigma)_{\sigma|\sigma_0,\overline{\sigma_0}}$.

Lemma 5.4 ([Gau14, Lemme de Siegel approché absolu, p. 24]). *Let k be a number field of degree D and let S be a finite set of embedding of k. Let $\overline{\mathcal{E}}$ and $\overline{\mathcal{F}}$ be two Hermitian adelic vector bundles over $\operatorname{Spec}\mathcal{O}_k$. For all $\sigma \in S$, let $a_\sigma : E_\sigma \to F_\sigma$ be a $\mathbb{C}$-linear map of rank ρ_σ, norm $\|a_\sigma\|$, and such that $\|a_\sigma\| = \|a_{\overline{\sigma}}\|$. Let $\overline{\mathcal{E}_a}$ be the Hermitian adelic vector bundle with $\mathcal{E}$ as base space and metrics*

$$\|x\|_\sigma := \begin{cases} \|a_\sigma x\|_\sigma & \text{if } \sigma \in S; \\ \|x\|_\sigma & \text{otherwise.} \end{cases}$$

There exists $s \in \overline{\mathcal{E}_a} \otimes_{\mathcal{O}_k} \overline{k} \setminus \{0\}$ such that

$$h_{\overline{\mathcal{E}_a}}(s) \leqslant \frac{1}{D \operatorname{rk}\mathcal{E}} \sum_{\sigma\in S} \rho_\sigma \log\sqrt{1+\|a_\sigma\|^2} + \frac{1}{2}\log\operatorname{rk}\mathcal{E} - \widehat{\mu}(\overline{\mathcal{E}}).$$

The rest of this chapter is devoted to estimate the quantities that appear in the lemma.

5.2 Estimation of the rank of U_σ

We give in this section an upper bound for the rank of the linear maps $(U_\sigma)_\sigma$. As the matrices U_σ and $U_{\overline{\sigma}}$ have always the same rank, we will only focus on the embeddings $\sigma : K \hookrightarrow \mathbb{C}$ extending σ_0. To do so we will change our basis $\mathbf{w}_\sigma$ to a basis that will be adapted to the subgroup H. The following lemma ensures that this change of basis will not change the rank of U_σ.

Lemma 5.5. *Let V be a $\mathbb{C}$-vector space and W be a vector subspace of V of dimension g. Let $\mathbf{w}_1 := (w_{1,1}, \dots, w_{1,g})$, $\mathbf{w}_2 := (w_{2,1}, \dots, w_{2,g})$ be two bases of W such that*

$$\operatorname{Span}_{\mathbb{C}}(w_{1,1}, \dots, w_{1,g-1}) = \operatorname{Span}_{\mathbb{C}}(w_{2,1}, \dots, w_{2,g-1}). \tag{5.2}$$

Let us denote by $\mathcal{O}(V)$ the $\mathbb{C}$-vector space of holomorphic functions on V, and let T be the number of g-tuples τ such that $|\tau| \leqslant T_0$ and $\tau_g \leqslant T_2$. Then for any $x \in V$ and integers T_0, T_2, the kernel of the linear maps

$$\left|\begin{array}{ccc} \mathcal{O}(V) & \longrightarrow & \mathbb{C}^T \\ f & \longmapsto & \left(\frac{1}{\tau!} D^\tau_{\mathbf{w}_i} f(x)\right)_{\substack{|\tau|\leqslant T_0 \\ \tau_g \leqslant T_2}} \end{array}\right.$$

for $i \in \{1, 2\}$ are the same. Moreover, if $T_2 = T_0$, then this is true even without the assumption (5.2).

Proof. We begin by computing the derivatives of a holomorphic function $f : V \to \mathbb{C}$ along $\mathbf{w}_2$ in terms of the ones along $\mathbf{w}_1$. For i between 1 and g write $w_{2,i} = \sum_{j=1}^{g} a_{i,j} w_{1,j}$ with $a_{i,j} \in \mathbb{C}$, and let $h_1, \dots h_g \in \mathbb{C}$. From the definition of the Taylor coefficients of f we have for $x \in V$,

$$f\left(x + \sum_{i=1}^{g} h_i w_{2,i}\right) = \sum_{\tau\in\mathbb{N}^g} \frac{1}{\tau!} D^\tau_{\mathbf{w}_2} f(x) h_1^{\tau_1} \cdots h_g^{\tau_g} = \sum_{\tau'\in\mathbb{N}^g} \frac{1}{\tau'!} D^{\tau'}_{\mathbf{w}_1} f(x) \prod_{j=1}^{g} \left(\sum_{i=1}^{g} a_{i,j} h_i\right)^{\tau'_j}.$$

From the multinomial formula we have

$$\left(\sum_{i=1}^{g} a_{i,j}h_i\right)^{\tau'_j} = \sum_{\tau_{1,j}+\cdots+\tau_{g,j}=\tau'_j} \frac{\tau'_j!}{\tau_{1,j}!\cdots\tau_{g,j}!}(a_{1,j}h_1)^{\tau_{1,j}}\cdots(a_{g,j}h_g)^{\tau_{g,j}}.$$

Identifying the coefficient of $h_1^{\tau_1}\cdots h_g^{\tau_g}$, we finally get

$$\frac{1}{\tau!}D^{\tau}_{\mathbf{w}_2}f(x) = \sum_{\substack{(\tau_{i,j})_{1\leqslant i,j\leqslant g}\\ \tau_{i,1}+\cdots+\tau_{i,g}=\tau_i\\ \text{for all } 1\leqslant i\leqslant g}} \left(\prod_{1\leqslant i,j\leqslant g}\frac{a_{i,j}^{\tau_{i,j}}}{\tau_{i,j}!}\right) D^{\tau'}_{\mathbf{w}_1}f(x), \tag{5.3}$$

where the components of $\tau' \in \mathbb{N}^g$ are $\tau'_j := \sum_{i=1}^{g}\tau_{i,j}$.

We now prove the result. From the symmetry of the setup, it is enough to prove that if $\frac{1}{\tau'!}D^{\tau'}_{\mathbf{w}_1}f(x) = 0$ for all $\tau' \in \mathbb{N}^g$ such that $|\tau'| \leqslant T_0$ and $\tau'_g \leqslant T_2$, then this is also true for the $\frac{1}{\tau'!}D^{\tau'}_{\mathbf{w}_2}f(x)$'s. Assume that $\frac{1}{\tau'!}D^{\tau'}_{\mathbf{w}_1}f(x) = 0$ for all $\tau' \in \mathbb{N}^g$ such that $|\tau'| \leqslant T_0$ and $\tau'_g \leqslant T_2$, and let $\tau \in \mathbb{N}^g$ be such that $|\tau| \leqslant T_0$ and $\tau_g \leqslant T_2$. Let us prove that all the terms in the sum of (5.3) vanish. Let $(\tau_{i,j})_{1\leqslant i,j\leqslant g}$ be such that $\tau_{i,1}+\cdots+\tau_{i,g} = \tau_i$ for all $1 \leqslant i \leqslant g$, and let $\tau' \in \mathbb{N}^g$ with components $\tau'_j = \sum_{i=1}^{g}\tau_{i,j}$.

If $T_2 = T_0$, then all the derivatives of f along $\mathbf{w}_1$ of order less or equal to T_0 vanish. Therefore,

$$\left(\prod_{1\leqslant i,j\leqslant g}\frac{a_{i,j}^{\tau_{i,j}}}{\tau_{i,j}!}\right) D^{\tau'}_{\mathbf{w}_1}f(x) = 0$$

and we are done. In the general case, under the assumption (5.2) we have $a_{i,g} = 0$ for all $i < g$. Thus, either $\prod_{1\leqslant i,j\leqslant g}\frac{a_{i,j}^{\tau_{i,j}}}{\tau_{i,j}!} = 0$, or $\tau_{i,g} = 0$ for all $i < g$. In this second case, we have

$$\tau'_g = \tau_{1,g}+\cdots+\tau_{g,g} = \tau_{g,g} \leqslant \tau_g \leqslant T_2.$$

Therefore, τ' satisfies $|\tau'| \leqslant T_0$ and $\tau'_g \leqslant T_2$ and $D^{\tau'}_{\mathbf{w}_1}f(x) = 0$. In all cases we again have $\left(\prod_{1\leqslant i,j\leqslant g}\frac{a_{i,j}^{\tau_{i,j}}}{\tau_{i,j}!}\right) D^{\tau'}_{\mathbf{w}_1}f(x) = 0$. ■

Let $\sigma : K \hookrightarrow \mathbb{C}$ extending σ_0. We outline the strategy we use to estimate the rank of U_σ. It mimics the method of [BG19, §3.5] adapted in our more general context. We construct a filtration $(F_\ell)_{\ell\geqslant -1}$ of $H^0(\overline{G_\sigma}, M(D_0,D_1)_\sigma)$ adapted to our distinguished subgroup H of $G_{\overline{k}}$ defined before definition 4.13. This filtration will be such that

$$F_{-1} = H^0(\overline{G_\sigma}, M(D_0,D_1)_\sigma) \quad \text{and} \quad F_{T_0} = \ker(U_\sigma).$$

Using the rank-nullity theorem, we get

$$\operatorname{rk}(U_\sigma) = \dim(F_{-1}) - \dim(F_{T_0}) = \sum_{\ell=0}^{T_0}\left(\dim(F_{\ell-1}) - \dim(F_\ell)\right).$$

An estimation of the dimension of the quotients $F_{\ell-1}/F_\ell$ will lead to an estimation of $\mathrm{rk}(U_\sigma)$.

Consider a basis $\boldsymbol{w}$ of W_σ such that the first $g - c_W(H) = \dim(W_{\overline{k}} \cap t_H)$ elements of $\boldsymbol{w}$ form a basis of $t_{H_\sigma} \cap W_\sigma$. For any $\ell \geqslant -1$, let X_ℓ be the set of $\tau \in \mathbb{N}^g$ such that $|\tau| \leqslant \ell$, $\tau_g \leqslant T_2$, and $\tau_1 = \cdots = \tau_{g-c_W(H)} = 0$. We define the vector subspace F_ℓ of $H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma)$ by

$$F_\ell := \left\{ s \in H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma), \forall |m| \leqslant S_0, \forall \xi \in t_{H_\sigma}, \forall \tau \in X_\ell,\ \frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(mu + \xi) = 0 \right\}.$$

Notice that the spaces $(F_\ell)_\ell$ form a descending filtration of $F_{-1} = H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma)$. Moreover, we claim that F_{T_0} lies in the kernel of U_σ. Indeed, if $s \in F_{T_0}$, then $\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(mu + \xi) = 0$ for all $\xi \in t_{H_\sigma}$ and $(m, \tau) \in \Upsilon$ such that $\tau \in X_{T_0}$. As the vectors $(w_1, \ldots, w_{g-c_W(H)})$ form a basis of $t_{H_\sigma} \cap W_\sigma$, we get that $\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(mu) = 0$ for all $(m, \tau) \in \Upsilon$. Finally, from the way the bases $\mathbf{w}_\sigma$ and $\boldsymbol{w}$ have been constructed lemma 5.5 applies and thus $s \in \ker(U_\sigma)$. From the rank-nullity theorem we get

$$\mathrm{rk}(U_\sigma) \leqslant \mathrm{h}^0(\overline{G}, M(D_0, D_1)) - \dim(F_{T_0}) = \dim(F_{-1}) - \dim(F_{T_0}) = \sum_{\ell=0}^{T_0} (\dim F_{\ell-1} - \dim F_\ell). \tag{5.4}$$

Our goal is now to give an upper-bound for the codimension of F_ℓ in $F_{\ell-1}$. We begin by relaxing the definition of F_ℓ. Consider now $\alpha_1, \ldots, \alpha_h$ a system of representatives of

$$\frac{\{mu, |m| \leqslant S_0\} + t_{H_\sigma} + \Omega_{A_\sigma}}{t_{H_\sigma} + \Omega_{A_\sigma}}.$$

As $\exp_{G_\sigma}$ is a bijection between $\frac{\{mu, |m| \leqslant S_0\} + t_{H_\sigma} + \Omega_{A_\sigma}}{t_{H_\sigma} + \Omega_{A_\sigma}}$ and $\frac{\Gamma_p(S_0) + H}{H}$, we have $h = \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)$. Let us define a seemingly different filtration $(G_\ell)_{\ell \geqslant -1}$ of $H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma)$ by

$$G_\ell := \left\{ s \in H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma),\ \forall i \leqslant h,\ \forall \xi \in t_{H_\sigma},\ \forall \tau \in X_\ell,\ \frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(\alpha_i + \xi) = 0 \right\}.$$

The following result tells us that it is in fact the same filtration as $(F_\ell)_\ell$.

Proposition 5.6. *For all $\ell \geqslant -1$, we have $F_\ell = G_\ell$.*

Proof. Let $s \in F_\ell$. From (4.9), s corresponds to a function

$$s^\star = \sum_j \vartheta_j P_j$$

on t_{G_σ}, where P_j is a polynomial on $t_{A_\sigma}/W_{0,\sigma}$ of degree less or equal to D_0 and ϑ_j is holomorphic on t_{A_σ}. Let i be an integer between 1 and h, and let $\xi \in t_{H_\sigma}$. There is $m \in \mathbb{Z}$, $|m| \leqslant S_0$, $\xi' \in t_{H_\sigma}$, and $\omega \in \Omega_{A_\sigma}$ such that $\alpha_i + \xi = mu + \xi' + \omega$. Write $\xi' := (\xi'_0, \xi'_A) \in t_{H_{0,\sigma}} \times t_{A_\sigma}$. Consider the factor of automorphy a coming from the Appel–Humbert data of $L_\sigma^{\otimes D_1}$ (see theorem 3.18). As the functions ϑ_j lies in the space $\Theta(a)$, we have

$$\begin{aligned} s^\star(\alpha_i + \xi) &= \sum_j \vartheta_j(mu_A + \xi'_A + \omega) P_j(mu_0 + \xi'_0) \\ &= \sum_j a(\omega, mu_A + \xi'_A) \vartheta_j(mu_A + \xi'_A) P_j(mu_0 + \xi'_0) \\ &= a(\omega, mu_A + \xi'_A) s^\star(mu + \xi'). \end{aligned}$$

Therefore, from Leibniz derivation formula we have for $\tau \in X_\ell$,

$$\frac{1}{\tau!}D^\tau_{\boldsymbol{w}} s^\star(\alpha_i+\xi) = \sum_{\tau_1+\tau_2=\tau} \frac{1}{\tau_1!} D^{\tau_1}_{\boldsymbol{w}} a(\omega, mu_A+\xi'_A) \underbrace{\frac{1}{\tau_2!} D^{\tau_2}_{\boldsymbol{w}} s^\star(mu+\xi')}_{=0 \text{ because } s\in F_\ell} = 0,$$

the derivative $D^{\tau_1}_{\boldsymbol{w}} a(\omega, mu_A+\xi'_A)$ being understood as the derivative of the holomorphic function of t_{G_σ} sending (x_0, x_A) to $a(\omega, x_A)$. Therefore, s lies in G_ℓ.

Conversely, let $s \in G_\ell$ and writes $s^\star = \sum_j \vartheta_j P_j$. For $m \in \mathbb{Z}$, $|m| \leqslant S_0$, and $\xi \in t_{H_\sigma}$, there are $i \in \{1,\dots,h\}$, $\xi \in t_{H_\sigma}$, and $\omega \in \Omega_{A_\sigma}$ such that $mu+\xi = \alpha_i + \xi' + \omega$, and we similarly have $s^\star(mu+\xi) = a(\omega, \alpha_{i,A}+\xi'_A) s^\star(\alpha_i+\xi')$. For $\tau \in X_\ell$, we deduce that

$$\frac{1}{\tau!}D^\tau_{\boldsymbol{w}} s^\star(mu+\xi) = \sum_{\tau_1+\tau_2=\tau} \frac{1}{\tau_1!} D^{\tau_1}_{\boldsymbol{w}} a(\omega, \alpha_{i,A}+\xi'_A) \underbrace{\frac{1}{\tau_2!} D^{\tau_2}_{\boldsymbol{w}} s^\star(\alpha_i+\xi')}_{=0 \text{ because } s\in G_\ell} = 0.$$

Therefore, $s \in F_\ell$. ∎

We now work with the filtration $(G_\ell)_\ell$. First, let us impose some constraints on our representatives $\alpha_1,\dots,\alpha_h$. For any $x \in t_{G_\sigma}$, the orthogonal projection of x onto $t^\perp_{H_\sigma}$ differs from x by an element of t_{H_σ}. Therefore, it lies in the same class modulo $t_{H_\sigma}+\Omega_{A_\sigma}$ as x. Replacing the α_i's by their orthogonal projection onto $t^\perp_{H_\sigma}$, we can assume they all lie in $t^\perp_{H_\sigma}$.

Let (χ, H) be the Appel–Humbert data for $(A, L^{\otimes D_1})$ (see theorem 3.18). For $\omega_B \in \Omega_{B_\sigma}$ (where B is the abelian part of H, see the discussion before lemma 4.9) and $z \in t_{A_\sigma}$, we have

$$\begin{aligned} a(\omega_B, \alpha_{i,A}+z) &= \chi(\omega_B)\exp\Big(\pi H(z,\omega_B) + \pi H(\alpha_{i,A},\omega_B) + \frac{\pi}{2}H(\omega_B,\omega_B)\Big) \\ &= \chi(\omega_B)\exp\Big(\pi H(z,\omega_B) + \frac{\pi}{2}H(\omega_B,\omega_B)\Big) \\ &= a(\omega_B, z). \end{aligned}$$

Therefore, given a section $s \in G_\ell$, an integer i between 1 and h, a period $\omega_B \in \Omega_{B_\sigma}$, and an element $\xi := (\xi_0, \xi_B) \in t_{H,\sigma} = t_{H_{0,\sigma}} \times t_{B_\sigma}$, we have

$$\begin{aligned} s^\star(\alpha_i+\xi+\omega_B) &= a(\omega_B, \alpha_{i,A}+\xi_B) s^\star(\alpha_i+\xi) \\ &= a(\omega_B, \xi_B) s^\star(\alpha_i+\xi). \end{aligned}$$

Thus, for $\tau \in X_\ell$ the map

$$\vartheta_B : \left\{ \begin{array}{ccc} t_{B_\sigma} & \longrightarrow & \mathbb{C} \\ \xi_B & \longmapsto & \frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(\alpha_i+\xi_0+\xi_B) \end{array} \right. ,$$

satisfies $\vartheta_B(\xi_B+\omega_B) = a(\omega_B,\xi_B)\vartheta_B(\xi_B)$ and comes from a section of $(B_\sigma, L_\sigma^{\otimes D_1})$.

Proposition 5.7. *For any $\ell \geqslant 0$, we have*

$$\dim(G_{\ell-1}) - \dim(G_\ell) \leqslant \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)\binom{t'+D_0}{t'} \mathrm{h}^0(B, L^{\otimes D_1}) \# X_\ell.$$

Proof. Let $\xi_{0,1},\dots,\xi_{0,N}$ be points of $t_{H_{0,\sigma}}$, with $N := \binom{t'+D_0}{t'}$ such that the map

$$\left|\begin{array}{ccc} H^0\left(H_{0,\sigma},\mathcal{O}(D_0)\right) & \longrightarrow & \mathbb{C}^N \\ P & \longmapsto & \left(P(\xi_{0,i})\right)_{i\leqslant N} \end{array}\right. ,$$

is an isomorphism of $\mathbb{C}$-vector spaces. This is possible as the vector space $H^0(H_{0,\sigma},\mathcal{O}(D_0))$ corresponds to polynomials on $t_{H_{0,\sigma}}$ of degree at most D_0. Let us define a linear map

$$i_\ell : \left|\begin{array}{ccc} G_{\ell-1} & \longrightarrow & \Theta(B_\sigma, L_\sigma^{\otimes D_1})^{hN\#X_\ell} \\ s & \longmapsto & \left(\xi_B \mapsto \frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(\alpha_i+\xi_{0,j}+\xi_B)\right)_{\substack{1\leqslant i\leqslant h,\ \tau\in X_\ell,\\ 1\leqslant j\leqslant N}} \end{array}\right. .$$

From the discussion above i_ℓ is well-defined and its kernel is exactly G_ℓ. We therefore get an injection $G_{\ell-1}/G_\ell \hookrightarrow \Theta(B_\sigma, L_\sigma^{\otimes D_1})^{hN\#X_\ell}$ and

$$\dim(G_{\ell-1}) - \dim(G_\ell) \leqslant \dim\left(\Theta(B_\sigma, L_\sigma^{\otimes D_1})^{hN\#X_\ell}\right) = hN\#X_\ell\, \mathrm{h}^0(B, L^{\otimes D_1}).$$

The result follows as $h = \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)$ and $N = \binom{t'+D_0}{t'}$. ∎

We can finally get a first upper-bound for the rank of U_σ. From (5.4) and proposition 5.6, it follows that

$$\begin{aligned}
\mathrm{rk}(U_\sigma) &\leqslant \sum_{\ell=0}^{T_0} (\dim(G_{\ell-1}) - \dim(G_\ell)) \\
&\leqslant \sum_{\ell=0}^{T_0} \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)\binom{t'+D_0}{t'} \mathrm{h}^0(B, L^{\otimes D_1})\#X_\ell \\
&\leqslant \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)\binom{t'+D_0}{t'} D_1^{g'}\, \mathrm{h}^0(B,L)\#\left\{\tau\in\mathbb{N}^{c_W(H)}, |\tau|\leqslant T_0, \tau_{c_W(H)}\leqslant T_2\right\} \\
&\leqslant \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)\binom{t'+D_0}{t'} D_1^{g'}\, \mathrm{h}^0(B,L) \\
&\qquad \times \left(\binom{T_0+c_W(H)}{c_W(H)} - \binom{T_0-T_2+c_W(H)-1}{c_W(H)}\right).
\end{aligned}$$

The last line follows from lemma 3.38.

Proposition 5.8. *For any embedding $\sigma : K \hookrightarrow \mathbb{C}$ extending σ_0 or $\overline{\sigma_0}$, we have*

$$\frac{\mathrm{rk}(U_\sigma)}{\mathrm{h}^0(\overline{G}, M(D_0,D_1))} \leqslant \frac{2.03\cdot 2^{2g-1}}{5^{2g+t}}.$$

Proof. From remark 5.2, we only need to consider the case $\sigma \mid \sigma_0$. Taking back the upper-bound we just got and using lemma 3.39, we deduce that

$$\frac{\mathrm{rk}(U_\sigma)}{\mathrm{h}^0(\overline{G}, M(D_0,D_1))} \leqslant \#\left(\frac{\Gamma_p(S_0)+H}{H}\right)\frac{\binom{t'+D_0}{t'} D_1^{g'}\, \mathrm{h}^0(B,L)}{\binom{t+D_0}{t} D_1^{g}\, \mathrm{h}^0(A,L)}(T_2+1)(T_0+1)^{c_W(H)-1}.$$

Because $g!h^0(A,L) = \deg_L(A)$, we can rewrite the fraction in the middle using the definition (4.5) of $x(H)$, as

$$\begin{aligned}\frac{\binom{t'+D_0}{t'} g! D_1^{g'} \deg_L B}{\binom{t+D_0}{t} g'! D_1^{g} \deg_L A} &= \left(\frac{\binom{g'+t'}{g'} \widetilde{D}_0^{t'} \widetilde{D}_1^{g'} \deg_L(B)}{\binom{g+t}{g} \widetilde{D}_0^{t} \widetilde{D}_1^{g} \deg_L(A)}\right) \times \widetilde{D}_0^{t-t'} \frac{(g+t)!(t'+D_0)!}{(g'+t')!(t+D_0)!} \left(\frac{\widetilde{D}_1}{D_1}\right)^{g-g'} \\ &= \left(x(H)\widetilde{D}_0\right)^{t-t'} \frac{2^g}{\#\left(\frac{\Gamma_p(S_1)+H}{H}\right) \widetilde{T}_1^{c_W(H)}} \times \frac{(g+t)!(t'+D_0)!}{(g'+t')!(t+D_0)!} \left(\frac{\widetilde{D}_1}{D_1}\right)^{g-g'}.\end{aligned}$$

The fractions $\frac{(g+t)!}{(g'+t')!}$ and $\frac{(t'+D_0)!}{(t+D_0)!}$ are bounded by $(g+t)^{g+t-(g'+t')}$ and $\frac{1}{(1+D_0)^{t-t'}}$ respectively. As $x(H)\widetilde{D}_0 \leqslant \lfloor x(H)\widetilde{D}_0 \rfloor + 1 = 1 + D_0$, we get

$$\frac{(g+t)!(t'+D_0)!}{(g'+t')!(t+D_0)!} (x(H)\widetilde{D}_0)^{t-t'} \leqslant (g+t)^{g+t-(g'+t')}.$$

Finally, from proposition 4.14.3 we have $\widetilde{D}_1 \leqslant D_1 + 1 \leqslant D_1\left(1 + \frac{1}{(2(g+t))^{2g+t+3}}\right)$. Therefore,

$$\begin{aligned}\frac{\mathrm{rk}(U_\sigma)}{\mathrm{h}^0(\overline{G}, M(D_0,D_1))} \leqslant \frac{\#\left(\frac{\Gamma_p(S_0)+H}{H}\right)}{\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)} \frac{T_2+1}{\widetilde{T}_1} \left(\frac{T_0+1}{\widetilde{T}_1}\right)^{c_W(H)-1} \\ \times 2^g (g+t)^{g+t-(g'+t')} \left(1 + \frac{1}{(2(g+t))^{2g+t+3}}\right)^{g-g'}.\end{aligned}$$

From the definition (4.7) of T_0 the fraction $\frac{T_0+1}{\widetilde{T}_1}$ is less than $2(g+t)$. Because $g-g'$ and $t-t'$ are positive by corollary 4.10, and $c_W \leqslant g$, we are left with

$$\begin{aligned}\frac{\mathrm{rk}(U_\sigma)}{\mathrm{h}^0(\overline{G}, M(D_0,D_1))} &\leqslant \frac{\#\left(\frac{\Gamma_p(S_0)+H}{H}\right)}{\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)} \frac{T_2+1}{\widetilde{T}_1} \times 2^{2g-1}(g+t)^{2g+t-1} \underbrace{\left(1 + \frac{1}{(2(g+t))^{2g+t+3}}\right)^{g}}_{\leqslant 1+(1/4)^6 \leqslant 1.001} \\ &\leqslant \frac{\#\left(\frac{\Gamma_p(S_0)+H}{H}\right)}{\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)} \frac{T_2+1}{\widetilde{T}_1} \times 2^{2g-1}(g+t)^{2g+t-1} \cdot 1.001.\end{aligned}$$

To conclude, from the values (4.3) and (4.7), we have $2\widetilde{S_1} + 1 \geqslant 10^6$ and therefore $\frac{2S+1}{2S_1+1} \leqslant \frac{C_0\mathfrak{a}}{0.999 C_0 C_1 \mathfrak{a}} \leqslant \frac{1.01}{C_1}$. We deduce that

$$\frac{\#\left(\frac{\Gamma_p(S_0)+H}{H}\right)}{\#\left(\frac{\Gamma_p(S_1)+H}{H}\right)} \frac{T_2+1}{\widetilde{T}_1} \leqslant \begin{cases} \frac{2S+1}{2S_1+1} \frac{2(g+t)T_1}{\widetilde{T}_1} \leqslant \frac{2.02(g+t)}{C_1} & \text{in the non-periodic case;} \\ \left(\left\lfloor \frac{\widetilde{T}_1}{C_1} \right\rfloor + 1\right) \frac{1}{\widetilde{T}_1} \leqslant \frac{2}{C_1} & \text{in the periodic case,} \end{cases}$$

and using the value $C_1 = (5(g+t))^{2g+t}$ we finally get

$$\frac{\mathrm{rk}(U_\sigma)}{h^0(\overline{G}, M(D_0,D_1))} \leqslant \frac{2.03 \cdot 2^{2g-1}}{5^{2g+t}}.$$

■

5.3 Estimation of the norm of U_σ

In this section we give a bound for the norm of U_σ. As in the previous section, for an embedding σ dividing σ_0, the norms of U_σ and $U_{\overline{\sigma}}$ are the same. We will therefore only consider the case $\sigma \mid \sigma_0$. We begin by a general lemma that we will use extensively throughout the rest of this part of the thesis. It applies with no assumption on the embedding.

Lemma 5.9. *Let K'/k be a finite extension of k and let $\sigma : K' \hookrightarrow \mathbb{C}$ be any embedding of K'. Consider a basis $\boldsymbol{w} := (w_1, \dots, w_g)$ of W_σ such that all the w_i are unitary. Let $s \in H^0(\overline{G_\sigma}, M(D_0, D_1)_\sigma)$, let $(x_0, x_A) \in t_{G_\sigma}$, and let $\tau \in \mathbb{N}^g$. For any $r > 0$, we have*

$$\left|\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(x_0, x_A)\right| \frac{\exp\left(-\frac{\pi}{2} D_1 \|x_A\|^2_\sigma\right)}{(1 + \|x_0\|^2_\sigma)^{D_0/2}} \leqslant \frac{\|s\|_{\infty,\sigma}}{r^{|\tau|}} \exp\left(\frac{\pi}{2} D_1 r(2g\|x_A\|_\sigma + rg^2)\right) \times \left(1 + rg + r^2 g^2\right)^{D_0/2}.$$

Proof. By Cauchy's inequality, we have for any $r > 0$,

$$\left|\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(x_0, x_A)\right| \leqslant \frac{1}{r^{|\tau|}} \sup_{\substack{(z_i)_{1 \leqslant i \leqslant g} \in \mathbb{C}^g \\ |z_i| = r}} \left| s^\star\left((x_0, x_A) + \sum_{i=1}^g z_i w_i\right)\right|.$$

Furthermore, applying (4.10), we get

$$\left|\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(x_0, x_A)\right| \leqslant \frac{\|s\|_{\infty,\sigma}}{r^{|\tau|}} \sup_{\substack{(z_i)_{1 \leqslant i \leqslant g} \in \mathbb{C}^g \\ |z_i| = r}} \exp\left(\frac{\pi}{2} D_1 \left\|x_A + \sum_{i=1}^g z_i w_{i,A}\right\|^2_\sigma\right) \times \left(1 + \left\|x_0 + \sum_{i=1}^g z_i w_{i,0}\right\|^2_\sigma\right)^{D_0/2}.$$

The w_i's are all of norm 1 and therefore $\|w_{i,A}\|_\sigma, \|w_{i,0}\|_\sigma \leqslant 1$. Using the triangle inequality, we have

$$\left\|x_A + \sum_{i=1}^g z_i w_{i,A}\right\|^2_\sigma \leqslant (\|x_A\|_\sigma + gr)^2 \leqslant \|x_A\|^2_\sigma + r(2g\|x_A\|_\sigma + rg^2).$$

Similarly, and using $2\|x_0\|_\sigma \leqslant 1 + \|x_0\|^2_\sigma$, we get

$$1 + \left\|x_0 + \sum_{i=1}^g z_i w_{i,0}\right\|^2_\sigma \leqslant 1 + \|x_0\|^2_\sigma + 2rg\|x_0\|_\sigma + r^2 g^2 \leqslant \left(1 + \|x_0\|^2_\sigma\right)\left(1 + rg + r^2 g^2\right).$$

This gives the result. ∎

Corollary 5.10. *With the same notations as lemma 5.9, for $T \geqslant |\tau|$, we have*

$$\left|\frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(x_0, x_A)\right| \frac{\exp\left(-\frac{\pi}{2} D_1 \|x_A\|^2_\sigma\right)}{(1 + \|x_0\|^2_\sigma)^{D_0/2}} \leqslant \|s\|_{\infty,\sigma} e^T \max\left(1, \frac{2\pi D_1 g\|x_A\|_\sigma + D_0 g}{2T} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T}}\right)^T.$$

Proof. Bounding $(1+rg+r^2g^2)^{D_0/2}$ by $\exp\left(\frac{D_0}{2}(rg+r^2g^2)\right)$, lemma 5.9 gives

$$\left|\frac{1}{\tau!}D^\tau_{\boldsymbol{w}}s^\star(x_0,x_A)\right|\frac{\exp\left(-\frac{\pi}{2}D_1\|x_A\|_\sigma^2\right)}{(1+\|x_0\|_\sigma^2)^{D_0/2}}\leqslant\frac{\|s\|_{\infty,\sigma}}{r^{|\tau|}}\exp\left(ar+br^2\right),$$

with a $=\pi D_1 g\|x_A\|_\sigma+\frac{D_0 g}{2}$, and $b=\frac{\pi D_1 g^2+D_0 g^2}{2}$. Set $r:=\frac{2T}{a+\sqrt{a^2+4bT}}$. It satisfies $ar+br^2=T$. Therefore,

$$\frac{1}{r^{|\tau|}}e^{ar+br^2}=e^T\left(\frac{a+\sqrt{a^2+4bT}}{2T}\right)^{|\tau|}\leqslant e^T\max\left(1,\frac{a}{T}+\sqrt{\frac{b}{T}}\right)^T.$$

In the last inequality we have bounded $\sqrt{x+y}$ by $\sqrt{x}+\sqrt{y}$. ∎

We will use corollary 5.10 in several cases during the proofs of our results. The most annoying term to bound is the one in the max function. The following result gives an upper-bound in the cases we will need.

Lemma 5.11. *For $(S',T')\in\{(S_0,T_0),((g+t)S_1,(g+t)T_1),(E((g+t)S_1+1),(g+t)T_1)\}$, we have*

$$\frac{2\pi gD_1S'\|u_A\|_\sigma+D_0g}{2T'}+\sqrt{\frac{\pi D_1g^2+D_0g^2}{2T'}}\leqslant\sqrt{1+\frac{(2\widetilde{S}+1)\log E}{C_0C_1}}.$$

Proof. Recall that we have $T_0=2(g+t)T_1-1$, and $S_0\leqslant(g+t)S_1$ from the definition (4.7). Therefore, in every case we have $T'\geqslant(g+t)T_1\geqslant\frac{g+t}{2}\widetilde{T}_1$ and $S'\leqslant E((g+t)S_1+1)\leqslant E\widetilde{S}_1(g+t+1)$. Therefore, it is enough to bound

$$\frac{2\pi g\widetilde{D}_1(g+t+1)E\widetilde{S}_1\|u_A\|_\sigma}{(g+t)\widetilde{T}_1}+\frac{g\widetilde{D}_0}{(g+t)\widetilde{T}_1}+\sqrt{\frac{\pi\widetilde{D}_1g^2+\widetilde{D}_0g^2}{(g+t)\widetilde{T}_1}}.$$

Let us begin with the first fraction. From proposition 4.14.2, we have $\widetilde{D}_1\leqslant\frac{\widetilde{T}_1}{C_0C_1}$ and $\widetilde{D}_1E^2\widetilde{S}_1^2\|u_A\|_\sigma^2\leqslant\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}$. Therefore,

$$\begin{aligned}\frac{2\pi g\widetilde{D}_1(g+t+1)E\widetilde{S}_1\|u_A\|_\sigma}{(g+t)\widetilde{T}_1}&\leqslant 2\pi g\left(1+\frac{1}{g+t}\right)\sqrt{\frac{\widetilde{D}_1E^2\widetilde{S}_1^2\|u_A\|_\sigma^2}{\widetilde{T}_1}}\sqrt{\frac{\widetilde{D}_1}{\widetilde{T}_1}}\\&\leqslant\underbrace{\frac{3\pi g}{\sqrt{C_0}}}_{\leqslant 1/\sqrt{2}}\sqrt{\frac{(2\widetilde{S}+1)\log E}{C_0C_1}}\\&\leqslant\sqrt{\frac{(2\widetilde{S}+1)\log E}{2C_0C_1}}.\end{aligned}$$

On the other hand, we have $\widetilde{D}_0\leqslant\frac{\widetilde{T}_1}{C_0C_1}$ and thus

$$\frac{g\widetilde{D}_0}{(g+t)\widetilde{T}_1}+\sqrt{\frac{\pi\widetilde{D}_1g^2+\widetilde{D}_0g^2}{(g+t)\widetilde{T}_1}}\leqslant\frac{1}{C_0C_1}+\sqrt{\frac{(\pi+1)g}{C_0C_1}}\leqslant\frac{1}{\sqrt{2}}.$$

Using the inequality $a+b\leqslant\sqrt{2(a^2+b^2)}$ finally gives the result. ∎

Let us use corollary 5.10 and lemma 5.9 to estimate the norm of U_σ. First recall a simple lemma on norms of linear maps.

Lemma 5.12. *Let $(E, \|\cdot\|)$ be a Hermitian vector space and let $U : E \to \mathbb{C}^n$ be a linear map. We have*

$$\|U\| \leqslant \sqrt{n} \sup_{\substack{1 \leqslant i \leqslant n \\ s \in E \setminus \{0\}}} \frac{|(Us)_i|}{\|s\|},$$

where $(Us)_i$ denotes the i-th component of Us in $\mathbb{C}^n$.

Proof. Let $s \in E$. We have

$$\|Us\|_2^2 = \sum_{i=1}^{n} |(Us)_i|^2 \leqslant n \sup_{1 \leqslant i \leqslant n} |(Us)_i|^2.$$

The result then follows directly from the definition of the norm of $\|U\|$. ∎

Let $\sigma : K \hookrightarrow \mathbb{C}$ extending σ_0. Applying lemma 5.12, the norm of U_σ is therefore bounded by

$$\sqrt{\#\Upsilon} \sup_{\substack{(m,\tau) \in \Upsilon \\ s \neq 0}} \left| \frac{1}{\tau! \|s\|_{2,\sigma}} D^\tau_{\mathbf{w}_\sigma} s^\star(mu) \frac{\exp\left(-\frac{\pi}{2} D_1 \|mu_A\|_\sigma^2\right)}{(1 + \|mu_0\|_\sigma^2)^{D_0/2}} \right|.$$

The following bounds the supremum

Proposition 5.13. *We have*

$$\sup_{\substack{(m,\tau) \in \Upsilon \\ s \neq 0}} \left| \frac{1}{\tau! \|s\|_{2,\sigma}} D^\tau_{\mathbf{w}_\sigma} s^\star(mu) \frac{\exp\left(-\frac{\pi}{2} D_1 \|mu_A\|_\sigma^2\right)}{(1 + \|mu_0\|_\sigma^2)^{D_0/2}} \right| \leqslant \exp\left(\frac{\widetilde{T}_1 (2\widetilde{S} + 1) \log E}{C_0} \times 2.01(g+t) \right) \times \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

Proof. Let us write C the quantity we want to bound. We first apply corollary 5.10 with $T = T_0$:

$$\begin{aligned} C &\leqslant \sup_{\substack{m \in \mathbb{Z}, |m| \leqslant S_0 \\ s \neq 0}} \frac{\|s\|_{\infty,\sigma}}{\|s\|_{2,\sigma}} e^{T_0} \max\left(1, \frac{2\pi D_1 g \|mu_A\|_\sigma + D_0 g}{2T_0} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T_0}}\right)^{T_0} \\ &\leqslant \left(\sup_{s \neq 0} \frac{\|s\|_{\infty,\sigma}}{\|s\|_{2,\sigma}} \right) e^{T_0} \max\left(1, \frac{2\pi D_1 g S_0 \|u_A\|_\sigma + D_0 g}{2T_0} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T_0}}\right)^{T_0}. \end{aligned}$$

Lemma 5.11 gives a bound for the max, and the inequalities $\log(1+x) \leqslant x$, and $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}$

from proposition 4.14.4 give

$$e^{T_0}\max\left(1,\frac{2\pi D_1 g S_0\|u_A\|_\sigma + D_0 g}{2T_0}+\sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T_0}}\right)^{T_0}$$
$$\leqslant \exp\left(T_0\left(1+\frac{1}{2}\log\left(1+\frac{(2\widetilde{S}+1)\log E}{C_0C_1}\right)\right)\right)$$
$$\leqslant \exp\left(2(g+t)\widetilde{T}_1\left(1+\frac{(2\widetilde{S}+1)\log E}{2C_0C_1}\right)\right)$$
$$\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2(g+t)\left(1+\frac{1}{2C_1}\right)\right).$$

On the other hand, lemma 4.18 allows us to bound the term $\sup_{s\neq 0}\frac{\|s\|_{\infty,\sigma}}{\|s\|_{2,\sigma}}$. We deduce with the value (4.2) of C_1 that

$$C\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\underbrace{\left(\frac{2(g+t)}{C_1}+2(g+t)+\frac{1}{DC_1}\right)}_{\leqslant 2.01(g+t)}\right)\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

■

To conclude this section, we have to bound the remaining term $\sqrt{\#\Upsilon}$.

Proposition 5.14. *We have* $\sqrt{\#\Upsilon}\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{8C_0}\right)$.

Proof. From lemma 3.38 and lemma 3.39, we have

$$\#\Upsilon=(2S_0+1)\left(\binom{T_0+g}{g}-\binom{T_0-T_2+g-1}{g}\right)\leqslant (2S_0+1)(T_2+1)(T_0+1)^{g-1}.$$

We check that in both the periodic and the non-periodic case, the right-hand side is bounded by $(2(g+t))^g\widetilde{T}_1^g(2\widetilde{S}+1)\log E$. From the inequality $(2\widetilde{S}+1)\log E\geqslant C_0$ of proposition 4.14.4, we then have

$$\#\Upsilon\leqslant (2(g+t))^g\widetilde{T}_1^g(2\widetilde{S}+1)\log E$$
$$\leqslant \frac{1}{(g+1)!}\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{4C_0}\right)^{g+1}\times\frac{(2(g+t))^g(g+1)!4^{g+1}C_0}{\widetilde{T}_1}$$
$$\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{4C_0}\right)\times\frac{2^{3g+2}(g+t)^g(g+1)^gC_0}{\widetilde{T}_1}.$$

From the lower bound of proposition 4.14.1 and the value of C_0, we finally bound the fraction:

$$\frac{2^{3g+2}(g+t)^g(g+1)^gC_0}{\widetilde{T}_1}\leqslant\frac{2^{3g+2}5^3(g+t)^{2g+3}}{(2(g+t))^{4g+2t+6}}\leqslant 1.$$

■

Combining proposition 5.13 and proposition 5.14, we get

Proposition 5.15. *For any $\sigma : K \hookrightarrow \mathbb{C}$ extending σ_0 or $\overline{\sigma_0}$, we have*

$$\|U_\sigma\| \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 2.1(g+t)\right) \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

5.4 Estimation of the slopes

We bound here the term $\frac{1}{2}\log \mathrm{rk}\, E - \widehat{\mu}(\overline{E})$ that appear in lemma 5.4.

Proposition 5.16. *We have*

$$\frac{1}{2}\log \mathrm{h}^0(\overline{G}, M(D_0, D_1)) - \widehat{\mu}\left(\overline{H^0(\overline{\mathcal{E}}, \mathcal{M}(D_0, D_1))}\right) = \left(\frac{1}{2} - \frac{D_0}{t+1}\right)\left(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A, L)\right) + \frac{g}{4}\log(2\pi^2 D_1) - \frac{1}{2}\log \gamma_{t,D_0} + \frac{D_0 h(W_0)}{t+1}.$$

In particular,

$$\frac{1}{2}\log \mathrm{h}^0(\overline{G}, M(D_0, D_1)) - \widehat{\mu}\left(\overline{H^0(\overline{G}, M(D_0, D_1))}\right) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}.$$

Proof. Using theorem 3.26.4, proposition 3.33, and the fact that normalised Arakelov slope turns tensor products into sums (see proposition 3.5), we have

$$\widehat{\mu}\left(\overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))}\right) = -\frac{1}{2}h_F(A) + \frac{1}{4}\log \mathrm{h}^0(A, L) - \frac{g}{4}\log\left(\frac{2\pi^2}{D_1}\right) + \frac{1}{2}\log\binom{t+D_0}{t} - D_0\frac{\widehat{\deg}_{\mathrm{n}}(\overline{t_{\mathcal{A}}}) - \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{W}_0})}{t+1} + \frac{1}{2}\log \gamma_{t,D_0}.$$

Moreover,

$$\log \mathrm{h}^0(\overline{G}, M(D_0, D_1)) = \log\binom{t+D_0}{t} + g\log D_1 + \log \mathrm{h}^0(A, L),$$

and from proposition 3.27

$$\widehat{\deg}_{\mathrm{n}}\left(\overline{t_{\mathcal{A}}}\right) = -\left(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A, L)\right).$$

Combining these identities, we get

$$\frac{1}{2}\log \mathrm{h}^0(\overline{G}, M(D_0, D_1)) - \widehat{\mu}\left(\overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))}\right) = \left(\frac{1}{2} - \frac{D_0}{t+1}\right)\left(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A, L)\right) + \frac{g}{4}\log(2\pi^2 D_1) - \frac{1}{2}\log \gamma_{t,D_0} + \frac{D_0 h(W_0)}{t+1}.$$

This gives the first part of the proposition. We then have from proposition 4.14.2, $D_1 \leqslant \frac{\widetilde{T}_1}{C_0 C_1}$, $D_0 h(W_0) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0 D}$, and $\gamma_{t,D_0} \geqslant 1$. Because $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0}$ from proposition 4.14.4, we

have

$$\frac{g}{4}\log(2\pi^2 D_1) - \frac{1}{2}\log\gamma_{t,D_0} - \frac{D_0\,\widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{W}}_0)}{t+1} \leqslant \frac{\pi^2 g\widetilde{T}_1}{2C_0C_1} + \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{(t+1)DC_0}$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\Big(\underbrace{\frac{1}{t+1} + \frac{\pi^2 g}{2C_0C_1}}_{\leqslant 3/4}\Big).$$

Next, we use propositions 4.14.3 and 4.14.2 to get

$$-\frac{\widetilde{T}_1}{C_0C_1(t+1)} \leqslant \frac{1}{2} - \frac{D_0}{t+1} \leqslant 0.$$

On the other hand, using Bost's bound of proposition 3.24, we have

$$h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A,L) \geqslant -\frac{g}{2}\log(2\pi^2).$$

Therefore,

$$\Big(\frac{1}{2} - \frac{D_0}{t+1}\Big)\Big(h_F(A) + \frac{1}{2}\log \mathrm{h}^0(A,L)\Big) \leqslant \frac{g\log(2\pi^2)\widetilde{T}_1}{2(t+1)C_0C_1}$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1} \times \frac{g\log(2\pi^2)}{2(t+1)C_0}$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1}.$$

Combining this with the other upper-bound, we finally get

$$\frac{1}{2}\log \mathrm{h}^0(\overline{G}, M(D_0,D_1)) - \widehat{\mu}\Big(\overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0,D_1))}\Big)$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1} + \frac{3\widetilde{T}_1(2\widetilde{S}+1)\log E}{4DC_0}$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}.$$

■

5.5 Construction of the auxiliary section

We are now ready to apply the lemma 5.4.

Proposition 5.17. *Let $\alpha \geqslant 1$ be such that $\log\alpha = \widetilde{T}_1(2\widetilde{S}+1)\log E \times 3(g+t)^3$. There exists a section $s \in H^0(\overline{G}, M(D_0,D_1)) \otimes \overline{K}$, $s \neq 0$ such that*

$$h_\alpha(s) \leqslant 1.6 \times \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} + \frac{g}{2D}\log^+\frac{1}{\rho(A_{\sigma_0}, L_{\sigma_0}^{\otimes D_1})}.$$

Proof. We apply lemma 5.4 to $\overline{\mathcal{E}} = \overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))}$, $\overline{\mathcal{F}} = \overline{\mathcal{O}_K^{\Upsilon}}$, $S = \{\sigma : K \hookrightarrow \mathbb{C}, \sigma \mid \sigma_0, \overline{\sigma_0}\}$, and $a_\sigma = \alpha U_\sigma$. There exists a non-zero section $s \in H^0(\overline{G}, M(D_0, D_1)) \otimes \overline{K}$ such that

$$h_\alpha(s) \leqslant \frac{[k_{\sigma_0} : \mathbb{R}]}{[K : \mathbb{Q}]} \sum_{\sigma \mid \sigma_0} \frac{\mathrm{rk}(U_\sigma)}{\mathrm{h}^0(\overline{G}, M(D_0, D_1))} \left(\log^+ \|U_\sigma\| + \log \alpha + \log \sqrt{2} \right) + \frac{1}{2} \log \mathrm{h}^0(\overline{G}, M(D_0, D_1)) - \widehat{\mu} \left(\overline{H^0(\overline{\mathcal{G}}, \mathcal{M}(D_0, D_1))} \right).$$

We have $[k_{\sigma_0} : \mathbb{R}] \leqslant 2$. Combining propositions 5.8, 5.15 and 5.16, we get

$$h_\alpha(s) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1) \log E}{D} \left(2 \cdot \frac{2.03 \cdot 2^{2g-11}}{5^{2g+t}} \left(\frac{2.1(g+t)}{C_0} + 3(g+t)^3 + \log \sqrt{2} \right) + \frac{1}{C_0} \right) + 2 \cdot \frac{2.03 \cdot 2^{2g-1}}{5^{2g+t}} \frac{g}{2D} \log^+ \frac{1}{\rho(A_{\sigma_0}, L_{\sigma_0}^{\otimes D_1})}.$$

To conclude, the term in the first pair of brackets is maximal at $g = t = 1$ and is smaller than 1.6, and we also have $\frac{2.03 \cdot 2^{2g}}{5^{2g+t}} \leqslant 2.03 \cdot \frac{4}{5^3} \leqslant 1$. ∎

Chapter 6

Jets of sections

6.1 The jets hermitian vector bundle

Consider the section s constructed in the previous chapter. It is defined over some extension K' of K. The degree of this extension will again not matter as it will disappear in the computation some height function. By lemma 4.16, there exists some pair $(m,\ell) \in \mathbb{Z}\times\mathbb{N}$ with $|m| \leqslant (g+t)S_1$ and $\ell \leqslant (g+t)T_1$ such that the section s does not vanish at mp at order $\ell+1$ along W. Let (m,ℓ) be minimal for the lexicographic order on $\{-(g+t)S_1,\dots,(g+t)S_1\}\times\{0,\dots,(g+t)T_1\}$ and such that s does not vanish at mp at order $\ell+1$. We consider the ℓ-th jet of s at the point mp. We refer to [Gau06, §5.6. Choix de l'espace des jets et de sa filtration] for the algebraic definition of the space $\mathrm{Jet}^\ell_{\mathcal{W}}(mp)$ of jets of order ℓ at the point mp along W. Let us recall the main properties of it.

Proposition 6.1 ([Gau06, §5.6])**.**

- *The Hermitian adelic vector bundle* $\overline{\mathrm{Jet}^\ell_{\mathcal{W}}(mp)}$ *is isometrically isomorphic to the one given by* $\overline{\mathrm{Sym}^\ell(\mathcal{W}^\vee)\otimes(mp)^\star\mathcal{M}(D_0,D_1)}$.
- *We have a morphism* $s\mapsto \mathrm{jet}^\ell_W\, s(mp)$ *from the space of sections* $s\in H^0(\mathcal{G},\mathcal{M}(D_0,D_1))$ *that vanishes at order* ℓ *at the point* mp *along* W*, to* $\mathrm{Jet}^\ell_{\mathcal{W}}(mp)$.
- *For any such section* s *defined over* K'*, any Archimedean place* σ *of* K'*, any basis* $\boldsymbol{w}=(\boldsymbol{w}_1,\dots,\boldsymbol{w}_g)$ *of* W_σ*, and any logarithm* $v=(v_0,v_A)$ *of* mp *in* t_{G_σ}*, the norm of* $\mathrm{jet}^\ell_W\, s(mp)$ *is equal to*

$$\|\mathrm{jet}^\ell_W\, s(mp)\|_\sigma = \frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|^2_\sigma\right)}{(1+\|v_0\|^2_\sigma)^{D_0/2}}\left\|\sum_{\tau\in\mathbb{N}^g,|\tau|=\ell}\frac{1}{\tau!}D^\tau_{\boldsymbol{w}}s^\star_\sigma(v)(\boldsymbol{w}_1^\vee)^{\tau_1}\cdots(\boldsymbol{w}_g^\vee)^{\tau_g}\right\|_{\mathrm{Sym}^\ell(W^\vee_\sigma)}. \tag{6.1}$$

  This definition is independent of the basis $\boldsymbol{w}$ *and the logarithm* v.

The crucial point of the rest of the proof is the inequality of proposition 3.10. In our context it states

$$h(\mathrm{jet}^\ell_W\, s(mp)) \geqslant -\widehat{\mu}_{\max}\left(\overline{\mathrm{Jet}^\ell_{\mathcal{W}}(mp)}\right). \tag{6.2}$$

The following result gives an upper-bound for the maximal slope of the jet bundle.

Proposition 6.2. *The maximal slope of* $\overline{\mathrm{Jet}^{\ell}_{\mathcal{W}}(mp)}$ *is bounded by*

$$\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\times(g+t)^4.$$

Proof. From proposition 3.11, we have

$$\widehat{\mu}_{\max}\left(\overline{\mathrm{Jet}^{\ell}_{\mathcal{W}}(mp)}\right)=\widehat{\mu}_{\max}\left(\overline{\mathrm{Sym}^{\ell}(\mathcal{W}^{\vee})}\right)+\widehat{\deg}_{\mathrm{n}}\left(\overline{(mp)^{\star}\mathcal{M}(D_0,D_1)}\right). \tag{6.3}$$

From theorem 3.26.2, proposition 3.31, and remark 3.32, the Arakelov degree of $\overline{(mp)^{\star}\mathcal{M}(D_0,D_1)}$ is equal to

$$\begin{aligned}\widehat{\deg}_{\mathrm{n}}\left(\overline{(mp)^{\star}\mathcal{M}(D_0,D_1)}\right)&=D_0h_{\mathcal{O}(1)}(mp_0)+D_1\widehat{h}_L(mp_A)\\&\leqslant D_0h_{\mathcal{O}(1)}(p_0)+D_0\log|m|+D_1m^2\widehat{h}_L(p_A).\end{aligned} \tag{6.4}$$

Moreover, by proposition 3.12 we have the upper-bound

$$\widehat{\mu}_{\max}\left(\overline{\mathrm{Sym}^{\ell}(\mathcal{W}^{\vee})}\right)\leqslant\ell\left(\widehat{\mu}_{\max}(\overline{\mathcal{W}^{\vee}})+2\log g\right). \tag{6.5}$$

To estimate the maximal slope of $\overline{\mathcal{W}^{\vee}}$, let $i^{\vee}$ be the dual application of the inclusion $t_A\to W$ defined by $x\mapsto(\lambda(x),x)$. By [Gau08, Lemme 6.3] we have

$$\widehat{\mu}_{\max}\left(\overline{\mathcal{W}^{\vee}}\right)\leqslant\widehat{\mu}_{\max}\left(\overline{t^{\vee}_{\mathcal{A}}}\right)+h(i^{\vee}), \tag{6.6}$$

where the height of $i^{\vee}$ is equal to $h(i^{\vee}):=\frac{1}{D}\sum_v[k_v:\mathbb{Q}_v]\log\|i^{\vee}\|_v$. By definition, we have

$$\|i^{\vee}\|_v=\sup_{\varphi\in W_v^{\vee}\setminus\{0\}}\sup_{x\in t_{A_v}\setminus\{0\}}\frac{|\varphi(\lambda(x),x)|}{\|\varphi\|_v\|x\|_v}\leqslant\sup_{x\in t_{A_v}\setminus\{0\}}\frac{\|(\lambda(x),x)\|_v}{\|x\|_v}.$$

If v is Archimedean we have $\|(\lambda(x),x)\|_v\leqslant\sqrt{2}\|x\|_v$ and thus $\|i^{\vee}\|_v\leqslant\sqrt{2}$. If v is non-Archimedean we have $\|(\lambda(x),x)\|_v\leqslant\max(\|\lambda(x)\|_v,\|x\|_v)\leqslant\|x\|_v$ and therefore $\|i^{\vee}\|_v\leqslant1$. We thus get

$$h(i^{\vee})\leqslant\frac{1}{D}\sum_{v\text{ non-Arch.}}[k_v:\mathbb{Q}_v]\log1+\frac{1}{D}\sum_{v\text{ Arch.}}[k_v:\mathbb{R}]\log\sqrt{2}\leqslant\log\sqrt{2}. \tag{6.7}$$

Combining (6.3), (6.4), (6.5), (6.6), and (6.7), we get

$$\widehat{\mu}_{\max}\left(\overline{\mathrm{Jet}^{\ell}_{\mathcal{W}}(mp)}\right)\leqslant\ell\left(\widehat{\mu}_{\max}\left(\overline{t^{\vee}_{\mathcal{A}}}\right)+\log\sqrt{2}+2\log g\right)+D_0h_{\mathcal{O}(1)}(p_0)+D_0\log|m|+D_1m^2\widehat{h}_L(p_A).$$

From proposition 3.28, we can bound the maximal slope of $\overline{t^{\vee}_{\mathcal{A}}}$ by

$$\widehat{\mu}_{\max}\left(\overline{t^{\vee}_{\mathcal{A}}}\right)\leqslant(0.6g+1)\left(h_F(A)+\frac{1}{2}\log\mathrm{h}^0(A,L)\right)+g^2\log(10g).$$

We have $\ell\leqslant(g+t)\widetilde{T}_1$, and using proposition 4.14.4, 1, $h_F(A)$, and $\log\mathrm{h}^0(A,L)$ are bounded by $\frac{(2\widetilde{S}+1)\log E}{DC_0}$. Therefore,

$$\begin{aligned}\ell\left(\widehat{\mu}_{\max}\left(\overline{t^{\vee}_{\mathcal{A}}}\right)+\log\sqrt{2}+2\log g\right)\leqslant\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}(g+t)\Bigg(&\frac{3}{2}(0.6g+1)+g^2\log(10g)\\&+\log\sqrt{2}+2\log g\Bigg).\end{aligned}$$

Dividing the term in parentheses by $(g+t)^3$, we see that it is less than $0.64(g+t)^3$.

Finally, we have $|m| \leqslant (g+t)S_1$. Therefore, from the definition (4.4) of $\widetilde{D}_1$ and $\widetilde{D}_0$, we have $D_0(h_{\mathcal{O}(1)}(p_0) + \log|m|) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\left(1 + \frac{\log(g+t)}{C_1}\right)$ and $D_1 m^2 \widehat{h}_L(p_A) \leqslant (g+t)^2 \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}$. Therefore,

$$D_0 h_{\mathcal{O}(1)}(p_0) + D_0 \log|m| + D_1 m^2 \widehat{h}_L(p_A) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0} \underbrace{\left(1 + \frac{\log(g+t)}{C_1} + (g+t)^2\right)}_{\leqslant 1.26(g+t)^2}.$$

Thus, the maximal slope of $\overline{\mathrm{Jet}^\ell_{\mathcal{W}}(mp)}$ is bounded by

$$\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\left(0.64(g+t)^4 + 1.26(g+t)^2\right) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0} \times (g+t)^4.$$

■

Now that we have bounded the maximal slope, we are going to estimate the height of the jet of the section s. We split the computation in three distinct parts. We first bound the norm of the jet with respect to the non-Archimedean places. Next we look at the norm of the jet at an Archimedean place dividing neither σ_0, nor $\overline{\sigma_0}$. Finally – and this will be the more tedious and important part – we estimate the norm of the jet with respect to an Archimedean place dividing σ_0 or $\overline{\sigma_0}$.

6.2 Non-Archimedean estimates

For two integers ℓ and h, we define the integer

$$\delta_\ell(h) := \mathrm{lcm}\left\{i_1 \cdots i_{h'}, 1 \leqslant h' \leqslant h, i_1, \ldots, i_{h'} \geqslant 1, i_1 + \cdots + i_{h'} \leqslant \ell\right\}.$$

The following estimate has been obtained by Gaudron using Chudnovsky change of variables.

Proposition 6.3 ([Gau06, Proposition 5.10])**.** *Let $\mathfrak{P}$ be a finite place of K'. We have*

$$\|\delta_\ell(D_0)\,\mathrm{jet}^\ell_W\, s(mp)\|_{\mathfrak{P}} \leqslant \|s\|_{\mathfrak{P}} = \|s\|_{\alpha,\mathfrak{P}}.$$

At the end of the proof we will need an upper-bound for the (real) absolute value of $\delta_\ell(D_0)$. A theorem of Bruiltet gives us such a bound.

Proposition 6.4 ([Bru02, Proposition 1])**.** *Let ℓ, h be two non-negative integers. We have*

$$\log \delta_\ell(h) \leqslant \ell \log(4h).$$

Lemma 6.5. *We have*

$$\log|\delta_\ell(D_0)| \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} \times 0.06(g+t).$$

Proof. From proposition 4.14.7, we have $\log D_0 \leqslant 7(g+t)^3 \frac{(2\widetilde{S}+1)\log E}{DC_0}$. Therefore, using proposition 6.4 we get

$$\begin{aligned}\log|\delta_\ell(D_0)| &\leqslant \ell \log(4D_0)\\ &\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} \times \frac{(g+t)(\log(4)+7(g+t)^3)}{C_0}.\end{aligned}$$

Using the value $C_0 = (5(g+t))^3$, we can bound the constant:

$$\frac{(g+t)\log(4)+7(g+t)^4}{C_0} = (g+t)\left(\frac{\log(4)}{(5(g+t))^3}+\frac{7}{5^3}\right) \leqslant 0.06(g+t).$$

■

6.3 Archimedean estimates at the places $\sigma \nmid \sigma_0,\ \overline{\sigma_0}$

We bound here the norm of $\operatorname{jet}^\ell_W s(mp)$ corresponding to an Archimedean place σ of K' not dividing σ_0 nor $\overline{\sigma_0}$. Let $\sigma : K' \hookrightarrow \mathbb{C}$ be an embedding dividing neither σ_0, nor $\overline{\sigma_0}$. The basis $\mathbf{w}_\sigma$ of W_σ defined in section 5.1 is an orthonormal basis of W_σ. Let $v := (v_0, v_A) \in t_{G_\sigma}$ be any logarithm of mp. From the definition (6.1) of $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ and because $\mathbf{w}_\sigma$ is orthonormal, we have

$$\begin{aligned}\|\operatorname{jet}^\ell_W s(mp)\|_\sigma &= \frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|^2_\sigma\right)}{(1+\|v_0\|^2_\sigma)^{D_0/2}} \sqrt{\sum_{\tau\in\mathbb{N}^g,|\tau|=\ell} \left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(v)\right|^2 \frac{\tau_1!\cdots\tau_g!}{\ell!}}\\ &\leqslant \sup_{\tau\in\mathbb{N}^g,|\tau|=\ell} \frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|^2_\sigma\right)}{(1+\|v_0\|^2_\sigma)^{D_0/2}} \left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(v)\right| \times \sqrt{\binom{g+\ell-1}{g-1}}.\end{aligned} \tag{6.8}$$

Note that the binomial coefficient comes from the upper-bound $\frac{\tau_1!\cdots\tau_g!}{\ell!} \leqslant 1$, together with lemma 3.38.1. Using lemma 3.39 and the lower bounds $\widetilde{T}_1 \geqslant (2(g+t))^{4g+2t+6}$ and $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{DC_0}$ from proposition 4.14.1 and proposition 4.14.4, we have

$$\begin{aligned}\sqrt{\binom{g+\ell-1}{g-1}} \leqslant (\ell+1)^{(g-1)/2} &\leqslant ((g+t)T_1+1)^{(g-1)/2}\\ &\leqslant \sqrt{\frac{1}{g!}\left(\frac{\widetilde{T}_1}{2^6}\right)^g} \times \frac{2^{3g}(g+t+1)^{(g-1)/2}\sqrt{g!}}{\widetilde{T}_1^{1/2}}\\ &\leqslant e^{\widetilde{T}_1/2^7} \times \sqrt{\frac{2^{6g}(g(g+t+1))^{g-1}}{(2(g+t))^{4g+2t+6}}}\\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2^7 DC_0}\right).\end{aligned} \tag{6.9}$$

We now treat the derivative part of (6.8). As we can choose any logarithm of mp in (6.8), we take $v := (v_0, v_A)$ of norm as small as possible. As Ω_{A_σ} is the kernel of $\exp_{A_\sigma}$, the norm of v_A satisfies

$$\|v_A\|_\sigma \leqslant r(A_\sigma, L_\sigma) := \sup_{x\in t_{A_\sigma}} d(x, \Omega_{A_\sigma}).$$

Using corollary 5.10 we get the following result.

Proposition 6.6. *Let $\tau \in \mathbb{N}^g$ be such that $|\tau| = \ell$. We have*

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|_\sigma^2\right)}{(1+\|v_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(v)\right| \leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\times 1.005(g+t)\right)$$
$$\times\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)^{(g+t)\widetilde{T}_1}\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

Proof. We apply corollary 5.10 with $\boldsymbol{w}=\mathbf{w}_\sigma$, $(x_0,x_A)=v$, and $T=(g+t)T_1$, to get

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|_\sigma^2\right)}{(1+\|v_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(v)\right| \leqslant \|s\|_{\infty,\sigma}e^{(g+t)T_1}\max\left(1,\frac{2\pi D_1 g\|v_A\|_\sigma+D_0 g}{2(g+t)T_1}\right.$$
$$\left.+\sqrt{\frac{\pi D_1 g^2+D_0 g^2}{2(g+t)T_1}}\right)^{(g+t)T_1}.$$

The upper-bound 4.14.2 gives $\frac{D_i}{T_1}\leqslant\frac{2\widetilde{D}_i}{\widetilde{T}_1}\leqslant\frac{2}{C_0C_1}$, for $i=0,\,1$, and leads to

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|_\sigma^2\right)}{(1+\|v_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(v)\right|$$
$$\leqslant \|s\|_{\infty,\sigma}e^{(g+t)T_1}\max\left(1,\frac{2\pi g\|v_A\|_\sigma+g}{(g+t)C_0C_1}+\sqrt{\frac{g^2(\pi+1)}{(g+t)C_0C_1}}\right)^{(g+t)T_1}$$
$$\leqslant \|s\|_{\infty,\sigma}e^{(g+t)T_1}\max\left(1,\frac{2\pi\|v_A\|_\sigma}{C_0C_1}+1\right)^{(g+t)T_1}.$$

We finally use lemma 4.18 to bound $\|s\|_{\infty,\sigma}$ in terms of $\|s\|_{2,\sigma}$ and proposition 4.14.4 to get

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|v_A\|_\sigma^2\right)}{(1+\|v_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(v_\sigma)\right| \leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1}+(g+t)T_1\right)$$
$$\times\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)^{(g+t)\widetilde{T}_1}\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}$$
$$\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\left(\frac{1}{C_1}+g+t\right)\right)$$
$$\times\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)^{(g+t)\widetilde{T}_1}\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

Bounding $\frac{1}{C_1}$ by $0.005(g+t)$ gives the result. ∎

As for an embedding $\sigma \nmid \sigma_0$, or $\overline{\sigma_0}$, $\|s\|_{2,\sigma}=\|s\|_{\alpha,\sigma}$, we deduce an upper-bound for the norm the jet.

Proposition 6.7. *For $\sigma : K' \hookrightarrow \mathbb{C}$ not dividing σ_0 and $\overline{\sigma_0}$ we have*

$$\|\operatorname{jet}^{\ell}_{W} s(mp)\|_{\sigma} \leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0} \times 1.01(g+t)\right) \times \left(\frac{2\pi}{C_0C_1} r(A_\sigma, L_\sigma) + 1\right)^{(g+t)\widetilde{T}_1} \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2}.$$

6.4 Archimedean estimates at the places $\sigma \mid \sigma_0$ or $\overline{\sigma_0}$

We now focus on bounding the Archimedean norm of the jet of s at the places above σ_0 and $\overline{\sigma_0}$. As before we only need to consider the case $\sigma \mid \sigma_0$, the other one being exactly the same by remark 5.2. In order for the distance of the point u to W_σ to appear, we shift our jet from the point p to the point $w := (\lambda(u_A), u_A) \in W_\sigma$.

6.4.1 Change of point

Proposition 6.8. *Let $\sigma : K' \hookrightarrow \mathbb{C}$ be a complex embedding of K' dividing σ_0 or $\overline{\sigma_0}$. Let $w := (\lambda(u_A), u_A) \in W_\sigma$. Let $(j,\tau) \in \mathbb{Z} \times \mathbb{N}^g$, let $T \geqslant |\tau|$, and assume $|j| D_0 d(u, W_{\sigma_0})\sqrt{2} \leqslant 1$. We have*

$$\left|\frac{1}{\tau!} D^{\tau}_{\mathbf{w}_\sigma} s^{\star}_{\sigma}(ju) - \frac{1}{\tau!} D^{\tau}_{\mathbf{w}_\sigma} s^{\star}_{\sigma}(jw)\right| \frac{\exp\left(-\frac{\pi}{2} D_1 \|ju_A\|^2_\sigma\right)}{(1+\|ju_0\|^2_\sigma)^{D_0/2}} \leqslant 3.8 d(u, W_{\sigma_0}) |j| D_0 \|s\|_{\infty,\sigma} \times e^T \max\left(1, \frac{2\pi g D_1 \|ju_A\|_\sigma + D_0 g}{2T} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T}}\right)^T.$$

Proof. If $j = 0$, there is nothing to prove. Therefore, assume $j \neq 0$. Let us first compare the distance between u and w to the distance from u to W_{σ_0}. Let $w_0 = (\lambda(x_0), x_0) \in W_{\sigma_0}$ be the point of W_{σ_0} minimising the distance between u and a point of W_{σ_0}. We then have

$$\begin{aligned} \|u - w\|_\sigma = \|\lambda(u_A) - u_0\|_\sigma &\leqslant \|\lambda(u_A) - \lambda(x_0)\|_\sigma + \|\lambda(x_0) - u_0\|_\sigma \\ &\leqslant \|u_A - x_0\|_\sigma + \|\lambda(x_0) - u_0\|_\sigma \\ &\leqslant \sqrt{2} d(u, W_{\sigma_0}). \end{aligned}$$

We define the holomorphic function

$$F : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{1}{\tau!} D^{\tau}_{\mathbf{w}_\sigma} s^{\star}_{\sigma}\left(ju + z\frac{w-u}{\|w-u\|_\sigma}\right) \end{array} \right. .$$

The function $z \mapsto \frac{F(0)-F(z)}{z}$ is holomorphic on $\mathbb{C}$ and from the maximum modulus principle we deduce that for any real number $X \geqslant |j|\|u-w\|_\sigma$,

$$\begin{aligned} \left|\frac{1}{\tau!} D^{\tau}_{\mathbf{w}_\sigma} s^{\star}_{\sigma}(ju) - \frac{1}{\tau!} D^{\tau}_{\mathbf{w}_\sigma} s^{\star}_{\sigma}(jw)\right| &= |j|\|u-w\|_\sigma \left|\frac{F(0) - F(j\|u-w\|_\sigma)}{j\|u-w\|_\sigma}\right| \\ &\leqslant \sqrt{2}|j| d(u, W_{\sigma_0}) \sup_{|z|=X} \left|\frac{F(0)-F(z)}{z}\right|. \end{aligned}$$

Using corollary 5.10 with $\boldsymbol{w} = \mathbf{w}_\sigma$, $(x_0, x_A) = \left(ju_0 + z\frac{\lambda(u_A)-u_0}{\|\lambda(u_A)-u_0\|_\sigma}, ju_A\right)$, and $T \geqslant |\tau|$ to bound $|F(z)|$ for any $z \in \mathbb{C}$, we get

$$\begin{aligned}|F(z)| &= \left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma\left(ju_0 + z\frac{\lambda(u_A)-u_0}{\|\lambda(u_A)-u_0\|_\sigma}, ju_A\right)\right| \\ &\leqslant \|s\|_{\infty,\sigma}\exp\left(\frac{\pi}{2}D_1\|ju_A\|^2_\sigma\right)\left(1 + \left\|ju_0 + z\frac{\lambda(u_A)-u_0}{\|\lambda(u_A)-u_0\|_\sigma}\right\|^2_\sigma\right)^{D_0/2} \\ &\quad \times e^T \max\left(1, \frac{2\pi D_1 g\|ju_A\|_\sigma + D_0 g}{2T} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T}}\right)^T.\end{aligned}$$

By the triangle inequality, we have

$$1 + \left\|ju_0 + z\frac{\lambda(u_A)-u_0}{\|\lambda(u_A)-u_0\|_\sigma}\right\|^2_\sigma \leqslant 1 + \|ju_0\|^2_\sigma + 2\|ju_0\|_\sigma|z| + |z|^2 \leqslant (1 + \|ju_0\|^2_\sigma)(1 + X + X^2).$$

To conclude, we just have to bound $\frac{1+(1+X+X^2)^{D_0/2}}{X}$ for some $X \geqslant |j|\|u-w\|_\sigma$. Let us choose $X = \frac{1}{D_0}$. It is indeed bigger than $|j|\|u-w\|_\sigma$ under the assumption $d(u, W_{\sigma_0})|j|D_0\sqrt{2} \leqslant 1$. With this value of X we have

$$\begin{aligned}\frac{1+(1+X+X^2)^{D_0/2}}{X} &= D_0\left(1 + \left(1 + \frac{1}{D_0} + \frac{1}{D_0^2}\right)^{D_0/2}\right) \\ &= D_0\left(1 + \exp\left(\frac{D_0}{2}\log\left(1 + \frac{1}{D_0} + \frac{1}{D_0^2}\right)\right)\right) \\ &\leqslant D_0\left(1 + \exp\left(\frac{1}{2} + \frac{1}{2D_0}\right)\right).\end{aligned}$$

Using the lower bound $D_0 \geqslant (2(g+t))^3 \geqslant 64$ from proposition 4.14.3, we get the comparison $\frac{1+(1+X+X^2)^{D_0/2}}{X} \leqslant 2.67 D_0$. The result follows from the inequality $2.67\sqrt{2} \leqslant 3.8$. ∎

Due to the hypothesis $d(u, W_{\sigma_0})|j|D_0\sqrt{2} \leqslant 1$ in the statement of proposition 6.8 we need to make a further assumption in what follows. From now on we assume that $d(u, W_{\sigma_0})$ is sufficiently small, more precisely.

Hypothesis 6.9. *Assume that* $d(u, W_{\sigma_0}) \leqslant \frac{1}{\sqrt{2}(g+t)D_0 S_1}$.

We will explicitly specify when we use this hypothesis in the following. We now specialise the proposition 6.8 in the two main cases we will need it. First with $\tau \in \mathbb{N}^g$ such that $|\tau| = \ell \geqslant (g+t)T_1$, $j \in \mathbb{Z}$ such that $|j| \leqslant (g+t)S_1$, and $T = (g+t)T_1$. Next with $\tau \in \mathbb{N}^g$ such that $|\tau| \leqslant T_0$, $m \in \mathbb{Z}$ such that $|j| \leqslant S_0$, and $T = T_0$.

Proposition 6.10. *Let* $\tau \in \mathbb{N}^g$ *be such that* $|\tau| \leqslant (g+t)T_1$ *and* $j \in \mathbb{Z}$ *such that* $|j| \leqslant (g+t)S_1$. *Under hypothesis 6.9 we have*

$$\begin{aligned}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(ju) - \frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(jw)\right| \frac{\exp\left(-\frac{\pi}{2}D_1\|ju_A\|^2_\sigma\right)}{(1 + \|ju_0\|^2_\sigma)^{D_0/2}} &\leqslant \|s\|_{2,\sigma} d(u, W_{\sigma_0}) \\ &\quad \times \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 1.01(g+t)\right).\end{aligned}$$

Proof. We apply proposition 6.8 with (j,τ) and $T=(g+t)T_1$. Notice that from hypothesis 6.9, the hypothesis of proposition 6.8 is indeed satisfied. First, from proposition 4.14.2 we have

$$\begin{aligned}3.8|jD_0| \leqslant \frac{3.8\widetilde{T}_1(g+t)S_1}{C_0C_1} &\leqslant \frac{3.8\widetilde{T}_1(g+t)(2\widetilde{S}_1+1)}{2C_0C_1}\\ &\leqslant \frac{1}{2}\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0C_1}\right)^2\frac{3.8(g+t)C_0C_1}{\widetilde{T}_1}.\end{aligned}$$

Because $\frac{x^2}{2}\leqslant e^x$ for all real number x, and $3.8(g+t)C_0C_1\leqslant\widetilde{T}_1$ from proposition 4.14.1, we get the inequality $3.8|jD_0|\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0C_1}\right)$.

Next, from lemma 4.18 and corollary 4.22 we have

$$\begin{aligned}\|s\|_{\infty,\sigma} &\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0C_1}\right)\max\left(1,\frac{1}{\rho(A_\sigma,L_\sigma^{\otimes D_1})}\right)^{g/2}\\ &\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left(\frac{1}{C_1}+\frac{g}{4\widetilde{T}_1}\right)\right).\end{aligned}$$

Finally from lemma 5.11 we have

$$\frac{2\pi gD_1\|ju_A\|_\sigma+D_0g}{2(g+t)T_1}+\sqrt{\frac{\pi D_1g^2+D_0g^2}{2(g+t)T_1}}\leqslant\sqrt{1+\frac{(2\widetilde{S}+1)\log E}{C_0C_1}},$$

and therefore

$$\begin{aligned}e^{(g+t)T_1}\max\left(1,\frac{2\pi gD_1\|ju_A\|_\sigma+D_0g}{2(g+t)T_1}+\sqrt{\frac{\pi D_1g^2+D_0g^2}{2(g+t)T_1}}\right)^{(g+t)T_1}&\\ \leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\underbrace{\left(g+t+\frac{g+t}{2C_1}\right)}_{\leqslant 1.001(g+t)}\right).&\end{aligned}$$

Therefore, $\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(ju)-\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(jw)\right|\frac{\exp\left(-\frac{\pi}{2}D_1\|ju_A\|^2_\sigma\right)}{(1+\|ju_0\|^2_\sigma)^{D_0/2}}$ is bounded by

$$\|s\|_{2,\sigma}d(u,W_{\sigma_0})\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\underbrace{\left(\frac{1}{C_1}+\frac{1}{C_1}+\frac{g}{4\widetilde{T}_1}+1.001(g+t)\right)}_{\leqslant 1.01(g+t)}\right).$$

■

Proposition 6.11. *Let $\tau\in\mathbb{N}^g$ be such that $|\tau|\leqslant T_0$ and $j\in\mathbb{Z}$ such that $|j|\leqslant S_0$. Under hypothesis 6.9 we have*

$$\begin{aligned}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(ju)-\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(jw)\right|\frac{\exp\left(-\frac{\pi}{2}D_1\|ju_A\|^2_\sigma\right)}{(1+\|ju_0\|^2_\sigma)^{D_0/2}} &\leqslant \|s\|_{2,\sigma}d(u,W_{\sigma_0})\\ &\times\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2.01(g+t)\right).\end{aligned}$$

Proof. The proof is exactly the same as the previous one. Because $S_0 \leqslant (g+t)S_1$, the upper-bound for $3.8|j|D_0$ is the same as the previous one, as well as the bound for $\|s\|_{\infty,\sigma}$:

$$3.8|j|D_0 \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0C_1}\right);$$
$$\|s\|_{\infty,\sigma} \leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left(\frac{1}{C_1}+\frac{g}{4\widetilde{T}_1}\right)\right).$$

The only inequality that changes is the last one. From lemma 5.11, we have

$$\frac{2\pi gD_1\|ju_A\|_\sigma + D_0 g}{2T_0} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T_0}} \leqslant \sqrt{1+\frac{(2\widetilde{S}+1)\log E}{C_0C_1}},$$

and therefore from the value $T_0 = 2(g+t)T_1 - 1$ we have

$$e^{T_0}\max\left(1, \frac{2\pi gD_1\|ju_A\|_\sigma + D_0 g}{2T_0} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2T_0}}\right)^{T_0}$$
$$\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\underbrace{\left(2(g+t)+\frac{2(g+t)}{2C_1}\right)}_{\leqslant 2.001(g+t)}\right).$$

We can thus bound $\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(ju) - \frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(jw)\right|\frac{\exp\left(-\frac{\pi}{2}D_1\|ju_A\|^2_\sigma\right)}{(1+\|ju_0\|^2_\sigma)^{D_0/2}}$ by

$$\|s\|_{2,\sigma}d(u,W_{\sigma_0})\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\underbrace{\left(\frac{1}{C_1}+\frac{1}{C_1}+\frac{g}{4\widetilde{T}_1}+2.001(g+t)\right)}_{\leqslant 2.01(g+t)}\right).$$

■

6.4.2 The interpolation lemma

We are now down to bound the derivatives of $s^\star_\sigma$ at the point mw. In order to do this appropriately (and this is in fact the heart of the Baker's method), we use an interpolation lemma. By that we mean bounding the value of a holomorphic function at a point in terms of the supremum of the function on a disc containing the point, and of the derivatives of the function at some chosen points.

For a holomorphic function f on an open subset of $\mathbb{C}$ containing a closed disc $D(0,R)$, we denote by $\|f\|_R$ the sup norm of f on $D(0,R)$. The interpolation lemma we will use to estimate the norm of $\mathrm{jet}^\ell_W s(mp)$ at the Archimedean places dividing σ_0 is the following one, coming from [BG19].

Proposition 6.12 ([BG19, Proposition 2.1])**.** *Let S be a non-negative integer, let r, R be two real numbers such that $R > r \geqslant S + \frac{1}{2}$, and let $\varepsilon \in \left]0, \frac{1}{2}\right[$. Let f be a holomorphic function on an*

open subset of $\mathbb{C}$ *containing the closed disc* $D(0,R)$*. Then, for every non-negative integer* T*, and every real number* $a>0$*, we have*

$$\|f\|_r \leqslant \frac{R}{R-r}\left(\frac{r}{R}\right)^{T+1}\left(\frac{R^2\left(r^2+\frac{(S+1)(2S+1)}{6}\right)}{R^4+r^2\frac{(S+1)(2S+1)}{6}}\right)^{S(T+1)} \times \|f\|_R + \frac{1}{2\varepsilon}\left(\sum_{\substack{|j|\leqslant S\\ 0\leqslant h\leqslant T}}\frac{|f^{(h)}(j)|}{2^h h!}\right)\left(\frac{r}{a\cos(\pi\varepsilon)}\right)^{T+1}\max\left(1,\frac{r}{a}\right)^{2S(T+1)}(\mathrm{sh}(\pi a))^{T+1}.$$

In order to make this proposition more usable for our purposes, we optimise the values of ε and a in the following lemma.

Lemma 6.13. *Let* T *be a positive integer and let* S *be a non-negative integer. We have*

$$\inf_{\substack{0<\varepsilon<\frac{1}{2}\\ a>0}}\frac{1}{2\varepsilon}\left(\frac{r\,\mathrm{sh}(\pi a)}{a\cos(\pi\varepsilon)}\right)^{T+1}\max\left(1,\frac{r}{a}\right)^{2S(T+1)} \leqslant \exp\left((T+1)(2S+1)\log\left(\frac{r\pi\mathrm{e}}{2S+1}\right)\right).$$

Proof. Let us take $\varepsilon=\frac{1}{\pi\sqrt{T+1}}$. We have $\frac{1}{2\varepsilon\cos(\pi\varepsilon)^{T+1}}=\frac{\pi\sqrt{T+1}}{2\cos\left(\frac{1}{\sqrt{T+1}}\right)^{T+1}}$. Because $\cos x\geqslant 1-\frac{x^2}{2}$ for $x\in[0,\frac{\pi}{2}]$, we have for $T\geqslant 1$,

$$\cos\left(\frac{1}{\sqrt{T+1}}\right)^{T+1}\geqslant\left(1-\frac{1}{2(T+1)}\right)^{T+1}\geqslant\left(1-\frac{1}{4}\right)^2=\frac{9}{16}.$$

Therefore, we get

$$\frac{\pi\sqrt{T+1}}{2\cos\left(\frac{1}{\sqrt{T+1}}\right)^{T+1}}\leqslant\frac{8\pi}{9}\sqrt{T+1}\leqslant 2.8\sqrt{T+1}. \tag{6.10}$$

On the other hand, let $a=\frac{2S+1}{\pi}$. From the assumption $r\geqslant S+\frac{1}{2}$, we have $r>a$. Therefore, since $\mathrm{sh}(x)\leqslant\frac{e^x}{2}$, we get

$$\begin{aligned}\left(\frac{r}{a}\right)^{T+1}\max\left(1,\frac{r}{a}\right)^{2S(T+1)}(\mathrm{sh}(\pi a))^{T+1} &= \mathrm{sh}(2S+1)^{T+1}\left(\frac{r\pi}{2S+1}\right)^{(T+1)(2S+1)}\\ &\leqslant\frac{1}{2^{T+1}}\exp\left((T+1)(2S+1)\left(1+\log\left(\frac{r\pi}{2S+1}\right)\right)\right)\\ &\leqslant\frac{1}{2^{T+1}}\exp\left((T+1)(2S+1)\log\left(\frac{r\pi\mathrm{e}}{2S+1}\right)\right).\end{aligned} \tag{6.11}$$

Combining (6.10) and (6.11), we get

$$\frac{1}{2\varepsilon}\left(\frac{r\,\mathrm{sh}(\pi a)}{a\cos(\pi\varepsilon)}\right)^{T+1}\max\left(1,\frac{r}{a}\right)^{2S(T+1)}\leqslant\frac{2.8\sqrt{T+1}}{2^{T+1}}\exp\left((T+1)(2S+1)\log\left(\frac{r\pi\mathrm{e}}{2S+1}\right)\right),$$

and because $T\geqslant 1$, we have $\frac{2.8\sqrt{T+1}}{2^{T+1}}\leqslant 1$. This finishes the proof. ∎

We can now simplify a bit proposition 6.12 using lemma 6.13.

Lemma 6.14. *Let S be a non-negative integer, let r be a real number such that $r \geqslant S + \frac{1}{2}$, and let $E > e$ be a real number. Let f be an holomorphic function on an open subset of $\mathbb{C}$ containing the closed disc $D(0,R)$. Then, for every positive integer T, we have*

$$\|f\|_r \leqslant \frac{2}{E^{(T+1)(2S+1)}} \left(1 + \frac{(S+1)(2S+1)}{6r^2}\right)^{S(T+1)} \times \|f\|_{Er} + \sum_{\substack{|j|\leqslant S \\ 0\leqslant h\leqslant T}} \frac{|f^{(h)}(j)|}{2^h h!} \times \exp\left((T+1)(2S+1)\log\left(\frac{r\pi \mathrm{e}}{2S+1}\right)\right).$$

Proof. Let us take $R = Er$ in the statement of proposition 6.12. Using lemma 6.13 we are reduced to prove the inequality

$$\frac{R}{R-r}\left(\frac{R^2\left(r^2 + \frac{(S+1)(2S+1)}{6}\right)}{R^4 + r^2\frac{(S+1)(2S+1)}{6}}\right)^{S(T+1)} \leqslant \frac{2}{E^{2S(T+1)}}\left(1 + \frac{(S+1)(2S+1)}{6r^2}\right)^{S(T+1)}.$$

First, recall that we have $E \geqslant \mathrm{e}$. Thus, $\frac{R}{R-r} = \frac{E}{E-1} \leqslant \frac{\mathrm{e}}{\mathrm{e}-1} \leqslant 2$. Next, bounding the denominator $R^4 + r^2\frac{(S+1)(2S+1)}{6}$ from below by R^4 we get

$$\frac{R^2\left(r^2 + \frac{(S+1)(2S+1)}{6}\right)}{R^4 + r^2\frac{(S+1)(2S+1)}{6}} \leqslant \frac{r^2 + \frac{(S+1)(2S+1)}{6}}{E^2r^2} \leqslant \frac{1}{E^2}\left(1 + \frac{(S+1)(2S+1)}{6r^2}\right).$$

■

We are going to use lemma 6.14 to bound the ℓ-th jet of $s^\star_\sigma$ at the point mw in two different ways depending on if we are in the periodic or the non-periodic case (see definition 4.13). From now on we split the proof according to these two cases.

6.4.3 The non-periodic case

We assume in this paragraph that we are in the non-periodic case. Recall that in this case we have $\Upsilon = \{(m,\tau) \in \mathbb{Z} \times \mathbb{N}^g, |m| \leqslant S_0, |\tau| \leqslant T_0\}$.

First, if $|m| \leqslant S_0$, then for any $\tau \in \mathbb{N}^g$ such that $|\tau| = \ell \leqslant (g+t)T_1 \leqslant T_0$, we have $(m,\tau) \in \Upsilon$. Therefore, from the definition (5.1) we have

$$\begin{aligned} \|\operatorname{jet}^\ell_W s(mp)\|_\sigma &= \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|^2_\sigma\right)}{(1+\|mu_0\|^2_\sigma)^{D_0/2}}\left(\sum_{\tau\in\mathbb{N}^g,|\tau|=\ell}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mu)\right|^2\frac{\tau_1!\cdots\tau_g!}{\ell!}\right)^{1/2} \\ &\leqslant \|U_\sigma s\| \\ &\leqslant \frac{1}{\alpha}\|s\|_{\alpha,\sigma}. \end{aligned} \tag{6.12}$$

In the end, this upper-bound will be smaller than the one we will obtain without the assumption $|m| \leqslant S_0$. We thus assume from now on that $|m| > S_0$ and we fix $\tau \in \mathbb{N}^g$ such that $|\tau| = \ell$. Our

goal is to bound $\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mw)\right|$. Define the holomorphic function

$$f:\left|\begin{array}{ccc}\mathbb{C}&\longrightarrow&\mathbb{C}\\ z&\longmapsto&\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(zw)\end{array}\right.\cdot$$

We thus want to bound $|f(m)|\leqslant\|f\|_{(g+t)S_1}$. In order to do this we are going to apply lemma 6.14. We will want to use the value of $\|s\|_{\alpha,\sigma}$ during the proof. Notice that it involves the derivatives of $s^\star_\sigma$ at order up to T_0 at the points ju for $|j|\leqslant S_0$. This leads us naturally to the values $r=(g+t)S_1$, $S=S_0$ and $T=T_0-(g+t)T_1=(g+t)T_1-1$ in lemma 6.14 (the "$-(g+t)T_1$" comes from the fact that the definition of f already involve a derivative at order $\ell\leqslant(g+t)T_1$). In this case, the interpolation lemma becomes

$$\begin{aligned}\|f\|_{(g+t)S_1}\leqslant&\frac{2}{E^{(g+t)(2S_0+1)T_1}}\left(1+\frac{(S_0+1)(2S_0+1)}{6(g+t)^2S_1^2}\right)^{(g+t)S_0T_1}\times\|f\|_{E(g+t)S_1}\\&+\sum_{\substack{|j|\leqslant S_0\\0\leqslant h\leqslant(g+t)T_1-1}}\frac{|f^{(h)}(j)|}{2^h h!}\times\exp\left((g+t)T_1(2S_0+1)\log\left(\frac{(g+t)S_1\pi\mathrm{e}}{2S_0+1}\right)\right).\end{aligned}$$

Let us first deal with the terms that are easy to bound. From the definition (4.3) of S_0 and S_1 we have $S_1\geqslant C_1\widetilde{S}$ and $S_0=S\leqslant\widetilde{S}$. Therefore,

$$\begin{aligned}\left(1+\frac{(S_0+1)(2S_0+1)}{6(g+t)^2S_1^2}\right)^{(g+t)S_0T_1}&\leqslant\left(1+\frac{(\widetilde{S}+1)(2\widetilde{S}+1)}{6(g+t)^2C_1^2\widetilde{S}^2}\right)^{(g+t)\widetilde{S}\widetilde{T}_1}\\&\leqslant\left(1+\frac{6}{6(g+t)^2C_1^2}\right)^{(g+t)\widetilde{T}_1\frac{2\widetilde{S}+1}{2}}\\&\leqslant\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\underbrace{\frac{1}{2(g+t)C_1^2}}_{\leqslant10^{-6}}\right).\end{aligned}\tag{6.13}$$

Similarly we have

$$\log\left(\frac{(g+t)S_1\pi\mathrm{e}}{2S+1}\right)\leqslant\log\left(2\pi\mathrm{e}(g+t)C_1\right).\tag{6.14}$$

Finally, from proposition 4.14.1, we have $\widetilde{T}_1\geqslant10^7$. Writing T_1 as $\widetilde{T}_1-\varepsilon$ with $\varepsilon\in[0,1[$, we get

$$T_1=\widetilde{T}_1-\varepsilon=\widetilde{T}_1\left(1-\frac{\varepsilon}{\widetilde{T}_1}\right)\geqslant\widetilde{T}_1\left(1-10^{-7}\right)\geqslant0.999\,\widetilde{T}_1.$$

Similarly, we have $2\widetilde{S}+1\geqslant C_0=(5(g+t))^3\geqslant10^3$. Writing S as $\widetilde{S}-\varepsilon'$ with $\varepsilon'\in[0,1[$ we deduce

$$2S+1=2\widetilde{S}+1-2\varepsilon'=(2\widetilde{S}+1)\left(1-\frac{2\varepsilon'}{2\widetilde{S}+1}\right)\geqslant(2\widetilde{S}+1)\left(1-2\cdot10^{-3}\right)=0.998(2\widetilde{S}+1).$$

This allows us to bound $2E^{-(g+t)T_1(2S+1)}$. Since $1\leqslant\frac{(2\widetilde{S}+1)\log E}{C_0}$ from proposition 4.14.4, and $C_0\widetilde{T}_1\geqslant10^{10}$, we have

$$\begin{aligned}\frac{2}{E^{-(g+t)T_1(2S+1)}}&\leqslant\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\left(-0.999\cdot0.998(g+t)+\frac{\log2}{C_0\widetilde{T}_1}\right)\right)\\&\leqslant\exp\left(-0.996(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right).\end{aligned}\tag{6.15}$$

Combining (6.13), (6.14), and (6.15), we get

$$\begin{aligned}\|f\|_{(g+t)S_1} \leqslant \|f\|_{E(g+t)S_1} \exp\left(-0.99(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) \\ + \sum_{\substack{|j|\leqslant S \\ 0\leqslant h\leqslant (g+t)T_1-1}} \frac{|f^{(h)}(j)|}{2^h h!} \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E \times (g+t)\log(2\pi \mathrm{e}(g+t)C_1)\right).\end{aligned} \tag{6.16}$$

We are essentially left with bounding $\|f\|_{E(g+t)S_1}$ and $\sum_{\substack{|j|\leqslant S \\ 0\leqslant h\leqslant (g+t)T_1-1}} \frac{|f^{(h)}(j)|}{2^h h!}$. We first look at $\|f\|_{E(g+t)S_1}$.

Proposition 6.15. *The sup norm of f on the disc $D(0, E(g+t)S_1)$ is bounded by*

$$\|s\|_{\alpha,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \frac{5}{2}(g+t)^2\right).$$

Proof. We use corollary 5.10 with $\boldsymbol{w} = \mathbf{w}_\sigma$, $(x_0, x_A) = zw$ with $z \in \mathbb{C}$ such that $|z| \leqslant E(g+t)S_1$, and $T = (g+t)T_1$ to get

$$\begin{aligned}\|f\|_{E(g+t)S_1} \leqslant &\exp\left(\frac{\pi}{2}D_1\|E(g+t)S_1u_A\|_\sigma^2\right)\left(1+\|E(g+t)S_1\lambda(u_A)\|_\sigma^2\right)^{D_0/2}\|s\|_{\infty,\sigma} \\ &\times e^{(g+t)T_1}\max\left(1, \frac{2\pi D_1 g\|E(g+t)S_1u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}}\right)^{(g+t)T_1}.\end{aligned}$$

From the value (4.4) of $\widetilde{D}_1$, we have $D_1\|ES_1u_A\|_\sigma^2 \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}$ and therefore

$$\exp\left(\frac{\pi}{2}D_1\|E(g+t)S_1u_A\|_\sigma^2\right) \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \frac{\pi}{2}(g+t)^2\right). \tag{6.17}$$

Moreover, from proposition 4.14.6 and proposition 4.14.2 we have

$$\begin{aligned}\left(1+\|E(g+t)S_1\lambda(u_A)\|_\sigma^2\right)^{D_0/2} &\leqslant (g+t)^{D_0}\left(1+\|ES_1\lambda(u_A)\|_\sigma^2\right)^{D_0/2} \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left(\frac{\log(g+t)}{C_1}+1.01\right)\right) \\ &\leqslant \exp\left(1.02\cdot\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\right).\end{aligned} \tag{6.18}$$

From lemma 4.18 and corollary 4.22, we have

$$\begin{aligned}\|s\|_{\infty,\sigma} &\leqslant \|s\|_{2,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0C_1}\right)\max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2} \\ &\leqslant \|s\|_{\alpha,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \underbrace{\left(\frac{1}{C_1}+\frac{g}{4\widetilde{T}_1}\right)}_{\leqslant 1/2}\right).\end{aligned} \tag{6.19}$$

From lemma 5.11 we have

$$\frac{2\pi D_1 g\|E(g+t)S_1 u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}} \leqslant \sqrt{1 + \frac{(2\widetilde{S}+1)\log E}{C_0 C_1}},$$

and with the inequality $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}$ from proposition 4.14.4, we deduce

$$\begin{aligned} e^{(g+t)T_1} \max\left(1, \frac{2\pi D_1 g\|E(g+t)S_1 u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}}\right)^{(g+t)T_1} \\ \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \underbrace{\left((g+t) + \frac{g+t}{2C_1}\right)}_{\leqslant 1.01(g+t)}\right). \end{aligned} \tag{6.20}$$

Combining (6.17), (6.18), (6.19), (6.20), we finally get

$$\|f\|_{E(g+t)S_1} \leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left(\frac{\pi}{2}(g+t)^2 + 1.02 + 0.5 + 1.01(g+t)\right)\right).$$

The upper-bound $\frac{\pi}{2}(g+t)^2 + 1.02 + 0.5 + 1.01(g+t) \leqslant \frac{5}{2}(g+t)^2$ gives the result. ∎

Let us now look at the derivatives of f. Let $w = \sum_{i=1}^{g} w_i \mathbf{w}_{\sigma,i}$ be the decomposition of w in the basis $\mathbf{w}_\sigma$. By Leibniz formula, the h-th derivative of f is equal to

$$\frac{1}{h!} f^{(h)}(z) = \sum_{\tau' \in \mathbb{N}^g, |\tau'|=h} \frac{1}{\tau'!\tau!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(zw) \prod_{i=1}^{g} w_i^{\tau'_i}.$$

To bound this sum, we change back to the point u. We have

$$\begin{aligned} \sum_{\substack{|j|\leqslant S \\ 0\leqslant h\leqslant (g+t)T_1-1}} \frac{|f^{(h)}(j)|}{2^h h!} \leqslant & \sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g, \\ |\tau'|\leqslant (g+t)T_1-1}} \frac{1}{2^{|\tau'|}} \left|\frac{1}{\tau'!\tau!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(jw) - \frac{1}{\tau'!\tau!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau'_i} \\ & + \sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g, \\ |\tau'|\leqslant (g+t)T_1-1}} \frac{1}{2^{|\tau'|}} \left|\frac{1}{\tau'!\tau!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau'_i}. \end{aligned}$$

We have $\frac{(\tau+\tau')!}{\tau!\tau'!} \leqslant 2^{|\tau|+|\tau'|}$ so that $\frac{1}{2^{|\tau'|}\tau'!\tau!} \leqslant \frac{2^\ell}{(\tau+\tau')!}$. We now treat the two sums separately. We warn the reader that the proof of the following result is quite technical.

Proposition 6.16. *Under hypothesis 6.9 we have*

$$\begin{aligned} 2^\ell \sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g, \\ |\tau'|\leqslant (g+t)T_1-1}} & \left|\frac{1}{(\tau+\tau')!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(jw) - \frac{1}{(\tau+\tau')!} D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau'_i} \\ & \leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\pi}{2} D_1 \|mu_A\|^2_\sigma\right) \left(1 + \|mu_0\|^2_\sigma\right)^{D_0/2} d(u, W_{\sigma_0}) \\ & \quad \times \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 4.2(g+t)\right). \end{aligned}$$

Proof. As we have $|\tau+\tau'| \leqslant T_0$ and $|j| \leqslant S_0 \leqslant |m|$, we can apply proposition 6.11 to get

$$\left|\frac{1}{(\tau+\tau')!}D_{\mathbf{w}_\sigma}^{\tau+\tau'}s_\sigma^\star(jw) - \frac{1}{(\tau+\tau')!}D_{\mathbf{w}_\sigma}^{\tau+\tau'}s_\sigma^\star(ju)\right| \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}} \leqslant \|s\|_{2,\sigma} d(u, W_{\sigma_0}) \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 2.01(g+t)\right).$$

Moreover, from the multinomial formula and the upper-bound $\tau'! \leqslant h!$, for $\tau' \in \mathbb{N}^g$ such that $|\tau'| = h$, we can bound the remaining part of the sum using the Cauchy–Schwarz inequality and lemma 3.39 (recall also that $\|w\|_\sigma = \sqrt{\|\lambda(u_A)\|_\sigma^2 + \|u_A\|_\sigma^2} \leqslant \sqrt{2}\|u_A\|_\sigma$):

$$\begin{aligned}
\sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} \prod_{i=1}^g |w_i|^{\tau_i'} &\leqslant (2S+1) \sum_{\substack{\tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} 1 \times \sqrt{\frac{|\tau'|!}{\tau'!}} \prod_{i=1}^g |w_i|^{\tau_i'} \\
&\leqslant (2S+1) \sqrt{\sum_{\substack{\tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} 1^2} \sqrt{\sum_{\substack{\tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} \frac{|\tau|!}{\tau!} \prod_{i=1}^g |w_i|^{2\tau_i'}} \\
&\leqslant (2S+1)\binom{g+(g+t)T_1-1}{g}^{1/2} \sqrt{\sum_{h=0}^{(g+t)T_1-1} \|w\|_\sigma^{2h}} \\
&\leqslant (2S+1)((g+t)T_1)^{g/2}\sqrt{(g+t)T_1}\max(1,\|w\|_\sigma)^{(g+t)T_1-1} \\
&\leqslant (2S+1)\left((g+t)T_1\right)^{(g+1)/2}\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{(g+t)T_1-1}.
\end{aligned}$$

As $\|s\|_{2,\sigma} \leqslant \|s\|_{\alpha,\sigma}$, the sum we want to bound is therefore less than or equal to

$$\begin{aligned}
\|s\|_{\alpha,\sigma} \exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2} d(u,W_{\sigma_0}) \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2.01(g+t)\right) \\
\times 2^\ell(2S+1)\left((g+t)T_1\right)^{g/2}\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{(g+t)T_1-1}.
\end{aligned} \tag{6.21}$$

As $\ell \leqslant (g+t)T_1 \leqslant (g+t)\widetilde{T}_1$ and $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}$ from proposition 4.14.4, we have

$$2^\ell = \exp(\ell\log 2) \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\log 2\right). \tag{6.22}$$

Moreover, because $\log^+\|u_A\|_\sigma$ is also less than or equal to $\frac{(2\widetilde{S}+1)\log E}{C_0}$ from proposition 4.14.4,

$$\begin{aligned}
\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{(g+t)T_1-1} &\leqslant \exp\left((g+t)\widetilde{T}_1(\log\sqrt{2}+\log^+\|u_A\|_\sigma)\right) \\
&\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\left(1+\log\sqrt{2}\right)\right).
\end{aligned} \tag{6.23}$$

Finally, by the inequality $\widetilde{T}_1 \geqslant (2(g+t))^{4g+2t+6}$ from proposition 4.14.1, we deduce that

$$\begin{aligned}(2S+1)\left((g+t)T_1\right)^{(g+1)/2} &\leqslant \frac{1}{\sqrt{(g+3)!}}\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2^3 C_0}\right)^{(g+3)/2} \frac{2^{3(g+3)/2}(g+t)^{(g+1)/2}\sqrt{(g+3)!}C_0}{\widetilde{T}_1} \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{8C_0}\right) \times \frac{2^{(g+3)/2}(g+t)^{(g+1)/2}(g+3)^{(g+2)/2}(5(g+t))^3}{(2(g+t))^{4g+2t+6}} \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{8C_0}\right).\end{aligned} \tag{6.24}$$

The inequalities (6.21), (6.22), (6.23), (6.24) lead to the upper-bound

$$\begin{aligned}2^\ell \sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} &\left|\frac{1}{(\tau+\tau')!}D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(jw) - \frac{1}{(\tau+\tau')!}D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(ju)\right| \prod_{i=1}^g |w_i|^{\tau'_i} \\ &\leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2} d(u,W_{\sigma_0}) \\ &\quad \times \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \left((g+t)\left(3.01+\frac{3}{2}\log 2\right)+\frac{1}{8}\right)\right).\end{aligned}$$

The inequality $(g+t)\left(3.01+\frac{3}{2}\log 2\right)+\frac{1}{8} \leqslant 4.2(g+t)$ finishes the proof. ∎

We now bound the second sum.

Proposition 6.17.

$$\begin{aligned}\sum_{\substack{|j|\leqslant S_0,\ \tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}} &\left|\frac{2^\ell}{(\tau+\tau')!}D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(ju)\right| \prod_{i=1}^g |w_i|^{\tau'_i} \leqslant \frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 2.1(g+t)\right) \\ &\times \exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}.\end{aligned}$$

Proof. Using the Cauchy–Schwarz inequality, the sum is less than

$$2^\ell \left(\sum_{\substack{|j|\leqslant S_0,\ \tau'\in\mathbb{N}^g\\ |\tau'|\leqslant(g+t)T_1-1}} \left|\frac{1}{(\tau+\tau')!}D^{\tau+\tau'}_{\mathbf{w}_\sigma} s^\star(ju)\right|^2\right)^{1/2} \left(\sum_{\substack{|j|\leqslant S_0,\ \tau'\in\mathbb{N}^g\\ |\tau'|\leqslant(g+t)T_1-1}} \prod_{i=1}^g |w_i|^{2\tau'_i}\right)^{1/2}. \tag{6.25}$$

From the assumption $|m| > S_0$, it follows that the first square root of (6.25) is bounded by $\frac{1}{\alpha}\|s\|_{\alpha,\sigma}\exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}$, and as in the proof of proposition 6.16 we can

bound the second square root:

$$\begin{aligned}\left(\sum_{\substack{|j|\leqslant S_0,\ \tau'\in\mathbb{N}^g\\ |\tau'|\leqslant(g+t)T_1-1}}\prod_{i=1}^{g}|w_i|^{2\tau_i'}\right)^{1/2} &\leqslant \sqrt{2S_0+1}\left(\sum_{\substack{\tau'\in\mathbb{N}^g\\ |\tau'|\leqslant(g+t)T_1-1}}\frac{|\tau'|!}{\tau'!}\prod_{i=1}^{g}|w_i|^{2\tau_i'}\right)^{1/2}\\ &\leqslant \sqrt{2S+1}\left(\sum_{h=0}^{(g+t)T_1-1}\|w\|_\sigma^{2h}\right)^{1/2}\\ &\leqslant \sqrt{(2S+1)(g+t)T_1}\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{(g+t)T_1-1}.\end{aligned}$$

From (6.22), we have

$$2^\ell \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\log 2\right), \tag{6.26}$$

from (6.23), we have

$$\left(\sqrt{2}\max\left(1,\|u_A\|_\sigma\right)\right)^{(g+t)T_1-1}\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\left(1+\log\sqrt{2}\right)\right), \tag{6.27}$$

and from (6.24), we have

$$\sqrt{(2S+1)(g+t)T_1}\leqslant(2S+1)((g+t)T_1)^{g/2}\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{8C_0}\right). \tag{6.28}$$

Combining (6.26), (6.27), and (6.28), we get

$$\begin{aligned}&\sum_{\substack{|j|\leqslant S,\ \tau'\in\mathbb{N}^g,\\ |\tau'|\leqslant(g+t)T_1-1}}\left|\frac{2^\ell}{(\tau+\tau')!}D_{\mathbf{w}_\sigma}^{\tau+\tau'}s_\sigma^\star(ju)\right|\prod_{i=1}^{g}|w_i|^{\tau_i'}\\ &\qquad\leqslant\frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\left(\frac{3}{2}\log 2+1\right)+\frac{1}{8}\right).\end{aligned}$$

The inequality $(g+t)\left(\frac{3}{2}\log 2+1\right)+\frac{1}{8}\leqslant 2.2(g+t)$ gives the result. ∎

Combining propositions 6.16 and 6.17 we get the following result.

Proposition 6.18. *We have under hypothesis 6.9,*

$$\begin{aligned}\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{\left(1+\|mu_0\|_\sigma\right)^{D_0/2}}\sum_{\substack{|j|\leqslant S\\ 0\leqslant h\leqslant(g+t)T_1-1}}\frac{|f^{(h)}(j)|}{2^h h!}&\leqslant\frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2.2(g+t)\right)\\ &\quad+\|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 4.2(g+t)\right).\end{aligned}$$

The equation (6.16), and propositions 6.15 and 6.18 give us a bound for $\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star(mw)\right|$.

Proposition 6.19. *Let $\tau \in \mathbb{N}^g$ be such that $|\tau| = \ell$. If $|m| > S_0$, then we have under hypothesis 6.9,*

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|^2_\sigma\right)}{(1+\|mu_0\|^2_\sigma)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star(mw)\right| \leqslant 2\|s\|_{\alpha,\sigma}\exp\left(-0.98(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(2.7(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right).$$

Proof. Let us replace the bounds for $\|f\|_{E(g+t)S_1}$ and $\sum_{\substack{|j|\leqslant S\\ 0\leqslant h\leqslant(g+t)T_1-1}}\frac{|f^{(h)}(j)|}{2^h h!}$ given by propositions 6.15 and 6.18 respectively in (6.16):

$$\begin{aligned}
&\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|^2_\sigma\right)}{(1+\|mu_0\|^2_\sigma)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star(mw)\right| \\
&\quad\leqslant \|s\|_{\alpha,\sigma}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\left(-0.99(g+t)+\frac{5(g+t)^2}{2C_0}\right)\right) \\
&\qquad+\frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left((g+t)\log(2\pi\mathrm{e}(g+t)C_1)+\frac{2.2(g+t)}{C_0}\right)\right) \\
&\qquad+\|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left((g+t)\log(2\pi\mathrm{e}(g+t)C_1)+\frac{4.2(g+t)}{C_0}\right)\right).
\end{aligned} \tag{6.29}$$

First, from the value $C_1 = (5(g+t))^{2g+t}$, we have

$$\begin{aligned}
\frac{\log(2\pi\mathrm{e}(g+t)C_1)}{(g+t)^2} &= \frac{\log(2\pi\mathrm{e})}{(g+t)^2}+\frac{(2g+t)\log 5}{(g+t)^2}+\frac{(2g+t+1)\log(g+t)}{(g+t)^2} \\
&\leqslant \frac{\log(2\pi\mathrm{e})}{4}+\frac{3\log 5}{4}+\frac{2\log(g+t)}{g+t} \\
&\leqslant \frac{\log(2\pi\mathrm{e})}{4}+\frac{3\log 5}{4}+\frac{2}{\mathrm{e}} \\
&\leqslant 2.66.
\end{aligned}$$

Therefore, the inner parenthesis of the third exponential of (6.29) is bounded by

$$(g+t)\log(2\pi\mathrm{e}(g+t)C_1)+\frac{4.2(g+t)}{C_0}\leqslant 2.66(g+t)^3+\frac{4.2}{5^3(g+t)^2}\leqslant 2.7(g+t)^3.$$

Next, from the value $C_0 = (5(g+t))^3$, we have

$$-0.99(g+t)+\frac{5(g+t)^2}{2C_0}\leqslant(g+t)\left(-0.99+\frac{5}{2\cdot 5^3(g+t)}\right)\leqslant -0.98(g+t).$$

Finally, we have

$$\begin{aligned}
(g+t)\log(2\pi\mathrm{e}(g+t)C_1)+\frac{2.2(g+t)}{C_0}-3(g+t)^3 &\leqslant 2.66(g+t)^3+\frac{2.2}{5^3(g+t)^2}-3(g+t)^3 \\
&\leqslant -0.3(g+t)^3 \\
&< -0.98(g+t).
\end{aligned}$$

Thus, as $\log \alpha = \widetilde{T}_1(2\widetilde{S}+1)\log E \times 3(g+t)^3$, we finally get from (6.29) that

$$\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star(mu)\right| \leqslant 2\|s\|_{\alpha,\sigma}\exp\left(-0.98(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(2.7(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right).$$

■

We finally obtain an upper-bound for the norm of the jet in the non-periodic case.

Proposition 6.20. *For an embedding $\sigma : K' \hookrightarrow \mathbb{C}$ dividing σ_0 or $\overline{\sigma_0}$ and under hypothesis 6.9, the norm $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ is bounded in the non-periodic case by*

$$\|\operatorname{jet}^\ell_W s(mp)\|_\sigma \leqslant \|s\|_{\alpha,\sigma}\exp\left(-0.96(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right).$$

Proof. First, if $|m| \leqslant S_0$, we have seen in (6.12), that

$$\|\operatorname{jet}^\ell_W s(mp)\|_\sigma \leqslant \frac{1}{\alpha}\|s\|_{\alpha,\sigma} = \|s\|_{\alpha,\sigma}\exp\left(-3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right). \tag{6.30}$$

Assume now that $|m| > S_0$. The norm of $\operatorname{jet}^\ell_W s(mp)$ is given by

$$\|\operatorname{jet}^\ell_W s(mp)\|_\sigma = \frac{\exp\left(-\frac{\pi}{2}D_1\|mu\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)}\left(\sum_{\substack{\tau\in\mathbb{N}^g,\\ |\tau|=\ell}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mu)\right|^2\frac{\tau_1!\cdots\tau_g!}{\ell!}\right)^{1/2}$$
$$\leqslant \frac{\exp\left(-\frac{\pi}{2}D_1\|mu\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\sup_{\substack{\tau\in\mathbb{N}^g,\\ |\tau|=\ell}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mu)-\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mw)\right|\sqrt{\binom{g+\ell-1}{g-1}}$$
$$+\frac{\exp\left(-\frac{\pi}{2}D_1\|mu\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\sup_{\substack{\tau\in\mathbb{N}^g,\\ |\tau|=\ell}}\left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma}s^\star_\sigma(mw)\right|\sqrt{\binom{g+\ell-1}{g-1}}.$$

As in (6.9), the term $\sqrt{\binom{g+\ell-1}{g-1}}$ is bounded by $\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2^7C_0}\right)$. Using propositions 6.10 and 6.19, and the value $C_0 = (5(g+t))^3$, we get

$$\|\operatorname{jet}^\ell_W s(mp)\|_\sigma \leqslant \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\left(\frac{1.01(g+t)}{C_0}+\frac{1}{2^7C_0}\right)\right)$$
$$+2\|s\|_{\alpha,\sigma}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left(-0.98(g+t)+\frac{1}{2^7C_0}\right)\right)$$
$$+\|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left(2.7(g+t)^3+\frac{1}{2^7C_0}\right)\right)$$
$$\leqslant 2\|s\|_{\alpha,\sigma}\exp\left(-0.97(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right)$$
$$+2\|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(2.8(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right).$$

Notice that this upper bound is always larger than (6.30), this is thus the only case we have to consider. To finish we have $2 = \exp\log 2 \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \frac{\log 2}{\widetilde{T}_1}\right) \leqslant \exp\left(0.01 \times \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\right)$. The norm of the jet is therefore bounded by

$$\|s\|_{\alpha,\sigma}\left(\exp\left(-0.96(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) + d(u,W_{\sigma_0})\exp\left(3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right)\right).$$

■

6.4.4 The periodic case

Let us now look at the periodic case. The proof of the non-periodic case almost works in the periodic case, except at the very end of the proof of proposition 6.18: because of the condition $\tau_g \leqslant T_2$ we imposed in the periodic case, we cannot bound the first square root of (6.25) in terms of $\|s_\sigma\|_{\alpha,\sigma}$. However, we will still proceed in a similar manner.

Let $\tau \in \mathbb{N}^g$ be such that $|\tau| = \ell$, and write $\tau = \tau' + (0, \tau_g)$ with $\tau' \in \mathbb{N}^g$ such that $\tau'_g = 0$. Let us define the holomorphic function

$$f : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{1}{\tau'!} D^{\tau'}_{\mathbf{w}_\sigma} s^\star_\sigma(zw) \end{array} \right. .$$

The derivatives of f are equal to

$$\frac{1}{h!} f^{(h)}(z) = \frac{1}{h!\tau'!} D^{\tau'+(0,h)}_{\boldsymbol{w}} s^\star_\sigma(zw), \tag{6.31}$$

where $\boldsymbol{w} := (\mathbf{w}_{\sigma,1}, \ldots, \mathbf{w}_{\sigma,g-1}, w)$. This family is indeed a basis of W_σ because by construction of the basis $\mathbf{w}_\sigma$ (see section 5.1) the last coordinate of w in non-zero. If we bound $\left|\frac{1}{\tau_g!} f^{(\tau_g)}(m)\right|$ we will have bounded all derivatives of $s^\star_\sigma$ at mw at order ℓ along the basis $\boldsymbol{w}$. As $\mathrm{jet}^\ell_{W_\sigma} s^\star_\sigma(mw)$ does not depend on the basis of W_σ we choose, this will not matter. To bound $\frac{1}{\tau_g!} f^{(\tau_g)}(m)$ we first use Cauchy's inequality:

$$\frac{1}{\tau_g!}|f^{(\tau_g)}(m)| \leqslant \sup_{|z|=1} |f(m+z)| \leqslant \|f\|_{|m|+1} \leqslant \|f\|_{(g+t)S_1+1}.$$

Now, as in the non-periodic case, we use the interpolation lemma 6.14 to bound $\|f\|_{(g+t)S_1+1}$. Let us choose $T = T_2 = \left\lfloor \frac{\widetilde{T}_1}{C_1} \right\rfloor$ and $S = S_0 = (g+t)S_1$ in lemma 6.14. We get

$$\begin{aligned}\|f\|_{(g+t)S_1+1} \leqslant \frac{2}{E^{(T_2+1)(2S_0+1)}}\left(1 + \frac{(S_0+1)(2S_0+1)}{6(S_0+1)^2}\right)^{(S_0+1)(T_2+1)} \times \|f\|_{E((g+t)S_1+1)} \\ + \sum_{\substack{|j|\leqslant(g+t)S_1 \\ 0\leqslant h\leqslant T_2}} \frac{|f^{(h)}(j)|}{2^h h!} \times \exp\left((T_2+1)(2S_0+1)\log\left(\frac{(S_0+1)\pi\mathrm{e}}{2S_0+1}\right)\right).\end{aligned}$$

Let us again bound some terms. From definition (4.3) we have $2\widetilde{S}_1 + 1 \geqslant C_0C_1 \geqslant 10^6$. Writing

$S_1 = \widetilde{S}_1 - \varepsilon$ with $\varepsilon \in [0,1[$, we get

$$\begin{aligned} 2S_0+1 = 2(g+t)S_1+1 &\geqslant 2(g+t)\widetilde{S}_1 - 2(g+t)\varepsilon \\ &\geqslant (g+t)(2\widetilde{S}_1+1)\left(1-\frac{2\varepsilon+1}{2\widetilde{S}_1+1}\right) \\ &\geqslant (g+t)(2\widetilde{S}_1+1)\left(1-\frac{3}{10^6}\right) \\ &\geqslant 0.999(g+t)C_1(2\widetilde{S}+1). \end{aligned}$$

We moreover have $\frac{\widetilde{T}_1}{C_1} \leqslant T_2+1$. Therefore, from the inequality $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}$ and the value of C_0, we have

$$\begin{aligned} \frac{2}{E^{(T_2+1)(2S_0+1)}} &\leqslant \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left(-0.999(g+t)+\frac{\log 2}{C_0\widetilde{T}_1}\right)\right) \\ &\leqslant \exp\left(-0.99(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right). \end{aligned} \tag{6.32}$$

Similarly, we have $T_2+1 \leqslant \frac{2\widetilde{T}_1}{C_1}$, $S_0+1 \leqslant (g+t)\widetilde{S}_1+1 \leqslant \frac{(g+t)(2\widetilde{S}_1+1)}{2} = \frac{(g+t)C_1(2\widetilde{S}+1)}{2}$, and $2S_0+1 \leqslant 2(S_0+1) \leqslant (g+t)C_1(2\widetilde{S}+1)$. We deduce that

$$\begin{aligned} \left(1+\frac{(S_0+1)(2S_0+1)}{6(S_0+1)^2}\right)^{(S_0+1)(T_2+1)} &= \exp\left((T_2+1)(S_0+1)\log\left(1+\frac{2S_0+1}{6(S_0+1)}\right)\right) \\ &\leqslant \exp\left((g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\times\log\frac{4}{3}\right) \\ &\leqslant \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times 0.3(g+t)\right), \end{aligned} \tag{6.33}$$

and

$$\begin{aligned} \exp\left((T_2+1)(2S_0+1)\log\left(\frac{(S_0+1)\pi\mathrm{e}}{2S_0+1}\right)\right) &\leqslant \exp\left(2(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\times\log\frac{2\pi\mathrm{e}}{3}\right) \\ &\leqslant \exp\left(3.5(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right). \end{aligned} \tag{6.34}$$

Combining (6.32), (6.33), and (6.34) the interpolation lemma now writes

$$\begin{aligned} \|f\|_{(g+t)S_1+1} \leqslant &\|f\|_{E((g+t)S_1+1)}\exp\left(-0.69(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) \\ &+\sum_{\substack{|j|\leqslant(g+t)S_1\\0\leqslant h\leqslant T_2}}\frac{|f^{(h)}(j)|}{2^h h!}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times 3.5(g+t)\right). \end{aligned} \tag{6.35}$$

We now bound $\|f\|_{E((g+t)S_1+1)}$ and $\sum_{\substack{|j|\leqslant(g+t)S_1\\0\leqslant h\leqslant T_2}}\frac{|f^{(h)}(j)|}{2^h h!}$.

Proposition 6.21. *The sup norm of f on the disc $D(0,E((g+t)S_1+1))$ is bounded by*

$$\|s\|_{\alpha,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2.4(g+t)^2\right).$$

Proof. We proceed in the exact same way as proposition 6.15. We use corollary 5.10 with $\boldsymbol{w} = \mathbf{w}_\sigma$, $(x_0, x_A) = zw$ with $z \in \mathbb{C}$ such that $|z| \leqslant E((g+t)S_1 + 1)$ and $T = (g+t)T_1$ to get

$$\begin{aligned}\|f\|_{E(S_0+1)} \leqslant \exp\left(\frac{\pi}{2} D_1 \|E((g+t)S_1+1)u_A\|_\sigma^2\right) \left(1 + \|E((g+t)S_1+1)\lambda(u_A)\|_\sigma^2\right)^{D_0/2} \|s\|_{\infty,\sigma} \\ \times e^{(g+t)T_1} \max\left(1, \frac{2\pi D_1 g \|E((g+t)S_1+1)u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}}\right)^{(g+t)T_1}.\end{aligned}$$

From the value (4.4) of D_1 we have $D_1 \|E\widetilde{S}_1 u_A\|_\sigma^2 \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}$. Moreover, $S_1 \geqslant \frac{1}{2}\widetilde{S}_1 \geqslant \frac{C_0 C_1}{2}$ and we deduce that

$$\begin{aligned}\exp\left(\frac{\pi}{2} D_1 \|E((g+t)S_1+1)u_A\|_\sigma^2\right) &\leqslant \exp\left(\frac{\pi}{2} D_1 \|E\widetilde{S}_1 u_A\|_\sigma^2 \left(g + t + \frac{1}{\widetilde{S}_1}\right)^2\right) \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \frac{\pi}{2}\left(g + t + \frac{2}{C_0 C_1}\right)^2\right) \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 1.6(g+t)^2\right).\end{aligned} \tag{6.36}$$

From proposition 4.14.2 and proposition 4.14.6 we have

$$\begin{aligned}\left(1 + \|E((g+t)S_1+1)\lambda(u_A)\|_\sigma^2\right)^{D_0/2} &\leqslant (g+t+1)^{D_0} \left(1 + \|E\widetilde{S}_1 \lambda(u_A)\|_\sigma^2\right)^{D_0/2} \\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \underbrace{\left(\frac{\log(g+t+1)}{C_1} + 1.01\right)}_{\leqslant 1.02}\right).\end{aligned} \tag{6.37}$$

From lemma 4.18 and corollary 4.22,

$$\begin{aligned}\|s\|_{\infty,\sigma} &\leqslant \|s\|_{2,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0 C_1}\right) \max\left(1, \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)^{g/2} \\ &\leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \underbrace{\left(\frac{1}{C_1} + \frac{g}{4\widetilde{T}_1}\right)}_{\leqslant 0.01}\right).\end{aligned} \tag{6.38}$$

Finally, from lemma 5.11 we have

$$\frac{2\pi D_1 g \|E((g+t)S_1+1)u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}} \leqslant \sqrt{1 + \frac{(2\widetilde{S}+1)\log E}{C_0 C_1}},$$

and therefore, because $1 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0}$ by proposition 4.14.4, we get

$$\begin{aligned}e^{(g+t)T_1} \max\left(1, \frac{2\pi D_1 g \|E((g+t)S_1+1)u_A\|_\sigma + D_0 g}{2(g+t)T_1} + \sqrt{\frac{\pi D_1 g^2 + D_0 g^2}{2(g+t)T_1}}\right)^{(g+t)T_1} \\ \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \underbrace{\left(g + t + \frac{g+t}{2C_1}\right)}_{\leqslant 1.01(g+t)}\right).\end{aligned} \tag{6.39}$$

Combining (6.36), (6.37), (6.38), and (6.39), we thus get

$$\|f\|_{E((g+t)S_1+1)} \leqslant \|s\|_{\alpha,\sigma} \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left(1.6(g+t)^2+1.03+1.01(g+t)\right)\right).$$

The result follows from the inequality $1.6(g+t)^2+1.03+1.01(g+t) \leqslant 2.4(g+t)^2$. ∎

We now look at the derivatives of f. Writing again $w = \sum_{i=1}^{g} w_i \mathbf{w}_{\sigma,i}$, from Leibniz' derivation formula we have for any integer $h \geqslant 0$,

$$\frac{1}{h!} f^{(h)}(z) = \sum_{\tau'' \in \mathbb{N}^g, |\tau''|=h} \frac{1}{\tau''!\tau'!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(zw) \prod_{i=1}^{g} w_i^{\tau_i''}.$$

As before, for τ', $\tau'' \in \mathbb{N}^g$ we can bound $\frac{1}{2^{|\tau''|}\tau''!\tau'!}$ by $\frac{2^{|\tau'|}}{(\tau'+\tau'')!}$, and we therefore have

$$\begin{aligned}\sum_{\substack{|j|\leqslant(g+t)S_1\\ 0\leqslant h\leqslant T_2}} \frac{|f^{(h)}(j)|}{2^h h!} \leqslant & \sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g, |\tau''|\leqslant T_2}} \left|\frac{2^\ell}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau_i''} \\ & + \sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}} \left|\frac{2^\ell}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(jw) - \frac{2^\ell}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau_i''}.\end{aligned}$$

Proposition 6.22. *Under hypothesis 6.9, we have*

$$\begin{aligned}2^\ell \sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}} & \left|\frac{1}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(jw) - \frac{1}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(ju)\right| \prod_{i=1}^{g} |w_i|^{\tau_i''} \\ & \leqslant \exp\left(\frac{\pi}{2} D_1 \|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2} \|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \\ & \quad \times \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 2(g+t)^2\right).\end{aligned}$$

Proof. First, from (6.22), we have

$$2^\ell \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times (g+t)\log 2\right). \tag{6.40}$$

Then, using proposition 6.11 we have for $j \in \mathbb{Z}$ such that $|j| \leqslant (g+t)S_1$,

$$\begin{aligned}\left|\frac{1}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(jw) - \frac{1}{(\tau'+\tau'')!} D_{\mathbf{w}_\sigma}^{\tau'+\tau''} s_\sigma^\star(ju)\right| & \frac{\exp\left(-\frac{\pi}{2} D_1 \|ju_A\|_\sigma^2\right)}{\left(1+\|ju_0\|_\sigma^2\right)^{D_0/2}} \\ & \leqslant \|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \times \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 2.01(g+t)\right)\end{aligned}$$

From the definition (4.4) of D_1, we have for $|j| \leqslant (g+t)S_1$,

$$\begin{aligned}\exp\left(\frac{\pi}{2}D_1\|ju_A\|_\sigma^2\right) &\leqslant \exp\left(\frac{\pi}{2}(g+t)^2 D_1 \widetilde{S}_1^2\|u_A\|_\sigma^2\right)\\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times \underbrace{\frac{\pi}{2\mathrm{e}^2}(g+t)^2}_{\leqslant 0.22(g+t)^2}\right).\end{aligned} \tag{6.41}$$

To bound term $\left(1+\|ju_0\|_\sigma^2\right)^{D_0/2}$ notice that

$$\|u_0\|_\sigma \leqslant \|u_0-\lambda(u_A)\|_\sigma + \|\lambda(u_A)\|_\sigma \leqslant \sqrt{2}d(u,W_{\sigma_0}) + \|\lambda(u_A)\|_\sigma \leqslant \sqrt{4d(u,W_0)^2+2\|\lambda(u_A)\|_\sigma^2}.$$

Using the assumption hypothesis 6.9 we have $d(u,W_{\sigma_0}) \leqslant \frac{1}{\sqrt{2}(g+t)S_1D_0}$ and from propositions 4.14.6 and 4.14.3 we get

$$\begin{aligned}\left(1+\|ju_0\|_\sigma^2\right)^{D_0/2} &\leqslant \left(1+(g+t)^2S_1^2\left(4d(u,W_{\sigma_0})^2+2\|\lambda(u_A)\|_\sigma^2\right)\right)^{D_0/2}\\ &\leqslant \left(1+\frac{2}{D_0^2}+2(g+t)^2S_1^2\|\lambda(u_A)\|_\sigma^2\right)^{D_0/2}\\ &\leqslant \left(2(g+t)^2\right)^{D_0/2}\left(1+S_1^2\|\lambda(u_A)\|_\sigma^2\right)^{D_0/2}\\ &\leqslant \exp\left(\frac{D_0}{2}\log(2(g+t)^2)+1.01\cdot\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\right)\\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times\underbrace{\left(\frac{\log(2(g+t)^2)}{2C_1}+1.01\right)}_{\leqslant 1.02}\right).\end{aligned} \tag{6.42}$$

Next, we have

$$\begin{aligned}\sum_{\substack{|j|\leqslant(g+t)S_1\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}}\prod_{i=1}^g|w_i|^{\tau_i''} &\leqslant (2(g+t)S_1+1)\sum_{\tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}\frac{|\tau''|!}{\tau''!}\prod_{i=1}^g|w_i|^{\tau_i''}\\ &\leqslant (g+t)(2S_1+1)\sum_{h=0}^{T_2}\left(\sum_{i=1}^g|w_i|\right)^h\\ &\leqslant (g+t)(2S_1+1)(T_2+1)\left(\sqrt{2g}\max(1,\|u_A\|_\sigma)\right)^{T_2}.\end{aligned}$$

Because we have $T_2=\left\lfloor\frac{\widetilde{T}_1}{C_1}\right\rfloor$ and $2S_1+1\leqslant C_1(2\widetilde{S}+1)$, we deduce that $T_2\leqslant\frac{\widetilde{T}_1}{C_1}$ and $T_2+1\leqslant\frac{2\widetilde{T}_1}{C_1}$. We thus get

$$\begin{aligned}(g+t)(2S_1+1)(T_2+1) &\leqslant 2(g+t)(2\widetilde{S}+1)\widetilde{T}_1\\ &\leqslant \frac{1}{2}\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2C_0}\right)^2\underbrace{\frac{16(g+t)C_0}{\widetilde{T}_1}}_{\leqslant 1}\\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2C_0}\right),\end{aligned} \tag{6.43}$$

and

$$\begin{aligned}\left(\sqrt{2g}\max(1,\|u_A\|_\sigma)\right)^{T_2} &\leqslant \exp\left(\frac{T_2(2\widetilde{S}+1)\log E}{C_0}\times\left(1+\log\sqrt{2g}\right)\right)\\ &\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times\underbrace{\frac{1+\log\sqrt{2g}}{C_1}}_{\leqslant 0.01}\right).\end{aligned} \tag{6.44}$$

The equations (6.40), (6.41), (6.42), (6.43), and (6.44) give

$$\begin{aligned}2^\ell \sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}} &\left|\frac{1}{(\tau'+\tau'')!}D_{\mathbf{w}_\sigma}^{\tau'+\tau''}s_\sigma^\star(jw)-\frac{1}{(\tau'+\tau'')!}D_{\mathbf{w}_\sigma}^{\tau'+\tau''}s_\sigma^\star(ju)\right|\prod_{i=1}^g|w_i|^{\tau_i''}\\ &\leqslant \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times\big((g+t)\log 2+2.01(g+t)\right.\\ &\qquad\left.+0.22(g+t)^2+1.02+0.5+0.01\big)\right)\\ &\leqslant \exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}\|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\\ &\quad\times\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2(g+t)^2\right),\end{aligned}$$

the last inequality coming from the fact that

$$\begin{aligned}(g+t)\log 2+2.01(g+t)+0.22(g+t)^2+1.53 &\leqslant (g+t)^2\left(\frac{\log 2+2.01}{2}+0.22+\frac{1.53}{4}\right)\\ &\leqslant 2(g+t)^2.\end{aligned}$$

■

Proposition 6.23. *Under hypothesis hypothesis 6.9, we have*

$$\begin{aligned}&\sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}}\left|\frac{2^\ell}{(\tau'+\tau'')!}D_{\mathbf{w}_\sigma}^{\tau'+\tau''}s_\sigma^\star(ju)\right|\prod_{i=1}^g|w_i|^{\tau_i''}\\ &\leqslant \exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}\frac{1}{\alpha}\|s\|_{\alpha,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)^2\right).\end{aligned}$$

Proof. We proceed roughly as in the proof of proposition 6.17. Using the Cauchy–Schwarz inequality, the sum is less than

$$2^\ell\left(\sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}}\left|\frac{1}{(\tau'+\tau'')!}D_{\mathbf{w}_\sigma}^{\tau'+\tau''}s_\sigma^\star(ju)\right|^2\right)^{1/2}\left(\sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,|\tau''|\leqslant T_2}}\prod_{i=1}^g|w_i|^{2\tau_i''}\right)^{1/2}. \tag{6.45}$$

From the definition (5.1) of $\|s\|_{\alpha,\sigma}$, the first square root of (6.45) is bounded by the quantity $\frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\frac{\pi}{2}D_1\|(g+t)S_1u_A\|_\sigma^2\right)\left(1+\|(g+t)S_1u_0\|_\sigma^2\right)^{D_0/2}$, and as in the proof of proposition 6.16 we have

$$\begin{aligned}\left(\sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,|\tau''|\leqslant T_2}}\prod_{i=1}^g|w_i|^{2\tau_i''}\right)^{1/2} &\leqslant \sqrt{2(g+t)S_1+1}\left(\sum_{\tau''\in\mathbb{N}^g,|\tau''|\leqslant T_2}\frac{|\tau''|!}{\tau''!}\prod_{i=1}^g|w_i|^{\tau_i''}\right)^{1/2}\\ &\leqslant \sqrt{2(g+t)S_1+1}\left(\sum_{h=0}^{T_2}\|w\|_\sigma^{2h}\right)^{1/2}\\ &\leqslant \sqrt{(2(g+t)S_1+1)(T_2+1)}\left(\max(1,\|w\|_\sigma)\right)^{T_2}\\ &\leqslant \sqrt{(2(g+t)S_1+1)(T_2+1)}\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{T_2}.\end{aligned}$$

From (6.22),

$$2^\ell \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)\log 2\right), \tag{6.46}$$

from (6.41),

$$\exp\left(\frac{\pi}{2}D_1\|(g+t)S_1u_A\|_\sigma^2\right)\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 0.22(g+t)^2\right), \tag{6.47}$$

and from (6.42), we again have

$$\left(1+(g+t)^2S_1^2\|u_0\|_\sigma^2\right)^{D_0/2}\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 1.02\right). \tag{6.48}$$

Moreover, as in (6.43) and (6.44), we have the two following inequalities.

$$\left(\sqrt{2}\max(1,\|u_A\|_\sigma)\right)^{T_2}\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times\underbrace{\frac{1+\log\sqrt{2}}{C_1}}_{\leqslant 0.01}\right), \tag{6.49}$$

$$\sqrt{(2(g+t)S_1+1)(T_2+1)}\leqslant(g+t)(2S_1+1)(T_2+1)\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2C_0}\right). \tag{6.50}$$

Combining (6.46), (6.47), (6.48), (6.49), and (6.50), we get

$$\begin{aligned}&\sum_{\substack{|j|\leqslant(g+t)S_1,\\ \tau''\in\mathbb{N}^g,\ |\tau''|\leqslant T_2}}\left|\frac{2^\ell}{(\tau'+\tau'')!}D_{\mathbf{w}_\sigma}^{\tau'+\tau''}s_\sigma^\star(ju)\right|\prod_{i=1}^g|w_i|^{\tau_i''}\\ &\qquad\leqslant\frac{1}{\alpha}\|s\|_{\alpha,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\left((g+t)\log 2+0.22(g+t)^2+1.53\right)\right)\\ &\qquad\leqslant\frac{1}{\alpha}\|s\|_{\alpha,\sigma}\exp\left(\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)\left(1+\|mu_0\|_\sigma^2\right)^{D_0/2}\\ &\qquad\quad\times\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)^2\right),\end{aligned}$$

the last inequality coming from the fact that

$$(g+t)\log 2 + 0.22(g+t)^2 + 1.53 \leqslant (g+t)^2\left(\frac{\log 2}{2} + 0.22 + \frac{1.53}{4}\right) \leqslant (g+t)^2.$$

■

Combining proposition 6.22 and proposition 6.23, we finally get a bound for the derivative term of (6.35).

Proposition 6.24.

$$\begin{aligned}\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma)^{D_0/2}} &\sum_{\substack{|j|\leqslant(g+t)S_1\\ 0\leqslant h\leqslant T_2}} \frac{|f^{(h)}(j)|}{2^h h!}\\ &\leqslant \frac{1}{\alpha}\|s\|_{\alpha,\sigma}\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times(g+t)^2\right)\\ &\quad + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 2(g+t)^2\right).\end{aligned}$$

We can now apply the interpolation lemma to get a upper-bound for derivatives of $s^\star(mu)$ along the basis $\boldsymbol{w} = (w_{\sigma,1},\dots,w_{\sigma,g-1},w)$.

Proposition 6.25. *Let $\tau \in \mathbb{N}^g$ be such that $|\tau| = \ell$. We have*

$$\begin{aligned}\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D_{\boldsymbol{w}}^\tau s^\star(mw)\right| &\leqslant 2\|s\|_{\alpha,\sigma}\exp\left(-0.68(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right)\\ &\quad + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(3.6(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right).\end{aligned}$$

Proof. By (6.31), (6.35), propositions 6.21 and 6.24, we get

$$\begin{aligned}\frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\left|\frac{1}{\tau!}D_{\boldsymbol{w}}^\tau s^\star(mw)\right| &\leqslant \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}}\|f\|_{(g+t)S_1+1}\\ &\leqslant \|s\|_{\alpha,\sigma}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\left(-0.69(g+t)+\frac{2.4(g+t)^2}{C_0}\right)\right)\\ &\quad + \frac{\|s\|_{\alpha,\sigma}}{\alpha}\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\left(3.5(g+t)+\frac{(g+t)^2}{C_0}\right)\right)\\ &\quad + \|s\|_{\alpha,\sigma}d(u,W_{\sigma_0})\exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E\times\left(3.5(g+t)+\frac{2(g+t)^2}{C_0}\right)\right).\end{aligned}$$

From the value $C_0 = (5(g+t))^3$, we have

$$-0.69(g+t)+\frac{2.4(g+t)^2}{C_0} = -0.69(g+t)+\frac{2.4}{5^3(g+t)} \leqslant -0.68(g+t),$$

$$3.5(g+t)+\frac{(g+t)^2}{C_0}-3(g+t)^3 = 3.5(g+t)+\frac{1}{5^3(g+t)}-3(g+t)^3 \leqslant -2(g+t)^3 < -0.68(g+t),$$

and

$$3.5(g+t)+\frac{2(g+t)^2}{C_0}=3.5(g+t)+\frac{2}{5^3(g+t)}\leqslant 3.6(g+t).$$

Therefore, with the value $\log\alpha=\widetilde{T}_1(2\widetilde{S}+1)\log E\times 3(g+t)^3$, we get the result. ∎

Now that we have a bound for the derivatives of $s^\star$ at mp, we can bound the norm of the jet. As the derivatives we have considered are along the basis $\boldsymbol{w}$, we need to consider this basis in the expression (6.1) of the norm of the jet. Write again $w=\sum_{i=1}^{g} w_i\mathbf{w}_{\sigma,i}$ the decomposition of w in the basis $\mathbf{w}_\sigma$ of W_σ, and let us express the dual basis of $\boldsymbol{w}$ in terms of the dual basis of $\mathbf{w}_\sigma$. We have

$$\mathbf{w}_{\sigma,i}=\begin{cases}\boldsymbol{w}_i & \text{if } 1\leqslant i\leqslant g-1;\\ -\sum_{i=1}^{g-1}\frac{w_i}{w_g}\boldsymbol{w}_i+\frac{1}{w_g}\boldsymbol{w}_g & \text{otherwise.}\end{cases}$$

Therefore, it follows that

$$\boldsymbol{w}_i^\vee=\begin{cases}\mathbf{w}_{\sigma,i}^\vee-\frac{w_i}{w_g}\mathbf{w}_{\sigma,g}^\vee & \text{if } 1\leqslant i\leqslant g-1;\\ \frac{1}{w_g}\mathbf{w}_{\sigma,g}^\vee & \text{otherwise.}\end{cases}$$

To bound the norm of an element $(\boldsymbol{w}_1^\vee)^{\tau_1}\cdots(\boldsymbol{w}_g^\vee)^{\tau_g}$ of $\mathrm{Sym}^\ell(W_\sigma^\vee)$ recall that the Hermitian structure on $\mathrm{Sym}^\ell(W_\sigma^\vee)$ is the quotient metric from the one on the tensor product $(W_\sigma^\vee)^{\otimes\ell}$. Therefore, given ℓ elements $\varphi_1,\dots,\varphi_\ell$ in $W_\sigma^\vee$, we have

$$\|\varphi_1\cdots\varphi_\ell\|_{\mathrm{Sym}^\ell(W_\sigma)}\leqslant\|\varphi_1\otimes\cdots\otimes\varphi_\ell\|_{(W_\sigma^\vee)^{\otimes\ell}}=\|\varphi_1\|\cdots\|\varphi_\ell\|.$$

We thus get,

$$\begin{aligned}\sum_{\tau\in\mathbb{N}^g,\ |\tau|=\ell}\|\boldsymbol{w}_1^\vee\|^{\tau_1}\cdots\|\boldsymbol{w}_g^\vee\|^{\tau_g}&\leqslant\left(\left\|\frac{\mathbf{w}_{\sigma,g}^\vee}{w_g}\right\|_\sigma+\sum_{i=1}^{g-1}\left\|\mathbf{w}_{\sigma,i}^\vee-\frac{w_i}{w_g}\mathbf{w}_{\sigma,g}^\vee\right\|_\sigma\right)^\ell\\&\leqslant\left(\frac{1}{|w_g|}+\sum_{i=1}^{g-1}\sqrt{1+\left|\frac{w_i}{w_g}\right|^2}\right)^\ell\\&\leqslant\left(\frac{g\max(1,\|w\|_\sigma)}{|w_g|}\right)^\ell\\&\leqslant\left(\frac{g\sqrt{2}\max(1,\|u_A\|_\sigma)}{|w_g|}\right)^\ell.\end{aligned}$$

In order to bound the jet, we therefore need to bound $\frac{1}{|w_g|}$ appropriately. This is achieved by the following proposition.

Proposition 6.26. *We have* $\frac{1}{|w_g|}\leqslant\frac{S_1(\deg_L(B))^2}{\rho(A_\sigma,L_\sigma)}$. *In particular*

$$\sum_{\tau\in\mathbb{N}^g,\ |\tau|=\ell}\|\boldsymbol{w}_1^\vee\|^{\tau_1}\cdots\|\boldsymbol{w}_g^\vee\|^{\tau_g}\leqslant\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\times 15(g+t)^4\right).$$

Proof. By the way the basis $\mathbf{w}_\sigma$ has been constructed (see section 5.1) we have $|w_g| = d(w, t_{H_\sigma} \cap W_\sigma)$. Because we are in the periodic case, there exists an integer m_0 such that $|m_0| \leqslant S_1$ and $m_0 u \in t_{H_\sigma} + \Omega_{A_\sigma}$. Therefore, we have

$$m_0 u_A = \omega + u_B,$$

for some period $\omega \in \Omega_{A_\sigma}$, $u_B \in t_{B_\sigma}$. From inclusion $t_{H_\sigma} \cap W_\sigma \subseteq t_{G_{0,\sigma}} \times t_{B_\sigma}$, we get

$$d(w, t_{H_\sigma} \cap W_\sigma) = \frac{1}{|m_0|} d(m_0 w, t_{H_\sigma} \cap W_\sigma) = \frac{1}{|m_0|} d((\lambda(m_0 u_A), \omega + u_B), t_{H_\sigma} \cap W_\sigma) \geqslant \frac{d(\omega, t_{B_\sigma})}{S_1}.$$

By the assumption hypothesis 4.2, $m_0 u_A$ does not lie in t_{B_σ}, hence $\omega \in \Omega_{A_\sigma} \setminus \Omega_{B_\sigma}$. By [GR14b, Proposition 4.3] we get

$$\frac{1}{|w_g|} \leqslant \frac{S_1}{d(\omega, t_{B_\sigma})} \leqslant \frac{S_1 (\deg_L B)^2}{\rho(A_\sigma, L_\sigma)}.$$

To prove the second upper-bound we need to bound $\deg_L B$. Let us use the definition (4.5) of x and the fact that $x \leqslant 1$. We have

$$\deg_L B \leqslant \frac{\binom{g+t}{g} 2^g \widetilde{D}_0^{t-t'} \widetilde{D}_1^{g-g'} \deg_L A}{\binom{g'+t'}{g'} \widetilde{T}_1^{c_W(H)} \#\left(\frac{\Gamma_p(S_1)+H}{H}\right)} \leqslant \frac{\widetilde{D}_0^{t-t'} \widetilde{D}_1^{g-g'}}{\widetilde{T}_1^{c_W(H)}} \binom{g+t}{g} 2^g \deg_L A.$$

From proposition 4.14.2 we have

$$\frac{\widetilde{D}_0^{t-t'} \widetilde{D}_1^{g-g'}}{\widetilde{T}_1^{c_W(H)}} \leqslant \left(\frac{y}{C_0 C_1}\right)^{g-g'} \frac{\widetilde{D}_0^{t-t'}}{\widetilde{T}_1^{c_W(H)-(g-g')}} \leqslant \left(\frac{y}{C_0 C_1}\right)^{c_W(H)} \widetilde{D}_0^{t-t'-(c_W(H)-(g-g'))}.$$

We have $(g-g') + (t-t') - c_W(H) \leqslant t$, and $c_W(H) \geqslant \max(g-g', t-t') \geqslant 1$ from corollary 4.10. Moreover, we have $S_1 \leqslant 2\widetilde{S}_1 + 1 = C_0 C_1 \mathfrak{a}$ and we deduce that

$$\frac{1}{|w_g|} \leqslant \frac{S_1 \widetilde{D}_0^{2t}}{\rho(A_\sigma, L_\sigma)} \frac{\binom{g+t}{g}^2 2^{2g}}{(C_0 C_1)^{2c_W(H)}} (y^{c_W(H)} \deg_L A)^2 \leqslant \underbrace{\frac{2^{2g+2(g+t)}}{C_0 C_1}}_{\leqslant 1} \frac{\mathfrak{a} \widetilde{D}_0^{2t}}{\rho(A_\sigma, L_\sigma)} (y^g \deg_L A)^2.$$

We now have

- $\log \mathfrak{a} \leqslant 2 \times \frac{(2\widetilde{S}+1)\log E}{C_0}$ from proposition 4.14.5;
- $2t \log \widetilde{D}_0 \leqslant \frac{(2\widetilde{S}+1)\log E}{C_0} \times 14(g+t)^3$ from proposition 4.14.7;
- $y^g \deg_L A \leqslant 1$ from proposition 4.1;
- $\frac{1}{\rho(A_\sigma, L_\sigma)} \leqslant \exp\left(\frac{(2\widetilde{S}+1)\log E}{C_0}(g+t)\right)$ from corollary 4.22,

and we deduce that

$$\frac{1}{|w_g|} \leqslant \exp\left(\frac{(2\widetilde{S}+1)\log E}{C_0} \times \left(2 + 14(g+t)^3 + (g+t)\right)\right).$$

Finally, using the inequality $\max(1, \|u_A\|_\sigma) \leqslant \exp\left(\frac{(2\widetilde{S}+1)\log E}{C_0}\right)$ from proposition 4.14.4, we deduce that

$$\left(\frac{g\sqrt{2}\max(1,\|u_A\|_\sigma)}{|w_g|}\right)^\ell \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times (g+t)\big(\log(g\sqrt{2}) + 3 + 14(g+t)^3 + (g+t)\big)\right)$$
$$\leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times 15(g+t)^4\right).$$

■

Putting together propositions 6.10, 6.25 and 6.26, we can finally bound the norm of the jet in the periodic case.

Proposition 6.27. *For an embedding $\sigma : K' \hookrightarrow \mathbb{C}$ dividing σ_0 or $\overline{\sigma_0}$ and hypothesis 6.9, the norm $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ is bounded in the periodic case by*

$$\|s_\sigma\|_{\alpha,\sigma} \exp\left(-0.56(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right)$$
$$+\|s_\sigma\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \exp\left(3.9(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right).$$

Proof. For $\tau = (\tau_1, \dots, \tau_g) \in \mathbb{N}^g$, let us write $(\boldsymbol{w}^\vee)^\tau$ for $(\boldsymbol{w}_1^\vee)^{\tau_1} \cdots (\boldsymbol{w}_g^\vee)^{\tau_g}$. From the definition (6.1) of $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ and its independence from the basis of W_σ, we have

$$\|\operatorname{jet}^\ell_W s(mp)\|_\sigma = \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}} \left\| \sum_{\tau\in\mathbb{N}^g,\ |\tau|=\ell} \frac{1}{\tau!} D^\tau_{\mathbf{w}_\sigma} s^\star(mu)(\mathbf{w}_\sigma^\vee)^\tau \right\|_\sigma$$
$$\leqslant \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}} \left\| \sum_{\tau\in\mathbb{N}^g,|\tau|=\ell} \left(\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star(mu) - \frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star(mw)\right)(\mathbf{w}_\sigma^\vee)^\tau \right\|_\sigma$$
$$+ \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}} \left\| \sum_{\tau\in\mathbb{N}^g,\ |\tau|=\ell} \frac{1}{\tau!} D^\tau_{\boldsymbol{w}} s^\star(mw)(\boldsymbol{w}^\vee)^\tau \right\|_\sigma$$
$$\leqslant \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}} \sup_{|\tau|=\ell} \left|\frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(mu) - \frac{1}{\tau!}D^\tau_{\mathbf{w}_\sigma} s^\star_\sigma(mw)\right| \sqrt{\binom{g+\ell-1}{g-1}}$$
$$+ \frac{\exp\left(-\frac{\pi}{2}D_1\|mu_A\|_\sigma^2\right)}{(1+\|mu_0\|_\sigma^2)^{D_0/2}} \sup_{\tau\in\mathbb{N}^g,\ |\tau|=\ell} \left|\frac{1}{\tau!}D^\tau_{\boldsymbol{w}} s^\star_\sigma(mw)\right| \sum_{\tau\in\mathbb{N}^g,\ |\tau|=\ell} \|\boldsymbol{w}_1^\vee\|_\sigma^{\tau_1} \cdots \|\boldsymbol{w}_g^\vee\|_\sigma^{\tau_g}.$$

From (6.9) the square root of the binomial coefficient is bounded by $\exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{2^7 C_0}\right)$. Applying

propositions 6.10, 6.24 and 6.26, we get that $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ is bounded by

$$\begin{aligned}
&\|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E \times \left(\frac{1.01(g+t)}{C_0} + \frac{1}{2^7 C_0}\right)\right) \\
+2&\|s\|_{\alpha,\sigma} \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E \left(-0.68(g+t) + \frac{16(g+t)^4}{C_0}\right)\right) \\
+&\|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \exp\left(\widetilde{T}_1(2\widetilde{S}+1)\log E \times \left(3.6(g+t) + \frac{15(g+t)^4}{C_0}\right)\right).
\end{aligned}$$

From the value $C_0 = (5(g+t))^3$, we have

$$\frac{1.01(g+t)}{C_0} + \frac{1}{2^7 C_0} \leqslant 0.01,$$

$$-0.68(g+t) + \frac{15(g+t)^4}{C_0} = -0.56(g+t),$$

and

$$3.6(g+t) + \frac{15(g+t)^4}{C_0} \leqslant 3.8(g+t).$$

The norm of the jet is therefore bounded by

$$\begin{aligned}
&2\|s\|_{\alpha,\sigma} \exp\left(-0.56(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) \\
+&2\|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \exp\left(3.8(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right).
\end{aligned}$$

To conclude we have $2 = \exp\log 2 \leqslant \exp\left(\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0} \times \frac{\log 2}{\widetilde{T}_1}\right) \leqslant \exp\left(0.01 \times \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{C_0}\right)$. The norm of the jet is therefore bounded by

$$\|s\|_{\alpha,\sigma}\left(\exp\left(-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) + d(u, W_{\sigma_0}) \exp\left(3.9(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right)\right).$$

■

If we compare the results of proposition 6.20 and proposition 6.27, we notice that the term in $d(u, W_{\sigma_0})$ is larger in the non-periodic case than in the periodic case, and the other term is smaller in the non-periodic case than in the periodic case. We therefore get

Proposition 6.28. *For an embedding $\sigma : K' \hookrightarrow \mathbb{C}$ dividing σ_0 or $\overline{\sigma_0}$ and under hypothesis 6.9, the norm $\|\operatorname{jet}^\ell_W s(mp)\|_\sigma$ is bounded in every case by*

$$\begin{aligned}
&\|s\|_{\alpha,\sigma} \exp\left(-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E\right) \\
+&\|s\|_{\alpha,\sigma} d(u, W_{\sigma_0}) \exp\left(3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E\right).
\end{aligned}$$

Chapter 7

End of the proof

7.1 Proof of theorem 4.3

Now that we have bounded the norm of $\operatorname{jet}_W^\ell s(mp)$ at all the places of K' we are finally ready to prove our two main results, namely theorems 4.3 and 4.6. From the definition of height of $\operatorname{jet}_W^\ell s(mp)$ we have

$$h(\operatorname{jet}_W^\ell s(mp)) = \sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\mathfrak{P} + \sum_{\substack{\sigma : K' \hookrightarrow \mathbb{C} \\ \sigma \nmid \sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K' : \mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\sigma + \sum_{\substack{\sigma : K' \hookrightarrow \mathbb{C} \\ \sigma \mid \sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K' : \mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\sigma.$$

Using the results of sections 6.2 to 6.4 let us bound each of the three sums. First, we use proposition 6.3 to bound the sum over the non-Archimedean places.

Proposition 7.1. *We have*

$$\sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\mathfrak{P} \leqslant 0.06(g+t) \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} + \sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} \log \|s\|_{\alpha,\mathfrak{P}}.$$

Proof. Applying proposition 6.3, we have

$$\begin{aligned}\sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\mathfrak{P} &\leqslant \sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} (\log \|s\|_{\alpha,\mathfrak{P}} - \log |\delta_\ell(D_0)|_\mathfrak{P}) \\ &\leqslant \log |\delta_\ell(D_0)| + \sum_{\substack{\mathfrak{P}|p \\ p \text{ prime}}} \frac{[K'_\mathfrak{P} : \mathbb{Q}_p]}{[K' : \mathbb{Q}]} \log \|s\|_{\alpha,\mathfrak{P}}.\end{aligned}$$

We now use lemma 6.5 to bound $\log |\delta_\ell(D_0)|$ by $0.06(g+t) \times \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D}$. ∎

We now turn to the sum ranging over the Archimedean places dividing neither σ_0, nor $\overline{\sigma_0}$. To bound it we use proposition 6.7.

Proposition 7.2. *We have*

$$\sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\log\|\operatorname{jet}^{\ell}_{W} s(mp)\|_{\sigma} \leqslant \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\left(\log\|s\|_{\alpha,\sigma} + \frac{g}{2}\log^{+}\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right) + 3.01(g+t)\cdot\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}.$$

Proof. By proposition 6.7, we have

$$\begin{aligned}\sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\log\|\operatorname{jet}^{\ell}_{W} s(mp)\|_{\sigma} &\leqslant \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\left(\log\|s\|_{\alpha,\sigma} + \frac{g}{2}\log^{+}\frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}\right)\\ &\quad + \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}(g+t)\widetilde{T}_1\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\\ &\quad + \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\times 1.01(g+t).\end{aligned}$$

Moreover, from proposition 4.23 we deduce that

$$\begin{aligned}\frac{(g+t)\widetilde{T}_1}{[K':\mathbb{Q}]}\sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\nmid\sigma_0 \text{ and } \overline{\sigma_0}}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right) &\leqslant \frac{(g+t)\widetilde{T}_1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\left(\frac{2\pi}{C_0C_1}r(A_\sigma,L_\sigma)+1\right)\\ &\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{DC_0}\times 2(g+t).\end{aligned}$$

The result follows. ∎

The final step toward a bound of the height of $\operatorname{jet}^{\ell}_{W} s(mp)$ is to bound the sum ranging over the Archimedean places dividing σ_0 or $\overline{\sigma_0}$. To do this we use proposition 6.28. Recall that the proof uses hypothesis 6.9.

Proposition 7.3. *Under hypothesis 6.9, we have*

$$\begin{aligned}&\sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\mid\sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\log\|\operatorname{jet}^{\ell}_{W} s(mp)\|_{\sigma}\\ &\qquad\leqslant \frac{2}{D}\log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)\\ &\qquad\quad + \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma\mid\sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]}\log\|s\|_{\alpha,\sigma}.\end{aligned}$$

Proof. This is a direct consequence of proposition 6.28. Indeed, it follows from this proposition

that

$$\sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma|\sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]} \log \|\operatorname{jet}_W^\ell s(mp)\|_\sigma$$
$$\leqslant \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma|\sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)$$
$$+ \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma|\sigma_0 \text{ or } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]} \log \|s\|_{\alpha,\sigma}.$$

The summand of the first sum is independent of σ and the sum is therefore equal to

$$\frac{\#\{\sigma : K' \hookrightarrow \mathbb{C}, \sigma \mid \sigma_0 \text{ or } \sigma_0'\}}{[K':\mathbb{Q}]} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)$$
$$= \frac{[k_{\sigma_0}:\mathbb{R}][K':k]}{[K':\mathbb{Q}]} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)$$
$$\leqslant \frac{2}{D} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right).$$

■

We now bound the height of $\operatorname{jet}_W^\ell s(mp)$. Combining propositions 5.17 and 7.1 to 7.3 we have

$$h(\operatorname{jet}_W^\ell s(mp)) \leqslant h_\alpha(s) + 0.06(g+t)\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D}$$
$$+ \frac{3.01(g+t)}{C_0} \cdot \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} + \frac{g}{2} \sum_{\substack{\sigma:K'\hookrightarrow\mathbb{C}\\ \sigma|\sigma_0 \text{ and } \overline{\sigma_0}}} \frac{1}{[K':\mathbb{Q}]} \log^+ \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}$$
$$+ \frac{2}{D} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)$$
$$\leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D}\left(1.6 + 0.06(g+t) + \frac{3.01(g+t)}{C_0}\right) + \frac{g}{2}\sum_{\sigma:k\hookrightarrow\mathbb{C}} \frac{1}{D} \log^+ \frac{1}{\rho(A_\sigma, L_\sigma^{\otimes D_1})}$$
$$+ \frac{2}{D} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right).$$

Corollary 4.22 gives us an upper-bound for the remaining sum over the embedding of k, and we get

$$h(\operatorname{jet}_W^\ell s(mp)) \leqslant \frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} \underbrace{\left(1.6 + 0.06(g+t) + \frac{3.01(g+t)}{C_0} + \frac{g}{4C_0\widetilde{T}_1}\right)}_{\leqslant 0.9(g+t)} \tag{7.1}$$
$$+ \frac{2}{D} \log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E} + e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right).$$

On the other hand the inequality (6.1) and proposition 6.2 give us a lower-bound for the height.

$$h(\mathrm{jet}_W^\ell s(mp)) \geqslant -\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} \times \frac{(g+t)^4}{C_0} = -\frac{\widetilde{T}_1(2\widetilde{S}+1)\log E}{D} \times 0.008(g+t). \tag{7.2}$$

Combining (7.1) and (7.2), we get a first lower-bound involving $d(u, W_{\sigma_0})$:

$$\begin{aligned}\log\left(d(u,W_{\sigma_0})e^{3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E}+e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)&\\ \geqslant -\widetilde{T}_1(2\widetilde{S}+1)\log E \times \frac{0.008(g+t)+0.9(g+t)}{2}&\\ \geqslant -0.5(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E.&\end{aligned}$$

We therefore deduce a lower bound for the distance $d(u, W_{\sigma_0})$ in terms of $\widetilde{T}_1(2\widetilde{S}+1)\log E$:

$$\begin{aligned}d(u,W_{\sigma_0}) &\geqslant e^{-3(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E}\left(e^{-0.5(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}-e^{-0.55(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)\\ &\geqslant e^{-\widetilde{T}_1(2\widetilde{S}+1)\log E\left(3(g+t)^3+0.5(g+t)\right)}\left(1-e^{-0.05(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right).\end{aligned}$$

Computing the derivative of the function $x \mapsto x^{-1}\log\left(1-e^{-0.05(g+t)x}\right)$, we see that it is increasing on $\mathbb{R}_+^\star$. Therefore, because $\widetilde{T}_1(2\widetilde{S}+1)\log E \geqslant (2(g+t))^{4g+2t+6}C_0 \geqslant 10^{10}$ from proposition 4.14.1 and proposition 4.14.4, we get

$$\begin{aligned}\log d(u,W_{\sigma_0}) &\geqslant -\widetilde{T}_1(2\widetilde{S}+1)\log E\left(3(g+t)^3+0.5(g+t)+\frac{\log\left(1-e^{-0.05(g+t)\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)}{\widetilde{T}_1(2\widetilde{S}+1)\log E}\right)\\ &\geqslant -\widetilde{T}_1(2\widetilde{S}+1)\log E\left(3(g+t)^3+0.5(g+t)+10^{-10}\log\left(1-e^{-0.05(g+t)\cdot 10^{-10}}\right)\right)\\ &\geqslant -4(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E.\end{aligned}$$

Let us now remove hypothesis 6.9. Assume that it does not hold. This means that

$$\log d(u,W_{\sigma_0}) \geqslant -\log\left(\sqrt{2}(g+t)S_1D_0\right).$$

From the definition (4.3), we have $S_1 \leqslant \frac{C_1}{2}(2\widetilde{S}+1)$, and from proposition 4.14.2 we have $D_0 \leqslant \frac{\widetilde{T}_1}{C_0C_1}$. Therefore, we have

$$\log d(u,W_{\sigma_0}) \geqslant -\log\left(\frac{\sqrt{2}(g+t)}{2C_0}\widetilde{T}_1(2\widetilde{S}+1)\right) \geqslant -4(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E.$$

We deduce that in any case we have

$$\log d(u,W_{\sigma_0}) \geqslant -4(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E.$$

To get the lower bound of theorem 4.3, let us replace $\widetilde{T}_1$ and $2\widetilde{S}+1$ by their values (4.6) and (4.3).

$$\begin{aligned}4(g+t)^3\widetilde{T}_1(2\widetilde{S}+1)\log E = 4(g+t)^3&\frac{(C_0C_1)^{(g+t)/t}}{\left(2^g\binom{g+t}{g}\right)^{1/t}}\#\Gamma_p(S_1)^{1/t}\left(1+\frac{\widetilde{S}_1^2D\log a}{(2\widetilde{S}_1+1)\log E}\right)^{g/t}\\ &\times(2\widetilde{S}+1)\log E\left(1+\frac{D(\log\widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E}\right)\frac{1}{y^{(g+t)/t}(\deg_L A)^{1/t}}.\end{aligned}$$

The set $\Gamma_p(S_1)$ has cardinality at most $2S_1+1 \leqslant C_0C_1\mathfrak{a}$. Moreover, we have $\widetilde{S}_1 \leqslant \frac{2\widetilde{S}_1+1}{2} \leqslant \frac{C_0C_1}{2}\mathfrak{a}$. Therefore,

$$1+\frac{\widetilde{S}_1^2 D\log a}{(2\widetilde{S}_1+1)\log E} \leqslant 1+\frac{C_0C_1\mathfrak{a}D\log a}{4\log E} \leqslant \frac{C_0C_1}{4}\left(1+\frac{\mathfrak{a}D\log a}{\log E}\right).$$

Then, using the inequalities $D\log\mathfrak{a} \leqslant 2\mathfrak{a}\log E$ and $D \leqslant \mathfrak{a}\log E$ from proposition 4.14.5 and 4.14.4, we have

$$\begin{aligned}
(2\widetilde{S}+1)\log E\left(1+\frac{D(\log\widetilde{S}_1+\log b)}{(2\widetilde{S}_1+1)\log E}\right) &= C_0\mathfrak{a}\log E+\frac{D}{C_1}\log\frac{C_0C_1}{2}+\frac{D\log\mathfrak{a}}{C_1}+\frac{D\log b}{C_1}\\
&\leqslant C_0\left(\mathfrak{a}\log E+\mathfrak{a}\log E\frac{\log\frac{C_0C_1}{2}}{C_0C_1}+\frac{2\mathfrak{a}\log E}{C_0C_1}+\frac{D\log b}{C_0C_1}\right)\\
&\leqslant C_0\left(\mathfrak{a}\log E\Bigg(\underbrace{1+\frac{\log\frac{C_0C_1}{2}}{C_0C_1}+\frac{2}{C_0C_1}}_{\leqslant 2}\Bigg)+\frac{D\log b}{C_1}\right)\\
&\leqslant 2C_0\left(\mathfrak{a}\log E+D\log b\right).
\end{aligned}$$

We thus get

$$\begin{aligned}
\log d(u,W_{\sigma_0}) \geqslant -8(g+t)^3\frac{(C_0C_1)^{(2g+2t+1)/t}}{2^{3g/t}\binom{g+t}{t}^{1/t}C_1}\mathfrak{a}^{1/t}\left(1+\frac{D\mathfrak{a}\log a}{\log E}\right)^{g/t}\\
\times(\mathfrak{a}\log E+D\log b)\frac{1}{y^{(g+t)/t}(\deg_L A)^{1/t}}.
\end{aligned}$$

To conclude, we look at the constant $8(g+t)^3\frac{(C_0C_1)^{(2g+2t+1)/t}}{2^{3g/t}\binom{g+t}{t}^{1/t}C_1}$. It is equal to

$$(5(g+t))^{(2g+t+3)(2g+2t+1)/t}\left(\frac{8(g+t)^3}{2^{3g/t}\binom{g+t}{t}^{1/t}}C_1\right).$$

As we have $(2g+t+3)(2g+2t+1) = 4(g+t+1)^2-(2t^2+2gt+t+1) \leqslant 4(g+t+1)^2-t(2t+2g+1)$, the constant is bounded by

$$(5(g+t))^{\frac{4(g+t+1)^2}{t}}\times\left(\frac{8(g+t)^3}{(5(g+t))^{2t+2g+1}2^{3g/t}\binom{g+t}{t}^{1/t}C_1}\right) \leqslant (5(g+t))^{\frac{4(g+t+1)^2}{t}}.$$

We finally deduce theorem 4.3:

$$\begin{aligned}
\log d(u,W_{\sigma_0}) \geqslant -(5(g+t))^{\frac{4(g+t+1)^2}{t}}\mathfrak{a}^{1/t}\left(1+\frac{D\mathfrak{a}\log a}{\log E}\right)^{g/t}\\
\times(\mathfrak{a}\log E+D\log b)\frac{1}{y^{1+g/t}\deg_L(A)^{1/t}}.
\end{aligned}$$

7.2 Proof of theorem 4.6

Our final goal is to prove theorem 4.6, removing the hypothesis 4.2 of theorem 4.3. Let again (A, L) be a polarised abelian variety over a number field k of degree D. Let $\sigma_0 : k \hookrightarrow \mathbb{C}$ be an embedding of k into $\mathbb{C}$. Let $p_A \in A(k)$ be a k-rational point of A, $u_A \in t_{A_{\sigma_0}}$ be a logarithm of p_A, and consider $W_0 < t_A$ a k-vector subspace of t_A.

Define A' to be the smallest subvariety of A_{σ_0} whose tangent subspace contains u_A. From [BG19, Proposition 4.2] (which follows from [Rém20, Théorème 1.1]) A' is defined over some Galois extension k_A/k of degree at most $f(g) := 2\alpha(g)6^{g-1}g!$, with $\alpha(2) = 2$, $\alpha(4) = 5$, $\alpha(5) = 7/6$, and $\alpha(g) = 1$ otherwise. The following lemma gives an upper-bound for $[k_A : k]$ that will be simpler to use.

Lemma 7.4. *For all integer g, we have $[k_A : k] \leqslant f(g) \leqslant (3.8g)^g$.*

Proof. Using the upper-bound $g! \leqslant 2\left(\frac{g}{2}\right)^g$, we have

$$f(g) = 2\alpha(g) \times 6^{g-1}g! \leqslant \frac{2\alpha(g)}{3}(3g)^g .$$

For every value of g except $g = 2$ and 4, we have $2\alpha(g) \leqslant 3$. This gives the announced result in these cases. For $g = 2$, we have $f(g) = 48 \leqslant (3.8 \cdot 2)^2$, and for $g = 4$, we have $f(g) = 51840 \leqslant (3.8 \cdot 4)^4$. ∎

Let $u_0 \in (t_{A'} + W_0 \otimes_k k_A)/(W_0 \otimes_k k_A) \subseteq t_A/W_0 \otimes_k k_A$ and let

$$W := \{(\lambda(x), x), x \in t_A\} \subset t_A/W_0 \times t_A,$$

where $\lambda : t_A \to t_A/W_0$ is the canonical projection. We want to find a lower bound for the distance $d((u_0, u_A), W_\sigma)$ for $\sigma : k_A \hookrightarrow \mathbb{C}$ extending σ_0. We fix such σ and we define $W_0' := (W_0 \otimes_k k_A) \cap t_{A'}$. Let φ be the linear map

$$\varphi : \left| \begin{array}{ccc} t_{A'}/W_0' & \longrightarrow & (t_{A'} + W_0 \otimes_k k_A)/(W_0 \otimes_k k_A) \\ x + W_0' & \longmapsto & x + W_0 \end{array} \right. .$$

We let $u_0' := \varphi^{-1}(u_0) \in t_{A'}/W_0'$. Our strategy to bound $d((u_0, u_A), W_\sigma)$ is to transpose our setup in a situation where theorem 4.3 applies, and to compare the quantities that will appear in terms of A, u_A, p_A, W_0, and u_0. The abelian variety A' satisfies hypothesis 4.2. Therefore, to apply theorem 4.3 to A', W_0', u_A, and u_0' we have to ensure that the vector space W_0' is a strict vector subspace of $t_{A'}$. To do so we make the following assumption.

Hypothesis 7.5. *Assume that u_A doesn't lie in $W_0 \otimes_{\sigma_0} \mathbb{C}$.*

Hypothesis 7.5 implies that W_0' is distinct from $t_{A'}$. Indeed, if $W_0' = t_{A'}$ then $W_0 \otimes_k k_A$ contains $t_{A'}$, but u_A lies in $t_{A',\sigma}$ but not in $W_{0,\sigma}$. Letting $W' := \{(\lambda'(x), x), x \in t_{A'}\} \subseteq t_{A'}/W_0' \times t_{A'}$, with $\lambda' : t_{A'} \to t_{A'}/W_0'$ the canonical projection, theorem 4.3 gives us a lower-bound for $d((u_0', u_A), W_\sigma')$. The following result allows us to compare $d((u_0, u_A), W_\sigma)$ and $d((u_0', u_A), W_\sigma')$.

Proposition 7.6. *We have*

$$d((u_0,u_A),W_\sigma)\geqslant\frac{d((u_0',u_A),W_\sigma')}{\sqrt{2}\|\varphi^{-1}\|_\sigma}.$$

Proof. First, we have $\|u_0-\lambda(u_A)\|_\sigma\leqslant\sqrt{2}d((u_0,u_A),W_\sigma)$. Indeed, let $(\lambda(x),x)\in(t_A/W_0\times t_A)_\sigma$ be such that $d((u_0,u_A),W_\sigma)^2=\|u_A-x\|_\sigma^2+\|u_0-\lambda(x)\|_\sigma^2$. We then have

$$\begin{aligned}\|\lambda(u_A))-u_0\|_\sigma^2&\leqslant(\|\lambda(u_A)-\lambda(x)\|_\sigma+\|u_0-\lambda(x)\|_\sigma)^2\\&\leqslant 2(\|u_A-x\|_\sigma^2+\|u_0-\lambda(x)\|_\sigma^2)\\&\leqslant 2d((u_0,u_A),W_\sigma)^2.\end{aligned}$$

Then, define $\widetilde{W}:=\{(\lambda(x),x),x\in t_{A'}\}\subseteq W$. By definition, we have

$$\|u_0-\lambda(u_A)\|_\sigma^2\geqslant\inf_{x\in t_{A'}}\left(\|u_0-\lambda(x)\|_\sigma^2+\|x-u_A\|_\sigma^2\right)=d((u_0,u_A),\widetilde{W}_\sigma)^2.$$

Finally, notice that the image of $\widetilde{W}$ by $\varphi^{-1}\times\mathrm{Id}$ is equal to W'. Therefore,

$$\begin{aligned}d((u_0',u_A),W_\sigma')&=d((\varphi^{-1}\times\mathrm{Id})(u_0,u_A),(\varphi^{-1}\times\mathrm{Id})(\widetilde{W}_\sigma))\\&\leqslant\|\varphi^{-1}\times\mathrm{Id}\,\|_\sigma d((u_0,u_A),\widetilde{W}_\sigma).\end{aligned}$$

To conclude, the norm $\varphi^{-1}\times\mathrm{Id}$ is smaller than $\max(\|\varphi^{-1}\|_\sigma,\|\,\mathrm{Id}\,\|_\sigma)=\max(\|\varphi^{-1}\|_\sigma,1)$. Moreover, the norm $\|\varphi\|_\sigma$ is smaller or equal to 1 because for $x\in t_{A'}/W_0'\otimes_{k_A}k_\sigma$, we have

$$\|\varphi(x+W_{0,v}')\|_\sigma=\inf_{w_0\in W_{0,\sigma}}\|x+w_0\|_\sigma\leqslant\inf_{w_0\in W_{0,\sigma}'}\|x+w_0\|_\sigma=\|x+W_{0,\sigma}'\|_\sigma,$$

meaning that $\|\varphi\|_\sigma\leqslant 1$ for any place σ. Finally, we get $\|\varphi^{-1}\|_\sigma\geqslant 1$ because $1\leqslant\|\,\mathrm{Id}\,\|_\sigma\leqslant\|\varphi\|_\sigma\|\varphi^{-1}\|_\sigma\leqslant\|\varphi^{-1}\|_\sigma$. ∎

From the lower-bound of proposition 7.6, let us apply theorem 4.3. Indeed, (A',u_A) satisfies hypothesis 4.2 by construction, we can apply the theorem to A', W_0', σ, u_A, and u_0 to get a lower bound for $d((u_0',u_A),W_\sigma')$. Taking $E=e$ in the theorem we get

$$\begin{aligned}d((u_0',u_A),W_\sigma')\geqslant-(5(g'+t'))^{\frac{4(g'+t'+1)^2}{t'}}\mathfrak{a}'^{1/t'}\left(1+[k_A:\mathbb{Q}]\mathfrak{a}'\log a'\right)^{g'/t'}\\\times\left(\mathfrak{a}'+[k_A:\mathbb{Q}]\log b'\right)\frac{1}{y'^{1+g'/t'}\deg_L(A')^{1/t'}},\end{aligned}\tag{7.3}$$

with

$$g':=\dim A',\qquad\log a':=\max\left(\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2e^2}{[k_A:\mathbb{Q}]}\right),$$

$$t':=\mathrm{codim}_{t_{A'}}(W_0'),\qquad\log b':=\max\left(h_{\mathcal{O}(1)}(p_0'),h(W_0')\right),$$

$$\mathfrak{a}':=\left\lceil[k_A:\mathbb{Q}]\max\left(1,h_F(A'),\log\mathrm{h}^0(A',L),\log[k_A:\mathbb{Q}],\log\log a'\right)\right\rceil,$$

$$\text{and }y':=\inf_{B\subsetneq A'}\left(\frac{\deg_L B}{\deg_L A'}\right)^{1/(\dim A'-\dim B)}.$$

The strategy to prove theorem 4.6 from proposition 7.6 and (7.3) is to compare the quantities $\|\varphi^{-1}\|_\sigma$, $\log a'$, $\log b'$, $\mathfrak{a}'$, and $\deg_L A'$, in terms of invariants depending on A, p_A, u_A, W_0, and u_0. This is achieved by the following lemmas 7.7 to 7.12, 7.14 and 7.15. Let us define

$$M_A := \max\left(1, \log D, h_F(A), \log \widehat{h}_L(p_A), \log \frac{\|u_A\|^2_{\sigma_0}}{D}\right).$$

Before going into the heart of the proof, we first treat the case $g = 1$ which is much simpler. In this case, the polarisation L is some tensor power L_0^n of the unique principal polarisation L_0 on A. We have $A' = A$, $W_0 = \{0\}$ and therefore

$$d_L((u_0, u_A), W_\sigma) = \sqrt{n} d_{L_0}((u_0, u_A), W_\sigma) \geqslant d_{L_0}((u_0, u_A), W_\sigma).$$

We can directly apply theorem 4.3 to $(A, L_0, p_A, u_A, W_0, u_0)$ as an elliptic curve always satisfies hypothesis 4.2. Taking $E = e$ we get

$$\log d_{L_0}((u_0, u_A), W_\sigma) \geqslant -10^{36} \mathfrak{a}_0 \left(1 + D\mathfrak{a}_0 \log a_0\right) \left(\mathfrak{a}_0 + D \log b_0\right),$$

where we have denoted $\mathfrak{a}_0$, $\log a_0$, and $\log b_0$ the quantities $\mathfrak{a}$, $\log a$, and $\log b$ corresponding to the datum $(A, L_0, p_A, u_A, W_0, u_0)$. We then have

$$\begin{aligned}\mathfrak{a}_0 &\leqslant 2D \max\left(1, h_F(A), \log D, \log^+ \widehat{h}_{L_0}(p_A), 2 + \log \frac{\|u_A\|^2_{\sigma, L_0}}{D}\right) \\ &\leqslant 6D \max\left(1, h_F(A), \log D, \log^+ \widehat{h}_L(p_A), \log \frac{\|u\|^2_{\sigma, L}}{D}\right),\end{aligned}$$

$\log a_0 \leqslant \mathrm{e}^2 \max\left(\widehat{h}_{L_0}(p_A), \frac{\|u_A\|^2_{\sigma, L_0}}{D}\right) \leqslant \mathrm{e}^2 \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma, L}}{D}\right)$, and $\log b_0 = \log b$. We therefore conclude that

$$\begin{aligned}\log d_L((u_0, u_A), W_\sigma) &\geqslant -10^{36} \times 6DM_A \times (1 + 6\mathrm{e}^2) DM_A \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma, L}}{D}\right) \\ &\quad \times 7D \max\left(M_A, \log b\right) \\ &\geqslant -2 \cdot 10^{39} D^3 M_A^2 \max\left(M_A, \log b\right) \max\left(1, \widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma, L}}{D}\right).\end{aligned}$$

Let us now assume that $g \geqslant 2$. A recent result of Rémond gives a very good comparison between $h_F(A')$ and $h_F(A)$.

Lemma 7.7 ([Rém22]). *We have $h_F(A') \leqslant h_F(A) + g \log(\pi\sqrt{2})$.*

The quantity $\log a'$ is also not so difficult to estimate.

Lemma 7.8. *We have $\log a' \leqslant e^2 \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right)$.*

To compare $\deg_L A'$ with invariants depending only on A and u_A, we use a result of Bosser and Gaudron.

Lemma 7.9. *If $g \geqslant 2$, we have*

$$\deg_L A' \leqslant (132g)^{4g^2} D^{2g+1} \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right)^g M_A^{g+1}.$$

Proof. [BG19, Théorème 1.1] states that for $g \geqslant 2$, we have

$$\deg_L A' \leqslant (100g)^{4gg'} \left(D\widehat{h}_L(p_A) + \|u_A\|^2_{\sigma_0}\right)^{g'} \times \left(D \max\left(1, \log(D), h_F(A), \log\left(D\widehat{h}_L(p_A) + \|u_A\|^2_{\sigma_0}\right)\right)\right)^{g'+1}.$$

We now have

$$D\widehat{h}_L(p_A) + \|u_A\|^2_{\sigma_0} \leqslant 2D \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right),$$

and

$$\begin{aligned}\log\left(D\widehat{h}_L(p_A) + \|u_A\|^2_{\sigma_0}\right) &\leqslant \log D + \log\left(2\max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right)\right) \\ &\leqslant (2+\log(2)) \max\left(1, \log D, \log \widehat{h}_L(p_A), \log \frac{\|u_A\|^2_{\sigma_0}}{D}\right).\end{aligned}$$

As g' is bounded by g, we get

$$\deg_L A' \leqslant (100g)^{4g^2} 2^g (2+\log 2)^{g+1} D^{2g+1} \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right)^g M_A^{g+1}.$$

We finally bound the constant. We have

$$2^g(2+\log 2)^{g+1} = \left(2^{1/(4g)}(2+\log 2)^{(g+1)/(4g^2)}\right)^{4g^2}.$$

The terms in the brackets is bounded by 1.32 if $g \geqslant 2$. Therefore, if $g \geqslant 2$, then

$$(100g)^{4g^2} 2^g (2+\log 2)^{g+1} \leqslant (132g)^{4g^2}.$$

■

Lemma 7.9 allows us immediately to bound the quantity $y'^{-(1+g'/t')}(\deg_L A')^{-1/t'}$.

Lemma 7.10. *If $g \geqslant 2$, then*

$$\frac{1}{y'^{1+g/t}(\deg_L A')^{1/t}} \leqslant (132g)^{4g^3} D^{g(2g+1)} \max\left(\widehat{h}_L(p_A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right)^{g^2} M_A^{g(g+1)}.$$

Proof. As $y' \deg_L A' \geqslant 1$ from proposition 4.1 we have

$$\frac{1}{y'^{1+g'/t'}(\deg_L A')^{1/t'}} \leqslant (\deg_L A')^{1+(g'-1)/t'} \leqslant (\deg_L A')^{g'}.$$

We then bound g' by g and use lemma 7.9 to conclude. ■

The result of lemma 7.9 also leads to an estimation for $\log \mathrm{h}^0(A', L)$.

Lemma 7.11. *If $g \geqslant 2$, then*

$$\log \mathrm{h}^0(A', L) \leqslant 13 g^3 M_A.$$

Proof. We have $\log \mathrm{h}^0(A', L) = \log \deg_L A' - \log g'! \leqslant \log \deg_L A'$. Therefore, using lemma 7.9 we have

$$\begin{aligned}\log \mathrm{h}^0(A', L) &\leqslant 4g^2 \log(132g) + (2g+1)\log D \\ &\qquad + g \log \max\left(\widehat{h}_L(A), \frac{\|u_A\|^2_{\sigma_0}}{D}\right) + (g+1)\log M_A \\ &\leqslant \left(4g^2 \log(132g) + (2g+1) + g + (g+1)\right) M_A.\end{aligned}$$

To conclude, if $g \geqslant 2$ we have

$$\begin{aligned}4g^2 \log(132g) + 4g + 2 &= g^3 \left(\frac{4\log(132g)}{g} + \frac{4g+2}{g^3}\right) \\ &\leqslant 13 g^3.\end{aligned}$$

We deduce that $\log \mathrm{h}^0(A', L) \leqslant 13 g^3 M_A$. ∎

We can use this result to bound the quantity $\mathfrak{a}'$.

Lemma 7.12. *If $g \geqslant 2$, then*

$$\mathfrak{a}' \leqslant (59g)^g D M_A.$$

Proof. Recall that we have

$$\mathfrak{a}' = \left\lceil [k_A : \mathbb{Q}] \max\left(1, h_F(A'), \log \mathrm{h}^0(A', L), \log[k_A : \mathbb{Q}], \log\log a'\right)\right\rceil.$$

Using lemmas 7.7, 7.8 and 7.11, we deduce that

$$\begin{aligned}\mathfrak{a}' &\leqslant 2 f(g) D \max\Big(1, h_F(A) + \frac{g}{2}\log(\pi\sqrt{2}), 13 g^3 M_A, \log D + \log f(g), \\ &\qquad 2 + \max\left(\log \widehat{h}_L(p_A), \log \frac{\|u_A\|^2_{\sigma_0}}{D}\right)\Big) \\ &\leqslant 26 g^3 f(g) \cdot D \max\left(1, \log D, h_F(A), \log \widehat{h}_L(p_A), \log \frac{\|u_A\|^2_{\sigma_0}}{D}\right).\end{aligned}$$

The last inequality is justified by the fact that $13g^3$ is always bigger than $1 + \frac{g}{2}\log(\pi\sqrt{2})$, $1 + \log f(g) \leqslant 1 + g\log(3.8g)$, and 3. To conclude, we have $f(g) \leqslant (3.8g)^g$ from lemma 7.4 and if $g \geqslant 2$, we have

$$26 g^3 f(g) \leqslant (3.8g)^g \left(26^{1/g} g^{3/g}\right)^g \leqslant (3.8g)^g \left(26^{1/2} \cdot 3\right)^g \leqslant (59g)^g.$$

∎

The remaining quantities to bound are $\log \|\varphi^{-1}\|_\sigma$ and $\log b'$. Until now, all the estimations only involved quantities related to our abelian variety A but the upcoming ones will also have to take into account W_0 and u_0. We define

$$\log b = \max\left(h_{\mathcal{O}(1)}(p_0), h(W_0)\right).$$

We first prove a general result about norms of linear applications that we will use to bound $\|\varphi^{-1}\|_\sigma$.

Lemma 7.13. *Let K be a number field and let $\overline{\mathcal{E}}$, $\overline{\mathcal{F}}$ be two Hermitian adelic vector bundles over $\operatorname{Spec}\mathcal{O}_K$ of dimension n. Let $\psi : \mathcal{E} \to \mathcal{F}$ be an isomorphism. For any place v of K, we have*

$$\|\psi\|_v \leqslant \|\psi^{-1}\|_v^{n-1} |\det \psi|_v,$$

for the operator norm induced by the structure of K_v-normed spaces on E_v and F_v.

Proof. First assume that v is non-Archimedean. Let $(e_1, \dots, e_n)$ be a basis of $\mathcal{E}$ such for any $a_1, \dots, a_n \in K_v$, we have

$$\left\| \sum_{i=1}^n a_i e_i \right\|_v = \max_{1 \leqslant i \leqslant n} |a_i|_v.$$

Similarly, consider a basis $(f_1, \dots, f_n)$ of $\mathcal{F}$, such that for all $b_1, \dots, b_n \in K_v$, we have

$$\left\| \sum_{j=1}^n b_j f_j \right\|_v = \max_{1 \leqslant j \leqslant n} |b_j|_v.$$

We get the following diagram of K_v-normed vector spaces.

$$\begin{array}{ccc} E_v & \xrightarrow{\psi} & F_v \\ \downarrow{\scriptstyle P} & & \downarrow{\scriptstyle Q} \\ K_v^n & \xrightarrow{\Psi} & K_v^n \end{array}$$

where P and Q are the applications induced by the bases $(e_1, \dots, e_n)$ and $(f_1, \dots, f_n)$, and Ψ is the matrix $Q\psi P^{-1}$ corresponding to ψ. By construction, we have $\|\psi\|_v = \|\Psi\|_v$. Moreover, the inverse of Ψ^{-1} is equal to $\det(\Psi)C^{\mathrm{T}}$, where C is the cofactor matrix of Ψ^{-1}. As the coefficients of C consist of minors of Ψ^{-1} of size $n-1$, we have $\|C\|_v \leqslant \|\Psi^{-1}\|_v^{n-1}$. Therefore, we get

$$\|\psi\|_v = \|\Psi\|_v \leqslant |\det \Psi|_v \|C\|_v \leqslant |\det \Psi|_v \|\Psi^{-1}\|_v^{n-1} = \|\psi^{-1}\|_v^{n-1} |\det \psi|_v.$$

If v is Archimedean, the v-norm of ψ is equal to the square root of the norm of the biggest eigenvalue of $\overline{\psi}^{\mathrm{T}}\psi$. Let us denote λ_1, $\lambda_2 \dots, \lambda_n$ the spectrum of $\overline{\psi}^{\mathrm{T}}\psi$ with $0 < |\lambda_1|_v \leqslant \dots \leqslant |\lambda_n|_v$. We then have $\|\psi\|_v^2 = |\lambda_n|_v$ and $\|\psi^{-1}\|_v^2 = |\lambda_1|_v^{-1}$. This leads to

$$\|\psi\|_v^2 = |\lambda_n|_v = |\lambda_1 \cdots \lambda_n|_v \times |\lambda_1 \cdots \lambda_{n-1}|_v^{-1} \leqslant |\det\left(\overline{\psi}^{\mathrm{T}}\psi\right)|_v |\lambda_1|_v^{-n+1} = \|\psi^{-1}\|_v^{2(n-1)} |\det \psi|_v^2.$$

This proves that $\|\psi\|_v \leqslant \|\psi^{-1}\|_v^{n-1} |\det \psi|_v$ in the Archimedean case too. ∎

We now apply lemma 5.12 to φ^{-1}.

Lemma 7.14. *If $g \geqslant 2$, we have*

$$\log \|\varphi^{-1}\|_\sigma \leqslant (94g)^g D \max(M_A, \log b).$$

Proof. Take $\psi := \varphi^{-1}$ in lemma 5.12 and any place v of k_A. We get $\|\varphi^{-1}\|_v \leqslant \|\varphi\|_v^{t'-1} |\det \varphi^{-1}\|_v$. We claim that the v-norm of φ is always less or equal to 1. Indeed, for $x \in t_{A'}/W_0' \otimes_{k_A} k_v$, we have

$$\|\varphi(x + W_{0,v}')\|_v = \inf_{w_0 \in W_{0,v}} \|x + w_0\|_v \leqslant \inf_{w_0 \in W_{0,v}'} \|x + w_0\|_v = \|x + W_{0,v}'\|_v,$$

meaning that $\|\varphi\|_v \leqslant 1$ for any place v. We deduce that for our embedding σ, we have $\log \|\varphi^{-1}\|_\sigma \leqslant \log |\det \varphi^{-1}|_\sigma \leqslant D[k_A : k] h(\det \varphi^{-1})$. Moreover, from [Gau21, Proposition 42] we can express the height of $\det \varphi$ in terms of Arakelov degrees in the following way:

$$h(\det \varphi^{-1}) = \widehat{\deg}_{\mathrm{n}} \left(\overline{(t_{\mathcal{A}'} + \mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A})/(\mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A})} \right) - \widehat{\deg}_{\mathrm{n}} \left(\overline{t_{\mathcal{A}'}/\mathcal{W}_0'} \right).$$

Using the inequalities $\widehat{\deg}_{\mathrm{n}} \left(\overline{\mathcal{W}_0'} \right), \widehat{\deg}_{\mathrm{n}} \left(\overline{t'_{\mathcal{A}} + \mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A}} \right) \leqslant g \max \left(0, \widehat{\mu}_{\max} \left(\overline{t_{\mathcal{A}}} \right) \right)$ coming from the very definition of the maximal slope, we deduce a first estimation for the norm of φ relative to $\sigma \mid \sigma_0$.

$$\begin{aligned} \log \|\varphi^{-1}\|_\sigma &\leqslant [k_A : k] D \left(\widehat{\deg}_{\mathrm{n}} \left(\overline{t_{\mathcal{A}'} + \mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A}} \right) - \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{W}_0}) - \widehat{\deg}_{\mathrm{n}}(\overline{t_{\mathcal{A}'}}) + \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{W}_0'}) \right) \\ &\leqslant f(g) D \left(2g \max(0, \widehat{\mu}_{\max}(\overline{t_{\mathcal{A}}})) + h(W_0) + h_F(A') + \frac{1}{2} \log \mathrm{h}^0(A', L) \right). \end{aligned}$$

From proposition 3.28, the maximal slope of $\overline{t_{\mathcal{A}}}$ is bounded by $12 h_F(A) + 16g \log(24g)$. Applying lemmas 7.7 and 7.11, we get

$$\begin{aligned} \log \|\varphi^{-1}\|_\sigma &\leqslant f(g) D \left(32g^2 \log(24g) + (24g+1) h_F(A) + g \log(\pi\sqrt{2}) + h(W_0) + \frac{13g^3}{2} M_A \right) \\ &\leqslant (3.8g)^g \left(32g^2 \log(24g) + 24g + 1 + g \log(\pi\sqrt{2}) + 1 + 6.5g^3 \right) D \max(M_A, \log b) \\ &\leqslant (94g)^g D \max(M_A, \log b). \end{aligned}$$

■

To conclude, we look at the term $\log b' = \max \left(h_{\mathcal{O}(1)}(p_0'), h(W_0') \right)$. The following result bounds it in terms of M_A and $\log b := \max \left(h_{\mathcal{O}(1)}(p_0), h(W_0) \right)$.

Lemma 7.15. *If $g \geqslant 2$, we have*

$$\log b' \leqslant 42g^3 \max(M_A, \log b).$$

Proof. First, applying the inequality $\widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{F}}) + \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{G}}) \leqslant \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{F} + \mathcal{G}}) + \widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{F} \cap \mathcal{G}})$ from proposition 3.6 with $\overline{\mathcal{F}} = \overline{\mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A}}$ and $\overline{\mathcal{G}} = \overline{t_{\mathcal{A}'}}$, we get

$$\begin{aligned} -\widehat{\deg}_{\mathrm{n}} \left(\overline{\mathcal{W}_0'} \right) &\leqslant -\widehat{\deg}_{\mathrm{n}} \left(\overline{\mathcal{W}_0} \right) - \widehat{\deg}_{\mathrm{n}}(\overline{t_{\mathcal{A}'}}) + \widehat{\deg}_{\mathrm{n}} \left(\overline{\mathcal{W}_0 \otimes_{\mathcal{O}_k} \mathcal{O}_{k_A} + t_{\mathcal{A}'}} \right) \\ &\leqslant h(W_0) + h_F(A') + \frac{1}{2} \log h^0(A', L) + g \max \left(0, \widehat{\mu}_{\max} \left(\overline{t_{\mathcal{A}}} \right) \right). \end{aligned}$$

Using the upper bound $g\max\left(0,\widehat{\mu}_{\max}\left(\overline{t_{\mathcal{A}}}\right)\right)\leqslant 12gh_F(A)+16g^2\log(24g)$ from proposition 3.28, and lemmas 7.7 and 7.11, we deduce

$$\begin{aligned}-\widehat{\deg}_{\mathrm{n}}(\overline{\mathcal{W}_0'}) &\leqslant h(W_0)+h_F(A)+g\log(\pi\sqrt{2})+\frac{13g^3}{2}M_A+12gh_F(A)+16g^2\log(24g)\\ &\leqslant \Big(1+1+g\log(\pi\sqrt{2})+6.5g^3+12g+16g^2\log(24g)\Big)\max(M_A,\log b)\\ &\leqslant 42g^3\max(M_A,\log b).\end{aligned}$$

Let us now bound $h_{\mathcal{O}(1)}(p_0')$. From the definition $u_0'=\varphi^{-1}(u_0)$ we deduce using [Gau06, §4.4.3] that $h_{\mathcal{O}(1)}(p_0')\leqslant h(\varphi)+h_{\mathcal{O}(1)}(p_0)$. As we have already seen, for any place v, the v-norm of φ is less than or equal to 1 and therefore $h(\varphi)$ is non-positive. We finally get

$$\log b'\leqslant\max\left(h_{\mathcal{O}(1)}(p_0'),h(W_0')\right)\leqslant 42g^3\max(M_A,\log b).$$

■

We are finally ready to prove theorem 4.6. Recall that from proposition 7.6 and (7.3), we have

$$\begin{aligned}\log d(u,W_\sigma)\geqslant{}&-(5(g'+t'))^{\frac{4(g'+t'+1)^2}{t'}}\mathfrak{a}'^{1/t'}\left(1+[k_A:\mathbb{Q}]\mathfrak{a}'\log a'\right)^{g'/t'}\\ &\times(\mathfrak{a}'+[k_A:\mathbb{Q}]\log b')\times\frac{1}{y'^{1+g'/t'}\deg_L(A')^{1/t'}}-\log\sqrt{2}-\log\|\varphi^{-1}\|_\sigma.\end{aligned}$$

Moreover, we have proved that

- $\mathfrak{a}'\leqslant(59g)^gDM_A$ (lemma 7.12);
- $\log a'\leqslant \mathrm{e}^2\max\left(\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)$ (lemma 7.8);
- $\log b'\leqslant 42g^3\max(M_A,\log b)$ (lemma 7.15);
- $\dfrac{1}{y'^{1+g'/t'}(\deg_L A')^{1/t'}}\leqslant(132g)^{4g^3}D^{g(2g+1)}\max\left(\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)^{g^2}M_A^{g(g+1)}$ (lemma 7.10);
- $\log\|\varphi^{-1}\|_\sigma\leqslant(94g)^gD\max(M_A,\log b)$ (lemma 7.14).

Using lemmas 7.8 and 7.12 we can bound the term $1+[k_A:\mathbb{Q}]\mathfrak{a}'\log a'$:

$$\begin{aligned}1+[k_A:\mathbb{Q}]\mathfrak{a}'\log a' &\leqslant(1+f(g)(59g)^g\mathrm{e}^2)\max\left(1,D\times DM_A\times\max\left(\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)\right)\\ &\leqslant\left(1+(3.8g)^g(59g)^g\mathrm{e}^2\right)D^2M_A\max\left(1,\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)\\ &\leqslant(25g)^{2g}D^2M_A\max\left(1,\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right).\end{aligned}$$

Similarly, we can bound the term $\mathfrak{a}'+[k_A:\mathbb{Q}]\log b'$ using lemmas 7.12 and 7.15:

$$\begin{aligned}\mathfrak{a}'+[k_A:\mathbb{Q}]\log b' &\leqslant(59g)^gDM_A+f(g)\times 42g^3D\max(M_A,\log b)\\ &\leqslant\left((59g)^g+(3.8g)^g\times 42g^3\right)D\max(M_A,\log b)\\ &\leqslant(92g)^gD\max(M_A,\log b).\end{aligned}$$

Using these inequalities together with lemmas 7.10 and 7.14, we get

$$\begin{aligned}\log d(u,W_\sigma) \geqslant &-\left(5(g'+t')\right)^{\frac{4(g'+t'+1)^2}{t'}}(59g)^{g/t'}(25g)^{2gg'/t'}(92g)^g(132g)^{4g^3}\Big)(DM_A)^{1/t'}\\ &\times D\max(M_A,\log b)\left(D^2M_A\max\left(1,\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)\right)^{g'/t'}\\ &\times D^{g(2g+1)}\max\left(\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)^{g^2}M_A^{g(g+1)}\\ &-\log\sqrt{2}-(94g)^gD\max(M_A,\log b)\\ \geqslant &-c(g)D^{(2g+1)(g+1)}\max\left(1,\widehat{h}_L(p_A),\frac{\|u_A\|_{\sigma_0}^2}{D}\right)^{g^2+g}M_A^{(g+1)^2}\max(M_A,\log b),\end{aligned}$$

with

$$c(g)=(10g)^{4(g+2)^2}(59g)^g(25g)^{2g^2}(92g)^g(132g)^{4g^3}+\log\sqrt{2}+(94g)^g\leqslant(265000g)^{4g^3}.$$

Notice that we have bounded $\frac{4(g'+t'+1)^2}{t'}$ by $4(g+2)^2$ because $x\mapsto\frac{4(g'+x+1)^2}{x}$ is decreasing for $x\in[1,g']$, therefore maximal at $x=1$ with value $4(g'+2)^2\leqslant 4(g+2)^2$. We are finally done in the case $g\geqslant 2$.

References on linear forms in abelian logarithms

[Aut13] Pascal Autissier. "Un lemme matriciel effectif". In: *Mathematische Zeitschrift* 273.1-2 (2013), pp. 355–361. DOI: 10.1007/s00209-012-1008-x (cited on p. 55).

[Bak66] A. Baker. "Linear forms in the logarithms of algebraic numbers. I, II, III". In: *Mathematika. A Journal of Pure and Applied Mathematics* 13 (1966), 204–216, ibid. 14 (1967), 102–107, ibid. 14 (1967), 220–228. DOI: 10.1112/s0025579300003843 (cited on pp. 18, 24).

[BG19] Vincent Bosser and Éric Gaudron. "Logarithmes des points rationnels des variétés abéliennes". In: *Canadian Journal of Mathematics. Journal Canadien de Mathématiques* 71.2 (2019), pp. 247–298. DOI: 10.4153/cjm-2018-005-7 (cited on pp. 21, 27, 36, 46, 55, 62, 83, 112, 115).

[BL04] Christina Birkenhake and Herbert Lange. *Complex Abelian Varieties*. Red. by A. Chenciner et al. Vol. 302. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. ISBN: 978-3-662-06307-1. DOI: 10.1007/978-3-662-06307-1 (cited on pp. 33–35).

[Bos91] Jean-Benoît Bost. "Théorie de l'intersection et théorème de Riemann-Roch arithmétiques". In: *Astérisque*. 201-203. 1991, Exp. No. 731, 43–88 (1992) (cited on p. 39).

[Bos96a] Jean-Benoît Bost. "Intrinsic heights of stable varieties and abelian varieties". In: *Duke Mathematical Journal* 82.1 (1996), pp. 21–70. DOI: 10.1215/S0012-7094-96-08202-2 (cited on p. 37).

[Bos96b] Jean-Benoît Bost. "Périodes et isogenies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)". In: *Astérisque*. 237. 1996, Exp. No. 795, 4, 115–161 (cited on p. 38).

[Bru02] S. Bruiltet. "D'une mesure d'approximation simultanée à une mesure d'irrationalité : le cas de $\Gamma(1/4)$ et $\Gamma(1/3)$". In: *Acta Arithmetica* 104 (2002), pp. 243–281. DOI: 10.4064/aa104-3-3 (cited on p. 77).

[Dav95] Sinnou David. "Minorations de formes linéaires de logarithmes elliptiques". In: *Mémoires de la Société Mathématique de France. Nouvelle Série* 62 (1995), pp. iv+143 (cited on pp. 19, 25).

[DH02] Sinnou David and Noriko Hirata-Kohno. "Recent progress on linear forms in elliptic logarithms". In: *A Panorama of Number Theory or the View from Baker's Garden (Zürich, 1999)*. Cambridge Univ. Press, Cambridge, 2002, pp. 26–37. DOI: 10.1017/CBO9780511542961.004 (cited on pp. 20, 26).

[Gau05] Éric Gaudron. "Mesures d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif". In: *Inventiones Mathematicae* 162.1 (2005), pp. 137–188. DOI: 10.1007/s00222-005-0440-5 (cited on pp. 19, 25).

[Gau06] Éric Gaudron. "Formes linéaires de logarithmes effectives sur les variétés abéliennes". In: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 39.5 (2006), pp. 699–773. DOI: 10.1016/j.ansens.2006.09.001 (cited on pp. 19–21, 25–27, 39, 41, 45, 46, 75, 77, 119).

[Gau08] Éric Gaudron. "Pentes des fibrés vectoriels adéliques sur un corps global". In: *Rendiconti del Seminario Matematico della Università di Padova. Mathematical Journal of the University of Padua* 119 (2008), pp. 21–95. DOI: 10.4171/RSMUP/119-2 (cited on pp. 29, 32, 76).

[Gau14] Éric Gaudron. "Minorations simultanées de formes linéaires de logarithmes de nombres algébriques". In: *Bulletin de la Société Mathématique de France* 142.1 (2014), pp. 1–62. DOI: 10.24033/bsmf.2658 (cited on pp. 19, 25, 29, 31, 45, 61).

[Gau19] Éric Gaudron. "Some explicit computations in Arakelov geometry of abelian varieties". In: *Journal of the Ramanujan Mathematical Society* 34.4 (2019), pp. 433–447 (cited on pp. 38, 41, 55).

[Gau21] Éric Gaudron. "Chapter II: Minima and slopes of rigid adelic spaces". In: *Arakelov Geometry and Diophantine Applications*. Vol. 2276. Lecture Notes in Math. Springer, Cham, 2021, pp. 37–76. DOI: 10.1007/978-3-030-57559-5_3 (cited on pp. 29–32, 118).

[Gel34] A. Gelfond. "On the seventh Hilbert problem". In: *Bulletin de l'Académie des Sciences de l'URSS. VII. Série* 1934.4 (1934), pp. 623–630 (cited on pp. 17, 23).

[GPZ94] J. Gebel, A. Pethö, and H. G. Zimmer. "Computing integral points on elliptic curves". In: *Acta Arithmetica* 68.2 (1994), pp. 171–192. DOI: 10.4064/aa-68-2-171-192 (cited on pp. 19, 25).

[GR13] Éric Gaudron and Gaël Rémond. "Minima, pentes et algèbre tensorielle". In: *Israel Journal of Mathematics* 195.2 (2013), pp. 565–591. DOI: 10.1007/s11856-012-0109-x (cited on pp. 29, 32).

[GR14a] Éric Gaudron and Gaël Rémond. "Polarisations et isogénies". In: *Duke Mathematical Journal* 163.11 (2014), pp. 2057–2108. DOI: 10.1215/00127094-2782528 (cited on p. 44).

[GR14b] Éric Gaudron and Gaël Rémond. "Théorème des périodes et degrés minimaux d'isogénies". In: *Commentarii Mathematici Helvetici. A Journal of the Swiss Mathematical Society* 89.2 (2014), pp. 343–403. DOI: 10.4171/CMH/322 (cited on pp. 36, 60, 103).

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496. ISBN: 978-0-387-90244-9 (cited on p. 38).

[Kem93] George R. Kempf. *Algebraic varieties*. Vol. 172. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1993. x+163. ISBN: 9780521426138. DOI: 10.1017/CBO9781107359956. URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1252397 (visited on 07/04/2022) (cited on p. 40).

[KR18] Tünde Kovács and Zsolt Rábai. "Equal values of pyramidal numbers". In: *Koninklijke Nederlandse Akademie van Wetenschappen. Indagationes Mathematicae. New Series* 29.5 (2018), pp. 1157–1166. DOI: 10.1016/j.indag.2018.01.010 (cited on pp. 19, 25).

[Lin82] F. Lindemann. "Über die Ludolph'sche Zahl". In: *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften* 1882 (1882), pp. 679–682 (cited on pp. 17, 23).

[Mor85] Laurent Moret-Bailly. "Pinceaux de variétés abéliennes". In: *Astérisque* 129 (1985) (cited on p. 37).

[Mum99] David Mumford. *The red book of varieties and schemes*. expanded. Vol. 1358. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1999. x+306. ISBN: 978-3-540-63293-1. DOI: 10.1007/b62130 (cited on p. 38).

[Nak07] Michael Nakamaye. "Multiplicity estimates on commutative algebraic groups". In: *Journal für die reine und angewandte Mathematik. [Crelle's Journal]* 607 (2007), pp. 217–235. DOI: 10.1515/CRELLE.2007.049 (cited on pp. 45, 52).

[PW88] Patrice Philippon and Michel Waldschmidt. "Formes linéaires de logarithmes sur les groupes algébriques commutatifs". In: *Illinois Journal of Mathematics* 32.2 (1988), pp. 281–314 (cited on pp. 19, 25).

[Rém20] Gaël Rémond. "Degré de définition des endomorphismes d'une variété abélienne". In: *Journal of the European Mathematical Society (JEMS)* 22.9 (2020), pp. 3059–3099. DOI: 10.4171/jems/981 (cited on p. 112).

[Rém22] Gaël Rémond. "Propriétés de la hauteur de Faltings". In: *Ann. Scuola Norm. Sup* (2022), pp. 1589–1596. DOI: 10.2422/2036-2145.202010_062 (cited on pp. 21, 27, 114).

[Sch35] Theodor Schneider. "Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen". In: *Journal für die reine und angewandte Mathematik. [Crelle's Journal]* 172 (1935), pp. 65–69. DOI: 10.1515/crll.1935.172.65 (cited on pp. 17, 23).

[SdW99] Roelof J. Stroeker and Benjamin M. M. de Weger. "Solving elliptic Diophantine equations: the general cubic case". In: *Acta Arithmetica* 87.4 (1999), pp. 339–365. DOI: 10.4064/aa-87-4-339-365 (cited on pp. 19, 25).

[ST94] R. J. Stroeker and N. Tzanakis. "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms". In: *Acta Arithmetica* 67.2 (1994), pp. 177–196. DOI: 10.4064/aa-67-2-177-196 (cited on pp. 19, 25).

[Tza02] N. Tzanakis. "Effective solution of two simultaneous Pell equations by the elliptic logarithm method". In: *Acta Arithmetica* 103.2 (2002), pp. 119–135. DOI: 10.4064/aa103-2-2 (cited on pp. 19, 25).

[Wei85] C. Weierstrass. "Zu Lindemann's Abhandlung: "Über die Ludolph'sche Zahl"". In: *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften* 1885 (1885), pp. 1067–1086 (cited on pp. 17, 23).

[Wüs89] G. Wüstholz. "Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen". In: *Annals of Mathematics. Second Series* 129.3 (1989), pp. 501–517. DOI: 10.2307/1971515 (cited on pp. 19, 25).

Part II

Modular Galois representations

Chapter 8

English introduction

This part of the thesis mainly comes from the article [Pea21]. Chapters 8 and 10 have been lengthened a bit, slight changes have been made in chapters 11 and 13 and sections 15.1 and 15.1.2, and chapter 14 and section 15.2 are mainly new and the corresponding section [Pea21, 5. Dihedral Representations] has been augmented with new results.

8.1 Residual modular representations

Among all modular forms, the most famous one is with no doubt the Ramanujan Delta function. Considered and first studied by Ramanujan in 1916 in [Ram00, §15-19], it can be defined as

$$\Delta := q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=0}^{\infty}\tau(n)q^n.$$

Since this seminal article, many mathematicians have studied the properties of the tau and delta functions. Apart from being the Fourier coefficients of a modular newform for the whole modular group, the coefficients $(\tau(n))_{n\in\mathbb{N}}$ satisfy the following surprising congruence relations.

$$\begin{array}{lll}
\tau(p) \equiv 1 + p^{11} & (\text{mod } 2^5), & \text{for all primes } p \neq 2;\\
\tau(p) \equiv p^2 + p^9 & (\text{mod } 3^3), & \text{for all primes } p;\\
\tau(p) \equiv p + p^{10} & (\text{mod } 5^2), & \text{for all primes } p;\\
\tau(p) \equiv p + p^4 & (\text{mod } 7), & \text{for all primes } p;\\
\tau(p) \equiv \left(\frac{p}{23}\right)\tau(p) & (\text{mod } 23), & \text{for all primes } p \neq 23;\\
\tau(p) \equiv 1 + p^{11} & (\text{mod } 691), & \text{for all primes } p,
\end{array} \tag{8.1}$$

where $\left(\frac{p}{23}\right)$ denotes the Legendre symbol at p and 23. Note the one can prove more general relations modulo higher powers of 2, 3, 5, 7, 23 and 691. See the beginning of [Swi73] for a statement and references for those congruences.

For long, no geometric setup had been given to explain the congruences (8.1). In his Delange–Pisot–Poitou lecture in 1968 [Ser69], Jean-Pierre Serre proposed a conjecture relative to the existence of a certain Galois representation attached to Δ. It states the following.

Conjecture 8.1 ([Ser69, 3.2. Conjecture]). *Let ℓ be a prime number and denote by K_ℓ the maximal extension of $\mathbb{Q}$ unramified outside ℓ. There exists a continuous linear representation*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}(V_\ell),$$

where V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension 2, satisfying the following condition:

(C) For every prime number $p \neq \ell$, the characteristic polynomial of a Frobenius element at p is equal to $X^2 - \tau(p)X + p^{11}$.

As explained by Serre, this conjecture gives a Galois theoretic explanation for the congruences (8.1). Indeed, there is always a lattice in V_ℓ that is stable under the action of Galois induced by ρ_ℓ. A choice of basis for this lattice induces a representation $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ that has the same trace and determinant as ρ_ℓ. One can then reduce this representation modulo ℓ^n to get a representation

$$\rho_{\ell,n} : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

In this setup, the previous congruences can be reformulated, up to semi-simplification, as

$$\begin{aligned} &\rho_{2,5} \cong \mathbb{1} \oplus \overline{\chi}_{2^5}^{11}; && \rho_{7,1} \cong \overline{\chi}_7 \oplus \overline{\chi}_7^4; \\ &\rho_{3,2} \cong \overline{\chi}_{3^3}^2 \oplus \overline{\chi}_{3^3}^9; && \rho_{23,1} \cong \left(\tfrac{\cdot}{23}\right) \otimes \rho_{23,1}; \\ &\rho_{5,2} \cong \overline{\chi}_{5^2} \oplus \overline{\chi}_{5^2}^{10}; && \rho_{691,1} \cong \mathbb{1} \oplus \overline{\chi}_{691}^{11}, \end{aligned} \tag{8.2}$$

where $\overline{\chi}_{\ell^n}$ is the cyclotomic character modulo ℓ^n. With this reformulation arise several questions. Are the primes 2, 3, 5, 7, 23, and 691 the only primes for which isomorphisms as in (8.2) appear? Is there a way to predict and compute these isomorphisms? Is conjecture 8.1 true and does it generalise to other modular newforms?

The answer to the last question is in fact affirmative since Deligne in 1969 and Deligne–Serre in 1974 proved the following result for all modular forms of weight $k \geqslant 2$ and $k = 1$ respectively.

Theorem 8.2 ([Del71], [DS74, Théorème 4.1]). *Let k, N be two positive integers, and let ε be a Dirichlet character modulo N. Let f be a newform of weight k, level N, and character ε. Denote by K_f the number field generated by the Fourier coefficients of f.*

For every prime ideal λ in the ring of integers of K_f of residue characteristic ℓ, there exists a continuous Galois representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(F),$$

where $F = K_{f,\lambda}$ is the λ-adic completion of K_f if $k \geqslant 2$, and $F = \mathbb{C}$ if $k = 1$, satisfying the following conditions:

1. *The representation $\rho_{f,\lambda}$ is unramified outside $N\ell$;*
2. *For every prime number $p \nmid N\ell$, the characteristic polynomial of a Frobenius element at p is equal to $X^2 - a_p(f)X + p^{k-1}\varepsilon(p)$, where $a_p(f)$ denotes the p-th Fourier coefficient of f.*

Theorem 8.2 is the starting point of many theorems and conjectures of the second half of the twentieth century and many are still active today. Among others, one can cite Serre's conjecture [Ser87], Wiles' modularity theorem [Wil95, Theorem 0.4], the questions of level raising [DT94] and lowering [Rib90, Theorem 1.1], and so on.

As explained by Ribet in [Rib77, Theorem (2.3)], the conditions 1 and 2 characterise entirely $\rho_{f,\lambda}$ up to isomorphism and ensure that it is always irreducible.

Let us now focus on the case $k \geqslant 2$ – the case of modular forms of weight 1 being a whole story on its own. We fix a newform f of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε. Let λ be a prime ideal of the ring of integers $\mathcal{O}_{K_f}$ of K_f. As before, one can construct a lattice of $K_{f,\lambda}^2$ that is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This leads to a representation with values in the local ring of $K_{f,\lambda}$ that we can reduce modulo λ. Writing $\mathbb{F}_\lambda$ the residue field of λ, we get a representation

$$\widetilde{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda).$$

This representation depends on the lattice used to reduce $\rho_{f,\lambda}$. However, the Brauer–Nesbitt theorem ensures that semi-simplifying $\widetilde{\rho}_{f,\lambda}$ leads to a representation $\overline{\rho}_{f,\lambda}$ with values in $\mathbb{F}_\lambda$ uniquely characterised up to isomorphism by the following properties:

1. The representation $\overline{\rho}_{f,\lambda}$ is semi-simple;
2. The represenattion $\overline{\rho}_{f,\lambda}$ is unramified outside $N\ell$;
3. For every prime number $p \nmid N\ell$, the characteristic polynomial of a Frobenius element at p is equal to $X^2 - a_p(f)X + p^{k-1}\varepsilon(p) \pmod{\lambda}$.

Remark 8.3. *Notice that the reduction modulo λ indeed makes sense for $a_p(f)$ and $\varepsilon(p)$ because it is a fact that the coefficients of f are all algebraic integers and that K_f contains the values of the character of f. See [Rib77, Corollary (3.1)] for a proof of this fact.*

Again Čebotarev density theorem and Brauer–Nesbitt theorem ensure that $\overline{\rho}_{f,\lambda}$ is entirely determined by the conditions 1, 2, and 3. However, $\overline{\rho}_{f,\lambda}$ may no longer be irreducible. The starting point of this part of the present thesis is the following theorem proved by Ribet in 1975 for modular forms of level 1 and in 1985 for modular forms of arbitrary level, and generalising results of Serre and Swinnerton-Dyer of 1973 for $N = 1$ and $K_f = \mathbb{Q}$ [Ser73; Swi73].

Theorem 8.4 ([Rib85, Theorem 2.1])**.** *For all but finitely many λ the representation $\overline{\rho}_{f,\lambda}$ is irreducible. Furthermore, if f is not a form with complex multiplication (see definition 14.3), then for all but finitely many λ, the order of the image of $\overline{\rho}_{f,\lambda}$ is divisible by ℓ.*

Theorem 8.4 gives a first answer to Serre's questions about the congruences of the tau function: there is indeed a finite number of primes ℓ such that for some integers a and b, $\tau(p)$ is congruent modulo ℓ to $p^a + p^b$ for all but finitely many primes (and they in fact appear only for $\ell = 2$, 3, 5, 7, and 691). Indeed, this kind of congruences corresponds exactly to the primes for which $\overline{\rho}_{\Delta,\ell}$ is reducible. To understand how the congruences of tau modulo 23 is related to Ribet's theorem, we need to make it more precise. The classification of the subgroups of PSL_2 of a finite field is known since Dickson [Dic01, Chapter XII]. It goes as follows.

Theorem 8.5 ([Hup67, Hauptsatz 8.27]). *Let $q := p^f$ be a power of a prime number p. A subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ is isomorphic to one the following groups.*

1. *A cyclic group of order z dividing $\frac{q\pm1}{\gcd(q-1,2)}$;*
2. *A dihedral group of order $2z$ with z dividing $\frac{q\pm1}{\gcd(q-1,2)}$;*
3. *The alternating group $\mathfrak{A}_4$, only if $p > 2$ or $q = 2^{2n}$;*
4. *The symmetric group $\mathfrak{S}_4$, only if $q^2 \equiv 1 \pmod{16}$;*
5. *The alternating group $\mathfrak{A}_5$, only if $p = 5$, or $q^2 \equiv 1 \pmod{5}$;*
6. *$(\mathbb{Z}/p\mathbb{Z})^n$ for some non-negative integers n;*
7. *A semi-direct product $(\mathbb{Z}/p\mathbb{Z})^n \rtimes \mathbb{Z}/m\mathbb{Z}$ for some non-negative integer n and m dividing $p^n - 1$ and $q - 1$ respectively;*
8. *$\mathrm{PSL}_2(\mathbb{F}_{p^n})$ for some integer n dividing f;*
9. *$\mathrm{PGL}_2(\mathbb{F}_{p^n})$ for some integer n dividing $2f$.*

Using theorem 8.5 and the fact that we can always embed $\mathrm{PGL}_2(\mathbb{F}_q)$ into $\mathrm{PSL}_2(\mathbb{F}_{q^2})$, we can reformulate Ribet's theorem.

Corollary 8.6. *Let f be a newform. There are only finitely many prime ideals λ that satisfy one of the following properties.*

1. *The representation $\overline{\rho}_{f,\lambda}$ is reducible;*
2. *The form f is not CM and the projective image of $\overline{\rho}_{f,\lambda}$ in $\mathrm{PGL}_2(\mathbb{F}_\lambda)$ is isomorphic to a dihedral group D_{2n} with $\ell \nmid 2n$, where ℓ is the residue characteristic of λ;*
3. *The projective image of $\overline{\rho}_{f,\lambda}$ in $\mathrm{PGL}_2(\mathbb{F}_\lambda)$ is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$, or $\mathfrak{A}_5$.*

We call a prime ideal that satisfies one of these properties an "exceptional ideal".

Remark 8.7. *Despite the fact that the hypothesis f not CM appears in the second part of theorem 8.4, the proof of [Rib85, Theorem 2.1] used it only in the dihedral case.*

The isomorphism modulo 23 in (8.2) falls in the second case of corollary 8.6. From this point two natural questions arise.

I) For each case of corollary 8.6, can we bound the residue characteristic of the "exceptional ideals" in terms of invariants of the modular f (such as the weight, the level, or the character)?

II) For each case of corollary 8.6, can we compute the exceptional ideals?

For modular forms of level 1, the result of Ribet from 1975 gives an explicit description of the prime ideals for which the associated representation is reducible. However, it was no more the case in 1985. For the second and third cases of corollary 8.6, even the 1975's proof was not effective. The first step in making Ribet's result effective has been accomplished by Billerey and Dieulefait in 2014 [BD14]. Assuming that the character of f is trivial, they gave explicit criteria for the residue characteristics ℓ of λ in terms of k and N, for $\overline{\rho}_{f,\lambda}$ to be reducible. In the two other cases, they gave explicit bounds for ℓ, in terms of k and N. The goal of this part of the thesis is to pursue this work and to give as many answers as possible to questions I and II.

8.2 Overview of the results

Let $f = q + \sum_{n=2}^{\infty} a_n(f)q^n$ be a newform of weight k, level N, and character ε of conductor $\mathfrak{c}$. Let $K_f := \mathbb{Q}(a_n(f))_{n\geqslant 2}$ be the coefficients' field of f, and let λ be a prime ideal in the ring of integers of K_f above a rational prime number ℓ. The contributions of this part of the thesis are twofold. On the one hand they extend the results of [BD14] to all newforms of arbitrary weight, level, and character, giving an explicit bound in all three cases of corollary 8.6 in terms of k, N, and ε. On the other hand, we give in the reducible and dihedral cases an algorithm that, given the level, the weight, the character, and a finite number of Fourier coefficients of f, computes all the reducible prime ideals and all the dihedral prime ideals.

The general ideas we use to prove our results come back to Serre and Swinnerton-Dyer [Ser73; Swi73]. The three special cases of corollary 8.6 can be formulated in terms of congruences satisfied by a set of Fourier coefficients of f of density 1 – namely the ones of index coprime to $N\ell$. From these congruences we deduce necessary conditions that need to be satisfied by the residue characteristic, and with some extra work a bound in all three cases. To get an algorithm in the dihedral and reducible cases, we work with necessary and sufficient conditions that lead, with the use of a new Sturm bound, to a finite set of congruences verified by the coefficients of f that are equivalent to the reducibility or dihedrality of $\overline{\rho}_{f,\lambda}$. Let us review in more details our approach in each case of corollary 8.6.

In the third case, we use the fact that $\mathfrak{A}_4$, $\mathfrak{S}_4$, and $\mathfrak{A}_5$ contain only elements of order at most 3, 4, and 5 respectively. Given the shape of the local representations attached to $\overline{\rho}_{f,\lambda}$, this gives huge restrictions for the possible residue characteristics that fall into this case. The argument given in [BD14] can be applied almost without modification to the case of a form with non-trivial character. The bound in this case in given by the following result.

Theorem 8.8 (theorem 10.15)**.** *If the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$, then either $\ell \mid N$ or $\ell \leqslant 5k-4$.*

Remark 8.9. *The proof of the corresponding result in [Pea21, Theorem 0.2] is not correct because it uses [BD14, Lemma 1.2] that assumes that the weight k is even. This assumption (which comes from the fact that the character of the forms in [BD14] is trivial) is not true in our general case. This has been corrected in the proof of theorem 10.15.*

In the dihedral case, we get congruences between twists of f. The strategy is then to use a Sturm bound in characteristic zero and Deligne bound for the coefficients of a modular form to

get a bound for ℓ. Our result is the following.

Theorem 8.10 (theorem 14.17)**.** *Assume $\overline{\rho}_{f,\lambda}$ has dihedral projective image of prime-to-ℓ order. If $N = 1$ then we have $\ell \leqslant k$ or $\ell \in \{2k-1, 2k-3\}$. Else, if $N \geqslant 2$ and f does not have complex multiplication, then we have*

$$\ell \leqslant \max\left(\frac{Nk}{3}\left(2\log\log(N) + 2.4\right), 25N^2\right)^{\frac{k-1}{2}[K_f:\mathbb{Q}]}.$$

This result gives us indeed an upper bound for ℓ in terms of N and k because $[K_f : \mathbb{Q}]$ can be bounded by the dimension of the $\mathbb{C}$-vector space generated by the newforms of weight k, level N and character ε (see for example [Mar05]).

In the reducible case, we deal instead with congruences involving Eisenstein series. Our approach in comparable to the one of Billerey and Dieulefait in [BD14, Section 2]. The restriction on the character in [BD14] was mainly due to a partial knowledge of the constant term of Eisenstein series at arbitrary cusps. This computation has been done in full generality in [BM18], allowing us to generalise their result. The following theorem then follows from combining this technical result with a detailed study of modular reducible representations, hence extending the strategy used for the proof of [BD14, Theorem 2.7].

Theorem 8.11 (theorem 13.19)**.** *Assume $\overline{\rho}_{f,\lambda}$ to be reducible. Then one of the following holds:*

1. *$\ell \leqslant k+1$;*
2. *$\ell \mid N\varphi(N)$, where φ denotes the Euler totient function;*
3. *there exists a prime-to-ℓ order primitive Dirichlet character η of conductor $\mathfrak{c}_0 \mid N$ such that $\eta(-1) = (-1)^k$ and ℓ divides the algebraic norm of one of the following non-zero quantities:*
   (a) *$p^k - \eta(p)$ for a prime number $p \mid N$;*
   (b) *the k-th Bernoulli number $B_{k,\eta}$ attached to η (see definition 11.1).*

The precise study of reducible and dihedral modular representations used in the proof of the two previous theorems is the main novelty of our results. The basic question we consider is as follows: How to characterise the reducibility and dihedrality of $\overline{\rho}_{f,\lambda}$ by a finite number of explicit congruences? In both the reducible and the dihedral case we give two answers to this question. A general one that applies without any restriction on ℓ or f, and, under some assumptions on ℓ, a second one for which the number of congruences to check is independent of ℓ. A weaker form of our two unconditional results state as follows.

Theorem 8.12 (theorem 13.12)**.** *The following are equivalent:*

1. *$\overline{\rho}_{f,\lambda}$ is reducible;*
2. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. There exist two primitive Dirichlet characters ε_1, ε_2 of conductor $\mathfrak{c}_1$, $\mathfrak{c}_2$ respectively, unramified at ℓ and such that $\mathfrak{c}_1\mathfrak{c}_2 \mid N$, and two integers m_1, m_2 such that $0 \leqslant m_1 \leqslant m_2 \leqslant \ell - 2$ and $\overline{\chi}_\ell^{m_1+m_2}\varepsilon_1\varepsilon_2 \equiv \overline{\chi}_\ell^{k-1}\varepsilon \pmod{\mathfrak{L}}$. Define*

$$\widetilde{k} = \begin{cases} 3 + \max(k, m_2 + 2m_1 + 1) & \text{if } \ell \mid N \\ \ell + 5 + \max(k, m_2 + \ell m_1 + 1) & \text{if } \ell \nmid N \end{cases}.$$

For every prime number $p \leqslant \frac{N\widetilde{k}}{3} \prod_{\substack{q \mid 2N \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right)$ *and not dividing* 2ℓ*, we have*

- $p \nmid N$ *and* $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$*;*
- *or,* $p \mid N$ *and* $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ *for some* b_p *in the set* $\{0, \varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$*.*

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$*, where* $\overline{\varepsilon_1}$ *and* $\overline{\varepsilon_2}$ *are the reductions of* ε_1 *and* ε_2 *modulo* $\mathfrak{L}$ *respectively.*

Theorem 8.13 (theorem 14.12)**.** *The following are equivalent.*

1. *The representation* $\overline{\rho}_{f,\lambda}$ *has dihedral projective image of prime-to-*ℓ *order;*
2. *There exist an integer* $e \in \{0, 1\}$ *and a primitive Dirichlet character* ψ *of conductor* $\mathfrak{c}_\psi \mid N$*, unramified at* ℓ*, and such that for a prime* p *dividing* N*.*
   - *if* $v_p(N) = 1$*,* $v_p(\mathfrak{c}) = 0$*, and* $p \neq \ell$*, then* $p \nmid \mathfrak{c}_\psi$*;*
   - *if* $v_p(N) = v_p(\mathfrak{c})$ *and* $p \neq \ell$*, then either* $p \nmid \mathfrak{c}_\psi$ *or the* p*-parts of* ψ *and* ε^{-1} *are equal modulo* λ*;*
   - *if* $v_2(N) \in \{2, 3\}$*, and* $v_2(\mathfrak{c}) < v_2(N)$*, then* $v_2(\mathfrak{c}_\psi) \leqslant 2$*.*

   Define

$$\widetilde{k} := \begin{cases} k + 4 + 3\left(1 + e\frac{\ell-1}{2}\right) & \text{if } \ell \mid N; \\ k + 4 + (\ell+1)\left(1 + e\frac{\ell-1}{2}\right) & \text{if } \ell \nmid N. \end{cases}$$

   For every prime $p \leqslant \dfrac{N \gcd(2, N)^2 \widetilde{k}}{12} \prod_{p \mid N} (p + 1)$*, the following congruences hold:*
   - $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$ *if* $p \nmid N\ell$*;*
   - $a_p(f)^2 \equiv p^{e\frac{\ell-1}{2}+k-1}(\psi\varepsilon)'_p(p) \pmod{\lambda}$ *if* $p \mid N$*,* $p \neq \ell$*,* $v_p(N) = v_p(\mathfrak{c})$*, and* ψ *is ramified at* p*. Here* $(\psi\varepsilon)'_p$ *denotes the prime-to-*p *part of the Dirichlet character* $\psi\varepsilon$*.*

Notice that these two results apply with no assumption on f and ℓ. In particular, they can be used to check the reducibility and the dihedrality of $\overline{\rho}_{f,\lambda}$ for any given λ, including the ones with small residue characteristic compared to the weight, or divides the level. Such restrictions appear for instance in the work of Anni [Ann13, Algorithms 7.2.4 and 10.1.3], where the author develops a different, "bottom-up" approach, towards these questions in the context of modular forms "à la Katz".

In theorems 8.12 and 8.13, the number of congruences to be satisfied depends not only on N, k and ε, but also on ℓ. Under some assumptions on ℓ, we have been able to remove this dependency in the bound. A weaker form of these two "big" characteristic results can be stated as follows.

Theorem 8.14 (theorem 13.17)**.** *Assume* $\ell > k + 1$ *and* $\ell \nmid N\varphi(N)$*, where* φ *denotes the Euler totient function. The following are equivalent:*

1. $\overline{\rho}_{f,\lambda}$ *is reducible;*

2. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. There exist two primitive Dirichlet characters ε_1, ε_2 of conductor $\mathfrak{c}_1$, $\mathfrak{c}_2$ respectively such that $\mathfrak{c}_1\mathfrak{c}_2 \mid N$, and $\varepsilon_1\varepsilon_2 = \varepsilon$. For all odd primes $p \leqslant \frac{Nk}{3} \prod_{\substack{q \mid 2N \\ q \text{ prime}}} \left(1 + \frac{1}{q}\right)$, we have*

   - *$p \nmid N$ and $a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$;*
   - *$p \mid N$ and $a_p(f) \equiv b_p \pmod{\mathfrak{L}}$ for some $b_p \in \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$.*

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon_2}$, where $\overline{\varepsilon_1}$ and $\overline{\varepsilon_2}$ are the reductions of ε_1 and ε_2 modulo $\mathfrak{L}$ respectively.

Theorem 8.15 (theorem 14.16)**.** *Assume $\ell \geqslant k-1$, $\ell \notin \{2k-1, 2k-3\}$, $\ell \nmid N$, $\ell \nmid p \pm 1$ for all primes p dividing N. The following are equivalent.*

1. *$\overline{\rho}_{f,\lambda}$ has dihedral projective image of prime-to-ℓ order.*
2. *There exists a primitive Dirichlet character ψ of conductor $\mathfrak{c}_\psi \mid N$ such that for a prime p dividing N*

   - *if $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then $p \nmid \mathfrak{c}_\psi$;*
   - *if $v_p(N) = v_p(\mathfrak{c})$, then either $p \nmid \mathfrak{c}_\psi$, or the p-parts of ψ and ε^{-1} are equal;*
   - *if $v_2(N) \in \{2, 3\}$, and $v_2(\mathfrak{c}) < v_2(N)$, then $v_2(\mathfrak{c}_\psi) \leqslant 2$.*

   Moreover, for every prime $p \leqslant \frac{N \gcd(N,2)^2 k}{12} \prod_{p \mid N} \left(1 + \frac{1}{p}\right)$, the following congruences hold.

   - *$a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$ if $p \nmid N$;*
   - *$a_p(f)^2 \equiv p^{k-1}(\psi\varepsilon)_0(p) \pmod{\lambda}$ if $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$ and ψ is ramified at p, where $(\psi\varepsilon)_0$ denotes the primitive character associated to $\psi\varepsilon$.*

We stress the fact that according to theorems 8.12 and 8.14, proving the reducibility of $\overline{\rho}_{f,\lambda}$ requires checking around $N \max(k^2, N) \log\log(N)$ congruences (and even $Nk \log\log(N)$ for the primes ℓ satisfying the assumptions $\ell > k+1$ and $\ell \nmid N\varphi(N)$). Notice that the $\log\log(N)$ part comes from the upper-bound we prove in lemma 12.23. Similarly, it follows from theorems 8.13 and 8.15 that proving the dihedrality of $\overline{\rho}_{f,\lambda}$ needs around $N \max(k^2, N) \log\log N$ congruences to check (and around $Nk \log\log N$ when the assumptions of theorem 8.15 hold).

To achieve such bounds, we extensively use the local description of $\overline{\rho}_{f,\lambda}$ at the bad prime numbers (*i.e.* the prime numbers dividing N), together with generalised Sturm bounds theorems and an appropriate use of degeneracy maps between modular forms spaces of various levels. Having a sharp bound is especially important from a computational point of view. Indeed, those four results also provide us two algorithms: one that explicitly computes the exact set of λ such that $\overline{\rho}_{f,\lambda}$ is reducible, and one that explicitly computes the exact set of λ's such that $\overline{\rho}_{f,\lambda}$ has dihedral projective image. We have implemented these algorithms in PARI/GP [21].

Chapitre 9

Introduction en français

Cette partie de la thèse vient principalement de l'article [Pea21]. Les chapitres 9 et 10 ont été rallongés légèrement. Quelques changements ont été effectués dans les chapitres 11, 13, et les sections 15.1, 15.1.2. Enfin, le chapitre 14, et la section 15.2 sont en grande partie nouveaux.

9.1 Représentations résiduelles modulaires

Parmi toutes les formes modulaires, la plus célèbre est sans nul doute la fonction Delta de Ramanujan. Définie et étudiée par Ramanujan en 1916 dans l'ouvrage [Ram00, §15-19], elle est définie par la série génératrice

$$\Delta := q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=0}^{\infty}\tau(n)q^n.$$

Depuis cet article fondateur de nombreux mathématiciens ont étudié les propriétés des fonctions tau et delta. Outre être les coefficients d'une forme modulaire nouvelle pour le tout le groupe modulaire, les coefficients $(\tau(n))_{n\in\mathbb{N}}$ satisfont les surprenantes congruences suivantes.

$$\begin{array}{lll}
\tau(p) \equiv 1 + p^{11} & (\mathrm{mod}\ 2^5), & \text{pour tout nombre premier } p \neq 2\ ; \\
\tau(p) \equiv p^2 + p^9 & (\mathrm{mod}\ 3^3), & \text{pour tout nombre premier } p\ ; \\
\tau(p) \equiv p + p^{10} & (\mathrm{mod}\ 5^2), & \text{pour tout nombre premier } p\ ; \\
\tau(p) \equiv p + p^4 & (\mathrm{mod}\ 7), & \text{pour tout nombre premier } p\ ; \\
\tau(p) \equiv \left(\frac{p}{23}\right)\tau(p) & (\mathrm{mod}\ 23), & \text{pour tout nombre premier } p \neq 23\ ; \\
\tau(p) \equiv 1 + p^{11} & (\mathrm{mod}\ 691), & \text{pour tout nombre premier } p,
\end{array} \tag{9.1}$$

où $\left(\frac{p}{23}\right)$ est le symbole de Legendre modulo 23 en p. Des congruences plus générales modulo des puissances plus grandes de 2, 3, 5, 7, 23 et 691 existent aussi. Nous renvoyons le lecteur à [Swi73] pour les énoncés et des références pour ces congruences.

Pendant de nombreuses années, les congruences (9.1) n'étaient expliquée par aucun cadre géométrique plus général. C'est en 1968 que Jean-Pierre Serre proposa une conjecture relative à l'existence d'une famille de représentations galoisiennes associée à Δ dans son Séminaire Delange–Pisot–Poitou de 1968 [Ser69]. Sa conjecture était la suivante.

Conjecture 9.1 ([Ser69, 3.2. Conjecture]). *Pour nombre premier ℓ, il existe une représentation linéaire continue*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}(V_\ell),$$

où K_ℓ est l'extension maximale non ramifiée en ℓ de $\mathbb{Q}$, et V_ℓ est un $\mathbb{Q}_\ell$-espace vectoriel de dimension 2, satisfaisant à la condition suivante :

(C) Pour tout nombre premier $p \neq \ell$, le polynôme caractéristique de $\rho_\ell(\mathrm{Frob}_p)$ est égale à $X^2 - \tau(p)X + p^{11}$.

Serre explique que cette conjecture donne une interprétation galoisienne des congruences (8.1). En effet, considérons un réseau Λ_ℓ stable par $\mathrm{Gal}(K_\ell/\mathbb{Q})$ dans V_ℓ (un tel réseau existe toujours). Le choix d'un tel réseau induit une représentation $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ ayant la même trace et le même déterminant que ρ_ℓ. En réduisant cette représentation modulo ℓ^n, on obtient une représentation

$$\rho_{\ell,n} : \mathrm{Gal}(K_\ell/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

On peut alors reformuler les congruences précédentes (à semi-simplification près) par les isomorphismes suivants.

$$\begin{aligned} &\rho_{2,5} \cong \mathbb{1} \oplus \overline{\chi}_{2^5}^{11} \ ; && \rho_{7,1} \cong \overline{\chi}_7 \oplus \overline{\chi}_7^4 \ ; \\ &\rho_{3,2} \cong \overline{\chi}_{3^3}^2 \oplus \overline{\chi}_{3^3}^9 \ ; && \rho_{23,1} \cong \left(\tfrac{\cdot}{23}\right) \otimes \rho_{23,1} \ ; \\ &\rho_{5,2} \cong \overline{\chi}_{5^2} \oplus \overline{\chi}_{5^2}^{10} \ ; && \rho_{691,1} \cong \mathbb{1} \oplus \overline{\chi}_{691}^{11}, \end{aligned} \tag{9.2}$$

où $\overline{\chi}_{\ell^n}$ est le caractère cyclotomique modulo ℓ^n. De ces isomorphismes émergent plusieurs questions : Est-ce que ce type d'isomorphismes apparaît uniquement pour les nombres premiers 2, 3, 5, 7, 23, et 691 ? Y a-t-il une procédure pour prédire et calculer ces isomorphismes ? La conjecture 9.1 est-elle vraie et se généralise-t-elle pour d'autres newform ?

La réponse à la dernière question est positive et a été apportée par Deligne en 1969 pour des formes de poids supérieur ou égal à 2, et par Deligne et Serre en 1974 pour des formes modulaires de poids 1. Leurs énoncés sont les suivants.

Théorème 9.1 ([Del71], [DS74, Théorème 4.1]). *Soient k et N deux entiers strictement positifs, et soit ε un caractère de Dirichlet modulo N. Soit f une newform de poids k, niveau N, et de caractère ε. On désigne par K_f le corps de nombres engendré par les coefficients de Fourier de f.*

Soit λ un idéal premier de l'anneau des entiers de K_f de caractéristique résiduelle ℓ. Il existe une représentation galoisienne linéaire continue

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(F),$$

où $F := K_{f,\lambda}$ est la complétion λ-adique de K_f si $k \geqslant 2$, et $F := \mathbb{C}$ si $k = 1$, qui satisfait les conditions suivantes :

1. *La représentation $\rho_{f,\lambda}$ est non ramifiée en dehors de $N\ell$;*
2. *Pour tout nombre premier $p \nmid N\ell$, le polynôme caractéristique de $\rho_{f,\lambda}$ en un Frobenuis en p est égal à $X^2 - a_p(f)X + p^{k-1}\varepsilon(p)$, où $a_p(f)$ est le p^e coefficient de Fourier de f.*

La démonstration du théorème 9.1 marque le point de départ de nombreux théorèmes et conjectures de la seconde moitié du XX$^{\text{e}}$ siècle – et beaucoup sont ouvertes encore aujourd'hui. Parmi eux on peut citer la conjecture de modularité de Serre [Ser87], le théorème de modularité de Wiles [Wil95, Theorem 0.4], les questions d'augmentations du niveau [DT94] et d'abaissement du niveau [Rib90, Theorem 1.1].

Comme l'explique Ken Ribet dans [Rib77, Theorem (2.3)], les conditions 1 et 2 caractérisent entièrement la représentation $\rho_{f,\lambda}$ à isomorphisme près, et imposent qu'elle soit irréductible.

Concentrons-nous désormais sur le cas du poids supérieur à 2 – le cas des formes modulaires de poids 1 étant toute une autre histoire. Soit f une newform de poids $k \geqslant 2$, niveau $N \geqslant 1$, et caractère de ε. Soit λ un idéal premier de l'anneau des entiers $\mathcal{O}_{K_f}$ du corps K_f des coefficients de f. Comme précédemment, on peut construire un réseau Galois-stable de K_f^2, et en conjuguant par ce réseau on obtient une représentation à valeurs dans l'anneau local de K_f. Notons $\mathbb{F}_\lambda$ le corps résiduel de λ. On peut alors réduire modulo λ la représentation obtenue et on trouve

$$\widetilde{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda).$$

Cette représentation dépend du choix du réseau utilisé pour réduire $\rho_{f,\lambda}$. Cependant, le théorème de Brauer–Nesbitt nous assure que la semi-simplifiée de $\widetilde{\rho}_{f,\lambda}$ est unique à isomorphisme près et est caractérisée par les propriétés suivantes.

1. La représentation $\overline{\rho}_{f,\lambda}$ est semi-simple ;
2. La représentation $\overline{\rho}_{f,\lambda}$ est non ramifiée en dehors de $N\ell$;
3. Pour tout nombre premier $p \nmid N\ell$, le polynôme caractéristique de $\overline{\rho}_{f,\lambda}$ en un Frobenius en p est égal à $X^2 - a_p(f)X + p^{k-1}\varepsilon(p) \pmod{\lambda}$.

Remarque 9.2. *La réduction modulo λ de $a_p(f)$ et $\varepsilon(p)$ est effectivement bien définie car les coefficients d'une newform sont toujours des entiers algébriques et que le corps K_f contient toujours les valeurs du caractère de la forme f. Nous renvoyons à [Rib77, Corollary (3.1)] pour une démonstration de ces résultats.*

De nouveau grâce au théorème de Brauer–Nesbitt et par le théorème de densité de Čebotarev, la représentation $\overline{\rho}_{f,\lambda}$ est entièrement déterminée par les propriétés 1, 2, et 3. Cependant, elle peut ne plus être irréductible – contrairement à $\rho_{f,\lambda}$. Le point de départ de cette partie de la thèse est un théorème démontré par Ribet en 1975 pour les formes de niveau 1, et en 1985 pour n'importe quelle forme modulaire. Il généralise les travaux de Swinnerton-Dyer et Serre de 1973 pour $N = 1$ et $K_f = \mathbb{Q}$ [Ser73 ; Swi73].

Théorème 9.3 ([Rib85, Theorem 2.1])**.** *Pour tout idéal premier λ en dehors d'un ensemble fini, la représentation $\overline{\rho}_{f,\lambda}$ irréductible. De plus, si f n'est pas à multiplication complexe (voir la définition 14.3), alors pour tout λ sauf un nombre fini, l'ordre de l'image de $\overline{\rho}_{f,\lambda}$ n'est pas divisible par ℓ.*

Le théorème 9.3 apporte une première réponse aux questions de Serre sur les congruences vérifiées par la fonction tau : il n'existe effectivement qu'un nombre fini de nombres premiers ℓ pour lesquels $\tau(p)$ est congruent modulo ℓ à $p^a + p^b$ pour tout p sauf un nombre fini, avec a, b

deux entiers (et on peut démontrer que ce phénomène se produit uniquement pour $\ell = 2$, 3, 5, 7, et 691 dans le cas de Δ). En effet, ces congruences correspondent exactement aux nombres premiers pour lesquels $\overline{\rho}_{\Delta,\ell}$ est réductible. Pour mieux comprendre les congruences vérifiées par τ modulo 23, nous avons besoin d'être plus précis quant au théorème de Ribet. La classification des sous-groupes de PSL_2 d'un corps fini est bien connue depuis Dickson [Dic01, Chapter XII]. Elle peut s'énoncée comme suit.

Théorème 9.4 ([Hup67, Hauptsatz 8.27]). *Soit $q := p^f$ une puissance d'un nombre premier p. Un sous-groupe de $\mathrm{PSL}_2(\mathbb{F}_q)$ est isomorphe à un des groupes suivants.*

1. *Un groupe cyclique d'ordre z divisant $\frac{q\pm1}{\gcd(q-1,2)}$;*
2. *Un groupe dihédral d'ordre $2z$ avec z divisant $\frac{q\pm1}{\gcd(q-1,2)}$;*
3. *Le groupe alterné $\mathfrak{A}_4$, uniquement si $p > 2$ ou $q = 2^{2n}$;*
4. *Le groupe symétrique $\mathfrak{S}_4$, uniquement si $q^2 \equiv 1 \pmod{16}$;*
5. *Le groupe alterné $\mathfrak{A}_5$, seulement si $p = 5$, ou $q^2 \equiv 1 \pmod{5}$;*
6. *$(\mathbb{Z}/p\mathbb{Z})^n$ pour un entier positif n ;*
7. *Un produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^n \rtimes \mathbb{Z}/m\mathbb{Z}$ pour des entiers n et m divisant $p^n - 1$ et $q - 1$ respectivement ;*
8. *$\mathrm{PSL}_2(\mathbb{F}_{p^n})$ pour un entier n divisant f ;*
9. *$\mathrm{PGL}_2(\mathbb{F}_{p^n})$ pour un entier n divisant $2f$.*

En utilisant le théorème 9.4 et le fait que l'on peut toujours plonger $\mathrm{PGL}_2(\mathbb{F}_q)$ dans $\mathrm{PSL}_2(\mathbb{F}_{q^2})$, nous pouvons reformuler le théorème de Ribet de la manière suivante.

Corollaire 9.5. *Soit f une newform. Il existe seulement un nombre fini d'idéaux premiers λ qui satisfont à au moins une des propriétés suivantes.*

1. *La représentation $\overline{\rho}_{f,\lambda}$ est réductible ;*
2. *La forme f n'est pas CM et l'image projective de $\overline{\rho}_{f,\lambda}$ dans $\mathrm{PGL}_2(\mathbb{F}_\lambda)$ est isomorphe à un groupe dihédral D_{2n} avec $\ell \nmid 2n$, où ℓ est la caractéristique résiduelle de λ ;*
3. *L'image projective de $\overline{\rho}_{f,\lambda}$ dans $\mathrm{PGL}_2(\mathbb{F}_\lambda)$ est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$, ou $\mathfrak{A}_5$.*

On appellera par la suite « idéaux exceptionnels », les idéaux qui vérifient une des propriétés ci-dessus.

Remarque 9.6. *Malgré le fait que l'hypothèse f non-CM apparaît dans la seconde moitié du théorème 9.3, la preuve de [Rib85, Theorem 2.1] ne l'utilise que dans le cas dihédral.*

L'isomorphisme modulo 23 dans (9.2) correspond alors au deuxième cas du corollaire 9.5. À partir de là, deux questions se posent.

I) Pour chaque cas du corollaire 9.5, peut-on borner la caractéristique résiduelle des idéaux exceptionnels en fonction des invariants de la forme f tels que son poids, son niveau, ou son caractère ?

II) Pour chaque cas du corollaire 9.5, peut-on calculer les idéaux exceptionnels ?

Pour des formes de niveau 1 les résultats de Ribet de 1975 donnent une description explicite des idéaux premiers pour lesquels la représentation résiduelle associée est réductible. Cependant, cela n'est plus le cas dans sa preuve générale de 1985, et cela n'était déjà pas le cas pour les deux autres cas en 1975. Le premier pas pour rendre les résultats de Ribet effectifs a été accompli par Billerey et Dieulefait en 2014 [BD14]. Dans le cas où le caractère de la forme f est trivial, ils donnent des critères explicites sur la caractéristique résiduelle ℓ de λ en fonction de k et N pour que la représentation $\overline{\rho}_{f,\lambda}$ soit réductible. Dans les deux autres cas ils donnent des bornes explicites sur ℓ en fonction de k et N. Le but de cette partie de la thèse est de continuer leur travail et de donner autant de réponses que possible aux questions I et II.

9.2 Résultats

Soit $f = q + \sum_{n=2}^{\infty} a_n(f)q^n$ une newform de poids k, niveau N, et de caractère ε de conducteur $\mathfrak{c}$. Soit $K_f := \mathbb{Q}(a_n(f))_{n\geqslant 2}$ le corps des coefficients de f, et soit λ un idéal premier de l'anneau des entiers de K_f, au-dessus d'un nombre premier ℓ. Les contributions de cette partie de la thèse sont doubles. D'une part, nous généralisons les résultats de [BD14] à n'importe quelle forme modulaire de poids, niveau, et caractère quelconque, et nous donnons une borne effective pour chacun des trois cas du corollaire 9.5 en fonction de k, N, et ε. D'autre part, nous développons un algorithme qui, étant donné le poids, le niveau, le caractère, et un nombre fini de coefficients de f, calcule tous les idéaux réductibles, et tous les idéaux dihédraux.

La stratégie que nous adoptons se base sur les idées de Serre et Swinnerton-Dyer [Ser73 ; Swi73]. Les trois cas du théorème de Ribet peuvent être reformulées en termes de congruences satisfaites par un ensemble de densité 1 de coefficients de Fourier de f – ceux d'indice premier à $N\ell$. À partir de ces congruences, nous déduisons des conditions nécessaires que doit vérifier la caractéristique résiduelle de λ, puis des bornes dans chacun des trois cas. Pour obtenir un algorithme dans les cas dihédraux et réductibles, nous travaillons par conditions nécessaires et suffisantes. Celles-ci nous conduisent, en utilisant des bornes de Sturm, à un ensemble fini de congruences que doivent satisfaire les coefficients de Fourier de f, équivalentes à la réductibilité de $\overline{\rho}_{f,\lambda}$ d'une part, et à sa dihédralité d'autre part. Nous détaillons notre approche pour chacun des trois cas ci-dessous.

Dans le troisième cas, nous utilisons le fait que les groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, et $\mathfrak{A}_5$ ne contiennent respectivement que des éléments d'ordre 3, 4, et 5. En connaissant la forme locale en ℓ de la représentation $\overline{\rho}_{f,\lambda}$, cela nous donne des contraintes sur les caractéristiques résiduelles possibles dans ce cas. L'argument donné dans [BD14] s'applique presque sans modification au cas général d'une forme de caractère non trivial, et nous déduisons la borne suivante.

Théorème 9.7 (10.15)**.** *Si l'image projective de $\overline{\rho}_{f,\lambda}$ est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$, alors soit $\ell \mid N$, soit $\ell \leqslant 5k-4$.*

Remarque 9.8. *La preuve du résultat correspondant dans [Pea21, Theorem 0.2] était fausse car elle utilisait le résultat [BD14, Lemma 1.2] qui supposait que le poids de f était pair. Cette hypothèse – qui venait du fait que le caractère dans [BD14] était trivial – n'est pas vrai dans notre cadre plus général. Nous avons corrigé cela dans la démonstration du théorème 10.15.*

Dans le cas dihédral, nous utilisons des congruences entre des tordues de la forme f. Notre stratégie est d'utiliser une borne de Sturm en caractéristique nulle et les bornes de Deligne pour les coefficients d'une forme modulaire pour obtenir un majorant de ℓ. Notre résultat est le suivant.

Théorème 9.9 (14.17)**.** *Supposons que $\overline{\rho}_{f,\lambda}$ est d'image projective dihédrale d'ordre premier à ℓ. Si $N = 1$, alors $\ell \leqslant k$, ou $\ell \in \{2k-1, 2k-3\}$. Si $N \geqslant 2$, et que f n'est pas à multiplication complexe, alors*

$$\ell \leqslant \max\left(\frac{Nk}{3}\left(2\log\log(N) + 2.4\right), 25N^2\right)^{\frac{k-1}{2}[K_f:\mathbb{Q}]}.$$

Ce résultat nous donne effectivement une borne sur ℓ en fonction de N et k car le degré $[K_f : \mathbb{Q}]$ peut être borné par la dimension du $\mathbb{C}$-espace vectoriel engendré par les newform de poids k, niveau N et de caractère ε (voir par exemple [Mar05]).

Dans le cas réductible, nous travaillons avec des congruences faisant intervenir des séries d'Eisenstein. Notre méthode est comparable à celle de Billerey et Dieulefait dans [BD14, Section 2]. Leur restriction sur le caractère de f venait principalement du manque de connaissance à l'époque sur le terme constant des séries d'Eisenstein en une pointe quelconque. Ce calcul a été effectué en toute généralité par [BM18], nous permettant de généraliser les calculs de [BD14]. Le résultat suivant est la combinaison de ce résultat technique et de l'étude détaillée des représentations modulaires résiduelles réductibles, généralisant ainsi la preuve de [BD14, Theorem 2.7].

Théorème 9.10 (13.19)**.** *Supposons que $\overline{\rho}_{f,\lambda}$ est réductible. Au moins une des propriétés suivantes est alors vraie.*

1. *$\ell \leqslant k+1$;*
2. *$\ell \mid N\varphi(N)$, où φ désigne la fonction caractéristique d'Euler ;*
3. *il existe un caractère de Dirichlet primitif η d'ordre premier à ℓ, de conducteur $\mathfrak{c}_0 \mid N$ tel que $\eta(-1) = (-1)^k$, et ℓ divise la norme algébrique d'une des quantités non-nulles suivantes :*
   (a) *$p^k - \eta(p)$ pour un nombre premier $p \mid N$;*
   (b) *le k^e nombre de Bernoulli $B_{k,\eta}$ de η (voir la définition 11.1).*

L'étude détaillée des représentations modulaires réductibles et dihédrales qui sont faites dans la thèse sont les principales nouveautés de nos résultats. La question que nous nous posons est la suivante : Comment caractériser la réductibilité (*resp.* la dihédralité) de $\overline{\rho}_{f,\lambda}$ par un nombre fini de congruences effectives ? Dans ces deux cas, nous donnons deux réponses à cette question. Une réponse générale, sans restriction sur la caractéristique résiduelle de l'idéal λ, ni sur la forme f. Et une seconde réponse qui, sous certaines hypothèses sur ℓ, donne un ensemble de congruences à satisfaire qui est indépendant de ℓ. Nous énonçons une version affaiblie de nos deux résultats inconditionnels ci-dessous.

Théorème 9.11 (Theorem 13.12)**.** *Les énoncés suivant sont équivalents.*

1. *La représentation $\overline{\rho}_{f,\lambda}$ est réductible ;*
2. *Soit $\mathfrak{L}$ une place de $\overline{\mathbb{Q}}$ au-dessus de λ. Il existe deux caractères de Dirichlet primitifs ε_1, ε_2, de conducteur $\mathfrak{c}_1$, $\mathfrak{c}_2$ respectivement, non ramifiés en ℓ, et tels que $\mathfrak{c}_1\mathfrak{c}_2 \mid N$. Il existe deux entiers m_1, m_2 tels que $0 \leqslant m_1 \leqslant m_2 \leqslant \ell - 2$ et $\overline{\chi}_\ell^{m_1+m_2}\varepsilon_1\varepsilon_2 \equiv \overline{\chi}_\ell^{k-1}\varepsilon \pmod{\mathfrak{L}}$. Soit*

$$\widetilde{k} = \begin{cases} 3 + \max(k, m_2 + 2m_1 + 1) & \text{si } \ell \mid N \ ; \\ \ell + 5 + \max(k, m_2 + \ell m_1 + 1) & \text{si } \ell \nmid N. \end{cases}$$

Pour tout nombre premier $p \leqslant \frac{N\widetilde{k}}{3} \prod_{\substack{q \mid 2N \\ q \text{ premier}}} \left(1 + \frac{1}{q}\right)$ et ne divisant pas 2ℓ, on a

- *$p \nmid N$ et $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$;*
- *ou, $p \mid N$ et $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$ pour un nombre $b_p \in \{0, \varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.*

Quand ces propriétés sont satisfaites, on a de plus $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$, où $\overline{\varepsilon_1}$ et $\overline{\varepsilon_2}$ sont les réductions de ε_1 et ε_2 modulo $\mathfrak{L}$.

Théorème 9.12 (Theorem 14.12)**.** *Les énoncés suivants sont équivalents.*

1. *La représentation $\overline{\rho}_{f,\lambda}$ est d'image projective dihédrale d'ordre premier à ℓ ;*
2. *Il existe un entier $e \in \{0, 1\}$ et un caractère de Dirichlet primitif ψ de conducteur $\mathfrak{c}_\psi \mid N$, non ramifié en ℓ, et tel que pour tout nombre premier p divisant N,*
   - *si $v_p(N) = 1$, $v_p(\mathfrak{c}) = 0$, et $p \neq \ell$, alors $p \nmid \mathfrak{c}_\psi$;*
   - *si $v_p(N) = v_p(\mathfrak{c})$ et $p \neq \ell$, alors soit $p \nmid \mathfrak{c}_\psi$, soit les p-parties de ψ et ε^{-1} sont égales modulo λ ;*
   - *si $v_2(N) \in \{2, 3\}$, et $v_2(\mathfrak{c}) < v_2(N)$, alors $v_2(\mathfrak{c}_\psi) \leqslant 2$.*

   Soit

$$\widetilde{k} := \begin{cases} k + 4 + 3\left(1 + e\frac{\ell-1}{2}\right) & \text{si } \ell \mid N \ ; \\ k + 4 + (\ell + 1)\left(1 + e\frac{\ell-1}{2}\right) & \text{si } \ell \nmid N. \end{cases}$$

   Pour tout nombre premier $p \leqslant \dfrac{N \gcd(2, N)^2\widetilde{k}}{12} \prod_{p \mid N}(p + 1)$, les congruences suivantes sont satisfaites :

   - *$a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$ si $p \nmid N\ell$;*
   - *$a_p(f)^2 \equiv p^{e\frac{\ell-1}{2}+k-1}(\psi\varepsilon)'_p(p) \pmod{\lambda}$ si $p \mid N$, $p \neq \ell$, $v_p(N) = v_p(\mathfrak{c})$, et ψ est ramifié en p, où $(\psi\varepsilon)'_p$ désigne la partie première à p du caractère de Dirichlet $\psi\varepsilon$.*

On notera que ces deux résultats s'appliquent quelques soient la forme f et le nombre premier ℓ. En particulier, ils peuvent être utilisés pour tester la réductibilité et la dihédralité de $\overline{\rho}_{f,\lambda}$ pour n'importe quel idéal premier λ, y compris ceux dont la caractéristique résiduelle est petite devant

le poids, ou divise le niveau. De telles hypothèses étaient par exemple présentes dans le travail d'Anni [Ann13, Algorithms 7.2.4 et 10.1.3], où l'auteur développait une approche différente – utilisant des connaissances sur les formes de petit poids pour en déduire pour des formes de poids supérieur – dans le contexte des formes modulaires de Katz.

Dans les théorèmes 9.11 and 9.12, le nombre de congruences à satisfaire ne dépendent pas seulement de N, k, et ε, mais aussi de la caractéristique ℓ. Sous des hypothèses sur ℓ, nous sommes parvenus à supprimer cette dépendance dans la borne. Nous énonçons ci-dessous une forme affaiblie de nos résultats « en grande caractéristique » pour les cas réductibles et dihédraux.

Théorème 9.13 (Theorem 13.17). *Supposons $\ell > k+1$ et $\ell \nmid N\varphi(N)$, où φ désigne la fonction caractéristique d'Euler. Les propriétés suivantes sont équivalentes.*

1. *La représentation $\overline{\rho}_{f,\lambda}$ est réductible ;*
2. *Soit $\mathfrak{L}$ une place de $\overline{\mathbb{Q}}$ au-dessus de λ. Il existe deux caractères de Dirichlet primitifs ε_1, ε_2, de conducteur $\mathfrak{c}_1$, $\mathfrak{c}_2$ respectivement, tels que $\mathfrak{c}_1\mathfrak{c}_2 \mid N$, et $\varepsilon_1\varepsilon_2 = \varepsilon$. Pour tout nombre premier impair $p \leqslant \frac{Nk}{3} \prod_{\substack{q \mid 2N \\ q \text{ premier}}} \left(1+\frac{1}{q}\right)$, on a*

   - *$p \nmid N$ et $a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$;*
   - *$p \mid N$ et $a_p(f) \equiv b_p \pmod{\mathfrak{L}}$ pour un $b_p \in \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$.*

Quand ces propriétés sont vérifiées, on a de plus $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon_2}$, où $\overline{\varepsilon_1}$ et $\overline{\varepsilon_2}$ sont les réductions de ε_1 et ε_2 modulo $\mathfrak{L}$.

Théorème 9.14 (Theorem 14.16). *Supposons $\ell \geqslant k-1$, $\ell \notin \{2k-1, 2k-3\}$, et $\ell \nmid N$, $\ell \nmid p \pm 1$ pour tout nombre premier p divisant N. Les énoncés suivants sont équivalents.*

1. *La représentation $\overline{\rho}_{f,\lambda}$ est d'image projective dihédrale d'ordre premier à ℓ ;*
2. *Il existe un caractère de Dirichlet primitif ψ de conducteur $\mathfrak{c}_\psi \mid N$ tel que pour tout nombre premier p divisant N*

   - *si $v_p(N) = 1$ et $v_p(\mathfrak{c}) = 0$, alors $p \nmid \mathfrak{c}_\psi$;*
   - *si $v_p(N) = v_p(\mathfrak{c})$, alors soit $p \nmid \mathfrak{c}_\psi$, soit les p-parties de ψ et ε^{-1} sont égales ;*
   - *si $v_2(N) \in \{2,3\}$, et $v_2(\mathfrak{c}) < v_2(N)$, alors $v_2(\mathfrak{c}_\psi) \leqslant 2$.*

   De plus, pour tout nombre premier $p \leqslant \frac{N\gcd(N,2)^2k}{12} \prod_{p \mid N} \left(1+\frac{1}{p}\right)$, les congruences suivantes sont satisfaites.

   - *$a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$ si $p \nmid N$;*
   - *$a_p(f)^2 \equiv p^{k-1}(\psi\varepsilon)_0(p) \pmod{\lambda}$ si $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$ et ψ est ramifié en p, où $(\psi\varepsilon)_0$ désigne le caractère primitif associé à $\psi\varepsilon$.*

Nous insistons sur le fait que selon les théorèmes 8.12 et 8.14, certifier la réductibilité de $\overline{\rho}_{f,\lambda}$ nécessite environ $N \max(k^2, N) \log\log(N)$ congruences (et même $Nk \log\log(N)$ pour les nombres premiers ℓ tels que $\ell > k+1$ et $\ell \nmid N\varphi(N)$). Le terme $\log\log(N)$ provenant de la majoration donnée dans le lemme 12.23. De même, il suit des théorèmes 8.13 et 8.15 que prouver la dihédralité de $\overline{\rho}_{f,\lambda}$ requiert vérifier de l'ordre de $N \max(k^2, N) \log\log N$ congruences (et $Nk \log\log N$ quand les hypothèses du théorème 8.15 sont satisfaites).

Pour obtenir de telles bornes, nous utilisons de manière cruciale la description locale de la représentation $\overline{\rho}_{f,\lambda}$ aux mauvais nombres premiers (c'est-à-dire les nombres premiers qui divisent le niveau N). Les autres ingrédients importants que sont de nouveaux théorèmes de type bornes de Sturm que nous démontrons, ainsi qu'une utilisation judicieuse des applications de dégénérescences entre les espaces de formes modulaires. Avoir des bornes aussi petites que possible est extrêmement important dans une optique algorithmique. En effet, nos résultats nous ont permis de développer deux algorithmes : un premier qui, étant donné une forme f, calcule l'ensemble exact des idéaux premiers λ tels que $\overline{\rho}_{f,\lambda}$ est réductible ; et un second qui calcule les λ tels que $\overline{\rho}_{f,\lambda}$ est d'image projective dihédrale d'ordre premier à ℓ. Nous avons de plus implémenté ces deux algorithmes dans PARI/GP [21].

Chapter 10

Background on Galois representations

We fix once and for all algebraic closures $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$, and $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ for all prime numbers p. We denote by $\overline{\mathbb{Z}}$ and $\overline{\mathbb{Z}_p}$ the rings of integers of $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}_p}$ respectively.

10.1 Generalities on Galois representations

We begin by recalling general notions of the theory of Galois representations we will be using. A Galois representation is a continuous morphism from the group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_n(F)$, for a positive integer n and some field F. The group $G_{\mathbb{Q}}$ is endowed with the Krull topology, a basis of open subsets of Id consisting of the subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for all number fields $K/\mathbb{Q}$. The topology on $\mathrm{GL}_n(F)$ depends on the field F. For $F = \mathbb{C}$ or a subfield of $\overline{\mathbb{F}}_p$ for a prime p it is the discrete one, and for F a subfield of $\overline{\mathbb{Q}_p}$ it is the p-adic topology. A result we will be using extensively to prove isomorphism between Galois representations is the so-called Brauer–Nesbitt theorem.

Theorem 10.1 (Brauer–Nesbitt [CR06, (30.16) and (30.14)])**.** *Let ρ, $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_n(F)$ be two semi-simple Galois representations. If ρ and ρ' have the same characteristic polynomials, then they are isomorphic. If F has characteristic zero, then ρ and ρ' are isomorphic if and only if for all $\sigma \in G_{\mathbb{Q}}$, the traces of $\rho(\sigma)$ and $\rho'(\sigma)$ are equal.*

The study of a Galois representation usually passes through the investigation of the ramification and the restriction of the representation to decomposition and inertia subgroups. We recall what they are. For a place v of $\overline{\mathbb{Q}}$ (Archimedean or not), the decomposition subgroup of $G_{\mathbb{Q}}$ associated to v is defined as

$$G_v := \{\sigma \in G_{\mathbb{Q}}, v \circ \sigma = v\}.$$

For a place p of $\mathbb{Q}$, all the decomposition subgroups G_v for $v \mid p$ are conjugated under Galois. We will denote by G_p an element of this conjugacy class of subgroups of $G_{\mathbb{Q}}$.

In the Archimedean case, G_∞ corresponds to a copy of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ inside $G_{\mathbb{Q}}$. A complex conjugation is the non-trivial element of such a subgroup, and any two complex conjugations are conjugated under $G_{\mathbb{Q}}$. A Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$ is said to be odd if for any complex conjugation c, we have

$$\det \rho(c) = -1.$$

In particular if $F \subseteq \overline{\mathbb{F}_2}$, every Galois representation is odd.

In the non-Archimedean case, let G_p be a decomposition subgroup of $G_\mathbb{Q}$ at a prime number p. The inertia subgroup I_p of G_p is the kernel of the projection $G_p \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. A Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(F)$ is said to be unramified at p if for any inertia subgroup I_p at p, we have $I_p \subseteq \ker \rho$. Otherwise, we say that ρ is ramified at p.

A Frobenius element Frob_p is any preimage in G_p of the Frobenius of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Two Frobenius elements of a fixed decomposition subgroup differ by an element of the inertia, and the sets of Frobenii of two decomposition subgroups are conjugated. Therefore, if a representation ρ is unramified at p, it makes sense to define the trace, the determinant, and the characteristic polynomial of ρ at a Frobenius element at p. The main reason we will use Frobenius elements in the rest of this part is the so-called Čebotarev theorem, which we now state.

Theorem 10.2 (Čebotarev)**.** *Let $K/\mathbb{Q}$ be a Galois extension (possibly infinite) that is unramified outside a finite set of primes S. Let P be a set of primes of density one not containing any element of S. The union of the conjugacy classes of Frobenius elements at $p \in P$ is dense in* $\mathrm{Gal}(K/\mathbb{Q})$.

Combining Čebotarev density theorem with Brauer–Nesbitt theorem 10.1, we get the following result.

Corollary 10.3 ([DS74, Lemme 3.2])**.** *Let ρ, $\rho' : G_\mathbb{Q} \to \mathrm{GL}_n(F)$ be two semi-simple Galois representations both unramified outside a finite set of primes S. If ρ and ρ' have the same characteristic polynomials (or the same traces if F has characteristic zero) at the Frobenius elements at $p \notin S$, then they are isomorphic.*

We conclude this section by recalling some facts on the Artin conductor. For a reference about this material, see [Ser68, Chapitres IV & VI]. Let $u \geqslant -1$ be a real number, and let v be a non-Archimedean place of $\overline{\mathbb{Q}}$ above a prime number p. Write G_v^u the u-th ramification subgroup of $G_\mathbb{Q}$ at the place v in upper-notation. For a Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}(V)$ acting on a F-vector space, with $F = \overline{\mathbb{Q}_\ell}$, $\overline{\mathbb{F}}_\ell$, or $\mathbb{C}$, the number

$$n_p := \int_{-1}^{+\infty} \dim V/V^{G_v^u} \mathrm{d}u,$$

is an integer if $p \neq \ell$. If ρ is unramified outside a finite number of places, the Artin conductor of ρ is defined as

$$N(\rho) := \prod_p p^{n_p},$$

where the product ranges over the primes $p \neq \ell$ if $F \neq \mathbb{C}$, and over all the primes if $F = \mathbb{C}$.

10.2 One dimensional Galois representations

10.2.1 Cyclotomic characters

Let ℓ be a prime number and n a positive integer. The group $G_\mathbb{Q}$ acts naturally on the group μ_{ℓ^n} of ℓ^n-th roots of unity. This gives rise to the cyclotomic character modulo ℓ^n:

$$\overline{\chi}_{\ell^n} : G_\mathbb{Q} \to \mathrm{Aut}(\mu_{\ell^n}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times .$$

This action is moreover compatible with the projection maps $\mathrm{Aut}(\mu_{\ell^n}) \to \mathrm{Aut}(\mu_{\ell^m})$ for $n \geqslant m$, giving a character

$$\chi_\ell := \varprojlim_{n \geqslant 1} \overline{\chi}_{\ell^n}.$$

This is the ℓ-adic cyclotomic character. As $\varprojlim_{n \geqslant 1} (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times$ this is an ℓ-adic character.

Let us compute the ramification of χ_ℓ and $\overline{\chi}_\ell$. The action of $G_\mathbb{Q}$ on μ_{ℓ^n} factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q})$ where ζ_{ℓ^n} is a primitive ℓ^n-th root of unity, and the only prime that ramifies in $\mathbb{Q}(\zeta_{\ell^n})$ is ℓ. Therefore, the inertia subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q})$ at a prime $p \neq \ell$ is trivial, and all the cyclotomic characters are unramified outside ℓ. Furthermore, for a prime p the action of a Frobenius element Frob_p on ζ_{ℓ^n} is given by $\mathrm{Frob}_p\, \zeta_{\ell^n} = \zeta_{\ell^n}^p$, and the one of a complex conjugation c is $c\zeta_{\ell^n} = \zeta_{\ell^n}^{-1}$. We get the following result.

Proposition 10.4. *Let ℓ be a prime number. The ℓ-adic and modulo ℓ cyclotomic characters are unramified outside ℓ. In particular, we have*

$$N(\chi_\ell) = N(\overline{\chi}_\ell) = 1.$$

Moreover, for all primes $p \neq \ell$ and complex conjugation c, we have

$$\begin{array}{llll} \chi_\ell(\mathrm{Frob}_p) = p & & \text{and} & \chi_\ell(c) = -1; \\ \overline{\chi}_\ell(\mathrm{Frob}_p) = p & \pmod{\ell} & \text{and} & \overline{\chi}_\ell(c) = -1 \pmod{\ell}. \end{array}$$

10.2.2 Dirichlet characters

Recall that a Dirichlet character of modulus $N \geqslant 1$ is a morphism $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Changing the field $\mathbb{C}$ to $\overline{\mathbb{F}}_\ell$, we get what we will call a residual Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_\ell^\times$. The conductor of a Dirichlet character (residual or not), is the smallest divisor of d of N such that the character factorises through $(\mathbb{Z}/d\mathbb{Z})^\times$.

We can go from one type of character to the other in the following way. As any Dirichlet character ε of modulus N has order at most $\varphi(N)$, its image lies in the ring of integers of $\mathbb{Q}(\zeta_{\varphi(N)})$. Choosing a prime ideal λ in this field above a prime number ℓ, we can reduce ε modulo λ to get a residual Dirichlet character $\overline{\varepsilon} : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_\ell^\times$. Note that the conductor of the character may decrease through this operation. In the other way, let us look at the behaviour of the roots of unity after reduction modulo some place $\mathfrak{L}$ of $\overline{\mathbb{Q}}$ above ℓ.

Lemma 10.5. *Let n be a positive integer and let ζ be a primitive n-th root of unity in $\overline{\mathbb{Q}}$. Let ℓ be a prime number and let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above ℓ. We have $\zeta \equiv 1 \pmod{\mathfrak{L}}$ if and only if n is a power of ℓ. In particular, a Dirichlet character is trivial modulo $\mathfrak{L}$ if and only if it has order a power of ℓ.*

Proof. According to [Coh07, Proposition 3.5.4], the algebraic norm of $1 - \zeta$ over $\mathbb{Q}(\zeta)$ is equal to:

$$\begin{cases} 0 & \text{if } n = 1; \\ q & \text{if } n = q^r \text{ with } q \text{ prime and } r \geqslant 1; \\ 1 & \text{otherwise.} \end{cases}$$

Thus, if n is not an ℓ-power, then ℓ does not divide the norm of $\zeta - 1$ and we have $\zeta \not\equiv 1 \pmod{\mathfrak{L}}$. Assume $n = \ell^r$, $r \geqslant 1$. We then have

$$\ell\mathbb{Z}[\zeta] = (1-\zeta)^{\ell^{r-1}(\ell-1)}\mathbb{Z}[\zeta].$$

Thus, the only prime ideal above ℓ in $\mathbb{Z}[\zeta]$ is $(1-\zeta)\mathbb{Z}[\zeta]$, and we therefore have $\zeta \equiv 1 \pmod{\mathfrak{L}}$.

For the second part of the lemma, let ε be a Dirichlet character modulo N. From above, ε is trivial modulo $\mathfrak{L}$ if and only if $\varepsilon(x)$ is a root of unity of order a power of ℓ for every $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. This happens if and only if ε has order a power of ℓ. ■

Lemma 10.5 implies that the kernel of the reduction modulo $\mathfrak{L}$ from the group of all roots of unity to $\overline{\mathbb{F}}_\ell^\times$, is the subgroup of primitive roots of unity of order a power of ℓ. In particular, the restriction of this map to the subgroup of roots of unity of order prime to ℓ is injective. Moreover, because the subgroup of roots of unity of order $\ell^n - 1$ maps to $\mathbb{F}_{\ell^n}^\times$, it is onto and therefore an isomorphism. Denoting μ_∞ the group of complex roots of unity, the inverse map

$$T_{\mathfrak{L}} : \overline{\mathbb{F}}_\ell^\times \to \{\zeta \in \mu_\infty, \gcd(\ell, \mathrm{ord}(\zeta)) = 1\},$$

is the so-called Teichmüller lift with respect to the place $\mathfrak{L}$. Therefore, given a residual Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_\ell^\times$, we can lift it to a Dirichlet character $T_{\mathfrak{L}} \circ \eta$ of prime-to-ℓ order. Moreover, the conductor of the character does not change during this process. Therefore, there is a correspondence between Dirichlet characters of modulus N (and of conductor $\mathfrak{c}$ respectively) with prime-to-ℓ order, and residual Dirichlet characters of modulus N (and of conductor $\mathfrak{c}$ respectively). Note that, there may be several ways to lift a residual Dirichlet characters depending on the place of $\overline{\mathbb{Q}}$ above ℓ we choose.

Next, we can see any Dirichlet character as a Galois representation of dimension one in the following way. For ζ_N a primitive root of unity, the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$. Therefore, we have the following diagram.

$$\begin{array}{ccc} G_{\mathbb{Q}} & \longrightarrow & \mathbb{Z}[\zeta_{\varphi(N)}]^\times \\ \downarrow & & \uparrow{\scriptstyle \varepsilon} \\ \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/N\mathbb{Z})^\times \end{array}$$

We will denote by ρ_ε the Galois representation $G_{\mathbb{Q}} \to \mathbb{Z}[\zeta_{\varphi(N)}]$ corresponding to ε. Conversely, given a one-dimensional complex representation $\rho : G_{\mathbb{Q}} \to \mathbb{C}^\times$, it has finite image and factors through a finite abelian extension of $\mathbb{Q}$. From Kronecker-Weber theorem, such extension is contained in a cyclotomic extension of $\mathbb{Q}$, and thus ρ comes from a Dirichlet character. Moreover, we have the following result.

Proposition 10.6 ([Ser68, Chapitres IV & VI])**.** *Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character of modulus N and conductor $\mathfrak{c}$. Denote by ρ_ε the associated Galois representation.*

The Artin conductor of ρ_ε is equal to $\mathfrak{c}$. Moreover, for a complex conjugation c and a Frobenius element Frob_p at a prime $p \nmid \mathfrak{c}$ we have

$$\rho_\varepsilon(c) = \varepsilon(-1) \qquad \text{and} \qquad \rho_\varepsilon(\mathrm{Frob}_p) = \varepsilon_0(p),$$

where ε_0 is the primitive Dirichlet character associated to ε. Finally, for a prime $p \mid \mathfrak{c}$, the representation $\rho_\varepsilon|_{I_p}$ corresponds to the p-part ε_p of ε.

Remark 10.7. *In the rest of the thesis Dirichlet characters of modulus N will also be regarded as totally multiplicative N-periodic functions ε from $\mathbb{Z}$ to $\mathbb{C}$ such that $\varepsilon(m) = 0$ if $\gcd(m, N) > 1$. This is indeed equivalent to the previous definition of Dirichlet characters because if $\varepsilon : \mathbb{Z} \to \mathbb{C}$ satisfies these properties, the function $\overline{n} \mapsto \varepsilon(n)$ is well-defined and a group homomorphism from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $\mathbb{C}^\times$. Conversely, if $\varepsilon \in \mathrm{Hom}\left((\mathbb{Z}/N\mathbb{Z})^\times, \mathbb{C}^\times\right)$, then one get a function*

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{C} \\ n & \longmapsto & \begin{cases} 0 & \text{if } \gcd(n, N) > 1 \\ \varepsilon(\overline{n}) & \text{otherwise} \end{cases} \end{array}$$

that satisfies the wanted properties.

10.3 Modular Galois representations

The main protagonists of the following chapters are the modular Galois representations, which have been of major interest in number theory in the last 50 years. The following theorem is the fundamental theorem of Deligne that states the existence of these objects.

Theorem 10.8 ([Del71])**.** *Let f be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε. Denote by K_f the number field generated by the Fourier coefficients of f, and let λ be a prime ideal in the ring of integers of K_f with residue characteristic ℓ. There exists a unique (up to isomorphism) odd Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda})$$

with values in the λ-adic completion $K_{f,\lambda}$ of K_f, such that

1. *$\rho_{f,\lambda}$ is unramified outside $N\ell$;*
2. *For every prime number $p \nmid N\ell$, the characteristic polynomial of $\rho_{f,\lambda}$ at Frob_p is equal to $X^2 - a_p(f)X + p^{k-1}\varepsilon(p)$.*

Remark 10.9. *Using the Čebotarev density theorem, the condition on the characteristic polynomial at the Frobenius elements can be reformulated as follows. For any prime $p \nmid N\ell$, we have $\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p(f)$ and the determinant of $\rho_{f,\lambda}$ is equal to $\chi_\ell^{k-1}\varepsilon$.*

We have seen in the introduction that any ℓ-adic Galois representation gives rise to a unique semi-simple residual Galois representation. This gives the following result.

Theorem 10.10. *Let $f := \sum_{n \geqslant 1} a_n(f)q^n$ be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε. Denote by K_f the number field generated by the Fourier coefficients of f, and let λ be a prime ideal in the ring of integers of K_f with residue characteristic ℓ and denote by $\mathbb{F}_\lambda$ the residue field of λ. There exists a unique (up to isomorphism) semi-simple, odd Galois representation*

$$\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

such that

1. *$\overline{\rho}_{f,\lambda}$ is unramified outside $N\ell$;*
2. *For every prime number $p \nmid N\ell$, the characteristic polynomial of $\overline{\rho}_{f,\lambda}$ at Frob_p is equal to $X^2 - a_p(f)X + p^{k-1}\varepsilon(p) \pmod{\lambda}$.*

Remark 10.11. *Again, the second condition is equivalent to the fact that the trace of $\overline{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is equal to $a_p(f) \pmod{\lambda}$ and that the determinant of $\overline{\rho}_{f,\lambda}$ is $\overline{\chi}_\ell^{k-1}\varepsilon \pmod{\lambda}$.*

Given f and λ, one can ask what are the Galois theoretical invariants of $\rho_{f,\lambda}$ and $\overline{\rho}_{f,\lambda}$ we discussed in section 10.1 such as their ramification, their Artin conductors, and their shape at the decompositions subgroups. The answer to these questions are now well-known but are in general difficult results. First, the Artin conductor of $\rho_{f,\lambda}$ has been computed by Carayol in [Car86, Théorème (A)], and the study of the behaviour the Artin conductor of $\overline{\rho}_{f,\lambda}$ has been independently obtained by Carayol in [Car89, Proposition 2] and Livné [Liv89, 2.3 Proposition].

Proposition 10.12 (Carayol-Livné)**.** *The Artin conductor of $\rho_{f,\lambda}$ is equal to the prime-to-ℓ part of the level N of f. The Artin conductor of $\overline{\rho}_{f,\lambda}$ satisfies*

$$N(\overline{\rho}_{f,\lambda}) \mid N.$$

Moreover, for a prime number $p \neq \ell$, we have

$$v_p(N) - v_p(N(\overline{\rho}_{f,\lambda})) \in \{0, 1, 2\}.$$

Next, the local behaviour of $\overline{\rho}_{f,\lambda}$ has been also well studied. First at a decomposition subgroup at ℓ, the following result has been obtained by Deligne when $a_\ell(f) \not\equiv 0 \pmod{\lambda}$, and by Fontaine when $a_\ell(f) \equiv 0 \pmod{\lambda}$. Before stating their result, we make the following definition.

Definition 10.13. *Let p be any prime number, and let $x \in \overline{\mathbb{Z}_p}$. We denote by $\mu_p(x)$ (or simply $\mu(x)$), the unique unramified character of G_p that send Frob_p to x.*

Proposition 10.14 (Deligne–Fontaine, [Edi92, Theorem 2.5 and Theorem 2.6])**.** *Assume that $2 \leqslant k \leqslant \ell + 1$ and $\ell \nmid N$.*

- *If f is ordinary at λ (that is if $a_\ell(f) \not\equiv 0 \pmod{\lambda}$), then $\overline{\rho}_{f,\lambda}|_{G_\ell}$ is reducible, and we have*

$$\overline{\rho}_{f,\lambda}|_{G_\ell} \cong \begin{pmatrix} \overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right) & \star \\ 0 & \mu\left(a_\ell(f)\right) \end{pmatrix}.$$

- *If f is not ordinary at λ, then $\overline{\rho}_{f,\lambda}|_{G_\ell}$ is irreducible, and we have*

$$\overline{\rho}_{f,\lambda}|_{I_\ell} \cong \begin{pmatrix} \phi^{k-1} & 0 \\ 0 & \phi'^{k-1} \end{pmatrix}.$$

Here $\{\phi, \phi'\} = \{\phi, \phi^\ell\}$ stands for the set of fundamental characters of level 2 (see [Edi92, §2.4]).

Using only proposition 10.14, we can prove a bound for the prime ideals λ of $\mathcal{O}_f$ for which the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$, or $\mathfrak{A}_5$. As mentioned in the introduction, the statement and the proof given in [Pea21] were not correct as mentioned in remark 8.9. We fix it here and give a more precise result.

Theorem 10.15. *Let f be a newform of weight k, level N, and character ε.*

- *If the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $\mathfrak{A}_4$, then either $\ell \mid N$, or $\ell \leqslant 3k-2$.*
- *If the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $\mathfrak{S}_4$, then either $\ell \mid N$, or $\ell \leqslant 4k-3$.*
- *If the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $\mathfrak{A}_5$, then either $\ell \mid N$, or $\ell \leqslant 5k-4$.*

Proof. Assume the order of the projective of image of $\overline{\rho}_{f,\lambda}$ is prime-to-ℓ and that $\ell \nmid N$ and that $\ell \geqslant k-1$. If f is ordinary at ℓ, by proposition 10.14, we have

$$\overline{\rho}_{f,\lambda}|_{I_\ell} \cong \begin{pmatrix} \overline{\chi}_\ell^{k-1} & \star \\ 0 & \mathbb{1} \end{pmatrix}.$$

As the projective order of the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, for a, $b \in \mathbb{F}_\lambda$, is equal to ℓ if $a \neq 1$ and $b \neq 0$, we necessarily have $\star = 0$ because the order of the projective image of $\overline{\rho}_{f,\lambda}$ is prime-to-ℓ by assumption. We deduce that the projective image of I_ℓ is isomorphic to $\overline{\chi}_\ell^{k-1}(I_\ell)$, which is a cyclic group of order

$$\#\mathbb{P}\overline{\rho}_{f,\lambda}(I_\ell) = \frac{\ell-1}{\gcd(\ell-1,k-1)}.$$

Similarly, if f is not ordinary at ℓ, by proposition 10.14 we have

$$\overline{\rho}_{f,\lambda}|_{I_\ell} \cong \begin{pmatrix} \phi^{k-1} & 0 \\ 0 & \phi^{(k-1)\ell} \end{pmatrix}.$$

Therefore, the projective image of I_ℓ is isomorphic to $\phi^{(k-1)(\ell-1)}(I_\ell)$, which is a cyclic group of order

$$\#\mathbb{P}\overline{\rho}_{f,\lambda}(I_\ell) = \frac{\ell^2-1}{\gcd(\ell^2-1,(k-1)(\ell-1))} = \frac{\ell+1}{\gcd(\ell+1,k-1)}.$$

Assume that we are in the $\mathfrak{A}_4$ case. As $\mathfrak{A}_4$ contains only elements of order less or equal to 3, the projective image of I_ℓ must be of order at most 3. In the ordinary case we get

$$\begin{aligned} \frac{\ell-1}{\gcd(\ell-1,k-1)} \leqslant 3 \quad &\Longrightarrow \quad \ell-1 \leqslant 3\gcd(\ell-1,k-1) \leqslant 3(k-1) \\ &\Longrightarrow \quad \ell \leqslant 3k-2. \end{aligned}$$

Similarly, in the non-ordinary case, we get

$$\begin{aligned} \frac{\ell+1}{\gcd(\ell+1,k-1)} \leqslant 3 \quad &\Longrightarrow \quad \ell+1 \leqslant 3\gcd(\ell+1,k-1) \leqslant 3(k-1) \\ &\Longrightarrow \quad \ell \leqslant 3k-4. \end{aligned}$$

Therefore, in the $\mathfrak{A}_4$ case, we necessarily have $\ell \leqslant 3k-2$.

Similarly, the group $\mathfrak{S}_4$ contains only elements of order less or equal to 4. With same calculations as above, we deduce that ℓ must be less or equal to $4k-3$. Finally, $\mathfrak{A}_5$ contains only elements of order less or equal to 5, and we get $\ell \leqslant 5k-4$ in this case. ∎

Finally, the shape of the local residual representation at the primes dividing the level but different from ℓ is also essentially known. It has been derived by Langlands and compiled in [LW12, Proposition 2.8]. In order to justify some details about it, we first need a result coming purely from the theory of modular forms.

Proposition 10.16 ([Miy06, Theorem 4.6.17])**.** *Let p be a prime dividing N and write $\mathfrak{c}$ for the conductor of ε.*

1. *If $v_p(N) = v_p(\mathfrak{c})$, then $|a_p(f)|^2 = p^{k-1}$.*
2. *If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then $a_p(f)^2 = \varepsilon'_p(p)p^{k-2}$, where ε'_p is the prime-to-p component of ε (in particular $\varepsilon'_p(p) \neq 0$).*
3. *If $v_p(N) \geqslant 2$ and $v_p(N) > v_p(\mathfrak{c})$, then $a_p(f) = 0$.*

Proposition 10.17. *Let $p \neq \ell$ be a prime dividing N and let $\mathfrak{c}$ be the conductor of ε. We denote by v_p the p-adic valuation.*

- *If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then we have*

$$\overline{\rho}_{f,\lambda}|_{G_p} \cong \begin{pmatrix} \mu(a_p(f))\overline{\chi}_\ell & \star \\ 0 & \mu(a_p(f)) \end{pmatrix}.$$

- *If $v_p(N) = v_p(\mathfrak{c})$, then $a_p(f)$ is a unit in $\mathcal{O}_{f,\lambda}$ and we have*

$$\overline{\rho}_{f,\lambda}|_{G_p} \cong \mu\left(a_p(f)\right) \oplus \mu\left(a_p(f)^{-1}\right) \overline{\chi}_\ell^{k-1}\overline{\varepsilon|_{G_p}},$$

where $\overline{\varepsilon|_{G_p}}$ stands for the reduction modulo λ of the restriction of ε to G_p.

Proof. From the first case of proposition 10.16, we have $|a_p(f)|^2 = p^{k-1}$ in the second case. Therefore, $a_p(f)$ is indeed invertible in $\mathcal{O}_{f,\lambda}$ because $p \neq \ell$.

The only thing to prove is that the hypothesis of [LW12, Proposition 2.8] holds in our cases, namely that f is p-primitive in the terminology of [LW12, Definition 2.7]. To do so, we use [LW15, Theorem]. We recall a direct consequence of this result. Let $u = \min\left(\left\lfloor \frac{v_p(N)}{2} \right\rfloor, v_p(N) - v_p(\mathfrak{c})\right)$. If $u = 0$, then f is p-primitive. We easily check that in our two cases we have $u = 0$. ∎

Chapter 11

Background on Eisenstein series

11.1 Generalised Bernoulli numbers and Gauß sums

Let ε be a primitive Dirichlet character of conductor $\mathfrak{c}$. We recall the definition and properties of the Gauß sums and generalised Bernoulli numbers attached to ε.

Definition 11.1. *The Bernoulli numbers $(B_{m,\varepsilon})_{m\geqslant 0}$ attached to ε are defined by the following generating series:*

$$\sum_{m=0}^{\infty} B_{m,\varepsilon}\frac{t^m}{m!} := \sum_{n=1}^{\mathfrak{c}} \varepsilon(n)\frac{te^{nt}}{e^{\mathfrak{c}t}-1}.$$

Remark 11.2. *If $\varepsilon = \mathbb{1}$ is the trivial character modulo 1, we get the classical Bernoulli numbers except when $m = 1$, in which case we have $B_{1,\mathbb{1}} = \frac{1}{2} = -B_1$.*

Proposition 11.3. *When ε is odd, we have*

$$B_{1,\varepsilon} = \frac{1}{\mathfrak{c}}\sum_{n=1}^{\mathfrak{c}-1} n\varepsilon(n),$$

and when ε is both even and non-trivial, we have

$$B_{2,\varepsilon} = \frac{1}{\mathfrak{c}}\sum_{n=1}^{\mathfrak{c}-1} n^2\varepsilon(n).$$

Proof. Let us compute the Taylor expansion of $\frac{te^{nt}}{e^{\mathfrak{c}t}-1}$ for some positive integer n.

$$\begin{aligned}
\frac{te^{nt}}{e^{\mathfrak{c}t}-1} &= \frac{te^{nt}}{\mathfrak{c}t + \frac{\mathfrak{c}^2t^2}{2} + \frac{\mathfrak{c}^3t^3}{6} + o(t^3)} \\
&= \frac{e^{nt}}{\mathfrak{c}\left(1 + \frac{\mathfrak{c}t}{2} + \frac{\mathfrak{c}^2t^2}{6} + o(t^2)\right)} \\
&= \frac{1}{\mathfrak{c}}\left(1 + nt + \frac{n^2t^2}{2} + o(t^2)\right)\left(1 - \left(\frac{\mathfrak{c}t}{2} + \frac{\mathfrak{c}^2t^2}{6}\right) + \frac{\mathfrak{c}^2t^2}{4} + o(t^2)\right) \\
&= \frac{1}{\mathfrak{c}} + t\left(\frac{n}{\mathfrak{c}} - \frac{1}{2}\right) + \frac{t^2}{2}\left(\frac{n^2}{\mathfrak{c}} - n + \frac{\mathfrak{c}}{6}\right) + o(t^2).
\end{aligned}$$

It follows that for any primitive Dirichlet character ε, we have $B_{1,\varepsilon} = \sum_{n=1}^{\mathfrak{c}} \varepsilon(n)\left(\frac{n}{\mathfrak{c}} - \frac{1}{2}\right)$ and $B_{2,\varepsilon} = \sum_{n=1}^{\mathfrak{c}} \varepsilon(n)\left(\frac{n^2}{\mathfrak{c}} - n + \frac{\mathfrak{c}}{6}\right)$.

Assume that ε is odd. As it is not the trivial character we have $\sum_{n=1}^{\mathfrak{c}} \varepsilon(n) = 0$ and therefore

$$B_{1,\varepsilon} = \sum_{n=1}^{\mathfrak{c}} \varepsilon(n)\left(\frac{n}{\mathfrak{c}} - \frac{1}{2}\right) = \frac{1}{\mathfrak{c}} \sum_{n=1}^{\mathfrak{c}} n\varepsilon(n).$$

Assume that ε is even and non-trivial. We have $\sum_{n=0}^{\mathfrak{c}-1} \varepsilon(n) = 0$. Moreover,

$$\sum_{n=1}^{\mathfrak{c}} n\varepsilon(n) \overset{n=\mathfrak{c}-m}{=} \sum_{m=0}^{\mathfrak{c}-1} (\mathfrak{c}-m)\varepsilon(\mathfrak{c}-m) = \sum_{m=0}^{\mathfrak{c}-1} (\mathfrak{c}-m)\varepsilon(m) = -\sum_{m=1}^{\mathfrak{c}} m\varepsilon(m).$$

This sum is therefore equal to zero and we get

$$B_{2,\varepsilon} = \sum_{n=1}^{\mathfrak{c}} \varepsilon(n)\left(\frac{\mathfrak{c}}{6} + \frac{n^2}{\mathfrak{c}} - n\right) = \frac{1}{\mathfrak{c}} \sum_{n=1}^{\mathfrak{c}} n^2\varepsilon(n).$$

■

We state below the main properties of the Bernoulli numbers. First, we exactly know when the Bernoulli numbers vanish (see [Miy06, Theorem 3.3.4] for a proof).

Proposition 11.4. *We have $B_{m,\varepsilon} = 0$ if and only if $\varepsilon(-1) \neq (-1)^m$.*

Secondly, the behaviour of the Bernoulli numbers after reduction modulo a prime ideal has been studied by Van-Staudt [Sta40] in the case $\varepsilon = \mathbb{1}$, and by Carlitz [Car59, Theorem 1] in the case $\varepsilon \neq \mathbb{1}$. We summarise their results in the following proposition.

Proposition 11.5. *Let m be a positive integer.*

1. *Let ℓ be a prime number. If $\ell - 1$ divides m, then we have $\ell B_{m,\mathbb{1}} \equiv -1 \pmod{\ell}$. Otherwise, $\frac{B_{m,\mathbb{1}}}{m}$ is ℓ-integral and its reduction modulo ℓ depends only on the residue class of m modulo $\ell - 1$. In particular, the denominator of $B_{m,\mathbb{1}}$ is equal to $\prod_{\substack{\ell \text{ prime} \\ \ell-1 \mid m}} \ell$.*

2. *For $\varepsilon \neq \mathbb{1}$, write $\frac{B_{m,\varepsilon}}{m} = \mathfrak{N}\mathfrak{D}^{-1}$, with $\mathfrak{N}$ and $\mathfrak{D}$ two coprime ideals of $\mathbb{Z}[\varepsilon]$, the ring spanned by the image of ε. If the conductor of ε admits at least two distinct prime factors, then $\mathfrak{D} = 1$. Otherwise, if the conductor of ε is a power of a prime number ℓ, then $\mathfrak{D}$ contains only prime ideals above ℓ.*

Another classical quantity attached to Dirichlet characters is its Gauß sum. We recall its definition and properties below.

Definition 11.6. *The Gauß sum attached to ε is defined as*

$$W(\varepsilon) := \sum_{n=1}^{\mathfrak{c}} \varepsilon(n) e^{\frac{2i\pi n}{\mathfrak{c}}}.$$

One can find the following result in [BD14, Lemma 2.1].

Proposition 11.7. *The prime divisors of the algebraic norm of $W(\varepsilon)$ are those of $\mathfrak{c}$.*

11.2 Eisenstein series

Let k be a positive integer and let ε_1, ε_2 be two Dirichlet characters modulo $\mathfrak{c}_1$ and $\mathfrak{c}_2$ respectively, and such that $\varepsilon_1\varepsilon_2(-1) = (-1)^k$. Moreover, if $k = 2$ and ε_1, ε_2 are both trivial, then assume $\mathfrak{c}_1 = 1$ and $\mathfrak{c}_2$ is a prime number. Otherwise, assume that ε_1 and ε_2 are primitive. For a complex number z in the upper-half plane $\mathcal{H}$, consider the following q-expansion:

$$E_k^{\varepsilon_1,\varepsilon_2}(z) := C + \sum_{n=1}^{\infty} \sigma_{k-1}^{\varepsilon_1,\varepsilon_2}(n) q^n, \tag{11.1}$$

with $\sigma_r^{\varepsilon_1,\varepsilon_2}(n) := \sum_{0<d|n} d^r \varepsilon_1\left(\frac{n}{d}\right)\varepsilon_2(d)$ for any $r \geqslant 0$ and

$$C := \begin{cases} 0 & \left| \begin{array}{ll} & \text{if } k \geqslant 2 \text{ and } \varepsilon_1 \neq \mathbb{1}, \\ \text{or} & \text{if } k = 1 \text{ and } \varepsilon_1, \varepsilon_2 \text{ are both non-trivial;} \end{array} \right. \\ \frac{1}{24}(\mathfrak{c}_2 - 1) & \text{if } k = 2 \text{ and } \varepsilon_1, \varepsilon_2 \text{ both trivial;} \\ -\frac{B_{k,\varepsilon_1\varepsilon_2}}{2k} & \text{otherwise.} \end{cases}$$

The following result is proved in [Miy06, Theorem 4.7.1] and [Miy06, (4.7.16)].

Proposition 11.8. *The q-series $E_k^{\varepsilon_1,\varepsilon_2}$ defines a modular form of weight k, level $\mathfrak{c}_1\mathfrak{c}_2$ and character $\varepsilon_1\varepsilon_2$. It is a normalised eigenform for all the Hecke operators at level $\mathfrak{c}_1\mathfrak{c}_2$.*

For $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, the definition of the series $E_k^{\mathbb{1},\mathbb{1}}$ agrees with the definition of the classical Eisenstein series of weight k. We simply write it E_k in this case. For $k = 2$, we denote by E_2 the q-series

$$E_2(z) := -\frac{1}{24} + \sum_{n=1}^{\infty} \left(\sum_{0<d|n} d \right) q^n.$$

Note that this formula defines a holomorphic function on $\mathcal{H}$, but E_2 is not modular.

In the case $k \geqslant 2$ and ε_1, ε_2 primitive, the behaviour of the constant coefficient of $E_k^{\varepsilon_1,\varepsilon_2}$ at a cusp of $\Gamma_1(N)$ has been computed in [BM18, Proposition 4]. It states the following:

Proposition 11.9. *Assume $k \geqslant 2$ and ε_1, ε_2 are primitive. Let M be a positive integer and let $\gamma := \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Put $\widetilde{v} := \frac{v}{\gcd(v,M)}$ and $\widetilde{M} := \frac{M}{\gcd(v,M)}$. We define*

$$\Upsilon_k^{\varepsilon_1,\varepsilon_2}(\gamma, M) := \lim_{\mathrm{Im}(z)\to+\infty} (E_k^{\varepsilon_1,\varepsilon_2}(M\cdot)|_k\gamma)(z),$$

where we denote by $|_k$ *the classical slash action of weight* k.

If $\mathfrak{c}_2 \nmid \widetilde{v}$ *then,* $\Upsilon_k^{\varepsilon_1,\varepsilon_2}(\gamma, M) = 0$. *Otherwise, if* $\mathfrak{c}_2 \mid \widetilde{v}$ *then* $\Upsilon_k^{\varepsilon_1,\varepsilon_2}(\gamma, M) \neq 0 \Leftrightarrow \gcd\left(\mathfrak{c}_1, \frac{\widetilde{v}}{\mathfrak{c}_2}\right) = 1$. *In this case, we moreover have*

$$\Upsilon_k^{\varepsilon_1,\varepsilon_2}(\gamma, M) = -\varepsilon_2^{-1}\left(\widetilde{M}u\right)\varepsilon_1\left(-\frac{\widetilde{v}}{\mathfrak{c}_2}\right)\frac{W((\varepsilon_1\varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \times \frac{B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}}{2k}\left(\frac{\mathfrak{c}_2}{\widetilde{M}\mathfrak{c}_0}\right)^k \prod_{p\mid\mathfrak{c}_1\mathfrak{c}_2}\left(1 - \frac{(\varepsilon_1\varepsilon_2^{-1})_0(p)}{p^k}\right),$$

where χ_0 *denotes the primitive character associated to a Dirichlet character* χ, *and* $\mathfrak{c}_0$ *the conductor of* $\varepsilon_1^{-1}\varepsilon_2$.

The proof of [BM18] is only given in the cases $k \geqslant 3$, and $k = 2$ and ε_1, ε_2 non-trivial. We give a proof of the result in the case $k = 2$, $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, based on the techniques used in [BM18].

Proof. As in [BM18, §1.3], we write for $\mathrm{Re}(\varepsilon) > 0$ and $z \in \mathcal{H}$,

$$G_{2,\varepsilon}(z) := \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^2|mz+n|^{2\varepsilon}}.$$

By [Miy06, Corollary 7.2.10 and Theorem 7.2.12], the function $\varepsilon \mapsto G_{2,\varepsilon}(z)$ is holomorphically continued to $\mathrm{Re}(\varepsilon) > -\frac{1}{2}$ and we have

$$\lim_{\varepsilon\to 0} G_{2,\varepsilon}(z) = -8\pi^2 E_2(z) - \frac{\pi}{\mathrm{Im}(z)}.$$

Now, because $\mathrm{Im}\left(M\frac{uz+\beta}{vz+\delta}\right) = \frac{M\,\mathrm{Im}(z)}{|vz+\delta|^2}$, we get

$$\begin{aligned}\Upsilon_2^{\mathbb{1},\mathbb{1}}(\gamma, M) &= \lim_{\mathrm{Im}(z)\to+\infty}\lim_{\varepsilon\to 0}\left(-\frac{1}{8\pi^2}G_{2,\varepsilon}(M\cdot)|_2\gamma(z) + \frac{1}{(vz+\delta)^2}\frac{1}{8\pi\,\mathrm{Im}\left(M\frac{uz+\beta}{vz+\delta}\right)}\right)\\ &= -\frac{1}{8\pi^2}\lim_{\mathrm{Im}(z)\to+\infty}\lim_{\varepsilon\to 0} G_{2,\varepsilon}(M\cdot)|_2\gamma(z) + \lim_{\mathrm{Im}(z)\to+\infty}\frac{|vz+\delta|^2}{8\pi M(vz+\delta)^2\,\mathrm{Im}(z)}\\ &= -\frac{1}{8\pi^2}\lim_{\mathrm{Im}(z)\to+\infty}\lim_{\varepsilon\to 0} G_{2,\varepsilon}(M\cdot)|_2\gamma(z).\end{aligned}$$

From this identity the proof of [BM18] still applies. Let us write $z^{2,\varepsilon} := z^2|z|^{2\varepsilon}$. The function $G_{2,\varepsilon}(M\cdot)|_2\gamma(z)$ writes as $T_\varepsilon(z) + R_\varepsilon(z)$, with

$$T_\varepsilon(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}\\ mMu+nv=0}} \frac{1}{(mM\beta+n\delta)^{2,\varepsilon}},$$

$$\text{and}\quad R_\varepsilon(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}\\ mMu+nv\neq 0}} \frac{1}{((mMu+nv)z+(mM\beta+n\delta))^{2,\varepsilon}}.$$

The function T_ε is independent of z and the series is absolutely convergent for $\varepsilon > \frac{1}{2}$. Therefore, we have

$$\lim_{\mathrm{Im}(z)\to+\infty} \lim_{\varepsilon\to 0} T_\varepsilon(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ mMu+nv=0}} \frac{1}{(mM\beta+n\delta)^2}.$$

Finally, writing n in $R_\varepsilon(z)$ as $Mn'+\rho$, with ρ between 0 and $M-1$, we have

$$\begin{aligned} R_\varepsilon(z) &= \sum_{(m,n')\in\mathbb{Z}^2} \sum_{\substack{0\leqslant\rho\leqslant M-1 \\ M(mu+n'v)+v\rho\neq 0}} \frac{1}{(z(M(mu+n'v)+v\rho)+M(m\beta+n'\delta)+\rho\delta)^{2,\varepsilon}} \\ &\overset{\substack{p=mu+n'v \\ q=m\beta+n'\delta}}{=} \sum_{\rho=0}^{M-1} \sum_{\substack{(p,q)\in\mathbb{Z}^2 \\ Mp+v\rho\neq 0}} \frac{1}{(z(Mp+v\rho)+Mq+\delta\rho)^{2,\varepsilon}}. \end{aligned}$$

The last equality is justified by the fact that $(p,q) = (m,n')\gamma$, and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Applying [BM18, Lemma 9] with $a_1 = v\rho$, $a_2 = \delta\rho$ and $D = M$, we get

$$\lim_{\mathrm{Im}(z)\to+\infty} \lim_{\varepsilon\to 0} R_\varepsilon(z) = 0.$$

Lemma 6 of [BM18] therefore still applies in the case $(k,\varepsilon_1,\varepsilon_2) = (2,\mathbb{1},\mathbb{1})$ and one easily checks that the proof of lemma 7 and proposition 4 of [BM18] only uses the fact that ε_1 and ε_2 are Dirichlet characters satisfying $\varepsilon_1\varepsilon_2(-1) = (-1)^k$. ■

Chapter 12

Preliminary results on modular forms

12.1 Theta operators

We fix for this paragraph a place $\mathfrak{L}$ of $\overline{\mathbb{Q}}$. Consider the operator θ acting on the space of holomorphic functions on $\mathcal{H}$ by $\frac{1}{2i\pi}\frac{\mathrm{d}}{\mathrm{d}z} = q\frac{\mathrm{d}}{\mathrm{d}q}$. On q-expansions, this operator maps $\sum_{n\geqslant 0} a_n q^n$ to $\sum_{n\geqslant 0} n a_n q^n$. It is well-known that if g is a modular form, then θg is no longer modular (see for example [Zag08, Chapter 5]). However, Swinnerton-Dyer and Serre [Swi73, § 3] have proved that for $\ell \geqslant 5$ and a level 1 modular form g with $\mathfrak{L}$-integral Fourier coefficients, one can construct a level 1 form with $\mathfrak{L}$-integral Fourier coefficients and which Fourier coefficients are congruent modulo $\mathfrak{L}$ to the one of θg. More generally, Katz [Kat77] has proved using his geometric theory of modular forms that there is an operator on the space of modular forms with coefficients in an algebraic closure of $\mathbb{F}_\ell$, whose action on the q-expansions is the same as the one of θ. For our purposes, the main drawbacks of this latter approach is that Katz' modular forms modulo $\mathfrak{L}$ do not always lift in characteristic 0, and have by essence a prime-to-ℓ level. To remedy this, we will construct for any given level $N \geqslant 1$ and place $\mathfrak{L}$, an operator $\widetilde{\theta}$ acting on $\mathrm{M}(N)$ – the graded algebra of modular forms of level N –, stabilising the subspace of modular forms with $\mathfrak{L}$-integral Fourier coefficients, and such that for every modular form g with $\mathfrak{L}$-integral coefficients we have

$$\widetilde{\theta} g \equiv \theta g \pmod{\mathfrak{L}},$$

meaning that $a_n\big(\widetilde{\theta} g\big)$ and $n a_n(g)$ are congruent modulo $\mathfrak{L}$ for all n.

The main tool we will use in the construction of $\widetilde{\theta}$ is the Rankin–Cohen bracket, introduced by Cohen in [Coh75, Corollary 7.2]. We recall its definition and properties below.

Proposition 12.1 (Rankin–Cohen bracket)**.** *Let g and h be two modular forms of weight k_g and k_h, level N_g and N_h, and character ε_g and ε_h respectively. The Rankin–Cohen bracket of g and h is*

$$[g,h] := k_g g\theta h - k_h h\theta g.$$

It is a cuspidal modular form of weight $k_g + k_h + 2$, level $\mathrm{lcm}(N_g, N_h)$ and character $\varepsilon_g\varepsilon_h$. Moreover, if both g and h have their Fourier coefficients in a ring R, then so has $[g,h]$.

Let N be a positive integer. For a prime number p, we denote by T_p^N the p-th Hecke operator acting on $\mathrm{M}(N)$. Recall that a modular form $g \in \mathrm{M}_k(N,\varepsilon)$ is an eigenform for T_p^N modulo $\mathfrak{L}$ with eigenvalue $a_p \in \overline{\mathbb{F}}_\ell$ in the sense of [DS74, §6(b)] if g has $\mathfrak{L}$-integral Fourier coefficients, and if

$$T_p^N g \equiv a_p g \pmod{\mathfrak{L}}.$$

If g is moreover normalised modulo $\mathfrak{L}$, that is if $a_1(g) \equiv 1 \pmod{\mathfrak{L}}$, then g is an eigenform for T_p^N modulo $\mathfrak{L}$ if and only if for all integer $n \geqslant 0$ prime to p, and all $\alpha \geqslant 1$, we have

$$\begin{cases} a_{np^\alpha}(g) \equiv a_n(g)a_{p^\alpha}(g) \pmod{\mathfrak{L}}; \\ a_{p^{\alpha+1}}(g) \equiv a_p(g)a_{p^\alpha}(g) - p^{k-1}\varepsilon(p)a_{p^{\alpha-1}}(g) \pmod{\mathfrak{L}}. \end{cases}$$

The eigenvalue is then moreover equal to the reduction of $a_p(g)$ modulo $\mathfrak{L}$. The following lemma is the central result that shows how to construct an operator $\widetilde{\theta}$ satisfying the properties described above, using Rankin–Cohen brackets.

Lemma 12.2. *Let k_A be a positive integer, and let χ_A be a Dirichlet character modulo N. Let $A \in \mathrm{M}_{k_A}(N,\chi_A)$ be such that A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral Fourier coefficients and satisfy*

$$A \equiv 1 \pmod{\mathfrak{L}}, \quad \frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}, \quad \text{and} \quad \chi_A \equiv \overline{\chi}_\ell^{-k_A} \pmod{\mathfrak{L}}.$$

Then, we have a well-defined operator $\widetilde{\theta}_A$ on $\mathrm{M}(N)$ given by $\widetilde{\theta}_A g := -\frac{1}{k_A}[g,A]$. For every $g \in \mathrm{M}_k(N,\varepsilon)$ with $\mathfrak{L}$-integral Fourier coefficients, this operator satisfies the following properties.

- *$\widetilde{\theta}_A g \in \mathrm{S}_{k+k_A+2}(N,\varepsilon\chi_A)$ and has $\mathfrak{L}$-integral Fourier coefficients;*
- *$\widetilde{\theta}_A g \equiv \theta g \pmod{\mathfrak{L}}$;*
- *If for some prime number p, g is a normalised eigenform for T_p^N modulo $\mathfrak{L}$ then so is $\widetilde{\theta}_A g$ with eigenvalue $pa_p(g) \pmod{\mathfrak{L}}$.*

In the following, when there will be no confusion on the form A, we shall write $\widetilde{\theta}$ for the operator $\widetilde{\theta}_A$.

Proof. According to proposition 12.1 above, this is clear that $\widetilde{\theta}_A$ is a well-defined operator and that $\widetilde{\theta}_A g$ has the announced weight, level, and character. Furthermore, we have $\widetilde{\theta}_A g = -\frac{k}{k_A} g\theta A + A\theta g$. Therefore, from the assumptions, if g has $\mathfrak{L}$-integral Fourier coefficients, then so does $\widetilde{\theta}_A g$ and we have

$$\widetilde{\theta}_A g = A\theta g - \frac{1}{k_A}\theta A \times kg \equiv \theta g \pmod{\mathfrak{L}}.$$

Assume g is a normalised eigenform for T_p^N modulo $\mathfrak{L}$. Then, $\widetilde{\theta}_A g$ is also normalised modulo $\mathfrak{L}$ because we have $a_1\left(\widetilde{\theta}_A g\right) \equiv 1 \times a_1(g) \equiv 1 \pmod{\mathfrak{L}}$. Let $n \geqslant 0$ be prime to p, and $\alpha \geqslant 1$. We have

$$a_{np^\alpha}\left(\widetilde{\theta}_A g\right) \equiv np^\alpha a_{np^\alpha}(g) \equiv na_n(g) \times p^\alpha a_{p^\alpha}(g) \equiv a_n\left(\widetilde{\theta}_A g\right) a_{p^\alpha}\left(\widetilde{\theta}_A g\right) \pmod{\mathfrak{L}},$$

and

$$\begin{aligned} a_{p^{\alpha+1}}\left(\widetilde{\theta}_A g\right) &\equiv p^{\alpha+1} a_{p^{\alpha+1}}(g) \pmod{\mathfrak{L}} \\ &\equiv p^{\alpha+1}\left(a_p(g)a_{p^\alpha}(g) - p^{k-1}\varepsilon(p)a_{p^{\alpha-1}}(g)\right) \pmod{\mathfrak{L}} \\ &\equiv pa_p(g) \times p^\alpha a_{p^\alpha}(g) - p^2 p^{k-1}\varepsilon(p) \times p^{\alpha-1}a_{p^{\alpha-1}}(g) \pmod{\mathfrak{L}} \\ &\equiv a_p\left(\widetilde{\theta}_A g\right) a_{p^\alpha}\left(\widetilde{\theta}_A g\right) - p^{k+1}\varepsilon(p)a_{p^{\alpha-1}}\left(\widetilde{\theta}_A g\right) \pmod{\mathfrak{L}}. \end{aligned}$$

We claim that $p^{k+1}\varepsilon(p)$ is congruent to $p^{(k+k_A+2)-1}(\varepsilon\chi_A)(p)$ modulo $\mathfrak{L}$. Indeed, if $p \mid N\ell$, then both sides are congruent to 0 modulo $\mathfrak{L}$. If $p \nmid N\ell$, we have $p^{k_A}\chi_A(p) \equiv 1 \pmod{\mathfrak{L}}$ by assumption, and therefore

$$p^{k+k_A+1}\varepsilon(p)\chi_A(p) \equiv p^{k+k_A+1}\varepsilon(p)p^{-k_A} \equiv p^{k+1}\varepsilon(p) \pmod{\mathfrak{L}}.$$

As desired, we get

$$a_{p^{\alpha+1}}\left(\widetilde{\theta}_A g\right) \equiv a_p\left(\widetilde{\theta}_A g\right) a_{p^\alpha}\left(\widetilde{\theta}_A g\right) - p^{(k+k_A+2)-1}\varepsilon\chi_A(p)a_{p^{\alpha-1}}\left(\widetilde{\theta}_A g\right) \pmod{\mathfrak{L}},$$

and the form $\widetilde{\theta}_A g$ is thus a normalised eigenform modulo $\mathfrak{L}$. ∎

Remark 12.3. *When ℓ does not divide N, the reduction of A modulo $\mathfrak{L}$ is the so-called Katz' Hasse invariant.*

The rest of this paragraph is devoted to construct, for each level N and place $\mathfrak{L}$, a form A that satisfies the hypotheses of lemma 12.2. Among all possible forms, the ones presented in table 12.1 are those we found with the smallest weight. Notice that if we have a form A of level M satisfying the hypotheses of lemma 12.2 for a given place $\mathfrak{L}$, this form also satisfies the hypotheses of lemma 12.2 at the multiple-of-M levels. We will use this fact to consider the smallest set of level possible. We divide our study in three parts: first the places $\mathfrak{L}$ of residue characteristic $\ell \geqslant 5$, then $\ell = 2$, and finally $\ell = 3$.

12.1.1 Theta operators in characteristic greater than 3

The following proposition was already known to Swinnerton-Dyer in [Swi73, Theorem 2].

Proposition 12.4. *Assume $\ell \geqslant 5$. The form $A := -2\ell E_{\ell-1} \in \mathrm{M}_{\ell-1}(1, \mathbb{1})$ satisfies the hypotheses of lemma 12.2 for any level N.*

Proof. Since $\ell \geqslant 5$, A is well-defined and the constant coefficient of A is equal to $\frac{\ell B_{\ell-1,\mathbb{1}}}{\ell-1}$. From proposition 11.5, it is $\mathfrak{L}$-integral and congruent to 1 modulo $\mathfrak{L}$. Moreover, because $E_{\ell-1}$ has integral coefficients except for the constant one, it follows that A and $-\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral Fourier coefficients and that $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. We finally check the condition on the character of A. We have $\overline{\chi}_\ell^{-k_A} = \overline{\chi}_\ell^{1-\ell} \equiv \mathbb{1} \pmod{\mathfrak{L}}$. ∎

If the level N is divisible by ℓ, the situation is in fact much more pleasant for us, in the sense that we can find a form with $k_A = 1$. We find a record of the following fact in [Rib94, (2.1) Theorem].

Proposition 12.5. *Assume $\ell \geqslant 5$ and $\ell \mid N$. Let $\chi_{\mathfrak{L}}$ be the Teichmüller lift of $\overline{\chi}_\ell$ with respect to the place $\mathfrak{L}$, viewed as a primitive Dirichlet character of modulus ℓ. The form $A := 2\ell E_1^{\mathbb{1},\chi_{\mathfrak{L}}^{-1}} \in \mathrm{M}_1(\ell, \chi_{\mathfrak{L}}^{-1})$ satisfies the hypotheses of lemma 12.2.*

Proof. The form A is well-defined because $\chi_{\mathfrak{L}}^{-1}$ is an odd character. Indeed, we have $\chi_{\mathfrak{L}}^{-1}(-1) \equiv \overline{\chi}_\ell^{-1}(-1) \equiv -1 \pmod{\mathfrak{L}}$, and because ℓ is odd, this lifts to $\chi_{\mathfrak{L}}^{-1}(-1) = -1$. From proposition 11.3 and (11.1), the constant term of A is equal to

$$-\ell B_{1,\chi_{\mathfrak{L}}^{-1}} = -\sum_{i=1}^{\ell-1} i\chi_{\mathfrak{L}}^{-1}(i),$$

which is $\mathfrak{L}$-integral. Therefore, because $\chi_{\mathfrak{L}}$ induces the identity modulo $\mathfrak{L}$, this coefficient is congruent to 1 modulo $\mathfrak{L}$, and because $E_1^{\mathbb{1},\chi_{\mathfrak{L}}^{-1}}$ has integral coefficients away from the constant one, A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral Fourier coefficients and we get $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, by definition we have $\overline{\chi}_\ell^{-k_A} = \overline{\chi}_\ell^{-1} \equiv \chi_A \pmod{\mathfrak{L}}$. Thus, A satisfies the hypotheses of lemma 12.2. ∎

This finishes the case $\ell \geqslant 5$. For $\ell \leqslant 3$, the two previous constructions do not always give well-defined modular forms. We present in the next two paragraphs specific constructions in the cases $\ell = 2$ and $\ell = 3$.

12.1.2 Theta operators in characteristic 2

For $\ell = 2$, the most favourable case is when $4 \mid N$. The following construction is very analogous to the one of proposition 12.5.

Proposition 12.6. *Assume $\ell = 2$ and N is divisible by 4. Let χ_4 be the only non-trivial Dirichlet character modulo 4. The form $A := 4E_1^{\mathbb{1},\chi_4} \in \mathrm{M}_1(4, \chi_4)$ satisfies the hypotheses of lemma 12.2.*

Proof. The form A is well-defined because χ_4 is odd. Moreover, from proposition 11.3 and (11.1) the constant coefficient of A is equal to

$$-2B_{1,\chi_4} = -\frac{1}{2}\left(1\chi_4(1) + 3\chi_4(3)\right) = 1.$$

Therefore, because $E_1^{\mathbb{1},\chi_4}$ has integral coefficients away from the constant one, A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral coefficients, $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, it is straightforward that χ_4 is trivial modulo $\mathfrak{L}$, as its reduction is the cyclotomic character modulo 2. ∎

The next favourable case is when N admits at least one odd prime divisor. The following result was inspired by [Mei17, Appendix A.]. As it has never been published, we prove it for the sake of completeness.

Proposition 12.7. *Assume $\ell = 2$ and N has an odd prime divisor. Let p be the least odd prime divisor of N, and let χ_N be a Dirichlet character modulo p of order 2^m, the greatest power of 2 dividing $p-1$. Let ζ be any primitive 2^m-th root of unity. The form $A := (\zeta-1)E_1^{\mathbb{1},\chi_N} \in \mathrm{M}_1(p, \chi_N)$ satisfies the hypotheses of lemma 12.2.*

Proof. First notice that χ_N exists because the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order divisible by 2^m. Let g be an integer which class modulo p generates $(\mathbb{Z}/p\mathbb{Z})^\times$. We claim that we can choose g such that $\chi_N(g) = \zeta$. Indeed, as χ_N has order 2^m, we have $\chi_N(g) = \zeta^k$ with $2 \nmid k$. Let u be an integer such that $ku \equiv 1 \pmod{2^m}$, and $u \equiv 1 \pmod{\frac{p-1}{2^m}}$. We have $\chi_N(g^u) = \zeta^{ku} = \zeta$, and by construction u is prime to $p-1$. Therefore, g^u still generates $(\mathbb{Z}/p\mathbb{Z})^\times$.

Because ζ is a root of unity of order 2^m, we have $\chi_N(-1) = \chi_N(g)^{\frac{p-1}{2}} = \zeta^{\frac{p-1}{2}} = -1$. Therefore, χ_N is odd, A is well-defined, and its constant coefficient is equal to $\frac{1-\zeta}{2}B_{1,\chi_N} = \frac{1-\zeta}{2p}\sum_{a=1}^{p-1} a\chi_N(a)$.

For i between 0 and $2^{m-1}-1$, we have $\chi_N(g^i) = \zeta^i$, and

$$\chi_N(-g^i) = -\zeta^i = \zeta^{i+2^{m-1}} = \chi_N(g^{i+2^{m-1}}).$$

Therefore, the set $\left\{\pm g^i, 0 \leqslant i \leqslant 2^{m-1}-1\right\}$ is a set of representatives of $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{Ker}(\chi_N)$. For an integer x, we write $[x]$ for the only integer between 0 and $p-1$ that is congruent to x modulo p. We then have

$$\begin{aligned}
\frac{1-\zeta}{2}B_{1,\chi_N} &= \frac{1-\zeta}{2p}\sum_{i=0}^{2^{m-1}-1}\sum_{e\in\mathrm{Ker}(\chi_N)}\left(\left[eg^i\right]\chi_N(g^i) + \left[-eg^i\right]\chi_N(-g^i)\right)\\
&= \frac{1-\zeta}{2p}\sum_{i=0}^{2^{m-1}-1}\sum_{e\in\mathrm{Ker}(\chi_N)}\left(\left[eg^i\right]\zeta^i + \left(p-\left[eg^i\right]\right)\left(-\zeta^i\right)\right)\\
&= \frac{1-\zeta}{2p}\sum_{i=0}^{2^{m-1}-1}\zeta^i\left(-p\cdot\#\mathrm{Ker}(\chi_N) + 2\sum_{e\in\mathrm{Ker}(\chi_N)}\left[eg^i\right]\right)\\
&= \frac{1-\zeta}{2p}\times\frac{1-\zeta^{2^{m-1}}}{1-\zeta}\times\left(-p\cdot\frac{p-1}{2^m}\right) + (1-\zeta)\left(\frac{1}{p}\sum_{i=0}^{2^{m-1}-1}\zeta^i\sum_{e\in\mathrm{Ker}(\chi_N)}\left[eg^i\right]\right)\\
&= -\frac{p-1}{2^m} + (1-\zeta)\left(\frac{1}{p}\sum_{i=0}^{2^{m-1}-1}\zeta^i\sum_{e\in\mathrm{Ker}(\chi_N)}\left[eg^i\right]\right).
\end{aligned}$$

The term inside the parentheses is $\mathfrak{L}$-integral and $\frac{p-1}{2^m}$ is an odd integer. Moreover, the only prime ideal above 2 in the ring $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ is $(1-\zeta)\mathbb{Z}[\zeta]$. Therefore, we have $\frac{1-\zeta}{2}B_{1,\chi_N} \equiv 1 \pmod{\mathfrak{L}}$. Because the non-constant Fourier coefficients of $E_1^{\mathbb{1},\chi_N}$ are integral, A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral coefficients, and we get $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, from lemma 10.5, because χ_N has order a power of 2, it is trivial modulo $\mathfrak{L}$ as well as the cyclotomic character modulo 2. This finishes the proof. ∎

Proposition 12.6 gives us a form A for all the levels divisible by 4, and proposition 12.7 gives us a form for all the odd levels. We are thus left with the cases $N = 1$ and $N = 2$. There is no modular form of weight 1 of these levels, so we have to look at bigger weights in order to construct the form A. For level 2, we show that weight 2 suffices.

Proposition 12.8. *Assume that $\ell = 2$ and $N = 2$. Let $\mathbb{1}_{(2)}$ be the trivial character modulo 2. The modular form $A := 24E_2^{\mathbb{1},\mathbb{1}_{(2)}} \in \mathrm{M}_2(2,\mathbb{1}_{(2)})$ satisfies the hypotheses of lemma 12.2.*

Proof. The constant coefficient of A is equal to 1 and $E_2^{\mathbb{1},\mathbb{1}_{(2)}}$ has integral coefficients away from the constant one. Therefore, the forms A and $\frac{1}{k_A}\theta A$ have both $\mathfrak{L}$-integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial modulo $\mathfrak{L}$ as well as the cyclotomic character modulo 2. ■

For $N = 1$, the weight needs to be at least 4, and we have the following result.

Proposition 12.9. *Assume $\ell = 2$ and $N = 1$. The form $A := 240E_4 \in \mathrm{M}_4(1, \mathbb{1})$ satisfies the hypotheses of lemma 12.2.*

Proof. The constant coefficient of A is equal to 1 and the non-constant Fourier coefficients of E_4 are integers. Therefore, A and $\frac{1}{k_A}\theta A$ have integer coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$, and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. The character of A is again trivial, as well as the cyclotomic character modulo 2. ■

12.1.3 Theta operators in characteristic 3

For N divisible by 3, the form of proposition 12.5 is still valid.

Proposition 12.10. *Assume $\ell = 3$ and N is divisible by 3. Let χ_3 be the unique non-trivial Dirichlet character modulo 3. The form $A := 6E_1^{\mathbb{1},\chi_3} \in \mathrm{M}_1(3, \chi_3)$ satisfies the hypotheses of lemma 12.2.*

Proof. We have $\chi_3 \equiv \overline{\chi_\ell}^{-1} \pmod{\mathfrak{L}}$ and the proof is exactly the same as the one of proposition 12.5. ■

For the levels containing a prime divisor congruent to 2 modulo 3, we can still consider an Eisenstein series for the form A.

Proposition 12.11. *Assume $\ell = 3$ and N has a prime divisor congruent to 2 modulo 3. Let p be the least such prime divisor, and let $\mathbb{1}_{(p)}$ be the trivial Dirichlet character modulo p. The form $A := \frac{24}{p-1}E_2^{\mathbb{1},\mathbb{1}_{(p)}} \in \mathrm{M}_2(p, \mathbb{1}_{(p)})$ satisfies the hypotheses of lemma 12.2.*

Proof. The constant coefficient of A is equal to 1. Moreover, $E_2^{\mathbb{1},\mathbb{1}_{(p)}}$ has integral Fourier coefficients away from the constant one. Because p is congruent to 2 modulo 3, $\frac{24}{p-1}$ is 0 modulo $\mathfrak{L}$. Therefore A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial, and we have $\overline{\chi_3}^{-2} \equiv \mathbb{1} \pmod{\mathfrak{L}}$. ■

The remaining cases are the levels containing only prime factors that are congruent to 1 modulo 3. For the levels divisible by a prime p congruent to 4 modulo 9 (that is if 3 divides $p-1$ only once), we found the following construction.

Proposition 12.12. *Assume $\ell = 3$ and N has a prime divisor congruent to 4 modulo 9. Let p be the least such prime divisor of N, and let χ^N be a Dirichlet character modulo p of order 3. The modular form $A := \frac{3}{p-1}\left(E_2^{\mathbb{1},\chi^N} - E_2^{\chi^N,\mathbb{1}}\right) \in \mathrm{M}_2\left(p, \chi^N\right)$ satisfies the hypotheses of lemma 12.2.*

Proof. First notice that χ^N indeed exists as $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ that is divisible by 3. Moreover, because χ^N has order 3, it is trivial modulo $\mathfrak{L}$ and even, and the two Eisenstein series $E_2^{\mathbb{1},\chi^N}$ and $E_2^{\chi^N,\mathbb{1}}$ exist.

The constant coefficient of A is equal to $\frac{3}{4(1-p)}B_{2,\chi^N}$ which is $\mathfrak{L}$-integral by proposition 11.5. We have from proposition 11.3,

$$\begin{aligned}\frac{3}{4(1-p)}B_{2,\chi^N} = \frac{3}{4p(1-p)}\sum_{a=1}^{p-1} a^2\chi^N(a) &\equiv \frac{3}{1-p}\sum_{a=1}^{p-1} a^2 \pmod{\mathfrak{L}}\\ &\equiv \frac{3}{1-p}\frac{p(p-1)(2p-1)}{6} \pmod{\mathfrak{L}}\\ &\equiv 1 \pmod{\mathfrak{L}}.\end{aligned}$$

Therefore, the constant coefficient of A is 1 modulo $\mathfrak{L}$, and because the non-constant Fourier coefficients of $E_2^{\mathbb{1},\chi^N}$ and $E_2^{\chi^N,\mathbb{1}}$ are integral, A and $\frac{1}{k_A}\theta A$ have $\mathfrak{L}$-integral coefficients. The weight k_A is invertible modulo 3, it consequently suffices to prove that $A \equiv 1 \pmod{\mathfrak{L}}$ to conclude.

The forms $E_2^{\mathbb{1},\chi^N}$ and $E_2^{\chi^N,\mathbb{1}}$ are both normalised eigenforms for all the Hecke operators at level p, and have the same weight and character. Thus, it is enough to prove that the congruence $a_r\left(E_2^{\mathbb{1},\chi^N}\right) \equiv a_r\left(E_2^{\chi^N,\mathbb{1}}\right) \pmod{\mathfrak{L}}$ hold for all prime numbers r. This last congruence is straightforward, because we have

$$a_r\left(E_2^{\mathbb{1},\chi^N}\right) = 1 + r\chi^N(r) \equiv \chi^N(r) + r = a_r\left(E_2^{\chi^N,\mathbb{1}}\right) \pmod{\mathfrak{L}}.$$

■

It only remains the levels containing only primes congruent to 1 modulo 9. We found no general way to express the modular form A as form of weight 2. Using computations in PARI/GP, we looked for a modular form of level $p \equiv 1 \pmod 9$ satisfying the hypotheses of lemma 12.2 for p up to 1000. We always find a form except for $p \in \{307, 379, 433, 487, 523, 613, 631, 757, 811, 829, 991\}$, *i.e.* we found 16 forms out of the 27 we were looking for. It can be proved that such a modular form cannot be expressed as a linear combination of forms in the Eisenstein space, meaning that one has necessarily to consider cusp forms to construct A. To fill this gap anyway, we can still consider the modular form $A := 240E_4$ as in the case of proposition 12.9.

Proposition 12.13. *Assume $\ell = 3$, and N contains only prime factors congruent to 1 modulo 9. The modular form $A := 240E_4$ satisfies the hypotheses of lemma 12.2.*

Proof. The constant coefficient of A is equal to 1 and the non-constant Fourier coefficients of E_4 are integral. Therefore, the forms A and $\frac{1}{k_A}\theta A$ have both $\mathfrak{L}$-integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial, and we have $\overline{\chi}_\ell^{-k_A} = \overline{\chi}_\ell^{-4} \equiv \mathbb{1} \pmod{\mathfrak{L}}$. ■

We have compiled in table 12.1 the definition of A depending on ℓ and N. When multiple definitions were possible, we have taken the one with the least weight among all the possible forms. The third column corresponds to the proposition where the properties of the form have been proved. Looking at the various results above, we state the following definition that will be useful in the proofs of the next paragraph.

Table 12.1: Various forms A used to construct the operator $\widetilde{\theta}$

$\ell \geqslant 5$	Form A	Proposition
$\ell \nmid N$	$-2\ell E_{\ell-1}$	12.4
$\ell \mid N$	$2\ell E_1^{\mathbb{1},\chi_{\mathfrak{L}}^{-1}}$	12.5

$\ell = 2$	Form A	Proposition
$4 \mid N$	$4E_1^{\mathbb{1},\chi_4}$	12.6
$N \geqslant 3$ and $4 \nmid N$	$(\zeta - 1)E_1^{\mathbb{1},\chi_N}$	12.7
$N = 2$	$24E_2^{\mathbb{1},\mathbb{1}_{(2)}}$	12.8
$N = 1$	$240E_4$	12.9

$\ell = 3$	Form A	Proposition
$\ell \mid N$	$6E_1^{\mathbb{1},\chi_3}$	12.10
$\ell \nmid N$ and N has a prime factor $q \equiv 2 \pmod 3$	$\frac{24}{p-1}E_2^{\mathbb{1},\mathbb{1}_{(p)}}$	12.11
$\forall d \mid N$, $d \equiv 1 \pmod 3$ and N has a prime factor $p \equiv 4 \pmod 9$	$\frac{3}{p-1}\left(E_2^{\mathbb{1},\chi^N} - E_2^{\chi^N,\mathbb{1}}\right)$	12.12
$\forall p \mid N$, $p \equiv 1 \pmod 9$	$240E_4$	12.13

Definition 12.14. *We say a pair (ℓ, N) is bad, if we have one of the following.*

- *$\ell = 2$ and $N = 1$;*
- *$\ell = 3$ and all the prime factors of N are congruent to 1 modulo 9.*

Remark 12.15. *When (ℓ, N) is bad, the modular form $-504E_6$ is also congruent to 1 modulo $\mathfrak{L}$. Its weight is greater than the one of table 12.1, but we will have to use it in the proof of proposition 12.17 in the next section.*

12.2 Sturm bounds

A Sturm bound for a space of modular forms is an upper bound on the number of leading coefficients that characterise a form of this space. Equivalently, it is the maximal number of zero leading coefficients that a non-zero form of this space can have. The study of such bounds has first been made by Sturm [Stu87] and was later generalised among others by Murty [Mur97]. The same kind of bounds exist if we look at modular forms modulo a prime ideal – and are in fact the same as the first ones. In the next lemma we give a slight improvement of Murty's result

for modular forms of same weight. We then state a more general result for modular forms of any weight and level.

For all this paragraph, we fix a prime number ℓ and a place $\mathfrak{L}$ of $\overline{\mathbb{Q}}$ above ℓ.

Lemma 12.16. *Let f, g be two modular forms of same weight $k \geqslant 0$, level N_f, N_g and character ε_f, ε_g respectively. Let N be the least common multiple of N_f and N_g. Assume that f and g have both $\mathfrak{L}$-integral Fourier coefficients and that $\varepsilon_f \equiv \varepsilon_g \pmod{\mathfrak{L}}$.*

If $a_n(f) \equiv a_n(g) \pmod{\mathfrak{L}}$ for every integer $n \leqslant \frac{kN}{12} \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$, then $f \equiv g \pmod{\mathfrak{L}}$.

Proof. We follow substantially the proof of Murty of [Mur97, §4]. Write $B := \frac{kN}{12} \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$. Consider $\phi = f - g$ and suppose that the vanishing order modulo $\mathfrak{L}$ at infinity of ϕ is at least equal to B, that is $a_n(\phi) \equiv 0 \pmod{\mathfrak{L}}$ for all $n \leqslant B$. If $\phi = 0$, there is nothing to prove. Otherwise, as explained in [Mur97, §4], for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ there is an element $A_\gamma \in \overline{\mathbb{Q}}^\times$ such that the modular form $A_\gamma \phi|_k \gamma$ has $\mathfrak{L}$-integral coefficients and is not congruent to 0 modulo $\mathfrak{L}$.

We write $m := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right)$ and consider a system of representatives $(\gamma_i)_{1 \leqslant i \leqslant m}$ of right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. We can further assume $\gamma_1 = I_2$, the identity matrix. Also choose a set $(\tau_j)_{1 \leqslant j \leqslant \varphi(N)}$ of representatives of $\Gamma_1(N)$ in $\Gamma_0(N)$ with $\tau_1 = I_2$. We then have,

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^{m} \Gamma_0(N)\gamma_i = \bigcup_{i=1}^{m} \bigcup_{j=1}^{\varphi(N)} \Gamma_1(N)\tau_j\gamma_i.$$

Taking the norm function of ϕ according to this system of representatives, we define

$$F := \left(\prod_{j=1}^{\varphi(N)} \phi|_k \tau_j \gamma_1 \right) \prod_{i=2}^{m} \prod_{j=1}^{\varphi(N)} A_{\tau_j\gamma_i} \phi|_k \tau_j \gamma_i \in \mathrm{M}_{km\varphi(N)}(\mathrm{SL}_2(\mathbb{Z})).$$

For $i = 1$ and j between 1 and $\varphi(N)$, we have

$$\phi|_k \tau_j \gamma_1 = \phi|_k \tau_j = (\varepsilon_f(\tau_j) f - \varepsilon_g(\tau_j) g) \equiv \varepsilon_f(\tau_j)\phi \pmod{\mathfrak{L}}. \tag{12.1}$$

Therefore, the modular forms $\phi|_k \tau_j \gamma_1$ have $\mathfrak{L}$-integral Fourier coefficients and thereby, the form F too, by the construction of the coefficients $A_{\tau_j\gamma_i}$. Moreover, by assumption the vanishing order at infinity of ϕ modulo $\mathfrak{L}$ is at least equal to $\frac{km}{12}$. Therefore, the one of the modular form $\Phi := \prod_{j=1}^{\varphi(N)} \phi|_k \tau_j \gamma_1$ is at least equal to $\frac{km\varphi(N)}{12}$, and the same goes for F. Applying Sturm's theorem for level 1 modular forms [Mur97, Theorem 5], F must vanish modulo $\mathfrak{L}$ and by construction of the coefficients $A_{\tau_j\gamma_i}$, the modular forms $A_{\tau_j\gamma_i}\phi|_k\tau_j\gamma_i$ are non-trivial modulo $\mathfrak{L}$ for $i \neq 1$. Thus Φ – and hence ϕ by (12.1) – must be trivial modulo $\mathfrak{L}$. ∎

The following proposition generalises the previous lemma to modular forms of arbitrary weights and levels. The proof uses extensively the construction of theta operators given in section 12.1. We warn the reader that we will write $0^0 = 1$.

Proposition 12.17. *Let f, g be two modular forms of weight k_f, $k_g \geqslant 0$, level N_f, $N_g \geqslant 1$ and character ε_f, ε_g respectively. Let m_f, m_g be two non-negative integers. Assume that f and g have both $\mathfrak{L}$-integral Fourier coefficients and that $\overline{\chi}_\ell^{k_f+2m_f}\varepsilon_f \equiv \overline{\chi}_\ell^{k_g+2m_g}\varepsilon_g \pmod{\mathfrak{L}}$. Let N be the least common multiple of N_f and N_g, and define*

$$a = \begin{cases} 4 & \text{if } \left| \begin{array}{l} k_f + 2m_f \equiv k_g + 2m_g + 2 \pmod 4, \\ \text{and } (\ell, N) \text{ is bad;} \end{array} \right. \\ 0 & \text{otherwise,} \end{cases}$$

$$b = \begin{cases} 4 & \text{if } \ell = 2 \text{ and } N = 2; \\ 3 & \text{if } \ell \mid N \text{ and } (\ell, N) \neq (2,2); \\ 6 & \text{if } (\ell, N) \text{ is bad;} \\ \ell + 1 & \text{otherwise,} \end{cases}$$

$$\text{and } k = a + \max(k_f + bm_f, k_g + bm_g),$$

where "bad" refers to definition 12.14.

If for every $n \leqslant \frac{Nk}{12} \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$, we have $n^{m_f} a_n(f) \equiv n^{m_g} a_n(g) \pmod{\mathfrak{L}}$, then this holds for all integers $n \geqslant 0$.

Proof. For the whole proof, we write A for the modular form associated with $\mathfrak{L}$ and N constructed in section 12.1. According to table 12.1, it has weight $b-2$ and level N. We write χ_A for the character of A and $B(N,k) := \frac{Nk}{12} \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$.

Assume without loss of generality that $k_f + bm_f \leqslant k_g + bm_g$. We first prove that the proposition is true assuming $b-2$ divides $k_g - k_f + b(m_g - m_f)$, that is if for all non-negative integers $n \leqslant B(N, k_g + bm_g)$ we have $n^{m_f} a_n(f) \equiv n^{m_g} a_n(g) \pmod{\mathfrak{L}}$, then these congruences hold for all non-negative integers n. Applying lemma 12.2 recursively, we have

$$\widetilde{\theta}^{m_f} f \in \mathrm{M}_{k_f + bm_f}(N, \varepsilon_f \chi_A^{m_f}) \quad \text{and} \quad \widetilde{\theta}^{m_g} g \in \mathrm{M}_{k_g + bm_g}(N, \varepsilon_g \chi_A^{m_g}).$$

We cannot apply lemma 12.16 to $\widetilde{\theta}^{m_f} f$ and $\widetilde{\theta}^{m_g} g$ directly since they do not have the same weight. However, the forms $A^{\frac{k_g - k_f + b(m_g - m_f)}{b-2}} \widetilde{\theta}^{m_f} f$ and $\widetilde{\theta}^{m_g} g$ are well-defined modular forms by assumption. They have the same weight $k_g + bm_g$, the same level N, and character $\varepsilon_f \chi_A^{m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}}$ and $\varepsilon_g \chi_A^{m_g}$ respectively. Moreover, from lemma 12.2 again, we have $\chi_A \equiv \overline{\chi}_\ell^{2-b} \pmod{\mathfrak{L}}$. By the assumption on the characters we get

$$\begin{aligned} \varepsilon_f \chi_A^{m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}} &\equiv \varepsilon_f \overline{\chi}_\ell^{-(b-2)\left(m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}\right)} \pmod{\mathfrak{L}} \\ &\equiv \varepsilon_f \overline{\chi}_\ell^{(2-b)m_f - k_g + k_f + b(m_f - m_g)} \pmod{\mathfrak{L}} \\ &\equiv \overline{\chi}_\ell^{k_f + 2m_f} \varepsilon_f \cdot \overline{\chi}_\ell^{-(k_g + bm_g)} \pmod{\mathfrak{L}} \\ &\equiv \overline{\chi}_\ell^{k_g + 2m_g} \varepsilon_g \cdot \overline{\chi}_\ell^{-(k_g + bm_g)} \pmod{\mathfrak{L}} \\ &\equiv \varepsilon_g \chi_A^{m_g} \pmod{\mathfrak{L}}. \end{aligned}$$

Therefore, the assumptions of lemma 12.16 are satisfied for these two modular forms. Since A reduces to 1 modulo $\mathfrak{L}$, we get that if the coefficients of $\widetilde{\theta}^{m_f} f$ and $\widetilde{\theta}^{m_g} g$ are congruent up to the $B(N, k_g + bm_g)$-th one, then $\widetilde{\theta}^{m_f} f$ and $\widetilde{\theta}^{m_g} g$ are congruent modulo $\mathfrak{L}$ by lemma 12.16.

We now look at the hypothesis $b-2 \mid k_g - k_f + b(m_g - m_f)$. We claim that if (ℓ, N) is not bad, then it is always satisfied. We have three cases: (i) $\ell = N = 2$, (ii) $\ell \mid N$ and $(\ell, N) \neq (2,2)$, (iii) $\ell \nmid N$ and (ℓ, N) is not bad.

(i) If $\ell = N = 2$, then $b - 2 = 2$, and $k_f \equiv k_g \equiv 0 \pmod 2$, because the weight of a level 2 modular form is necessarily even. Thus, $k_g - k_f + 4(m_g - m_f)$ is divisible by $b - 2$.

(ii) If $\ell \mid N$, then $b - 2 = 1$ and there is nothing to prove.

(iii) If $\ell \nmid N$ and (ℓ, N) is not bad, we have $b - 2 = \ell - 1$. Because $\ell \nmid N$, ε_f and ε_g are unramified at ℓ. From the assumption $\overline{\chi}_\ell^{k_f+2m_f}\varepsilon_f \equiv \overline{\chi}_\ell^{k_g+2m_g}\varepsilon_g \pmod{\mathfrak{L}}$, we get that $k_g - k_f + 2(m_g - m_f) \equiv 0 \pmod{\ell - 1}$, hence $b - 2 \mid k_g - k_f + b(m_g - m_f)$.

Therefore, when (ℓ, N) is not bad, the proposition is proved because we have $a = 0$ and $k = k_g + bm_g$.

From now on, assume that (ℓ, N) is bad. By definition, we have $b = 6$, and either $(\ell, N) = (2,1)$, or $\ell = 3$ and $\ell \nmid N$. Let us first prove that we have $k_g - k_f + 6(m_g - m_f) \equiv 0 \pmod 2$ (*i.e.* $k_g \equiv k_f \pmod 2$). When $(\ell, N) = (2,1)$, it is true because the weights k_f and k_g are both even. When $\ell = 3$ and $\ell \nmid N$, the hypothesis on the characters again implies that $k_f + 2m_f \equiv k_g + 2m_g \pmod 2$ and the conclusion follows.

If the even number $k_g - k_f + 6(m_g - m_f)$ is divisible by $4 = b - 2$, then by definition we have $a = 0$ and $k = k_g + bm_g$. The result follows as before in this case. Otherwise, we have $4 \mid k_g - k_f + 6(m_g - m_f) - 2$ and $a = 4$. Write $A_4 := 240E_4$ and $A_6 := -504E_6$. We have seen in proposition 12.13 and remark 12.15, that both A_4 and A_6 are congruent to 1 modulo $\mathfrak{L}$. We set

$$f' := A_6 f \quad \text{and} \quad g' = A_4 g.$$

Then f' and g' are modular forms with $\mathfrak{L}$-integral Fourier coefficients of weight $k_{f'} = k_f + 6$, $k_{g'} = k_g + 4$, level N and character ε_f, ε_g respectively. Since $\overline{\chi}_\ell^2$ is trivial for $\ell = 2, 3$, the congruence

$$\overline{\chi}_\ell^{k_{f'}+bm_f}\varepsilon_f \equiv \overline{\chi}_\ell^{k_{g'}+bm_g}\varepsilon_g \pmod{\mathfrak{L}}$$

is satisfied. Moreover, we have $k_{f'} + bm_f \leqslant k_{g'} + bm_g$, and $b-2 = 4$ divides $k_{g'} - k_{f'} + b(m_g - m_f)$. According to the discussion at the beginning of the proof, we therefore get the desired result since f', g' reduce to f, g respectively and $k_{g'} + bm_g = a + k_g + bm_g = k$. ∎

Remark 12.18. *Notice that lemma 12.16 corresponds to the special case $m_f = m_g = 0$ and $k_f = k_g = k$. Moreover, in practice we can always take $m_f \in \{0, 1\}$ and $0 \leqslant m_g \leqslant \ell - 1$.*

In chapter 13 we will mainly deal with eigenforms. It is well-known that the knowledge of the Fourier coefficients of prime index and of the constant coefficient characterises such forms. We can therefore simplify proposition 12.17 and get the following corollary.

Corollary 12.19. *Let f, g be as in proposition 12.17 and define also N and k similarly. Assume further that f and g are normalised eigenforms for the Hecke operators at level N modulo $\mathfrak{L}$ of prime index less than $\frac{Nk}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$ (and different from ℓ if m_f, $m_g \geqslant 1$).*

If $0^{m_f}a_0(f) \equiv 0^{m_g}a_0(g) \pmod{\mathfrak{L}}$ (with $0^0 = 1$) and if for every prime $p \leqslant \frac{Nk}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$ we have $p^{m_f}a_p(f) \equiv p^{m_g}a_p(g) \pmod{\mathfrak{L}}$, then we have $n^{m_f}a_n(f) \equiv n^{m_g}a_n(g) \pmod{\mathfrak{L}}$ for every non-negative integer n.

We finally state a Sturm bound result in characteristic zero that we will be used in the proof of theorem 14.17. It is a well-known result, but we do not find a suitable reference for it. For the sake of completeness we give a proof of it due essentially to Buzzard.

Proposition 12.20. *Let f, g be two modular forms of same weight $k \geqslant 0$, same level N, and same character ε. If $a_n(f) = a_n(g)$ for every integer $n \leqslant \frac{kN}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$, then $f = g$.*

Proof. We reduce to the case of trivial character. Let s be the order of the character ε, and define

$$\phi := (f-g)^s \in \mathrm{M}_{ks}(N, \mathbb{1}).$$

By assumption, the first $s \cdot \frac{Nk}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$ Fourier coefficients of ϕ vanish. Applying [Mur97, Theorem 1], we get $\phi = 0$ and therefore $f = g$. ∎

Remark 12.21. *We can in fact deduce proposition 12.20 from lemma 12.16. Indeed, it is well known that the denominators of the Fourier coefficients of a modular form are bounded. Therefore, we can reduce f and g modulo infinitely many places $\mathfrak{L}$. Applying lemma 12.16, f and g are congruent modulo infinitely many places $\mathfrak{L}$ and are thus equal.*

As in the positive characteristic case, to check the equality of two eigenforms it is enough to check only the coefficients of prime index.

Corollary 12.22. *Let f, g be two modular forms of same weight $k \geqslant 0$, same level N, and same character ε. Assume further that f and g are normalised eigenforms for the Hecke operators T_p^N of prime index less or equal to $\frac{Nk}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$.*

If $a_0(f) = a_0(g)$ and $a_p(f) = a_p(g)$ for every prime $p \leqslant \frac{Nk}{12}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1+\frac{1}{p}\right)$, then $f = g$.

We now give an upper-bound for the product appearing in the Sturm bound. We use a technique of Kraus [Kra95] to get a slightly better bound than the one suggested by Serre in Kraus' article.

Lemma 12.23. *Let n be an integer greater than or equal to 2, we have:*

$$\prod_{\substack{p|n\\ p \text{ prime}}}\left(1+\frac{1}{p}\right) \leqslant 2\log\log(n) + 2.4.$$

Proof. We first split the product in two parts: $\prod_{\substack{p|n \\ p \text{ prime}}} \left(1+\frac{1}{p}\right) = P(n)Q(n)$ with

$$P(n) = \prod_{\substack{p|n \\ p>\log n}} \left(1+\frac{1}{p}\right) \quad \text{and} \quad Q(n) = \prod_{\substack{p|n \\ p\leqslant \log n}} \left(1+\frac{1}{p}\right).$$

Let m be the number of primes p dividing n and being greater than $\log n$. As $n \geqslant \log(n)^m$, we get $m \leqslant \frac{\log n}{\log\log n}$. Thus,

$$P(n) \leqslant \exp\left(\frac{\log n}{\log\log n}\log\left(1+\frac{1}{\log n}\right)\right) \leqslant \exp\left(\frac{1}{\log\log n}\right). \tag{12.2}$$

Applying [RS62, (3.27)], we get an upper bound for Q:

$$Q(n) \leqslant \prod_{p\leqslant \log n}\left(1-\frac{1}{p}\right)^{-1} < e^{\gamma}\log\log(n)\left(1-\frac{1}{(\log\log n)^2}\right)^{-1}, \tag{12.3}$$

where γ is the Euler-Mascheroni constant. Putting (12.2) and (12.3) together we have

$$\prod_{\substack{p|n \\ p \text{ prime}}}\left(1+\frac{1}{p}\right) \leqslant e^{\gamma}\log\log(n)\exp\left(\frac{1}{\log\log n}\right)\left(1-\frac{1}{(\log\log n)^2}\right)^{-1}.$$

The function $x \mapsto e^{\gamma+x}(1-x^2)^{-1}$ is bounded by 2 for $x \in [0, 0.1]$. Therefore, the lemma holds for all integers $n \geqslant \exp(\exp(10))$. For n between 2 and $\exp\exp(10)$, we first notice that it is enough to deal with square-free integers. Then, among the square-free integers having k prime factors, it suffices to only check the lemma for $n_k = \prod_{i=1}^{k} p_i$, p_i being the i-th prime number, as it is for this value of n that the left hand side product is the biggest and the right-hand side the smallest. The greatest k such that $n_k \leqslant \exp\exp(10)$ is 2486, and we have checked the lemma with a computer for all those n_k. ∎

12.3 Modifying modular forms

In this paragraph we discuss a way to construct from a given eigenform, another eigenform with slightly different Fourier coefficients but with a bigger level. It will be crucial in chapters 13 and 14.

Let $\mathcal{O}(\mathcal{H})$ be the space of holomorphic functions on the complex upper-half plane. For an integer $n \geqslant 1$ and a complex number b, we define two operators V_n and $S_n(b)$ on $\mathcal{O}(\mathcal{H})$ by

$$V_n : \left\{\begin{array}{ccc} \mathcal{O}(\mathcal{H}) & \longrightarrow & \mathcal{O}(\mathcal{H}) \\ h & \longmapsto & (z \mapsto h(nz)) \end{array}\right. \quad \text{and} \quad S_n(b) : \left\{\begin{array}{ccc} \mathcal{O}(\mathcal{H}) & \longrightarrow & \mathcal{O}(\mathcal{H}) \\ h & \longmapsto & h - bV_nh \end{array}\right..$$

For a prime number p, we denote by U_p the operator which action on Fourier expansions is given by

$$U_p\left(\sum_{n=0}^{\infty} a_n q^n\right) := \sum_{n=0}^{\infty} a_{np} q^n.$$

We recall the following facts about the operators U_p and V_p: for any primes p and r, the operators V_p and V_r commute and the image of $\mathrm{M}_k(M,\varepsilon)$ by V_p is $\mathrm{M}_k(Mp,\varepsilon)$. Letting V_p act on q-expansions, it commutes with U_r for $r \neq p$ and satisfies $U_pV_p = \mathrm{Id}$. Moreover, T_p^M decomposes on the space $\mathrm{M}_k(M,\varepsilon)$ as

$$T_p^M = U_p + p^{k-1}\varepsilon(p)V_p.$$

We therefore have the following lemma for eigenforms of T_p^M.

Lemma 12.24. *Let M' be a multiple of M and assume either that $p \mid M$, or that $p \nmid M'$. On q-expansions, the actions of T_p^M and $T_p^{M'}$ are the same. Therefore, if $f \in M_k(M,\varepsilon)$ is an eigenform for T_p^M, then, seeing f in level M', it is also an eigenform for $T_p^{M'}$.*

From now on, consider a modular form g of weight $k \geqslant 1$, level $M \geqslant 1$, and character ε that is a normalised eigenform for all the Hecke operators at level M. For any prime number p, we denote by α_p, β_p the roots of the Hecke polynomial $X^2 - a_p(g)X + p^{k-1}\varepsilon(p)$.

Lemma 12.25. *Let p be a prime number and let $b \in \{\alpha_p, \beta_p\}$. The function $S_p(b)g$ is a modular form of same weight and character as g and of level Mp^{n_p} with*

$$n_p = \begin{cases} 1 & \text{if } b \neq 0; \\ 0 & \text{if } b = 0. \end{cases}$$

It is a normalised eigenform for all the Hecke operators at level Mp^{n_p}, and for any prime r we have

$$a_r\left(S_p(b)g\right) = \begin{cases} a_r(g) & \text{if } r \neq p; \\ a_p(g) - b & \text{if } r = p. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R, then those of $S_p(b)g$ lie in the ring $R[b]$.

Proof. If $b = 0$, then there is nothing to prove as $S_p(0)g = g$. Assume $b \neq 0$. Because both g and V_pg are modular forms of weight k, level Mp, and character ε, it is also the case for $S_p(b)g$. Let us compute the action of the Hecke operators at level Mp on $S_p(b)g$.

Let r be a prime number different from p. From lemma 12.24, $T_r^{Mp}g$ and T_r^Mg are equal. Thus, because the operators V_p and T_r^M commute, we have

$$T_r^{Mp}S_p(b)g = T_r^Mg - bV_pT_r^Mg = a_r(g)g - ba_r(g)V_pg = a_r(g)S_p(b)g.$$

For $r = p$, we have $T_p^{Mp}g = U_pg = T_p^Mg - p^{k-1}\varepsilon(p)V_pg = a_p(g)g - p^{k-1}\varepsilon(p)V_pg$. It gives

$$T_p^{Mp}S_p(b)g = \left(a_p(g)g - p^{k-1}\varepsilon(p)V_pg\right) - bU_pV_pg = \left(a_p(g) - b\right)g - p^{k-1}\varepsilon(p)V_pg.$$

As b is a root of $X^2 - a_p(g)X + p^{k-1}\varepsilon(p)$, it satisfies $b(a_p(g) - b) = p^{k-1}\varepsilon(p)$. We finally get

$$T_p^{Mp}S_p(b)g = \left(a_p(g) - b\right)g - \left(a_p(g) - b\right)bV_pg = \left(a_p(g) - b\right)S_p(b)g.$$

The form $S_p(b)g$ is thus a normalised eigenform for the all Hecke operators at level Mp. The fact about the ring of Fourier coefficients of $S_p(b)g$ is straightforward. ∎

We now apply this result to construct from the eigenform g, an eigenform which p-th Fourier coefficient is a chosen number b in $\{\alpha_p, \beta_p, 0\}$.

Proposition 12.26. *Let p be a prime number and let $b \in \{\alpha_p, \beta_p, 0\}$. Define*

$$\begin{cases} g_p^b = g & \text{and } n_p = 0, \quad \text{if } b = a_p(g); \\ g_p^b = S_p(a_p(g) - b)g & \text{and } n_p = 1, \quad \text{if } b \neq a_p(g) \text{ and } b \in \{\alpha_p, \beta_p\}; \\ g_p^b = S_p(\alpha_p) \circ S_p(\beta_p)g & \text{and } n_p = 2, \quad \text{if } b \neq a_p(g) \text{ and } b \notin \{\alpha_p, \beta_p\}. \end{cases}$$

Then, g_p^b is a modular form of same weight and character as g and of level Mp^{n_p}. It is a normalised eigenform for all the Hecke operators at level Mp^{n_p}, and for any prime r we have

$$a_r\left(g_p^b\right) = \begin{cases} a_r(g) & \text{if } r \neq p; \\ b & \text{if } r = p. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R, then those of g_p^b lie in the ring $R[b]$.

Proof. In the first two cases, we have $g_p^b = S_p(a_p(g) - b)g$ and lemma 12.25 gives directly the result. In the third case, we necessarily have $b = 0$ and α_p, β_p non-zero. From lemma 12.25 applied to g and β_p, the p-th Hecke polynomial of $S_p(\beta_p)g$ is $X^2 - \alpha_p X$, of which α_p is a root. We can then apply lemma 12.25 to $S_p(\beta_p)g$ and α_p to conclude. Finally, the calculation

$$\begin{aligned} S_p(\alpha_p) \circ S_p(\beta_p)g &= (g - \beta_p V_p g) - \alpha_p V_p (g - \beta_p V_p g) \\ &= g - (\alpha_p + \beta_p)V_p g + \alpha_p \beta_p V_p^2 g \\ &= g - a_p(g)V_p g + p^{k-1}\varepsilon(p)V_p^2 g, \end{aligned}$$

proves that the Fourier coefficients of g_p^b lie in the same ring as g, because the values of the character of an eigenform always lie in the ring spanned by its Fourier coefficients (see [Rib77, Corollary (3.1)]). ∎

Remark 12.27. *The form g_p^b reads "the modular form g which p-th Fourier coefficient has been changed to the number b".*

Remark 12.28. *Notice that the modular form g_p^b is always of the shape $P(V_p)g$ with $P = 1 - \varepsilon_p X + \delta_p X^2$ and $(\varepsilon_p, \delta_p) \in \{(\alpha_p, 0), (\beta_p, 0), (a_p(g), p^{k-1}\varepsilon(p))\}$.*

For any prime number p and $b_p \in \{0, \alpha_p, \beta_p\}$, define

$$S_p^{b_p} = \begin{cases} \mathrm{Id} & \text{if } b_p = a_p(g); \\ \mathrm{Id} - (a_p(g) - b_p)V_p & \text{if } b_p \neq a_p(g) \text{ and } b_p \in \{\alpha_p, \beta_p\}; \\ \mathrm{Id} - a_p(g)V_p + p^{k-1}\varepsilon(p)V_p^2 & \text{if } b_p \neq a_p(g) \text{ and } b_p \notin \{\alpha_p, \beta_p\}, \end{cases}$$

so that we have $g_p^{b_p} = S_p^{b_p} g$. By proposition 12.26, applying $S_p^{b_p}$ to g only modifies the Fourier coefficients of index divisible by p. Moreover, it gives us a modular form that is still a normalised eigenform for the whole Hecke algebra at its level. It means that for another prime r and $b_r \in \{0, \alpha_r, \beta_r\}$, the modular forms $\left(g_p^{b_p}\right)_r^{b_r}$ and $\left(g_r^{b_r}\right)_p^{b_p}$ are well-defined and equal to $S_p^{b_p} S_r^{b_r} g = S_r^{b_r} S_p^{b_p} g$.

For any finite set of primes $\mathbf{P}$ and any $\mathbf{b} \in \prod_{p\in\mathbf{P}} \{0, \alpha_p, \beta_p\}$, we define

$$g_{\mathbf{P}}^{\mathbf{b}} := \prod_{p\in\mathbf{P}} S_p^{b_p} g.$$

With the notations of proposition 12.26, we deduce the following result.

Corollary 12.29. *The function $g_{\mathbf{P}}^{\mathbf{b}}$ is a modular form of same weight and character as g and of level $M\prod_{p\in\mathbf{P}} p^{n_p}$. It is a normalised eigenform for all the Hecke operators at level $M\prod_{p\in\mathbf{P}} p^{n_p}$, and for any prime r we have*

$$a_r\left(g_{\mathbf{P}}^{\mathbf{b}}\right) = \begin{cases} a_r(g) & \text{if } r \notin \mathbf{P}; \\ b_r & \text{if } r \in \mathbf{P}. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R, then those of $g_{\mathbf{P}}^{\mathbf{b}}$ lie in the ring $R[\mathbf{b}]$.

Since the beginning of this section, our results were about "true" modular forms. There is another function that we can modify with the operator $S_p(b)$ and get a modular form: the Eisenstein series E_2.

Proposition 12.30. *Let p be any prime number and $b \in \{1, 0\}$. Define*

$$\begin{cases} (E_2)_p^b = S_p(p)E_2 & \text{and } n_p = 1 \quad \text{if } b = 1; \\ (E_2)_p^b = S_p(1) \circ S_p(p)E_2 & \text{and } n_p = 2 \quad \text{if } b = 0. \end{cases}$$

The function $(E_2)_p^b$ is a modular form of weight 2, level p^{n_p}, and trivial character. It is a normalised eigenform for all the Hecke operators at level p^{n_p}, and for any prime r we have

$$a_r\left((E_2)_p^b\right) = \begin{cases} r+1 & \text{if } r \neq p; \\ b & \text{if } r = p. \end{cases}$$

Moreover, all the Fourier coefficients of $(E_2)_p^b$ are integers, except maybe the constant one that is rational.

Proof. An easy computation shows that for any prime p, we have $S_p(p)E_2 = E_2^{\mathbb{1},\mathbb{1}_{(p)}}$. In particular, the form $S_p(p)E_2 = S_p(a_p(E_2) - 1)E_2$ is a normalised eigenform of weight 2, level p, trivial character, and for any prime r, its r-th Fourier coefficient is equal to $r + 1 = a_r(E_2)$ if $r \neq p$, and 1 if $r = p$. Moreover, the Hecke polynomial at p of $E_2^{\mathbb{1},\mathbb{1}_{(p)}}$ is $X(X - 1)$. Thus, $S_p(1)E_2^{\mathbb{1},\mathbb{1}_{(p)}} = S_p(1) \circ S_p(p)E_2$ is a normalised eigenform of weight 2, trivial character and level p^2 and we have $a_p(S_p(1) \circ S_p(p)E_2) = 0$. ∎

We can then state a result of the shape of corollary 12.29 for E_2.

Corollary 12.31. *Let $\mathbf{P}$ be a finite set of primes and let $\mathbf{b} \in \prod_{p\in\mathbf{P}} \{0, 1, p\} \setminus (p)_{p\in\mathbf{P}}$. There is a modular form $(E_2)_{\mathbf{P}}^{\mathbf{b}}$ of weight 2, level $\prod_{p\in\mathbf{P}} p^{n_p}$, and trivial character. It is a normalised eigenform for all the Hecke operators at its level, and for any prime number r we have*

$$a_r\left((E_2)_{\mathbf{P}}^{\mathbf{b}}\right) = \begin{cases} r+1 & \text{if } r \notin \mathbf{P}; \\ b_r & \text{if } r \in \mathbf{P}. \end{cases}$$

Moreover, all the Fourier coefficients of $(E_2)_{\mathbf{P}}^{\mathbf{b}}$ *are integers, except maybe the constant one that is rational.*

We finally give a result on the constant coefficient of an Eisenstein series that has been modified with corollary 12.29.

Proposition 12.32. *Let* $k \geqslant 2$*, let* ε_1*,* ε_2 *be two primitive Dirichlet characters. Let* $\mathbf{P}$ *be a finite set of prime numbers and let* $\mathbf{b} := (b_p) \in \prod_{p\in\mathbf{P}} \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$*, different from* $(1)_{p\in\mathbf{P}}$ *if* $(k, \varepsilon_1, \varepsilon_2) = (2, \mathbb{1}, \mathbb{1})$*. Then the constant coefficient of* $\left(E_k^{\varepsilon_1,\varepsilon_2}\right)_{\mathbf{P}}^{\mathbf{b}}$ *is equal to*

$$\begin{cases} 0 & \text{if } \varepsilon_1 \neq \mathbb{1}; \\ -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p\in\mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)) & \text{if } \varepsilon_1 = \mathbb{1}. \end{cases}$$

Proof. First, if $\varepsilon_1 \neq \mathbb{1}$, then the constant coefficient of $E_k^{\varepsilon_1,\varepsilon_2}$ is trivial by (11.1). Assume $\varepsilon_1 = \mathbb{1}$. Then the modular form $\left(E_k^{\varepsilon_1,\varepsilon_2}\right)_{\mathbf{P}}^{\mathbf{b}}$ is equal to

$$\prod_{p\in\mathbf{P}} \left(\mathrm{Id} - \varepsilon_p V_p + \delta_p V_p^2\right) E_k^{\varepsilon_1,\varepsilon_2},$$

where

$$(\varepsilon_p, \delta_p) = \begin{cases} (1 + p^{k-1}\varepsilon_2(p), p^{k-1}\varepsilon_2(p)) & \text{if } b_p = 0; \\ (1, 0) & \text{if } b_p = p^{k-1}\varepsilon_2(p); \\ (p^{k-1}\varepsilon_2(p), 0) & \text{if } b_p = 1. \end{cases} \tag{12.4}$$

Therefore, the constant coefficient is equal to $-\frac{B_{k,\varepsilon_2}}{2k} \prod_{p\in\mathbf{P}} (1 - \varepsilon_p + \delta_p)$. A straightforward computation gives that $1 - \varepsilon_p + \delta_p$ is equal to 0 if $b_p \in \{0, p^{k-1}\varepsilon_2(p)\}$, and to $1 - p^{k-1}\varepsilon_2(p)$ if $b_p = 1$. Therefore, if one of the b_p's is equal to 0 or $p^{k-1}\varepsilon_2(p)$, then the constant coefficient is equal to

$$0 = -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p\in\mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)).$$

Else, if all the b_p's are equal to 1, then the constant coefficient is equal to

$$-\frac{B_{k,\varepsilon_2}}{2k} \prod_{p\in\mathbf{P}} (1 - p^{k-1}\varepsilon_2(p)) = -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p\in\mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)).$$

■

Proposition 12.33. *Let* k*,* ε_1*,* ε_2*,* $\mathbf{P}$ *and* $\mathbf{b}$ *be as in proposition 12.32. Let* $\mathfrak{c}_1$*,* $\mathfrak{c}_2$ *be the conductors of* ε_1 *and* ε_2 *respectively. Then the constant coefficient of* $\left(E_k^{\varepsilon_1,\varepsilon_2}\right)_{\mathbf{P}}^{\mathbf{b}}$ *at the cusp* $\frac{1}{\mathfrak{c}_2}$ *is equal to*

$$-\varepsilon_1(-1)\frac{W((\varepsilon_1\varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})}\frac{B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}}{2k}\left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0}\right)^k \prod_{p\mid\mathfrak{c}_1\mathfrak{c}_2}\left(1 - \frac{(\varepsilon_1\varepsilon_2^{-1})_0(p)}{p^k}\right)$$
$$\times \prod_{b_p\neq\varepsilon_1(p)}\left(1 - \frac{\varepsilon_1\varepsilon_2^{-1}(p)}{p^k}\right) \prod_{b_p\neq p^{k-1}\varepsilon_2(p)}\left(1 - \frac{1}{p}\right).$$

Proof. Let $\gamma := \begin{pmatrix} 1 & 0 \\ \mathfrak{c}_2 & 1 \end{pmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\infty = \frac{1}{\mathfrak{c}_2}$. Write the modular form $\left(E_k^{\varepsilon_1,\varepsilon_2}\right)_{\mathbf{P}}^{\mathbf{b}}$ as

$$\prod_{p\in\mathbf{P}} \left(\mathrm{Id} - \varepsilon_p V_p + \delta_p V_p^2\right) E_k^{\varepsilon_1,\varepsilon_2},$$

with ε_p and δ_p defined by (12.4). By proposition 11.9, for an integer M, the constant coefficient of $\left(V_M E_k^{\varepsilon_1,\varepsilon_2}\right)|_k\gamma$ is non-zero if and only if M and $\mathfrak{c}_2$ are coprime. Under this assumption, we have, with the notations of proposition 11.9,

$$\Upsilon_k^{\varepsilon_1,\varepsilon_2}(\gamma, M) = \frac{\varepsilon_2^{-1}(M)}{M^k}\left[-\varepsilon_1(-1)\frac{W((\varepsilon_1\varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})}\frac{B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}}{2k} \times \left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0}\right)^k \prod_{p\mid \mathfrak{c}_1\mathfrak{c}_2}\left(1 - \frac{(\varepsilon_1\varepsilon_2^{-1})_0(p)}{p^k}\right)\right]. \tag{12.5}$$

The expression in brackets is independent of M, let us write it $\mathbf{D}$. Notice that if M is not coprime to $\mathfrak{c}_2$, the formula still holds, as $\varepsilon_2(M) = 0$. Define

$$P := \prod_{p\in\mathbf{P}} \left(1 - \varepsilon_p X_p + \delta_p X_p^2\right) \in \mathbb{C}\left[(X_p)_{p\in\mathbf{P}}\right].$$

As (12.5) is fully multiplicative in M, the constant coefficient of $\left(E_k^{\varepsilon_1,\varepsilon_2}\right)_{\mathbf{P}}^{\mathbf{b}}$ is then equal to

$$\lim_{\mathrm{Im}(z)\to+\infty} P((V_p)_{p\in\mathbf{P}})E_k^{\varepsilon_1,\varepsilon_2}|_k\gamma(z) = \mathbf{D}\cdot P\left(\left(\frac{\varepsilon_2^{-1}(p)}{p^k}\right)_{p\in\mathbf{P}}\right).$$

We just have to compute the value of $P\left(\left(\frac{\varepsilon_2^{-1}(p)}{p^k}\right)_{p\in\mathbf{P}}\right)$ to conclude. Let $P_p(X_p) = 1-\varepsilon_p X_p+\delta_p X_p^2$, so that we have $P = \prod_{p\in\mathbf{P}} P_p(X_p)$. A straightforward calculation shows that the value of $P_p\left(\frac{\varepsilon_2^{-1}(p)}{p^k}\right)$ is

$$\begin{cases} \left(1 - \frac{\varepsilon_1\varepsilon_2^{-1}(p)}{p^k}\right)\left(1 - \frac{1}{p}\right) & \text{if } (\varepsilon_p,\delta_p) = (\varepsilon_1(p) + p^{k-1}\varepsilon_2(p), p^{k-1}\varepsilon_1\varepsilon_2(p)); \\ 1 - \frac{\varepsilon_1\varepsilon_2^{-1}(p)}{p^k} & \text{if } (\varepsilon_p,\delta_p) = (\varepsilon_1(p), 0); \\ 1 - \frac{1}{p} & \text{if } (\varepsilon_p,\delta_p) = (p^{k-1}\varepsilon_2(p), 0). \end{cases}$$

■

Chapter 13

Reducible modular representations

13.1 General study of reducible representations

Let $f = q + \sum_{n=2}^{\infty} a_n(f) q^n$ be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε of conductor $\mathfrak{c}$. Let K_f be the number field generated by $(a_n(f))_{n \geqslant 2}$ and let λ be a prime ideal of the ring of integers of K_f above a prime number ℓ. Our goal is to characterise the fact that $\overline{\rho}_{f,\lambda}$ is reducible by a finite set of congruences. We begin by looking at the possible factors that can appear in the reduction of $\overline{\rho}_{f,\lambda}$. The set we define in the following corresponds these possible pairs of factors (see the upcoming proposition 13.2).

Definition 13.1. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. Define the set $R_{N,k,\varepsilon}(\mathfrak{L})$ as the set of quadruples $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ consisting of two Dirichlet characters ε_1, ε_2 of prime-to-ℓ order and unramified at ℓ, and of two integers m_1, m_2 satisfying*

1. $0 \leqslant m_1 \leqslant m_2 \leqslant \ell - 2$;
2. $\overline{\chi}_\ell^{m_1+m_2} \overline{\varepsilon_1 \varepsilon_2} = \overline{\chi}_\ell^{k-1} \overline{\varepsilon}$;
3. *For every prime $p \neq \ell$, $v_p\left(\frac{N}{\mathfrak{c}_1 \mathfrak{c}_2}\right) \in \{0, 1, 2\}$,*

where $\bar{\cdot}$ denotes the reduction modulo $\mathfrak{L}$, and $\mathfrak{c}_i$ is the conductor of ε_i, and up to the equivalence relation $(\varepsilon_1, \varepsilon_2, m, m) \sim (\varepsilon_2, \varepsilon_1, m, m)$.

In particular if $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, then $\mathfrak{c}_1 \mathfrak{c}_2 \mid N$. The set $R_{N,k,\varepsilon}(\mathfrak{L})$ is therefore finite.

Proposition 13.2. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ extending λ. The representation $\overline{\rho}_{f,\lambda}$ is reducible if and only if there exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon_2}$, where $\overline{\varepsilon_i}$ denotes the reduction of ε_i modulo $\mathfrak{L}$.*

Proof. The representation $\overline{\rho}_{f,\lambda}$ is semi-simple and odd. Therefore, it is reducible if and only if there exist two characters $\eta_i : G_{\mathbb{Q}} \to \mathbb{F}_\lambda^\times$ such that

$$\overline{\rho}_{f,\lambda} \cong \eta_1 \oplus \eta_2.$$

Using section 10.2.2 to lift η_i with respect to the place $\mathfrak{L}$, we can write it $\eta_i = \overline{\chi}_\ell^{m_i}\overline{\varepsilon_i}$, with $0 \leqslant m_i \leqslant \ell - 2$ and ε_i a primitive Dirichlet character of conductor $\mathfrak{c}_i$ not divisible by ℓ, and of prime-to-ℓ order. Without loss of generality we can assume that $m_1 \leqslant m_2$. Looking at the determinant of $\overline{\rho}_{f,\lambda}$ we get

$$\overline{\chi}_\ell^{k-1}\overline{\varepsilon} = \overline{\chi}_\ell^{m_1+m_2}\overline{\varepsilon_1\varepsilon_2}.$$

Moreover, by propositions 10.4 and 10.6 the Artin conductor of $\overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$ is equal to $\mathfrak{c}_1\mathfrak{c}_2$. By proposition 10.12, we necessarily have $v_p\left(\frac{N}{\mathfrak{c}_1\mathfrak{c}_2}\right) \in \{0,1,2\}$ for all primes $p \nmid N$, $p \neq \ell$. ∎

Remark 13.3. *We consider $(\varepsilon_1, \varepsilon_2, m, m)$ to be equivalent to $(\varepsilon_2, \varepsilon_1, m, m)$ in $R_{n,k,\varepsilon}(\mathfrak{L})$ because these two quadruplets leads to the same representation $\overline{\chi}_\ell^m \otimes (\overline{\varepsilon_1} \oplus \overline{\varepsilon_2}) \cong \overline{\chi}_\ell^m \otimes (\overline{\varepsilon_2} \oplus \overline{\varepsilon_1})$.*

Remark 13.4. *We will see later that the set $R_{N,k,\varepsilon}(\mathfrak{L})$ depends in fact only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$ (and obviously on N, k and ε). For now, this dependency will not matter, and we postpone this proof to section 13.3.*

Now that the possible shape of the reduction of $\overline{\rho}_{f,\lambda}$ is parametrise by a finite set, we need to translate the isomorphism $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$ by a system of congruences between two modular forms. The following result is the key step in this direction. It uses in a crucial way the local description of $\overline{\rho}_{f,\lambda}$ at the bad prime numbers (see section 10.3).

Lemma 13.5. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. If the representation $\overline{\rho}_{f,\lambda}$ is reducible, then there exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that for any prime number $p \neq \ell$, we have*

$$a_p(f) \equiv \begin{cases} p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}} & \text{if } p \nmid N; \\ p^{m_1}b_p \pmod{\mathfrak{L}} & \text{if } p \mid N, \end{cases} \tag{13.1}$$

for some $b_p \in \{0, \varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.

Conversely, if for some $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, those congruences hold for every prime p in a set of density 1, then we have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$.

Proof. Let us prove the second statement first. Write $\overline{\rho} := \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$. By construction, the determinants of $\overline{\rho}_{f,\lambda}$ and $\overline{\rho}$ agree. Moreover, by assumption for any prime number $p \nmid N\ell$ in a set of density 1, we have

$$\operatorname{Tr}\left(\overline{\rho}_{f,\lambda}(\operatorname{Frob}_p)\right) \equiv a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \equiv \operatorname{Tr}\left(\overline{\rho}(\operatorname{Frob}_p)\right) \pmod{\mathfrak{L}}.$$

By corollary 10.3, $\overline{\rho}_{f,\lambda}$ must be isomorphic to $\overline{\rho}$ and is thus reducible.

We now prove the first statement. Assume $\overline{\rho}_{f,\lambda}$ to be reducible. Proposition 13.2 gives us the existence of $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, such that $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$. For any prime $p \nmid N\ell$, taking the trace at a Frobenius at p gives the congruence

$$a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}.$$

Let us now consider a prime $p \mid N$ and different from ℓ. We treat 3 cases separately:

(i) If $v_p(N) \geqslant 2$ and $v_p(N) > v_p(\mathfrak{c})$, we know from proposition 10.16 that $a_p(f) = 0$. Hence, we have $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$ with $b_p = 0$.

(ii) If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then by proposition 10.17 the local representation $\overline{\rho}_{f,\lambda}|_{G_p}$ upper-triangular with unramified characters on the diagonal. It is moreover reducible by assumption. Therefore, the characters ε_1 and ε_2 are unramified and we have an equality of sets of characters of G_p:

$$\{\mu(a_p(f)), \mu(a_p(f))\,\overline{\chi}_\ell\} = \left\{\overline{\chi}_\ell^{m_1}\overline{\varepsilon_1}, \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}\right\}.$$

There are two cases to look at:

- If $\mu(a_p(f)) = \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1}$, then we have $a_p(f) \equiv \varepsilon_1(p)p^{m_1} \pmod{\mathfrak{L}}$. In this case, we put $b_p = \varepsilon_1(p)$.
- If $\mu(a_p(f)) = \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$, then we have $a_p(f) \equiv \varepsilon_2(p)p^{m_2} \pmod{\mathfrak{L}}$, and we define $b_p = p^{m_2-m_1}\varepsilon_2(p)$.

In both cases we have $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$ with $b_p \in \{\varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.

(iii) Finally, if $v_p(N) = v_p(\mathfrak{c})$, we are in the second case of proposition 10.17, and we get the equality

$$\left\{\mu(a_p(f)), \mu\left(a_p(f)^{-1}\right)\overline{\varepsilon}_{|G_p}\overline{\chi}_\ell^{k-1}\right\} = \left\{\overline{\chi}_\ell^{m_1}\overline{\varepsilon_1}, \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}\right\},$$

We again have two cases to consider:

- If $\mu(a_p(f)) = \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1}$, then $a_p(f) \equiv \varepsilon_1(p)p^{m_1} \pmod{\mathfrak{L}}$. We define $b_p = \varepsilon_1(p)$.
- If $\mu(a_p(f)) = \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$, then $a_p(f) \equiv \varepsilon_2(p)p^{m_2} \pmod{\mathfrak{L}}$. We put $b_p = p^{m_2-m_1}\varepsilon_2(p)$.

In both cases, we again have $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$ with $b_p \in \{\varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.

■

Lemma 13.5 states that the reducibility of $\overline{\rho}_{f,\lambda}$ is equivalent to an infinite set of congruences satisfied by the coefficients $a_p(f)$, one for each prime number except ℓ. This lack of congruence for $a_\ell(f)$ is in fact not a problem because we always have $\ell a_\ell(f) \equiv 0 \pmod{\mathfrak{L}}$. This will become handy later. In order to transform this infinite set of congruences into a finite one we will use the Sturm bound we develop in section 12.2. In order to do this we need to express the right-hand side of (13.1) as the coefficients of a modular form with $\mathfrak{L}$-integral coefficients. We proceed in three steps.

- First we define a q-series which coefficients will be congruent to $\varepsilon_1(p) + p^{m_2-m_1}\varepsilon_2(p)$ for every prime p. This series will sometimes not be modular, or not has integral Fourier coefficients.
- Next, we modify slightly this series in order to correct these defaults.
- Finally, we will modify it a second time in order to take into account the congruences at $p \mid N$, $p \neq \ell$. This will lead to the wanted modular form except for the small modification we may have done in the second step. To take this into account, we will have to also modify the form f slightly.

Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ dividing λ, and let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, we define

$$k' := \begin{cases} m_2 - m_1 + 1 & \text{if } \ell > 2; \\ 2 & \text{if } \ell = 2, \end{cases} \quad \text{and} \quad E_0 := E_{k'}^{\varepsilon_1,\varepsilon_2}. \tag{13.2}$$

Proposition 13.6. *We have $\varepsilon_1\varepsilon_2(-1) = (-1)^{k'}$. In particular, E_0 is well-defined and modular if and only if $(k', \varepsilon_1, \varepsilon_2) \neq (2, \mathbb{1}, \mathbb{1})$, in which case E_0 is a normalised eigenform of weight k', level $\mathfrak{c}_1\mathfrak{c}_2$, and character $\varepsilon_1\varepsilon_2$. Moreover, for every prime number p we have $a_p(E_0) = \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)$ in any case.*

Proof. If $\ell = 2$, then ε_1 and ε_2 are even, and we have $\varepsilon_1\varepsilon_2(-1) = 1 = (-1)^{k'}$. Otherwise, we have

$$\varepsilon_1\varepsilon_2(-1) = (-1)^{m_2+m_1+1} = (-1)^{m_2-m_1+1} = (-1)^{k'}.$$

The rest of the proposition follows from proposition 11.8 and (11.1). ∎

As mentioned above, we need the coefficients our modular form to be $\mathfrak{L}$-integral. The following result states when it may not be the case.

Lemma 13.7. *Assume $(k', \varepsilon_1, \varepsilon_2) \neq (2, \mathbb{1}, \mathbb{1})$. The Fourier coefficients of E_0 are $\mathfrak{L}$-integral unless perhaps in the following cases:*

- *$\ell = 2$, $\varepsilon_1 = \mathbb{1}$ and $\varepsilon_2 \neq \mathbb{1}$;*
- *$\ell \geqslant 5$, $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, and $(m_1, m_2) = (0, \ell - 2)$.*

Proof. Apart from the constant one, the coefficients of E_0 are all algebraic integers. We therefore only need to focus on the constant Fourier coefficient a_0 of E_0.

In the case $\ell \neq 2$, if $(\varepsilon_1, \varepsilon_2) \neq (\mathbb{1}, \mathbb{1})$, then a_0 is always $\mathfrak{L}$-integral by proposition 11.5, because ε_1 and ε_2 are unramified at ℓ. If $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, then $a_0 = -\frac{1}{2k'}B_{k'}$. By proposition 11.5 again, if $(m_1, m_2) \neq (0, \ell - 2)$, then a_0 is always $\mathfrak{L}$-integral. If $(m_1, m_2) = (0, \ell - 2)$, then a_0 is always not $\mathfrak{L}$-integral. Notice moreover that we must have $\ell \neq 3$, because otherwise $k' = 2$ and $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, which is excluded.

Assume $\ell = 2$, hence $k' = 2$. If $\varepsilon_1 \neq \mathbb{1}$, then as before we have $a_0 = 0$. Else, if $\varepsilon_1 = \mathbb{1}$, then $a_0 = -\frac{B_{2,\varepsilon_2}}{4}$ which may not be $\mathfrak{L}$-integral. Moreover, we must have $\varepsilon_2 \neq \mathbb{1}$ because otherwise we would have $(k', \varepsilon_1, \varepsilon_2) = (2, \mathbb{1}, \mathbb{1})$. ∎

We can now construct from $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ (and hence k' and E_0), a modular form with $\mathfrak{L}$-integral Fourier coefficients which corresponds to the right-hand side of equation (13.1). With the notations of proposition 12.26 and proposition 12.30, define

$$\begin{cases} r := 4 \quad \text{and } E := (E_0)_2^0 & \text{if } \left| \begin{array}{l} \text{we are in one of the cases listed in lemma 13.7} \\ \text{or } \ (k', \varepsilon_1, \varepsilon_2) = (2, \mathbb{1}, \mathbb{1}); \end{array} \right. \\ r := 1 \quad \text{and } E := E_0 & \text{otherwise.} \end{cases} \tag{13.3}$$

The following proposition sums up the properties of E.

Proposition 13.8. *The function E is a modular form of weight k', level $M := \mathrm{lcm}(\mathfrak{c}_1\mathfrak{c}_2, r)$, and character $\varepsilon_1\varepsilon_2$. It is a normalised eigenform for all the Hecke operators at level M, all its Fourier coefficients are $\mathfrak{L}$-integral, and for any prime p, we have*

$$a_p(E) = \begin{cases} \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p) & \text{if } p \nmid r; \\ 0 & \text{if } p \mid r. \end{cases}$$

Proof. The only thing to prove is that M is indeed the level of E. The rest of the proposition then follows from proposition 12.26, proposition 12.30, lemma 13.7 and proposition 13.6. If $r = 1$, the level of E is equal to $\mathfrak{c}_1\mathfrak{c}_2 = \mathrm{lcm}(\mathfrak{c}_1\mathfrak{c}_2, r)$. Assume $r = 4$. We then always have $\mathfrak{c}_1 = 1$ and either $\varepsilon_2 = \mathbb{1}$ or $\ell = 2$. In the first case, $\mathfrak{c}_2 = 1$ and $\varepsilon_2(2) = 1 \neq 0$. In the second case, $\mathfrak{c}_2$ is odd because prime to ℓ. Thus, we have $\varepsilon_2(2) \neq 0$. In every case, the level of E is equal to $4\mathfrak{c}_1\mathfrak{c}_2 = \mathrm{lcm}(\mathfrak{c}_1\mathfrak{c}_2, 4)$. ∎

As mentioned above, as we have modified the second coefficient of E when $r \neq 1$, we need to also modify the second coefficient of f in consequence. With the notations of proposition 12.26, we define

$$\begin{cases} f' := f_2^0 \quad \text{and } N' := \begin{cases} N & \text{if } 2 \mid N \text{ and } a_2(f) = 0; \\ 2N & \text{if } 2 \mid N \text{ and } a_2(f) \neq 0; \\ 4N & \text{if } 2 \nmid N, \end{cases} & \text{if } r = 4; \\ f' := f \quad \text{and } N' := N, & \text{if } r = 1. \end{cases} \tag{13.4}$$

Proposition 13.9. *The form f' is a normalised eigenform of weight k, level N', and character ε. Its Fourier coefficients are $\mathfrak{L}$-integral and if a prime p divides r, then $a_p(f') = a_p(E) = 0$. Moreover, the level $M = \mathrm{lcm}(\mathfrak{c}_1\mathfrak{c}_2, r)$ of E (see proposition 13.8) always divides N', and if $\ell = 2$, then $N' \geqslant 3$.*

Proof. The only facts that do not follow directly from proposition 12.26 are those on the level N'. First recall that $\mathfrak{c}_1\mathfrak{c}_2$ always divide N. For $M = \mathrm{lcm}(\mathfrak{c}_1\mathfrak{c}_2, r)$ to divide N' thus need to prove that r divides N'. If $r = 1$ this straightforward. Assume $r = 4$. If $2 \nmid N$, then $N' = 4N$ is divisible by r. If $2 \mid N$ and $a_2(f) \neq 0$, then 4 divides $N' = 2N$. Finally, if $2 \mid N$ and $a_2(f) = 0$, then by proposition 10.16 we necessarily have $v_2(N) \geqslant 2$. Therefore, $N' = N$ is again divisible by r. In every case, we have $M \mid N'$.

Finally, assume $\ell = 2$. If $\varepsilon_1 = \mathbb{1}$, then we necessarily have $r = 4$ and $N' \geqslant 4$. Otherwise, if $\varepsilon_1 \neq \mathbb{1}$, we then have $N' \geqslant \mathfrak{c}_1 \geqslant 3$ because there is no non-trivial primitive character of conductor less than 3. ∎

We can finally construct the modular form we need. Indeed, for a prime number p, the Hecke polynomial of E at p is equal to

$$X^2 - \left(\varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)\right) X + p^{k'-1}\varepsilon_1\varepsilon_2(p) = (X - \varepsilon_1(p))(X - p^{k'-1}\varepsilon_2(p)).$$

Therefore, we can apply corollary 12.29 to E with $b_p \in \{0, \varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$ to get a modular form with the same Fourier coefficients of prime index as E except at some prime p where it equals b_p. The following lemma allows us to moreover control the level of the resulting modular form.

Lemma 13.10. *Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, let $p \neq \ell$ be any prime number dividing N, and let $b_p \in \{0, \varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$.*

If we have a congruence $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$, then we have

$$1 \leqslant v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p \leqslant v_p(N),$$

where n_p is defined as in proposition 12.26 with respect to $g = E$ and b_p. In particular, those inequalities are independent of the choice of b_p.

Proof. First, we always have $v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p \geqslant 1$, because $n_p = 0$ only if $b_p = a_p(E) = \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)$, which implies that $v_p(\mathfrak{c}_1\mathfrak{c}_2) \geqslant 1$.

Next, we claim the following:

$$b_p = 0 \text{ if and only if } v_p(\mathfrak{c}) < v_p(N) \text{ and } v_p(N) \geqslant 2.$$

Indeed, we have $b_p = 0$ if and only if $a_p(f) \equiv 0 \pmod{\mathfrak{L}}$. Moreover, by proposition 10.16 we have either $v_p(\mathfrak{c}) < v_p(N)$, $v_p(N) \geqslant 2$ and $a_p(f) = 0$, or $|a_p(f)|^2 = p^s$ with $s \geqslant 0$. Therefore, we have $a_p(f) \equiv 0 \pmod{\mathfrak{L}}$ if and only if $v_p(\mathfrak{c}) < v_p(N)$ and $v_p(N) \geqslant 2$.

We now prove that $v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p \leqslant v_p(N)$. If $n_p = 0$, it follows from the fact that $\mathfrak{c}_1\mathfrak{c}_2 \mid N$. If $n_p = 2$, then from proposition 12.26, we must have $b_p = 0 \notin \{\varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$. Therefore, $p \nmid \mathfrak{c}_1\mathfrak{c}_2$ and from the discussion above we have $v_p(N) \geqslant 2 = v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p$.

Assume finally that $n_p = 1$. We have $b_p \neq \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)$ and $b_p \in \{\varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$. Therefore, p does not divide both $\mathfrak{c}_1$ and $\mathfrak{c}_2$. If $p \nmid \mathfrak{c}_1\mathfrak{c}_2$, we have $v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p = 1 \leqslant v_p(N)$. Otherwise, assume that $p \mid \mathfrak{c}_1$ and $p \nmid \mathfrak{c}_2$. We then necessarily have $b_p = 0$ and from the discussion above we get $v_p(\mathfrak{c}) < v_p(N)$. Looking at the p-part of the Artin conductor of both sides of the equality $\overline{\chi}_\ell^{k-1}\overline{\varepsilon} = \overline{\chi}_\ell^{m_1+m_2}\overline{\varepsilon_1\varepsilon_2}$, we get $v_p(\bar{\mathfrak{c}}) = v_p(\overline{\mathfrak{c}_1})$ where $\bar{\mathfrak{c}}$ and $\overline{\mathfrak{c}_1}$ denote the conductors of $\overline{\varepsilon}$ and $\overline{\varepsilon_1}$ respectively. Because ε_1 has prime-to-ℓ order, we have $\overline{\mathfrak{c}_1} = \mathfrak{c}_1$. On the other sides we always have $\bar{\mathfrak{c}} \mid \mathfrak{c}$. Therefore, we have $v_p(\mathfrak{c}_1\mathfrak{c}_2) = v_p(\mathfrak{c}_1) \leqslant v_p(\mathfrak{c})$. Hence, we get $v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p \leqslant v_p(N)$. The case $p \mid \mathfrak{c}_2$ and $p \nmid \mathfrak{c}_1$ is treated in exactly the same way. ∎

This leads to the fundamental result of our discussion.

Corollary 13.11. *Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$. Define k', r and E as in (13.2) and (13.3) respectively. Consider $\mathbf{P} \subseteq \{p \text{ prime}, p \mid N, p \nmid r\ell\}$ and $\mathbf{b} := (b_p)_{p\in\mathbf{P}} \in \prod_{p\in\mathbf{P}} \{0, \varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$ such that for all $p \in \mathbf{P}$, we have $p^{m_1} b_p \equiv a_p(f) \pmod{\mathfrak{L}}$.*

The modular form $E' := E_{\mathbf{P}}^{\mathbf{b}}$ is of weight k', character $\varepsilon_1\varepsilon_2$, and its level divides N'. It has $\mathfrak{L}$-integral Fourier coefficients and for every prime p such that either $p \nmid N\ell$ or $p \in \mathbf{P} \cup \{r\}$, E' is a normalised eigenform for the Hecke operator $T_p^{N'}$.

Proof. From corollary 12.29, the form E' is a normalised eigenform for all the Hecke operators at its level $N_{E'} := \operatorname{lcm}(\mathfrak{c}_1\mathfrak{c}_2, r) \prod_{p\in\mathbf{P}} p^{n_p}$. Moreover, the action of $T_p^{N'}$ and $T_p^{N_{E'}}$ on E' is the same if p divides both N' and $N_{E'}$ or none of them. If $p \nmid N\ell$, then $p \nmid N_{E'}$. If $p \in \mathbf{P} \cup \{r\}$, by lemma 13.10 we have

$$1 \leqslant v_p(N_{E'}) \leqslant v_p(N').$$

Therefore, $N_{E'}$ divides N' and E' is a normalised eigenform for the announced Hecke operators. The rest of the corollary follows from corollary 12.29. ∎

We now able to prove the main result of this section. It gives for a given λ, an explicit finite set of congruences that characterises the reducibility of the representation $\overline{\rho}_{f,\lambda}$.

Theorem 13.12. *Let f be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε. Let λ be a prime ideal of K_f above a prime number ℓ. The following assertions are equivalent:*

1. *$\overline{\rho}_{f,\lambda}$ is reducible;*
2. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. There exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ (see definition 13.1) such that the following holds. Let k', r, and N' be as in (13.2), (13.3) and (13.4) respectively. Define*

$$a = \begin{cases} 4 & \text{if } \left| \begin{array}{l} k \equiv m_1 + m_2 + 3 \pmod 4, \\ \ell = 3 \text{ and } \forall p \mid N', p \equiv 1 \pmod 9; \end{array} \right. \\ 0 & \text{otherwise,} \end{cases}$$

$$b = \begin{cases} 3 & \text{if } \ell \mid N'; \\ 6 & \text{if } \left| \begin{array}{l} \ell = 3 \text{ and } \forall p \mid N', \\ p \equiv 1 \pmod 9; \end{array} \right. \\ \ell + 1 & \text{otherwise,} \end{cases} \qquad \text{and } \widetilde{k} = a + b + \max(k, k' + bm_1).$$

For every prime $p \leqslant B := \frac{N'\widetilde{k}}{12} \prod_{q \mid N'} \left(1 + \frac{1}{q}\right)$ not dividing $r\ell$, we have

- *$p \nmid N$ and $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$;*
- *or, $p \mid N$ and $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ for some b_p in the set $\{0, \varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.*

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$.

Proof. Assertion (2) is weaker than the second part of lemma 13.5. Therefore, (1) implies (2).

Assume that 2 holds. Consider again k', r, E, N', and f' defined in (13.2), (13.3) and (13.4) respectively. Define $\mathbf{P} := \{p \text{ prime}, p \mid N, p \nmid \ell r, p \leqslant B\}$, and $\mathbf{b} := (b_p)_{p \in \mathbf{P}}$. Finally, with the notation of corollary 12.29, consider the form $E' := E_{\mathbf{P}}^{\mathbf{b}}$.

We wish to apply corollary 12.19 with $f = f'$, $g = E'$, $m_f = 1$ and $m_g = m_1 + 1$. By corollary 13.11, we have $E' \in \mathrm{M}_{k'}(N', \varepsilon_1\varepsilon_2)$, it has $\mathfrak{L}$-integral Fourier coefficients, and it is an eigenform for all the Hecke operators at level N' of index less than B, except maybe at ℓ. Moreover, from the identity $\overline{\chi}_\ell^{m_1+m_2}\overline{\varepsilon_1\varepsilon_2} = \overline{\chi}_\ell^{k-1}\overline{\varepsilon}$, we have

$$\overline{\chi}_\ell^{k'+2(m_1+1)}\overline{\varepsilon_1\varepsilon_2} = \overline{\chi}_\ell^{(m_2-m_1+1)+2(m_1+1)}\overline{\varepsilon_1\varepsilon_2} = \overline{\chi}_\ell^{m_1+m_2+3}\overline{\varepsilon_1\varepsilon_2} = \overline{\chi}_\ell^{k+2}\overline{\varepsilon}.$$

Let p be a prime number less than B. If $p \mid \ell r$, then we have

$$p^{m_1+1}a_p(E') \equiv 0 \equiv pa_p(f') \pmod{\mathfrak{L}}.$$

Otherwise, by corollary 12.29 we have $p^{m_1+1}a_p(E') \equiv p^{m_1+1}b_p \equiv pa_p(f') \pmod{\mathfrak{L}}$. The definitions of a, b and $\widetilde{k}$ correspond to those of a, b and k in proposition 12.17 (the case $\ell = 2$ and $N' \leqslant 2$ never occurs as proved in proposition 13.9). By corollary 12.19, we therefore obtain the congruence $na_n(f') \equiv n^{m_1+1}a_n(E') \pmod{\mathfrak{L}}$ for every non-negative integer n. By lemma 13.5, we thus have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$. ∎

Remark 13.13. *From this theorem, we can deduce an algorithm that takes a prime ideal λ as input and decides whether the representation $\overline{\rho}_{f,\lambda}$ is reducible or not, and computes the representation if it is reducible. In particular, it justifies the reducibility modulo 11 of the representation treated in [BD14, 5.1.2]. We give further details on how to explicitly do this in PARI/GP in chapter 15. Moreover, the theorem extends the case $m = 1$ of [Kra97, Proposition 2.].*

13.2 Reducible modular representations in big characteristic

The previous theorem holds without any restriction on ℓ, but the result depends on ℓ through

1. the set $R_{N,k,\varepsilon}(\mathfrak{L})$;
2. the integer B that bounds the number of congruences to check.

The goal of this section is to remove these dependencies on ℓ under some assumptions. We first remove the dependency in ℓ in the set $R_{N,k,\varepsilon}(\mathfrak{L})$.

Definition 13.14. *Define $R_{N,\varepsilon}$ as the set of pairs $(\varepsilon_1, \varepsilon_2)$ of primitive Dirichlet characters such that $\varepsilon_1\varepsilon_2 = \varepsilon$ and for every prime number p, we have $v_p\left(\frac{N}{\mathfrak{c}_1\mathfrak{c}_2}\right) \in \{0,1,2\}$, where $\mathfrak{c}_i$ is the conductor of ε_i.*

Proposition 13.15. *Assume $\ell \geqslant k-1$ and $\ell \nmid N\varphi(N)$. The representation $\overline{\rho}_{f,\lambda}$ is reducible if and only if there exists $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ such that $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon_2}$. We moreover have $a_\ell(f) \equiv \varepsilon_1(\ell) + \ell^{k-1}\varepsilon_2(\ell) \pmod{\mathfrak{L}}$.*

Proof. From proposition 13.2, if $\overline{\rho}_{f,\lambda}$ is reducible, then there exists a quadruple $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$. By the assumptions $\ell \nmid N$ and $\ell \geqslant k-1$, together with proposition 10.14, f must be ordinary at λ, and we have an equality of sets

$$\left\{\mu\left(a_\ell(f)\right), \overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right)\right\} = \left\{\overline{\chi}_\ell^{m_1}\overline{\varepsilon_1}, \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}\right\}.$$

It follows that $(m_1, m_2) = (0, k-1)$ and $a_\ell(f) \equiv \varepsilon_1(\ell) \equiv \varepsilon_1(\ell) + \ell^{k-1}\varepsilon_2(\ell) \pmod{\mathfrak{L}}$. Finally, the character $\varepsilon(\varepsilon_1\varepsilon_2)^{-1}$ reduces to the trivial character modulo $\mathfrak{L}$, and because $\ell \nmid \varphi(N)$, it must have prime-to-ℓ order. Using lemma 10.5, it must be trivial, and we get $\varepsilon = \varepsilon_1\varepsilon_2$. ∎

The following result will allow us to both remove the dependency in ℓ in the bound B of theorem 13.12, and bound the set of ℓ such that $\overline{\rho}_{f,\lambda}$ is reducible.

Proposition 13.16. *Assume $\ell > k+1$ and $\ell \nmid N\varphi(N)$. The representation $\overline{\rho}_{f,\lambda}$ is reducible if and only if there exist a pair $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$, and $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$, with $\mathbf{P} := \{p \text{ prime}, p \mid N, p \nmid \ell r\}$, such that $f' \equiv E' \pmod{\mathfrak{L}}$, with f' defined as in (13.4) and $E' := E^{\mathbf{b}}_{\mathbf{P}}$ with E defined in (13.3).*

Proof. If we have $f' \equiv E' \pmod{\mathfrak{L}}$, then in particular for all primes $p \nmid N\ell r$, we have

$$a_p(f) = a_p(f') \equiv a_p(E') \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}.$$

By lemma 13.5, $\overline{\rho}_{f,\lambda}$ is therefore reducible.

Assume that $\overline{\rho}_{f,\lambda}$ is reducible. The existence of $(\varepsilon_1, \varepsilon_2)$ is granted by proposition 13.15. Moreover, by lemma 13.5 there exists $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$ such that for every prime number p, we have a congruence $a_p(f') \equiv a_p(E') \pmod{\mathfrak{L}}$. By corollary 13.11, $E' \in \mathrm{M}_k(N', \varepsilon)$ has $\mathfrak{L}$-integral Fourier coefficients and is an eigenform for all the Hecke operators at level N'. By proposition 13.9, f' has the same properties and therefore the modular form $f' - E'$ is constant modulo $\mathfrak{L}$.

By the assumptions $\ell > k+1$ and $\ell \nmid N\varphi(N)$, we have $\ell \geqslant 5$ and $\ell \nmid N$. Therefore, we know from [DI95, Theorem 12.3.7] this Katz' modular form spaces with coefficients in $\overline{\mathbb{F}}_\ell$ are isomorphic to the spaces of reduction modulo $\mathfrak{L}$ of modular forms with $\mathfrak{L}$-integral coefficients. Therefore, from [Kat73, Corollary 4.4.2], for $f' - E'$ to be congruent to a non-zero constant we must have $k \equiv 0 \pmod{\ell - 1}$. This cannot hold under the assumption $\ell > k+1$, and we get $f' \equiv E' \pmod{\mathfrak{L}}$. ∎

We now state our second main result. It is analogous to theorem 13.12 for the prime numbers $\ell > k+1$ and $\ell \nmid N\varphi(N)$.

Theorem 13.17. *Let f be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε. Let λ be a prime ideal of K_f above a prime number ℓ. Assume $\ell > k+1$ and $\ell \nmid N\varphi(N)$. The following assertions are equivalent.*

1. *$\overline{\rho}_{f,\lambda}$ is reducible.*
2. *Let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above λ. There exists $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ such that the following holds. Let r be as is (13.3) (recall that $(m_1, m_2) = (0, k-1)$) and let N' be as in (13.4). Define*

$$C = \begin{cases} 0 & \text{if } r > 1 \text{ or } \varepsilon_1 \neq \mathbb{1}; \\ -\frac{B_{k,\varepsilon_0}}{2k} \prod_{p \mid N} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) & \text{otherwise,} \end{cases}$$

where ε_0 is the primitive character associated to ε.

We have $C \equiv 0 \pmod{\mathfrak{L}}$, and for all primes $p \leqslant B := \frac{N'k}{12} \prod_{q \mid N'} \left(1 + \frac{1}{q}\right)$, we have either $p \mid r$ or

- *$a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$, if $p \nmid N$;*
- *$a_p(f) \equiv b_p \pmod{\mathfrak{L}}$ for some $b_p \in \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$, if $p \mid N$.*

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon_2}$.

Proof. Assume $\overline{\rho}_{f,\lambda}$ to be reducible. Introduce f' and E' as in proposition 13.16. The congruences for $a_p(f)$ follow from the congruence $f' \equiv E' \pmod{\mathfrak{L}}$. It only remains to prove that $C \equiv 0 \pmod{\mathfrak{L}}$. Because f' is cuspidal, its constant coefficient at infinity is equal to 0. Therefore, the one of E' must be congruent to 0 modulo $\mathfrak{L}$.

The congruence $C \equiv 0 \pmod{\mathfrak{L}}$ is non-trivial only if $r = 1$ and $\varepsilon_1 = \mathbb{1}$. In this case, we have $\varepsilon_2 = \varepsilon_0$, the set $\mathbf{P}$ of proposition 13.16 is the set of prime divisors of N and for all $p \in \mathbf{P}$ we have $b_p \equiv a_p(f) \pmod{\mathfrak{L}}$. Therefore, the constant coefficient of E' is equal to

$$-\frac{B_{k,\varepsilon_2}}{2k}\prod_{p\in\mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)) \equiv -\frac{B_{k,\varepsilon_0}}{2k}\prod_{p|N} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) \pmod{\mathfrak{L}}$$
$$\equiv C \pmod{\mathfrak{L}}.$$

This proves that (1) implies (2).

Assume now that the second part of the theorem holds. Consider again the modular forms E and f', and define $\mathbf{P}_{\leqslant B} := \{p \text{ prime}, p \mid N, p \leqslant B\}$ and $\mathbf{b}_{\leqslant B} := (b_p)_{p\in\mathbf{P}_{\leqslant B}}$, and let $E' := E^{\mathbf{b}_{\leqslant B}}_{\mathbf{P}_{\leqslant B}}$. By corollary 13.11, we have $E' \in \mathrm{M}_k(N', \varepsilon)$, it has $\mathfrak{L}$-integral coefficients, and it is an eigenform for all the Hecke operators at level N' of index less than B. The form f' has moreover the same properties and for all prime numbers $p \leqslant B$, we have by assumption $a_p(f') \equiv a_p(E') \pmod{\mathfrak{L}}$. In order to apply corollary 12.19 to $f = f'$, $g = E'$, $m_f = m_g = 0$, we need to have $a_0(E') \equiv 0 \pmod{\mathfrak{L}}$. From proposition 12.32, we have $a_0(E') = 0$ if $\varepsilon_1 \neq \mathbb{1}$ or $r > 1$. Else, if $\varepsilon_1 = \mathbb{1}$ and $r = 1$, we have $\varepsilon_2 = \varepsilon_0$ and

$$a_0(E') = -\frac{B_{k,\varepsilon_2}}{2k}\prod_{p|N,p\leqslant B} b_p(b_p - p^{k-1}\varepsilon_2(p))$$
$$\equiv -\frac{B_{k,\varepsilon_0}}{2k}\prod_{p|N,p\leqslant B} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) \pmod{\mathfrak{L}}.$$

By the assumption $C \equiv 0 \pmod{\mathfrak{L}}$, we have either $a_0(E') \equiv 0 \pmod{\mathfrak{L}}$, or there exists $p_0 \mid N$, $p_0 > B$, such that $a_{p_0}(f)(a_{p_0}(f) - p_0^{k-1}\varepsilon_0(p_0)) \equiv 0 \pmod{\mathfrak{L}}$. Define then,

$$E'' := \begin{cases} E' & \text{if } a_0(E') \equiv 0 \pmod{\mathfrak{L}}; \\ E'^{b_{p_0}}_{p_0} & \text{otherwise.} \end{cases}$$

$$\text{with } b_{p_0} = \begin{cases} 0 & \text{if } a_{p_0}(f) \equiv 0 \pmod{\mathfrak{L}}; \\ p_0^{k-1}\varepsilon_0(p_0) & \text{if } a_{p_0}(f) \equiv p_0^{k-1}\varepsilon_0(p_0) \pmod{\mathfrak{L}}. \end{cases}$$

By corollary 13.11, E'' still lies in $\mathrm{M}_k(N', \varepsilon)$, has $\mathfrak{L}$-integral Fourier coefficients, is an eigenform for the Hecke operators at level N' of index less than B, for any prime $p \leqslant B$, we have $a_p(E'') \equiv a_p(f')$ (mod $\mathfrak{L}$), and its constant Fourier coefficient vanishes modulo $\mathfrak{L}$. By corollary 12.19, we finally get $E'' \equiv f' \pmod{\mathfrak{L}}$, and we therefore have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi_\ell}^{k-1}\overline{\varepsilon_2}$. ■

Remark 13.18. *Notice that we could have always taken $r = 4$ from the start (i.e. from (13.3)) without modifying any of the results of chapter 13. The version of theorem 13.12 and theorem 13.17 we exposed in the introduction assumed that. The coefficient C is then equal to zero, and we get back the results announced previously.*

From theorem 13.17 we also deduce a bound for the reducible primes in terms of N, k and ε only.

Theorem 13.19. *Assume that $\overline{\rho}_{f,\lambda}$ is reducible, then one of the following conditions holds.*

- $\ell \leqslant k+1$;
- $\ell \mid N\varphi(N)$;
- *there exists* $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ *such that* ℓ *divides the algebraic norm of one the following non-zero quantities*
  1. $B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}$;
  2. $p^k - (\varepsilon_1\varepsilon_2^{-1})_0(p)$ *for a prime* p *such that* $p \mid \mathfrak{c}_1\mathfrak{c}_2$, $p \nmid \mathfrak{c}_0$ *with* $\mathfrak{c}_0$ *the conductor of* $(\varepsilon_1\varepsilon_2^{-1})_0$.

Proof. Assume $\ell > k+1$ and $\ell \nmid N\varphi(N)$. From proposition 13.16, if $\overline{\rho}_{f,\lambda}$ is reducible, we have a congruence modulo $\mathfrak{L}$ between the cuspidal modular form f', and the Eisenstein series E'. Therefore, by Katz' q-expansion principle (see [Kat73]) the constant coefficient of E' must be congruent to 0 modulo $\mathfrak{L}$ at every cusp. By proposition 12.33, the constant coefficient of E' at the cusp $\frac{1}{\mathfrak{c}_2}$ divides the quantity

$$-\varepsilon_1(-1)\frac{W((\varepsilon_1\varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})}\frac{B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}}{2k}\left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0}\right)^k \times \prod_{p\mid\mathfrak{c}_1\mathfrak{c}_2}\left(1-\frac{(\varepsilon_1\varepsilon_2^{-1})_0(p)}{p^k}\right)\prod_{p\mid N'}\left(1-\frac{\varepsilon_1(p)\varepsilon_2^{-1}(p)}{p^k}\right)\left(1-\frac{1}{p}\right).$$

Let us look at the prime factors of the norm of this coefficient.

- The number $-\varepsilon_1(-1)$ is a unit. Its norm has no prime factor.
- By proposition 11.7, the prime factors of the norm of $\frac{W((\varepsilon_1\varepsilon_2^{-1})_0)}{W(\overline{\varepsilon_2})}\left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0}\right)^k$ are only powers of prime factors of N. By assumption, ℓ does not divide them.
- For $p \mid N'$, we have $1-\frac{1}{p} = \frac{p-1}{p}$. By the assumption $\ell \nmid N\varphi(N)$, this cannot vanish modulo $\mathfrak{L}$.
- For $p \mid N'$ again, let us prove that the prime factors of the norm of $\left(1-\frac{\varepsilon_1(p)\varepsilon_2^{-1}(p)}{p^k}\right)$ are redundant with the ones of N and $\left(p^k-(\varepsilon_1\varepsilon_2^{-1})_0(p)\right)$. Note that we either have $p=2$ and $(k,\varepsilon_1,\varepsilon_2) = (2,\mathbb{1},\mathbb{1})$, or $N' = N$. In the first case we have $1-\frac{\varepsilon_1(p)\varepsilon_2^{-1}(p)}{p^k} = \frac{3}{4}$. This cannot vanish modulo $\mathfrak{L}$ by assumption because 2 and 3 are less or equal to $k+1=3$. Otherwise, we have $p \mid N$, then either $p \mid \mathfrak{c}_0$ and $1-\frac{\varepsilon_1(p)\varepsilon_2^{-1}(p)}{p^k} = 1 \not\equiv 0 \pmod{\mathfrak{L}}$, or $p \nmid \mathfrak{c}_0$ and $1-\frac{\varepsilon_1(p)\varepsilon_2^{-1}(p)}{p^k} = \frac{p^k-(\varepsilon_1\varepsilon_2^{-1})_0(p)}{p^k}$. Therefore, ℓ must divide the algebraic norm of $p^k-(\varepsilon_1\varepsilon_2^{-1})_0(p)$.
- Finally, ℓ divides either the norm of $\frac{B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}}{2k}$ and thus $B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}$ because $2k$ is non-zero modulo $\mathfrak{L}$ by assumption, or $p^k-(\varepsilon_1\varepsilon_2^{-1})_0(p)$ for $p \mid \mathfrak{c}_1\mathfrak{c}_2$. This final quantity contains only prime factors of N if $p \mid \mathfrak{c}_0$. We can therefore consider only the primes $p \nmid \mathfrak{c}_0$.

■

13.3 Checking the reducibility

We explain here how to use theorem 13.12 and theorem 13.17 to explicitly compute the prime ideals λ for which the representation $\overline{\rho}_{f,\lambda}$ is reducible. We begin by discussing the dependency of the set $R_{N,k,\varepsilon}(\mathfrak{L})$ (see definition 13.1) in the place $\mathfrak{L}$.

Proposition 13.20. *Let $N \geqslant 1$ and $k \geqslant 2$ be integers, and let ε be a Dirichlet character modulo N. Let ℓ be a prime number and let $\mathfrak{L}$ be a place of $\overline{\mathbb{Q}}$ above ℓ. The set $R_{N,k,\varepsilon}(\mathfrak{L})$ depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$ (and on N, k and ε).*

Proof. Write $\pi_{\mathfrak{L}}$ for the projection modulo $\mathfrak{L}$, and $T_{\mathfrak{L}}$ for the associated Teichmüller lift (see section 10.2.2). Recall that for $x \in \overline{\mathbb{F}}_\ell^\times$, $T_{\mathfrak{L}}(x)$ is the only root of unity of order prime to ℓ and such that $\pi_{\mathfrak{L}}(T_{\mathfrak{L}}(x)) = x$.

We first prove that the map $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}$ depends only on ℓ. Let ζ be a root of unity of order $n = \ell^m q$ with $m \geqslant 0$ and $\ell \nmid q$. We can then write $\zeta = \zeta^{\ell^m a} \cdot \zeta^{qb}$, with $\ell \nmid b$ and a prime to q. Because ζ is a root of unity of order n, $\zeta^{\ell^m a}$ is a root of unity of order q and ζ^{qb} is a root of unity of order ℓ^m. From lemma 10.5, we get $\zeta \equiv \zeta^{\ell^m a} \pmod{\mathfrak{L}}$, and $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\zeta) = \zeta^{\ell^m a}$. Therefore, it depends only on ℓ.

Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$. The only dependency on the place $\mathfrak{L}$ is the congruence

$$\overline{\chi}_\ell^{k-1}\varepsilon \equiv \overline{\chi}_\ell^{m_1+m_2}\varepsilon_1\varepsilon_2 \pmod{\mathfrak{L}}.$$

Decompose ε as $\varepsilon_\ell\varepsilon'$, where ε_ℓ is the ℓ-part of ε, and ε' is unramified at ℓ. Looking at the ℓ-part of the congruence on the one hand, and at the prime-to-ℓ part on the another hand, the congruence is equivalent to

$$\overline{\chi}_\ell^{k-1}\varepsilon_\ell \equiv \overline{\chi}_\ell^{m_1+m_2} \pmod{\mathfrak{L}} \quad \text{and} \quad \varepsilon' \equiv \varepsilon_1\varepsilon_2 \pmod{\mathfrak{L}}. \tag{13.5}$$

Applying $T_{\mathfrak{L}}$ to the second equation, we get $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon') = T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon_1\varepsilon_2)$. We have seen that this depends only on ℓ. Let us look at the first equation. The projection of ε_ℓ modulo $\mathfrak{L}$ depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$. Moreover, $\pi_{\mathfrak{L}}(\varepsilon_\ell)$ is a character modulo $\mathfrak{L}$ of conductor ℓ. Therefore, there exists an integer k_ℓ between 0 $\ell - 1$, depending only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$, such that $\pi_{\mathfrak{L}}(\varepsilon_\ell) = \overline{\chi}_\ell^{k_\ell}$. The equation $\overline{\chi}_\ell^{k-1}\varepsilon_\ell \equiv \overline{\chi}_\ell^{m_1+m_2} \pmod{\mathfrak{L}}$ is therefore equivalent to $k + k_\ell - 1 \equiv m_1 + m_2 \pmod{\ell - 1}$ and depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$. ∎

Notice that we have in fact proved that $R_{N,k,\varepsilon}(\mathfrak{L})$ depends only on $\mathfrak{L} \cap \mathbb{Q}(T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon_\ell))$ but we will only use what we have stated. A practical application of this result is that we can compute the set $R_{N,k,\varepsilon}(\mathfrak{L})$ while knowing only a prime ideal λ below $\mathfrak{L}$ in a finite extension of $\mathbb{Q}(\varepsilon)$, like K_f for example. For λ a prime ideal in an extension of $\mathbb{Q}(\varepsilon)$, we will freely write $R_{N,k,\varepsilon}(\lambda)$ for the set $R_{N,k,\varepsilon}(\mathfrak{L})$ for any place $\mathfrak{L}$ above λ. We also deduce from proposition 13.20, a procedure to compute $R_{N,k,\varepsilon}(\lambda)$:

Algorithm 13.21. ***Input**: Two integers $N \geqslant 1$, $k \geqslant 2$, a Dirichlet character ε modulo N, and a prime ideal λ in a finite extension of $\mathbb{Q}(\varepsilon)$ above a prime number ℓ.*
***Output**: The set $R_{N,k,\varepsilon}(\lambda)$.*

1. *Compute ε_ℓ and ε', the ℓ-part and prime-to-ℓ part of ε respectively.*

2. *Compute the unique Dirichlet character ε'' modulo N such that ε'' has prime-to-ℓ order, is unramified at ℓ and $\varepsilon'\varepsilon''^{-1}$ has order a power of ℓ. This corresponds to the character $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon')$ for any place $\mathfrak{L}$ above λ.*

3. *Compute the integers k_ℓ such that $0 \leqslant k_\ell \leqslant \ell - 2$ and for all integer $1 \leqslant n \leqslant N$ prime to N, $\varepsilon_\ell(n) \equiv n^{k_\ell} \pmod{\lambda}$. We then have $\varepsilon_\ell \equiv \overline{\chi}_\ell^{k_\ell} \pmod{\lambda}$.*

4. *Compute the set $M_{N,k,\varepsilon}(\lambda)$ of pairs of integers (m_1, m_2) such that $0 \leqslant m_1 \leqslant m_2 < \ell - 1$ and $m_1 + m_2 \equiv k + k_\ell - 1 \pmod{\ell - 1}$.*

5. *Compute the set $E_{N,k,\varepsilon}(\lambda)$ of pairs of Dirichlet characters $(\varepsilon_1, \varepsilon_2)$ of conductor $(\mathfrak{c}_1, \mathfrak{c}_2)$ and such that ε_1 and ε_2 have prime-to-ℓ order, are unramified at ℓ, satisfy $\varepsilon_1\varepsilon_2 = \varepsilon''$ and for all primes $p \neq \ell$, we have $v_p\left(\frac{N}{\mathfrak{c}_1\mathfrak{c}_2}\right) \in \{0, 1, 2\}$.*

6. *Return the set $E_{N,k,\varepsilon}(\lambda) \times M_{N,k,\varepsilon}(\lambda) = R_{N,k,\varepsilon}(\lambda)$.*

We now give the two main algorithm that follows from theorem 13.17 and theorem 13.12 respectively. The first algorithm computes the prime ideals λ of $\mathcal{O}_f$, of residual characteristic ℓ such that $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the description of $\overline{\rho}_{f,\lambda}$. The correctness of the algorithm is granted by theorem 13.17.

Algorithm 13.22. ***Input****: A newform f, described by its Fourier coefficients $(a_n(f))_{n\geqslant 0}$ as elements of the number field K_f, together with its level N, weight k, and character ε.*
Output*: The set of prime ideals λ of $\mathcal{O}_f$ of residual characteristic ℓ such that $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the shape of $\overline{\rho}_{f,\lambda}$.*

1. *Set* $\mathrm{Red}(f) = \emptyset$.

2. *Compute the set $R_{N,\varepsilon}$ (see definition 13.14).*

3. *For $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$,*

   (a) *Compute r, C, and B defined in (13.3), and theorem 13.17 respectively.*

   (b) *Compute the set $P(\varepsilon_1, \varepsilon_2)$ of prime divisors of the* gcd *of the algebraic norms of*

   - *C;*
   - *$a_p(f) - \varepsilon_1(p) - p^{k-1}\varepsilon_2(p)$, for $p \nmid Nr$, $p \leqslant B$;*
   - *and $a_p(f)\left(a_p(f) - \varepsilon_1(p)\right)\left(a_p(f) - p^{k-1}\varepsilon_2(p)\right)$, for $p \mid N$, $p \nmid r$, $p \leqslant B$,*

   that are bigger than $k + 1$ and do not divide $N\varphi(N)$. By theorem 13.17, these are the only prime numbers bigger than $k + 1$ and not dividing $N\varphi(N)$ for which $\overline{\rho}_{f,\lambda}$ can be reducible.

4. *For $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ and for $\ell \in P(\varepsilon_1, \varepsilon_2)$,*

   (a) *Compute the prime ideals λ of $\mathcal{O}_f$ above ℓ.*

   (b) *For each such λ, compute a prime ideal $\mathfrak{L}$ in the ring of integers of $K_f(\varepsilon_1, \varepsilon_2)$ above λ.*

   (c) *For each such $\mathfrak{L}$, check the following congruences.*

- $C \equiv 0 \pmod{\mathfrak{L}}$;
- $a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$ *for all* $p \nmid Nr$, $p \leqslant B$;
- $a_p(f)(a_p(f) - \varepsilon_1(p))(a_p(f) - p^{k-1}\varepsilon_2(p)) \equiv 0 \pmod{\mathfrak{L}}$ *for all* $p \mid N$, $p \nmid r$, $p \leqslant B$.

If they all hold, add $(\lambda, \varepsilon_1, \varepsilon_2, 0, k-1)$ *to* $\mathrm{Red}(f)$. *By theorem 13.17,* $\overline{\rho}_{f,\lambda}$ *is reducible and we have* $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon_2}$.

5. *Return* $\mathrm{Red}(f)$.

We now turn to the computation of the reducible primes of residue characteristic ℓ such that $\ell \leqslant k+1$ or $\ell \mid N\varphi(N)$. The correctness of the following algorithm follows by theorem 13.12.

Algorithm 13.23. ***Input****: A newform f, described by its Fourier coefficients $(a_n(f))_{n\geqslant 0}$ as elements of the number field K_f, together with its level N, weight k, and character ε.*
Output*: The set of prime ideals λ of $\mathcal{O}_f$ of residual characteristic ℓ such that $\ell \leqslant k+1$ or $\ell \mid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the shape of $\overline{\rho}_{f,\lambda}$.*

1. *Set* $\mathrm{Red}(f) = \emptyset$.
2. *Compute the set P of prime numbers ℓ such that $\ell \leqslant k+1$ or $\ell \mid N\varphi(N)$.*
3. *For each $\ell \in P$, compute the set $P(\ell)$ of prime ideals λ in $\mathcal{O}_f$ above ℓ.*
4. *For each $\ell \in P$ and for each $\lambda \in P(\ell)$, compute $R_{N,k,\varepsilon}(\lambda)$ using algorithm 13.21. We can do this because we have $\mathbb{Q}(\varepsilon) \subset K_f$.*
5. *For each $\ell \in P$, for each $\lambda \in P(\ell)$, and for each $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\lambda)$,*
   (a) *Compute a prime ideal $\mathfrak{L}$ in the ring of integers of $K_f(\varepsilon_1, \varepsilon_2)$ above λ.*
   (b) *Compute r and B defined in (13.3) and theorem 13.12 respectively.*
   (c) *Check the following congruences.*
   - $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$ *for all* $p \nmid Nr$, $p \leqslant B$;
   - $a_p(f)(a_p(f) - p^{m_1}\varepsilon_1(p))(a_p(f) - p^{m_2}\varepsilon_2(p)) \equiv 0 \pmod{\mathfrak{L}}$ *for all* $p \mid N$, $p \nmid r$, $p \leqslant B$.

   If they all hold, add $(\lambda, \varepsilon_1, \varepsilon_2, m_1, m_2)$ *to* $\mathrm{Red}(f)$. *By theorem 13.12,* $\overline{\rho}_{f,\lambda}$ *is reducible and we have* $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon_1} \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon_2}$.
6. *Return* $\mathrm{Red}(f)$.

The correctness of algorithm 13.22 and algorithm 13.23 follows directly from theorem 13.17 and theorem 13.12 respectively. The most time-consuming computation is step 3(*b*) of algorithm 13.22. This depends on the size of the "big" reducible primes. We have implemented these algorithms in PARI/GP [21], and we have been able to execute them as long as the degree of K_f keeps reasonable (say $[K_f : \mathbb{Q}] \leqslant 20$). The second limiting factor being the weight k that controls the size of the Fourier coefficients of f. Our code is available on GitHub at the following address:

https://github.com/bpeaucelle/mfexceptional

Chapter 14

Dihedral modular representations

14.1 General study of dihedral modular representations

Let $f = q + \sum_{n=2}^{\infty} a_n(f) q^n$ be a newform of weight $k \geqslant 2$, level $N \geqslant 1$, and character ε of conductor $\mathfrak{c}$. Let λ be a prime ideal in the ring of integers of the field of coefficients K_f of f above a rational prime number ℓ. We study in this section the case where $\overline{\rho}_{f,\lambda}$ has projective dihedral image of order prime to ℓ. We therefore assume in this chapter that ℓ is bigger than 2. The main result of this section is theorem 14.12. It is the analogue in the dihedral case of theorem 13.12. It characterises the fact that $\overline{\rho}_{f,\lambda}$ has dihedral projective image by a finite number of congruences. We begin this section by recalling some results on twists of modular forms and CM forms.

Let ψ be a primitive Dirichlet character of conductor $\mathfrak{c}_\psi$. We define the twist of f by ψ as the only newform denoted $f \otimes \psi$ such that $a_p(f \otimes \psi) = \psi(p) a_p(f)$ for all primes p not dividing $N\mathfrak{c}_\psi$. We have the following result from [AL78, §§1-3].

Proposition 14.1. *Let f and ψ be as above.*

- *The form $f \otimes \psi$ has weight k, its level divides $\mathrm{lcm}(N, \mathfrak{c}_\psi^2, \mathfrak{c}\mathfrak{c}_\psi)$, and its character is $\psi^2\varepsilon$.*
- *For all primes $p \nmid \mathfrak{c}_\psi$ we have $a_p(f \otimes \psi) = \psi(p) a_p(f)$, and the p-part of the level of $f \otimes \psi$ is equal to $p^{v_p(N)}$.*
- *If $v_p(N) = v_p(\mathfrak{c})$ and $\psi_p = \varepsilon_p^{-1}$, where ψ_p and ε_p denote the p-parts of ψ and ε respectively, then we have $a_p(f \otimes \psi) = (\varepsilon\psi)_0(p)\overline{a_p(f)}$, where $\overline{a_p(f)}$ denotes the complex conjugate of $a_p(f)$ and $(\varepsilon\psi)_0$ is the primitive character associated to $\varepsilon\psi$. Moreover, the p-parts of the level of $f \otimes \psi$ and f are equal.*
- *For any prime number p dividing N, if $v_p(\mathfrak{c}_\psi) \geqslant v_p(N)$ and the p-part of the conductor of $\varepsilon\psi$ is equal to $p^{v_p(\mathfrak{c}_\psi)}$, then the p-part of the level of $f \otimes \psi$ is exactly $p^{v_p(\mathrm{lcm}(N, \mathfrak{c}_\psi^2, \mathfrak{c}\mathfrak{c}_\psi))}$.*

Remark 14.2. *It is enough to consider twists by primitive characters. Indeed, if ψ is a Dirichlet character modulo M, and ψ_0 for the primitive character associated to ψ, the newforms $f \otimes \psi$ and $f \otimes \psi_0$ are necessarily equal because their Fourier coefficients at a prime p not dividing MN both coincide with $\psi(p)a_p(f)$.*

We take this definition of CM forms from [Rib77, p. 34].

Definition 14.3. *Suppose ψ is not the trivial character. The form f is said to have complex multiplication by ψ if $\psi(p)a_p(f) = a_p(f)$ for all primes p in a set of primes of density 1, that is if $f \otimes \psi = f$.*

The starting point of our study is the following proposition that characterises the dihedral case. To have dihedral projective image is in fact equivalent to be isomorphic to one of its twists.

Proposition 14.4. *The projective image $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}}) \subset \mathrm{PGL}_2(\mathbb{F}_\lambda)$ is dihedral of order prime to ℓ if and only if there exists a quadratic Galois character ψ such that $\overline{\rho}_{f,\lambda} \cong \psi \otimes \overline{\rho}_{f,\lambda}$.*

Proof. Assume the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to the dihedral group D_{2n} of order $2n$, with $2n$ prime to ℓ. We necessarily have $\ell \neq 2$. Denote C_n a cyclic subgroup of order n of D_{2n} (it is unique if $n > 2$). Recall that the set $D_{2n} \setminus C_n$ contains only elements of order 2. Composing $\mathbb{P}\overline{\rho}_{f,\lambda}$ with the projection $D_{2n} \to D_{2n}/C_n \cong \{1, -1\}$, we get a quadratic Galois character:

$$G_{\mathbb{Q}} \xrightarrow[\mathbb{P}\overline{\rho}_{f,\lambda}]{} D_{2n} \longrightarrow \{1, -1\}. \qquad \overset{\psi_{f,\lambda}}{\frown} \tag{14.1}$$

Let us prove that $\overline{\rho}_{f,\lambda} \cong \psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda}$. As $\psi_{f,\lambda}$ has order 2, we have

$$\det(\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda}) = \psi_{f,\lambda}^2 \det(\overline{\rho}_{f,\lambda}) = \det(\overline{\rho}_{f,\lambda}).$$

Let p be a prime number not dividing $N\ell$. The character $\psi_{f,\lambda}$ is unramified at p because $\overline{\rho}_{f,\lambda}$ is, and for a Frobenius element Frob_p at p we have

$$\mathrm{Tr}\left((\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda})(\mathrm{Frob}_p)\right) \equiv \psi_{f,\lambda}(\mathrm{Frob}_p)a_p(f) \pmod{\lambda}.$$

If $\psi_{f,\lambda}(\mathrm{Frob}_p) = 1$, we have $\mathrm{Tr}\left((\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda})(\mathrm{Frob}_p)\right) \equiv a_p(f) \equiv \mathrm{Tr}(\overline{\rho}_{f,\lambda}(\mathrm{Frob}_p)) \pmod{\lambda}$. If Frob_p is mapped to -1 by $\psi_{f,\lambda}$, then $\mathbb{P}\overline{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is an element of $D_{2n} \setminus C_n$ and has order 2. It is therefore annihilated by $X^2 - 1$ and has trace $0 \equiv a_p(f) \pmod{\lambda}$. We then get

$$\mathrm{Tr}\left((\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda})(\mathrm{Frob}_p)\right) \equiv a_p(f) \equiv 0 \equiv \mathrm{Tr}(\overline{\rho}_{f,\lambda}(\mathrm{Frob}_p)) \pmod{\lambda}.$$

We have proved that the determinant and the trace at $(\mathrm{Frob}_p)_{p \nmid N\ell}$ of $\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda}$ and $\overline{\rho}_{f,\lambda}$ agree. By theorem 10.1, we deduce that $\psi_{f,\lambda} \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f,\lambda}$.

Conversely, assume that there exists a quadratic Galois character ψ such that $\psi \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f,\lambda}$. As there is no character of order 2 with value in $\overline{\mathbb{F}}_2$, we necessarily have $\ell > 2$. Let G be the kernel of ψ. By Galois theory, the group G is the absolute Galois group of a number field K. Moreover, as ψ has values in $\{1, -1\}$, G_K has index 2 in $G_{\mathbb{Q}}$, and K is therefore a quadratic extension of $\mathbb{Q}$. Let $P \in \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be such that $\overline{\rho}_{f,\lambda} = \psi \otimes \left(P\overline{\rho}_{f,\lambda}P^{-1}\right)$, and let $\tau \in G_{\mathbb{Q}} \setminus G_K$. We have

$$\overline{\rho}_{f,\lambda}(\tau) = -P\overline{\rho}_{f,\lambda}(\tau)P^{-1}. \tag{14.2}$$

Let v be an eigenvector of P with eigenvalue λ. The vector $\overline{\rho}_{f,\lambda}(\tau)v$ is then an eigenvector of P with eigenvalue $-\lambda \neq \lambda$ (because $\ell \neq 2$). We deduce that P is diagonalisable. Let $\sigma \in G_K$. We have

$$\overline{\rho}_{f,\lambda}(\sigma)P = P\overline{\rho}_{f,\lambda}(\sigma).$$

Therefore, $P\overline{\rho}_{f,\lambda}(\sigma)v = \overline{\rho}_{f,\lambda}(\sigma)Pv = \lambda\overline{\rho}_{f,\lambda}(\sigma)v$. That is, $\overline{\rho}_{f,\lambda}(\sigma)v$ is an eigenvector for P with eigenvalue λ. Because the λ-eigenspace of P is one dimensional, there exists $\alpha(\sigma) \in \overline{\mathbb{F}}_\ell^\times$ such that $\overline{\rho}_{f,\lambda}(\sigma)v = \alpha(\sigma)v$. Similarly, $\overline{\rho}_{f,\lambda}(\sigma)\overline{\rho}_{f,\lambda}(\tau)v$ is an eigenvector for P with eigenvalue $-\lambda$, hence there exists $\beta(\sigma) \in \overline{\mathbb{F}}_\ell^\times$ such that $\overline{\rho}_{f,\lambda}(\sigma)\overline{\rho}_{f,\lambda}(\tau)v = \beta(\sigma)\overline{\rho}_{f,\lambda}(\tau)v$. The functions α and β are in fact characters of G_K and we have

$$\overline{\rho}_{f,\lambda}|_{G_K} \cong \alpha \oplus \beta.$$

Moreover, for $\sigma \in G_K$ we have

$$\alpha(\sigma)v = \overline{\rho}_{f,\lambda}(\sigma)v = \overline{\rho}_{f,\lambda}(\tau^{-1})\overline{\rho}_{f,\lambda}(\tau\sigma\tau^{-1})\overline{\rho}_{f,\lambda}(\tau)v = \overline{\rho}_{f,\lambda}(\tau^{-1})\beta(\tau\sigma\tau^{-1})\overline{\rho}_{f,\lambda}(\tau)v = \beta(\tau\sigma\tau^{-1})v.$$

The character α is thus equal to $\beta^\tau := \left(\sigma \mapsto \beta(\tau\sigma\tau^{-1})\right)$.

We can prove from this that $\mathbb{P}\overline{\rho}_{f,\lambda}(G_\mathbb{Q})$ is dihedral. Let $C := \mathbb{P}\overline{\rho}_{f,\lambda}(G_K)$. It is isomorphic to $\beta\alpha^{-1}(G_K) \subseteq \overline{\mathbb{F}}_\ell^\times$ and is thus cyclic of order some integer n prime to ℓ, and generated by $\mathbb{P}\overline{\rho}_{f,\lambda}(\sigma_0)$ for some $\sigma_0 \in G_K$. Moreover, we have

$$\mathbb{P}\overline{\rho}_{f,\lambda}(G_\mathbb{Q}) = C \sqcup \mathbb{P}\overline{\rho}_{f,\lambda}(\tau)C.$$

This decomposition is indeed disjoint because if we had $C \cap \mathbb{P}\overline{\rho}_{f,\lambda}(\tau)C \neq \emptyset$, we would get an element of the form $\tau\sigma_0^k$ in the kernel of $\mathbb{P}\overline{\rho}_{f,\lambda}$. Therefore, $\overline{\rho}_{f,\lambda}(\tau\sigma_0^k)$ would be scalar but because $\tau\sigma_0^k \notin G_K$ this is in contradiction with (14.2). Next, because $\tau^2 \in G_K$, we have

$$\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)^2 = \mathbb{P}\left(\beta^\tau(\tau^2) \oplus \beta(\tau^2)\right) = \mathbb{P}\left(\beta(\tau^2) \oplus \beta(\tau^2)\right) = \mathbb{P}I_2.$$

Therefore, $\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)$ has order 2 because it can not be trivial from (14.2). Finally, we have

$$\begin{aligned}
\mathbb{P}\overline{\rho}_{f,\lambda}(\tau\sigma_0\tau^{-1}) &= \mathbb{P}\left(\beta^\tau(\tau\sigma_0\tau^{-1}) \oplus \beta(\tau\sigma_0\tau^{-1})\right) \\
&= \mathbb{P}\left(\beta(\tau^2\sigma_0\tau^{-2}) \oplus \beta^\tau(\sigma_0)\right) \\
&= \mathbb{P}\left(\beta(\sigma_0) \oplus \beta^\tau(\sigma_0)\right) \\
&= \mathbb{P}\left(\beta^\tau(\sigma_0^{-1}) \oplus \beta(\sigma_0^{-1})\right).
\end{aligned}$$

The group $\mathbb{P}\overline{\rho}_{f,\lambda}(G_\mathbb{Q})$ is therefore generated by $\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)$ and $\mathbb{P}\overline{\rho}_{f,\lambda}(\sigma_0)$, with $\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)$ of order 2, $\mathbb{P}\overline{\rho}_{f,\lambda}(\sigma_0)$ of order n prime to ℓ, and such that $\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)\mathbb{P}\overline{\rho}_{f,\lambda}(\sigma_0)\mathbb{P}\overline{\rho}_{f,\lambda}(\tau)^{-1} = \mathbb{P}\overline{\rho}_{f,\lambda}(\sigma_0)^{-1}$. It is therefore dihedral of order prime to ℓ. ■

To refine this result, we look at the local properties of the possible characters ψ that leave $\overline{\rho}_{f,\lambda}$ invariant by twisting. We first state a lemma that is a general property of Dirichlet characters.

Lemma 14.5. *Let ψ be a quadratic primitive Dirichlet character of conductor $\mathfrak{c}_\psi$ and let p be a prime number dividing $\mathfrak{c}_\psi$. If p is odd, then $v_p(\mathfrak{c}_\psi) = 1$, and if $p = 2$, then $v_2(\mathfrak{c}_\psi) \in \{1, 2, 3\}$.*

Proof. Write n_p the p-adic valuation of $\mathfrak{c}_\psi$. Assume first that p is odd. The group $(\mathbb{Z}/p^{n_p}\mathbb{Z})^\times$ is cyclic. Let x be any generator. Since ψ is quadratic, the kernel of ψ_p contains $\langle x^2\rangle$, and the kernel of the projection $(\mathbb{Z}/p^{n_p}\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ is $\langle x^{p-1}\rangle \supseteq \langle x^2\rangle$. As ψ is primitive, we need to have $n_p = 1$.

Similarly, the group $(\mathbb{Z}/2^{n_2}\mathbb{Z})^\times$ is generated by -1 and 5 and the kernel of ψ_2 contains $\langle 5^2\rangle$. Moreover, if $n_p \geqslant 3$, the kernel of the projection $(\mathbb{Z}/2^{n_2}\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ is $\langle 5^2\rangle$. It follows that $n_2 \leqslant 3$. ■

Using the knowledge of the local shape of $\overline{\rho}_{f,\lambda}$ given by proposition 10.17, we now deduce local properties that the possible twists ψ may satisfy. It is similar to lemma 13.5.

Proposition 14.6. *Assume $\overline{\rho}_{f,\lambda}$ has projective dihedral image of order prime to ℓ and let ψ be a quadratic character of $G_{\mathbb{Q}}$ such that $\overline{\rho}_{f,\lambda} \cong \psi \otimes \overline{\rho}_{f,\lambda}$. Write $\mathfrak{c}_\psi$ for its conductor and let p be a prime number.*

1. *If p is odd then $v_p(\mathfrak{c}_\psi) \leqslant 1$ and if $p = 2$ then $v_2(\mathfrak{c}_\psi) \leqslant 3$..*
2. *If $p \nmid N\ell$, then $p \nmid \mathfrak{c}_\psi$ and $a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$.*
3. *If $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, then ψ is unramified at p and either $\psi(p) = 1$, or $\psi(p) = -1 \equiv p \pmod{\lambda}$.*
4. *If $p \mid N$, $p \neq \ell$, and $v_p(N) = v_p(\mathfrak{c})$, then either ψ is unramified at p and $\psi(p) = 1$, or ψ is ramified at p, $\psi_p \equiv \varepsilon_p^{-1} \pmod{\lambda}$, and $a_p(f)^2 \equiv p^{k-1}\psi'_p(p)\varepsilon'_p(p) \pmod{\lambda}$, where ψ_p and ε_p denote the p-parts of ψ and ε respectively, and ψ'_p and ε'_p denote the prime-to-p part of ψ and ε respectively.*

   In particular, in the second case ε_p has order 2 modulo λ.
5. *If $v_2(N) \in \{2, 3\}$ and $v_2(\mathfrak{c}) < v_2(N)$, then $v_2(\mathfrak{c}_\psi) \leqslant 2$.*

Proof. 1. It follows immediately from lemma 14.5.

2. The representation $\overline{\rho}_{f,\lambda}$ is unramified outside $N\ell$. Therefore, as $\overline{\rho}_{f,\lambda} \cong \psi \otimes \overline{\rho}_{f,\lambda}$, the character ψ is necessarily unramified outside $N\ell$ too. Moreover, looking at the trace at Frob_p, we have $a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$ for all $p \nmid N\ell$.

3. Assume that $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$. By proposition 10.17 and the assumption, we have

$$\overline{\rho}_{f,\lambda}|_{G_p} \cong \begin{pmatrix} \mu(a_p(f)) & \star \\ 0 & \mu(pa_p(f)) \end{pmatrix} \cong \begin{pmatrix} \psi|_{G_p}\mu(a_p(f)) & \star \\ 0 & \psi|_{G_p}\mu(pa_p(f)) \end{pmatrix} \cong \psi \otimes \overline{\rho}_{f,\lambda}|_{G_p}.$$

   Therefore, we have an equality of sets of characters of G_p:

$$\{\mu(a_p(f)), \mu(pa_p(f))\} = \left\{\psi|_{G_p}\mu(a_p(f)), \psi|_{G_p}\mu(pa_p(f))\right\}.$$

   We deduce that ψ needs to be unramified at p and we have an equality of sets of elements of $\mathbb{F}_\lambda$,

$$\left\{\overline{a_p(f)}, \overline{pa_p(f)}\right\} = \left\{\overline{\psi(p)a_p(f)}, \overline{p\psi(p)a_p(f)}\right\}.$$

   By proposition 10.16, the coefficient $a_p(f)$ is invertible modulo λ. Therefore, we either have $\psi(p) = 1$, or $\psi(p) = -1$ and $\psi(p) \equiv p \pmod{\lambda}$.

4. If $p \mid N$, $p \neq \ell$, and $v_p(N) = v_p(\mathfrak{c})$, then from proposition 10.17 and the assumption, we have

$$\begin{aligned} \overline{\rho}_{f,\lambda}|_{G_p} &\cong \mu(a_p(f)) \oplus \mu(p^{k-1}a_p(f)^{-1})\overline{\varepsilon}|_{G_p} \\ &\cong \mu(a_p(f))\psi|_{G_p} \oplus \mu(p^{k-1}a_p(f)^{-1})\,(\psi\overline{\varepsilon})\,|_{G_p} \cong \psi \otimes \overline{\rho}_{f,\lambda}|_{G_p}. \end{aligned} \tag{14.3}$$

We deduce again an equality of sets of characters of G_p:

$$\{\mu(a_p(f)), \mu(p^{k-1}a_p(f)^{-1})\overline{\varepsilon}|_{G_p}\} = \{\mu(a_p(f))\psi|_{G_p}, \mu(p^{k-1}a_p(f)^{-1})(\psi\overline{\varepsilon})|_{G_p}\}.$$

If $\mu(a_p(f)) = \mu(a_p(f))\psi|_{G_p}$, then ψ is unramified at p we get $\psi(p) = 1$ because $a_p(f)$ is invertible modulo λ by proposition 10.16. Otherwise, ψ is ramified at p and $\psi\overline{\varepsilon}$ needs to be unramified at p. We deduce that $\psi_p \equiv \varepsilon_p^{-1} \pmod{\lambda}$, the value of $\psi\overline{\varepsilon}$ at Frob_p is equal to $\psi'_p(p)\varepsilon'_p(p) \pmod{\lambda}$, and

$$a_p(f) \equiv p^{k-1}a_p(f)^{-1}\psi'_p(p)\varepsilon'_p(p) \pmod{\lambda}.$$

5. First notice that $\psi \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f\otimes\psi,\lambda}$. We can prove this by looking at the trace of both representations at Frobenius elements at the primes $p \nmid N\ell$ and using theorem 10.1. Write $N_{f\otimes\psi}$ for the level of $f \otimes \psi$. Since $\overline{\rho}_{f,\lambda}$ and $\overline{\rho}_{f\otimes\psi,\lambda}$ are isomorphic their Artin conductor $N(\overline{\rho}_{f,\lambda})$ and $N(\psi \otimes \overline{\rho}_{f,\lambda})$ are equal. We find using proposition 10.12 that for any prime p,

$$v_p(N_{f\otimes\psi}) \leqslant v_p(N(\psi \otimes \overline{\rho}_{f,\lambda})) + 2 = v_p(N(\overline{\rho}_{f,\lambda})) + 2 \leqslant v_p(N) + 2. \tag{14.4}$$

Assume that $v_2(N) \in \{2, 3\}$ and $v_2(\mathfrak{c}) < v_2(N)$. If $v_2(\mathfrak{c}_\psi) > 3$, we get from the last point of proposition 14.1 that

$$v_2(N_{f\otimes\psi}) = v_2(\mathrm{lcm}(N, \mathfrak{c}_\psi^2, \mathfrak{c}\mathfrak{c}_\psi)) = 2v_2(\mathfrak{c}_\psi) > v_2(N) + 2.$$

This is in contradiction with (14.4) and therefore $v_2(\mathfrak{c}_\psi) \leqslant 2$ in this case.

■

We can now define a set that characterises the possible characters ψ for which could have $\overline{\rho}_{f,\lambda} \cong \psi \otimes \overline{\rho}_{f,\lambda}$. This is the dihedral counterpart of the set $R_{N,k,\varepsilon}(\mathfrak{L})$ of definition 13.1 in the reducible case.

Definition 14.7. *Let $T_{N,\varepsilon}(\lambda)$ be the set of pairs (e, ψ) with $e \in \{0, 1\}$ and ψ a primitive Dirichlet character of order less or equal to 2 such that $(e, \psi) \neq (0, \mathbb{1})$ and*

- *The character ψ is unramified outside N and unramified at ℓ;*
- *For a prime p such that $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, the character ψ is unramified at p and either $p^{e\frac{\ell-1}{2}}\psi(p) \equiv 1 \pmod{\ell}$, or $p^{e\frac{\ell-1}{2}}\psi(p) \equiv p \equiv -1 \pmod{\ell}$;*
- *For a prime p such that $p \mid N$, $p \neq \ell$, and $v_p(N) = v_p(\mathfrak{c})$, either ψ is unramified at p and $p^{e\frac{\ell-1}{2}}\psi(p) \equiv 1 \pmod{\ell}$, or ψ is ramified at p and $\psi_p \equiv \varepsilon_p^{-1} \pmod{\lambda}$;*
- *If $v_2(N) \in \{2, 3\}$ and $v_2(\mathfrak{c}) < v_2(N)$, then the conductor of ψ_2 is strictly less than 8.*

Combining propositions 14.4 and 14.6, we deduce a first characterisation of the dihedral case in terms of congruences.

Corollary 14.8. *The representation $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ if and only if there exists $(e, \psi) \in T_{N,\varepsilon}(\lambda)$ such that the following congruences hold for all prime numbers p in a set of density one.*

- *If* $p \nmid N\ell$, *then* $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$;
- *If* $p \mid N$, $p \neq \ell$, $v_p(N) = v_p(\mathfrak{c})$, *and the character* ψ *is ramified at* p, *then* $a_p(f)^2 \equiv p^{e\frac{\ell-1}{2}+k-1}\psi'_p(p)\varepsilon'_p(p) \pmod{\lambda}$.

Proof. First assume that there exists $(e,\psi) \in T_{N,\varepsilon}(\lambda)$ such that the congruences of the corollary hold. From theorem 10.1, the congruences $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$ for $p \nmid N\ell$ imply the isomorphism $\overline{\rho}_{f,\lambda} \cong \left(\overline{\chi}_\ell^{e\frac{\ell-1}{2}}\overline{\psi}\right) \otimes \overline{\rho}_{f,\lambda}$. Moreover, it follows from the definition of $T_{N,\varepsilon}(\lambda)$ that the character $\overline{\chi}_\ell^{e\frac{\ell-1}{2}}\overline{\psi}$ is quadratic. From proposition 14.4, $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ.

Conversely, assume that $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ. By proposition 14.4, there exists a quadratic character η such that $\eta \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f,\lambda}$. Let us decompose η as $\eta_\ell \cdot \eta'_\ell$, with η_ℓ ramified only at ℓ, and η'_ℓ unramified at ℓ. As η is quadratic, so are η_ℓ and η'_ℓ. Therefore, either η_ℓ is trivial, or $\eta_\ell = \overline{\chi}_\ell^{\frac{\ell-1}{2}}$. We can thus write η_ℓ as $\overline{\chi}_\ell^{e\frac{\ell-1}{2}}$ with $e \in \{0,1\}$. Let ψ be the Teichmüller lift of η'_ℓ with respect to λ (see section 10.2.2). From proposition 14.6, the pair (e,ψ) lies in the set $T_{N,\varepsilon}(\lambda)$ and the announced congruences hold. ∎

Our goal is now to refine corollary 14.8 in a way that requires checking only a finite number of congruences. Let $(e,\psi) \in T_{N,\varepsilon}(\lambda)$ and denote by $\mathfrak{c}_\psi$ the conductor of ψ. We construct a new Dirichlet character from ψ that will be better suited for our study. Let $\widetilde{\psi}$ be the Dirichlet character that is unramified outside $\mathfrak{c}_\psi$ and such that for a prime $p \mid \mathfrak{c}_\psi$,

$$\widetilde{\psi}_p = \begin{cases} \varepsilon_p^{-1} & \text{if } p \mid N,\ p \neq \ell \text{ and, } v_p(N) = v_p(\mathfrak{c}); \\ \psi_p & \text{otherwise.} \end{cases} \tag{14.5}$$

Notice that from the definition of $T_{N,\varepsilon}(\lambda)$, we have $\widetilde{\psi} \equiv \psi \pmod{\lambda}$ because at the primes p for which we have modified ψ_p, we have $\widetilde{\psi}_p = \varepsilon_p^{-1} \equiv \psi_p \pmod{\lambda}$. Moreover, for the primes p for which we have not modified ψ, the p-adic valuation of the conductor of $\widetilde{\psi}$ is the same as the p-adic valuation of $\mathfrak{c}_\psi$. We now define a modular form g by

$$g := f \otimes \widetilde{\psi}. \tag{14.6}$$

From proposition 14.1 we deduce the following result.

Proposition 14.9. *The modular form* g *has integral Fourier coefficients and is a normalised eigenform of weight* k, *level* N_g, *and character* $\widetilde{\psi}^2\varepsilon$. *Let* p *be a prime number.*

1. *If* $p \nmid N$ *or* $p = \ell$, *then* $a_p(g) = \widetilde{\psi}(p)a_p(f)$ *and* $v_p(N_g) = v_p(N)$;
2. *If* $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, *and* $v_p(\mathfrak{c}) = 0$, *then* $a_p(g) = \widetilde{\psi}(p)a_p(f)$ *and* $v_p(N_g) = v_p(N)$;
3. *If* $p \mid N$, $p \neq \ell$, *and* $v_p(N) = v_p(\mathfrak{c})$, *then* $v_p(N_g) = v_p(N)$. *Moreover, if* ψ *is unramified at* p, *then* $a_p(g) = \widetilde{\psi}(p)a_p(f)$, *and otherwise* $a_p(g) = \overline{a_p(f)}(\widetilde{\psi}\varepsilon)_0(p)$;
4. *If* $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, *and* $v_p(N) > v_p(\mathfrak{c})$, *then if* p *is odd, we have* $v_p(N_g) \leqslant v_p(N)$, *and if* $p = 2$, *we have* $v_2(N_g) \leqslant v_2(N) + 2$.

In particular we have $N_g \mid N \cdot \gcd(N,2)^2$.

Proof. The formula for the weight and the character of g follow from proposition 14.1. Let p be a prime number.

1. If $p \nmid N$ or if $p = \ell$, then from the definition of $T_{N,\varepsilon}(\lambda)$ the character $\widetilde{\psi}$ is unramified at p. Therefore, by proposition 14.1 the p-adic parts of the levels of g and f are the same and $a_p(g) = \widetilde{\psi}(p)a_p(f)$.

2. If $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, then the character $\widetilde{\psi}$ is also unramified at p and the result follows just as before.

3. If $p \mid N$, $p \neq \ell$, and $v_p(N) = v_p(\mathfrak{c})$, then from the definition of $\widetilde{\psi}$ either ψ is unramified at p and $\widetilde{\psi}$ is too, or ψ is ramified at p and $\widetilde{\psi}_p = \varepsilon_p^{-1}$. In both cases the result follows from proposition 14.1.

4. Finally, assume that $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, and $v_p(N) > v_p(\mathfrak{c})$. If p is odd, then from proposition 14.6.1 we have $v_p(\mathfrak{c}_\psi) = 1$ and from proposition 14.1 deduce

$$v_p(N_g) \leqslant \max(v_p(N), 2v_p(\mathfrak{c}_\psi), v_p(\mathfrak{c}_\psi) + v_p(\mathfrak{c})) = \max(v_p(N), 2, v_p(\mathfrak{c}) + 1) = v_p(N).$$

   If now $p = 2$, we have $v_2(\mathfrak{c}_\psi) \in \{0, 2, 3\}$ from proposition 14.6.1. By the same computation as above, we have $v_2(N_g) \leqslant \max(v_2(N), 2v_2(\mathfrak{c}_\psi), v_2(\mathfrak{c}_\psi\mathfrak{c}))$. If $v_2(N) \in \{2, 3\}$, we have $v_2(\mathfrak{c}_\psi) \leqslant 2$ by definition 14.7 and we deduce $v_2(N_g) \leqslant v_2(N) + 2$. If $v_2(N) \geqslant 4$, we have

$$v_2(N_g) \leqslant \max(v_2(N), 6, v_2(\mathfrak{c}) + 3) \leqslant v_2(N) + 2.$$

■

Before we get to the main result of this section we need to modify the form g slightly in order to get congruences at the primes $p \mid N$, $p \neq \ell$ lacking a suitable congruence. The following result solves this issue.

Proposition 14.10. *Let g be the modular form defined in (14.6) and consider two sets of primes $\mathbf{P}_1$, $\mathbf{P}_2$ such that*

$$\begin{aligned} &\mathbf{P}_1 \subseteq \{p \mid N,\ p \neq \ell,\ v_p(N) = 1 \text{ and } v_p(\mathfrak{c}) = 0\}, \\ \text{and} \quad &\mathbf{P}_2 \subseteq \{p \mid N,\ p \neq \ell,\ v_p(N) \geqslant 2 \text{ and } v_p(\mathfrak{c}) < v_p(N)\}. \end{aligned}$$

Define $\mathbf{P} := \mathbf{P}_1 \cup \mathbf{P}_2$ and, with the notations of corollary 12.29,

$$h := g_{\mathbf{P}}^{(0)_{p\in\mathbf{P}}}.$$

The form h has integral Fourier coefficients and is of weight k and character $\widetilde{\psi}^2\varepsilon$. Its level N_h satisfies $N_h \mid N' := N\gcd(N,2)^2 \prod_{p\in\mathbf{P}_1} p$ and has the same prime factors as N. It is a normalised eigenform for all the Hecke operators $T_p^{N'}$ except maybe at the primes p such that $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, $v_p(N) > v_p(\mathfrak{c})$ and $p \notin \mathbf{P}_2$. Finally, for any prime number p we have

$$a_p(h) = \begin{cases} a_p(g) & \text{if } p \notin \mathbf{P}; \\ 0 & \text{if } p \in \mathbf{P}. \end{cases}$$

Proof. Everything follows directly from corollary 12.29 and proposition 14.9 except the assertions about the level of h. The level of h may differ from the level of g only at the primes in $\mathbf{P}$. Write N_h and N_g for the levels of h and g respectively and let $p \in \mathbf{P}$.

If $p \in \mathbf{P}_1$, then from proposition 14.9 we have $v_p(N_g) = v_p(N) = 1$, and $a_p(g) = \widetilde{\psi}(p)a_p(f) \neq 0$ from proposition 10.16. Therefore $v_p(N_h) = v_p(N_g) + 1 = v_p(N) + 1$ from corollary 12.29.

If $p \in \mathbf{P}_2$, then we have $v_p(N) \geqslant 2$ and $v_p(\mathfrak{c}) < v_p(N)$.

- If $a_p(g) = 0$, then we have $v_p(N_h) = v_p(N_g)$ and the result follows in this case from proposition 14.9.
- If $a_p(g) \neq 0$ and $v_p(N_g) = 0$, then $v_p(N_h) = 2 \leqslant v_p(N)$.
- Finally, if $a_p(g) \neq 0$ and $v_p(N_g) > 0$, then we get $v_p(N_h) = v_p(N_g) + 1$. If $v_p(N_g) = 1$, then we have $v_p(N_h) = 2 \leqslant v_p(N)$. Otherwise, by proposition 10.16 the p-adic valuation of N_g is necessarily equal to the p-adic valuation of the conductor of $\widetilde{\psi}^2\varepsilon$. As the p-part of $\widetilde{\psi}^2\varepsilon$ is equal to ε_p in this case, we get $v_p(N_h) = v_p(N_g) + 1 = v_p(\mathfrak{c}) + 1 \leqslant v_p(N)$.

To conclude, it follows from proposition 14.9 that N_h has the same prime factors as $N' := N \gcd(N, 2)^2 \prod_{p \in \mathbf{P}_1} p$, except maybe for the primes p such that $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, $v_p(\mathfrak{c}) < v_p(N)$, and $p \notin \mathbf{P}_2$. Therefore, from lemma 12.24 it is also an eigenform for the Hecke operators at this level. ∎

Remark 14.11. *The modular form h in the previous proposition is an eigenform for all the Hecke operators at its level N_h but not necessarily for all the Hecke operators at level N'. Indeed, the p-adic valuation of N_h and N' may not be the same for the primes p not in the set $\mathbf{P}_2$ but such that $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, and $v_p(N) > v_p(\mathfrak{c})$.*

We now prove the main result of this chapter. We give a finite list of explicit congruences that suffice to prove that a given modular representation is dihedral.

Theorem 14.12. *The following are equivalent.*

1. *The representation $\overline{\rho}_{f,\lambda}$ has projective dihedral image of order prime to ℓ;*
2. *There exists $(e, \psi) \in T_{N,\varepsilon}(\lambda)$ such that the following holds. Define the set*

$$\mathbf{P}_1 := \left\{ p \text{ prime}, \ p \mid N, \ p \neq \ell, v_p(N) = 1, \ v_p(\mathfrak{c}) = 0, \text{ and } \psi(p)p^{e\frac{\ell-1}{2}} \equiv -1 \pmod{\ell} \right\}$$

and

$$a := \begin{cases} 4 & \text{if } \ell = 3 \text{ and } \forall p \mid N, \ p \equiv 1 \pmod 9; \\ 0 & \text{otherwise,} \end{cases} \qquad b := \begin{cases} 3 & \text{if } \ell \mid N; \\ \ell + 1 & \text{if } \ell \nmid N. \end{cases}$$

Let $B := \dfrac{N \gcd(2, N)^2 \left(k + a + b\left(1 + e\frac{\ell-1}{2}\right)\right)}{12} \prod_{p \in \mathbf{P}_1} p \prod_{p \mid N} \left(1 + \dfrac{1}{p}\right)$. For every prime $p \leqslant B$, we have

- $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$ *if* $p \nmid N\ell$;

- $a_p(f)^2 \equiv p^{e\frac{\ell-1}{2}+k-1}(\psi\varepsilon)'_p(p) \pmod{\lambda}$ *if* $p \mid N$, $p \neq \ell$, $v_p(N) = v_p(\mathfrak{c})$, *and* ψ *is ramified at* p.

Proof. The implication $1 \Rightarrow 2$ follows directly from corollary 14.8. Assume that the second part of the theorem holds. We define the set

$$\mathbf{P}_2 := \{p \text{ prime}, p \leqslant B,\ p \mid N,\ p \neq \ell,\ v_p(N) \geqslant 2,\ v_p(N) > v_p(\mathfrak{c})\},$$

and $\mathbf{P} := \mathbf{P}_1 \cup \mathbf{P}_2$. Let $\widetilde{\psi}$ be defined as in (14.5) and put

$$h := \left(f \otimes \widetilde{\psi}\right)_{\mathbf{P}}^{(0)_{p\in\mathbf{P}}} \quad \text{and} \quad f' := f_{\mathbf{P}_1}^{(0)_{p\in\mathbf{P}_1}}.$$

We claim that, with the notations of section 12.1, the modular forms $\widetilde{\theta}^{1+e\frac{\ell-1}{2}}h$ and $\widetilde{\theta}f'$ are congruent modulo λ. To prove this, let us check that the hypotheses of corollary 12.19 are satisfied by the forms f' and h, and the integers $m_f = 1$, and $m_g = 1 + e\frac{\ell-1}{2}$.

From proposition 14.10 and corollary 12.29, the forms h and f' are of weight k, character $\widetilde{\psi}^2\varepsilon$ and ε respectively, and level $N_h \mid N\gcd(2,N)^2 \prod_{p\in\mathbf{P}_1} p$ and $N \prod_{p\in\mathbf{P}_1} p$ respectively. Moreover, h and f' are both normalised eigenforms at level $N\gcd(2,N)^2 \prod_{p\in\mathbf{P}_1} p$. Next, by construction we have $\widetilde{\psi}^2 \equiv \psi^2 \equiv \mathbb{1} \pmod{\lambda}$. Therefore, we have

$$\overline{\chi}_\ell^{k+2\left(1+e\frac{\ell-1}{2}\right)}\widetilde{\psi}^2\varepsilon \equiv \overline{\chi}_\ell^{k+2}\varepsilon \pmod{\lambda}.$$

To apply corollary 12.19 we finally need to check that $pa_p(f') \equiv p^{1+e\frac{\ell-1}{2}}a_p(h) \pmod{\lambda}$ for all prime numbers $p \leqslant B$. Let p be a prime number less than or equal to B.

- If $p = \ell$, then we have $p^{1+e\frac{\ell-1}{2}}a_p(h) \equiv 0 \equiv pa_p(f') \pmod{\lambda}$.
- If $p \nmid N\ell$, then we have $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \equiv p^{e\frac{\ell-1}{2}}\widetilde{\psi}(p)a_p(f) \pmod{\lambda}$ by assumption, and from propositions 14.9 and 14.10, we deduce that
$$p^{1+e\frac{\ell-1}{2}}a_p(h) = p^{1+e\frac{\ell-1}{2}}\widetilde{\psi}(p)a_p(f) \equiv pa_p(f) \equiv pa_p(f') \pmod{\lambda}.$$
- If $p \mid N$, $p \neq \ell$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, then if $p \in \mathbf{P}_1$, we have from corollary 12.29, $pa_p(f') = 0 = p^{1+e\frac{\ell-1}{2}}a_p(h)$. If $p \notin \mathbf{P}_1$, we have from the definition of $T_{N,\varepsilon}(\lambda)$, $\widetilde{\psi}(p)p^{e\frac{\ell-1}{2}} \equiv \psi(p)p^{e\frac{\ell-1}{2}} \equiv 1 \pmod{\lambda}$. We then get
$$\begin{aligned} p^{1+e\frac{\ell-1}{2}}a_p(h) &= p^{1+e\frac{\ell-1}{2}}a_p\left(f \otimes \widetilde{\psi}\right) && \text{from proposition 14.10} \\ &= p^{1+e\frac{\ell-1}{2}}\widetilde{\psi}(p)a_p(f) && \text{from proposition 14.9} \\ &\equiv pa_p(f) \pmod{\lambda}. \end{aligned}$$
- If $p \mid N$, $p \neq \ell$, and $v_p(N) = v_p(\mathfrak{c})$, then either ψ is unramified at p and because ψ and $\widetilde{\psi}$ are congruent modulo λ we have $p^{e\frac{\ell-1}{2}}\widetilde{\psi}(p) \equiv p^{e\frac{\ell-1}{2}}\psi(p) \equiv 1 \pmod{\ell}$, or ψ is ramified at p. In the first case we have from propositions 14.9 and 14.10,
$$p^{1+e\frac{\ell-1}{2}}a_p(h) = p^{1+e\frac{\ell-1}{2}}\psi(p)a_p(f) \equiv pa_p(f) = pa_p(f') \pmod{\lambda}.$$

In the second case, we have $a_p(h) = \overline{a_p(f)}(\widetilde{\psi\varepsilon})_0(p) \equiv \overline{a_p(f)}(\psi\varepsilon)'_p(p) \pmod{\lambda}$ from propositions 14.9 and 14.10 again. Therefore, since $\overline{a_p(f)} = a_p(f)^{-1}p^{k-1}$ from proposition 10.16, we deduce from the assumption that

$$p^{1+e\frac{\ell-1}{2}}a_p(h) \equiv a_p(f)^{-1}p^{k+e\frac{\ell-1}{2}}(\psi\varepsilon)'_p(p) \equiv pa_p(f) = pa_p(f') \pmod{\lambda}.$$

- Finally if $p \mid N$, $p \neq \ell$, $v_p(N) \geqslant 2$, and $v_p(N) > v_p(\mathfrak{c})$, then from proposition 10.16 and corollary 12.29 we have $p^{1+e\frac{\ell-1}{2}}a_p(h) = 0 = pa_p(f) = pa_p(f')$.

Therefore, corollary 12.19 applies and for every prime p, we have $p^{1+e\frac{\ell-1}{2}}a_p(h) \equiv pa_p(f') \pmod{\lambda}$. In particular, for every prime $p \nmid N\ell$, we have

$$a_p(f) \equiv p^{e\frac{\ell-1}{2}}a_p(h) = p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}.$$

From corollary 14.8, we deduce that $\overline{\rho}_{f,\lambda}$ has projective dihedral image. ■

Remark 14.13. *As theorem 13.12, theorem 14.12 applies with no restriction on the prime ideal λ. It can therefore be used to check if any representation $\overline{\rho}_{f,\lambda}$ has dihedral projective image or not. For example, one can recover the example [BD14, §5.2] with tools coming only from the theory of modular forms. See section 15.2 for more details.*

14.2 Dihedral modular representations in big characteristic

Theorem 14.12 applies for every prime ideal λ in $\mathcal{O}_f$, but the bound for the number of prime index coefficients depends on ℓ. Under some assumptions on ℓ, we remove this dependency. We first get rid of ℓ in the definition of $T_{N,\varepsilon}(\lambda)$ by looking at the shape of $\overline{\rho}_{f,\lambda}$ at ℓ. A result similar the following one can be found in [BD14, Proposition 3.3].

Proposition 14.14. *Let ψ be a quadratic character such that $\psi \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f,\lambda}$. Assume further that $\ell \geqslant k-1$ and $\ell \nmid N$.*

1. *If f is ordinary at λ, then either ψ is unramified at ℓ and $\psi(\ell) = 1$, or ψ is ramified at ℓ, $\ell = 2k-1$ and $a_\ell(f)^2 \equiv \psi'_\ell(\ell)\varepsilon(\ell) \pmod{\lambda}$;*
2. *If f is not ordinary at λ, then either $\ell = 2k-3$, or ψ is unramified at ℓ.*

Proof. We are under the hypotheses of proposition 10.14. In its notations we are in one of the following two cases.

- If f is ordinary at λ, then we have

$$\begin{aligned}\overline{\rho}_{f,\lambda}|_{G_\ell} &\cong \begin{pmatrix} \overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right) & \star \\ 0 & \mu(a_\ell(f))\end{pmatrix} \\ &\cong \begin{pmatrix} \psi|_{G_\ell}\overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right) & \star \\ 0 & \psi|_{G_\ell}\mu(a_\ell(f))\end{pmatrix} \cong \psi \otimes \overline{\rho}_{f,\lambda}|_{G_\ell}.\end{aligned}$$

Therefore, we have an equality of characters of G_ℓ:

$$\left\{\overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right), \mu(a_\ell(f))\right\} = \left\{\psi|_{G_\ell}\overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right), \psi|_{G_\ell}\mu(a_\ell(f))\right\}.$$

If $\psi|_{G_\ell}\mu(a_\ell(f)) = \mu(a_\ell(f))$, then ψ is unramified at ℓ and $a_\ell(f) \equiv \psi(\ell)a_\ell(f) \pmod{\lambda}$. Otherwise, we have $\psi|_{G_\ell}\overline{\chi}_\ell^{k-1}\mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right) = \mu(a_\ell(f))$. Therefore, $\psi|_{G_\ell}\overline{\chi}_\ell^{k-1}$ is unramified, and the character ψ is ramified at ℓ and quadratic. We deduce that $\psi_\ell \equiv \overline{\chi}_\ell^{\frac{\ell-1}{2}} \pmod{\lambda}$ and $k-1 \equiv \frac{\ell-1}{2} \pmod{\ell-1}$. From the assumption $\ell \geqslant k-1$, we need to have $\ell = 2k-1$. Moreover, the value of $\psi|_{G_\ell}\overline{\chi}_\ell^{k-1}$ at Frob_ℓ is $\psi'_\ell(\ell)$, and we get $\psi'_\ell(\ell)\frac{\varepsilon(\ell)}{a_\ell(f)} \equiv a_\ell(f) \pmod{\lambda}$.

- If f is not ordinary at λ, then we have

$$\overline{\rho}_{f,\lambda}|_{I_\ell} \cong \begin{pmatrix}\phi^{k-1} & 0\\ 0 & \phi^{\ell(k-1)}\end{pmatrix} \cong \begin{pmatrix}\psi|_{I_\ell}\phi^{k-1} & 0\\ 0 & \psi|_{I_\ell}\phi^{\ell(k-1)}\end{pmatrix} \cong \psi \otimes \overline{\rho}_{f,\lambda}|_{I_\ell}.$$

This means that either $\phi^{k-1} = \psi|_{I_\ell}\phi^{k-1}$ or $\phi^{k-1} = \psi|_{I_\ell}\phi^{\ell(k-1)}$. In the first case, we get that ψ is unramified at ℓ. In the second case, ψ is ramified at ℓ and quadratic, therefore $\psi_\ell \equiv \overline{\chi}_\ell^{\frac{\ell-1}{2}} \equiv \phi^{(\ell+1)\frac{\ell-1}{2}} \pmod{\lambda}$. We deduce that $k-1$ is congruent to $\frac{\ell+1}{2}$ modulo $\ell+1$, and from the assumption $\ell \geqslant k-1$, we get $\ell = 2k-3$.

■

Proposition 14.14 tells us that under the assumption $\ell \geqslant k-1$, $\ell \nmid N$, and $\ell \notin \{2k-1, 2k-3\}$, the possible quadratic twists of $\overline{\rho}_{f,\lambda}$ are unramified at ℓ. This means that we no longer need the number e in $T_{N,\varepsilon}(\lambda)$ that encoded the ramification at ℓ.

Definition 14.15. *Let $T_{N,\varepsilon}$ be the set of quadratic Dirichlet characters ψ such that*

- *The character ψ is unramified outside N;*
- *For a prime p such that $p \mid N$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, ψ is unramified at p and $\psi(p) = 1$;*
- *For a prime p such that $p \mid N$ and $v_p(N) = v_p(\mathfrak{c})$, either ψ is unramified at p and $\psi(p) = 1$, or ψ is ramified at p and $\psi_p = \varepsilon_p^{-1}$.*

We now prove the second main theorem of this section.

Theorem 14.16. *Let ℓ be a prime number such that $\ell \geqslant k-1$, $\ell \notin \{2k-1, 2k-3\}$, $\ell \nmid N$, $\ell \nmid p+1$ for all primes p with $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, and $\ell \nmid p-1$ for all primes $p \mid N$ with $v_p(N) = v_p(\mathfrak{c})$. The following are equivalent.*

1. *The representation $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ.*
2. *There exists $\psi \in T_{N,\varepsilon}$ such that the following holds. Let $B := \frac{N\gcd(N,2)^2 k}{12}\prod_{p\mid N}\left(1+\frac{1}{p}\right)$. For every prime $p \leqslant B$, we have*
   - *$a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$ if $p \nmid N$;*

- $a_p(f)^2 \equiv p^{k-1}(\psi\varepsilon)_0(p) \pmod{\lambda}$ *if* $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$, *and* ψ *is ramified at* p.

Proof. Assume that $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ. Then, from corollary 14.8 there exists a pair $(e, \psi) \in T_{N,\varepsilon}(\lambda)$ such that $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$ for all primes $p \nmid N\ell$, and $a_p^2 \equiv p^{k-1+e\frac{\ell-1}{2}}\psi'_p(p)\varepsilon'_p(p) \pmod{\lambda}$ if $p \nmid N$, $p \neq \ell$, $v_p(N) = v_p(\mathfrak{c})$, and ψ is ramified at p. We have to prove that $e = 0$, $\psi \in T_{N,\varepsilon}$, and that $a_\ell(f) \equiv \psi(\ell)a_p(f) \pmod{\lambda}$.

For the first point, it follows from theorem 10.1 that $\left(\overline{\chi}_\ell^{e\frac{\ell-1}{2}}\psi\right) \otimes \overline{\rho}_{f,\lambda} \cong \overline{\rho}_{f,\lambda}$ and from proposition 14.14 we necessarily have $e = 0$. Let us prove that $\psi \in T_{N,\varepsilon}$. From the definition of $T_{N,\varepsilon}(\lambda)$, the character ψ is unramified outside N, at ℓ, and as $\ell \nmid N$, also at the primes p such that $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$. For a prime p such that $p \mid N$ and $v_p(N) = v_p(\mathfrak{c})$ either ψ is unramified at p and $\psi(p) = 1$, or ψ is ramified at p and $\psi_p \equiv \varepsilon_p^{-1} \pmod{\lambda}$. In the second case, the character $\psi_p\varepsilon_p$ is trivial modulo λ and therefore of order a power of ℓ by lemma 10.5. However, as we assumed $\ell \nmid N$, and $\ell \nmid q-1$ for all prime divisors q of N such that $v_q(N) = v_q(\mathfrak{c})$, ℓ does not divide the order of the group $\left(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}\right)^\times$. Therefore, $\psi_p\varepsilon_p$ is trivial and $\psi_p = \varepsilon_p^{-1}$. Finally, for a prime $p \mid N$ such that $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, we either have $\psi(p) = 1$ or $\psi(p) = -1 \equiv p \pmod{\ell}$. However, as we assume that $\ell \nmid q+1$ for all prime divisors q of N such that $v_q(N) = 1$ and $v_q(\mathfrak{c}) = 0$, the second case cannot occur. We conclude that $\psi \in T_{N,\varepsilon}$. Finally, from proposition 14.14, either f is ordinary, we have $\psi(\ell) = 1$ and therefore $a_\ell(f) = \psi(\ell)a_\ell(f)$, or f is not ordinary. In this second case we have $a_\ell(f) \equiv 0 \equiv \psi(\ell)a_\ell(f) \pmod{\lambda}$.

Assume now that the second part holds. We define the set

$$\mathbf{P}_2 := \{p \text{ prime such that } p \leqslant B, p \mid N, v_p(N) \geqslant 2, v_p(N) > v_p(\mathfrak{c})\},$$

and the modular form

$$h := (\psi \otimes f)_{\mathbf{P}_2}^{(0)_{p\in\mathbf{P}_2}}.$$

Let us apply corollary 12.19 to h, f, and $m_f = m_g = 0$. From propositions 14.9 and 14.10, h and f are modular forms of weight k, character ε, level $N_h \mid N' := N\gcd(N,2)^2$ and N respectively, and are normalised eigenforms for all the $T_p^{N'}$ for $p \leqslant B$. The assumption of corollary 12.19 on the characters is satisfied. Finally, we need to check the congruences $a_p(f) \equiv a_p(h) \pmod{\lambda}$ for all primes $p \leqslant B$. Let $p \leqslant B$ be a prime number.

- If $p \nmid N\ell$, then from propositions 14.9 and 14.10 and the assumption, we have
$$a_p(h) = \psi(p)a_p(f) \equiv a_p(f) \pmod{\lambda}.$$
- If $p = \ell$, then as ψ is unramified at ℓ we have from the assumption
$$a_\ell(h) = \psi(\ell)a_\ell(f) \equiv a_\ell(f) \pmod{\lambda}.$$
- If $p \mid N$, $v_p(N) = 1$, and $v_p(\mathfrak{c}) = 0$, then by assumption we have $\psi(p) = 1$. Thus, from propositions 14.9 and 14.10 we have $a_p(h) = \psi(p)a_p(f) = a_p(f)$.
- If $p \mid N$ and $v_p(N) = v_p(\mathfrak{c})$, then from propositions 14.9 and 14.10 we have $a_p(h) = \overline{a_p(f)}(\psi\varepsilon)_0(p) = p^{k-1}a_p(f)^{-1}(\psi\varepsilon)_0(p)$. Therefore, $a_p(h) \equiv a_p(f) \pmod{\lambda}$.

- Finally, if $p \mid N$, $v_p(N) \geqslant 2$, and $v_p(\mathfrak{c}) < v_p(N)$, then we have from propositions 10.16 and 14.10, $a_p(h) = 0 = a_p(f)$.

We therefore have $a_p(h) \equiv a_p(f) \pmod{\lambda}$ for all primes $p \leqslant B$. From corollary 12.19, we deduce that $a_p(h) \equiv a_p(f) \pmod{\lambda}$ for all primes p. In particular, for the primes $p \nmid N\ell$ we have

$$a_p(h) = \psi(p)a_p(f) \equiv a_p(f) \pmod{\lambda}.$$

As $(0, \psi) \in T_{N,\varepsilon}(\lambda)$, it follows from corollary 14.8 that $\overline{\rho}_{f,\lambda}$ has dihedral projective image. ■

From theorem 14.16 we can also deduce a bound for the dihedral primes in terms of N, k, ε, and the degree of K_f.

Theorem 14.17. *Assume $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ. If $N = 1$, then we have $\ell \leqslant k$ or $\ell \in \{2k-1, 2k-3\}$. Else, if $N > 1$ and f does not have complex multiplication, then we have*

$$\ell \leqslant \max\left(\frac{Nk}{3}\left(2\log\log(N) + 2.4\right), 25N^2\right)^{\frac{k-1}{2}[K_f:\mathbb{Q}]}.$$

Proof. Assume that $\overline{\rho}_{f,\lambda}$ has dihedral projective image of order prime to ℓ. From theorem 14.16, we either have $\ell \leqslant k-1$, $\ell \mid N$, $\ell \mid p-1$ for some prime $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$, $\ell \mid p+1$ for some prime $p \mid N$, $v_p(N) = 1$, $v_p(\mathfrak{c}) = 0$, $\ell \in \{2k-1, 2k-3\}$, or there exists $\psi \in T_{N,\varepsilon}$ such that

$$\ell \mid \gcd\left(\left(\mathrm{Norm}\left(a_p(f)\right)\right)_{\substack{p\leqslant B, p\nmid N,,\\ \psi(p)=-1}}, \left(\mathrm{Norm}\left(a_p(f)^2 - p^{k-1}(\varepsilon\psi)_0(p)\right)\right)_{\substack{p\leqslant B, p\mid N,\\ v_p(N)=v_p(\mathfrak{c})\\ p\mid \mathfrak{c}_\psi}}\right), \tag{14.7}$$

where $B := \frac{N\gcd(N,2)^2 k}{12}\prod_{p\mid N}\left(1+\frac{1}{p}\right)$. This greatest common divisor being understood as the gcd of all the quantities in brackets in the ring $\mathbb{Z}$.

If $N = 1$, then the set $T_{1,\mathbb{1}}$ contains only quadratic Dirichlet characters unramified outside 1. Therefore, $T_{1,\mathbb{1}}$ is empty and $\overline{\rho}_{f,\lambda}$ can have dihedral projective image only if $\ell \leqslant k-1$ or $\ell \in \{2k-1, 2k-3\}$. The result follows in this case.

Assume that $N > 1$. Using Deligne's bounds for the coefficients of a newform (see [Del74, Théorème 8.2]) and lemma 12.23, this means that for $p \leqslant B$ we have either.

$$\begin{aligned}
\ell \mid |\mathrm{Norm}(a_p(f))| &= \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} |\sigma(a_p(f))| \\
&\leqslant \left(2p^{\frac{k-1}{2}}\right)^{[K_f:\mathbb{Q}]} \\
&\leqslant \left(\frac{Nk}{3}\left(2\log\log(N) + 2.4\right)\right)^{\frac{k-1}{2}[K_f:\mathbb{Q}]},
\end{aligned}$$

or $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$, $p \mid \mathfrak{c}_\psi$, and

$$\begin{aligned}\ell \mid \left|\mathrm{Norm}\left(a_p(f)^2 - (\varepsilon\psi)_0(p)p^{k-1}\right)\right| &\leqslant \prod_{\sigma:K_f\hookrightarrow\mathbb{C}}\left(\left|\sigma\left(a_p(f)^2\right)\right| + p^{k-1}\right)\\ &\leqslant \left(5p^{k-1}\right)^{[K_f:\mathbb{Q}]}\\ &\leqslant \left(5N^{k-1}\right)^{[K_f:\mathbb{Q}]}.\end{aligned}$$

To conclude, we must prove that the quantity

$$\gcd\left(\left(\mathrm{Norm}\left(a_p(f)\right)\right)_{\substack{p\leqslant B, p\nmid N,\\ \psi(p)=-1}}, \left(\mathrm{Norm}\left(a_p(f)^2 - p^{k-1}(\varepsilon\psi)_0(p)\right)\right)_{\substack{p\leqslant B, p\mid N,\\ v_p(N)=v_p(\mathfrak{c})\\ p\mid\mathfrak{c}_\psi}}\right)$$

is non-zero. If it was the case, we would have,

- $a_p(f) = \psi(p)a_p(f)$, for all $p \leqslant B$ such that $p \nmid N$;
- and $a_p(f)^2 = (\psi\varepsilon)_0(p)p^{k-1}$, for all $p \leqslant B$, such that $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$, and $p \mid \mathfrak{c}_\psi$.

Define $\mathbf{P}_2 := \{p \text{ prime }, p \leqslant B, v_p(N) \geqslant 2, v_p(N) > v_p(\mathfrak{c})\}$, and $g := (f \otimes \psi)^{(0)_{p\in\mathbf{P}_2}}_{\mathbf{P}_2}$. From proposition 14.10, it is a modular form of weight k, level $N_g \mid N' := N\gcd(2, N)^2$, and character $\psi^2\varepsilon = \varepsilon$, and an eigenform for all the Hecke operators $T_p^{N'}$ for $p \leqslant B$, as well as f. Moreover, we have for all primes $p \leqslant B$,

- $a_p(g) = \psi(p)a_p(f) = a_p(f)$ if $p \nmid N$;
- $a_p(g) = \underbrace{\psi(p)}_{=1}a_p(f) = a_p(f)$ if $p \mid N$, $v_p(N) = 1$, $v_p(\mathfrak{c}) = 0$;
- $a_p(g) = \overline{a_p(f)}(\psi\varepsilon)_0(p) = a_p(f)^{-1}p^{k-1}(\psi\varepsilon)_0(p) = a_p(f)$, if $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$ and $p \mid \mathfrak{c}_\psi$;
- $a_p(g) = \underbrace{\psi(p)}_{=1}a_p(f) = a_p(f)$, if $p \mid N$, $v_p(N) = v_p(\mathfrak{c})$ and $p \nmid \mathfrak{c}_\psi$;
- $a_p(g) = 0 = a_p(f)$, if $p \mid N$, $v_p(N) \geqslant 2$, $v_p(N) > v_p(\mathfrak{c})$.

We deduce from corollary 12.22 that $g = f$. It follows that $a_p(f) = \psi(p)a_p(f)$ for all primes $p \nmid N$, and that f must have CM. This concludes the proof. ■

14.3 Checking the dihedrality

We explain in this section how to use theorems 14.12 and 14.16 to explicitly compute, given a modular newform f, the exact set of prime ideals of $\mathcal{O}_f$ for which $\mathbb{P}\overline{\rho}_{f,\lambda}(G_\mathbb{Q})$ is a dihedral group of order prime to ℓ. We begin by what we would call "the small potentially dihedral primes". For a practical use, we make the following definition.

Definition 14.18. *A prime number ℓ is said to be a small potentially dihedral prime for f, if it satisfies at least of the following conditions:*

- $\ell \leqslant k-2$;
- $\ell \mid N$;
- $\ell \mid p+1$ *for some prime* $p \mid N$ *with* $v_p(N)=1$ *and* $v_p(\mathfrak{c})=0$;
- $\ell \mid p-1$ *for some prime* $p \mid N$ *with* $v_p(N)=v_p(\mathfrak{c})$;
- $\ell \in \{2k-1, 2k-3\}$.

The small potentially dihedral primes are those which do not satisfy the hypotheses of theorem 14.16.

For the small potentially dihedral primes, we apply theorem 14.12. Notice that the computation of the set $T_{N,\varepsilon}(\lambda)$ makes no difficulty as it involves only computations of Dirichlet characters modulo N and congruences involving rational integers.

Algorithm 14.19. ***Input**: A newform f, described by its Fourier coefficients $(a_n(f))_{n\geqslant 0}$ as elements of the number field K_f, together with its level N, weight k, and character ε.*
***Output**: The set of prime ideals λ of $\mathcal{O}_f$ which residual characteristic is a small dihedral prime and such that $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}})$ is a dihedral group of order prime to ℓ.*

1. *Set* $\mathrm{Dih}(f)=\emptyset$.
2. *Compute the set P of small potentially dihedral primes (see definition 14.18).*
3. *For each $\ell \in P$, compute the set $P(\ell)$ of prime ideals λ in $\mathcal{O}_f$ above ℓ.*
4. *For each $\ell \in P$ and for each $\lambda \in P(\ell)$, compute the set $T_{N,\varepsilon}(\lambda)$ (see definition 14.7).*
5. *For each $\ell \in P$, for each $\lambda \in P(\ell)$, and for each $(\psi, e) \in T_{N,\varepsilon}(\lambda)$,*
   (a) *Compute the bound B defined in theorem 14.12.*
   (b) *For all prime number $p \nmid N\ell$, $p \leqslant B$, check the congruence $a_p(f) \equiv p^{e\frac{\ell-1}{2}}\psi(p)a_p(f) \pmod{\lambda}$.*
   (c) *For all prime numbers $p \mid N$, $p \neq \ell$, $p \leqslant B$, such that $v_p(N)=v_p(\mathfrak{c})$ and ψ is ramified at p, check that congruence $a_p(f)^2 \equiv p^{k-1+e\frac{\ell-1}{2}}(\psi\varepsilon)'_p(p) \pmod{\lambda}$.*
   (d) *If they all hold, add λ to $\mathrm{Dih}(f)$. The representation $\overline{\rho}_{f,\lambda}$ has projective dihedral image of order prime to ℓ.*
6. *Return* $\mathrm{Dih}(f)$.

For the big prime numbers – that is the ones that are not small according to definition 14.18 – we proceed mainly as in the reducible case. The bound of theorem 14.17 is impractical for computations, and examples suggest that it is much bigger compared to the effective dihedral

prime numbers. We can instead use the characterisation given by theorem 14.16: if $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}})$ is dihedral for a prime ideal above a big prime number ℓ, then there exists $\psi \in T_{N,\varepsilon}$ such that

$$\ell \mid \gcd\left((\mathrm{Norm}\,(a_p(f)))_{\substack{p\leqslant B, p\nmid N,\\ \psi(p)=-1}}, \left(\mathrm{Norm}\left(a_p(f)^2 - p^{k-1}(\varepsilon\psi)_0(p)\right)\right)_{\substack{p\leqslant B, p\mid N,\\ v_p(N)=v_p(\mathfrak{c})}} \right).$$

This gives us the following algorithm.

Algorithm 14.20. ***Input****: A newform f, described by its Fourier coefficients $(a_n(f))_{n\geqslant 0}$ as elements of the number field K_f, together with its level N, weight k, and character ε.*
Output*: The set of primes ideals λ of $\mathcal{O}_f$ which residual characteristic is not a small dihedral prime and such that $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}})$ is a dihedral group of order prime to ℓ.*

1. *Set* $\mathrm{Dih}(f) = \emptyset$.
2. *Compute the set $T_{N,\varepsilon}$ (see definition 14.15).*
3. *Compute the bound B defined in theorem 14.16.*
4. *For $\psi \in T_{N,\varepsilon}$, compute the set $P(\psi)$ of prime divisors of the* gcd *of the algebraic norms of*
   - *$a_p(f)(1-\psi(p))$ for $p \nmid N$, $p \leqslant B$;*
   - *$a_p(f)^2 - p^{k-1}(\psi\varepsilon)_0(p)$, for $p \mid N$ such that $v_p(N) = v_p(\mathfrak{c})$ and ψ is ramified at p,*

   that are not small dihedral prime numbers according to definition 14.18.
5. *For $\psi \in T_{N,\varepsilon}$ and for $\ell \in P(\psi)$,*
   (a) *Compute the prime ideals λ of $\mathcal{O}_f$ above ℓ.*
   (b) *For each such λ, check the following congruences:*
   - *$a_p(f) \equiv \psi(p)a_p(f) \pmod{\lambda}$ for $p \nmid N$, $p \leqslant B$;*
   - *$a_p(f)^2 \equiv p^{k-1}(\psi\varepsilon)_0(p) \pmod{\lambda}$.*

   If they all hold, add λ to $\mathrm{Dih}(f)$. The representation $\overline{\rho}_{f,\lambda}$ has projective dihedral image of order prime to ℓ.

Remark 14.21. *Notice that their may be some overlap between the reducible case and the dihedral case. Indeed, assume that $\overline{\rho}_{f,\lambda}$ is reducible, isomorphic to $\eta_1 \oplus \eta_2$ for two residual characters η_1, η_2. In this case, the projective image of $\overline{\rho}_{f,\lambda}$ is isomorphic to $(\eta_1\eta_2^{-1})(G_{\mathbb{Q}})$ which is a cyclic group. It can be dihedral in exactly two cases :*

- *If $\eta_1 = \eta_2$, then the projective image of $\overline{\rho}_{f,\lambda}$ is trivial.*
- *If $(\eta_1\eta_2^{-1})(G_{\mathbb{Q}}) = \{1,-1\}$, then $\eta_1\eta_2^{-1}$ is a quadratic character and the projective image of $\overline{\rho}_{f,\lambda}$ is $\mathbb{Z}/2\mathbb{Z} = D_2$.*

The first case will not be detected by our theorem because the corresponding twist would be the trivial character. However, the second case will be detected as a dihedral case. For example, consider the modular form $\Delta \in S_{12}(1,\mathbb{1})$ at $\ell = 3$. The representation $\overline{\rho}_{\Delta,(3)}$ is isomorphic to $\overline{\chi}_3 \oplus \overline{\chi}_3^2$. The projective image of $\overline{\rho}_{\Delta,(3)}$ is isomorphic to $\overline{\chi}_3(G_{\mathbb{Q}}) \cong \mathbb{Z}/2\mathbb{Z}$ and the quadratic character $\overline{\chi}_3$ is indeed a non-trivial twist of $\overline{\rho}_{\Delta,(3)}$.

Chapter 15

Numerical applications

We present here some examples of applications of the algorithms described in sections 13.3 and 14.3 to compute the reducible and dihedral primes of a given newform. Throughout this section we use the Conrey representation $(\varepsilon_a(b))_{b\wedge a=1}$ for the Dirichlet characters of modulus a. This is the way they are described in the LMFDB for example (and in some extent in PARI/GP). Notice that there would be no possible confusion with the characters ε_1, ε_2 from the algorithms above.

15.1 The reducible case

15.1.1 A concrete example

Consider the space $S_7^{\text{new}}(7, \varepsilon_7(3))$. It has dimension 6 over $\mathbb{C}$ and is generated by 2 newforms, f_1 and f_2, up to conjugation by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\varepsilon_7(3)))$. We have $K_{f_1} = \mathbb{Q}[t]/(t^2 - t + 1)$ and $K_{f_2} = \mathbb{Q}[x]/(x^4 + 2x^2 + 4)$. Notice that $\left(1, x, \frac{x^2}{2}, \frac{x^3}{2}\right)$ is an integer basis of $\mathcal{O}_{f_2}$, and that $\varepsilon_7(3)$ sends 3 to t in K_{f_1} and to $-\frac{x^2}{2}$ in K_{f_2}. The q-expansions of f_1 and f_2 are given by

$$f_1 = q + 12tq^2 + (-7t - 7)q^3 + (80t - 80)q^4 + (-105t + 210)q^5 + (-168t + 84)q^6 - 343q^7 + O(q^8),$$

$$f_2 = q + \left(3 \cdot \frac{x^3}{2} + 2x^2 + 3x\right) q^2 + \left(13x^3 - \frac{3}{2}x^2 + 13x + 3\right) q^3 + (15x^2 - 24x + 30)q^4 + \left(-25x^3 - \frac{25}{2}x^2 + 50x - 50\right) q^5 + O(q^6).$$

The set of prime numbers less than $k + 1 = 8$ or dividing $N\varphi(N) = 42$ is equal to $\{2, 3, 5, 7\}$. We treat those primes separately below.

- $\ell = 2$: The ideal $2\mathcal{O}_{f_1}$ is prime and the ideal $2\mathcal{O}_{f_2}$ decomposes as $2\mathcal{O}_{f_2} = ((x, 2)\mathcal{O}_{f_2})^2$. Because, the ideal generated by 2 in $\mathbb{Z}[\varepsilon_7(3)]$ is prime, algorithm 13.21 gives us

$$R_{7,7,\varepsilon_7(3)}(2\mathcal{O}_{f_1}) = R_{7,7,\varepsilon_7(3)}((2, x)\mathcal{O}_{f_2}) = \{(\mathbb{1}, \varepsilon_7(4), 0, 0)\}.$$

According to theorem 13.12, we have for $(\varepsilon_1, \varepsilon_2, m_1, m_2) = (\mathbb{1}, \varepsilon_7(4), 0, 0)$,

$$k' = 2, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 3, \quad \widetilde{k} = 10, \quad B = 6 + \frac{2}{3}.$$

To check the reducibility of $\overline{\rho}_{f_1,(2)}$ and $\overline{\rho}_{f_2,(2,x)}$ we only have to check the third and fifth coefficients of f_1 and f_2. The table below shows the reduction modulo the prime ideals above of $a_p(f_i) - 1 - \varepsilon_7(4)(p)$ for $i = 1$, 2, and $p = 3$, 5. From theorem 13.12, we know that $\overline{\rho}_{f_i,\lambda}$ is reducible if and only if the row corresponding to f_i contains only zeros.

p	3	5
$a_p(f_1) - (1 + \varepsilon_7(4)(p)) \pmod 2$	0	0
$a_p(f_2) - (1 + \varepsilon_7(4)(p)) \pmod{(2,x)}$	0	0

Therefore, we have $\overline{\rho}_{f_1,(2)} \cong \mathbb{1} \oplus \overline{\varepsilon_7(4)}$ and $\overline{\rho}_{f_2,(2,x)} \cong \mathbb{1} \oplus \overline{\varepsilon_7(4)}$.

- $\ell = 3$: We have $3\mathcal{O}_{f_1} = ((3, t+1)\mathcal{O}_{f_1})^2$ and $3\mathcal{O}_{f_2} = \big((3, x^2+1)\mathcal{O}_{f_2}\big)^2$. As for $\ell = 2$, the ideal generated by 3 in $\mathbb{Z}[\varepsilon_7(3)]$ is prime. Therefore, we have from algorithm 13.21

$$\begin{aligned} R_{7,7,\varepsilon_7(3)}((3, t+1)\mathcal{O}_{f_1}) &= R_{7,7,\varepsilon_7(3)}((3, x^2+1)\mathcal{O}_{f_2}) \\ &= \{(\mathbb{1}, \varepsilon_7(6), 0, 0); (\mathbb{1}, \varepsilon_7(6), 1, 1)\}. \end{aligned}$$

According to theorem 13.12, we have in both cases

$$k' = 1, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 4, \quad \widetilde{k} = 11, \quad B = 7 + \frac{1}{3}.$$

We have to look at the second, fifth, and seventh coefficients of f_1 and f_2. Let us look at the second and fifth first.

p	2	5
$a_p(f_1) - (1 + \varepsilon_7(6)(p)) \pmod{(3, t+1)}$	1	0
$a_p(f_1) - (p + p\varepsilon_7(6)(p)) \pmod{(3, t+1)}$	2	0
$a_p(f_2) - (1 + \varepsilon_7(6)(p)) \pmod{(3, x^2+1)}$	2	0
$a_p(f_2) - (p + p\varepsilon_7(6)(p)) \pmod{(3, x^2+1)}$	0	0

From these computations, we deduce that the only representation that can be reducible is $\overline{\rho}_{f_2,(3,x^2+1)}$, and that it can only be isomorphic to $\overline{\chi}_3 \oplus \overline{\chi}_3\overline{\varepsilon_7(6)}$. To confirm this isomorphism, we finally have to check that there exists some $b_7 \in \{0, 7, 7\varepsilon_7(6)(7)\} = \{0, 7\}$ such that $a_7(f_2) \equiv 7b_7 \pmod{(3, x^2+1)}$. We find that we have $a_7(f_2) \equiv 7 \pmod{(3, x^2+1)}$. Therefore, the representation $\overline{\rho}_{f_1,(3,t+1)}$ is irreducible, and we have $\overline{\rho}_{f_2,(3,x^2+1)} \cong \overline{\chi}_3 \oplus \overline{\chi}_3\overline{\varepsilon_7(6)}$.

- $\ell = 5$: The rational prime number 5 is prime in $\mathcal{O}_{f_1}$, and $5\mathcal{O}_{f_2} = (5, x^2-2x-2)(5, x^2+2x-2)$. There is again only one prime ideal above 5 in $\mathbb{Z}[\varepsilon_7(3)]$ and we have

$$\begin{aligned} R_{7,7,\varepsilon_7(3)}(5\mathcal{O}_{f_1}) &= R_{7,7,\varepsilon_7(3)}(5, x^2 \pm 2x - 2) \\ &= \{(\mathbb{1}, \varepsilon_7(3), 0, 2); (\varepsilon_7(3), \mathbb{1}, 2, 0); (\mathbb{1}, \varepsilon_7(3), 1, 1)\}. \end{aligned}$$

Looking at the congruences at $p = 3$ for f_1, and $p = 2$ for f_2, we have

$$a_3(f_1) - \left(1 + 3^2\varepsilon_7(3)(3)\right) \equiv 4t + 2 \pmod 5,$$
$$a_3(f_1) - \left(\varepsilon_7(3)(3) + 3^2\right) \equiv 2t + 4 \pmod 5,$$
$$a_2(f_2) - \left(1 + 2^2\varepsilon_7(3)(2)\right) \equiv \begin{cases} 2 \pmod{(5, x^2 - 2x - 2)}; \\ 4x \pmod{(5, x^2 + 2x - 2)}, \end{cases}$$
$$a_2(f_2) - \left(\varepsilon_7(3)(2) + 2^2\right) \equiv \begin{cases} 2x + 3 \pmod{(5, x^2 - 2x - 2)}; \\ 2x + 1 \pmod{(5, x^2 + 2x - 2)}, \end{cases}$$
$$a_2(f_2) - (2 + 2\varepsilon_7(3)(2)) \equiv \begin{cases} 3x + 2 \pmod{(5, x^2 - 2x - 2)}; \\ x \pmod{(5, x^2 + 2x - 2)}. \end{cases}$$

The only candidate remaining is $(\mathbb{1}, \varepsilon_7(3), 1, 1)$ for $\overline{\rho}_{f_1,(5)}$. We have

$$k' = 1, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 6, \quad \widetilde{k} = 13, \quad B = 8 + \frac{2}{3}.$$

We check the second, third, and seventh coefficients, and we get

$$a_2(f_1) \equiv 2 + 2\varepsilon_7(3)(2) \pmod 5,$$
$$a_3(f_1) \equiv 3 + 3\varepsilon_7(3)(3) \pmod 5,$$
$$a_7(f_1) \equiv 7 \pmod 5.$$

Therefore, the representations $\overline{\rho}_{f_2,(5,x^2-2x-2)}$ and $\overline{\rho}_{f_2,(5,x^2+2x-2)}$ are irreducible, and we have an isomorphism $\overline{\rho}_{f_1,(5)} \cong \overline{\chi}_5 \oplus \overline{\chi}_5\overline{\varepsilon_7(3)}$.

- $\ell = 7$: We have $7\mathcal{O}_{f_1} = (7, t-5)(7, t-3)$ and $7\mathcal{O}_{f_2} = (7, x-1)(7, x-2)(7, x+2)(7, x+1)$. This time 7 decomposes in $\mathbb{Z}[\varepsilon_7(3)]$ and we have

$$\begin{aligned} R_{7,7,\varepsilon_7(3)}(7, t-3) &= R_{7,7,\varepsilon_7(3)}(7, x \pm 1) \\ &= \{(\mathbb{1}, \mathbb{1})\} \times \{(0,1); (2,5); (3,4)\} \\ \text{and } R_{7,7,\varepsilon_7(3)}(7, t-5) &= R_{7,7,\varepsilon_7(3)}(7, x \pm 2) \\ &= \{(\mathbb{1}, \mathbb{1})\} \times \{(0,5); (1,4); (2,3)\}. \end{aligned}$$

For f_1, looking at $p = 2$ leaves us only with $(\varepsilon_1, \varepsilon_2, m_1, m_2) = (\mathbb{1}, \mathbb{1}, 2, 5)$ for the ideal $(7, t-3)$ and $(\mathbb{1}, \mathbb{1}, 1, 4)$ for $(7, t-5)$. In both cases we have to look at congruences up to $p = 5$, and we get

$$\overline{\rho}_{f_1,(7,t-3)} \cong \overline{\chi}_7^2 \oplus \overline{\chi}_7^5 \quad \text{and} \quad \overline{\rho}_{f_1,(7,t-5)} \cong \overline{\chi}_7 \oplus \overline{\chi}_7^4.$$

For f_2, looking at $p = 3$ leaves us with $(\mathbb{1}, \mathbb{1}, 2, 5)$ for $(7, x+1)$, $(\mathbb{1}, \mathbb{1}, 1, 4)$ for $(7, x+2)$, $(\mathbb{1}, \mathbb{1}, 2, 3)$ for $(7, x-2)$, and $(\mathbb{1}, \mathbb{1}, 3, 4)$ for $(7, x-1)$. In the first two cases we have $r = 1$, and we have to look at congruences up to $p = 5$. In the last two cases we have $r = 4$, and we have to check congruences up to $p = 53$ and $p = 67$ respectively. In every case, theorem 13.12 shows that the corresponding representation is reducible. To sum up we have

$$\overline{\rho}_{f_2,(7,x-1)} \cong \overline{\chi}_7^3 \oplus \overline{\chi}_7^4, \quad \overline{\rho}_{f_2,(7,x+1)} \cong \overline{\chi}_7^2 \oplus \overline{\chi}_7^5,$$
$$\overline{\rho}_{f_2,(7,x-2)} \cong \overline{\chi}_7^2 \oplus \overline{\chi}_7^3, \quad \overline{\rho}_{f_2,(7,x+2)} \cong \overline{\chi}_7 \oplus \overline{\chi}_7^4.$$

We finally look at the prime numbers $\ell > 7$. We have

$$R_{7,\varepsilon_7(3)} = \{(\mathbb{1}, \varepsilon_7(3)), (\varepsilon_7(3), \mathbb{1})\}.$$

Let $(\varepsilon_1, \varepsilon_2) \in R_{7,\varepsilon_7(3)}$. We have $r = 1$, $N' = 1$, $B = 4 + \frac{1}{3}$, and

$$C(\varepsilon_1, \varepsilon_2) = \begin{cases} 0 & \text{if } (\varepsilon_1, \varepsilon_2) = (\varepsilon_7(3), \mathbb{1}); \\ -\frac{B_{7,\varepsilon_7(3)}}{14} a_7\left(f_i\right)^2 & \text{if } (\varepsilon_1, \varepsilon_2) = (\mathbb{1}, \varepsilon_7(3)). \end{cases}$$

We first look at f_1. We find that 43 is the only prime factor greater than 7 of the gcd of the algebraic norms of $C(\varepsilon_1, \varepsilon_2)$ and $a_p(f_1) - \varepsilon_1(p) - p^6\varepsilon_2(p)$, for $p = 2$, 3. In $\mathcal{O}_{f_1}$ we have $43\mathcal{O}_{f_1} = (43, t-7)(43, t+6)$ and we get the following table.

$(\varepsilon_1, \varepsilon_2)$	$(\mathbb{1}, \varepsilon_7(3))$			$(\varepsilon_7(3), \mathbb{1})$	
	$C(\mathbb{1}, \varepsilon_7(3))$	$a_p(f_1) - 1 - p^6\varepsilon_7(3)(p)$		$a_p(f_1) - \varepsilon_7(3)(p) - p^6$	
		$p = 2$	$p = 3$	$p = 2$	$p = 3$
$(43, t-7)$	0	0	0	14	25
$(43, t+6)$	40	31	22	0	0

Therefore, we get $\overline{\rho}_{f_1,(43,t-7)} \cong \mathbb{1} \oplus \overline{\chi}_{43}^6\overline{\varepsilon_7(3)}$ and $\overline{\rho}_{f_1,(43,t+6)} \cong \overline{\varepsilon_7(3)} \oplus \overline{\chi}_{43}^6$.

We now turn to f_2. Computing again the gcd of the algebraic norm of $C(\varepsilon_1, \varepsilon_2)$ and $a_p(f_2) - \varepsilon_1(p) - p^7\varepsilon_2(p)$, for $p = 2$, 3, we find that the only possible residue characteristics are 97 and 3919. We have the following decompositions in $\mathcal{O}_{f_2}$:

$$97\mathcal{O}_{f_2} = (97, x-19)(97, x-5)(97, x+5)(97, x+19),$$

$$3919\mathcal{O}_{f_2} = (3919, x-934)(3919, x-621)(3919, x+621)(3919, x+934),$$

and we get the following values for the reduction of $C(\mathbb{1}, \varepsilon_7(3))$, $a_p(f_2) - 1 - p^6\varepsilon_7(3)(p)$, and $a_p(f_2) - \varepsilon_7(3)(p) - p^6$ for $p \in \{2, 3\}$.

$(\varepsilon_1, \varepsilon_2)$	$(\mathbb{1}, \varepsilon_7(3))$			$(\varepsilon_7(3), \mathbb{1})$	
	$C(\mathbb{1}, \varepsilon_7(3))$	$a_p(f_2) - 1 - p^6\varepsilon_7(3)(p)$		$a_p(f_2) - \varepsilon_7(3)(p) - p^6$	
		$p = 2$	$p = 3$	$p = 2$	$p = 3$
$(97, x-19)$	9	33	75	30	57
$(97, x-5)$	0	0	0	8	66
$(97, x+5)$	0	80	15	88	81
$(97, x+19)$	11	3	18	0	0
$(3919, x-934)$	3160	3231	1337	0	0
$(3919, x-621)$	0	0	0	3042	609
$(3919, x+621)$	0	1685	2010	808	2619
$(3919, x+934)$	1455	3038	3047	3726	1710

Therefore, the representations $\overline{\rho}_{f_2,(97,x-19)}$, $\overline{\rho}_{f_2,(97,x+5)}$, $\overline{\rho}_{f_2,(3919,x+621)}$ and $\overline{\rho}_{f_2,(3919,x+934)}$ are irreducible, and we have

$$\overline{\rho}_{f_2,(97,x-5)} \cong \mathbb{1} \oplus \overline{\chi}_{97}^6\overline{\varepsilon_7(3)}, \quad \overline{\rho}_{f_2,(97,x+19)} \cong \overline{\varepsilon_7(3)} \oplus \overline{\chi}_{97}^6,$$

$$\overline{\rho}_{f_2,(3919,x-934)} \cong \overline{\varepsilon_7(3)} \oplus \overline{\chi}_{3919}^6, \quad \overline{\rho}_{f_2,(3919,x-621)} \cong \mathbb{1} \oplus \overline{\chi}_{3919}^6\overline{\varepsilon_7(3)}.$$

The following table sums up all the cases for which $\overline{\rho}_{f_i,\lambda}$ is reducible.

<table>
<tr><td>ℓ</td><td colspan="2">f_1</td><td colspan="4">f_2</td></tr>
<tr><td>2</td><td colspan="2">(2)
$\mathbb{1} \oplus \overline{\varepsilon_7(4)}$</td><td colspan="4">$(2, x)$
$\mathbb{1} \oplus \overline{\varepsilon_7(4)}$</td></tr>
<tr><td>3</td><td colspan="2">Irreducible</td><td colspan="4">$(3, x^2+1)$
$\overline{\chi}_3 \oplus \overline{\chi}_3\overline{\varepsilon_7(6)}$</td></tr>
<tr><td>5</td><td colspan="2">(5)
$\overline{\chi}_5 \oplus \overline{\chi}_5\overline{\varepsilon_7(3)}$</td><td colspan="4">Irreducible</td></tr>
<tr><td>7</td><td>$(7, t-3)$
$\overline{\chi}_7^2 \oplus \overline{\chi}_7^5$</td><td>$(7, t-5)$
$\overline{\chi}_7 \oplus \overline{\chi}_7^4$</td><td>$(7, x-2)$
$\overline{\chi}_7^2 \oplus \overline{\chi}_7^3$</td><td>$(7, x-1)$
$\overline{\chi}_7^3 \oplus \overline{\chi}_7^4$</td><td>$(7, x+1)$
$\overline{\chi}_7^2 \oplus \overline{\chi}_7^5$</td><td>$(7, x+2)$
$\overline{\chi}_7 \oplus \overline{\chi}_7^4$</td></tr>
<tr><td rowspan="2">$\ell > k+1$

$\ell \nmid N\varphi(N)$</td><td rowspan="2">$(43, t-7)$
$\mathbb{1} \oplus \overline{\chi}_{47}^6\overline{\varepsilon_7(3)}$</td><td rowspan="2">$(43, t+6)$
$\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{43}^6$</td><td colspan="2">$(97, x-5)$
$\mathbb{1} \oplus \overline{\chi}_{97}^6\overline{\varepsilon_7(3)}$</td><td colspan="2">$(97, x+19)$
$\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{97}^6$</td></tr>
<tr><td colspan="2">$(3919, x-934)$
$\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{3919}^6$</td><td colspan="2">$(3919, x-621)$
$\mathbb{1} \oplus \overline{\chi}_{3919}^6\overline{\varepsilon_7(3)}$</td></tr>
</table>

15.1.2 An irreducible everywhere representation

We present an example of a modular form which all residual representations are irreducible. Fix $(N, k, \varepsilon) = (35, 4, \mathbb{1})$. The space $S_4^{\text{new}}(35, \mathbb{1})$ has dimension 6 over $\mathbb{C}$ and contains 3 newforms up to conjugation by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let f be the newform of this space which q-expansion is

$$f = q + (y+4)q^2 + (1-4y)q^3 + O\left(q^4\right),$$

where y is a root of $X^2 - 2$. The coefficient field of f is equal to $K_f = \mathbb{Q}(y)$. We have in this case

$$R_{35,\mathbb{1}} = \{(\mathbb{1}, \mathbb{1})\}.$$

Therefore, by theorem 13.19 the only prime ideals λ of $\mathcal{O}_f$ for which $\overline{\rho}_{f,\lambda}$ can be reducible are of residue characteristic $\ell \in \{2, 3, 5, 7\}$ (because we have $B_{4,\mathbb{1}} = -\frac{1}{30}$). Let us look at each of these cases.

- $\ell = 2$: We have $2\mathcal{O}_f = (2, y)^2$ and $R_{35,4,\mathbb{1}}(2, y) = \{(\mathbb{1}, \mathbb{1}, 0, 0)\}$. However, we have

$$\text{Tr}\left(\overline{\rho}_{f,(2,y)}(\text{Frob}_3)\right) \equiv a_3(f) \equiv 1 \pmod{(2, y)}$$

and

$$\text{Tr}\left((\mathbb{1} \oplus \mathbb{1})(\text{Frob}_3)\right) \equiv 0 \pmod{(2, y)}.$$

  Therefore, $\overline{\rho}_{f,(2,y)}$ is irreducible.

- $\ell = 3$: The ideal $3\mathcal{O}_f$ is prime, and we have $R_{35,4,\mathbb{1}}(3) = \{(\mathbb{1}, \mathbb{1}, 0, 1)\}$. However, we have

$$\text{Tr}\left(\overline{\rho}_{f,(3)}\left(\text{Frob}_2\right)\right) \equiv a_2(f) \equiv y + 1 \pmod{3}$$

and

$$\text{Tr}\left((\mathbb{1} \oplus \overline{\chi}_3)\left(\text{Frob}_2\right)\right) \equiv 0 \pmod{3}.$$

  Therefore, $\overline{\rho}_{f,(3)}$ is irreducible.

- $\ell = 5$: Again, 5 is prime in $\mathcal{O}_f$, and we have $R_{35,4,\mathbb{1}}(5) = \{(\mathbb{1}, \mathbb{1}, 0, 3); (\mathbb{1}, \mathbb{1}, 1, 2)\}$. Looking at a Frobenius element at 2, we have

$$\mathrm{Tr}\left(\overline{\rho}_{f,(5)}\left(\mathrm{Frob}_2\right)\right) \equiv a_2(f) \equiv y + 4 \pmod 5$$

and

$$\mathrm{Tr}\left(\left(\mathbb{1} \oplus \overline{\chi}_5^3\right)\left(\mathrm{Frob}_2\right)\right) \equiv 4 \pmod 5, \quad \mathrm{Tr}\left(\left(\overline{\chi}_5 \oplus \overline{\chi}_5^2\right)\left(\mathrm{Frob}_2\right)\right) \equiv 0 \pmod 5.$$

  Therefore, $\overline{\rho}_{f,(5)}$ is irreducible.

- $\ell = 7$: In this case we have $7\mathcal{O}_f = (7, y-3)(7, y+3)$ and $R_{35,7,\mathbb{1}}(7, y \pm 3) = \{(\mathbb{1}, \mathbb{1})\} \times \{(0,3); (1,2); (4,5)\}$. However, for a Frobenius element at 7 we have

$$\begin{cases} \mathrm{Tr}\left(\overline{\rho}_{f,(7,y-3)}\left(\mathrm{Frob}_3\right)\right) \equiv 3 \pmod{(7, y-3)}; \\ \mathrm{Tr}\left(\overline{\rho}_{f,(7,y+3)}\left(\mathrm{Frob}_3\right)\right) \equiv 6 \pmod{(7, y+3)}, \end{cases}$$

and

$$\begin{cases} \mathrm{Tr}\left(\left(\mathbb{1} \oplus \overline{\chi}_7^3\right)\left(\mathrm{Frob}_3\right)\right) \equiv 0 \pmod{7, y \pm 3}; \\ \mathrm{Tr}\left(\left(\overline{\chi}_7 \oplus \overline{\chi}_7^2\right)\left(\mathrm{Frob}_3\right)\right) \equiv 5 \pmod 7; \\ \mathrm{Tr}\left(\left(\overline{\chi}_7^4 \oplus \overline{\chi}_7^5\right)\left(\mathrm{Frob}_3\right)\right) \equiv 2 \pmod 7. \end{cases}$$

  Therefore, the representations $\overline{\rho}_{f,(7,y-3)}$ and $\overline{\rho}_{f,(7,y+3)}$ are both irreducible.

Thus, for all prime ideals λ in $\mathcal{O}_f$, the representation $\overline{\rho}_{f,\lambda}$ is irreducible.

15.2 The dihedral case

In [BD14, 5.2. Dihedral representation], Billerey and Dieulefait consider a modular form f in the space $S_2(1888, \mathbb{1})$ and proved that its Galois representation modulo a prime ideal above 5 is dihedral using the theory of elliptic curves. Let us illustrate our method on their example to prove that this is in fact the only prime ideal which is dihedral for this form.

Consider the space $S_2(1888, \mathbb{1})$. It has dimension 58 over $\mathbb{C}$ is splits into 16 orbits under the action of $G_{\mathbb{Q}}$. Let f be the modular form in the Galois orbit labeled 1888.2.*a.k* in the LMFDB which q-expansion is given by

$$\begin{aligned} f = q + &\left(2y^4 - 5y^3 - 12y^2 + 20y + 10\right) q^3 \\ &\left(2y^4 - 5y^3 - 11y^2 + 19y + 8\right) q^5 + O(q^7), \end{aligned}$$

where y is a root of $X^5 - 2X^4 - 7X^3 + 7X^2 + 9X + 2$.

Remark 15.1. *This is in fact the same modular form as the one considered in [BD14, 5.2. Dihedral representation]. To go from one form to the other, one can consider the isomorphisms of field defined by*

$$\begin{array}{ccc} \dfrac{\mathbb{Q}[X]}{(X^5 - 2X^4 - 7X^3 + 7X^2 + 9X + 2)} & \longrightarrow & \dfrac{\mathbb{Q}[X]}{(X^5 + 6X^4 - 20X^3 - 128X^2 + 48X + 320)} \\ X & \longmapsto & -\frac{1}{16}X^4 - \frac{1}{8}X^3 + \frac{3}{2}X^2 + \frac{3}{2}X - 4 \\ 4X^4 - 10X^3 - 24X^2 + 40X + 20 & \longleftarrow & X \end{array}.$$

Let us apply algorithms 14.19 and 14.20. The small prime ideals are $\ell = 3$, 5, and 59. We treat them separately.

- $\ell = 3$: The ideal generated by 3 is prime is ring of integer of the coefficient field of f. The set $T_{1888,\mathbb{1}}(3)$ is equal to

$$T_{1888,\mathbb{1}}(3) = \{(1,\mathbb{1}), (0,\varepsilon_8(3)), (1,\varepsilon_8(3)), (0,\varepsilon_8(5)), (1,\varepsilon_8(5)), (0,\varepsilon_4(3)), (1,\varepsilon_4(3))\}.$$

  For every pair (e,ψ) of $T_{1888,\mathbb{1}}(3)$, we can find a congruence $a_p(f)(1-p^e\psi(p)) \equiv 0 \pmod 3$ for $p \nmid N\ell$ that fails. The following table contains the first such prime number p for each pair (e,ψ).

(e,ψ)	p	(e,ψ)	p
$(1,\mathbb{1})$	5	$(1,\varepsilon_8(5))$	13
$(0,\varepsilon_8(3))$	5	$(0,\varepsilon_4(3))$	7
$(1,\varepsilon_8(3))$	7	$(1,\varepsilon_4(3))$	5
$(0,\varepsilon_8(5))$	5		

  Therefore, $\overline{\rho}_{f,(3)}$ does not have dihedral projective image.

- $\ell = 5$: There are two prime ideals above 5, $\lambda_{5,1} := (5, y-1)$ and $\lambda_{5,2} := (5, y^4 - y^3 - 8y^2 + 4y + 8)$. For both $\lambda_{1,5}$ and $\lambda_{2,5}$, we again have

$$T_{1888,\mathbb{1}}(\lambda_{5,i}) = \{(1,\mathbb{1}), (0,\varepsilon_8(3)), (1,\varepsilon_8(3)), (0,\varepsilon_8(5)), (1,\varepsilon_8(5)), (0,\varepsilon_4(3)), (1,\varepsilon_4(3))\}.$$

  For most pairs (e,ψ) in both $T_{1888,\mathbb{1}}(\lambda_{5,1})$ and $T_{1888,\mathbb{1}}(\lambda_{5,2})$ we can again find a congruence $a_p(f)(1-p^{2e}\psi(p)) \equiv 0 \pmod{\lambda_{5,i}}$ for $p \nmid 5 \cdot 1888$ that fails. We compile in the following table the first prime p that fails for each triplet $(e,\psi,\lambda_{5,i})$ except $(0,\varepsilon_4(3),\lambda_{5,1})$.

$(e,\psi,\lambda_{5,1})$	p	$(e,\psi,\lambda_{5,2})$	p
$(0,\mathbb{1},\lambda_{5,1})$	13	$(0,\mathbb{1},\lambda_{5,2})$	3
$(0,\varepsilon_8(3),\lambda_{5,1})$	13	$(0,\varepsilon_8(3),\lambda_{5,2})$	7
$(1,\varepsilon_8(3),\lambda_{5,1})$	17	$(1,\varepsilon_8(3),\lambda_{5,2})$	3
$(0,\varepsilon_8(5),\lambda_{5,1})$	13	$(0,\varepsilon_8(5),\lambda_{5,2})$	3
$(1,\varepsilon_8(5),\lambda_{5,1})$	17	$(1,\varepsilon_8(5),\lambda_{5,2})$	7
$(0,\varepsilon_4(3),\lambda_{5,1})$		$(1,\varepsilon_4(3),\lambda_{5,2})$	3
$(1,\varepsilon_4(3),\lambda_{5,1})$	13	$(1,\varepsilon_4(3),\lambda_{5,2})$	11

  The only triplet remaining is $(0,\varepsilon_4(3),\lambda_{5,1})$. To prove that $\overline{\rho}_{f,\lambda_{5,1}}$ has dihedral projective image, we have to check that $a_p(f)(1-\varepsilon_4(3)(p)) \equiv 0 \pmod{\lambda_{5,1}}$ for all prime numbers $p \leqslant B = 453{,}120$. We have checked that with a computer. We therefore deduce that $\overline{\rho}_{f,\lambda_{5,1}}$ has dihedral projective image.

- $\ell = 59$: There are two prime ideals above 59, $\lambda_{59,1} := (59, y+15)$ and $\lambda_{59,2} := (59, y^4 - 17y^3 + 12y^2 + 63y + 8)$, and the sets $T_{1888,\mathbb{1}}(\lambda_{59,1})$ and $T_{1888,\mathbb{1}}(\lambda_{59,2})$ are both equal to

$$\{(1,\mathbb{1}), (0,\varepsilon_8(3)), (1,\varepsilon_8(3)), (0,\varepsilon_8(5)), (1,\varepsilon_8(5)), (0,\varepsilon_4(3)), (1,\varepsilon_4(3))\}.$$

  As for $\ell = 3$, for both prime ideals $\lambda_{59,1}$, $\lambda_{59,2}$, and each pair (e,ψ) in $T_{1888,\mathbb{1}}(\lambda_{59,i})$, one can find a congruence $a_p(f)\left(1-p^{29e}\psi(p)\right) \equiv 0 \pmod{\lambda_{59,i}}$ that fails.

$(e,\psi,\lambda_{5,1})$	p	$(e,\psi,\lambda_{5,2})$	p
$(0,\mathbb{1},\lambda_{59,1})$	11	$(0,\mathbb{1},\lambda_{59,2})$	11
$(0,\varepsilon_8(3),\lambda_{59,1})$	5	$(0,\varepsilon_8(3),\lambda_{59,2})$	5
$(1,\varepsilon_8(3),\lambda_{59,1})$	5	$(1,\varepsilon_8(3),\lambda_{59,2})$	5
$(0,\varepsilon_8(5),\lambda_{59,1})$	3	$(0,\varepsilon_8(5),\lambda_{59,2})$	3
$(1,\varepsilon_8(5),\lambda_{59,1})$	3	$(1,\varepsilon_8(5),\lambda_{59,2})$	3
$(0,\varepsilon_4(3),\lambda_{59,1})$	3	$(1,\varepsilon_4(3),\lambda_{59,2})$	3
$(1,\varepsilon_4(3),\lambda_{59,1})$	3	$(1,\varepsilon_4(3),\lambda_{59,2})$	3

We deduce that representations $\overline{\rho}_{f,\lambda_{59,i}}$ do not have dihedral projective image.

We finally look at the "big" dihedral prime numbers. First, the set $T_{1888,\mathbb{1}}$ contains only the character $\varepsilon_8(3)$ and the bound B is equal to $\frac{1888\cdot 4\cdot 2}{12}\left(1+\frac{1}{2}\right)\left(1+\frac{1}{59}\right)=1920$. Then, we have

$$\gcd\left((\mathrm{Norm}(a_p(f)))_{\substack{p\leqslant 1920, p\nmid 1888,\\ \varepsilon_8(3)(p)=-1}}\right)=1.$$

In fact, we even have $\varepsilon_8(3)(5)=\varepsilon_8(3)(7)=-1$ and $\gcd(\mathrm{Norm}(a_5(f)),\mathrm{Norm}(a_7(f)))=1$. Therefore, there are no big dihedral primes and the only prime ideal λ for which $\overline{\rho}_{f,\lambda}$ is dihedral is $\lambda_{5,1}=(5,y-1)$.

References on modular Galois representations

[21] *PARI/GP version 2.13.3*. available from http://pari.math.u-bordeaux.fr/. Univ. Bordeaux, 2021 (cited on pp. 134, 143, 190).

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. "Twists of newforms and pseudo-eigenvalues of W-operators". In: *Inventiones Mathematicae* 48.3 (1978), pp. 221–243. DOI: 10.1007/BF01390245 (cited on p. 191).

[Ann13] Samuele Anni. "Images des représentations galoisiennes". These de doctorat. Bordeaux 1, Oct. 24, 2013 (cited on pp. 133, 142).

[BD14] Nicolas Billerey and Luis V. Dieulefait. "Explicit large image theorems for modular forms". In: *Journal of the London Mathematical Society. Second Series* 89.2 (2014), pp. 499–523. DOI: 10.1112/jlms/jdt072 (cited on pp. 131, 132, 139, 140, 155, 184, 200, 212).

[BM18] Nicolas Billerey and Ricardo Menares. "Strong modularity of reducible Galois representations". In: *Transactions of the American Mathematical Society* 370.2 (2018), pp. 967–986. DOI: 10.1090/tran/6979 (cited on pp. 132, 140, 155–157).

[Car59] L. Carlitz. "Arithmetic properties of generalized Bernoulli numbers". In: *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]* 202 (1959), pp. 174–182. DOI: 10.1515/crll.1959.202.174 (cited on p. 154).

[Car86] Henri Carayol. "Sur les représentations l-adiques associées aux formes modulaires de Hilbert". In: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 19.3 (1986), pp. 409–468 (cited on p. 150).

[Car89] Henri Carayol. "Sur les représentations galoisiennes modulo l attachées aux formes modulaires". In: *Duke Mathematical Journal* 59.3 (1989), pp. 785–801. DOI: 10.1215/S0012-7094-89-05937-1 (cited on p. 150).

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*. Vol. 239. Graduate Texts in Mathematics. Springer, New York, 2007. xxiv+650. ISBN: 978-0-387-49922-2 (cited on p. 147).

[Coh75] Henri Cohen. "Sums involving the values at negative integers of L-functions of quadratic characters". In: *Mathematische Annalen* 217.3 (1975), pp. 271–285. DOI: 10.1007/BF01436180 (cited on p. 159).

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. xiv+689. ISBN: 978-0-8218-4066-5. DOI: 10.1090/chel/356 (cited on p. 145).

[Del71] Pierre Deligne. "Formes modulaires et représentations l-adiques". In: *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*. Vol. 175. Lecture Notes in Math. Springer, Berlin, 1971, Exp. No. 355, 139–172 (cited on pp. 128, 136, 149).

[Del74] Pierre Deligne. "La conjecture de Weil : I". In: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307 (cited on p. 203).

[DI95] Fred Diamond and John Im. "Modular forms and modular curves". In: *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*. Vol. 17. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1995, pp. 39–133 (cited on p. 185).

[Dic01] Leonard E. Dickson. *Linear groups with an exposition of the Galois field theory*. Leipzig : B.G. Teubner, 1901. 334 pp. (cited on pp. 129, 138).

[DS74] Pierre Deligne and Jean-Pierre Serre. "Formes modulaires de poids 1". In: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 7 (1974), 507–530 (1975) (cited on pp. 128, 136, 146, 160).

[DT94] Fred Diamond and Richard Taylor. "Nonoptimal levels of mod l modular representations". In: *Inventiones Mathematicae* 115.3 (1994), pp. 435–462. DOI: 10.1007/BF01231768 (cited on pp. 129, 137).

[Edi92] Bas Edixhoven. "The weight in Serre's conjectures on modular forms". In: *Inventiones Mathematicae* 109.3 (1992), pp. 563–594. DOI: 10.1007/BF01232041 (cited on p. 150).

[Hup67] Bertram Huppert. *Endliche Gruppen. I*. Die Grundlehren Der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967. xii+793 (cited on pp. 130, 138).

[Kat73] Nicholas M. Katz. "p-adic properties of modular schemes and modular forms". In: *Modular Functions of One Variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. 1973, 69–190. Lecture Notes in Mathematics, Vol. 350 (cited on pp. 185, 187).

[Kat77] Nicholas M. Katz. "A result on modular forms in characteristic p". In: *Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*. 1977, 53–61. Lecture Notes in Math., Vol. 601 (cited on p. 159).

[Kra95] Alain Kraus. "Une remarque sur les points de torsion des courbes elliptiques". In: *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique* 321.9 (1995), pp. 1143–1146 (cited on p. 170).

[Kra97] Alain Kraus. "Majorations effectives pour l'équation de Fermat généralisée". In: *Canadian Journal of Mathematics. Journal Canadien de Mathématiques* 49.6 (1997), pp. 1139–1161. DOI: 10.4153/CJM-1997-056-2 (cited on p. 184).

[Liv89] Ron Livné. "On the conductors of mod l Galois representations coming from modular forms". In: *Journal of Number Theory* 31.2 (1989), pp. 133–141. DOI: 10.1016/0022-314X(89)90015-2 (cited on p. 150).

[LW12] David Loeffler and Jared Weinstein. "On the computation of local components of a newform". In: *Mathematics of Computation* 81.278 (2012), pp. 1179–1200. DOI: 10.1090/S0025-5718-2011-02530-5 (cited on p. 152).

[LW15] David Loeffler and Jared Weinstein. "Erratum: "On the computation of local components of a newform" [MR2869056]". In: *Mathematics of Computation* 84.291 (2015), pp. 355–356. DOI: 10.1090/S0025-5718-2014-02867-6 (cited on p. 152).

[Mar05] Greg Martin. "Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$". In: *Journal of Number Theory* 112.2 (2005), pp. 298–331. DOI: 10.1016/j.jnt.2004.10.009 (cited on pp. 132, 140).

[Mei17] Lennart Meier. "(Topological) modular forms with level structures: decompositions and duality". Feb. 20, 2017. arXiv: 1609.09264 [math] (cited on p. 162).

[Miy06] Toshitsune Miyake. *Modular forms*. English. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006. x+335. ISBN: 978-3-540-29592-1 (cited on pp. 152, 154–156).

[Mur97] M. Ram Murty. "Congruences between modular forms". In: *Analytic Number Theory (Kyoto, 1996)*. Vol. 247. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1997, pp. 309–320. DOI: 10.1017/CBO9780511666179.020 (cited on pp. 166, 167, 170).

[Pea21] Baptiste Peaucelle. "Explicit small image theorems for residual modular representations". In: *International Journal of Number Theory* (Oct. 18, 2021), pp. 1–60. DOI: 10.1142/S1793042122500609 (cited on pp. 127, 131, 135, 140, 150).

[Ram00] S. Ramanujan. "On certain arithmetical functions [Trans. Cambridge Philos. Soc. 22 (1916), no. 9, 159–184]". In: *Collected Papers of Srinivasa Ramanujan*. AMS Chelsea Publ., Providence, RI, 2000, pp. 136–162. DOI: 10.1016/s0164-1212(00)00033-9 (cited on pp. 127, 135).

[Rib77] Kenneth A. Ribet. "Galois representations attached to eigenforms with Nebentypus". In: *Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*. 1977, 17–51. Lecture Notes in Math., Vol. 601 (cited on pp. 129, 137, 173, 192).

[Rib85] Kenneth A. Ribet. "On l-adic representations attached to modular forms. II". In: *Glasgow Mathematical Journal* 27 (1985), pp. 185–194. DOI: 10.1017/S0017089500006170 (cited on pp. 129, 130, 137, 138).

[Rib90] K. A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms". In: *Inventiones Mathematicae* 100.2 (1990), pp. 431–476. DOI: 10.1007/BF01231195 (cited on pp. 129, 137).

[Rib94] Kenneth A. Ribet. "Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$". In: *Motives (Seattle, WA, 1991)*. Vol. 55. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 1994, pp. 639–676 (cited on p. 161).

[RS62] J. Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois Journal of Mathematics* 6 (1962), pp. 64–94 (cited on p. 171).

[Ser68] Jean-Pierre Serre. *Corps locaux*. Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968. 245 pp. (cited on pp. 146, 148).

[Ser69] Jean-Pierre Serre. "Une interprétation des congruences relatives à la fonction τ de Ramanujan". In: *Séminaire Delange-Pisot-Poitou: 1967/68, Théorie Des Nombres, Fasc. 1, Exp. 14*. Secrétariat mathématique, Paris, 1969, p. 17 (cited on pp. 127, 128, 135, 136).

[Ser73] Jean-Pierre Serre. "Congruences et formes modulaires". In: *Séminaire Bourbaki Vol. 1971/72 Exposés 400–417*. Ed. by A. Dold and B. Eckmann. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer, 1973, pp. 319–338. ISBN: 978-3-540-38403-8. DOI: 10.1007/BFb0069289 (cited on pp. 129, 131, 137, 139).

[Ser87] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)". In: *Duke Mathematical Journal* 54.1 (1987), pp. 179–230. DOI: 10.1215/S0012-7094-87-05413-5 (cited on pp. 129, 137).

[Sta40] K. G. C. Staudt. "Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffen." In: *Journal für die reine und angewandte Mathematik* 21 (1840), pp. 372–374 (cited on p. 154).

[Stu87] J. Sturm. "On the congruence of modular forms". In: *Number Theory*. Vol. 1240. Lecture Notes in Math. Springer, Berlin, 1987, pp. 275–280. DOI: 10.1007/BFb0072985 (cited on p. 166).

[Swi73] H. P. F. Swinnerton-Dyer. "On ℓ-adic Representations and Congruences for Coefficients of Modular Forms". In: *Modular Functions of One Variable III*. Ed. by Willem Kuijk and Jean-Pierre Serre. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer, 1973, pp. 1–55. ISBN: 978-3-540-37802-0. DOI: 10.1007/978-3-540-37802-0_1 (cited on pp. 127, 129, 131, 135, 137, 139, 159, 161).

[Wil95] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". In: *Annals of Mathematics. Second Series* 141.3 (1995), pp. 443–551. DOI: 10.2307/2118559 (cited on pp. 129, 137).

[Zag08] Don Zagier. "Elliptic Modular Forms and Their Applications". In: *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. Ed. by Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, Don Zagier, and Kristian Ranestad. Universitext. Berlin, Heidelberg: Springer, 2008, pp. 1–103. ISBN: 978-3-540-74119-0. DOI: 10.1007/978-3-540-74119-0_1 (cited on p. 159).