université de BORDEAUX

Thèse présentée
pour obtenir le grade de

Docteur de
l'université de Bordeaux

Spécialité : mathématiques

Par Nicolas Mascot

Calcul de représentations galoisiennes modulaires

Directeur : Jean-Marc Couveignes
Co-directeur : Karim Belabas

Soutenue le mardi 15 juillet 2014 à 15h

Devant le jury formé de :

Henri Cohen	Professeur émérite	Université de Bordeaux	Président
John Cremona	Professeur	University of Warwick	Rapporteur
Benedict Gross	Professeur	Harvard university	Rapporteur
Jean-Marc Couveignes	Professeur	Université de Bordeaux	Directeur
Karim Belabas	Professeur	Université de Bordeaux	Co-directeur
Kamal Khuri-Makdisi	Professeur	American university of Beirut	Examinateur
John Voight	Professeur associé	Dartmouth college	Examinateur

Computing modular Galois representations

Nicolas Mascot

Doctoral thesis

Advisor:
Jean-Marc Couveignes

Defended on Tuesday, July 15th, 2014

Reviewers:

J. Cremona	Warwick University
B. Gross	Harvard University

Jury:

K. Belabas	Université de Bordeaux
H. Cohen, president	Université de Bordeaux
J.-M. Couveignes	Université de Bordeaux
J. Cremona	Warwick University
B. Gross	Harvard University
K. Khuri-Makdisi	American University of Beirut
J. Voight	Dartmouth College

Institut de mathématiques de Bordeaux
Université de Bordeaux
France

Remerciements

Je tiens tout d'abord à remercier chaleureusement mon directeur de thèse, Jean-Marc Couveignes, non seulement de m'avoir donné l'occasion de travailler sur ce passionnant sujet, mais aussi pour son soutien sans faille, sa disponibilité permanente, et l'extrême ingéniosité des réponses qu'il a apportées aux innombrables questions que je lui ai posées, et sans lesquelles cette thèse n'aurait pas acquis une telle substance. Il fut un directeur de thèse exemplaire, et certainement pas seulement pour avoir, un soir de juin 2012, renversé le monde en me préparant une tasse de café alors que nous attendions les premiers résultats de mes calculs. Mon codirecteur, Karim Belabas, n'est pas en reste, et je le remercie vivement pour la disponibilité et la gentillesse dont il a toujours fait preuve envers moi, notamment en sacrifiant son dimanche après-midi pour me permettre de répéter mon exposé de soutenance.

Plus généralement, c'est pour moi un grand plaisir de témoigner de ma reconnaissance à l'égard des membres de l'équipe de théorie algorithmique des nombres de Bordeaux, et en particulier à Bill Allombert, Henri Cohen, Andreas Enge et Damien Robert, ainsi qu'à mes condisciples Barinder Banwait, Maël Mevel, Enea Milio, Louis Nebout, Stéphanie Réglade, Thomas Selig et bien évidemment Aurel Page (mention spéciale pour les soirées raclette-Civilization sur vidéoprojecteur). Travailler dans un tel environnement fut un privilège inestimable doublé d'un réel plaisir, et je garderai un souvenir fabuleux de ces trois années passées à travailler avec vous. Je remercie également les équipes de la cellule informatique pour leur assistance lors de mes premiers pas sur le cluster de calcul PlaFRIM, et de la bibliothèque de l'IMB pour leur sympathie.

Par ailleurs, je souhaite également remercier Cécile Armana, John Cremona, Bas Edixhoven, Noam Elkies, Aurélien Galateau, Benedict Gross, Kamal Khuri-Makdisi, David Lubicz, Marusia Rebolledo, Bruno Salvy, Jean-Pierre Serre et John Voight pour l'intérêt et l'enthousiasme qu'ils ont manifestés pour mon travail.

Enfin, je voudrais remercier Jean-François, Martine, Vivien et 费明安 pour leur soutien et leur amour.

Résumé

Soit $f = q + \sum_{n \geqslant 2} a_n q^n \in S_k(N, \varepsilon)$ une *newform* (c'est-à-dire une forme parabolique nouvelle, propre, et normalisée) de poids $k \in \mathbb{N}^*$, de niveau $N \in \mathbb{N}^*$ et de nebentypus ε. On sait alors que le corps

$$K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$$

engendré par les coefficients de Fourier de f est un corps de nombres, et qu'il contient les valeurs prises par ε.

En observant la forme des congruences dites "de Ramanujan" satisfaites par les coefficients de Fourier du discriminant modulaire

$$\Delta = q \prod_{n=1}^{+\infty} (1 - q^n)^{24} \in S_{12}(1),$$

J.-P. Serre a conjecturé dans [Ser69] que pour toute newform f de poids $k \geqslant 2$ comme ci-dessus, et pour tout premier $\mathfrak{l}$ du corps de nombres K_f, il existe une représentation galoisienne $\mathfrak{l}$-adique

$$\rho_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$$

non-ramifiée hors de ℓN et telle que l'image de tout élément de Frobenius en $p \nmid \ell N$ ait pour polynôme caractéristique

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{Z}_{K_{f,\mathfrak{l}}}[X],$$

ce qui caractérise $\rho_{f,\mathfrak{l}}$ à isomorphisme près, où $\mathbb{Z}_{K_{f,\mathfrak{l}}}$ est la complétion $\mathfrak{l}$-adique de l'anneau des entiers $\mathbb{Z}_{K_f}$ de K_f, et ℓ est la caractéristique résiduelle de $\mathfrak{l}$. L'existence de $\rho_{f,\mathfrak{l}}$ fut prouvée peu de temps après par P. Deligne dans [Del71].

Soit $\mathbb{F}_\mathfrak{l}$ le corps résiduel de $\mathfrak{l}$. En réduisant la représentation galoisienne $\mathfrak{l}$-adique ci-dessus modulo $\mathfrak{l}$ et en semi-simplifiant, on obtient une représentation galoisienne modulo $\mathfrak{l}$

$$\overline{\rho}_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$$

bien définie à isomorphisme près, non-ramifiée hors de ℓN, et telle que l'image de tout élément de Frobenius en $p \nmid \ell N$ ait pour polynôme caractéristique

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{F}_\mathfrak{l}[X].$$

En particulier, la trace de cette image est a_p mod $\mathfrak{l}$, ce qui, comme remarqué par J.-M. Couveignes et B. Edixhoven inspirés par le travail précurseur de R. Schoof (cf. [Sch95]), rend possible le calcul rapide de a_p modulo $\mathfrak{l}$ pour p gigantesque. Les coefficients a_p peuvent ensuite être reconstitués par restes chinois en faisant varier $\mathfrak{l}$, ce qui fournit l'unique moyen théorique connu à ce jour de calculer a_p en temps polynomial en $\log p$, ainsi qu'expliqué dans le livre [CE11]; cependant, le coût prohibitif du calcul de la représentation galoisienne $\overline{\rho}_{f,\mathfrak{l}}$ pour ℓ grand fait que cette approche est malheureusement irréaliste à l'heure actuelle.

L'objet de cette thèse est l'étude et l'implémentation d'un algorithme, basé sur les idées contenues dans le livre [CE11] édité par J.-M. Couveignes et B. Edixhoven, qui calcule cette représentation galoisienne modulo $\mathfrak{l}$, à condition que son image contienne $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ (ce qui est le cas générique, et aussi le plus intéressant), que $k < \ell$, que N soit premier à ℓ, et que $\mathfrak{l}$ soit de degré 1 de sorte que $\mathbb{F}_\mathfrak{l} \simeq \mathbb{F}_\ell$. De plus, le corps de nombres $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\overline{\rho}_{f,\mathfrak{l}}}$ coupé par cette représentation, qui possède de nombreuses propriétés intéressantes (il est notamment souvent solution au problème inverse de Galois pour $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, ou même au problème de Gross), est calculé explicitement au cours de l'exécution de l'algorithme.

Cet algorithme, que je décris en détail dans la partie B, repose sur le fait que si $k < \ell$, alors la représentation galoisienne $\overline{\rho}_{f,\mathfrak{l}}$ est réalisée par l'action de Galois sur le sous-$\mathbb{F}_\mathfrak{l}$-plan vectoriel

$$V_{f,\mathfrak{l}} = \bigcap_{n=1}^{+\infty} \mathrm{Ker}(T_n - a_n \bmod \mathfrak{l})_{|J_1(N')[\ell]} \subset J_1(N')[\ell]$$

de la ℓ-torsion de la jacobienne $J_1(N')$ de la courbe modulaire $X_1(N')$, où $N' = N$ si $k = 2$ et $N' = \ell N$ si $k > 2$. Dans le cas de poids $k = 2$, ceci découle de la relation d'Eichler-Shimura, et le cas de poids suprieur s'en déduit grâce à un théorème d'abaissement du poids dû à B. Gross qui entraîne l'existence d'une forme de poids 2 et de niveau ℓN qui est congrue à f modulo $\mathfrak{l}$, comme expliqué dans la section A.3.3.3.

L'algorithme commence par donner une description analytique de l'espace $V_{f,\mathfrak{l}}$ plongé dans la jacobienne

$$J_1(N') \simeq \mathrm{Hom}\left(S_2\big(\Gamma_1(N')\big), \mathbb{C}\right)/H_1\big(X_1(N'), \mathbb{Z}\big)$$

vue comme un tore complexe, en calculant numériquement le réseau des périodes de la courbe modulaire $X_1(N')$ à grande précision. Ceci nécessite de choisir soigneusement les symboles modulaires le long desquels les formes sont intégrées en vue de maximiser la vitesse de convergence des séries en q, et de calculer un grand nombre de coefficients du q-développement de ces formes.

L'algorithme transforme ensuite ce modèle analytique en un modèle algébrique en représentant les points de $V_{f,\mathfrak{l}}$ par des diviseurs sur $X_1(N')(\mathbb{C})$, en inversant localement l'application d'Abel-Jacobi

$$\begin{array}{rccc} \jmath\colon & \mathrm{Div}^0\left(X_1(N')\right) & \longrightarrow & J_1(N') \\ & \sum n_i(Q_i - P_i) & \longmapsto & \sum n_i \displaystyle\int_{P_i}^{Q_i} \end{array}$$

grâce à une itération de Newton. Afin d'aider la convergence de l'itération de Newton, l'algorithme vise en fait des points de $2^m\ell$-torsion au lieu de points de ℓ-torsion, où $m \approx 10$ est un entier, puis il double m fois la classe d'équivalence linéaire du diviseur obtenu.

Cette nouvelle représentation algébrique étant Galois-équivariante, ceci permet de déterminer le corps de nombres $L = \overline{\mathbb{Q}}^{\operatorname{Ker}\overline{\rho}_{f,\mathfrak{l}}}$ coupé par la représentation, en évaluant les valeurs prises par une fonction $\alpha \in \mathbb{Q}\big(J_1(N')\big)$ en les points de $V_{f,\mathfrak{l}}$, puis en formant le polynôme

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

dont ces valeurs sont les racines et dont le corps de décomposition est donc L. Le choix de la fonction d'évaluation α fait l'objet d'un attention particulière, afin de modérer autant que possible la hauteur arithmétique du polynôme $F(X)$. Ce même polynôme est ensuite réduit progressivement en tirant parti de la structure du treillis de sous-corps de L. On obtient alors une description de la représentation galoisienne $\overline{\rho}_{f,\mathfrak{l}}$ sous la forme d'un ensemble fini de nombres algébriques conjugués sur lesquels l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est connue et correspond à son action sur les points de $V_{f,\mathfrak{l}} - \{0\}$.

Enfin, l'algorithme utilise une méthode due à T. et V. Dokchitser pour calculer l'image par $\overline{\rho}_{f,\mathfrak{l}}$ d'un élement de Frobenius en p en fonction d'un premier rationnel $p \nmid \ell N$ choisi. Comme un tel élément de Frobenius n'est défini qu'à conjugaison et inertie près, le résultat est une classe de similitude dans $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, dont on peut examiner la trace afin de déterminer la valeur du coefficient a_p de f modulo $\mathfrak{l}$. Seule cette dernière étape de l'algorithme doit être renouvelée pour calculer l'image d'un élément de Frobenius en un autre premier p, et ainsi un autre coefficient a_p mod $\mathfrak{l}$.

Grâce à de nombreuses améliorations par rapport à la version décrite dans [CE11], telles que

- l'utilisation d'une nouvelle méthode permettant de calculer le q-développement à grande précision d'une base de $S_2\big(\Gamma_1(N)\big)$ en temps quasi-linéaire en la précision q-adique (cf. section B.3.1),
- l'application des méthodes de K. Khuri-Makdisi (cf. section A.1.3) pour calculer dans la jacobienne modulaire $J_1(N)$,
- la construction d'une fonction $\alpha \in \mathbb{Q}\big(J_1(N)\big)$ au bon comportement arithmétique suivant des idées nouvelles et naturellement adaptées au mode de représentation des diviseurs utilisé par les algorithmes de K. Khuri-Makdisi (cf. section B.3.4),
- ou encore l'utilisation d'une représentation galoisienne "quotient" (cf. section B.3.5.1) permettant de part sa taille inférieure de réduire la taille des coefficients du polynôme qui la définit (cf. section B.3.5.2) sans pour autant sacrifier d'informations essentielles,

cet algorithme est très rapide et permet d'atteindre des valeurs de ℓ jusqu'alors inaccessibles tout en fournissant une description compacte du corps de nombres L coupé par la représentation. Je l'ai ainsi utilisé pour battre des records de niveau et de genre dans le calcul de représentations galoisiennes modulaires (jusqu'à $\ell = 31$, ce qui implique de calculer dans la jacobienne d'une courbe modulaire de genre $g = 26$), ainsi qu'illustré par les tables de coefficients a_p mod $\mathfrak{l}$ figurant à la section C.1.

Puisque l'algorithme repose sur le calcul d'approximations complexes de points de ℓ-torsion dans la jacobienne modulaire, il doit à un moment donné identifier des nombres rationnels à partir de leur approximation flottante. Pour cette raison, je présente dans la dernière section C.2 de cette thèse une méthode basée sur la conjecture de modularité de Serre pour prouver rigoureusement, dans le cas particulier où f est de niveau $N = 1$, que le corps de nombres L coupé par la représentation galoisienne a bien été correctement identifié.

Je commence par prouver que le groupe de Galois du corps L_{proj} coupé par la version projective de la représentation galoisienne calculée par l'algorithme est bien un sous-groupe de $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$ en vérifiant que son action sur $\mathbb{P}^1\mathbb{F}_\mathfrak{l}$ préserve le birapport; j'en déduis que cette représentation projective est la bonne, en déterminant son poids de Serre par l'examen de la valuation ℓ-adique du discriminant de L_{proj}.

Je vérifie ensuite que le groupe de Galois du corps L_{quot} coupé par la représentation quotient calculée par l'algorithme est isomorphe au quotient attendu de $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, en classifiant certaines extensions centrales de $\mathrm{PGL}_2(\mathbb{F}_\ell)$ et en m'appuyant sur le fait que L_{quot} n'est ramifié qu'en ℓ pour faire le tri parmi les cas possibles. Il est alors facile de conclure que le corps L_{quot} calculé par l'algorithme est isomorphe au corps coupé par la représentation quotient associée à f modulo $\mathfrak{l}$.

La première partie de cette thèse rappelle la théorie et les résultats utilisés par la suite, du théorème de Riemann-Roch pour les courbes algébriques à la conjecture de modularité de Serre en passant par la définition d'une forme modulaire et d'une représentation galoisienne, afin que la description détaillée de l'algorithme de calcul de représentations galoisiennes modulaires soit accessible au non-spécialiste. Par conséquent, cette partie, malgré sa longueur, ne contient aucun résultat original. **J'invite donc fortement le lecteur à survoler très rapidement cette partie A et à passer directement aux parties B et C qui commencent page 137, quitte à revenir à la partie A pour compléter ses connaissances sur un sujet qui ne lui serait pas familier.** Mon travail est présenté dans les parties B (description de l'algorithme) et C (tables de résultats de mes calculs et preuve de ceux-ci).

Summary

Let $f = q + \sum_{n \geqslant 2} a_n q^n \in S_k(N, \varepsilon)$ be a newform of weight $k \in \mathbb{N}$, level $N \in \mathbb{N}$ and nebentypus ε. It is known that the field

$$K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$$

spanned by the Fourier coefficients of f is a number field, which contains the values assumed by ε.

As he observed the form of the so-called Ramanujan congruences satisfied by the Fourier coefficients of the modular discriminant

$$\Delta = q \prod_{n=1}^{+\infty} (1 - q^n)^{24} \in S_{12}(1),$$

J.-P. Serre conjectured in [Ser69] that for each newform f of weight $k \geqslant 2$ as above, and for each prime $\mathfrak{l}$ of the number field K_f, there exists an $\mathfrak{l}$-adic Galois representation

$$\rho_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$$

which is unramified outside ℓN and such that the characteristic polynomial of the image of any Frobenius element at $p \nmid \ell N$ is

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{Z}_{K_{f,\mathfrak{l}}}[X],$$

which characterises $\rho_{f,\mathfrak{l}}$ up to isomorphism, where $\mathbb{Z}_{K_{f,\mathfrak{l}}}$ is the $\mathfrak{l}$-adic completion of the ring of integers $\mathbb{Z}_{K_f}$ of K_f, and ℓ denotes the residual characteristic of $\mathfrak{l}$. The existence of $\rho_{f,\mathfrak{l}}$ was proved shortly after by P. Deligne in [Del71].

Let $\mathbb{F}_{\mathfrak{l}}$ be the residual field of $\mathfrak{l}$. Reducing the above $\mathfrak{l}$-adic Galois representation modulo $\mathfrak{l}$ and semi-simplifying yields a modulo $\mathfrak{l}$ Galois representation

$$\overline{\rho}_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$$

which is well-defined up to isomorphism, unramified outside ℓN, and such that the characteristic polynomial of the image of any Frobenius element at $p \nmid \ell N$ is

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{F}_{\mathfrak{l}}[X].$$

In particular, the trace of this image is $a_p \bmod \mathfrak{l}$, which, as noticed by J.-M. Couveignes and B. Edixhoven inspired by R. Schoof's pioneering work (cf. [Sch95]), makes it possible to compute a_p modulo $\mathfrak{l}$ for huge p. The coefficients a_p may then be recovered by Chinese remainders by letting $\mathfrak{l}$ vary, which yields the to date only known theoretical way to compute a_p in time polynomial in $\log p$, as explained in the book [CE11]; however, the prohibitive cost of the computation of the Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ for large ℓ unfortunately makes this approach unrealistic at present.

The goal of this thesis is to describe and implement an algorithm, based on ideas from the book [CE11] edited by J.-M. Couveignes and B. Edixhoven, which aims to compute this modulo $\mathfrak{l}$ Galois representation, provided that its image contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ (which is the generic and also most interesting case), that $k < \ell$, and that $\mathfrak{l}$ is of degree 1 so that $\mathbb{F}_\mathfrak{l} \simeq \mathbb{F}_\ell$. Besides, the number field $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\overline{\rho}_{f,\mathfrak{l}}}$ cut out by this representation, which enjoys various interesting properties (it is a solution to the inverse Galois problem for $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, and even to the Gross problem), is computed explicitly along the algorithm execution.

This algorithm, which I describe in details in part B, relies on the fact that if $k < \ell$, then the Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ is afforded by the Galois action on the sub-$\mathbb{F}_\mathfrak{l}$-vector plane

$$V_{f,\mathfrak{l}} = \bigcap_{n=1}^{+\infty} \mathrm{Ker}(T_n - a_n \bmod \mathfrak{l})_{|J_1(N')[\ell]} \subset J_1(N')[\ell]$$

of the ℓ-torsion of the jacobian $J_1(N')$ of the modular curve $X_1(N')$, where $N' = N$ if $k = 2$ and $N' = \ell N$ if $k > 2$. In the case of weight $k = 2$, this is a consequence of the Eichler-Shimura relation, and the higher-weight case follows thanks to a weight-lowering theorem of B. Gross's, which implies the existence of a form of weight 2 and level ℓN which is congruent to f modulo $\mathfrak{l}$, as explained in section A.3.3.3.

To begin with, the algorithm gives an analytic description of the space $V_{f,\mathfrak{l}}$ embedded in the jacobian

$$J_1(N') \simeq \mathrm{Hom}\left(S_2\big(\Gamma_1(N')\big), \mathbb{C}\right)/H_1\big(X_1(N'), \mathbb{Z}\big)$$

seen as a complex torus, by numerically computing the period lattice of the modular curve $X_1(N')$ with high accuracy. This requires a careful selection of the modular symbols along which cuspforms are integrated so as to maximise the speed of convergence of the q-series, and to compute a large number of q-expansion coefficients of these cuspforms.

The algorithm then switches from this analytic model to an algebraic one by representing points on $V_{f,\mathfrak{l}}$ by divisors on $X_1(N')(\mathbb{C})$, through a local inversion of the Abel-Jacobi map

$$\begin{array}{rccc} \jmath\colon & \mathrm{Div}^0\left(X_1(N')\right) & \longrightarrow & J_1(N') \\ & \sum n_i(Q_i - P_i) & \longmapsto & \sum n_i \displaystyle\int_{P_i}^{Q_i} \end{array}$$

performed thanks to a Newton iteration scheme. In order to help the Newton iteration to converge, the algorithm actually aims for $2^m\ell$-torsion points instead of ℓ-torsion ones, with $m \approx 10$ an integer, and then doubles m times the linear equivalence class of the divisor thus computed.

As this new algebraic representation is Galois-equivariant, this allows to determine the number field $L = \overline{\mathbb{Q}}^{\operatorname{Ker}\overline{\rho}_{f,\mathfrak{l}}}$ cut out by the representation, by evaluating the values assumed by a rational function $\alpha \in \mathbb{Q}\big(J_1(N')\big)$ at the points of $V_{f,\mathfrak{l}}$, and then by forming the polynomial

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

whose roots are these values and whose splitting field is thus L. The evaluation function α is constructed especially carefully, so as to curb the arithmetic height of the polynomial $F(X)$ as much as possible. This polynomial is then inductively reduced by drawing on the structure of the lattice of subfields of L. This yields a description of the Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ in terms of a finite set of conjugate algebraic numbers on which the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is known and corresponds to its action on $V_{f,\mathfrak{l}} - \{0\}$.

Finally, the algorithm uses a method of T. and V. Dokchitser's to compute the image by $\overline{\rho}_{f,\mathfrak{l}}$ of a Frobenius element at a chosen rational prime $p \nmid \ell N$. Since such a Frobenius element is defined up to conjugation and inertia, the result is a similarity class in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, whose trace can be looked up so as to determine the value modulo $\mathfrak{l}$ of the coefficient a_p of f. Only this last step of the algorithm must be repeated in order to compute the image of a Frobenius element at another prime p, and hence another coefficient $a_p \bmod \mathfrak{l}$.

Thanks to numerous improvements over the version described in [CE11], such as

- a new method allowing to compute the q-expansion with high accuracy of a basis of $S_2\big(\Gamma_1(N)\big)$ in time quasi-linear in the q-adic accuracy (cf. section B.3.1),
- the use of K. Khuri-Makdisi's methods (cf. section A.1.3) to compute in the modular jacobian $J_1(N)$,
- the construction of an arithmetically well-behaved function $\alpha \in \mathbb{Q}\big(J_1(N)\big)$ following new ideas naturally suited to the representation mode of divisors in K. Khuri-Makdisi's algorithms (cf. section B.3.4),
- and the introduction of a quotient Galois representation (cf. section B.3.5.1) whose smaller size allows to reduce the complexity of the polynomial defining it (cf. section B.3.5.2) without discarding any essential information,

this algorithm performs very well and allows to reach values of ℓ which were so far out of reach while giving a compact description of the number field L cut out by the representation. I have thus used it so as to beat records of level and genus in the computation of modular Galois representations (up to $\ell = 31$, which implies computing in the jacobian of a modular curve of genus $g = 26$), as illustrated by the tables of values of coefficients $a_p \bmod \mathfrak{l}$ which appear in section C.1.

Since the algorithm relies on the computation of complex approximations of ℓ-torsion points in the modular jacobian, it eventually has to identify rational numbers from their floating-point approximations. In the last section C.2 of this thesis, I therefore present a method based on Serre's modularity conjecture to rigorously prove, in the case when f is of level $N = 1$, that the number field L cut out by the Galois representation has been correctly identified.

I start by proving that the Galois group of the field L_{proj} cut out by the projective version of the Galois representation computed by the algorithm is indeed a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$, by checking that its action on $\mathbb{P}^1\mathbb{F}_\mathfrak{l}$ preserves cross-ratios. From this I deduce that this projective representation is correct, by determining its Serre weight out of the ℓ-adic valuation of the discriminant of L_{proj}.

I then check that the Galois group of the field L_{quot} cut out by the quotient representation computed by the algorithm is isomorphic to the expected quotient of $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, by classifying certain central extensions of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and relying on the fact that L_{quot} ramifies only at ℓ to exclude all possible cases but one. It is then easy to conclude that the field L_{quot} computed by the algorithm is isomorphic to the number field cut out by the quotient representation attached to f modulo $\mathfrak{l}$.

The first part of this thesis presents the background theory and results, from the Riemann-Roch theorem for algebraic curves to Serre's modularity conjecture along with the definition of a modular form and of a mod $\mathfrak{l}$ Galois representation, aiming to make the next parts accessible to the non-specialist. As a consequence, this part does not contain any original work although it is quite long. **The reader is therefore strongly invited to skip part A and proceed directly to parts B and C starting page 137, and come back to part A only if he or she would like to get information about a point he or she is not familiar with.** My work is presented in parts B (description of the algorithm) and C (tables of computation results and proof of these results).

Contents

A Theoretical prerequisites **15**
A.1 Curves and their jacobians . . . 15
A.1.1 The Riemann-Roch theorem . . . 15
A.1.2 The jacobian variety . . . 31
A.1.3 Computing in the jacobian . . . 44
A.2 Modular curves and modular forms . . . 54
A.2.1 Modular curves . . . 54
A.2.2 Modular forms . . . 67
A.2.3 Modular symbols . . . 93
A.3 Galois representations . . . 102
A.3.1 Definitions and first examples . . . 102
A.3.2 The Dokchitsers' resolvents . . . 108
A.3.3 Modular Galois representations . . . 111
A.3.4 The Serre conjecture . . . 127

B Computing modular Galois representations **137**
B.1 Overview of the algorithm . . . 138
B.2 Computing in $J_1(\ell)$ . . . 140
B.2.1 Arithmetic in the jacobian $J_1(\ell)$ . . . 140
B.2.2 Finding the appropriate Eisenstein series . . . 141
B.3 Detailed description of the algorithm . . . 143
B.3.1 Expanding the cuspforms of weight 2 to high precision . . . 143
B.3.2 Computing the periods of $X_1(\ell)$ . . . 146
B.3.3 Computing an ℓ-torsion basis . . . 148
B.3.4 Evaluating the torsion divisors . . . 150
B.3.5 Finding the Frobenius elements . . . 153
B.4 Complexity analysis . . . 157

C Tables and proof of the computation results **159**
C.1 Tables . . . 159
C.2 Certifying the polynomials . . . 185
C.2.1 Sanity checks . . . 185
C.2.2 Proving the polynomials . . . 186

Bibliography **203**

Part A

Theoretical prerequisites

Do Not Read Part A.

— Marc Hindry & Joseph Silverman, *Diophantine geometry: an introduction*

I shall begin by introducing some theoretical background, in order to set the framework, fix some notation, and mainly for the sake of self-containedness. In particular, this first section contains mainly folklore, and no original work. **I therefore urge the reader to skim very lightly through this first section, or even to proceed directly to my original work whose description begins on page 137.**

In this first part, I shall first present the Riemann-Roch theorem and the notion of the jacobian variety of an algebraic curve, including a description of K. Khuri-Makdisi's algorithms to perform arithmetic in a jacobian. Next, I shall introduce notions about modular curves and modular forms which will be used in the description of my algorithm in section B. Finally, I shall conclude by recalling some facts about Galois representations, and especially the connection between modular forms and Galois representations.

A.1 Curves and their jacobians

A.1.1 The Riemann-Roch theorem

Let me begin by introducing the Riemann-Roch theory, which is the workhorse of algebraic curve study. In what follows, I shall denote by X a projective, non-singular, geometrically integral algebraic curve X, defined over a perfect field K. I shall often have $K = \mathbb{C}$ in mind, and shall frequently use this case to give examples. However, the statements I shall give will be, of course, valid for every perfect K.

I let $K(X)$ be the function field of X, and I fix an algebraic closure $\overline{K}$ of K. For each algebraic extension L of K, I denote by $X(L)$ the set of L-rational points of X, and whenever I mention a point $P \in X$, I mean a point in $X(\overline{K})$.

In the case $K = \mathbb{C}$, the points of X naturally form a compact, connected Riemann surface, as shown on figure A.1.1.1, and $K(X)$ is the field of meromorphic functions

on X. The number g of handles of this surface is called the *genus* of X. I shall give a definition of the genus for general K later.

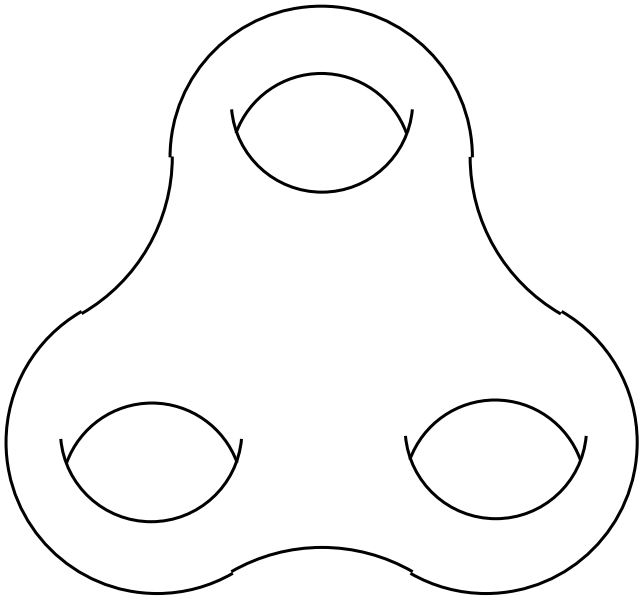


Figure A.1.1.1: A curve of genus $g = 3$ over $\mathbb{C}$

A.1.1.1 Divisors

Definition A.1.1.2. A *divisor* over X is a formal finite linear combination

$$D = \sum_{P \in X} n_P P$$

of points on X with coefficients n_P in $\mathbb{Z}$. The *support* of D is the set of points P for which $n_P \neq 0$.

The divisor D is *defined over* K if it is invariant under Galois, that is to say if $n_{\sigma(P)} = n_P$ for all $P \in X$ and for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. **In what follows, I shall implicitly assume that all the divisors are defined over** K.

Divisors over X (which are defined over K) form an abelian group, which I denote by $\mathrm{Div}(X)$.

Definition A.1.1.3. A divisor $D = \sum_{P \in X} n_P P$ is said to be *effective* if its coefficients n_P all lie in $\mathbb{Z}_{\geqslant 0}$, in which case I shall write $D \geqslant 0$. The set of effective divisors on X will be denoted by $\mathrm{Eff}(X)$.

Definition A.1.1.4. The *degree* of a divisor is defined by

$$\deg\left(\sum_{P \in X} n_P P\right) = \sum_{P \in X} n_P.$$

It is plain that the degree map

$$\deg\colon \mathrm{Div}(X) \longrightarrow \mathbb{Z}$$

is a group morphism. I denote its kernel by $\mathrm{Div}^0(X)$. More generally, I let

$$\mathrm{Div}^d(X) = \{D \in X \mid \deg(D) = d\}$$

for each $d \in \mathbb{Z}$. Note that a divisor of positive degree need not be effective.

Non-zero rational functions on the curve X provide a supply of divisors:

Definition A.1.1.5. For $f \in K(X)^*$, define

$$\mathrm{div}(f) = \sum_{P \in X} \mathrm{ord}_P(f) P,$$

where the integers $\mathrm{ord}_P(f)$ are

$$\mathrm{ord}_P(f) = \begin{cases} n, & \text{if } f \text{ has a zero of order } n \text{ at } P, \\ -n, & \text{if } f \text{ has a pole of order } n \text{ at } P, \\ 0, & \text{if } f \text{ has a neither zero nor pole at } P. \end{cases}$$

A divisor is said to be *principal* if it is of the form $\mathrm{div}(f)$ for some $f \in K(X)^*$.

Notice the analogy with a fractional principal ideal in a number field.

Remark A.1.1.6. Let s, $t \in K(X)^*$ be two non-zero rational functions on X. One has $\mathrm{div}(s) = \mathrm{div}(t)$ if and only if there exists a non-zero constant $\lambda \in K^*$ such that $t \equiv \lambda s$ identically.

Remark A.1.1.7. The relation $\mathrm{div}(st) = \mathrm{div}(s) + \mathrm{div}(t)$ shows that principal divisors form a subgroup of $\mathrm{Div}(X)$.

Example A.1.1.8. Take $X = \mathbb{P}^1_K$, which is made up of two copies of $\mathbb{A}^1_K$ with respective coordinates x and w, overlapping along $\mathbb{A}^1_K - \{0\}$ and glued by the transition map $w = 1/x$. For each $a \in K$, denote by $P_a \in \mathbb{P}^1_K$ the point of coordinate $x = a$, and denote by $P_\infty \in \mathbb{P}^1_K$ the point of coordinate $w = 0$. Consider the rational function $f = x^2 - x \in K(X)$. This function vanishes at order 1 at P_0 and also at order 1 at P_1, but it also has a double pole at P_∞ since $f = \frac{1}{w^2} - \frac{1}{w}$. Since f has no other zero or pole, one concludes that

$$\mathrm{div}(f) = P_0 + P_1 - 2P_\infty,$$

and so the divisor $P_0 + P_1 - 2P_\infty$ is principal.

As I shall demonstrate soon, not every divisor is principal. Actually, the following theorem expresses a first obstruction for a divisor to be principal.

Theorem A.1.1.9. *Let $D \in \mathrm{Div}(X)$ be a divisor on X. If D is principal, then $\deg(D) = 0$.*

This can be reformulated this into the catchphrase "a rational function has as many poles as zeroes", provided of course that these are counted with multiplicity. This common number is called the *degree* of f, cf. remark A.1.1.16 below.

Proof. I shall content myself here with giving the proof only in the case $K = \mathbb{C}$, since it is most illuminating. The proof for general K may be found in [Liu02, corollary 7.3.9].

So let $K = \mathbb{C}$, so that X can be viewed as a compact, connected Riemann surface. Let $D = \sum_{i=1}^{r} n_i P_i$ be a principal divisor on X, so that $D = \mathrm{div}(f)$ for some rational (i.e. meromorphic) function f on X. Consider the meromorphic differential 1-form $\omega = \frac{\mathrm{d}f}{f}$ on X. Its only poles are the points P_i, with residue $\mathrm{Res}_{P_i}\,\omega = \mathrm{ord}_{P_i}\,f = n_i$, so that the following lemma concludes the proof. □

Lemma A.1.1.10. *Let ω be a meromorphic differential 1-form on a Riemann surface X. Then*

$$\sum_{P \in X} \mathrm{Res}_P\,\omega = 0.$$

Proof. Let P_i, $i = 1, \cdots, r$, denote the poles of ω. For each i, let a_i denote the residue of ω at P_i, choose a coordinate chart containing P_i, and draw in this coordinate chart a small closed disk $D_i = D(P_i, \varepsilon)$ centred at P_i and of radius $\varepsilon > 0$ chosen small enough for the disks D_i not to overlap. One then has

$$\sum_{P \in X} \mathrm{Res}_P\,\omega = \sum_{i=1}^{r} a_i = \sum_{i=1}^{r} \frac{1}{2\pi i} \int_{\partial D_i} \omega = \frac{1}{2\pi i} \int_{\bigcup_{i=1}^{r} \partial D_i} \omega,$$

where ∂D_i denotes the boundary of the disk D_i, oriented in the standard way. Since the D_i's do not overlap, $\bigcup_{i=1}^{r} \partial D_i = \partial \bigcup_{i=1}^{r} D_i$, and by the Stokes theorem, the latter integral is equal to

$$\iint_{X - \bigcup_{i=1}^{r} D_i} \mathrm{d}\omega.$$

This is 0, since $\mathrm{d}\omega$ is a 2-form, which has to vanish identically on the 1-(complex) dimensional manifold X. □

This implies that the group of principal divisors is a subgroup of $\mathrm{Div}^0(X)$. This subgroup is usually strict, which means that a divisor over degree 0 on X need not be principal. This defect is measured by the *class group* of X.

Definition A.1.1.11. The *class group* of X, denoted by $\mathrm{Cl}^0(X)$, is the quotient of the group $\mathrm{Div}^0(X)$ by the subgroup of principal divisors on X.

Two divisors on X having the same image in $\mathrm{Cl}^0(X)$, that is to say, whose difference is principal, are said to be *linearly equivalent*. The linear equivalence class of a divisor $D \in \mathrm{Div}^0(X)$ is denoted by $[D] \in \mathrm{Cl}^0(X)$.

This definition is summed up in the following exact sequence of abelian groups:

$$1 \longrightarrow K^* \longrightarrow K(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(X) \longrightarrow \mathrm{Cl}^0(X) \longrightarrow 0.$$

Notice the analogy with the ideal class group of a number field.

Remark A.1.1.12. The terminology "linearly equivalent" hints that other equivalence relations (namely, algebraic equivalence and numerical equivalence) are commonly considered on divisors on varieties. However, in the case of curves, linear equivalence is the most interesting one.

Example A.1.1.13. The class group of $X = \mathbb{P}^1_K$ is trivial. To see this, one must show that every divisor of degree 0 of $\mathbb{P}^1_K$ is principal, so let $D = \sum_{P\in\mathbb{P}^1_K} n_P P$ be a divisor of degree $\sum_{P\in\mathbb{P}^1_K} n_P = 0$. Consider, with the notations of example A.1.1.8, the polynomial

$$f = \prod_{\substack{P\in\mathbb{P}^1_K \\ P\neq P_\infty}} \big(x - x(P)\big)^{n_P},$$

where (by definition) $x(P_\lambda) = \lambda$. The coefficients of f are invariant under Galois since D is assumed to be defined over K, so f lies in $K[x]$ as K is perfect, and may thus be seen as a rational function in $K(X) = K(\mathbb{P}^1_K)$. By construction, the divisor of this rational function is

$$\operatorname{div}(f) = \sum_{\substack{P\in\mathbb{P}^1_K \\ P\neq P_\infty}} n_P P + (\operatorname{ord}_{P_\infty} f)P_\infty.$$

To determine $\operatorname{ord}_{P_\infty} f$, one expresses f in terms of the local coordinate $w = 1/x$ at P_∞. Since $\deg f = \sum_{\substack{P\in\mathbb{P}^1_K \\ P\neq P_\infty}} n_P = -n_{P_\infty}$ by hypothesis, one has

$$f = x^{\deg f}\big(1 + O(1/x)\big) = w^{n_{P_\infty}}\big(1 + O(w)\big),$$

so that $\operatorname{ord}_{P_\infty} f = n_{P_\infty}$. It follows that $D = \operatorname{div}(f)$ is principal.

Consider now a non-constant morphism $f\colon X \longrightarrow Y$ between projective, non-singular, geometrically integral algebraic curves.

Definition A.1.1.14. For each $P \in X$, define the *ramification index* $e_P \in \mathbb{N}$ to be such that if x is a local coordinate at P on X and if y is a local coordinate at $f(P)$ on Y, then $y \circ f = Cx^{e_P} + O(x^{e_P+1})$ for some non-zero constant C.

The number

$$d = \sum_{f(P)=Q} e_P$$

does not depend on the point $Q \in Y$, and is called the *degree* of the morphism f. I shall denote it by $\deg f$.

The degree is multiplicative ($\deg f_1 \circ f_2 = \deg f_1 \times \deg f_2$), and a morphism between projective, non-singular, geometrically integral algebraic curves is of degree 1 if and only if it is an isomorphism.

Example A.1.1.15. Take $X = Y = \mathbb{P}^1_K$, and let $f\colon X \longrightarrow Y$ be induced by a polynomial $f(x) = ax^d + \cdots \in K[x]$ of degree $d \geqslant 1$. Then for each $\lambda \in \overline{K}$, the ramification index e_{P_λ} of f at P_λ is the vanishing order of $f(x) - f(\lambda)$ at $x = \lambda$, and the ramification index of f at P_∞ is d since $f(P_\infty) = P_\infty$ and $w \circ f = 1/f = \frac{1}{a}w^{-d} + O(w^{-d+1})$.

Remark A.1.1.16. More generally, a non-constant rational function $f \in K(X)$ on X can be seen as a non-constant morphism from X to $\mathbb{P}^1_K$, whose degree

$$\deg f = \sum_{\substack{Q\in X \\ f(Q)=P_0}} e_Q = \sum_{\substack{Q\in X \\ f(Q)=P_\infty}} e_Q$$

is the number of zeroes of f counted with multiplicity, which agrees with the number of poles of f counted with multiplicity, as noted in theorem A.1.1.9.

Example A.1.1.17. Let X be a projective, non-singular, geometrically integral algebraic curve such that $\mathrm{Cl}^0(X)$ is trivial. After possibly replacing the ground field K by a finite extension, one may suppose that there exist two distinct K-rational points $A, B \in X(K)$. Let w be a local coordinate at B. Since $\mathrm{Cl}^0(X)$ is trivial, the divisor $A - B$ is principal, so there exists a rational map $f\colon X \longrightarrow \mathbb{P}^1_K$ such that $\mathrm{div}(f) = A - B$. After renormalising f by multiplying it by a non-zero scalar, one may suppose that $f = 1/w + O(1)$. One then has

$$\deg f = \sum_{\substack{Q \in X \\ f(Q) = P_\infty}} e_Q = e_B = 1$$

since B is the only pole of f and this pole is simple. Therefore, f is an isomorphism. In conclusion, a curve X whose class group is trivial is, possibly after a finite extension of the ground field, isomorphic to $\mathbb{P}^1_K$ (one says that X is a *twist* of $\mathbb{P}^1_K$); this is a converse to example A.1.1.13.

One can use a morphism $f\colon X \longrightarrow Y$ to transfer divisors between X and Y. More precisely, one defines

$$\begin{array}{rcl} f_*\colon \mathrm{Div}(X) & \longrightarrow & \mathrm{Div}(Y) \\ \displaystyle\sum_{P \in X} n_P P & \longrightarrow & \displaystyle\sum_{P \in X} n_P f(P), \end{array}$$

and

$$\begin{array}{rcl} f^*\colon \mathrm{Div}(Y) & \longrightarrow & \mathrm{Div}(X) \\ \displaystyle\sum_{Q \in Y} n_Q Q & \longrightarrow & \displaystyle\sum_{\substack{P \in X \\ f(P) = Q}} e_P n_{f(P)} P. \end{array}$$

Note that f_* preserves the degree, whereas f^* multiplies the degree by $\deg f$. In particular, $f^* \circ f_*$ is multiplication by $\deg f$ on $\mathrm{Div}(X)$, and $f_* \circ f^*$ is multiplication by $\deg f$ on $\mathrm{Div}(Y)$.

Since f_* and f^* map degree-zero divisors to degree zero-divisors, and since $f^*\big(\mathrm{div}(\beta)\big) = \mathrm{div}(\beta \circ f)$ for all $\beta \in K(Y)^*$, and $f_*\big(\mathrm{div}(\alpha)\big) = \mathrm{div}(N_f \alpha)$ for all $\alpha \in K(X)^*$, where $N_f \alpha \in K(Y)^*$ is the rational function on Y defined by

$$(N_f \alpha)(Q) = \prod_{f(P) = Q} \alpha(P)^{e_P},$$

the morphisms f_* and f^* induce morphisms between $\mathrm{Cl}^0(X)$ and $\mathrm{Cl}^0(Y)$, which I shall still denote by f_* and f^*.

The morphism $f\colon X \longrightarrow Y$ also defines a morphism of function fields

$$\begin{array}{rcl} f^*\colon K(Y) & \hookrightarrow & K(X) \\ \alpha & \longmapsto & \alpha \circ f \end{array}$$

which allows one to see $K(X)$ as an extension of $K(Y)$ of degree $\deg f$. If the characteristic of K is $p \neq 0$, the function field $K(Y)$ may not be perfect even though the

ground field K is, so the extension $K(X)/K(Y)$ might not be separable. One says that f is *separable* (respectively *purely inseparable*, etc.) if the extension $K(X)/K(Y)$ is separable (respectively purely inseparable, etc.). The maximal separable subextension $K(X)^{\mathrm{sep}} = K(Z)$ of $K(X)/K(Y)$ corresponds to a curve Z such that the extension $K(Z)/K(Y)$ is separable whereas the extension $K(X)/K(Z)$ is purely inseparable, so that the morphism $f\colon X \longrightarrow Y$ factors into a purely inseparable morphism $X \longrightarrow Z$ followed by a separable morphism $Z \longrightarrow Y$. One defines the *separable degree* $\deg_{\mathrm{sep}} f$ of f as $\deg(Z \longrightarrow Y) = [K(Z)\colon K(Y)]$, and the *inseparable degree* $\deg_{\mathrm{ins}} f$ of f as $\deg(X \longrightarrow Z) = [K(X)\colon K(Z)]$, which is necessarily a power of p. For instance, f is separable if and only if $\deg_{\mathrm{ins}} f = 1$, whereas f is purely inseparable if and only if $\deg_{\mathrm{sep}} f = 1$. Note that $\deg_{\mathrm{sep}}$ and $\deg_{\mathrm{ins}}$ are multiplicative just like deg, and that $\deg = \deg_{\mathrm{sep}} \times \deg_{\mathrm{ins}}$.

Let $\sigma_p\colon x \mapsto x^p$ be the *Frobenius automorphism* in $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. It can be extended into a morphism $\sigma_p\colon X \longrightarrow X^{\sigma_p}$ which is purely inseparable of degree p, where X^{σ_p} denotes the curve defined by letting σ_p act on the coefficients of the equations defining X. This morphism corresponds to the inclusion of $K(X^{\sigma_p}) = K(X)^p$ into $K(X)$. Conversely, a purely inseparable morphism of degree p^r factors into the r-fold composition of σ_p followed by an isomorphism, so one can take $Z = X^{\sigma_p^r}$ above. In particular, a purely inseparable morphism induces a bijection on the $\overline{K}$-points. Since the ramification indexes e_P of a separable morphism are 1 for almost all P, it follows that for almost all points $Q \in Y(\overline{K})$, the number of pre-images $P \in X(\overline{K})$ of Q by f is $\deg_{\mathrm{sep}} f$.

A.1.1.2 Line bundles

In order to move on toward the Riemann-Roch theorem, it is useful to perform a slight change of language, by reformulating linear equivalence of divisors in term of line bundles over the curve X. By a *line bundle*, I mean a locally free module $\mathcal{L}$ of rank one over the structure sheaf $\mathcal{O}_X$ of X and which is defined over K (that is to say $\sigma^*\mathcal{L} = \mathcal{L}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$). Recall that $\mathcal{O}_X$ is the K-vector-space-valued sheaf on X such that

$$\mathcal{O}_X(U) = \{f \in K(X) \mid f \text{ has no pole on } U\} \quad \text{for every open subset } U \subseteq X.$$

I shall denote by Γ the "global sections" functor $\mathcal{A} \longmapsto \mathcal{A}(X)$, where $\mathcal{A}$ is a sheaf on X. Since X is projective, one has the following very useful result (cf. [Har77, theorem II.5.19]):

Theorem A.1.1.18. *For any line bundle $\mathcal{L}$ on X, the global sections space $\Gamma\mathcal{L}$ has finite dimension over K.*

Example A.1.1.19. Theorem A.1.1.9 implies that $\Gamma\mathcal{O}_X$ is reduced to K.

To a divisor $D \in \mathrm{Div}(X)$ on X, I shall associate the line bundle $\mathcal{O}_X(D)$, defined by

$$\mathcal{O}_X(D)(U) = \Big\{f \in K(X) \mid \big(\mathrm{div}(f) + D\big)_{|U} \geqslant 0\Big\} \text{ for every open subset } U \subseteq X.$$

In particular, one has

$$\Gamma\mathcal{O}_X(D) = \{f \in K(X)^* \mid \mathrm{div}(f) + D \geqslant 0\} \cup \{0\}.$$

Riemann-Roch theory, as shall be seen, deals with the study of spaces of this form.

The following fact, although very basic, will be of constant use:

Lemma A.1.1.20. *Let $D \in \mathrm{Div}(X)$ be a divisor on X. If $\deg(D) < 0$, then $\Gamma\mathcal{O}_X(D)$ is reduced to $\{0\}$.*

Proof. Assume on the contrary that there exists a non-zero section $s \in \Gamma\mathcal{O}_X(D)$. Then one would have $\mathrm{div}(s) + D \geqslant 0$ by definition, and thus, by taking the degree, $\deg D \geqslant 0$ since $\deg \mathrm{div}(s) = 0$ by theorem A.1.1.9, which contradicts the hypothesis. □

The following theorem explains the relation between the line bundles $\mathcal{O}_X(D)$ and the class group $\mathrm{Cl}^0(X)$.

Theorem A.1.1.21. *Let D, $D' \in \mathrm{Div}(X)$ be divisors on X. The associated line bundles $\mathcal{O}_X(D)$ and $\mathcal{O}_X(D')$ are isomorphic if and only if the divisors D and D' are linearly equivalent. Furthermore, every line bundle $\mathcal{L}$ on X is isomorphic to a line bundle of the form $\mathcal{O}_X(D)$ for some divisor $D \in \mathrm{Div}^0(X)$.*

Proof. The proof of the first statement is not difficult from the definitions. For instance, it is easy to see that for every $f \in K(X)^*$, multiplication of the sections by f yields an isomorphism from $\mathcal{O}_X(\mathrm{div}(f) + D)$ to $\mathcal{O}_X(D)$. The proof of the fact that every line bundle is of the form $\mathcal{O}_X(D)$, however, is more technical, and I shall not give it here; instead, I shall just mention that it stems from the fact that I assumed the curve X to be absolutely integral, and refer the interested reader to [Har77, proposition II.6.15]. □

In view of the previous theorem and of theorem A.1.1.9, the following definition makes sense:

Definition A.1.1.22. Let $\mathcal{L}$ be a line bundle on X. The degree of $\mathcal{L}$ is defined to be the degree of any divisor $D \in \mathrm{Div}(X)$ such that $\mathcal{L} \simeq \mathcal{O}_X(D)$.

Recall that the tensor product over $\mathcal{O}_X$ endows the set $\mathrm{Pic}(X)$ of isomorphism classes of line bundles over X with an abelian group structure, for which the inverse of the class of a line bundle $\mathcal{L}$ is the class of the *dual* bundle $\mathcal{L}^\vee = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$. By the previous theorem, isomorphic line bundles have the same degree, so that one gets a well-defined map

$$\deg\colon \mathrm{Pic}(X) \longrightarrow \mathbb{Z}.$$

One checks easily that $\mathcal{O}_X(D) \underset{\mathcal{O}_X}{\otimes} \mathcal{O}_X(D') \simeq \mathcal{O}_X(D + D')$ and that $\mathcal{O}_X(D)^\vee \simeq \mathcal{O}_X(-D)$ for $D, D' \in \mathrm{Div}(X)$, which implies that this map is a group morphism, whose kernel I denote by $\mathrm{Pic}^0(X)$. The above theorem can thus be rephrased by saying that the map $D \longmapsto \mathcal{O}_X(D)$ yields an isomorphism $\mathrm{Cl}^0(X) \simeq \mathrm{Pic}^0(X)$.

In the next section, I shall give yet another description of the class group, as an abelian variety.

A.1.1.3 Differential forms and the genus

An especially interesting line bundle is the bundle Ω^1_X of regular differential 1-forms on X. These are simply objects which, in a chart with coordinate x, read $\omega = f(x)\mathrm{d}x$ for some function $f \in K(X)$ which is regular (i.e. has no pole) in this chart, and which transform through transition maps by taking the $\mathrm{d}x$ into account, cf. example A.1.1.24 below.

Since the sheaf Ω^1_X is a line bundle, it must be isomorphic to some $\mathcal{O}_X(D)$ by theorem A.1.1.21.

Definition A.1.1.23. A *canonical divisor* is a divisor D such that $\Omega^1_X \simeq \mathcal{O}_X(D)$. Canonical divisors on X form a single, whole linear equivalence class, called the *canonical class*.

In other words, a canonical divisor is a divisor of the form

$$\mathrm{div}(\omega) = \sum_{P \in X} \mathrm{ord}_P(\omega)$$

for some (not necessarily regular) differential 1-form ω on X, where $\mathrm{ord}_P(\omega)$ means $\mathrm{ord}_P(f)$ if ω reads $f(x)\mathrm{d}x$ in a chart with coordinate x and containing P.

Example A.1.1.24. Let $X = \mathbb{P}^1_K$ again, with charts x and $w = 1/x$ as in example A.1.1.8. Consider the differential form $\omega = (x^2 - x)\mathrm{d}x$. Then one also has $\omega = \left(\frac{1}{w^2} - \frac{1}{w}\right) \mathrm{d}\left(\frac{1}{w}\right) = \left(\frac{1}{w^3} - \frac{1}{w^4}\right) \mathrm{d}w$, so that $\mathrm{div}(\omega) = P_0 + P_1 - 4P_\infty$, where P_a denotes the point corresponding to $x = a$, and P_∞ denotes the point corresponding to $w = 0$. Consequently, the divisor $P_0 + P_1 - 4P_\infty$ is a canonical divisor.

The fact that the canonical class is well defined can be checked by remarking that the ratio of two differential 1-forms is a rational function, whose divisor is by definition principal.

I can now define the most important invariant of the curve X.

Definition A.1.1.25. The *genus* of X is the dimension of the space $\Gamma\Omega^1_X$ of regular differential 1-forms on X, which is finite by theorem A.1.1.18.

In what follows, I shall denote the genus of X by g.

Remark A.1.1.26. In the case $K = \mathbb{C}$, the curve X can be seen as a compact, connected Riemann surface, and I have already defined the genus of such a surface as the number of its "handles". It happens that this old definition agrees with the new one. The proof of this is not easy, cf. for instance [Bos89, theorem B.2.5].

Example A.1.1.27. Consider $X = \mathbb{P}^1_K$ with the notations of example A.1.1.8. Let $\omega \in \Gamma\Omega^1_X$ be a regular differential 1-form on X. Then one can write $\omega = f(x)\mathrm{d}x$ for some rational fraction $f(x) \in K(x)$. Since ω is regular, $f(x)$ cannot have a pole except maybe at P_∞, so it lies in $K[x]$. To examine the behaviour of $f(x)$ at P_∞, one switches to the coordinate $w = 1/x$, which yields $\omega = f(1/w)\mathrm{d}(1/w) = -\frac{f(1/w)}{w^2}\mathrm{d}w$. It follows that ω has a pole of order $2 + \deg f \geqslant 2$ at P_∞, so that it cannot be regular unless $f = 0$. The space of regular differential 1-forms $\Gamma\Omega^1_X$ is therefore reduced to $\{0\}$; in particular, the genus of X is $g = 0$.

Example A.1.1.28. Let $g \in \mathbb{N}$, and let X be the projective normal curve corresponding to the affine equation

$$Y^2 = \prod_{n=1}^{2g+2} (X - \alpha_n),$$

where the α_i are $2g+2$ pairwise distinct elements of K. Then the differential 1-forms

$$\omega_i = \frac{x^i \mathrm{d}x}{y}, \quad i = 0, \cdots, g-1$$

are regular. Indeed, the only suspicious points to check are the $2g+2$ points

$$(x = \alpha_n, y = 0)$$

and the two points at infinity of X, but

- at the points $(x = \alpha_n, y = 0)$, one has $x = Cy^2 + O(y^3)$ for some non-zero constant C, so y can be used at a local coordinate there, and

  $$\omega_i = \frac{C^i y^{2i} 2Cy}{y}\big(1 + O(Y)\big)\mathrm{d}y$$

  is regular there, and

- at the two points at infinity, $w = 1/x$ can be used as a local coordinate since $1/y = \pm w^{g+1} + O(w^{g+2})$, and $\omega_i = \pm\frac{-w^{-i-2}}{w^{-g-1}}\big(1 + O(w)\big)\mathrm{d}w$ is regular there since $i < g$.

Conversely, one sees that $\omega_0 = \frac{\mathrm{d}x}{y}$ vanishes at the order $g-1$ at the two points at infinity, and does not vanish anywhere else, so that a regular differential 1-form on X can be written $\omega = f\omega_0$ where $f \in K(X)$ is a rational function which is regular except possibly at the points at infinity. Thus $f \in K[x, y]$ is a polynomial, which can be written

$$f = P(x) + yQ(x)$$

in view of the equation defining X. Since

$$\omega = \frac{P(x)\mathrm{d}x}{y} + Q(x)\mathrm{d}x = \left(\pm\frac{-w^{-\deg(P)-2}}{w^{-g-1}} - w^{-\deg(Q)-2}\right)\big(1 + O(w)\big)\mathrm{d}w$$

must be regular at the points at infinity, this forces $Q = 0$ and $\deg P < g$, so that the forms ω_i form a basis of the space $\Gamma\Omega^1_X$ of regular differential 1-forms on X. In particular, the genus of X is g.

The genus is a crucial invariant of the curve, which will play a central role in the Riemann-Roch theorem.

A.1.1.4 The Riemann-Roch theorem

Let me begin by reviewing some sheaf cohomology. Let $\mathfrak{A}$ be an abelian category. The category of $\mathfrak{A}$-valued sheaves over X is then abelian itself, and the "global sections" functor Γ is easily seen to be left exact, but not right exact in general. It is thus natural to introduce its right derived functors $R^i\Gamma$, which I shall denote by $H^i(X, \cdot)$. In particular, $H^0(X, \cdot)$ is merely a new notation for Γ, which I shall use from now on. Furthermore, every short exact sequence of $\mathfrak{A}$-valued sheaves over X

$$0 \longrightarrow \mathcal{A} \longrightarrow \mathcal{B} \longrightarrow \mathcal{C} \longrightarrow 0$$

gives rise in $\mathfrak{A}$ to a long exact sequence

$$\begin{array}{l} 0 \longrightarrow H^0(X,\mathcal{A}) \longrightarrow H^0(X,\mathcal{B}) \longrightarrow H^0(X,\mathcal{C}) \\ \qquad\longrightarrow H^1(X,\mathcal{A}) \longrightarrow H^1(X,\mathcal{B}) \longrightarrow H^1(X,\mathcal{C}) \\ \qquad\longrightarrow H^2(X,\mathcal{A}) \longrightarrow \cdots \end{array}$$

Finally, since X has dimension 1, the $H^i(X, \cdot)$ vanish identically for $i \geqslant 2$:

Lemma A.1.1.29. *(Grothendieck, [Har77, theorem III.2.7]) Let V be an algebraic variety of dimension d. The $H^i(X, \cdot)$ vanish identically for all $i > d$.*

Example A.1.1.30 (A little technical)**.** Let $\mathcal{K}_X^*$ be the constant sheaf with stalk $K(X)^*$. It fits in the short exact sequence

$$1 \longrightarrow \mathcal{O}_X^* \longrightarrow \mathcal{K}_X^* \longrightarrow \mathcal{K}_X^*/\mathcal{O}_X^* \longrightarrow 1$$

and $H^1(X, \mathcal{K}_X^*) = 0$ since $\mathcal{K}_X^*$ is constant, hence flasque. Besides, $H^0(X, \mathcal{K}_X^*/\mathcal{O}_X^*)$ is the group of Cartier divisors on X, which agrees with $\mathrm{Div}(X)$ since X is non singular and absolutely integral ([Har77, Remark 6.11.1A]). Taking cohomology thus yields the exact sequence

$$1 \longrightarrow K^* \longrightarrow K(X)^* \longrightarrow \mathrm{Div}(X) \longrightarrow H^1(X, \mathcal{O}_X^*) \longrightarrow 0\ ,$$

which proves that $H^1(X, \mathcal{O}_X^*)$ is isomorphic to $\mathrm{Pic}(X)$.

As I announced previously, the goal of Riemann-Roch theory is to study the global section spaces $H^0\big(X, \mathcal{O}_X(D)\big)$ for $D \in \mathrm{Div}(X)$. For the sake of brevity, I shall write $H^i(X, D)$ instead of $H^i\big(X, \mathcal{O}_X(D)\big)$ from now on, or even $H^i(D)$ if no confusion about X can arise. I shall also write $h^i(X, D)$, or even $h^i(D)$, to mean $\dim_K H^i\big(X, \mathcal{O}_X(D)\big)$, and I define h^i similarly for line bundles. Finally, I define $\Omega^1_X(D)$ to be $\mathcal{O}_X(D) \underset{\mathcal{O}_X}{\otimes} \Omega_1^X$, so that

$$\Omega^1_X(D)(U) = \big\{\omega \mid \big(\mathrm{div}(\omega) + D\big)_{|U} \geqslant 0\big\} \text{ for every open subset } U \subseteq X.$$

Lemma A.1.1.31 (Serre duality)**.** *Let $D \in \mathrm{Div}(X)$ be a divisor on X. Then there exists a perfect pairing*

$$t\colon H^1\big(\mathcal{O}_X(D)\big) \underset{K}{\otimes} H^0\big(\Omega^1_X(D)\big) \longrightarrow K.$$

In particular, $h^1(D) = h^0(C - D)$, where C denotes a (any) canonical divisor.

In the language of line bundles, this can be rephrased as $h^1(\mathcal{L}) = h^0(\Omega^1_X \otimes \mathcal{L})$.

I shall not give the proof here, and refer instead to [Har77, section III.7]. I would still like to mention that the pairing t can be made explicit in the case of Riemann surfaces ($K = \mathbb{C}$), cf. [Bos89, sections B.5 to B.8].

I can now finally state the Riemann-Roch theorem.

Theorem A.1.1.32 (Riemann-Roch)**.** *Let $\mathcal{L}$ be a line bundle on X of degree d.*

(i) $h^0(\mathcal{L}) = d + 1 - g + h^0(\Omega^1_X \otimes \mathcal{L}^\vee)$.

(ii) $\deg \Omega^1_X = 2g - 2$.

(iii) $h^0(\mathcal{L}) = d + 1 - g$ *if* $d \geqslant 2g - 1$.

(iv) If $K = \overline{K}$, $h^0(\mathcal{L}) = \max(d+1-g, 1)$ *for* $\mathcal{L} = \mathcal{O}_X(\sum_{i=1}^d P_i)$ *with generic* $P_i \in X$.

(v) If $K = \overline{K}$, $h^0(\mathcal{L}) = \max(d + 1 - g, 0)$ *for generic* $\mathcal{L}$.

I first rephrase this in terms of divisors, since I shall mostly use it in this way:

Corollary A.1.1.33 (Riemann-Roch)**.** *Let $D \in \mathrm{Div}(X)$ be a divisor on X of degree d, and let C be a canonical divisor.*

(i) $h^0(D) = d + 1 - g + h^0(C - D)$.

(ii) $\deg C = 2g - 2$.

(iii) $h^0(D) = d + 1 - g$ *if* $d \geqslant 2g - 1$.

(iv) If $K = \overline{K}$, $h^0(D) = \max(d + 1 - g, 1)$ *for generic* ***effective*** D.

(v) If $K = \overline{K}$, $h^0(D) = \max(d + 1 - g, 0)$ *for generic* D.

Proof. I shall only give a sketch of the proof here, and refer the reader to [Har77, theorem IV.1.3] for the details.

(i) Notice first that the formula is true in the case $\mathcal{L} = \mathcal{O}_X$, since one has then $d = 0$, $h^0(\mathcal{O}_X) = 1$ by example A.1.1.19, and $h^0(\Omega^1_X) = g$ by definition.

Next, define the *Euler characteristic* of $\mathcal{L}$ by

$$\chi(D) = \sum_{i=0}^{+\infty} (-1)^i h^i(\mathcal{L}).$$

By lemma A.1.1.29, the terms of this sum are actually 0 for $i \geqslant 2$, so that

$$\chi(\mathcal{L}) = h^0(\mathcal{L}) - h^1(\mathcal{L}) = h^0(\mathcal{L}) - h^0(\Omega^1_X \otimes \mathcal{L}^\vee)$$

by Serre duality (lemma A.1.1.31). This means that part (i) rewrites as

$$\chi(\mathcal{L}) = d + 1 - g, \qquad (\star)$$

which I now prove. By theorem A.1.1.21, one may assume without loss of generality that $\mathcal{L} = \mathcal{O}_X(D)$. I have already pointed out that $(\star)$ holds for $D = 0$. To conclude, I shall now show that $(\star)$ holds for D if and only it holds for $D + E$, where $E = P_1 + \cdots + P_r \in \mathrm{Eff}(X)$ denotes an irreducible effective divisor on X, that is to say a whole $\mathrm{Gal}(\overline{K}/K)$-orbit of points on X. View E as a subvariety of X of dimension 0, let $L = K(E) \simeq K(P_1)$ denote the field of Galois-equivariant functions (that is to say $f\big(\sigma(P_i)\big) = \sigma\big(f(P_i)\big)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$) on E, and let $\mathcal{O}_E$ denote its structure sheaf, so that one has the short exact sequence

$$0 \longrightarrow \mathcal{O}_X(-E) \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_E \longrightarrow 0.$$

Tensoring with $\mathcal{O}_X(D + E)$, one gets

$$0 \longrightarrow \mathcal{O}_X(D) \longrightarrow \mathcal{O}_X(D + E) \longrightarrow \mathcal{O}_E \longrightarrow 0.$$

Since the Euler characteristic is additive on short exact sequences, as can be easily seen by looking at the associated long exact sequence in cohomology, this implies that $\chi\big(\mathcal{O}_X(D+E)\big) = \chi\big(\mathcal{O}_X(D)\big) + \chi(\mathcal{O}_E)$. But $h^1(O_E) = 0$ by lemma A.1.1.29 since E is 0-dimensional, so that $\chi(\mathcal{O}_E) = h^0(\mathcal{O}_E) = \dim_K L = r$, hence $\chi\big(\mathcal{O}_X(D + P)\big) = \chi\big(\mathcal{O}_X(D)\big) + r$. On the other hand, one also has $\deg(D + E) = \deg(D) + r$. This concludes the proof of (i).

(ii) Follows immediately from (i) by taking $\mathcal{L} = \Omega^1_X$.

(iii) By (ii), $\Omega^1_X \otimes \mathcal{L}^\vee$ has degree $2g-2-d$, which is negative by hypothesis. Lemma A.1.1.20 then implies that $h^0(\Omega^1_X \otimes \mathcal{L}^\vee)$ vanishes.

(iv) One sees by induction on d that $h^0\big(\Omega^1_X(-\sum_{i=1}^d P_i)\big) = \max(g-d, 0)$ for generic $P_i \in X$. The result then follows from (i).

(v) Again, one can assume without loss of generality that $\mathcal{L} = \mathcal{O}_X(D)$. Now, if $h^0(D) > 0$, then $h^0(D - P) = h^0(D) - 1$ for generic P. The result then follows from (iv).

□

I shall now give two examples illustrating the power of the Riemann-Roch theorem.

Example A.1.1.34. Let X be a curve of genus 0. Then, by the Riemann-Roch theorem A.1.1.33(iii), $h^0(D) = \deg(D) + 1$ for every divisor D on X provided that $\deg D \geqslant -1$. In particular, $h^0(D) = 1$ for all $D \in \mathrm{Div}^0(X)$, so that for

each such D there exists a non-zero rational function $f \in K(X)^*$ such that $E = \mathrm{div}(f) + D$ is effective. But $\deg(E) = \deg\big(\mathrm{div}(f)\big) + \deg(D) = 0$, so $E = 0$ and $D = -\mathrm{div}(f) = \mathrm{div}(1/f)$ is principal. It follows that the class group $\mathrm{Cl}^0(X)$ is trivial, so that X is a twist of $\mathbb{P}^1_K$ by example A.1.1.17. This is a converse to example A.1.1.27.

Example A.1.1.35 (Elliptic curves)**.** Let X be of genus $g = 1$, and assume that there exists a K-rational point $O \in X(K)$. Such a curve is called an *elliptic curve*. The Riemann-Roch theorem A.1.1.33(iii) then implies that $h^0(D) = \deg(D)$ for all $D \in \mathrm{Div}(X)$ such that $\deg D \geqslant 1$.

In particular, $h^0(O) = 1$ so $H^0(O) = K$ since it clearly contains K, whereas $h^0(2O) = 2$ so that $H^0(2O) = K \oplus Kx = \langle 1, x\rangle_K$ for some rational function $x \in K(X)^*$ which has thus a double pole at O and no other pole. Continuing, one finds that $H^0(3O) = \langle 1, x, y\rangle_K$ for some $y \in K(X)^*$ having a pole of order 3 at O and no other pole. Next, $h^0(4O) = 4$, but $x^2 \in H^0(4O)$, so that $H^0(4O) = \langle 1, x, y, x^2\rangle_K$. Similarly, $H^0(5O) = \langle 1, x, y, x^2, xy\rangle_K$. Then, one sees that $H^0(6O)$ contains the 7 functions $1, x, y, x^2, xy, x^3$ and y^2, but since its dimension is 6, these functions must be linearly dependent, and by looking at the order of their poles at O one sees that the linear dependence relation must be of the form

$$y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6 \qquad (A)$$

for some scalars $a_0, \cdots, a_6 \in K$ such that $a_0 \neq 0$. The functions x and y thus define a morphism f from X to the plane curve A which is the projective completion of the affine curve of equation (A).

Let $P, Q \in X(\overline{K})$ be distinct from O. If $f(P) = f(Q)$ but $P \neq Q$, then the functions $x - x(P)$ and $y - y(P)$ both lie in $H^0(3O - P - Q)$ which is of dimension 1, so are proportional, but this is absurd since the order of their pole at O is not the same. The morphism f is therefore injective, so it has degree 1, which proves that f is an isomorphism from X to A.

Furthermore, for every divisor D on X of degree 0, the space $H^0(D + O)$ has dimension 1, so there exists a non-zero function $f \in K(X)^*$ such that $E = D + O + \mathrm{div}(f)$ is effective. Since E has degree 1, it consists in a single K-rational point $P \in X(K)$. Every divisor of degree 0 is therefore linearly equivalent to a divisor of the form $P - O$, and the point P is unique since if there existed two distinct points $P, Q \in X(K)$ such that $P \sim Q$, then there would exist a rational function $f \in K(X)$ such that $\mathrm{div}(f) = P - Q$, which would imply that f is an isomorphism from X to $\mathbb{P}^1_K$ as in example A.1.1.17, which is impossible since X is of genus 1 whereas $\mathbb{P}^1_K$ is of genus 0. It follows that $P \mapsto P - O$ is a bijection between $X(K)$ and $\mathrm{Cl}^0(X)$. In particular, the abelian group structure of $\mathrm{Cl}^0(X)$ yields an abelian group structure on $X(K)$, with neutral element $O \in X(K)$. Let $\boxplus$ denote the resulting group law on $X(K)$. By construction, one has the equivalence

$$\sum_{P\in X} n_P P \in \mathrm{Div}(X) \text{ is principal } \iff \sum_{P\in X} n_P = 0 \text{ in } \mathbb{Z} \text{ and } \boxplus_{P\in X} n_P P = O \text{ in } X(K).$$

Besides, upon identification of X with the plane curve A, if one takes 3 pairwise distinct points $P, Q, R \in X(K)$ distinct from O and which lie on a line of equation

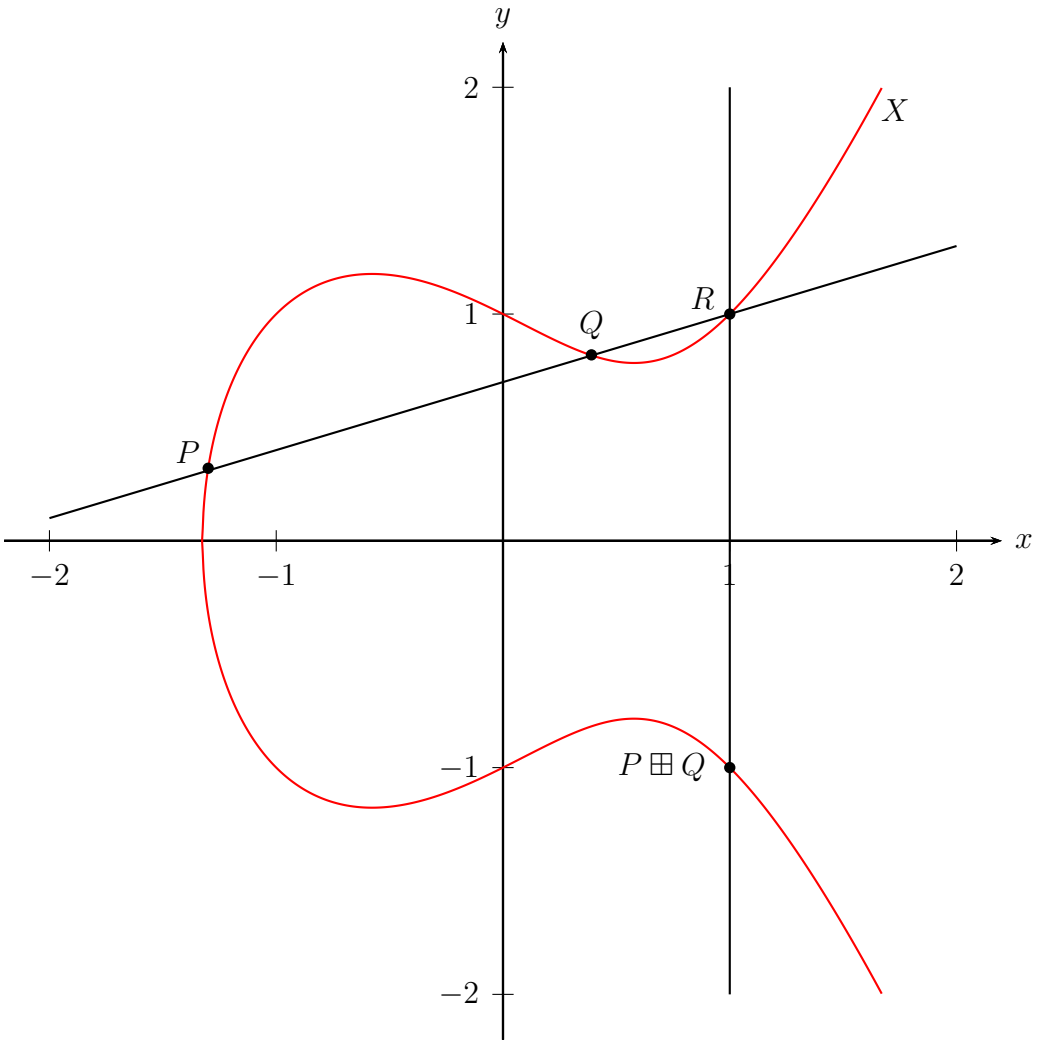


Figure A.1.1.36: The group law on an elliptic curve

$ax+by+c=0$, then one sees that the divisor of the function $f=ax+by+c\in K(X)$ is $\mathrm{div}(f)=P+Q+R-3O$ since b cannot be 0, so that $(P-O)+(Q-O)+(R-O)\sim 0$, i.e. $P\boxplus Q\boxplus R=O$ in the group $X(K)$. It follows that the group law $\boxplus$ on $X(K)$ is defined by the famous "chord process", as illustrated on figure A.1.1.36.

I shall finish this first section by stating a very useful consequence of the Riemann-Roch theorem.

Proposition A.1.1.37. *Fix a divisor $D_0\in\mathrm{Div}(X)$ of X of degree n. If $n\geqslant g$, the every divisor $D\in\mathrm{Div}^0(X)$ of degree 0 is linearly equivalent to a divisor of the form $E-D_0$, where $E\in\mathrm{Eff}^n(X)$ is an effective divisor of degree n. Furthermore, if $n=g$, then E is unique for generic D.*

Proof. Since the degree of $D+D_0$ is $n\geqslant g$, the Riemann-Roch theorem A.1.1.33(i) implies that $h^0(D+D_0)>0$. In particular, $H^0(D+D_0)$ is not reduced to $\{0\}$, so there exists a non-zero rational function $f\in K(X)^*$ such that

$$E=\mathrm{div}(f)+D+D_0$$

is effective. This divisor E has the same degree n by lemma A.1.1.9, and $D \sim D + \operatorname{div}(f) = E - D_0$. Furthermore, if $n = g$ and if $D \sim E - D_0 \sim E' - D_0$, then there exists a non-zero rational function $\alpha \in K(X)^*$ such that $E' - D_0 = E - D_0 + \operatorname{div}(\alpha)$, hence $\operatorname{div}(\alpha) + E = E'$ is effective, so $\alpha \in H^0(E)$. But $H^0(E) = K$ consists only of the constant functions for generic E by the Riemann-Roch theorem A.1.1.33, so that for generic D one has $\alpha \in K$ hence $\operatorname{div}(\alpha) = 0$ and thus $E = E'$. □

Corollary A.1.1.38. *Fix a K-rational origin point $O \in X(K)$ (assuming that such a point exists). Every divisor $D \in \operatorname{Div}^0(X)$ of degree 0 is linearly equivalent to a divisor of the form $E - gO$, where $E \in \operatorname{Eff}^g(X)$ is an effective divisor of degree g. Furthermore, E is unique for generic D.*

I shall conclude by stating another theorem, which is especially useful for computing the genus of a curve, which is an essential information in order to be able to use the Riemann-Roch theorem.

Theorem A.1.1.39 (Riemann-Hurwitz)**.** *Let X and Y be projective, non-singular, geometrically integral curves of respective genera g_X and g_Y, and let $f\colon X \longrightarrow Y$ be a non-constant morphism of degree $d \in \mathbb{N}$. If the characteristic of the ground field K does not divide any of the ramification indices e_P (or is 0), then*

$$2g_X - 2 = (2g_Y - 2)d + \sum_{P \in X} (e_P - 1).$$

This theorem is generally used to deduce the genus of X form the one of Y. Typically, one takes $Y = \mathbb{P}^1_K$, that is to say f is just a non-constant rational function on X. One can then deduce information about the genus of X from information about the ramification of f, since $g_Y = 0$ by example A.1.1.27.

Proof. Let ω_Y be a (possibly not regular) differential 1-form on Y, and let $C_Y = \sum_{Q \in Y} m_Q Q$ be its divisor. Then C_Y is a canonical divisor on Y, and therefore $\deg C_Y = 2g_Y - 2$ according to the Riemann-Roch theorem A.1.1.33(ii).

Let now $f^*\omega_Y$ be the pull-back of ω_Y by f, and let $C_X = \sum_{P \in X} n_P P$ be its divisor. Then C_X is a canonical divisor on X, so that $\deg C_X = 2g_X - 2$ for the same reason. Furthermore, let P be a point of X with local coordinate x, and let y be a local coordinate at $Q = f(P)$. Then ω_Y can be written

$$\omega = y^{m_Q} u(y) \mathrm{d}y$$

where $u \in K(Y)^*$ is a rational function which has neither a zero nor a pole at Q by definition of m_Q. Since one may suppose that $y \circ f = x^{e_P}$ by definition of e_P, one has

$$f^*\omega_Y = x^{e_P m_Q} u(x^{e_P}) e_P x^{e_P - 1} \mathrm{d}x = x^{e_P m_Q + e_P - 1} v(x) \mathrm{d}x,$$

where the rational function $v(x) = e_P u(x^{e_P}) \in K(X)^*$ on X has neither zero nor pole at P since $e_P \neq 0$ in K by hypothesis. It follows that

$$C_X = \operatorname{div}(f^*\omega_Y) = \sum_{P \in X} (e_P m_{f(P)} + e_P - 1) P$$

$$= f^* \left(\sum_{Q \in Y} m_Q Q \right) + \sum_{P \in X} (e_P - 1) P = f^* C_Y + \sum_{P \in X} (e_P - 1) P.$$

Since f^* multiplies the degrees by $\deg f$, the result follows by taking the degrees. □

A.1.2 The jacobian variety

I shall now explain the construction of the jacobian of the curve X. I shall assume the same hypotheses on X and use the same notations as in the previous part. In particular, X is a curve of genus g defined over the perfect field K.

The jacobian variety of X is an abelian variety (that is to say a projective variety which, much like an elliptic curve, is endowed with an abelian[1] group structure compatible with the algebraic variety structure) of dimension g which is an avatar of the class group $\mathrm{Pic}^0(X)$ of X. I shall denote this jacobian by $\mathrm{Jac}(X)$. This realisation of $\mathrm{Pic}^0(X)$ as an algebraic variety is extremely fruitful, in that it gives a lot of new structure and information on it.

Although $\mathrm{Jac}(X)$ exists whatever the base field K is, I shall mainly focus on the case $K = \mathbb{C}$ in this section, and hence view X as a compact, connected Riemann surface of genus g. There are two reasons for this: the first is that the construction of $\mathrm{Jac}(X)$ is much more visual over $\mathbb{C}$, and the second is that the algorithms which are the core of my thesis mostly use $\mathrm{Jac}(X)$ over $\mathbb{C}$. I shall, however, give a few words on the general case in the end of this section.

I first show that the problem of giving a meaning to integrals of the form $\int_A^B \omega$ on X leads naturally to the notion of a period on X and to the definition of the Abel-Jacobi map from X to $\mathrm{Jac}(X)$, the latter being seen as a complex torus. I then prove the Abel-Jacobi theorem, and explain why $\mathrm{Jac}(X)$ can be embedded into a projective space.

For the sake of brevity, I shall denote by $\Omega^1(X)$ the $\mathbb{C}$-vector space $\Gamma\Omega^1_X$ of holomorphic differential 1-forms on X.

A.1.2.1 The period lattice

To begin with, consider the problem of assigning a value to the integral

$$\int_A^B \omega,$$

where A, B are points on X and $\omega \in \Omega^1(X)$ is a differential form. The value of this integral is not well-defined, since it depends on the path from A to B one chooses to integrate along.

This dependence is however "discrete". By this, I mean that Cauchy's theorem implies that homologous paths will yield the same value. In attempt to get rid of the ambiguity, it is thus natural to have a look at the homology group $H_1(X, \mathbb{Z})$ of the Riemann surface X.

As shown on figure A.1.2.1, $H_1(X, \mathbb{Z})$ is a free abelian group of rank $2g$, with 2 generators for each handle of X. In order to remedy to the ill-definedness of integrals of the form $\int_A^B \omega$, it is thus natural to study the integration pairing

$$\begin{array}{ccc} H_1(X, \mathbb{Z}) \otimes \Omega^1(X) & \longrightarrow & \mathbb{C} \\ \gamma \otimes \omega & \longmapsto & \displaystyle\int_\gamma \omega \end{array}.$$

[1] The fact that the group law is abelian is actually a consequence of the projectiveness of the variety, cf. [HS00, lemma A.7.1.3].

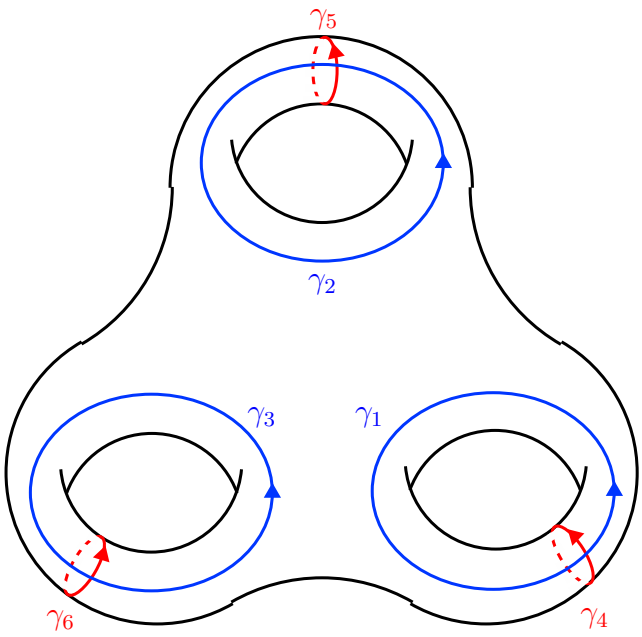


Figure A.1.2.1: A Riemann surface of genus $g = 3$ with a symplectic homology basis

Definition A.1.2.2. An integral of the form $\int_\gamma \omega$ for some $\gamma \in H_1(X, \mathbb{Z})$ and some $\omega \in \Omega^1_X$ is called a *period* of X.

Fix a $\mathbb{C}$-basis $(\omega_i)_{1 \leqslant i \leqslant g}$ of $\Omega^1(X)$ and a $\mathbb{Z}$-basis $(\gamma_j)_{1 \leqslant j \leqslant 2g}$ of $H_1(X, \mathbb{Z})$. The matrix

$$\left[\int_{\gamma_j} \omega_i \right]_{\substack{1 \leqslant i \leqslant g \\ 1 \leqslant j \leqslant 2g}} \in \mathrm{Mat}_{g \times 2g}(\mathbb{C})$$

is called the *period matrix* of X with respect to these bases.

Due to the ambiguity in the choice of bases, the period matrix for X is well-defined only up to multiplication by $\mathrm{GL}_g(\mathbb{C})$ on the left and by $\mathrm{GL}_{2g}(\mathbb{Z})$ on the right.

The period matrix has a nicer structure if one restricts the choice of basis of $H_1(X, \mathbb{Z})$ to bases of a special kind. In order to single out this better kind of basis, I shall first review the intersection pairing on $H_1(X, \mathbb{Z})$.

Definition A.1.2.3. The *intersection number* of two oriented cycles α, β which intersect transversally is defined to be

$$\alpha \wedge \beta = \sum_{P \in \alpha \cap \beta} \epsilon_P,$$

where ϵ_P is $+1$ if the oriented tangent vectors of α and β, in this order, form an oriented basis of the tangent space of X at P, whereas ϵ_P is -1 if they form an anti-oriented basis of the tangent space.

One can show (cf. [GH78, first subsection of 0.4]) that every null-homologous cycle has intersection number 0 with every cycle which it intersects transversally, so

that $\alpha \wedge \beta$ depends only on the homology class of α and β, and can thus be defined even if α and β fail to intersect transversely. This yields an alternating pairing

$$H_1(X, \mathbb{Z}) \wedge H_1(X, \mathbb{Z}) \longrightarrow \mathbb{Z},$$

called the intersection pairing.

Definition A.1.2.4. A basis $(\gamma_j)_{1 \leqslant j \leqslant 2g}$ of $H_1(X, \mathbb{Z})$ is said to be *symplectic* if the matrix of the intersection paring in this basis is

$$J_g = \begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix} \in M_{2g \times 2g}(\mathbb{Z}),$$

where I_g denotes the identity matrix of size g.

Example A.1.2.5. The homology basis shown in figure A.1.2.1 is symplectic.

I shall only consider *symplectic* bases of $H_1(X, \mathbb{Z})$ from now on. This means that period matrices of X are all equivalent up to multiplication by $\mathrm{GL}_g(\mathbb{C})$ on the left, and by multiplication by $\mathrm{Sp}_{2g}(\mathbb{Z})$ on the right, where

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \{A \in M_{2g \times 2g}(\mathbb{Z}) \mid {}^{\mathrm{t}}A J_g A = J_g\}$$

denotes the *symplectic group* of degree $2g$ over $\mathbb{Z}$.

Figure A.1.2.6 below attempts to show that if one were to use scissors to cut X along a symplectic basis of its homology, one would obtain a connected, simply connected domain, which is actually a $4g$-gon if one identifies the scissor cuts with boundary edges.

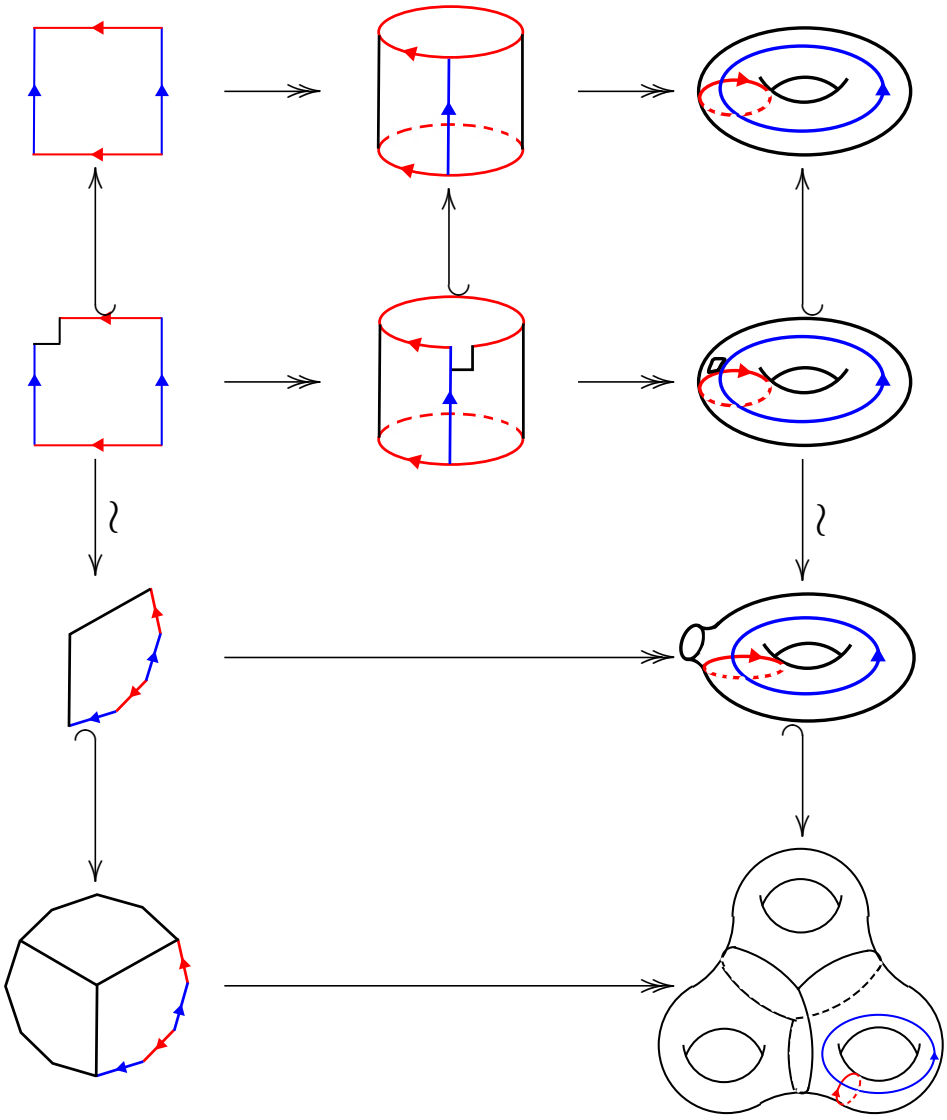


Figure A.1.2.6: The canonical dissection of a Riemann surface of genus $g = 3$

This means that the Riemann surface X can be constructed by gluing the edges of a $4g$-gon Π is a certain way. More precisely, if one labels the vertices of Π by A_k, B_k, C_k D_k, A_{k+1}... where the index k is understood modulo g, then X can be constructed by gluing D_kA_{k+1} to C_kB_k and C_kD_k to B_kA_k for each $k \in \mathbb{Z}/k\mathbb{Z}$, as shown on figure A.1.2.7. Once this is done, the images of C_0D_0, C_1D_1, $\cdots$, $C_{g-1}D_{g-1}$, D_0A_1, D_1A_2, $\cdots$, $D_{g-1}A_0$ form a symplectic basis of $H_1(X,\mathbb{Z})$, as shown on figure A.1.2.6.

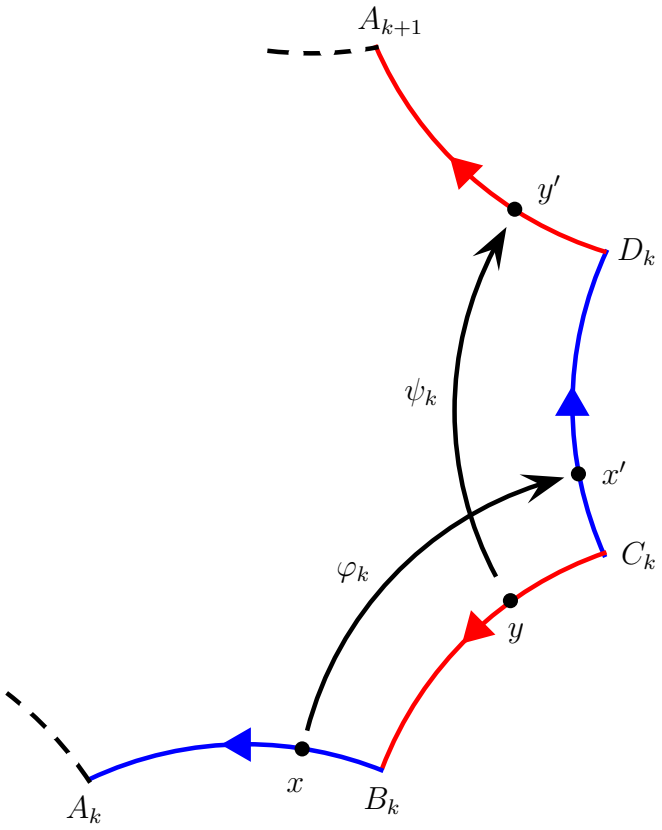


Figure A.1.2.7: Construction of X by gluing the edges of a $4g$-gon

In order to study the structure of the period matrix of X, I shall now temporarily forget the complex structure on X, and view it as an oriented surface over $\mathbb{R}$. With this point of view, I can establish the following formula:

Lemma A.1.2.8. *Let $(\gamma_j)_{1\leqslant j\leqslant 2g}$ be a symplectic basis of $H_1(X,\mathbb{Z})$. For any two closed smooth differential 1-forms ω_1 and ω_2 on X, one has the relation*

$$\iint_X \omega_1 \wedge \omega_2 = \sum_{k=1}^{g} \left(\int_{\gamma_k} \omega_1 \int_{\gamma_{g+k}} \omega_2 - \int_{\gamma_k} \omega_2 \int_{\gamma_{g+k}} \omega_1 \right).$$

Proof. Let $p\colon \Pi \twoheadrightarrow X$ be the gluing as described above, and let $\eta_1 = p^*\omega_1$, $\eta_2 = p^*\omega_2$ be the pull-backs of ω_1 and ω_2 on Π. They are closed since ω_1 and ω_2 are, hence exact since Π is simply connected. In particular, there exists a smooth function $f_1 = \int \eta_1 \colon \Pi \longrightarrow \mathbb{C}$ such that $\eta_1 = \mathrm{d}f_1$. One then has $\mathrm{d}(f_1\eta_2) = \mathrm{d}(f_1)\wedge\eta_2 + f_1\mathrm{d}(\eta_2) = \eta_1 \wedge \eta_2$ since η_2 is closed, so that the Stokes theorem yields

$$\iint_X \omega_1 \wedge \omega_2 = \iint_\Pi \eta_1 \wedge \eta_2 = \oint_{\partial\Pi} f_1\eta_2.$$

Write this contour integral as

$$\sum_{k=1}^{g}\left(\int_{A_k}^{B_k}+\int_{B_k}^{C_k}+\int_{C_k}^{D_k}+\int_{D_k}^{A_{k+1}}\right)f_1\eta_2,$$

and study each of the g terms of the sum separately.

Let x, $x'=\varphi_k(x)$, y and $y'=\psi_k(y)$ be as on figure A.1.2.7. Then one has

$$f_1(x')-f_1(x)=\int_x^{x'}\eta_1=\left(\int_x^{B_k}+\int_{B_k}^{C_k}+\int_{C_k}^{x'}\right)\eta_1=\int_{B_k}^{C_k}\eta_1=-\int_{\gamma_{g+k}}\omega_1$$

because $\eta_1=p^*\omega_1$ is the same on C_kD_k as on B_kA_k, so that the two outer integrals cancel out. Similarly, one finds that

$$f_1(y')-f_1(y)=\int_y^{y'}\eta_1=\left(\int_y^{C_k}+\int_{C_k}^{D_k}+\int_{D_k}^{y'}\right)\eta_1=\int_{C_k}^{D_k}\eta_1=\int_{\gamma_k}\omega_1.$$

One then concludes that

$$\left(\int_{A_k}^{B_k}+\int_{C_k}^{D_k}\right)f_1\eta_2=\left(\int_{C_k}^{D_k}-\int_{B_k}^{A_k}\right)f_1\eta_2=-\int_{\gamma_{g+k}}\omega_1\int_{C_k}^{D_k}\eta_2=-\int_{\gamma_{g+k}}\omega_1\int_{\gamma_k}\omega_2$$

since replacing C_kD_k with B_kA_k does not affect $\eta_2=p^*\omega_2$ and shifts f_1 by $-\int_{\gamma_{g+k}}\omega_1$ as seen above, and similarly that

$$\left(\int_{B_k}^{C_k}+\int_{D_k}^{A_{k+1}}\right)f_1\eta_2=\left(\int_{D_k}^{A_{k+1}}-\int_{C_k}^{B_k}\right)f_1\eta_2=\int_{\gamma_k}\omega_1\int_{D_k}^{A_{k+1}}\eta_2=-\int_{\gamma_k}\omega_1\int_{\gamma_{g+k}}\omega_2,$$

hence the result. □

Come back to viewing X as a Riemann surface. One can make some easy observations about the double integral in the above lemma:

Lemma A.1.2.9. *(a) Let ω_1 and $\omega_2\in\Omega^1(X)$ be holomorphic differential forms on X. Then $\iint_X\omega_1\wedge\omega_2=0$.*

(b) Let ω be a non-zero holomorphic differential form on X. Then $i\iint_X\omega\wedge\overline{\omega}>0$.

(c) If $\iint_X\omega\wedge\overline{\omega}=0$ for a holomorphic differential form ω on X, then $\omega=0$.

Proof. (a) Locally, one can write $\omega_1=f_1(z)\mathrm{d}z$, $\omega_2=f_2(z)\mathrm{d}z$ with respect to some coordinate z. Then $\omega_1\wedge\omega_2=0$ since $\mathrm{d}z\wedge\mathrm{d}z=0$.

(b) Let $\omega=f(z)\mathrm{d}z$, $z=x+iy$ locally. Then $\overline{\omega}=\overline{f(z)}\mathrm{d}\overline{z}$, so that

$$i\omega\wedge\overline{\omega}=|f(z)|^2i\mathrm{d}z\wedge\mathrm{d}\overline{z}=2|f(z)|^2dx\wedge dy.$$

(c) Follows directly from (b).

□

One then finds that the period matrix of X has a particular structure.

Proposition A.1.2.10. *Let $P \in \mathrm{Mat}_{g\times 2g}(\mathbb{C})$ be a period matrix of X with respect to a symplectic basis of $H_1(X,\mathbb{Z})$ and to a basis $(\omega_i)_{1\leqslant i\leqslant g}$ of $\Omega^1(X)$. Consider the left $g\times g$ block of P. Then this block cannot be singular.*

Proof. If this block were singular, then there would exist a non-trivial $\mathbb{C}$-linear combination of its lines which vanishes. Let $\omega \in \Omega^1(X)$ be the $\mathbb{C}$-linear combination of the ω_i with the same coefficients. Then $\omega \neq 0$ since these coefficients are not all 0, and yet $\int_{\gamma_j}\omega = 0$ for all $1 \leqslant j \leqslant g$ by definition of the period matrix. But then one also has $\int_{\gamma_j}\overline{\omega} = \overline{\int_{\gamma_j}\omega} = 0$ for all $1 \leqslant j \leqslant g$, hence $\iint_X \omega\wedge\overline{\omega} = 0$ by lemma A.1.2.8. But this contradicts lemma A.1.2.9(c). □

This implies that, once the symplectic basis of $H_1(X,\mathbb{Z})$ is fixed, there exists a *dual* basis of $\Omega^1(X)$, that is to say a basis $(\omega_i)_{1\leqslant i\leqslant g}$ such that

$$\int_{\gamma_j}\omega_i = \mathbb{1}_{i=j}.$$

The period matrix with respect to these bases thus reads

$$P = \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \tau \\ 0 & & 1 & \end{array}\right]$$

for some $\tau \in \mathrm{Mat}_{g\times g}(\mathbb{C})$.

Theorem A.1.2.11 (Riemann bilinear relations)**.** *The matrix τ is symmetric, and its imaginary part is positive definite.*

Proof. One computes that

$$\tau_{j,i}-\tau_{i,j} = \int_{\gamma_{g+i}}\omega_j - \int_{\gamma_{g+j}}\omega_i = \sum_{k=1}^{g}\left(\int_{\gamma_k}\omega_i\int_{\gamma_{g+k}}\omega_j - \int_{\gamma_k}\omega_j\int_{\gamma_{g+k}}\omega_i\right) = \iint_X \omega_i\wedge\omega_j = 0$$

by lemmas A.1.2.8 and A.1.2.9(a). Hence τ is symmetric.

Let $(v_i)_{1\leqslant i\leqslant g} \in \mathbb{R}^g \setminus \{0\}$ be a non-zero real vector, and let $\omega = \sum_{i=1}^g v_i\omega_i$, which is non-zero as v is non-zero. Then

$$\begin{aligned}
{}^t v(\operatorname{Im}\tau)v &= \sum_{i=1}^{g}\sum_{j=1}^{g} v_i \operatorname{Im}\tau_{i,j} v_j = \frac{i}{2}\sum_{i=1}^{g}\sum_{j=1}^{g} v_i v_j(\overline{\tau_{i,j}} - \tau_{i,j}) \\
&= \frac{i}{2}\sum_{j=1}^{g}\left(v_j\sum_{i=1}^{g} v_i\overline{\int_{\gamma_{g+j}}\omega_i} - v_j\sum_{i=1}^{g} v_i\int_{\gamma_{g+j}}\omega_i\right) \\
&= \frac{i}{2}\sum_{j=1}^{g}\left(\int_{\gamma_j}\omega\int_{\gamma_{g+j}}\overline{\omega} - \int_{\gamma_j}\overline{\omega}\int_{\gamma_{g+j}}\omega\right) = \frac{i}{2}\iint_X \omega\wedge\overline{\omega} > 0
\end{aligned}$$

by lemmas A.1.2.8 and A.1.2.9(b). Hence $\operatorname{Im}\tau$ is positive-definite. □

Corollary A.1.2.12. *The $2g$ columns of the period matrix of X span a lattice in $\mathbb{C}^g$, called the* period lattice.

Actually, the above theorem has even stronger consequences, as I shall explain in the last part of this section.

With all this material at hand, it is finally time to define the jacobian variety $\mathrm{Jac}(X)$ of X.

Definition A.1.2.13. The jacobian of X is the complex torus

$$\mathrm{Jac}(X) = \mathbb{C}^g/\Lambda,$$

where Λ denotes the period lattice of X.

More canonically, I should use the coordinate-free definition

$$\mathrm{Jac}(X) = \Omega_1(X)^\vee/H_1(X,\mathbb{Z}),$$

where $V^\vee$ denotes the dual space of a $\mathbb{C}$-vector space V, and where the elements of homology group $H_1(X,\mathbb{Z})$ are seen as linear forms on $\Omega^1(X)$ by identifying a cycle γ to the linear form $\int_\gamma$.

A.1.2.2 The Abel-Jacobi map

Now that the periods are quotiented out, there is a well defined integration map

$$\begin{array}{rccc} \jmath: & X & \longrightarrow & \mathrm{Jac}(X) \\ & P & \longmapsto & \left(\displaystyle\int_O^P \omega_i\right)_{1\leqslant i\leqslant g} \end{array},$$

or, in more canonical terms,

$$P \longmapsto \int_O^P \mod H_1(X,\mathbb{Z}),$$

where $O \in X$ is a fixed origin point. One can show that this map actually embeds X in $\mathrm{Jac}(X)$, provided of course that the genus g is non-zero, cf. [HS00, corollary A.6.3.3]. I shall not prove this fact here, since I shall not need it.

This map may be extended by linearity to divisors on X, yielding a group morphism

$$\begin{array}{rccc} \jmath: & \mathrm{Div}(X) & \longrightarrow & \mathrm{Jac}(X) \\ & \displaystyle\sum_{k=1}^n n_k P_k & \longmapsto & \left(\displaystyle\sum_{k=1}^n n_k \int_O^{P_k} \omega_i\right)_{1\leqslant i\leqslant g} \end{array}.$$

This still depends on the choice of the origin point O. However, if one restricts it to the subgroup $\mathrm{Div}^0(X)$ of divisors of degree zero, one gets a canonical map.

Definition A.1.2.14. The map

$$\begin{array}{rccc} \jmath: & \mathrm{Div}^0(X) & \longrightarrow & \mathrm{Jac}(X) \\ & \displaystyle\sum_{k=1}^n n_k P_k & \longmapsto & \left(\displaystyle\sum_{k=1}^n n_k \int_O^{P_k} \omega_i\right)_{1\leqslant i\leqslant g} \end{array}$$

does not depend on O. It is called the *Abel-Jacobi* map.

The reason to introduce this map is explained by the following fundamental theorem.

Theorem A.1.2.15 (Abel-Jacobi)**.** *The Abel-Jacobi map* $\jmath\colon \mathrm{Div}^0(X) \longrightarrow \mathrm{Jac}(X)$ *is surjective, and its kernel consists exactly of the subgroup of principal divisors.*

In other words, the Abel-Jacobi map factors into a group isomorphism

$$\mathrm{Pic}^0(X) \xrightarrow{\sim} \mathrm{Jac}(X)\ .$$

This explains why the jacobian of X is so interesting: it is a concrete, geometric realisation of the class group $\mathrm{Pic}^0(X)$ of X. One can thus use the jacobian to establish various properties of the class group. For instance, one sees that, unless $g = 0$ of course, the class group is infinite, and uncountable.

More interestingly, one sees that the class group is divisible, and that for any $n \in \mathbb{N}$, its n-torsion subgroup is

$$\mathrm{Pic}^0(X)[n] \simeq \mathrm{Jac}(X)[n] = (\mathbb{C}^g/\Lambda)[n] = \frac{1}{n}\Lambda/\Lambda \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Example A.1.2.16. If the genus of X is $g = 1$, then I explained in example A.1.1.35 that X is an elliptic curve, and that $\mathrm{Pic}^0(X)$ is in bijection with X. This means that the jacobian of X, which is of dimension $g = 1$, is X itself. In particular, one recovers the fact that the Riemann surface X is a complex torus of dimension 1. One also sees that the subgroup $X[n]$ of n-torsion points of X is abstractly isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

Proof. • $\jmath$ is surjective

Consider the holomorphic map

$$\begin{array}{ccc} X^g & \longrightarrow & \mathrm{Jac}(X) \\ (P_1, \cdots, P_g) & \longmapsto & \jmath\left(\sum_{k=1}^g P_k - gO\right) \end{array}\ .$$

The matrix of its differential at $(P_1, \cdots, P_g)$ is $\Big[\omega_i(P_j)\Big]_{1\leqslant i,j\leqslant g}$, which cannot be singular for all $(P_1, \cdots, P_g)$ since the ω_i form a basis of $\Omega^1(X)$, so this map is not constant. Its image is therefore open, and it is also closed since it is the image of the compact X^g. Hence it must be all of $\mathrm{Jac}(X)$ since $\mathrm{Jac}(X)$, which is a complex torus, is connected.

• D principal $\Rightarrow \jmath(D) = 0$

Let $D = \mathrm{div}(f)$ be a principal divisor on X, and consider the morphism

$$\begin{array}{rccc} \phi\colon & \mathbb{P}^1\mathbb{C} & \longrightarrow & \mathrm{Jac}(X) \\ & [\lambda : \mu] & \longmapsto & \jmath\big(\,\mathrm{div}(\lambda f + \mu)\big). \end{array}$$

Let $z_1, \cdots, z_g$ be a system of coordinates on $\mathrm{Jac}(X) = \mathbb{C}^g/\Lambda$ near 0. Then $\mathrm{d}z_1, \cdots, \mathrm{d}z_g$ is a basis of the space of holomorphic differential 1-forms on $\mathrm{Jac}(X)$. Besides, the pull-backs $\phi^*\mathrm{d}z_i$ of these differentials to $\mathbb{P}^1\mathbb{C}$ are holomorphic, hence vanish identically since the space of holomorphic 1-forms on $\mathbb{P}^1\mathbb{C}$ has dimension $\mathrm{genus}(\mathbb{P}^1\mathbb{C}) = 0$. This means that ϕ is constant. In particular,

$$\jmath(D) = \phi\big([1:0]\big) = \phi\big([0:1]\big) = \jmath(0) = 0.$$

• $\jmath(D) = 0 \Rightarrow D$ principal

Write $D = \sum_{k=1}^{r} n_k P_k$. I must construct a meromorphic function f on X such that $\operatorname{div}(f) = D$. Such an f, if it exists, is only defined up to a multiplicative constant, so it is natural to attempt to construct the logarithmic differential of f instead. In other words, fixing an origin O, I shall construct f as

$$f(P) = \exp\left(\int_O^P \xi\right)$$

for some well-chosen meromorphic differential form ξ on X. Then f will be well-defined provided that

(i) the residues of ξ are integers,

(ii) the "periods" $\int_{\gamma_j} \xi$ all lie in $2\pi i\mathbb{Z}$,

and f will have divisor D provided that

(iii) ξ has simple poles at the points P_k with respective residues n_k, and no other poles.

Note that (iii) $\Rightarrow$ (i), so I only have to ensure that (ii) and (iii) hold. Also note that I may assume that the cycles γ_j do not meet any of the P_k by deforming them a little if necessary, which does not affect the Abel-Jacobi map $\jmath$.

I first claim that there exist meromorphic differential forms ξ satisfying (iii). To see this, take the short exact sequence

$$0 \longrightarrow \Omega^1_X \longrightarrow \Omega^1_X(\textstyle\sum_{k=1}^{r} P_k) \xrightarrow{\text{Res}} \bigoplus_{k=1}^{r} \mathbb{C}_{P_k} \longrightarrow 0,$$

where $\mathbb{C}_P$ denotes the skyscraper sheaf $\mathcal{O}_X(P)/\mathcal{O}_X$ standing at P, which yields

$$H^0\big(\Omega^1_X(\textstyle\sum_{k=1}^{r} P_k)\big) \xrightarrow{\text{Res}} \bigoplus_{k=1}^{r} \mathbb{C} \longrightarrow H^1(\Omega^1_X)$$

by taking cohomology. Now $H^1(\Omega^1_X) = H^0(\mathcal{O}_X) = \mathbb{C}$ by Serre duality A.1.1.31 and by example A.1.1.19, so that the image of the residue map Res in the cohomology sequence above has codimension at most 1. But this image is contained in the trace-zero hyperplane by lemma A.1.1.10, so that this image is actually exactly the trace-zero hyperplane. In other words, there exists a meromorphic differential form with only simple poles at the P_k and with respective residues a_k if and only if $\sum_{k=1}^{r} a_k = 0$. Since in my case $\sum_{k=1}^{r} n_k = \deg D = 0$, this proves my claim.

So let ξ by a meromorphic differential form satisfying (iii). I shall ensure that (ii) also holds by adding a suitable linear combination of the holomorphic differential forms ω_i to ξ, which does not affect (iii). First, it is easy to arrange that

$$\int_{\gamma_j} \xi = 0$$

for $1 \leqslant j \leqslant g$, since $\int_{\gamma_j} \omega_i = \mathbb{1}_{i=j}$. In order to compute $\int_{\gamma_{g+j}} \xi$ for $1 \leqslant j \leqslant g$, let $p\colon \Pi \twoheadrightarrow X$ be the construction of X by identifying edges of a $4g$-gon Π, and let

$\eta_j = p^*\omega_j$, $\eta_2 = p^*\omega_2$ be the pull-backs of ω_1 and ω_2 on Π. Fix an origin O in the interior of Π. Then the holomorphic function $f_j(P) = \int_O^P \eta_j$ is well-defined since Π is simply connected. Since $\int_{\gamma_j} \xi = 0$ for $1 \leqslant j \leqslant g$ and $\int_{\gamma_j} \omega_i = \mathbb{1}_{i=j}$, one has

$$\int_{\gamma_{g+j}} \xi = \sum_{k=1}^{g} \left(\int_{\gamma_k} \omega_j \int_{\gamma_{g+k}} \xi - \int_{\gamma_k} \xi \int_{\gamma_{g+k}} \omega_j \right).$$

By the same reasoning as in the proof of lemma A.1.2.8, one sees that this sum is the contour integral

$$\oint_{\partial\Pi} f_j \xi,$$

which is

$$2\pi i \sum_{k=1}^{r} n_k \int_O^{P_k} \eta_j = 2\pi i \sum_{k=1}^{r} n_k \int_{\alpha_k} \omega_j$$

by the residue theorem, where α_k denotes a path joining O to P_k and staying inside Π. Now, the hypothesis $\jmath(D) = 0$ means that there exist integers m_k such that

$$\sum_{k=1}^{r} n_k \int_{\alpha_k} = \sum_{k=1}^{2g} m_k \int_{\gamma_k}$$

as linear forms on $\Omega^1(X)$, so that finally

$$\int_{\gamma_{g+j}} \xi = 2\pi i \sum_{k=1}^{2g} m_k \int_{\gamma_k} \omega_j = 2\pi i \left(m_j + \sum_{k=1}^{g} m_{g+k} \tau_{j,k} \right)$$

by definition of the matrix τ. Replace then ξ with

$$\xi' = \xi - 2\pi i \sum_{k=1}^{g} m_{g+k} \omega_k.$$

Then $\int_{\gamma_j} \xi' = -2\pi i\, m_{g+j} \in 2\pi i\mathbb{Z}$, and

$$\int_{\gamma_{g+j}} \xi' = 2\pi i \left(m_j + \sum_{k=1}^{g} m_{g+k} \tau_{j,k} \right) - 2\pi i \sum_{k=1}^{g} m_{g+k} \tau_{k,j} = 2\pi i\, m_j \in 2\pi i\mathbb{Z}$$

because τ is symmetric. □

A.1.2.3 The general ground field case

I shall now briefly explain how the construction of the jacobian $\mathrm{Jac}(X)$ generalises over any perfect ground field K. The first thing to do is to make sure that the construction over $K = \mathbb{C}$ described above is algebraic, that is to say that the jacobian of a connected compact Riemann surface can be embedded analytically into some complex projective space. This is not so obvious at first, since according to the following theorem, most complex tori are **not** projective varieties:

Theorem A.1.2.17. *Let $g \in \mathbb{N}$, and let $T = \mathbb{C}^g/\Lambda$ be a complex torus of dimension g, where Λ is some full-rank lattice in $\mathbb{C}^g$. There exists an analytic embedding of T into $\mathbb{P}^n\mathbb{C}$ for some $n \in \mathbb{N}$ if and only if there exists a* Riemann form *with respect to Λ, that is to say a positive definite hermitian form on $\mathbb{C}^g$ whose imaginary part assumes integral values on $\Lambda \times \Lambda$.*

Remark A.1.2.18. A compact complex manifold which can be embedded analytically into a complex projective space is automatically algebraic. This is Chow's theorem, cf. [GH78, p. 167].

I refer to [HS00, section A.5] for the details of the proof of theorem A.1.2.17. The idea is that one needs sufficiently many meromorphic functions on T to define an embedding into a projective space, and that the existence of a Riemann form with respect to Λ makes it possible to construct such functions, called Θ functions. Also note that in the case where there does exist a Riemann form, the dimension n of the projective space the torus is embedded into tends to grow exponentially with g: typically, $n = 3^g - 1$ in the generic case.

Example A.1.2.19. Every complex torus of dimension $g = 1$ is projective. To see this, just notice that the lattice Λ can be written $\Lambda = \mathbb{Z}\tau_1 \oplus \mathbb{Z}\tau_2$ for some $\tau_1, \tau_2 \in \mathbb{C}$ such that $\mathrm{Im}(\tau_2/\tau_1) > 0$, and that the form $z, w \mapsto \frac{1}{\mathrm{Im}(\tau_2/\tau_1)}\overline{z}w$ is a Riemann form with respect to Λ.

While it is easy to normalise a hermitian form into a Riemann form in dimension 1, it becomes generically impossible to do it in higher dimension, so that "most" complex tori of dimension at least 2 are not projective. However, the Riemann bilinear relations A.1.2.11 imply that jacobians are always projective:

Theorem A.1.2.20. *Let X be a connected compact Riemann surface of genus g, with period matrix*

$$\left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \tau \\ 0 & & 1 & \end{array}\right]$$

with respect to a symplectic homology basis and to the corresponding dual basis of differential forms. Let $A = \mathrm{Re}\,\tau$ and $B = \mathrm{Im}\,\tau$. Then the form

$$z, w \longmapsto \overline{{}^t z} B^{-1} w$$

is a Riemann from on $\mathbb{C}^g$ with respect to the period lattice.

Proof. By the Riemann bilinear relations A.1.2.11, the matrices A and B are symmetric real matrices, and B is positive definite. In particular, B is nonsingular, so this hermitian form is well-defined and is positive definite. The period lattice of X is $\Lambda = \mathbb{Z}^g \oplus \tau\mathbb{Z}^g$, and an easy computation using the symmetry of A and B shows that the matrix of this hermitian form in the canonical basis is

$$\left[\begin{array}{c|c} B^{-1} & B^{-1}A + iI_g \\ \hline AB^{-1} - iI_g & AB^{-1}A \end{array}\right],$$

where I_g denotes the identity matrix of size g. It is then clear that this form is a Riemann form. □

In view of this result, it is natural to attempt to generalise the construction of the jacobian for a curve X over any ground field K. Of course, it is then no longer possible to rely on integrals of differential forms, so that the jacobian has to be constructed directly as an algebraic variety representing $\mathrm{Pic}^0(X)$. The construction in this abstract algebraic setting is rather technical, so I shall barely scratch its surface here, and refer the reader to [HS00, section A.8] or to [Mil12] instead. Eventually, one ends up with the following result:

Theorem A.1.2.21. *Let X be a projective, non-singular, geometrically integral curve of genus g defined over a perfect field K, such that there exists a K-rational point $O \in X(K)$ on X. There exists an abelian variety — that is to say a projective variety endowed with a (necessarily abelian) group law defined by polynomial equations — called the* jacobian *of X and denoted by $\mathrm{Jac}(X)$, which is defined over K and of dimension g, and an embedding $\jmath\colon X \hookrightarrow \mathrm{Jac}(X)$ defined over K and which, extended by additivity to $\mathrm{Div}(X)$, factors into an isomorphism*

$$\jmath\colon \mathrm{Pic}^0(X) \xrightarrow{\sim} \mathrm{Jac}(X).$$

Furthermore, for any algebraic extension $K \subseteq L \subseteq \overline{K}$ of K, the L-rational points of $\mathrm{Jac}(X)$ correspond to the divisor classes in $\mathrm{Div}^0\left(X(\overline{K})\right)$ which are invariant[2] under the action of $\mathrm{Gal}(\overline{K}/L)$.

Recall that according to corollary A.1.1.38, every divisor $D \in \mathrm{Div}^0(X)$ is linearly equivalent to a divisor of the form $E - gO$ for some effective divisor $E \in \mathrm{Eff}^g(X)$ of degree g which is generically unique. The idea is to start with the g^{th} symmetric power $\mathrm{Sym}^g(X) = X^g/\mathfrak{S}_g$ of X, where the symmetric group $\mathfrak{S}_g$ acts by permuting the factors of X^g. The following lemma shows that this is an algebraic variety:

Lemma A.1.2.22 (Hilbert, cf. [HS00, proposition A.8.3.2])**.** *Let A be a K-algebra of finite type, and let $G \subset \mathrm{Aut}_K(X)$ be a* ***finite*** *group of K-automorphisms of A. Then the subalgebra of fixed points A^G is also of finite type over K.*

The L-rational points of $\mathrm{Sym}^g(X)$ correspond to the effective divisors on $X(\overline{K})$ which are defined over L, so according to part (iv) of the Riemann-Roch theorem A.1.1.32, there should be a morphism from $\mathrm{Sym}^g(X)$ to $\mathrm{Jac}(X)$ which is generically one-to-one. One then proceeds to construct $\mathrm{Jac}(X)$ by identifying the points in $\mathrm{Sym}^g(X)$ which represent linearly equivalent divisors (which is rarely the case according to corollary A.1.1.38), and proceed to show that this yields an algebraic variety which is projective over K.

[2]The word "invariant" here applies indifferently to the divisor or to its linear equivalence class. Indeed, the existence of a K-rational point $O \in X(K)$ implies that a divisor class in $\mathrm{Pic}^0\left(X(\overline{K})\right)$ is invariant under $\mathrm{Gal}(\overline{K}/L)$ if and only if it can be represented by a divisor in $\mathrm{Div}^0\left(X(\overline{K})\right)$ which is globally invariant under $\mathrm{Gal}(\overline{K}/L)$.

A.1.3 Computing in the jacobian

Performing arithmetic operations in the jacobian $\mathrm{Jac}(X)$ of a curve X of genus g is not as easy as one might think. Of course, $\mathrm{Jac}(X)$ is an abelian variety, so it can be embedded into some projective space $\mathbb{P}^n_K$, and the group law is given by polynomial equations on the coordinates in this embedding, but these equations are insanely complicated, even in genus $g = 2$ (cf. [Fly90, appendix A]) which is the smallest non-trivial case in view of example A.1.1.35. In fact, the best one can do in general is to use so-called Θ functions to embed $\mathrm{Jac}(X)$, which is of dimension g, into a projective space of dimension $n = 3^g - 1$.

I shall now present a method, due to K. Khuri-Makdisi (cf. [KM04, KM07]), to compute in the jacobian $\mathrm{Jac}(X)$, that is to say in the class group $\mathrm{Pic}^0(X)$, of any projective, nonsingular, absolutely integral curve X of genus g, provided only that the perfect field K it is defined on be computational, that is to say such that there exist algorithms to perform arithmetic in K. The advantage this method is that it relies merely on linear algebra, which makes it very fast. Besides, it does not requires the knowledge of a plane model for X, but merely of a certain section space $H^0(X, D)$. Obviously, computing in $\mathrm{Jac}(X)$ is completely trivial if $g = 0$ since $\mathrm{Jac}(X)$ is then reduced to a point, so I shall assume that g is non-zero from now on.

A.1.3.1 Computing with section spaces

Let me first present a few ideas informally. Begin by fixing a divisor $D_0 \in \mathrm{Div}(X)$ of large enough degree d_0, so that the Abel-Jacobi map

$$\jmath\colon D \longmapsto [D - D_0] \qquad (\deg D = \deg D_0)$$

be surjective. A point $x \in \mathrm{Pic}^0(X)$ can then be represented, albeit perhaps not uniquely, by a divisor $D \in \mathrm{Div}^{d_0}(X)$ such that $[D - D_0] = x$. The novelty of K. Khuri-Makdisi's method rests on two points.

- First, $d_0 > g$ is chosen to be large, even though, by proposition A.1.1.37, $d_0 = g$ would be enough to ensure that $\jmath$ is surjective. The benefit of this, as I shall explain in more details, is that all the fibres of the Abel-Jacobi map are isomorphic, and more generally that the h^1 cease to be a nuisance (cf. part (iii) of the Riemann-Roch theorem A.1.1.32). The price to pay is a loss of rigidity, in that the divisor D representing a point $x \in \mathrm{Pic}^0(X)$ is far from unique.

- Next, a divisor D on X is no longer represented as a sum of points on X, but by the K-subspace $H^0(\Delta - D)$ of $K(X)$, where Δ denotes a fixed divisor. The degree of this divisor must of course be high enough for this representation to be faithful.

I shall make all of this more precise in a moment. The advantage of this representation way is that it brings all the computations in $\mathrm{Pic}^0(X)$ down to mere linear algebra computations. In order to perform these computations, one uses formulae of the kind

$$\begin{aligned} H^0(A+B) &= H^0(A)\cdot H^0(B) \\ f\cdot H^0(A) &= H^0\big(A - \mathrm{div}(f)\big) \\ H^0(B-A) &= \big\{s \in K(X) \mid sH^0(A) \subseteq H^0(B)\big\} \end{aligned}$$

where I used the notation

$$V \cdot W = \{vw \mid v \in V,\ w \in W\}$$

for V and W subspaces of $K(X)$, and where A and B are divisors on X and $f \in K(X)$.

Of course, such formulae only stand under certain conditions (large enough degree...). I shall now justify all of this rigorously.

A.1.3.2 Technical preliminaries

In order to prove the necessary technical results, I shall of course make intensive use of the Riemann-Roch theorem A.1.1.32.

Recall that the line bundle $\mathcal{O}_X(D)$, $D \in \mathrm{Div}(X)$, is defined by

$$\mathcal{O}_X(D)(U) = \{s \in K(X) \mid \mathrm{div}(s) + D \geqslant 0 \text{ on } U\} \qquad (U \subset X \text{ open}).$$

The notion of *base point* allows one to examine the behaviour of the sections of $\mathcal{O}_X(D)$ when the degree of D is small.

Definition A.1.3.1. Let D be a divisor on X. By definition, the divisor

$$B = D + \inf_{s \in H^0(D)} \mathrm{div}(s)$$

is then effective. The divisor is call the *base locus* of D, or of $\mathcal{O}_X(D)$. The *base points* are the points in its support.

If $B = 0$, then D and $\mathcal{O}_X(D)$ are said to be *base point free*.

In other words, D is base point free if $\inf_{s \in H^0(D)} \mathrm{div}(s) = -D$, that is to say if "the global sections of $\mathcal{O}_X(D)$ do everything they are allowed to do".

Example A.1.3.2. Let E be an elliptic curve, P a point on $E(K)$, and take $D = P$. It is well-known (cf. A.1.1.35) that

$$H^0(E, D) = K$$

only consists of the constant functions. Thus, although the definition of the sections $H^0(E, D)$ allows them to have a pole at P, they do not take advantage of it. The point P is hence a base point of D; actually, it is the only one.

Intuitively, base points can only exist be because the degree of D is too small compared to the genus g in order for the sections in $H^0(D)$ to have enough freedom. The following proposition shows that this intuition is correct:

Proposition A.1.3.3. *Let $\mathcal{L}$ be a line bundle of degree d on X.*

1. *If $d \geqslant 2g$, then $\mathcal{L}$ is base point free.*
2. *If $\mathcal{L}$ is generic and $d \geqslant g + 1$, then $\mathcal{L}$ is base point free.*

Proof. Extend the scalars to $\overline{K}$. If $\mathcal{L}$ has degree $d \geqslant 2g$, then for every point $P \in X$, $\mathcal{L}(-P)$ has degree $d-1 \geqslant 2g-1$, so that $h^0(\mathcal{L}(-P)) = h^0(\mathcal{L}) - 1$ by the Riemann-Roch theorem A.1.1.33(iii). Now, if P were a base point of $\mathcal{L}$, one would have $H^0(\mathcal{L}(-P)) = H^0(\mathcal{L})$, thus $h^0(\mathcal{L}(-P)) = h^0(\mathcal{L})$. Hence $\mathcal{L}$ is base point free.

The case of generic $\mathcal{L}$ is dealt with in the same way, by using the generic case (v) of the Riemann-Roch theorem A.1.1.33. □

The above example shows that the condition $\deg \mathcal{L} \geqslant 2g$ is optimal.

A moment of thought reveals that a line bundle $\mathcal{L}$ is base point free if and only if it is *generated by its global sections*, that is to say that the map

$$H^0(\mathcal{L}) \otimes \mathcal{O}_X \longrightarrow \mathcal{L}$$

is surjective. I shall denote its kernel by $\mathcal{M}_{\mathcal{L}}$, so that for each base point free line bundle $\mathcal{L}$, there is a short exact sequence

$$0 \longrightarrow \mathcal{M}_{\mathcal{L}} \longrightarrow H^0(\mathcal{L}) \otimes \mathcal{O}_X \longrightarrow \mathcal{L} \longrightarrow 0$$

of vector bundles on X. Thanks to this information, one can determine a sufficient condition for the multiplication map

$$H^0(\mathcal{L}_1) \underset{K}{\otimes} H^0(\mathcal{L}_2) \longrightarrow H^0(\mathcal{L}_1 \otimes \mathcal{L}_2)$$

to be surjective.

Lemma A.1.3.4 (Base point free pencil trick)**.** *Let $\mathcal{L}$ be a* generic *line bundle of degree $g+1$ on the curve X. Then $\mathcal{M}_{\mathcal{L}}$ is also a line bundle on X, and is isomorphic to the dual bundle $\mathcal{L}^\vee = \mathrm{Hom}(\mathcal{L}, \mathcal{O}_X)$ of $\mathcal{L}$.*

Proof. Since $\mathcal{L}$ is generic, the Riemann-Roch theorem A.1.1.32(v) implies that

$$\dim H^0(\mathcal{L}) = \deg \mathcal{L} + 1 - g = g + 1 + 1 - g = 2.$$

One can therefore write[3]

$$H^0(\mathcal{L}) = K s_1 \oplus K s_2$$

where s_1, s_2 are elements of $H^0(\mathcal{L}) \setminus \{0\}$. Besides, again because $\mathcal{L}$ is generic, it is base point free according to proposition A.1.3.3, hence the short exact sequence

$$0 \longrightarrow \mathcal{M}_{\mathcal{L}} \longrightarrow H^0(\mathcal{L}) \otimes \mathcal{O}_X \longrightarrow \mathcal{L} \longrightarrow 0.$$

Now let $U \subseteq X$ be an open subset of X. From the definition of $\mathcal{M}_{\mathcal{L}}$, there is an isomorphism

$$\mathcal{M}_{\mathcal{L}}(U) \simeq \left\{ (t_1, t_2) \in \mathcal{O}_X(U)^2 \;\middle|\; s_1 t_1 + s_2 t_2 = 0 \right\} \simeq \left\{ (t_1, t_2) \in \mathcal{O}_X(U)^2 \;\middle|\; s_1 t_2 - s_2 t_1 = 0 \right\},$$

which is functorial in U, where (t_1, t_2) has been replaced with $(t_2, -t_1)$ in the last step.

[3] $H^0(\mathcal{L})$ has thus projective dimension 1, hence the term *pencil*.

Define $u_i = \frac{t_i}{s_i} \in K(X)$ for $i \in \{1,2\}$. The condition $s_1t_2 - s_2t_1 = 0$ defining $\mathcal{M}_\mathcal{L}$ is tantamount to the equality $u_1 = u_2$; furthermore, letting $u = u_1 = u_2$, the $t_i = us_i$ have to be regular on U. To sum up, there is an isomorphism

$$\mathcal{M}_\mathcal{L}(U) \simeq \Big\{ u \in K(X) \;\Big|\; \forall i \in \{1,2\},\ us_i|_U \in \mathcal{O}_X(U) \Big\} \simeq \Big\{ u \in K(X) \;\Big|\; uH^0(\mathcal{L})|_U \subseteq \mathcal{O}_X(U) \Big\},$$

so that $\mathcal{M}_\mathcal{L}$ is isomorphic to the dual bundle $\mathcal{L}^\vee$, since $\mathcal{L}$ is base point free, hence generated by its global sections. □

Theorem A.1.3.5. *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be two line bundles on X, with respective degrees d_1 and d_2, and let g denote the genus of X. If d_1, $d_2 \geqslant 2g+1$, then the multiplication map*

$$\mu : H^0(\mathcal{L}_1) \underset{K}{\otimes} H^0(\mathcal{L}_2) \longrightarrow H^0(\mathcal{L}_1 \otimes \mathcal{L}_2)$$

is surjective.

Proof. I may extend the scalars to $\overline{K}$, and by symmetry, I can suppose without loss of generality that $d_1 \leqslant d_2$. Start by writing down the short exact sequence associated to $\mathcal{L}_1$, which is base point free according to proposition A.1.3.3:

$$0 \longrightarrow \mathcal{M}_{\mathcal{L}_1} \longrightarrow H^0(\mathcal{L}_1) \otimes \mathcal{O}_X \longrightarrow \mathcal{L}_1 \longrightarrow 0.$$

Since $\mathcal{L}_2$ is locally free, this sequence remains exact after tensoring by $\mathcal{L}_2$, so that

$$0 \longrightarrow \mathcal{M}_{\mathcal{L}_1} \otimes \mathcal{L}_2 \longrightarrow H^0(\mathcal{L}_1) \otimes \mathcal{L}_2 \longrightarrow \mathcal{L}_1 \otimes \mathcal{L}_2 \longrightarrow 0.$$

Taking the global sections, one gets the long exact sequence in cohomology

$$0 \longrightarrow H^0(\mathcal{M}_{\mathcal{L}_1} \otimes \mathcal{L}_2) \longrightarrow H^0(\mathcal{L}_1) \otimes H^0(\mathcal{L}_2) \xrightarrow{\mu} H^0(\mathcal{L}_1 \otimes \mathcal{L}_2) \longrightarrow H^1(\mathcal{M}_{\mathcal{L}_1} \otimes \mathcal{L}_2) \longrightarrow \cdots$$

in which the multiplication map μ shows up. I shall now prove that $H^1(\mathcal{M}_{\mathcal{L}_1} \otimes \mathcal{L}_2)$ vanishes, which implies that μ is surjective.

Define $r = d_1 - g - 1$, and let $P_1, \cdots, P_r$ be points in generic position on X. As $r \geqslant g$ by hypothesis on d_1, proposition A.1.1.37 ensures that the Abel-Jacobi-like map $\mathrm{Eff}^r(X) \longrightarrow \mathrm{Pic}^r(X)$ is surjective. The line bundle $\mathcal{L}_1\big(-\sum_{i=1}^r P_i\big)$, which is of degree $d_1 - r = g + 1$, is therefore generic, so it is base point free by proposition A.1.3.3. The short exact sequences attached to $\mathcal{L}_1$ and to $\mathcal{L}_1\big(-\sum_{i=1}^r P_i\big)$ fit into the

following commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{M}_{\mathcal{L}_1(-\sum_{i=1}^r P_i)} & \longrightarrow & H^0\left(\mathcal{L}_1\Big(-\sum_{i=1}^r P_i\Big)\right)\otimes\mathcal{O}_X & \longrightarrow & \mathcal{L}_1\Big(-\sum_{i=1}^r P_i\Big) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{M}_{\mathcal{L}_1} & \longrightarrow & H^0(\mathcal{L}_1)\otimes\mathcal{O}_X & \longrightarrow & \mathcal{L}_1 & \longrightarrow & 0. \\
 & & \downarrow & & & & & & \\
 & & \bigoplus_{i=1}^r \mathcal{O}_X(-P_i) & & & & & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

Since, by the base point free pencil trick,

$$\mathcal{M}_{\mathcal{L}_1(-\sum_{i=1}^r P_i)} \simeq \mathcal{L}_1^\vee\left(\sum_{i=1}^r P_i\right),$$

this yields the short exact sequence

$$0 \longrightarrow \mathcal{L}_1^\vee\left(\sum_{i=1}^r P_i\right) \longrightarrow \mathcal{M}_{\mathcal{L}_1} \longrightarrow \bigoplus_{i=1}^r \mathcal{O}_X(-P_i) \longrightarrow 0.$$

Tensoring again by $\mathcal{L}_2$ and taking the cohomology results in the exact sequence

$$\cdots \longrightarrow H^1\left(\mathcal{L}_1^\vee\otimes\mathcal{L}_2\Big(\sum_{i=1}^r P_i\Big)\right) \longrightarrow H^1(\mathcal{M}_{\mathcal{L}_1}\otimes\mathcal{L}_2) \longrightarrow \bigoplus_{i=1}^r H^1\big(\mathcal{L}_2(-P_i)\big) \longrightarrow \cdots$$

To conclude, I shall prove that the middle term vanishes, by using Serre duality A.1.1.31 to show that both extreme terms vanish.

First, for the right-hand term, one has

$$h^1\big(\mathcal{L}_2(-P_i)\big) = h^0\big(\Omega_1\otimes\mathcal{L}_2^\vee(P_i)\big),$$

and the line bundle $\Omega_1\otimes\mathcal{L}_2^\vee(P_i)$ has degree $2g-2-d_2+1<0$ since $d_2\geqslant 2g+1$. By A.1.1.20, this proves that $H^1\big(\mathcal{L}_2(-P_i)\big)$ vanishes.

Next, for the left-hand term,

$$h^1\left(\mathcal{L}_1^\vee\otimes\mathcal{L}_2\Big(\sum_{i=1}^r P_i\Big)\right) = h^0\left(\Omega_1\otimes\mathcal{L}_1\otimes\mathcal{L}_2^\vee\Big(-\sum_{i=1}^r P_i\Big)\right),$$

and this time the degree of the line bundle $\Omega_1 \otimes \mathcal{L}_1 \otimes \mathcal{L}_2^\vee\big(-\sum_{i=1}^r P_i\big)$ is

$$2g-2+d_1-d_2-r \leqslant g-2$$

since I have assumed $d_1 \leqslant d_2$. For generic P_i's, this line bundle is thus generic of degree $g-2<g$, so by the Riemann-Roch theorem A.1.1.32(v) it has no non-zero global section either, which concludes the proof. □

A.1.3.3 Building blocks

Recall that a point $x \in \mathrm{Pic}^0(X)$ is to be represented by a divisor D on X such that $x=[D-D_0]$, where D_0 is a fixed origin divisor, whose degree I denote d_0. The divisor D representing x thus also has degree d_0. As I announced above, I must choose a large value of d_0 instead of $d_0=g$, so as to avoid nuisances such as base points or inconclusiveness in the Riemann-Roch theorem. I shall show that $d_0 \geqslant 2g+1$ is enough to ensure the correctness of K. Khuri-Makdisi's algorithm.

Besides, the divisor D is itself to be represented as $H^0(\Delta-D)$, where Δ is a fixed divisor. For this representation to be faithful, it is sufficient that $\Delta-D$ be base point free, hence that $\deg\Delta \geqslant \deg D+2g$ by proposition A.1.3.3. As I shall explain, the algorithm deals with divisors of degree d_0 and $2d_0$, so that $\deg\Delta$ must be at least $2d_0+2g$. The choice $\Delta=3D_0$ is thus natural. Consequently, I shall denote

$$V=H^0(3D_0),$$

and a divisor D will be represented by the subspace

$$W_D=H^0(3D_0-D)\subset V.$$

In practice, these spaces, which are finite-dimensional over K, will be represented by a K-basis, hence by matrices with coefficients in K. The elements forming these bases, which are rational functions on X, can be represented in several ways.

1. The first solution consists in picking a rational point $P \in X(K)$, and to represent a function by its truncated Taylor series at P. This means that a function is represented by an element in a K-algebra of truncated power series.

2. Another solution consists in picking rational points $P_i \in X(K)$ on the curve $X$and to represent a function by its values at these points. If it is not possible to find sufficiently many rational points, e.g. because K is a number field, one can use points defined on a small extension of K instead. A function is then represented by an element in an étale K-algebra.

3. More generally, one can do a little of both, that is to say represent a function by its truncated Taylor series at various fixed points, in other words, by evaluating the function at an effective divisor.

Denote by $Z \in \mathrm{Eff}(X)$ the divisor at which functions are evaluated to represent them. It will turn out that the functions considered along the algorithms below all lie in $V=H^0(3D_0)$ or in $H^0(6D_0)$. Therefore, for this representation system to be faithful, it is necessary and sufficient that $H^0(3D_0-Z)=H^0(6D_0-Z)=\{0\}$. The

easiest (and safest) way to ensure this is to pick Z of degree at least $6d_0+1$. By the way, it is better if possible to avoid that the supports of D_0 and Z intersect, since if they do, functions will have poles where they are evaluated, and one has to shift the valuation in power series or use Laurent series, which makes the implementation more difficult. To sum up, a space W of functions will be represented by a matrix, with $\deg Z$ lines, $\dim W$ columns, and coefficients in K.

Before describing the actual algorithms for computing in $\mathrm{Pic}^0(X)$, I present three "building blocks", that is to say three basic operations these algorithms rely on, and which correspond to the three formulae given in the beginning of this section.

Algorithm A.1.3.6 (Add)**.** Knowing $H^0(A)$ and $H^0(B)$, compute $H^0(A+B)$.

Theorem A.1.3.5 asserts that if A and B both have degree at least $2g+1$, then $H^0(A+B) = H^0(A)\cdot H^0(B)$. Provided that this condition is fulfilled, in order to compute $H^0(A+B)$, it is thus enough to multiply every basis element of $H^0(A)$ by every basis element of $H^0(B)$, and then to extract a basis of $H^0(A+B)$ by performing linear elimination. Actually, if one accepts to introduce randomness, it is much more efficient to compute n products of a randomly chosen basis element of $H^0(A)$ by a randomly chosen basis element of $H^0(B)$ for n a little larger than $h^0(A+B)$, and then to ensure that these products do span $H^0(A+B)$ and to extract a basis out of them.

Algorithm A.1.3.7 (Multiply by function)**.** Knowing a function f and $H^0(A)$, compute $H^0\big(A-(f)\big)$.

It is plain that

$$\begin{aligned} f\cdot H^0(A) &= \big\{fs \mid \operatorname{div}(s) \geqslant -A\big\} \\ &= \big\{t = fs \mid \operatorname{div}(t) = \operatorname{div}(f)+\operatorname{div}(s) \geqslant \operatorname{div}(f) - A\big\} \\ &= H^0\big(A - \operatorname{div}(f)\big) \end{aligned}$$

unconditionally. Therefore, one simply multiplies each basis element of $H^0(A)$ by f to get a basis of $H^0\big(A-(f)\big)$.

Algorithm A.1.3.8 (Subtract)**.** Knowing $H^0(A)$ and $H^0(B)$, compute $H^0(B-A)$. One has

$$\begin{aligned} \big(H^0(B) : H^0(A)\big) &= \big\{s \in K(X) \mid s\cdot H^0(A) \subseteq H^0(B)\big\} \\ &= \big\{s \in K(X) \mid \operatorname{div}(a) \geqslant -A \Rightarrow \operatorname{div}(s)+\operatorname{div}(a) \geqslant -B\big\} \\ &= \big\{s \in K(X) \mid \operatorname{div}(s) - A \geqslant -B\big\} \quad \text{if } A \text{ is base point free} \\ &= H^0(B-A). \end{aligned}$$

Hence, provided that A is base point free (e.g. because $\deg A \geqslant 2g$), $H^0(B-A)$ can be computed as follows: compute a matrix K_B whose kernel is exactly $H^0(B)$; then, for each basis element a_i of $H^0(A)$, twist the matrix K_B into a matrix $K_{a_i,B}$ such that for all $s \in B$, $K_{a_i,B}x = 0 \iff K_B a_i x = 0$ (the explicit way that K_B must be twisted depends on how functions on X are represented). Next, stack up the matrices $K_{a_i,B}$ into a big matrix. One must stack up an extra equation matrix at the top of this big matrix, so as to ensure hat its kernel only contains vectors representing actual

functions; for instance, if A is effective one can stack up an extra copy of K_B since $H^0(B-A) \subseteq H^0(B)$ in this case. In practice $H^0(B-A)$ is a subspace of V, so one can stack up a precomputed matrix K_V whose kernel is exactly V instead. It then only remains to compute the kernel of the big matrix in order to get $H^0(B-A)$.

Remark A.1.3.9. Note that the equations encoded in the big matrix are in general very redundant, so extra care should be taken in the computation of the kernel if the base field K is not exact. For instance, I shall use K. Khuri-Makdisi's algorithms with $K = \mathbb{C}$ in my algorithm, so I must keep numerical stability in mind. My solution consists in using QR-decomposition by Householder reflections (cf. for instance [Dem97, sections 3.2.2 and 3.4.1]) instead of the numerically-unstable Gaussian elimination. The expected dimension d of the kernel is known beforehand thanks to the Riemann-Roch theorem, so the kernel can be computed as the space corresponding to the d diagonal entries of R with smallest modulus. The experiments I have run seem to indicate that this method was a reasonable compromise between numerical stability and speed of execution.

Remark A.1.3.10. Also note that the big matrix can be made smaller, and hence the computation faster, by stacking up $K_{a_i,B}$ no longer for a_i's ranging over the basis of $H^0(A)$, but for a few a_i's chosen at random in $H^0(A)$. The result is then correct if $\inf_i \operatorname{div}(a_i) = -A$, else the dimension of the kernel of the big matrix will be larger than expected according to the Riemann-Roch theorem, and this is easy to detect, so one can just start again until the kernel is of the expected dimension. This yields a probabilistic algorithm of Las Vegas type. When the ground field K is infinite, the probability that the computation fails is zero even if one takes only two[4] (linearly independent) a_i's. On the other hand, if K is finite of small cardinal, it may be better to take a larger number of a_i's in order to reduce the probability of failure, cf. [KM07, section 4] for a precise estimation.

Remark A.1.3.11. I would like to stress once again that these three building blocks merely rely on linear algebra over K.

A.1.3.4 The actual algorithms

I can now present the two algorithms used to compute in $\mathrm{Pic}^0(X)$. These algorithms only rely on the three building blocks presented above. For simplicity, I shall assume that the base divisor D_0 is effective, although it is not necessary for K. Khuri-Makdisi's algorithms to work. Recall that a point $x \in \mathrm{Pic}^0(X)$ is represented by an effective divisor D of degree d_0 such that $[D - D_0] = x$, and that this divisor is itself represented by the subspace $W_D = H^0(3D_0 - D)$ of $V = H^0(3D_0)$.

The spaces V and $W_{D_0} = H^0(2D_0)$, which represents $0 \in \mathrm{Pic}^0(X)$, are assumed to be given as an input representing X. If not also given, one also precomputes a matrix K_V whose kernel is exactly V.

[4] Clearly, the computation cannot succeed if one takes only one a_i, since the condition $\inf_i \operatorname{div}(a_i) = -A$ cannot be satisfied then.

Algorithm A.1.3.12 (Chord)**.** Given two points x_1 and $x_2 \in \mathrm{Pic}^0(X)$, this algorithm computes $x_3 = -x_1 - x_2 \in \mathrm{Pic}^0(X)$.

In other words, knowing $W_{D_1} = H^0(3D_0 - D_1)$, with D_1 effective of degree d_0 such that $[D_1 - D_0] = x_1$, and $W_{D_2} = H^0(3D_0 - D_2)$, with D_2 effective of degree d_0 such that $[D_2 - D_0] = x_2$, compute $W_{D_3} = H^0(3D_0 - D_3)$, with D_3 effective of degree d_0 such that $D_1 + D_2 + D_3 \sim 3D_0$.

This is achieved as follows.

1. First, use the "add" block to compute $H^0(6D_0 - D_1 - D_2) = W_{D_1} \cdot W_{D_2}$. This is legitimate since $3D_0 - D_1$ et $3D_0 - D_2$ both have degree $4d_0 \geqslant 2g + 1$.

2. Next, use the "subtract" block to compute

$$H^0(3D_0 - D_1 - D_2) = \big\{s \in V \mid s \cdot V \subseteq H^0(6D_0 - D_1 - D_2)\big\},$$

   which is possible since $V = H^0(3D_0)$ is base point free according to proposition A.1.3.3. Here one can use the precomputed matrix K_V.

3. Then, choose a non-zero function f in $H^0(3D_0 - D_1 - D_2)$, for instance the first basis element thereof. The divisor of f has the form

$$\mathrm{div}(f) = -3D_0 + D_1 + D_2 + D_3,$$

   where D_3 is effective of degree d_0, and $D_1 + D_2 + D_3$ is linearly equivalent to $3D_0$, so D_3 is exactly what is needed. To catch it, use then the block "multiply by function" to compute $f \cdot V = H^0(6D_0 - D_1 - D_2 - D_3)$.

4. It only remains to use the "subtract" block to compute

$$W_{D_3} = H^0(3D_0 - D_3) = \big\{s \in V \mid s \cdot H^0(3D_0 - D_1 - D_2) \subseteq H^0(6D_0 - D_1 - D_2 - D_3)\big\}.$$

   This is legitimate since $H^0(3D_0 - D_1 - D_2)$ is base point free[5] by proposition A.1.3.3. Note that since $3D_0 - D_1 - D_2$ is not effective *a priori*, one must stack up K_V instead of $K_{3D_0 - D_1 - D_2}$ on the top of the big matrix, since the space one wants to compute is a subspace of V.

A few words might be in order to explain how to use the "chord" algorithm above to compute in $\mathrm{Pic}^0(X)$. To compute the opposite of the point represented by W_D, apply the "chord" algorithm to W_D and W_{D_0}. To add the points represented by W_{D_1} and W_{D_2}, apply the "chord" algorithm to W_{D_1} and W_{D_2}, then compute the opposite of the result. To subtract the point represented by W_{D_2} from the point represented by W_{D_1}, compute the opposite of W_{D_1}, then apply the "chord" to the result and to W_{D_2}.

It is also crucial to be able to determine whether two subspaces W_{D_1} and W_{D_2} represent the same point of $\mathrm{Pic}^0(X)$, since as I stressed the divisor D representing a point is far from being unique. Now W_{D_1} and W_{D_2} represent the same point in $\mathrm{Pic}^0(X)$ if and only if D_1 and D_2 are linearly equivalent, which is tantamount to $H^0(D_1 - D_2)$ being a non-zero space. The idea is thus to almost compute $H^0(D_1 - D_2)$.

[5] It is at this point that the condition $d_0 \geqslant 2g$ is required.

Algorithm A.1.3.13 (Equality test)**.**

1. First pick a non-zero function f in W_{D_1}, e.g. the first basis element thereof. The divisor of f is of the form

$$\mathrm{div}(f) = -3D_0 + D_1 + E$$

where E is effective and has degree $2d_0$. Next, use the "multiply by function" block to compute $H^0(6D_0 - D_1 - D_2 - E) = f \cdot W_{D_2}$.

2. It only remains to compute

$$H^0(3D_0 - D_2 - E) = \big\{s \in V \mid s \cdot W_{D_1} \subseteq H^0(6D_0 - D_1 - D_2 - E)\big\},$$

and output `TRUE` is this space is non-zero, and `FALSE` else. Indeed, $H^0(3D_0 - D_2 - E) = f \cdot H^0(D_1 - D_2)$, since V is base point free by proposition A.1.3.3. Just like above, one must stack up K_V on the top of the big matrix. However, the acceleration trick described in remark A.1.3.10 must not be used here, since this time, the dimension of the kernel of the big matrix is not known beforehand: on the contrary, it is what is being computed !

Remark A.1.3.14. Note that it is possible to perform many other operations on divisors (max, min, set-theoretic difference, ...) by using these three "building blocks". For further details, cf. [KM04].

I conclude this section by explaining how to get the input data $V = H^0(3D_0)$ and $W_{D_0} = H^0(2D_0)$. It is enough to have $H^0(D_0)$, since one can then construct successively W_{D_0} and V using the multiplication map A.1.3.5 as $d_0 \geqslant 2g + 1$. It thus remains to compute $H^0(D_0)$. The methods for this differ, depending on how the curve X is given. However, the curve X one wishes to compute with is often particular, and there is then a natural choice for D_0 for which $H^0(D_0)$ is known explicitly. For instance, the curves I shall work with are modular curves (cf. section A.2 below), and I shall arrange for $H^0(D_0)$ to be a space of modular forms.

A.1.3.5 Complexity analysis and comments

The above two algorithms make it possible to compute in $\mathrm{Pic}^0(X)$ for any curve X defined over any computational perfect base field K. Furthermore, it merely relies on linear algebra, on matrices of size $O(g) \times O(g)$ (at least when the ground field K is infinite), where g denotes the genus of the curve X. This means that one operation in $\mathrm{Pic}^0(X)$ requires[6] $O(g^3)$ operations in K.

It may seem surprising that the section space $H^0(D_0)$ alone contains enough information about X to make it possible to compute in $\mathrm{Pic}^0(X)$. This is due to the fact that the assumption $d_0 \geqslant 2g + 1$ implies that D_0 is *very ample*, so that the associated section space contains enough functions to set up a projective embedding of X.

[6]This can be improved by using fast linear algebra algorithms. However, when the ground field K is not exact (e.g. $K = \mathbb{C}$ in my case), such fast algorithms may be numerically instable.

A.2 Modular curves and modular forms

I shall now proceed to the presentation of some well-known facts about modular forms and other related modular objects, namely modular curves and modular symbols, making the extraordinarily rich arithmetic structure of these objects apparent along the way.

A.2.1 Modular curves

I start with modular curves, which may be naively defined as Riemann surfaces constructed by quotienting the extended upper half plane by subgroups of $\mathrm{SL}_2(\mathbb{Z})$, although they are much better understood once one sees them as moduli spaces for elliptic curves endowed with torsion data. This makes natural the definition of Hecke correspondences, and explains why these curves admit models over $\mathbb{Q}$ (or at least, over a cyclotomic field).

A.2.1.1 Modular curves as manifolds

Let $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\,\tau > 0\}$ denote the Poincaré upper half-plane. The group $\mathrm{GL}_2(\mathbb{R})^+$ of 2×2 real matrices with positive determinant acts on $\mathcal{H}$ by the well-known formula

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})^+.$$

I am interested in quotients of $\mathcal{H}$ by discrete subgroups Γ of $\mathrm{GL}_2(\mathbb{R})^+$, such as $\mathrm{SL}_2(\mathbb{Z})$. More precisely, I shall focus on the case where Γ is a certain kind of finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Definition A.2.1.1. Let $N \in \mathbb{N}$. The subgroup $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the kernel of the projection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. In other words, a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ lies in $\Gamma(N)$ if and only if $b \equiv c \equiv 0 \bmod N$ and $a \equiv d \equiv 1 \bmod N$.

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if it contains $\Gamma(N)$ for some $N \in \mathbb{N}$. The least such N is called the *level* of Γ.

For instance, $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$ is the only congruence subgroup of level 1. The terminology "congruence subgroup" comes form the fact that membership of a congruence subgroup Γ of level N is defined by congruence conditions modulo N on the entries of the matrix $\big($consider the image of Γ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\big)$. The most famous examples of congruence subgroups, apart the $\Gamma(N)$ themselves, are the

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\} \quad \text{and}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \;\middle|\; a \equiv d \equiv 1 \bmod N \right\}.$$

Example A.2.1.2. Write $N = \prod_{p|N} p^{v_p}$. $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, with quotient $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{p|N} \mathrm{SL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z})$ by Chinese remainders. From the short exact sequence

$$1 \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p^{v_p}\mathbb{Z})^* \longrightarrow 1\,,$$

one sees that $\#\,\mathrm{SL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z})}{\#(\mathbb{Z}/p^{v_p}\mathbb{Z})^*}$, and from the short exact sequence

$$1 \longrightarrow 1 + p\,\mathrm{Mat}_{2\times 2}(\mathbb{Z}/p^{v_p-1}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 1\,,$$

one deduces that

$$\#\,\mathrm{GL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) = \left(p^{v_p-1}\right)^4 (p^2-1)(p^2-p) = (p^{v_p})^4 \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p}\right),$$

so that the index of $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is

$$\prod_{p|N} \#\,\mathrm{SL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z}) = \prod_{p|N} \frac{(p^{v_p})^4 \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p}\right)}{p^{v_p}\left(1-\frac{1}{p}\right)} = N^3 \prod_{p|N}\left(1-\frac{1}{p^2}\right).$$

Furthermore, $\Gamma(N)$ is normal in $\Gamma_1(N)$ with quotient $\Gamma_1(N)/\Gamma(N) \simeq \mathbb{Z}/N\mathbb{Z}$ by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto b \bmod N$, and $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ with quotient $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*$ by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto d \bmod N$, so that

$$\Gamma(N) \underset{N}{\lhd} \Gamma_1(N) \underset{N\prod_{p|N}\left(1-\frac{1}{p}\right)}{\lhd} \Gamma_0(N) \underset{N\prod_{p|N}\left(1+\frac{1}{p}\right)}{\subset} \mathrm{SL}_2(\mathbb{Z})$$

where the numbers under the inclusions denote the indices.

Example A.2.1.3. Let A_N be the set of vectors in $(\mathbb{Z}/N\mathbb{Z})^2$ of order exactly N, and let $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ be the quotient of A_N by $(\mathbb{Z}/N\mathbb{Z})^*$ acting diagonally (this agrees with $\mathbb{P}^1\mathbb{F}_N$ when N is prime). By viewing the elements of A_N as column vectors, one has a canonical action of $\mathrm{SL}_2(\mathbb{Z})$ on A_N, which is transitive, and which induces a transitive action on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Since $\Gamma_1(N)$ is the stabiliser of $(1,0) \in A_N$, one sees that for all γ, $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, the cosets $\gamma\Gamma_1(N)$ and $\gamma'\Gamma_1(N)$ agree if and only if the left columns of γ and of γ' agree in A_N, and in particular one gets the coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{(\overline{a},\overline{c})\in A_N} \gamma_{(\overline{a},\overline{c})}\Gamma_1(N),$$

where $\gamma_{(\overline{a},\overline{c})}$ denotes any matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ such that $a \equiv \overline{a}$ and $c \equiv \overline{c} \bmod N$. Similarly, since the stabiliser of $(1:0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is $\Gamma_0(N)$, the cosets $\gamma\Gamma_0(N)$ and $\gamma'\Gamma_0(N)$ agree if and only if the left columns of γ and of γ' agree in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, and one has the coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{(\overline{a}:\overline{c})\in\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} \gamma_{(\overline{a}:\overline{c})}\Gamma_0(N),$$

where $\gamma_{(\overline{a},\overline{c})}$ denotes any matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ such that $(a:c) = (\overline{a}:\overline{c})$ in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

One can also view the elements of A_N as row-vectors and let $\mathrm{SL}_2(\mathbb{Z})$ act on A_N on the right, which leads to the criteria $\Gamma_1(N)\gamma = \Gamma_1(N)\gamma'$ if and only if the bottom rows of γ and of γ' agree in A_N, $\Gamma_0(N)\gamma = \Gamma_0(N)\gamma'$ if and only if the bottom rows of γ and of γ' agree in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, and to the coset decompositions

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{(\overline{c},\overline{d})\in A_N} \Gamma_1(N)\gamma_{(\overline{c},\overline{d})},$$

and

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{(\overline{c}:\overline{d})\in\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} \Gamma_0(N)\gamma_{(\overline{c}:\overline{d})}$$

with the obvious notations.

Fix a congruence subgroup Γ of level N, and let $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ denote the quotient of $\mathcal{H}$ by Γ. One can show (cf. [DS05, section 2.1]) that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ is properly discontinuous, that is to say every $\tau \in \mathcal{H}$ has a neighbourhood V such that

$$\forall \gamma \in \mathrm{SL}_2(\mathbb{Z}),\ \gamma V \cap V \neq \emptyset \Longrightarrow \gamma\tau = \tau,$$

so that the topology $Y(\Gamma)$ inherits from $\mathcal{H}$ is Hausdorff.

Defining a complex atlas on $Y(\Gamma)$ is a little more difficult though. At each $\tau \in \mathcal{H}$, one would like to use the local coordinate given by the action[7] of the matrix $\delta_\tau = \left[\begin{smallmatrix} 1 & -\tau \\ 1 & -\overline{\tau}\end{smallmatrix}\right]$ which maps $\tau \in \mathcal{H}$ to $0 \in \mathbb{C}$, but this map does not descend to $Y(\Gamma)$, even locally, if τ is one of those points with non-trivial stabiliser.

Definition A.2.1.4. Let τ be a point in $\mathcal{H}$, with stabiliser Γ_τ. One says that τ is an *elliptic point* for Γ if $\mathrm{P}\Gamma_\tau$ is non-trivial.

Here and in what follows, I denote by $\mathrm{P}H$ the image of a subgroup H of $\mathrm{GL}_2(\mathbb{R})^+$ in $\mathrm{PSL}_2(\mathbb{R})$. The reason for this is that scalar matrices, and in particular -1, act trivially on $\mathcal{H}$.

Since the stabilisers of two points in the same orbit are conjugate, it makes sense to say that a point on $Y(\Gamma)$ is elliptic.

Example A.2.1.5. Let $\tau \in \mathcal{H}$ be an elliptic point, so that there exists a non-scalar matrix $\gamma = \left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\tau = \tau$. This is a quadratic equation on τ, whose discriminant is $\Delta = (d-a)^2 + 4bc = (\mathrm{tr}\,\gamma)^2 - 4$ since $\det\gamma = 1$. Since $\tau \notin \mathbb{R}$, Δ must be negative, so $\mathrm{tr}\,\gamma$ can only be -1, 0 or 1. In particular, $Y\big(\Gamma_1(N)\big)$ has no elliptic point if $N \geqslant 4$.

Example A.2.1.6. By looking at the famous fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ shown on figure A.2.1.7, one sees that the elliptic points on $Y\big(\mathrm{SL}_2(\mathbb{Z})\big)$ are the images of i and of $\rho = e^{\pi i/3}$. Their stabilisers are cyclic, generated respectively by $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0\end{smallmatrix}\right]$ and by $\left[\begin{smallmatrix} 1 & -1 \\ 1 & 0\end{smallmatrix}\right]$.

From this example, one deduces the following result:

[7] Here and in what follows, I implicitly extend the definition of the action of $\mathrm{GL}_2(\mathbb{R})^+$ on $\mathcal{H}$, and rather consider the action on $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{P}^1\mathbb{C}$.

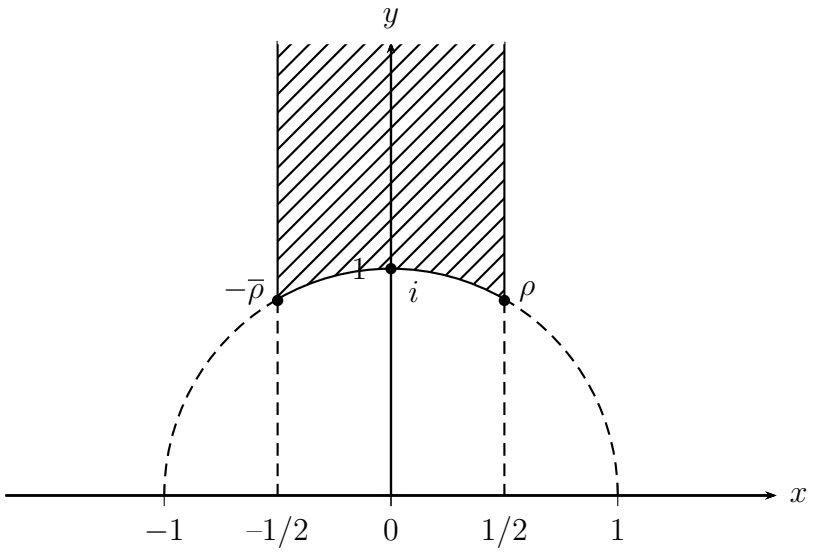


Figure A.2.1.7: A fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Proposition A.2.1.8. *Let $\tau \in \mathcal{H}$ be elliptic for Γ. Then $\mathrm{P}\Gamma_\tau$ is cyclic, of order 2 or 3.*

Accordingly, I define the *order* of an elliptic point to be 2 or 3.

Let $\tau \in \mathcal{H}$ be an elliptic point of order $h \in \{2, 3\}$ for Γ. Then the elements of its stabiliser Γ_τ also stabilise $\overline{\tau}$. Since δ_τ also maps $\overline{\tau}$ to ∞, the elements in $\delta_\tau \Gamma_\tau \delta_\tau^{-1}$ are fractional linear transformations which fix 0 and ∞, hence of the form $z \mapsto az$ for some $a \in \mathbb{C}^*$. Besides, since $\mathrm{P}\Gamma_\tau$ is cyclic of order h, necessarily $a \in \mu_h$ is a h^{th} root of 1. Consequently, by composing the action of δ_τ with $z \mapsto z^h$, one gets a well-defined continuous map from a neighbourhood of $\Gamma\tau \in Y(\Gamma)$ to a neighbourhood of $0 \in \mathbb{C}$. Taking these maps as charts for elliptic points, and simply δ_τ for the non-elliptic points, one proves (cf. [DS05, section 2.2]) that one gets a complex atlas on $Y(\Gamma)$, thus making $Y(\Gamma)$ a Riemann surface.

This is still not the end of it yet though, since $Y(\Gamma)$ is not compact. In order to fix this, one extends the upper half plane $\mathcal{H}$ into

$$\mathcal{H}^\bullet = \mathcal{H} \cup \mathbb{P}^1\mathbb{Q} = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

The new points $s \in \mathbb{P}^1\mathbb{Q}$ thus added are called *cusps*. Note that the obvious action of $\mathrm{SL}_2(\mathbb{Z})$ on them is transitive.

Topologise $\mathcal{H}^\bullet$ by keeping the complex topology on $\mathcal{H}$, by declaring that the $V_y = \{\tau \in \mathcal{H} \mid \mathrm{Im}\,\tau > y\} \cup \{\infty\}$ for $y > 0$ form a basis of neighbourhoods of ∞, and by letting a cusp $s \in \mathbb{Q}$ have the αV_y, $y > 0$, as a basis of neighbourhoods, where $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\alpha\infty = s$. Note that this does not depend on the choice of α since the stabiliser of ∞ under $\mathrm{SL}_2(\mathbb{Z})$ is the group of horizontal translations

$$\left\{ \pm \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}, n \in \mathbb{Z} \right\},$$

and those leave the V_y invariant. As fractional linear transformations transform lines into lines or circles, this means that a basis of neighbourhoods of $s \in \mathbb{Q}$ is formed by the closed disks in $\mathcal{H}^\bullet$ which are tangent at s to the real line, as shown on figure

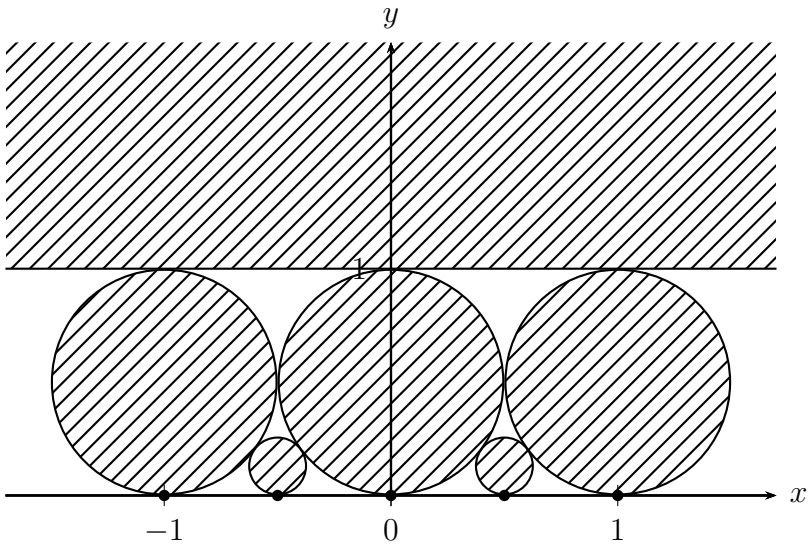


Figure A.2.1.9: Neighbourhoods of some cusps

A.2.1.9. Note that since the V_y form a basis of neighbourhoods of the cusp ∞, this cusp should actually be thought of as $+i\infty$.

This turns $\mathcal{H}^\bullet$ into a Hausdorff space on which $\mathrm{SL}_2(\mathbb{Z})$ acts properly discontinuously, so that the quotient space

$$X(\Gamma) = \Gamma\backslash\mathcal{H}^\bullet$$

is Hausdorff. It is also easy to see that it is compact. In the case $\Gamma = \Gamma(N)$ (respectively $\Gamma_1(N)$, $\Gamma_0(N)$), one writes $X(N)$ (respectively $X_1(N)$, $X_0(N)$) for $X(\Gamma)$. In particular, $X(1) = X\big(\mathrm{SL}_2(\mathbb{Z})\big)$. The images of the cusps in $X(\Gamma)$ are called the *cusps* of $X(\Gamma)$.

Example A.2.1.10. $X(\mathrm{SL}_2(\mathbb{Z}))$ has only one cusp since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1\mathbb{Q}$.

More generally, $X(\Gamma)$ has finitely many cusps since Γ, being a congruence subgroup, has finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Example A.2.1.11. Let $\ell \in \mathbb{N}$ be prime. By example A.2.1.3, one has

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=0}^{\ell} \Gamma_0(\ell)\gamma_i,$$

where $\gamma_i = \left[\begin{smallmatrix} 1 & 0 \\ i & 1 \end{smallmatrix}\right]$ for $0 \leqslant i < \ell$ and $\gamma_\ell = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. From this, one deduces that

$$\mathbb{P}^1\mathbb{Q} = \mathrm{SL}_2(\mathbb{Z})\infty = \mathrm{SL}_2(\mathbb{Z})0 = \bigcup_{i=0}^{\ell} \Gamma_0(\ell)\gamma_i 0 = \Gamma_0(\ell)0 \cup \Gamma_0(\ell)\infty.$$

Since an element of $\Gamma_0(\ell)$ cannot send 0 to ∞, this union is disjoint, which means that $X_0(\ell)$ has two cusps, namely $\Gamma_0(\ell)0$ and $\Gamma_0(\ell)\infty$.

In order to make $X(\Gamma)$ a Riemann surface, it remains to define charts around the cusps. Let $s \in \mathbb{P}^1\mathbb{Q}$ be a cusp. Then $s = \alpha\infty$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, so that the

stabiliser of s in Γ is of the form

$$\left\{\begin{bmatrix} 1 & hn \\ 0 & 1 \end{bmatrix}, n \in \mathbb{Z}\right\} \quad \text{or} \quad \left\{\pm\begin{bmatrix} 1 & hn \\ 0 & 1 \end{bmatrix}, n \in \mathbb{Z}\right\}$$

for some $h \in \mathbb{N}$ called the *width* of the cusp s. It does not depend on α and is the same on the Γ-orbit of s since it is actually the index of $\mathrm{P}\Gamma_s$ in $\mathrm{PSL}_2(\mathbb{Z})$. I then define a chart about s by composing the action of α^{-1} with $z \mapsto e^{2\pi i z/h}$. This descends to a neighbourhood of $\Gamma s \in X(\Gamma)$ by construction, and one checks (cf. [DS05, section 2.4]) that this yields a *bona fide* complex atlas on $X(\Gamma)$.

Definition A.2.1.12. The compact Riemann surface $X(\Gamma) = \Gamma\backslash\mathcal{H}^\bullet$ is called the *modular curve* of *level* Γ.

Example A.2.1.13. Let $\ell \in \mathbb{N}$ be a prime which is at least 5, and consider the modular curve $X_1(\ell)$. Since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1\mathbb{Q}$, every element of $\mathrm{SL}_2(\mathbb{Z})$ stabilizing a cusp is conjugate in $\mathrm{SL}_2(\mathbb{Z})$ to $\pm\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$ for some $n \in \mathbb{N}$, and hence has trace ± 2, so that for all $s \in \mathbb{P}^1\mathbb{Q}$ one has $\Gamma_0(\ell)_s = \pm\Gamma_1(\ell)_s$. In particular, the cusp $\Gamma_0(\ell)s \in X_0(\ell)$ has the same width as $\Gamma_1(\ell)s \in X_1(\ell)$, which proves that the projection $X_1(\ell) \longrightarrow X_0(\ell)$ is unramified at the cusps. In particular, since its degree is $[\mathrm{P}\Gamma_0(\ell)\colon \mathrm{P}\Gamma_1(\ell)] = (\ell-1)/2$, it follows from example A.2.1.11 that the curve $X_1(\ell)$ has $\ell - 1$ cusps.

For instance, one may compute the following formula:

Theorem A.2.1.14. *The genus of $X(\Gamma)$ is*

$$g = 1 + \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \mathrm{P}\Gamma]}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2},$$

where ε_2, ε_3 and ε_∞ denote respectively the number of elliptic points of order 2, 3, and the number of cusps of $X(\Gamma)$.

Proof. Apply the Riemann-Hurwitz formula A.1.1.39 to the projection

$$f\colon X(\Gamma) \twoheadrightarrow X(1).$$

It is of degree $d = [\mathrm{PSL}_2(\mathbb{Z}) : \mathrm{P}\Gamma]$, and ramification can only come from elliptic points or cusps, since a chart at a point which is neither, δ_τ yields a coordinate chart both on $X(\Gamma)$ and $X(1)$, so that f is the identity in local coordinates there.

Let me deal with the elliptic points first. Let $y_2 = \mathrm{SL}_2(\mathbb{Z})i$ be the elliptic point of order 2 of $X(1)$, and similarly let $y_3 = \mathrm{SL}_2(\mathbb{Z})\rho$, $\rho = e^{\pi i/3}$. Take $h \in \{2, 3\}$, and consider a point $x \in X(\Gamma)$ such that $f(x) = y_h$. The stabiliser $\mathrm{P}\Gamma_\tau$ of a $\tau \in \mathcal{H}$ such that $x = \Gamma\tau$ is a subgroup of $\mathrm{PSL}_2(\mathbb{Z})_\tau$. Since the latter is cyclic of prime order h, the former is either the whole of the latter, or reduced to 1. In the first case, x is elliptic of order h, and hence unramified since f is the identity in local coordinates, whereas in the second case, x is not elliptic, hence is ramified of order h since f reads $z \mapsto z^h$ in local coordinates. This yields $d = \sum_{f(x)=y_h} e_x = \varepsilon_h + h\big(\#f^{-1}(y_h) - \varepsilon_h\big)$ whence $\#f^{-1}(y_h) = \frac{d-\varepsilon_h}{h} + \varepsilon_h$, so that the contribution of the ramification of elliptic points of order h in the Riemann-Hurwitz formula is

$$\sum_{f(x)=y_h} e_x - 1 = d - \#f^{-1}(y_h) = \frac{h-1}{h}(d - \varepsilon_h).$$

Next, one finds directly that the contribution of the ramification of the cusps is

$$\sum_{f(x)=\mathrm{SL}_2(\mathbb{Z})\infty} e_x - 1 = d - \varepsilon_\infty.$$

Since $X(1)$ has genus 0 as can be seen on figure A.2.1.7, the Riemann-Hurwitz formula A.1.1.39 then yields

$$2g - 2 = -2d + \frac{1}{2}(d - \varepsilon_2) + \frac{2}{3}(d - \varepsilon_3) + d - \varepsilon_\infty,$$

hence the result. □

Example A.2.1.15. Let $\ell \in \mathbb{N}$ be a prime which is at least 5, and consider the modular curve $X_1(\ell)$. It has no elliptic points by example A.2.1.5, and it has $\ell - 1$ cusps by example A.2.1.13. Since $[\mathrm{PSL}_2(\mathbb{Z})\colon \mathrm{P}\Gamma_1(\ell)] = (\ell^2-1)/2$ by example A.2.1.2, it follows by theorem A.2.1.14 that its genus is

$$g = 1 + \frac{\ell^2 - 1}{24} - \frac{\ell - 1}{2} = \frac{(\ell - 5)(\ell - 7)}{24}.$$

A.2.1.2 Moduli interpretation and Hecke operators

In order to understand the rich structure of modular curves, it is essential to view them as *moduli spaces*, that is to say as spaces classifying certain families of objects.

I begin by introducing the Weil pairing on an elliptic curve, since I shall soon need it. Let E be an elliptic curve with origin O (cf. example A.1.1.35) defined over a perfect field K, let $N \in \mathbb{N}$ be an integer, prime to the characteristic of K if the latter is non-zero, and denote by $E[N]$ the N-torsion subgroup of $E(\overline{K})$ and by μ_N the group of N^{th} roots of 1 in $\overline{K}$. As explained in example A.1.2.16, if $K = \mathbb{C}$ then E is a torus $\mathbb{C}/\Lambda$ for some lattice $\Lambda \in \mathbb{C}$, and so $E[N]$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ as an abstract group, whereas $\mu_N \simeq \mathbb{Z}/N\mathbb{Z}$. By [DS05, theorem 8.1.2], this remains true for every K since I assumed N to be prime to the characteristic of K. Recall from example A.1.1.35 that a divisor $\sum_{P\in E} n_P P$ on E is principal if and only if $\sum_{P\in E} n_P = 0$ in $\mathbb{Z}$ and $\boxplus_{P\in E}[n_P]P = O$ in $E(\overline{K})$, where $[n]$ denotes the "multiplication by n" endomorphism of E for $n \in \mathbb{Z}$. Let now $P, Q \in E[N]$ be N-torsion points. Then the divisor $D_{P,Q} = \sum_{n\in\mathbb{Z}/N\mathbb{Z}} \big((P \boxplus [n]Q) - [n]Q\big)$ is principal, so defines a function $f_{P,Q} \in \overline{K}(E)$ up to multiplication by a constant. Besides, the divisor of the translated function $f(\cdot \boxplus Q)$ is also $D_{P,Q}$, so the ratio $\frac{f(\cdot\boxplus Q)}{f(\cdot)}$ is a non-zero constant function on E which does not depend on the choice of f. This constant is called the *Weil pairing* of P and Q, and is denoted by $\langle P, Q\rangle_N \in \overline{K}^*$, or even by $\langle P, Q\rangle$ if N is clear from the context. It is not difficult to establish the following properties (cf. [DS05, section 7.4]:

- the Weil pairing $\langle\cdot,\cdot\rangle\colon E[N]\times E[N] \longrightarrow \overline{K}^*$ is bilinear (hence the term pairing) and alternate $\big(\langle Q, P\rangle = 1/\langle P, Q\rangle\big)$; in particular, it takes values in μ_N,
- it is a *perfect* pairing $\big(\langle P, Q\rangle = 1$ for all $Q \in E[N] \Longrightarrow P = O\big)$,
- it is Galois-equivariant $\big(\langle\sigma(P), \sigma(Q)\rangle = \sigma(\langle P, Q\rangle)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)\big)$.

In particular, it is necessary that K contain μ_N for $E(K)$ to contain all of $E[N]$.

By A.1.2.16, every elliptic curve over $\mathbb{C}$ is a torus $\mathbb{C}/\Lambda$ for some lattice $\Lambda \in \mathbb{C}$; besides, from the fact that $\mathbb{C}$ is simply connected, one can prove that two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if there exists an $\alpha \in \mathbb{C}^*$ such that $\Lambda' = \alpha\Lambda$. In particular, every elliptic curve is isomorphic to the curve $E_\tau = \mathbb{C}/\Lambda_\tau$, $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ for some $\tau \in \mathbb{C} - \mathbb{R}$, and, possibly after dividing by τ so as to replace τ with $1/\tau$, one may suppose that $\tau \in \mathcal{H}$. Then, for $\tau, \tau' \in \mathcal{H}$, the curves E_τ and $E_{\tau'}$ are isomorphic if and only if τ and τ' lie in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, so the curve $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ classifies elliptic curves over $\mathbb{C}$ up to isomorphism. Passing to the compact curve $X(1)$ amounts to adding the cusp ∞, which may be thought as representing an "elliptic curve with singularities" as a limit of a family of elliptic curves as some parameters tend to ∞.

From there, it is easy to see that for every $N \in \mathbb{N}^*$, the maps

$$\begin{aligned} Y_0(N) = \Gamma_0(N)/\mathcal{H} &\longrightarrow \left\{(E, C) \;\middle|\; \begin{array}{c} E \text{ elliptic curve over } \mathbb{C}, \\ C \subset E \text{ cyclic subgroup of order } N \end{array}\right\} \Big/ \sim \\ \Gamma_0(N)\tau &\longmapsto \big(E_\tau,\ \langle 1/N \bmod \Lambda_\tau\rangle\big), \\ Y_1(N) = \Gamma_1(N)/\mathcal{H} &\longrightarrow \left\{(E, P) \;\middle|\; \begin{array}{c} E \text{ elliptic curve over } \mathbb{C}, \\ P \in E[N] \text{ of order exactly } N \end{array}\right\} \Big/ \sim \\ \Gamma_1(N)\tau &\longmapsto \big(E_\tau,\ 1/N \bmod \Lambda_\tau\big), \end{aligned}$$

and

$$\begin{aligned} Y(N) = \Gamma(N)/\mathcal{H} &\longrightarrow \left\{(E, P, Q) \;\middle|\; \begin{array}{c} E \text{ elliptic curve over } \mathbb{C}, \\ (P, Q) \text{ symplectic basis of } E[N] \end{array}\right\} \Big/ \sim \\ \Gamma(N)\tau &\longmapsto \big(E_\tau,\ 1/N \bmod \Lambda_\tau,\ \tau/N \bmod \Lambda_\tau\big) \end{aligned}$$

are bijections. Here, $E[N]$ denotes the N-torsion subgroup of E, a basis (P, Q) of $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ is said to be symplectic if the Weil pairing $\langle P, Q\rangle$ is $e^{2\pi i/N} \in \mu_N$, and the isomorphism sign $\sim$ means that $(E, T) \sim (E', T')$ if and only if there exists an isomorphism from E to E' mapping the N-torsion data T to T'.

This means that the modular curves $X_0(N)$, $X_1(N)$ and $X(N)$ classify elliptic curves equipped with N-torsion structure (respectively: cyclic subgroup of order N, point of order N, and symplectic basis of the N-torsion) up to isomorphism, the cusps corresponding to "degenerate" curves. For instance, the canonical projections $X(N) \longrightarrow X_1(N)$ and $X_1(N) \longrightarrow X_0(N)$ correspond to the forgetful maps $(E, P, Q) \mapsto (E, P)$ and $(E, P) \mapsto (E, \langle P\rangle)$. The curious reader may find an example of moduli interpretation of a modular curve attached to another congruence subgroup in [RW14]. In what follows, I shall be mainly interested in $X_1(N)$ and $X_0(N)$.

The subgroup $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, with quotient isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$ by $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto d \bmod N$. Since $\Gamma_1(N)$ acts trivially on $X_1(N)$, this yields an action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $X_1(N)$ inducing the identity on $X_0(N)$, which is explicitly

$$\begin{array}{rccc} \langle d\rangle & : & X_1(N) & \longrightarrow & X_1(N) \\ & & (E, P) & \longmapsto & (E, dP) \end{array} \qquad \big(d \in (\mathbb{Z}/N\mathbb{Z})^*\big).$$

The operators $\langle d\rangle$ are called the *Diamond operators* of level N. Note that $\langle d\rangle = \langle -d\rangle$ since $\left[\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right]$ acts trivially on $\mathcal{H}^\bullet$; this reflects the fact that $(E,P) \sim (E,-P)$ by the automorphism $[-1]$ of E.

Similarly, the map

$$\begin{array}{rccc} W_N\colon & X_1(N) & \longrightarrow & X_1(N) \\ & \big(E,P\big) & \longmapsto & \big(E/\langle P\rangle, Q \bmod \langle P\rangle\big), \end{array}$$

where $Q \in E[N]$ is[8] such that $\langle P,Q\rangle = e^{2\pi i/N}$, defines an involution on $X_1(N)$, called the *Fricke involution*.

Finally, recalling that an *isogeny* is a non-constant morphism $\phi\colon E \longrightarrow E'$ between two elliptic curves which sends the origin $O \in E$ to the origin $O' \in E'$, making it automatically a group morphism, one defines for each $n \in N$ prime to N a correspondence

$$\begin{array}{rccc} T_n \quad : & X_1(N) & \longrightarrow & \mathrm{Div}\,\big(X_1(N)\big) \\ & \big(E,P\big) & \longmapsto & \displaystyle\sum_{\substack{\phi\colon E\longrightarrow E' \\ \text{isogeny of degree } n}} \big(E',\phi(P)\big) \end{array}$$

called the n^{th} *Hecke correspondence*, and similarly for $X_0(N)$.

If n is not prime to the level N, the image by an isogeny of degree n of a point $P \in E[N]$ of order exactly N may be of order strictly less than N. For this reason, one defines the Hecke correspondence T_n by

$$\begin{array}{rccc} T_n \quad : & X_1(N) & \longrightarrow & \mathrm{Div}\,\big(X_1(N)\big) \\ & \big(E,P\big) & \longmapsto & \displaystyle\sum_{\substack{\phi\colon E\longrightarrow E' \\ \text{isogeny of degree } n \\ \phi(P) \text{ of order } N}} \big(E',\phi(P)\big), \end{array}$$

the sum being restricted to the isogenies preserving the order of P. When $n = p$ is prime dividing N, the correspondence T_p is often denoted by U_p so as to stress this difference.

More explicitly, an isogeny ϕ of degree n from $E = E_\tau$ to E' may be written as $\mathbb{C}/\Lambda_\tau \longrightarrow \mathbb{C}/\Lambda'$, and so corresponds to a lattice Λ' containing $\Lambda_\tau = \langle \tau, 1\rangle$ with index n. Then $n\Lambda'$ is a sublattice of Λ_τ of index n, and the theory of Hermite reduction (cf. [Coh93, section 2.4]) shows that it is of the form $\langle a\tau + b, d\rangle$ for some uniquely determined $a,d \in \mathbb{N}$ such that $ad = n$ and $b \in \mathbb{Z}$ such that $0 \leqslant b < d$. The image of

$$(E,P) = \left(\mathbb{C}/\langle \tau,1\rangle, \frac{1}{N}\right)$$

by ϕ is then

$$\left(\mathbb{C}\Big/\left\langle \frac{a\tau+b}{n}, \frac{d}{n}\right\rangle, \frac{1}{N}\right) \sim \left(\mathbb{C}\Big/\left\langle \frac{a\tau+b}{d}, 1\right\rangle, \frac{a}{N}\right),$$

[8] Since the Weil pairing is a perfect alternate pairing, the possible choices of Q differ by multiples of P, so W_N is well defined.

so that

$$T_n\big(\Gamma_1(N)\tau\big) = \sum_{\substack{a,d\in\mathbb{N}\\ \gcd(a,N)=1\\ ad=n\\ 0\leqslant b<d}} \langle a\rangle\big(\Gamma_1(N)\left[\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right]\cdot\tau\big). \tag{A.2.1.16}$$

Examining how a sublattice Λ' can be inserted with respective indexes m and n between a lattice Λ'' and a sublattice Λ of index mn, like this:

$$\Lambda'' \underset{mn}{\supset} \Lambda \;\rightsquigarrow\; \Lambda'' \underset{m}{\supset} \Lambda' \underset{n}{\supset} \Lambda,$$

leads to the following formulae (cf. [Ser70, chapitre VII §5 proposition 10]):

Proposition A.2.1.17.

$$\begin{aligned}
T_mT_n &= T_nT_m,\ T_n\langle d\rangle = \langle d\rangle T_n, \quad m,n\in\mathbb{N}, d\in(\mathbb{Z}/N\mathbb{Z})^*\\
T_{mn} &= T_mT_n, \quad \gcd(m,n)=1,\\
T_{p^r} &= T_pT_{p^{r-1}} - p\langle p\rangle T_{p^{r-2}}, \quad p\nmid N \text{ prime}, r\geqslant 2,\\
T_{p^r} &= U_p^r, \quad p|N \text{ prime},
\end{aligned}$$

which can be summarised by writing the formal identity

$$\sum_{n=1}^{+\infty} T_n n^{-s} = \prod_{p|N}\frac{1}{1-U_pp^{-s}}\prod_{p\nmid N}\frac{1}{1-T_pp^{-s}+p^{1-2s}\langle p\rangle}$$

and by saying that the *Hecke algebra* $\mathbb{T}=\mathbb{Z}[T_n,\langle d\rangle]\subset \mathrm{End}_{\mathbb{Z}}\big(\mathrm{Div}(X_1(N))\big)$ is commutative and is generated by the T_p, p prime. For this reason, one often only deals with the Hecke correspondences T_p and U_p for $n=p$ prime only.

Finally, one can show (cf. [DS05, section 6.3]) that the Hecke correspondences T_n and the diamond operators $\langle d\rangle$, seen as endomorphisms of the groups $\mathrm{Div}^0\big(X_0(N)\big)$ and $\mathrm{Div}^0\big(X_1(N)\big)$, preserve the subgroup of principal divisors, and so factor into endomorphisms of $\mathrm{Pic}^0\big(X_0(N)\big)\simeq J_0(N)$ and of $\mathrm{Pic}^0\big(X_1(N)\big)\simeq J_1(N)$.

A.2.1.3 Modular curves as algebraic curves

Although I have defined the modular curves $X_0(N)$, $X_1(N)$ and $X(N)$ as Riemann surfaces, one can prove (cf. [DS05, sections 7.5 to 7.7]) that the curves $X_0(N)$ and $X_1(N)$ can be defined over $\mathbb{Q}$. On the other hand, the curve $X(N)$ can be defined over the cyclotomic field $\mathbb{Q}(\mu_N)$ but not over $\mathbb{Q}$, as its moduli space description

$$X(N)=\big\{(E,P,Q)\mid (P,Q)\text{ basis of }E[N],\ \langle P,Q\rangle=\zeta\big\}$$

uses a fixed primitive N^{th} root ζ of 1. For any extension K of $\mathbb{Q}$, the K-points of $X_0(N)$ correspond to elliptic curves E defined over K and which have a cyclic subgroup $C\subset E[N]$ of order N which is defined over K (that is to say, which is globally invariant under $\mathrm{Gal}(\overline{K}/K)$), in other words, an elliptic curve E admitting an degree N isogeny $\phi\colon E\longrightarrow E'$ which is defined over K, whereas the K-points of $X_1(N)$ correspond to elliptic curves E defined over K and which have a K-rational

point $P \subset E[N](K)$ of order exactly N, and, if K is an extension of $\mathbb{Q}(\mu_N)$, the K-points of $X(N)$ correspond to elliptic curves E defined over K and such that there exist two K-rational points $P, Q \in E[N]$ forming a symplectic basis of $E[N]$.

Example A.2.1.18. For instance, if one can prove that the only $\mathbb{Q}$-rational points on $X_1(11)$ are cusps, then one can conclude that there exists no (non-degenerate) elliptic curve defined over $\mathbb{Q}$ which hasS a rational 11-torsion point.

In [Maz78], B. Mazur was able to determine the finitely many values of N for which $X_0(N)(\mathbb{Q})$ does not only consist of cusps, from which it follows that for **every** elliptic curve E defined over $\mathbb{Q}$, the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of E is isomorphic either to $\mathbb{Z}/n\mathbb{Z}$ with $n \leqslant 10$ or $n = 12$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $n \leqslant 4$ (note that all these cases occur).

In [Mer96], L. Merel improved Mazur's bounds by showing that for all $d \in \mathbb{N}$, the exists a constant $B(d) \in \mathbb{N}$ depending only on d such that for every number field K of degree d and for every elliptic curve E defined over K, the order of a torsion point $P \in E(K)_{\text{tors}}$ is at most $B(d)$.

By section A.1.2.3, the jacobians $J_0(N)$ and $J_1(N)$ of $X_0(N)$ and $X_1(N)$ can thus be viewed as abelian varieties over $\mathbb{Q}$. Since the multiplication-by-d map $[d]$ on an elliptic curve E defined over a field K is itself defined over K, the diamond operators $\langle d \rangle$ seen as endomorphisms of $J_1(N)$ are defined over $\mathbb{Q}$, and since the Galois conjugate of an elliptic curve isogeny $\phi\colon E \longrightarrow E'$ of degree n is also an isogeny of degree n, the Hecke operators T_n seen as endomorphisms of $J_0(N)$ or $J_1(N)$ are also defined over $\mathbb{Q}$. However, the Fricke involution W_N is only defined on the cyclotomic field $\mathbb{Q}(\mu_N)$, since it depends on the choice of a primitive N^{th} root of 1.

The interpretation of modular curves as moduli spaces implies that these curves can be seen as representing functors which, to an extension K of $\mathbb{Q}$, associate the set of elliptic curves with N-torsion data defined over K, up to isomorphism. J. Igusa studied the problem of the representability of these functors extended to general schemes S instead of just fields K. In particular, he proved the following in [Igu59]:

Theorem A.2.1.19 (Igusa)**.** *If $N \geqslant 4$, then the curve $X_1(N)$ admits a canonical model over $\mathbb{Z}[1/N]$ which is smooth over $\mathbb{Z}[1/N]$ and whose geometric fibres are irreducible.*

This means that it makes sense to talk about the reduction modulo a prime $p \nmid N$ of the modular curve $X_1(N)$, and that this reduction $\overline{X_1(N)} = X_1(N)_{\mathbb{F}_p}$ is a non-singular and irreducible curve defined over $\mathbb{F}_p$ which, as expected, classifies the elliptic curves over $\mathbb{F}_p$ having a rational point of order exactly N. Besides, the operators $\langle d \rangle$ and T_n descend to endomorphisms $\overline{T_n}$ and $\overline{\langle d \rangle}$ of the jacobian $\overline{J_1(N)} = \text{Jac}\left(\overline{X_1(N)}\right) = J_1(N)_{\mathbb{F}_p}$. The *Eichler-Shimura relation*, which I am about to introduce, describes the action of the Hecke operator $\overline{T_p}$ on the reduction $\overline{J_1(N)}$ of $J_1(N)$ modulo p. In what follows, I fix a prime $p \nmid N$, and I shall denote reduction modulo p by a bar.

Recall that for every isogeny $\phi\colon E \longrightarrow E'$ between elliptic curves, there exists a *dual isogeny* $\widehat{\phi}\colon E' \longrightarrow E$ of the same degree as ϕ such that $\widehat{\phi} \circ \phi = [\deg \phi]_E$ and $\phi \circ \widehat{\phi} = [\deg \phi]_{E'}$, where I denote by $[n]_E$ the multiplication-by-n endomorphism of an

elliptic curve E; upon identification of an elliptic curve with its Pic^0 as in example A.1.1.35, $\widehat{\phi}$ may be constructed as $\phi^*\colon \mathrm{Pic}^0(E') \longrightarrow \mathrm{Pic}^0(E)$. Let $\overline{E}$ be an elliptic curve defined over $\overline{\mathbb{F}_p}$, and let $\sigma_p\colon x \mapsto x^p$ denote the Frobenius automorphism in $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. It induces a morphism $\sigma_p\colon \overline{E} \longrightarrow \overline{E}^{\sigma_p}$ which is a purely inseparable isogeny of degree p, so the dual isogeny $\widehat{\sigma_p}$ is also of degree p. As p is prime, it is therefore either separable, in which case $[p]_{\overline{E}}$ has separable degree p and inseparable degree p, or purely inseparable, in which case $[p]_{\overline{E}}$ is purely inseparable of degree p^2. In the first case, one says that $\overline{E}$ is *ordinary*, and in the second case, one says that $\overline{E}$ is *supersingular*. This distinction is visible on the p-torsion of $\overline{E}$: the cardinal of almost all the fibres of a morphism $f\colon X \longrightarrow Y$ is $\deg_{\mathrm{sep}} f$ as noted in the end of section A.1.1.1, and for every $r \in \mathbb{N}$, the cardinal of the fibres of $[p^r]_{\overline{E}}$ is $\#\operatorname{Ker}[p^r]_{\overline{E}} = \#\overline{E}(\overline{\mathbb{F}_p})[p^r]$, whence

$$\#\overline{E}(\overline{\mathbb{F}_p})[p^r] = \deg_{\mathrm{sep}}[p^r]_{\overline{E}} = (\deg_{\mathrm{sep}}[p]_{\overline{E}})^r = (\deg_{\mathrm{sep}}\widehat{\sigma_p})^r$$

as $[p]_{\overline{E}} = \widehat{\sigma_p}\sigma_p$ and σ_p is purely inseparable, and so for all $r \in \mathbb{N}$,

$$\overline{E}(\overline{\mathbb{F}_p})[p^r] \simeq \begin{cases} \mathbb{Z}/p^r\mathbb{Z}, & \overline{E} \text{ ordinary,} \\ \{0\}, & \overline{E} \text{ supersingular.} \end{cases}$$

This distinction leads to the following crucial property:

Theorem A.2.1.20 (Eichler-Shimura relation)**.** *Let $N \in N$, and let $p \nmid N$ be a prime. Then the relation*

$$\overline{T_p} = \sigma_p + p\overline{\langle p\rangle}\sigma_p^{-1}$$

holds in $\mathrm{End}\left(J_1(N)_{\mathbb{F}_p}\right)$.

Remark A.2.1.21. Since σ_p is ramified of degree p everywhere, $p\sigma_p^{-1}$ agrees with the pullback σ_p^*, and so $p\overline{\langle p\rangle}\sigma_p^{-1}$ is indeed an endomorphism of $\mathrm{Pic}^0\left(\overline{X_1(N)}\right) \simeq J_1(N)_{\mathbb{F}_p}$.

Proof. If $N < 4$, then $X_1(N)$ has genus 0, so one may define $J_1(N)_{\mathbb{F}_p} = \{0\}$ in this case even though Igusa's theorem A.2.1.19 does not apply, and the Eichler-Shimura relation trivially holds. Assume henceforth that $N \geqslant 4$. Let $(E, P) \in X_1(N)(\overline{\mathbb{Q}})$ be a $\overline{\mathbb{Q}}$-point of $X_1(N)$ seen as a moduli space, so that E is an elliptic curve over $\overline{\mathbb{Q}}$ and P is a point of E of order exactly N, and fix a prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ lying above p. Then, by definition,

$$T_p(E,P) = \sum_{\substack{\phi\colon E \longrightarrow E' \\ \text{isogeny of degree } p}} \left(E', \phi(P)\right) = \sum_{\substack{C \subset E[p] \\ \text{subgroup of order } p}} (E/C, P + C)$$

by identifying an isogeny ϕ with its kernel C, and so

$$\overline{T_p}(\overline{E}, \overline{P}) = \sum_{\substack{C \subset E[p] \\ \text{subgroup of order } p}} (\overline{E/C}, \overline{P + C})$$

provided that E has good reduction at $\mathfrak{p}$.

Let $\phi\colon E \longrightarrow E'$ be an isogeny of degree p, let $P' = \phi(P)$, let $\psi = \widehat{\phi}\colon E' \longrightarrow E$ be the dual isogeny, and let $\overline{\phi}\colon \overline{E} \longrightarrow \overline{E'}$ and $\overline{\psi}\colon \overline{E'} \longrightarrow \overline{E}$ denote their reductions modulo $\mathfrak{p}$. Observe that

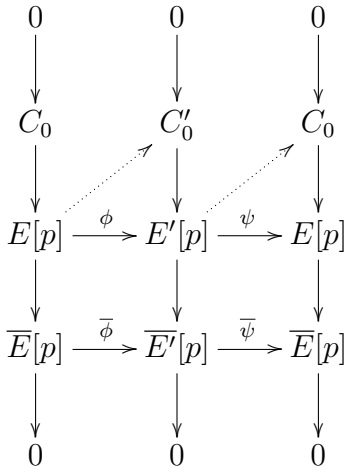
(i) if $\overline{\phi} = \iota \circ \sigma_p$ is purely inseparable, hence is the Frobenius $\sigma_p \colon \overline{E} \longrightarrow \overline{E}^{\sigma_p}$ followed by an isomorphism $\iota \colon \overline{E}^{\sigma_p} \xrightarrow{\sim} \overline{E'}$, then $\overline{\phi}(\overline{E}, \overline{P}) \sim \sigma_p(\overline{E}, \overline{P})$ are isomorphic by ι^{-1}, and

(ii) if $\overline{\psi} = \iota \circ \sigma_p$ is purely inseparable, hence is the Frobenius $\sigma_p \colon \overline{E'} \longrightarrow \overline{E'}^{\sigma_p}$ followed by an isomorphism $\iota \colon \overline{E'}^{\sigma_p} \xrightarrow{\sim} \overline{E}$, then since ψ maps $P' = \phi(P)$ to pP, the isomorphism ι maps $\overline{P'}^{\sigma_p}$ to $p\overline{P}$, and applying σ_p^{-1} to the coefficients of ι yields an isomorphism

$$\begin{aligned} \iota^{\sigma_p^{-1}} \colon \overline{E'} &\longrightarrow \overline{E}^{\sigma_p^{-1}} \\ \overline{P'} &\longmapsto p\overline{P}^{\sigma_p^{-1}}, \end{aligned}$$

so that $(\overline{E'}, \overline{P'}) \sim (\overline{E}^{\sigma_p^{-1}}, p\overline{P}^{\sigma_p^{-1}}) = \langle p \rangle \sigma_p^{-1}(\overline{E}, \overline{P})$.

Assume first that the reduction $\overline{E}$ of E modulo $\mathfrak{p}$ is ordinary. Then $\overline{E}[p] \simeq \mathbb{Z}/p\mathbb{Z}$, so the kernel C_0 of the reduction modulo $\mathfrak{p}$ map $E[p] \longrightarrow \overline{E}[p]$ is one of the $p+1$ subgroups C of order p of $E[p]$. The isomorphism class of the pair $(\overline{E/C}, \overline{P+C})$ then only depends on whether $C = C_0$ or not. To see this, take a subgroup C or order p of $E[p]$, let $E' = E/C$, $P' = P + C \in E'$, and let $C'_0 \subset E'[p]$ denote the kernel of the reduction modulo $\mathfrak{p}$ map $E'[p] \longrightarrow \overline{E'}[p]$, which is a subgroup of order p of $E'[p]$ as E', being isogenous to E, is also ordinary at $\mathfrak{p}$. One has the following commutative diagram with exact columns:



Besides, both ϕ and ψ are of degree p. Note that $\psi(E'[p])$ is of order p since the fibres of ψ are of order $\deg \psi = p$, and $\psi(E'[p]) \subset \operatorname{Ker} \phi$ since $\phi\psi(E'[p]) = pE'[p] = 0$. Since $\operatorname{Ker} \phi$ is also of order p, it follows that $\psi(E'[p]) = \operatorname{Ker} \phi = C$, and similarly $\phi(E[p]) = \operatorname{Ker} \psi = C'$.

Assume that $C = C_0$. Then $\psi(E'[p]) = \operatorname{Ker} \phi = C = C_0$. By looking at the right part of the diagram above, one sees that $\overline{\psi}_{|\overline{E'}[p]} = 0$, so that $\overline{E'}[p] \subset \operatorname{Ker} \overline{\psi}$. But on the other hand, $\operatorname{Ker} \overline{\psi} \subset \operatorname{Ker} \overline{\phi\psi} = \overline{E'}[p]$, so that $\operatorname{Ker} \overline{\psi} = \overline{E'}[p]$ is of order p as $\overline{E'}$ is ordinary. It follows that $\deg_{\mathrm{sep}} \overline{\psi} = p$, so that $\deg_{\mathrm{ins}} \overline{\psi} = 1$, and $\deg_{\mathrm{sep}} \overline{\phi} = 1$ and $\deg_{\mathrm{ins}} \overline{\phi} = p$ by multiplicativity of the degrees. Therefore, $\overline{\phi}$ is purely inseparable, hence (i) applies and so $(\overline{E/C}, \overline{P+C}) \sim \sigma_p(\overline{E}, \overline{P})$ for $C = C_0$.

Assume now that that $C \neq C_0$. In this case, $\phi(C_0) = \phi(E[p]) = \operatorname{Ker} \psi = C'$ is of order p. Also $\phi(C_0) \subset C'_0$ by commutativity of the diagram, so that $C' = C'_0$.

Then, just as in the previous case, one deduces that $\overline{\phi}_{|\overline{E}[p]} = 0$ and hence that $\operatorname{Ker}\overline{\phi} = \overline{E}[p]$. It follows that $\deg_{\text{sep}}\overline{\phi} = p$ and $\deg_{\text{ins}}\overline{\phi} = 1$, so that $\deg_{\text{sep}}\overline{\psi} = 1$ and $\deg_{\text{ins}}\overline{\psi} = p$, so this time $\overline{\psi}$ is purely inseparable, hence (ii) applies and so $(\overline{E/C}, \overline{P+C}) \sim (\overline{E}^{\sigma_p^{-1}}, p\overline{P}^{\sigma_p^{-1}}) \sim \langle p\rangle\sigma_p^{-1}(\overline{E}, \overline{P})$ for $C \neq C_0$.

Summing up, one gets

$$\begin{aligned}
\overline{T_p}(\overline{E}, \overline{P}) &= \sum_{\substack{C\subset E[p]\\ \text{subgroup of order } p}} (\overline{E/C}, \overline{P+C}) \\
&= \sum_{C=C_0} (\overline{E/C}, \overline{P+C}) + \sum_{C\neq C_0} (\overline{E/C}, \overline{P+C}) \\
&= \sigma_p(\overline{E}, \overline{P}) + p\langle p\rangle\sigma_p^{-1}(\overline{E}, \overline{P}) \\
&= (\sigma_p + p\langle p\rangle\sigma_p^{-1})(\overline{E}, \overline{P})
\end{aligned}$$

provided that $\overline{E}$ is ordinary.

This still holds if $\overline{E}$ is supersingular, since in this case one has

$$(\overline{E/C}, \overline{P+C}) = \sigma_p(\overline{E}, \overline{P}) = \langle p\rangle\sigma_p^{-1}(\overline{E}, \overline{P}).$$

Indeed, one then has $\operatorname{Ker}\overline{\phi} \subset \overline{E}[p] = 0$, and also $\operatorname{Ker}\overline{\psi} \subset \overline{E'}[p] = 0$ since E' is also supersingular, so that $\overline{\phi}$ and $\overline{\psi}$ are both purely inseparable and so both (i) and (ii) apply.

The relation

$$\overline{T_p}(\overline{E}, \overline{P}) = (\sigma_p + p\langle p\rangle\sigma_p^{-1})(\overline{E}, \overline{P})$$

is thus valid in all cases, and the proof is complete. □

A.2.2 Modular forms

I now proceed to a brief study of modular forms, which are the natural inhabitants of modular curves.

A.2.2.1 Definitions and examples

Fix an integer $k \in \mathbb{Z}_{\geqslant 0}$, and let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Definition A.2.2.1. The weight-k (right) action of the group $\mathrm{GL}_2(\mathbb{R})^+$ of elements of $\mathrm{GL}_2(\mathbb{R})$ with positive determinant on the space of functions $f\colon \mathcal{H}^\bullet \longrightarrow \mathbb{C}$ is defined by

$$(f|_k\gamma)(\tau) = (\det\gamma)^{k/2}(c\tau+d)^{-k}f(\gamma\tau), \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})^+.$$

A *modular form* of *weight* k and *level* Γ is a holomorphic function

$$f\colon \mathcal{H}^\bullet \longrightarrow \mathbb{C}$$

satisfying the functional equation

$$f|_k\gamma = f \tag{A.2.2.2}$$

for all $\gamma \in \Gamma$.

Since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on the cusps, one can rephrase the holomorphy condition on f by demanding that f be holomorphic on $\mathcal{H}$ and that $f|_k\gamma$ be bounded at ∞ for γ ranging over a system of coset representatives of $\Gamma \setminus \mathrm{SL}_2(\mathbb{Z})$.

It is clear that modular forms of weight k and level Γ form a $\mathbb{C}$-vector space, which I shall denote by $M_k(\Gamma)$.

Example A.2.2.3. For even $k \geqslant 4$, the form

$$G_k(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m\tau+n)^k}$$

is a non-trivial form in $M_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$.

Remark A.2.2.4. Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. It is clear that if $f \in M_k(\Gamma)$ is a modular form of weight k and level Γ, then $f|_k\alpha$ is a modular form of weight k and level $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ (which is also a congruence subgroup by [DS05, lemma 5.1.1]).

In particular, take $\alpha = \left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right]$ for some $t \in \mathbb{N}$. Then $(f|_k\alpha)(\tau)$ is $f(t\tau)$ up to a multiplicative constant, and since

$$\alpha^{-1}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\alpha = \begin{bmatrix} a & b/t \\ tc & d \end{bmatrix},$$

$f(t\tau) \in M_k\big(\Gamma_0(tN)\big)$ if $f \in M_k\big(\Gamma_0(N)\big)$, and $f(t\tau) \in M_k\big(\Gamma_1(tN)\big)$ if $f \in M_k\big(\Gamma_1(N)\big)$.

Let N be the level of Γ. Then $\left[\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$, which means that a modular form for Γ must be N-periodic, hence have a Fourier expansion

$$f = \sum_{n=0}^{\infty} a_n(f) q_N^n$$

called the q_N-*expansion* of f, where I let $q_N = e^{2\pi i\tau/N}$. Indeed, the fact that f is bounded at ∞ forces the coefficients $a_n(f)$ to vanish for $n < 0$, since $q_N \to 0$ when $\tau \to i\infty$.

In practice, I shall only consider $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, so that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \Gamma,$$

and the q_N-expansion of modular forms will be understood to be in terms of

$$q = q_1 = e^{2\pi i\tau},$$

and will be referred to as the q-expansion of the form. When it is understood that $\Gamma = \Gamma_0(N)$ (respectively $\Gamma_1(N)$), I shall say that a form has level N to mean that it has level $\Gamma_0(N)$ (respectively $\Gamma_1(N)$).

Example A.2.2.5. For the forms G_k from example A.2.2.3, one computes (cf. [Ser70, corollaire p.151]) that $G_k = 2\zeta(k)E_k$,

$$E_k = 1 - \frac{2k}{b_k}\sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_h(n) = \sum_{0<d|n} d^h$ and the b_k are the Bernoulli numbers, defined by

$$\frac{T}{\exp(T)-1} = \sum_{k=0}^{+\infty} b_k \frac{T^k}{k!}.$$

For instance,

$$E_4 = 1 + 240 \sum_{n=1}^{+\infty} \sigma_3(n) q^n,$$

$$E_6 = 1 - 504 \sum_{n=1}^{+\infty} \sigma_5(n) q^n,$$

$$E_8 = 1 + 480 \sum_{n=1}^{+\infty} \sigma_7(n) q^n,$$

$$E_{10} = 1 - 264 \sum_{n=1}^{+\infty} \sigma_9(n) q^n,$$

and so on.

In particular, one computes that

$$j = \frac{1728 E_4^3}{E_4^3 - E_6^2} = \frac{1}{q} + 744 + 196884 q^2 + O(q^3).$$

This j is not holomorphic, but it is of weight 0, so it descends to a meromorphic function of $X(1)$. One can show that it has degree 1, so that $\mathbb{C}\big(X(1)\big) = \mathbb{C}(j)$. In particular, it is injective on $X(1)$, so that by the moduli interpretation of $X(1)$, two elliptic curves defined over $\mathbb{C}$ are isomorphic if and only if they give rise to the same value of j. For this reason, j is called the *modular invariant*.

As the above example shows, the q-expansion coefficients of modular forms often carry interesting arithmetic information. Here are two other examples (more can be found in [Ste07, section 1.5]):

Example A.2.2.6. Let $\Theta = \sum_{n\in\mathbb{Z}} q^{n^2}$. One can prove (cf. [DS05, section 1.2]) that for all[9] $k \in \mathbb{N}$, $\Theta^{2k} \in M_k\big(\Gamma_0(4)\big)$ is modular of weight k and level $\Gamma_0(4)$. Its q-expansion coefficients are $a_n = r(n, 2k)$, the number of ways to write n as the sum of $2k$ squares in $\mathbb{Z}$.

Example A.2.2.7. Consider

$$\Delta = q \prod_{n=1}^{+\infty} (1-q^n)^{24} = q + \sum_{n=2}^{+\infty} \tau(n) q^n.$$

One can show that Δ is a modular form of weight 12 and level 1. This identity defines *Ramanujan's tau function* $\tau(n)$, which is the related to the construction of expander graphs, which play a role in communication network theory.

[9] Actually, one can generalise definition A.2.2.1 to the case of half-integral weight k. It then turns out that Θ is modular of level $\Gamma_0(4)$ and weight $1/2$, so one can also study odd powers of Θ. I shall not do it here.

Assume from now on that k is even. One computes that

$$\mathrm{d}(\gamma\tau) = \frac{\det\gamma}{(c\tau+d)^2}\mathrm{d}\tau \text{ for } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})^+,$$

so that the functional equation (A.2.2.2) defining modularity can be rephrased by saying that the form

$$\omega_f = f(\tau)(\mathrm{d}\tau)^{k/2}$$

is invariant under the action of Γ, that is to say $\gamma^*\omega_f = \omega_f$ for all $\gamma \in \Gamma$. Thus for instance modular forms of weight zero correspond to functions on $X(\Gamma)$, whereas modular forms of weight 2 correspond to differential 1-forms on $X(\Gamma)$. However, in order for these differential forms to be holomorphic on $X(\Gamma)$, the modular form f must vanish at the cusps, since, at the cusp $\Gamma\infty$ for instance, the local parameter for $X(\Gamma)$ is q, and $\mathrm{d}\tau = \frac{\mathrm{d}q}{q}$. This leads to the notion of cusp forms.

Definition A.2.2.8. A *cusp form* is a modular form which vanishes at the cusps.

In particular, $a_0(f) = 0$ if f is a cusp form. I shall denote[10] the subspace of cusp forms of weight k for Γ by $S_k(\Gamma)$.

Example A.2.2.9. $\Delta \in S_{12}(1)$ is a cuspform, since it vanishes at ∞, which is the only cusp of $X(1)$.

The Riemann-Roch theorem A.1.1.33 shows that $M_k(\Gamma)$ and $S_k(\Gamma)$ are finite-dimensional vector spaces over $\mathbb{C}$, and leads to formulae for their dimensions:

Theorem A.2.2.10. *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, and let $X(\Gamma)$ be the associated modular curve. Denote its genus, the number of its elliptic points of order 2, 3, and the number of its cusps respectively by g, ε_2, ε_3 and ε_∞. Then, for every even integer $k \in \mathbb{Z}$,*

$$\dim_{\mathbb{C}} M_k(\Gamma) = \begin{cases} (g-1)(k-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty & \text{if } k \geqslant 2, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0, \end{cases}$$

and

$$\dim_{\mathbb{C}} S_k(\Gamma) = \begin{cases} (g-1)(k-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + (\frac{k}{2}-1)\varepsilon_\infty & \text{if } k \geqslant 4, \\ g & \text{if } k = 2, \\ 0 & \text{if } k \leqslant 0. \end{cases}$$

Proof. Let π denote the projection from $\mathcal{H}^\bullet$ to $X(\Gamma)$. For each even $k \in \mathbb{N}$, the pullback by π defines a $\mathbb{C}$-linear isomorphism

$$\pi^* \colon \Omega^{\otimes k/2}_{\mathrm{mer}}\big(X(\Gamma)\big) \xrightarrow{\sim} \Omega^{\otimes k/2}_{\mathrm{mer}}(\mathcal{H})^\Gamma$$

from the space $\Omega^{\otimes k/2}_{\mathrm{mer}}\big(X(\Gamma)\big)$ of meromorphic $k/2$-fold multi-differential forms on $X(\Gamma)$ to the space $\Omega^{\otimes k/2}_{\mathrm{mer}}(\mathcal{H})^\Gamma$ of meromorphic $k/2$-fold multi-differential forms ξ on

[10] This is the standard notation, the S comes from the German term "Spitzenform".

$\mathcal{H}$ which are Γ-invariant, that is to say such that $\gamma^*\xi = \xi$ for all $\gamma \in \Gamma$. The idea is to describe a criterion on a non-zero $\omega \in \Omega^{\otimes k/2}_{\mathrm{mer}}\big(X(\Gamma)\big)$ for $f = \pi^*\omega/(\mathrm{d}\tau)^{k/2}$ to lie in $M_k(\Gamma)$ or $S_k(\Gamma)$.

Pick a point $\tau_0 \in \mathcal{H}$, and let $h \in \mathbb{N}$ be 1 if τ_0 is not elliptic for Γ, 2 if τ_0 is elliptic or order 2, and 3 if τ_0 is elliptic of order 3. Then $z = (\tau - \tau_0)^h$ is a local coordinate about $\pi(\tau_0)$, and in a neighbourhood of $\pi(\tau_0)$, ω reads

$$\omega = a(z^n + \cdots)(\mathrm{d}z)^{k/2}$$

where $n = \mathrm{ord}_{\pi(\tau_0)}\,\omega \in \mathbb{Z}$ and $a \in \mathbb{C}^*$. One computes that

$$\mathrm{d}z = h(\tau - \tau_0)^{h-1}\mathrm{d}\tau,$$

so that

$$\pi^*\omega = a\big((\tau - \tau_0)^{nh} + \cdots\big)\big(h(\tau - \tau_0)^{h-1}\mathrm{d}\tau\big)^{k/2} = b\big((\tau - \tau_0)^{nh+(h-1)k/2} + \cdots\big)(\mathrm{d}\tau)^{k/2}$$

for some $b \in \mathbb{C}^*$, hence

$$f \text{ is holomorphic at } \tau_0 \iff \mathrm{ord}_{\pi(\tau_0)}\,\omega + \left(1 - \frac{1}{h}\right) k/2 \geqslant 0.$$

Let now $s \in \mathbb{P}^1\mathbb{Q}$ be a cusp of width $h \in \mathbb{N}$. A local coordinate at $\pi(s)$ is $q = e^{2\pi i\tau/h}$ preceded by an fractional linear transformation from $\mathrm{SL}_2(\mathbb{Z})$, which is biholomorphic, hence does not ramify and can be neglected. Writing again

$$\omega = a(q^n + \cdots)(\mathrm{d}q)^{k/2}$$

about $\pi(s)$, where $n = \mathrm{ord}_{\pi(s)}\,\omega \in \mathbb{Z}$ and $a \in \mathbb{C}^*$, one computes that

$$\mathrm{d}q = \frac{2\pi i}{h} e^{2\pi i\tau/h}\mathrm{d}\tau,$$

so that

$$\pi^*\omega = a\big(e^{2n\pi i\tau/h} + \cdots\big)\big(\frac{2\pi i}{h} e^{2\pi i\tau/h}\mathrm{d}\tau\big)^{k/2} = b\big(e^{2(n+k/2)\pi i\tau/h} + \cdots\big)(\mathrm{d}\tau)^{k/2}$$

for some $b \in \mathbb{C}^*$, hence

$$f \text{ is holomorphic at } s \iff f \text{ is bounded at } s \iff \mathrm{ord}_{\pi(s)}\,\omega + k/2 \geqslant 0,$$

and

$$f \text{ vanishes at } s \iff \mathrm{ord}_{\pi(s)}\,\omega + k/2 - 1 \geqslant 0.$$

Besides, since $(\mathrm{d}j)^{k/2} \in \Omega^{\otimes k/2}_{\mathrm{mer}}\big(X(\Gamma)\big)$, on has $\omega = \phi \cdot (\mathrm{d}j)^{k/2}$ for some non-zero rational map $\phi \in \mathbb{C}\big(X(\Gamma)\big)^*$. The above then shows that

$$\begin{aligned}
&\pi^*\omega/(\mathrm{d}\tau)^{k/2} \in M_k(\Gamma) \\
&\iff \operatorname{div}(\omega) + \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 2}}} \frac{k}{4}P + \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 3}}} \frac{k}{3}P + \sum_{\substack{P\in X(\Gamma)\\ \text{cusp}}} \frac{k}{2}P \geqslant 0 \\
&\iff \operatorname{div}(\omega) + \left\lfloor\frac{k}{4}\right\rfloor \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 2}}} P + \left\lfloor\frac{k}{3}\right\rfloor \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 3}}} P + \frac{k}{2}\sum_{\substack{P\in X(\Gamma)\\ \text{cusp}}} P \geqslant 0 \\
&\iff \operatorname{div}(\phi) + D \geqslant 0,
\end{aligned}$$

where $D = \left\lfloor\frac{k}{4}\right\rfloor \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 2}}} P + \left\lfloor\frac{k}{3}\right\rfloor \sum_{\substack{P\in X(\Gamma)\\ \text{elliptic}\\ \text{of order 3}}} P + \frac{k}{2}\sum_{\substack{P\in X(\Gamma)\\ \text{cusp}}} P + \frac{k}{2}C$

and $C = \operatorname{div}(\mathrm{d}j)$ is a canonical divisor by definition A.1.1.23. Similarly,

$$\pi^*\omega/(\mathrm{d}\tau)^{k/2} \in S_k(\Gamma) \iff \operatorname{div}(\phi) + D - \sum_{\substack{P\in X(\Gamma)\\ \text{cusp}}} P \geqslant 0.$$

It follows that $\dim M_k(\Gamma) = h^0(D)$ and that $\dim S_k(\Gamma) = h^0\left(D - \sum_{P \text{ cusp}} P\right)$.

By the Riemann-Roch theorem A.1.1.33(ii), the degree of C is $2g-2$, so

$$\begin{aligned}
\deg D &= \left\lfloor\frac{k}{4}\right\rfloor \varepsilon_2 + \left\lfloor\frac{k}{3}\right\rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty + \frac{k}{2}(2g-2) \\
&\geqslant \frac{k-2}{4}\varepsilon_2 + \frac{k-2}{3}\varepsilon_3 + \frac{k}{2}\varepsilon_\infty + \frac{k}{2}(2g-2) \\
&= \frac{k-2}{2}\left(\frac{1}{2}\varepsilon_2 + \frac{2}{3}\varepsilon_3 + \varepsilon_\infty + 2g - 2\right) + \varepsilon_\infty + 2g - 2.
\end{aligned}$$

By the genus formula A.2.1.14, the term between parentheses is $[\mathrm{PSL}_2(\mathbb{Z})\colon \mathrm{P}\Gamma]/6$, which is positive, so for $k \geqslant 2$ one has $\deg D > 2g-2$ and the Riemann-Roch theorem A.1.1.33(iii) shows that

$$\dim M_k(\Gamma) = \deg D + 1 - g = \left\lfloor\frac{k}{4}\right\rfloor \varepsilon_2 + \left\lfloor\frac{k}{3}\right\rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty + (k-1)(g-1).$$

Similarly, if $k \geqslant 4$,

$$\deg\left(D - \sum_{P \text{ cusp}} P\right) \geqslant \frac{k-2}{2}\left(\frac{1}{2}\varepsilon_2 + \frac{2}{3}\varepsilon_3 + \varepsilon_\infty + 2g - 2\right) + 2g - 2 > 2g - 2$$

so for $k \geqslant 4$,

$$\dim S_k(\Gamma) = \deg D - \varepsilon_\infty + 1 - g = \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 \left(\frac{k}{2} - 1\right) \varepsilon_\infty + (k-1)(g-1).$$

For $k = 2$, one has $D - \sum_{P \text{ cusp}} P = C$, so the cuspforms of weight 2 correspond exactly to the holomorphic differential forms on $X(\Gamma)$ as explained above, and $\dim S_2(\Gamma) = g$ by definition of the genus.

For $k = 0$, the elements of $M_0(\Gamma)$ correspond to holomorphic functions on $X(\Gamma)$ and are hence constant since $X(\Gamma)$ is compact. In particular, $S_0(\Gamma) = \{0\}$.

Finally, if $k < 0$, then a form $f \in M_k(\Gamma)$ would satisfy $f^{12}\Delta^{|k|} \in S_0(\Gamma) = \{0\}$, so that $M_k(\Gamma) = \{0\}$. □

Example A.2.2.11. By example A.2.1.15, if ℓ is a prime which is at least 5, the dimension of $S_2\big(\Gamma_1(\ell)\big)$ is $\frac{(\ell-5)(\ell-7)}{24}$.

Example A.2.2.12. Examine the case of level 1 ($\Gamma = \mathrm{SL}_2(\mathbb{Z})$) more closely. One can prove that the graded ring

$$M\big(\mathrm{SL}_2(\mathbb{Z})\big) = \bigoplus_{k=0}^{+\infty} M_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$$

is generated by the forms E_4 and E_6, which are algebraically independent (cf. [Ste07, theorem 2.17]), so that it is isomorphic to $\mathbb{C}[E_4, E_6]$, where E_4 has grading 4 and E_6 has grading 6. In particular, the forms $E_4^a E_6^b$, $4a + 6b = k$, a, $b \in \mathbb{Z}_{\geqslant 0}$, form a basis of $M_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$ over $\mathbb{C}$, so that $\dim_{\mathbb{C}} M_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$ is the number of ways to write k as $4a + 6b$, a, $b \in \mathbb{Z}_{\geqslant 0}$. This is 0 if k is odd, $\lfloor k/12 \rfloor - 1$ if $k \equiv 2 \bmod 12$, and $\lfloor k/12 \rfloor$ in the other cases, which agrees with theorem A.2.2.10 since $X(1)$ has genus $g = 0$, $\varepsilon_2 = 1$ elliptic point of order 2, $\varepsilon_3 = 1$ elliptic point of order 3, and $\varepsilon_\infty = 1$ cusp, as can be seen on figure A.2.1.7.

In particular, this implies that E_8 and E_4^2, which both lie in the 1-dimensional space $M_8\big(\mathrm{SL}_2(\mathbb{Z})\big)$, are proportional, hence equal by looking at the constant term a_0, and similarly that $E_4 E_6 = E_{10}$. From this and example A.2.2.5, one deduces the surprising identities

$$\forall n \in \mathbb{N},\ \sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)$$

and

$$\forall n \in \mathbb{N},\ 11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n).$$

I now have a look at the cuspform spaces $S_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$. Since ∞ is the only cusp of $X(1)$, a modular form of level 1 is a cusp form if and only if it vanishes at ∞,

that is to say if and only if its coefficient a_0 is 0. Thus for instance the form $E_4^3 - E_6^2$ is a cusp form of weight 1 and level 1, just like the form Δ introduced in example A.2.2.7 above.

Multiplication by Δ induces isomorphisms

$$M_k\big(\mathrm{SL}_2(\mathbb{Z})\big) \simeq S_{k+12}\big(\mathrm{SL}_2(\mathbb{Z})\big),$$

so that $\dim_{\mathbb{C}} S_k\big(\mathrm{SL}_2(\mathbb{Z})\big) = \dim_{\mathbb{C}} M_{k-12}\big(\mathrm{SL}_2(\mathbb{Z})\big)$ for $k \geqslant 12$. In particular, $S_k\big(\mathrm{SL}_2(\mathbb{Z})\big)$ has dimension 1 exactly when $k \in \{12, 16, 18, 20, 22, 26\}$, and is then respectively spanned by Δ, $E_4\Delta$, $E_6\Delta$, $E_8\Delta$, $E_{10}\Delta$ and $E_{14}\Delta$. In the case of weight $k = 12$, one sees by looking at the coefficient of q^1 that

$$\Delta = \frac{1}{12^3}(E_4^3 - E_6^2).$$

Example A.2.2.13. Come back to the forms $\Theta^{2k} \in M_k\big(\Gamma_0(4)\big)$ from example A.2.2.6 and take $k = 2$. One can prove with theorem A.2.2.10 that the space $M_2\big(\Gamma_0(4)\big)$ has dimension 2 over $\mathbb{C}$, and is spanned by the forms

$$1 + 24\sum_{n=1}\sum_{\substack{0<d|n\\ d \text{ odd}}} dq^n = 1 + 24q + O(q^2), \text{ and}$$
$$1 + 8\sum_{n=1}\sum_{\substack{0<d|n\\ 4\nmid d}} dq^n = 1 + 8q + O(q^2).$$

Since Θ^4 lies in this space, it must be a linear combination of these two forms. Actually, since $\Theta = 1 + 2q + O(q^2)$, $\Theta^4 = 1 + 8q + O(q^2)$ equals the latter of these two forms, hence the identity

$$r(n,4) \overset{\text{def}}{=} \sharp\Big\{(x,y,z,t) \in \mathbb{Z}^4 \mid n = x^2 + y^2 + z^2 + t^2\Big\} = 8\sum_{\substack{0<d|n\\ 4\nmid d}} d.$$

Similarly, one finds formulae for $r(n, 2k)$ for $k = 3, 4, 5$. However, for $k \geqslant 6$, such formulae no longer exist. The deep reason for that is that $M_k\big(\Gamma_0(4)\big)$ contains non-zero cusp forms for $k \geqslant 6$, and there are no simple formulae for the q-expansion coefficients of cusp forms. Indeed, as I shall explain, the coefficients of modular forms are related to *Galois representations*, and the Galois representations attached to cusp forms have non-abelian image, which means that the coefficients of cusp forms cannot be expressed with characters through class field theory. For instance, since $\Delta \in S_{12}\big(\mathrm{SL}_2(\mathbb{Z})\big)$ is a cusp form, there are no simple formulae for $\tau(n)$. These coefficients can however be efficiently computed one by one through the attached Galois representations, and this is the heart of this thesis. Eisenstein series, which I introduce below in section A.2.2.3, are the opposite case: in a sense which I will detail later, they form the orthogonal complement to cusp forms, and the Galois representations attached to them have abelian image, so that there are simple formulae in terms of characters for their q-expansion coefficients. For instance, the forms E_k are Eisenstein series, and so are the two forms making up the basis of $M_2\big(\Gamma_0(4)\big)$.

A.2.2.2 Hecke operators and newforms

Let Γ be either $\Gamma_1(N)$ or[11] $\Gamma_0(N)$ for some fixed level $N \in \mathbb{N}$, and also fix some even weight $k \in 2\mathbb{N}$. In view of the diamond and Hecke operators introduced in section A.2.1.2, one defines the operators $\langle \overline{d} \rangle$ and T_n on $M_k(\Gamma)$ for $n \in \mathbb{N}$ and $\overline{d} \in (\mathbb{Z}/N\mathbb{Z})^*$ by

$$\langle \overline{d} \rangle f = f|_k \gamma, \ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N), \ d \equiv \overline{d} \bmod N$$

and

$$T_n f = n^{k/2-1} \sum_{\substack{a,d \in \mathbb{N} \\ \gcd(a,N)=1 \\ ad=n \\ 0 \leqslant b < d}} (\langle a \rangle f)|_k \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \quad \big(\text{cf. (A.2.1.16)}\big),$$

where $f \in M_k(\Gamma)$. The coefficient n^{k-1} is included in the definition of T_n in order to avoid denominators; it shall soon be apparent that this is the "good" normalisation. The Fricke involution W_N is given by the matrix $w_N = \left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Q})^+$, that is to say

$$(W_N f)(\tau) = (f|_k w_N)(\tau) = \frac{1}{N^{k/2} \tau^k} f\left(\frac{-1}{N\tau}\right).$$

The fact that W_N is an involution is reflected in the fact that w_N^2 is a scalar matrix.

The Hecke operators T_n and the diamond operators $\langle d \rangle$ span a subalgebra

$$\mathbb{T}_{k,N} = \mathbb{Z}[T_n, \langle d \rangle \mid n \in \mathbb{N}, d \in (\mathbb{Z}/N\mathbb{Z})^*]$$

of $\mathrm{End}_{\mathbb{C}}\big(M_k(\Gamma)\big)$ called the *Hecke algebra* of weight k and level N, and denoted by $\mathbb{T}$ when the weight and level are clear from the context. In view of proposition A.2.1.17, $\mathbb{T}_{k,N}$ is commutative and is spanned by the T_n alone, which satisfy the relations

$$\begin{aligned} &T_{mn} = T_m T_n, \quad \gcd(m,n) = 1, \\ &T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}, \quad p \nmid N \text{ prime}, r \geqslant 2, \\ &U_{p^r} = U_p^r, \quad p | N \text{ prime}, r \geqslant 2. \end{aligned}$$

The diamond operators $\langle d \rangle$ are automorphisms of $M_k(\Gamma)$, and hence yield a representation

$$\rho \colon (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathrm{GL}\big(M_k(\Gamma)\big),$$

which is semi-simple since the characteristic of $\mathbb{C}$ is 0, and whose irreducible components are of dimension 1 over $\mathbb{C}$ since $(\mathbb{Z}/N\mathbb{Z})^*$ is abelian. In other words, one has a decomposition

[11] If $\Gamma = \Gamma_0(N)$, then the diamond operators $\langle d \rangle$ all reduce to the identity, and so all the discussion about them below is of course vacuous.

$$M_k\big(\Gamma_1(N)\big) = \bigoplus_{\varepsilon} M_k(N,\varepsilon),$$

$$M_k(N,\varepsilon) = \big\{ f \in M_k\big(\Gamma_1(N)\big) \mid \forall d \in (\mathbb{Z}/N\mathbb{Z})^*,\ \langle d\rangle f = \varepsilon(d) f \big\},$$

where the direct sum ranges over the Dirichlet characters $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$. One says that a form lying in $M_k(N,\varepsilon)$ has *nebentypus* (or *character*) ε. Note that when $\varepsilon = \mathbb{1}$ is the trivial character, $M_k(N,\mathbb{1})$ is simply $M_k\big(\Gamma_0(N)\big)$.

Actually, since $\langle -1\rangle$ is the identity as noted in section A.2.1.2, the representation ρ factors into a representation of $(\mathbb{Z}/N\mathbb{Z})^*/\pm 1$, so $M_k(N,\varepsilon) = \{0\}$ if ε is odd ($\varepsilon(-1) = -1$) and only the terms $M_k(N,\varepsilon)$ with ε even ($\varepsilon(-1) = +1$) are left.

Remark A.2.2.14. In this thesis, I only deal with modular forms of even weight. However, one may also consider modular forms of odd weight; if k is odd, then one finds that $M_k(N,\varepsilon) = \{0\}$ when ε is even, so only terms with ε odd remain is the decomposition of $M_k\big(\Gamma_1(N)\big)$ by nebentypus.

Besides, it is clear from the definition of the Hecke operators that the Hecke algebra $\mathbb{T}_{k,N}$ stabilises the subspace $S_k(\Gamma)$ of cuspforms. The Hecke algebra may thus also be seen as a commutative subalgebra of $\mathrm{End}_{\mathbb{C}}\big(S_k(\Gamma)\big)$, which is also denoted $\mathbb{T}_{k,N}$, and one similarly has the decomposition

$$S_k\big(\Gamma_1(N)\big) = \bigoplus_{\varepsilon \text{ even}} S_k(N,\varepsilon).$$

Proposition A.2.2.15. *The Fricke involution W_N maps $M_k(N,\varepsilon)$ onto $M_k(N,\overline{\varepsilon})$ and $S_k(N,\varepsilon)$ onto $S_k(N,\overline{\varepsilon})$, where $\overline{\varepsilon} = \varepsilon^{-1}$ denotes the complex conjugate of the Dirichlet character ε.*

Proof. As W_N is an involution and hence a bijection, it is enough to show that $W_N M_k(N,\varepsilon) \subseteq M_k(N,\overline{\varepsilon})$ and that $W_N S_k(N,\varepsilon) \subseteq S_k(N,\overline{\varepsilon})$. For all $\gamma = \left[\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right] \in \Gamma_0(N)$, one has $w_N \gamma w_N^{-1} = \left[\begin{smallmatrix} d & -c \\ -bN & a \end{smallmatrix}\right]$, so w_N normalises $\Gamma_0(N)$ and $\Gamma_1(N)$, and so W_N stabilises $M_k\big(\Gamma_1(N)\big)$. Furthermore, conjugating by w_N exchanges the a and d entries of γ, so that W_N indeed maps $M_k(N,\varepsilon)$ to $M_k(N,\overline{\varepsilon})$. Besides, as w_N normalises $\Gamma_1(N)$, its action on $\mathcal{H}^\bullet$ induces a well-defined action on the cusps of $X_1(N)$, and consequently stabilises the cusps; therefore W_N stabilises $S_k\big(\Gamma_1(N)\big)$ and hence maps $S_k(N,\varepsilon)$ to $S_k(N,\overline{\varepsilon})$. □

The action of the Hecke operators T_n on the q-expansions can be made explicit:

Proposition A.2.2.16. *Let $f = \sum_{m=0}^{+\infty} a_m q^m \in M_k(N,\varepsilon)$. Then for all $n \in \mathbb{N}$,*

$$T_n f = \sum_{m=0}^{+\infty} \left(\sum_{0<d\mid \gcd(n,m)} d^{k-1}\varepsilon(d) a_{nm/d^2} \right) q^m,$$

with the usual convention that $\varepsilon(d) = 0$ if $\gcd(d,N) > 1$.

The action of W_N on q-expansions shall be made explicit a little later.

Proof. By definition,

$$\begin{aligned}
(T_n f)(\tau) &= n^{k/2-1} \sum_{\substack{u,v\in\mathbb{N}\\ \gcd(u,N)=1\\ uv=n\\ 0\leqslant w<v}} \varepsilon(u) n^{k/2} v^{-k} f\left(\frac{u\tau+w}{v}\right) \\
&= \frac{1}{n} \sum_{\substack{u,v\in\mathbb{N}\\ uv=n\\ 0\leqslant w<v}} u^k \varepsilon(u) f\left(\frac{u\tau+w}{v}\right) \\
&= \frac{1}{n} \sum_{\substack{u,v\in\mathbb{N}\\ uv=n\\ 0\leqslant w<v}} u^k \varepsilon(u) \sum_{m=0}^{+\infty} a_m e^{2\pi i m(u\tau+w)/v} \\
&= \sum_{\substack{u,v\in\mathbb{N}\\ uv=n}} \frac{u^k}{n} \varepsilon(u) \sum_{m=0}^{+\infty} a_m e^{2\pi i m u\tau/v} \sum_{w=0}^{v-1} e^{2\pi i m w/v} \\
&= \sum_{\substack{u,v\in\mathbb{N}\\ uv=n}} \frac{u^{k-1}}{v} \varepsilon(u) \frac{1}{n} \sum_{m=0}^{+\infty} a_m e^{2\pi i m u\tau/v} \mathbb{1}_{v|m} v \\
&\underset{m=m'v}{=} \sum_{\substack{u,v\in\mathbb{N}\\ uv=n}} u^{k-1} \varepsilon(u) \sum_{m'=0}^{+\infty} a_{m'v} q^{m'u} \\
&= \sum_{0<u|n} u^{k-1} \varepsilon(u) \sum_{m'=0}^{+\infty} a_{m'n/u} q^{m'u} \\
&\underset{m''=m'u}{=} \sum_{m''=0}^{+\infty} q^{m''} \sum_{\substack{0<u|n\\ u|m''}} u^{k-1} \varepsilon(u) a_{m''n/u^2}.
\end{aligned}$$

□

Example A.2.2.17. In particular, if $f = \sum_{n=1}^{+\infty} a_n q^n$ is a cuspform, one has

$$T_n f = a_n q + O(q^2).$$

In order to further study the properties of the Hecke algebra, one enriches the structure of the space $S_k(\Gamma)$ by endowing it with the *Petersson inner product*

$$\langle f_1, f_2 \rangle = \frac{1}{\mu\big(X(\Gamma)\big)} \iint_{X(\Gamma)} \overline{f_1(x+iy)} f_2(x+iy) y^k \mathrm{d}\mu(x,y).$$

Here, μ is the $\mathrm{GL}_2(\mathbb{R})^+$-invariant measure on $\mathcal{H}^\bullet$ defined by

$$\mathrm{d}\mu(x,y) = \frac{\mathrm{d}x\mathrm{d}y}{y^2},$$

and $\iint_{X(\Gamma)}$ means integration over the fundamental domain

$$\mathcal{F} = \bigcup_i \gamma_i \mathcal{F}_1$$

for Γ, where

$$\mathrm{PSL}_2(\mathbb{Z}) = \bigsqcup_i \mathrm{P}\Gamma\gamma_i, \quad \gamma_i \in \mathrm{SL}_2(\mathbb{Z}),$$

and $\mathcal{F}_1$ is the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ shown on figure A.2.1.7. Since the function $\tau \mapsto \overline{f_1(\tau)} f_2(\tau)(\operatorname{Im}\tau)^k$ is Γ-invariant as f_1 and f_2 are modular of weight k and level Γ, this integral does not depend on the choice of the γ_i, and can be computed as

$$\sum_i \iint_{\mathcal{F}_1} \overline{f_1(\gamma_i \cdot \tau)} f_2(\gamma_i \cdot \tau)(\operatorname{Im}\gamma_i \cdot \tau)^k \mathrm{d}\mu(\tau)$$

as μ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. It converges since the cuspforms f_1 and f_2 decay exponentially at the cusps. The normalisation factor $\frac{1}{\mu(X(\Gamma))}$ is introduced to ensure that the inner product of f_1 and f_2 remains the same when they are seen as modular forms of level $\Gamma' \subset \Gamma$.

Remark A.2.2.18. Actually, since a cuspform decays exponentially at a cusp and a modular form remains bounded, this integral would still converge if only one of f_1 and f_2 were a cuspform.

One computes (cf. [DS05, section 5.5]) that in $\mathrm{End}_{\mathbb{C}}\left(S_k(\Gamma)\right)$, the adjoint of the diamond operator $\langle d\rangle$ with respect to the Petersson inner product is $\langle d\rangle^{-1} = \langle d^{-1}\rangle$, and that the adjoint of T_p is $\langle p^{-1}\rangle T_p$ for $p \nmid N$. This means that the *anaemic Hecke algebra*

$$\mathbb{T}^0 = \mathbb{Z}[T_p, p \nmid N] = \mathbb{Z}[T_n, \langle d\rangle \mid \gcd(n, N) = 1, d \in (\mathbb{Z}/N\mathbb{Z})^*] \subset \mathbb{T}$$

is a commutative algebra of normal operators on $S_k(\Gamma)$. It follows that $S_k(\Gamma)$ admits a (generally **not** unique) basis made up of *eigenforms*, that is to say of cuspforms which are simultaneous eigenvectors for the anaemic Hecke algebra $\mathbb{T}^0$.

Remark A.2.2.19. Actually, one can show (cf. [DS05, exercise 5.5.1]) that for every Hecke operator $T \in \mathbb{T}_{k,n}$, the adjoint T^* of T is $W_N T W_N$. In particular, W_N is self-adjoint and unitary.

Let $f = \sum_{n=1}^{+\infty} a_n(f) q^n \in S_k(\Gamma)$. Then $T_n f = a_n(f) q + O(q^2)$ for all $n \in \mathbb{N}$ by example A.2.2.17, so if f is an eigenform for T_n such that $a_1(f) = 0$, then $a_n(f) = 0$. Therefore, a non-zero eigenform f for the full Hecke algebra $\mathbb{T}$ necessarily has $a_1(f) \neq 0$, so one may divide it by $a_1(f)$ to get an eigenform $q + \sum_{n \geqslant 2} a_n q^n$. Such an eigenform is called a *normalised* eigenform. Besides, if f is normalised, then the T_n-eigenvalue of f is $a_n(f)$, again by example A.2.2.17. In view of the relations satisfied by the T_n in $\mathbb{T} = \mathbb{T}_{k,N}$, one deduces that the coefficients of $f = q + \sum_{n \geqslant 2} a_n q^n$ satisfy the relations

$$\left.\begin{array}{l} a_{mn} = a_m a_n, \quad \gcd(m,n) = 1, \\ a_{p^r} = a_p a_{p^{r-1}} - p^{k-1}\varepsilon(p) a_{p^{r-2}}, \quad p \nmid N \text{ prime}, r \geqslant 2, \\ a_{p^r} = a_p^r, \quad p | N \text{ prime}, r \in \mathbb{N}, \end{array}\right\} \tag{A.2.2.20}$$

which can be summarised by writing that the *L-series*

$$L(f, s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s} \quad (s \in \mathbb{C}, \operatorname{Re} s \gg 0)$$

attached to f factors into an *Euler product*

$$L(f,s) = \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}\varepsilon(p)},$$

where ε is the nebentypus of f, which exists since f is an eigenform (note that one can prove that these converge for $\operatorname{Re} s \gg 0$, cf. for instance example A.3.3.5). Besides, it follows from remark A.2.3.10 below that there exists a number field K_f (that is to say, of **finite** degree over $\mathbb{Q}$) such that the coefficients a_n of f all lie in the ring of integers of K_f.

Eigenforms are thus very friendly, but unfortunately the space $S_k(\Gamma)$ need not have a basis of forms which are eigenforms for the full Hecke algebra $\mathbb{T}$, because the Hecke operators U_p need not be semi-simple for $p|N$.

Example A.2.2.21. Let $M \in \mathbb{N}$ be such that there exists a non-zero form $f = \sum_{n=1}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(M)\big)$ which is an eigenform for the full Hecke algebra $\mathbb{T}_{k,M}$ of level M (this exists, see below), and let $N = p^3 M$ where p is a prime which does not divide M. Since f is an eigenform, it has in particular a nebentypus ε, and there exists a scalar $\lambda \in \mathbb{C}$ such that $T_p^{(M)} f = \lambda f$, where $T_p^{(M)} \in \mathbb{T}_{k,M}$ denotes the Hecke operator T_p in level M. Besides, f can also be seen as a cuspform of level N, and more generally, the forms $f_i(\tau) = f(p^i\tau)$ lie in $S_k\big(\Gamma_1(N)\big)$ for $i = 0, \cdots, 3$ by remark A.2.2.4. Let $U_p^{(N)} \in \mathbb{T}_{k,N}$ denote the Hecke operator U_p in level N. On the one hand, since f is an eigenform for the full Hecke algebra $\mathbb{T}_{k,M}$ of level M, the forms f_i are eigenvectors for the operators $T_q^{(M)} = T_q^{(N)}$, $q \nmid M$ prime, $q \neq p$ and $U_q^{(M)} = U_q^{(N)}$, $q|M$ prime, with the same eigenvalues as f. On the other hand, the actions of $T_p^{(M)}$ and $U_p^{(N)}$ on q-expansions are

$$T_p^{(M)} \sum_{n=1}^{+\infty} a_n q^n = \sum_{n=1}^{+\infty} a_{pn} q^n + p^{k-1}\varepsilon(p) \sum_{n=1}^{+\infty} a_n q^{pn}$$

and

$$U_p^{(N)} \sum_{n=1}^{+\infty} a_n q^n = \sum_{n=1}^{+\infty} a_{pn} q^n$$

according to proposition A.2.2.16, so that $U_p^{(N)} f_i = f_{i-1}$ for $i = 1, \cdots, 3$, and $U_p^{(N)} f_0 = \lambda f_0 - p^{k-1}\varepsilon(p) f_1$. Therefore, the subspace $V = \bigoplus_{i=0}^{3} \mathbb{C} f_i$ of $S_k\big(\Gamma_1(N)\big)$ is stable under $U_p^{(N)}$, and the matrix of $U_p^{(N)}$ acting on it is

$$\begin{bmatrix} \lambda & 1 & 0 & 0 \\ -p^{k-1}\varepsilon(p) & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which is not semi-simple. It follows that V is stable under the full Hecke algebra $\mathbb{T}_{k,N}$, and that the action of this algebra on it is not semi-simple. In particular, $S_k\big(\Gamma_1(N)\big)$ cannot have a base of cuspforms which are eigenforms for the full Hecke algebra $\mathbb{T}_{k,N}$.

In order to avoid this unpleasant phenomenon, one makes the following definitions:

Definition A.2.2.22. Fix a weight $k \in \mathbb{N}$ and a level $N \in \mathbb{N}$. The *old subspace* of $S_k\big(\Gamma_1(N)\big)$ is the subspace $S_k\big(\Gamma_1(N)\big)^{\text{old}}$ spanned by the cuspforms $f(t\tau)$ for $f \in S_k\big(\Gamma_1(M)\big)$, $M|N$ and $t|\frac{N}{M}$. The *new subspace* $S_k\big(\Gamma_1(N)\big)^{\text{new}}$ is the orthogonal of $S_k\big(\Gamma_1(N)\big)^{\text{old}}$ with respect to the Petersson inner product.

One makes of course the same definition with Γ_0 instead of Γ_1. In what follows, I shall consider Γ_1, but all the results also stand for Γ_0.

Example A.2.2.23. If N is prime and $k < 12$, then $S_2\big(\Gamma_1(N)\big)^{\text{old}} = \{0\}$ since $S_k(1) = \{0\}$ by example A.2.2.12, and so $S_2\big(\Gamma_1(N)\big)^{\text{new}}$ is the whole of $S_2\big(\Gamma_1(N)\big)$.

Example A.2.2.24. The space $S_2\big(\Gamma_0(11)\big)$ has dimension 1, and is spanned by $f_{11} = q - 2q^2 - q^3 + O(q^4)$, which is thus a new form of level 11. One finds that the space $S_2\big(\Gamma_0(22)\big)$ is of dimension 2, so it is spanned by $f_{11}(\tau)$ and $f_{11}(2\tau)$; in particular $S_2\big(\Gamma_0(22)\big)^{\text{old}}$ is the whole of $S_2\big(\Gamma_0(22)\big)$, and so $S_2\big(\Gamma_0(22)\big)^{\text{new}} = \{0\}$.

One also finds that $S_2\big(\Gamma_0(33)\big)$ is of dimension 3; since $S_2\big(\Gamma_0(3)\big) = \{0\}$, it follows that $S_2\big(\Gamma_0(33)\big)^{\text{old}} = \langle f_{11}(\tau), f_{11}(3\tau)\rangle$ has dimension 2, and so the dimension of $S_2\big(\Gamma_0(33)\big)^{\text{new}}$ is 1.

The decomposition $S_k\big(\Gamma_1(N)\big) = S_k\big(\Gamma_1(N)\big)^{\text{old}} \overset{\perp}{\oplus} S_k\big(\Gamma_1(N)\big)^{\text{new}}$ is actually more than an orthogonal decomposition:

Proposition A.2.2.25. *The old subspace and the new subspace of $S_k\big(\Gamma_1(N)\big)$ are both stable under the full Hecke algebra $\mathbb{T}$, so that*

$$S_k\big(\Gamma_1(N)\big) = S_k\big(\Gamma_1(N)\big)^{\text{old}} \oplus S_k\big(\Gamma_1(N)\big)^{\text{new}}$$

is actually a $\mathbb{T}$-module decomposition.

Proof. Cf. [DS05, proposition 5.6.2]. The idea is to first prove that $S_k\big(\Gamma_1(N)\big)^{\text{old}}$ is stable under $\mathbb{T}$ by examining carefully the difference between T_p on level N/p and U_p in level N as in example A.2.2.21 for $p\|N$ prime, and then to deduce that $S_k\big(\Gamma_1(N)\big)^{\text{new}}$ is stable under $\mathbb{T}$ by using the formulae for the adjoints of the Hecke operators. □

The interest of the new subspace is that it always admits a basis of eigenforms, as implied by the following theorem:

Theorem A.2.2.26. *Let $f \in S_k\big(\Gamma_1(N)\big)^{\text{new}}$ be an eigenform for the anaemic Hecke algebra $\mathbb{T}^0$. Then f is also an eigenform for the full Hecke algebra T.*

This leads to the following definition:

Definition A.2.2.27. A *newform* in $S_k\big(\Gamma_1(N)\big)$ is a cuspform $f \in S_k\big(\Gamma_1(N)\big)$ lying in the new subspace and which is a normalised eigenform.

One can show (cf. [DS05, theorem 5.8.3]) that one has the decomposition

$$S_k\big(\Gamma_1(N)\big) = \bigoplus_{0<M|N} \bigoplus_{0<t|\frac{N}{M}} \bigoplus_{\substack{f\in S_k(\Gamma_1(M))\\ \text{newform}}} \mathbb{C}f(t\tau), \tag{A.2.2.28}$$

and similarly for $S_k\big(\Gamma_0(N)\big)$ and $S_k\big(N,\varepsilon\big)$.

As a consequence, remark A.2.3.10 shows that there exists a number field $K_{k,N}$ such that the space $S_k\big(\Gamma_1(N)\big)$ admits a basis made up of cuspforms whose coefficients a_n all lie in the ring of integers of $K_{k,N}$.

Remark A.2.2.29. In the next section, I shall prove by explicit q-expansion computations (cf. corollary A.2.2.41) that this fact still holds on the whole space of modular forms $M_k\big(\Gamma_1(N)\big)$.

One can use Hilbert's theorem 90 (cf. [Ser62, proposition X.1.2]) to deduce from this that there exists a free $\mathbb{Z}$-submodule $S_k(\Gamma_1(N),\mathbb{Z}\big)$ of the power series ring $\mathbb{Z}[[q]]$ such that

$$S_k\big(\Gamma_1(N)\big) = S_k\big(\Gamma_1(N),\mathbb{Z}\big) \underset{\mathbb{Z}}{\otimes} \mathbb{C}.$$

In other words, $S_k\big(\Gamma_1(N)\big)$ admits an "integral structure". This allows to see $S_k\big(\Gamma_1(N),\mathbb{Z}\big)$ and the Hecke algebra $\mathbb{T}_{k,N}$ as the $\mathbb{Z}$-dual of each other:

Lemma A.2.2.30. *For each $n\in\mathbb{N}$, let a_n denote the linear form $\sum_{m\geqslant 1} a_m q^m \mapsto a_n$ on $S_k\big(\Gamma_1(N)\big)$. Then the pairing*

$$\begin{array}{rcl} \mathbb{T}_{k,N} \underset{\mathbb{Z}}{\otimes} S_k\big(\Gamma_1(N),\mathbb{Z}\big) & \longrightarrow & \mathbb{Z} \\ T\otimes f & \longmapsto & a_1(Tf) \end{array}$$

is perfect.

Proof. If $T\in\mathbb{T}_{k,N}$ is in the left kernel of this pairing, then as the Hecke algebra is commutative, one has

$$0 = a_1(TT_nf) = a_1(T_nTf) = a_n(Tf)$$

for all $f\in S_k\big(\Gamma_1(N)\big)$ and $n\in\mathbb{N}$, where the last equality comes from example A.2.2.17, so that $Tf=0$ for all f, which means that $T=0$ as an operator.

Similarly, if $f\in S_k\big(\Gamma_1(N)\big)$ is on the right kernel of this pairing, then

$$0 = a_1(T_nf) = a_n(f)$$

for all $n\in\mathbb{N}$, so that $f=0$. □

In [Stu87], J. Sturm proved a useful result concerning the congruence properties of the coefficients a_n:

Theorem A.2.2.31 (Sturm bound)**.** *Let $f=\sum_{n=0}^{+\infty} a_nq^n \in M_k\big(\Gamma_1(N)\big)$ be a modular forms whose coefficients a_n lie in the ring of integers $\mathbb{Z}_K$ of a number field K, and let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_K$. If $a_n\equiv 0 \bmod \mathfrak{a}$ for all $n\leqslant \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}):\Gamma_1(N)] = \frac{k}{12}N^2\prod_{p|N}\left(1-\frac{1}{p^2}\right)$, then $a_n\equiv 0 \bmod \mathfrak{a}$ for all n.*

This leads to a bound on the number of Hecke operators T_n required to span $\mathbb{T}_{k,N}$:

Proposition A.2.2.32. *The Hecke operators T_n, $n \leqslant \frac{k}{12}N^2\prod_{p|N}\left(1-\frac{1}{p^2}\right)$, span the image of the Hecke algebra $\mathbb{T}_{k,N}$ in $\mathrm{End}_{\mathbb{C}}\left(S_k(\Gamma_1(N))\right)$ as a $\mathbb{Z}$-module.*

Proof. Let $p \in \mathbb{N}$ be a prime number. The above Sturm bound shows that the Hecke operators T_n, $n \leqslant \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}):\Gamma]$, span the space $\mathrm{Hom}_{\mathbb{Z}}\left(S_k(\Gamma_1(N)),\mathbb{Z}\right) \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$, hence span $\mathbb{T}_{N,k} \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$ by lemma A.2.2.30. Since p is arbitrary, the result follows. □

The action of the Fricke involution on the q-expansion of a newform can be made explicit if the level N is squarefree (cf. [Asa76, theorem 2]). In particular, in the case where N is prime (which will be of interest for me later), one has the following formula:

Theorem A.2.2.33. *Let $f = q + \sum_{n\geqslant 2} a_n q^n \in S_k(N,\varepsilon)$ be a newform of weight k, level N and nebentypus ε. If N is prime, then $W_N f$ is the cuspform of weight k, level N and character $\overline{\varepsilon}$ defined by*

$$W_N f = \lambda_N(f)\left(q + \sum_{n\geqslant 2}\overline{a_n}q^n\right),$$

where $\lambda_N(f) \in \overline{\mathbb{Q}}$ is the pseudo-eigenvalue *of f, which is given by*

$$\lambda_N(f) = \begin{cases} -N^{1-k/2}\overline{a_N} & \text{if } \varepsilon \text{ is trivial,} \\ N^{-k/2}g(\varepsilon)\overline{a_N} & \text{if } \varepsilon \text{ is non-trivial.} \end{cases}$$

Besides, $\lambda_N(f) \neq 0$, and $\frac{1}{\lambda_N(f)}f = q + \sum_{n\geqslant 2}\overline{a_n}q^n$ is also a newform.

I also state a formula giving the action of the Fricke involution on a twisted newform, since I shall need it later. Recall (cf. [AL78, proposition 3.1]) that if $f = \sum_{n=1}^{+\infty} a_n q^n \in S_k(N,\varepsilon)$ is a cuspform of weight k, level N and nebentypus ε and $\chi\colon (\mathbb{Z}/M\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ is a Dirichlet character modulo M, then the *twisted form*

$$f \otimes \chi \overset{\text{def}}{=} \sum_{n=1}^{+\infty} a_n\chi(n)q^n \in S_k(M^2N,\chi^2\varepsilon)$$

is a cuspform of weight k, level M^2N and nebentypus $\chi^2\varepsilon$. The following result may be found in [AL78, p. 228]:

Theorem A.2.2.34. *Let $f \in S_k(N,\varepsilon)$ be a newform of weight k, level N and nebentypus ε, and let χ be a Dirichlet character of conductor M prime to N. Then $f \otimes \chi \in S_k(M^2N,\chi^2\varepsilon)$ is a newform of weight k, level M^2N and nebentypus $\chi^2\varepsilon$, and*

$$W_{M^2N}(f\otimes\chi) = \frac{g(\chi)}{g(\overline{\chi})}\varepsilon(M)\chi(-N)\cdot(W_N f)\otimes\overline{\chi},$$

that is to say

$$W_{M^2N}\left(q + \sum_{n\geqslant 2}a_n\chi(n)q^n\right) = \frac{g(\chi)}{g(\overline{\chi})}\varepsilon(M)\chi(-N)\lambda_N(f)\left(q+\sum_{n\geqslant 2}\overline{a_n}\,\overline{\chi}(n)q^n\right),$$

where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character.

A.2.2.3 Eisenstein series

Although I defined the Petersson inner product on cuspforms, I noted in remark A.2.2.18 that it is still well-defined on couples of modular forms, provided that at least one of them is a cuspform. This makes the following definition possible:

Definition A.2.2.35. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, and let $k \in \mathbb{N}$ be even. The Eisenstein subspace $E_k(\Gamma)$ is the orthogonal subspace of $S_k(\Gamma)$ in $M_k(\Gamma)$.

The dimension formulae A.2.2.10 yield

$$\dim E_k(\Gamma) = \dim M_k(\Gamma) - \dim S_k(\Gamma) = \begin{cases} \varepsilon_\infty & \text{if } k \geqslant 4, \\ \varepsilon_\infty - 1 & \text{if } k = 2, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0. \end{cases}$$

Besides, the formulae $\langle d\rangle^* = \langle d^{-1}\rangle$, $T_p^* = \langle p^{-1}\rangle T_p$ giving the adjoints of the Hecke operators in the anaemic Hecke algebra $\mathbb{T}^0$ show that these operators preserve the Eisenstein subspace. In particular, for $\Gamma = \Gamma_1(N)$, the diamond operators $\langle d\rangle$ split $E_k(N) = E_k\big(\Gamma_1(N)\big)$ into a $\mathbb{T}^0$-direct sum $E_k(N) = \bigoplus_\chi E_k(N,\chi)$, and the orthogonal decomposition

$$M_k(N,\chi) = E_k(N,\chi) \overset{\perp}{\oplus} S_k(N,\chi)$$

is also a $\mathbb{T}^0$-module decomposition.

Because of the different convergence behaviour of the series of weight $k = 2$, I shall study the Eisenstein subspace in weight $k \geqslant 4$ and in weight $k = 2$ separately.

The case of weight $k \geqslant 4$

Let $v \in (\mathbb{Z}/N\mathbb{Z})^2$ be a line-vector of order exactly N. Consider, for $k \geqslant 4$, the locally normally convergent series

$$G_k^v(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\equiv v \bmod N}} \frac{1}{(c\tau+d)^k}.$$

Rewriting G_k^v as

$$G_k^v(\tau) = \frac{1}{N^k} \sum_{c,d\in\mathbb{Z}} \frac{1}{\left(\frac{c_v\tau+d_v}{N} + c\tau + d\right)^k}$$

where c_v and d_v are lifts to $\mathbb{Z}$ of the coordinates of v, one can interpret $G_k^v(\tau)$ as being, up to the multiplicative constant N^k, the evaluation of the elliptic function

$$\wp_{k,\tau}(z) = \sum_{\omega\in\mathbb{Z}\tau+\mathbb{Z}} \frac{1}{(z+\omega)^k}$$

at the N-torsion point $z = \frac{c_v\tau+d_v}{N}$. In the case of level $N = 1$, there is only one possible choice of v, and one recovers the series $G_k \in M_k(1)$ defined in example A.2.2.3.

I have shown that this series G_k can be normalised as

$$G_k(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2\\(c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^k} = \sum_{n=1}^{+\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2\\ \gcd(c,d)=n}} \frac{1}{(c\tau+d)^k} = 2\zeta(k)E_k,$$

$$E_k(\tau) = \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2\\ \gcd(c,d)=1}} \frac{1}{(c\tau+d)^k},$$

the factor $1/2$ ensuring that E_k evaluates to 1 at the cusp ∞ owing to the symmetry in $\pm(c,d)$. Define similarly

$$E_k^v(\tau) = \epsilon_N \sum_{\substack{(c,d)\equiv v \bmod N\\ \gcd(c,d)=1}} \frac{1}{(c\tau+d)^k},$$

where $\epsilon_N = \frac{1}{2}$ for $N = 1$ or 2 and $\epsilon_N = 1$ for $N > 2$. One then has

$$G_k^v = \sum_{\substack{n\geqslant 1\\ \gcd(n,N)=1}} \frac{1}{n^k} \sum_{\substack{(c,d)\equiv v \bmod N\\ \gcd(c,d)=n}} \frac{1}{(c\tau+d)^k} = \frac{1}{\epsilon_N} \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^*} \left(\sum_{\substack{m\geqslant 1\\ m\equiv n \bmod N}} \frac{1}{m^k} \right) E_k^{n^{-1}v},$$

and conversely

$$E_k^v = \epsilon_N \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^*} \left(\sum_{\substack{m\geqslant 1\\ m\equiv n \bmod N}} \frac{\mu(m)}{m^k} \right) G_k^{n^{-1}v}$$

by Möbius inversion, so that the E_k^v span the same subspace of $M_k\big(\Gamma(N)\big)$ as the G_k^v, which will turn out to be exactly the Eisenstein subspace $E_k\big(\Gamma(N)\big)$.

It is immediately checked that

$$\lim_{\operatorname{Im}\tau\to+\infty} E_k^v(\tau) = \begin{cases} 1, & \text{if } v = \pm(0,1)\\ 0, & \text{else,} \end{cases}$$

and that

$$E_k^v|_k\gamma = E_k^{v\gamma}$$

for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, γ being understood to act on the right on v seen as a line-vector. Consequently, for all $v = (\overline{c}_v, \overline{d}_v) \in (\mathbb{Z}/N\mathbb{Z})^2$, $E_k^v \in M_k\big(\Gamma(N)\big) - S_k\big(\Gamma(N)\big)$ is a modular form which evaluates to 1 at the cusp $\Gamma(N)(-d_v/c_v)$ but vanishes at all of the other cusps of $X(N)$.

Proposition A.2.2.36. *The G_k^v and the $E_k^v \in E_k\big(\Gamma(N)\big)$ lie in the Eisenstein subspace of $M_k\big(\Gamma(N)\big)$.*

Proof. One must show that

$$\langle E_k^v, f\rangle = 0$$

for all cuspforms $f \in S_k\big(\Gamma(N)\big)$. Now if f is a cuspform, one has $a_0(f) = 0$ whence

$$\forall y > 0, \quad \int_0^N f(x+iy)\mathrm{d}x = 0$$

and so

$$0 = \int_0^{+\infty} y^{k-2}\mathrm{d}y \int_0^N f(x+iy)\mathrm{d}x = \iint_{\mathcal{D}_N} f(\tau)(\operatorname{Im}\tau)^k \mathrm{d}\mu(\tau),$$

where

$$\mathcal{D}_N = \{\tau \in \mathcal{H}^\bullet \mid \tau = \infty \text{ or } 0 \leqslant \operatorname{Re}\tau \leqslant N\}$$

is a fundamental domain for the action of the group $P_+(N)$ made up of the matrices $\left[\begin{smallmatrix} 1 & nN \\ 0 & 1 \end{smallmatrix}\right]$, $n \in \mathbb{Z}$. Writing

$$\Gamma(N) = \bigsqcup_i P_+(N)\alpha_i \text{ and } \mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i'} \Gamma(N)\beta_{i'},$$

one has

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i,i'} P_+(N)\alpha_i\beta_{i'} \text{ and } \mathcal{D}_N = \bigsqcup_{i,i'}{}' \alpha_i\beta_{i'}\mathcal{F}_1,$$

where $\mathcal{F}_1$ is the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ depicted on figure A.1.2.7 and $\bigsqcup'$ means that the union is disjoint up to the boundaries, which have measure 0, so that

$$0 = \sum_{i,i'} \iint_{\mathcal{F}_1} f(\alpha_i\beta_{i'}\cdot\tau)(\operatorname{Im}\alpha_i\beta_{i'}\cdot\tau)^k \mathrm{d}\mu(\tau) = \sum_{i,i'} \iint_{\mathcal{F}_1} f(\beta_{i'}\cdot\tau)(\operatorname{Im}\beta_{i'}\cdot\tau)^k \overline{1/j(\alpha_i,\tau)}\mathrm{d}\mu(\tau)$$

since $\operatorname{Im}\gamma\cdot\tau = \frac{\operatorname{Im}\tau}{|j(\gamma,\tau)|}$, $j(\gamma,\tau) = c\tau+d$, $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, and $f(\gamma\cdot\tau) = f(\tau)j(\gamma,\tau)^k$ for $\gamma \in \Gamma(N)$ by modularity of f. Now,

$$\sum_{i'} \iint_{\mathcal{F}_1} \phi(\beta_{i'}\cdot\tau)\mathrm{d}\mu(\tau) = \iint_{X(N)} \phi(\tau)\mathrm{d}\mu(\tau)$$

by definition, and

$$\sum_i \frac{1}{j(\alpha_i,\tau)} = \frac{1}{\epsilon_N} E_k^{v_0}(\tau)$$

for $v_0 = (0,1) \in (\mathbb{Z}/N\mathbb{Z})^2$, so this proves that $\langle E_k^{v_0}, f\rangle = 0$. One concludes by writing any $v \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N as $v_0\cdot\gamma$ for some $\gamma = \mathrm{SL}_2(\mathbb{Z})$ and by computing that

$$\langle E_k^v, f\rangle = \langle E_k^{v_0}|_k\gamma, f\rangle = \langle E_k^{v_0}, f|_k\gamma^{-1}\rangle = 0$$

as $f|_k\gamma^{-1}$ is a cuspform of level $\gamma\Gamma(N)\gamma^{-1} = \Gamma(N)$ since $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$. □

One may construct Eisenstein series in $E_k(N,\chi)$ by symmetrising over the E_k^v. Let ψ and φ be two Dirichlet characters with respective conductors u and v such that $uv = N$, and define

$$G_k^{\psi,\varphi} = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1} \psi(r)\overline{\varphi}(s) G_k^{(rv,s+tv)}.$$

It is straightforward to check that $G_k^{\psi,\varphi} \in E_k(N, \psi\varphi)$. In particular, $G_k^{\psi,\varphi}$ vanishes identically if $\psi\varphi$ is odd, so I shall assume that $\psi\varphi$ is even from now on.

I shall now compute the q-expansion of $G_k^{\psi,\varphi}$. To begin with, it is natural to determine what the q-expansion of the G_k^v's is made up of. To clarify notations, define

$$C_k = \frac{(-2\pi i)^k}{(k-1)!}.$$

I start with the following classical formula (cf. [Ser70, formula (32) p. 150]:

Lemma A.2.2.37.

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau+d)^k} = C_k \sum_{m=1}^{+\infty} m^{k-1} q^m \quad (\tau \in \mathcal{H}).$$

Using this, I may compute the q-expansion of G_k^v :

Proposition A.2.2.38. *Let $v = (\overline{c_v}, \overline{d_v})$ be of order exactly N in $(\mathbb{Z}/N\mathbb{Z})^2$. Then*

$$\begin{aligned} G_k^v(\tau) &= \mathbb{1}_{\overline{c_v}=\overline{0}} \sum_{d\equiv d_v \bmod N} \frac{1}{d^k} + \frac{C_k}{N^k} \sum_{n=1}^{+\infty} \left(\sum_{\substack{m|n \\ n/m\equiv c_v \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m} \right) q_N^n \\ &= \mathbb{1}_{\overline{c_v}=\overline{0}} \sum_{d\equiv d_v \bmod N} \frac{1}{d^k} + \frac{C_k}{N^k} \sum_{\substack{mn>0 \\ n\equiv c_v \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m} q_N^{mn}. \end{aligned}$$

Here and in what follows, the symbol $\mathbb{1}_C$ means 1 if the condition C is satisfied and 0 else. Observe that this is an expansion with respect to $q_N = \exp(2\pi i\tau/N)$ instead of the usual $q = q_1$, since the width of the cusp ∞ of $X(N)$ is N and not 1.

Proof. First observe that

$$G_k^v(\tau) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ (c,d)\equiv v \bmod N}} \frac{1}{(c\tau+d)^k} = \frac{1}{N^k} \sum_{c\equiv c_v \bmod N} \sum_{d\in\mathbb{Z}} \frac{1}{\left(\frac{c\tau+d_v}{N} + d\right)^k}.$$

I shall now treat separately the terms corresponding to $c = 0$ (if any), $c > 0$ and $c < 0$. First, for $c = 0$, one clearly gets

$$\mathbb{1}_{\overline{c_v}=\overline{0}} \sum_{d\equiv d_v \bmod N} \frac{1}{d^k}.$$

Next, for $c > 0$, one has

$$\frac{1}{N^k} \sum_{\substack{c>0 \\ c\equiv c_v \bmod N}} \sum_{d\in\mathbb{Z}} \frac{1}{\left(\frac{c\tau+d_v}{N} + d\right)^k} = \frac{C_k}{N^k} \sum_{\substack{c>0 \\ c\equiv c_v \bmod N}} \sum_{m=1}^{+\infty} m^{k-1} \mu_N^{d_v m} q_N^{cm}$$

$$\underset{n=cm}{=} \frac{C_k}{N^k} \sum_{n=1}^{+\infty} \left(\sum_{\substack{m>0 \\ m|n \\ \frac{n}{m} \equiv c_v \bmod N}} m^{k-1} \mu_N^{d_v m} \right) q_N^n,$$

And similarly, for $c < 0$, one has

$$\frac{1}{N^k} \sum_{\substack{c<0 \\ c \equiv c_v \bmod N}} \sum_{d \in \mathbb{Z}} \frac{1}{\left(\frac{c\tau + d_v}{N} + d\right)^k} = \frac{(-1)^k}{N^k} \sum_{\substack{c<0 \\ c \equiv c_v \bmod N}} \sum_{d \in \mathbb{Z}} \frac{1}{\left(\frac{-c\tau - d_v}{N} + d\right)^k}$$

$$= \frac{C_k}{N^k} \sum_{\substack{c<0 \\ c \equiv c_v \bmod N}} \sum_{m=1}^{+\infty} -(-1)^{k-1} m^{k-1} \mu_N^{-d_v m} q_N^{-cm}$$

$$\underset{\substack{n=-cm \\ m'=-m}}{=} \frac{C_k}{N^k} \sum_{n=1}^{+\infty} \left(\sum_{\substack{m'<0 \\ m'|n \\ \frac{n}{m'} \equiv c_v \bmod N}} -m'^{k-1} \mu_N^{d_v m'} \right) q_N^n.$$

Summing up[12],

$$G_k^v(\tau) = \mathbb{1}_{\overline{c_v} = \overline{0}} \sum_{d \equiv d_v \bmod N} \frac{1}{d^k} + \frac{C_k}{N^k} \sum_{n=1}^{+\infty} \left(\sum_{\substack{m|n \\ n/m \equiv c_v \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m} \right) q_N^n,$$

which I shall soon use under the slightly different form

$$= \mathbb{1}_{\overline{c_v} = \overline{0}} \sum_{d \equiv d_v \bmod N} \frac{1}{d^k} + \frac{C_k}{N^k} \sum_{\substack{mn>0 \\ n \equiv c_v \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m} q_N^{mn}.$$

□

I can now achieve the computation of the q-expansion of $G_k^{\psi,\varphi}$:

Theorem A.2.2.39. $G_k^{\psi,\varphi}(\tau) = \frac{C_k g(\overline{\varphi})}{v^k} E_k^{\psi,\varphi}(\tau)$,

$$E_k^{\psi,\varphi}(\tau) = \mathbb{1}_{\psi \text{ trivial}} L(1-k, \varphi) + 2 \sum_{n=1}^{+\infty} \left(\sum_{\substack{m>0 \\ m|n}} \psi(n/m) \varphi(m) m^{k-1} \right) q^n.$$

Here, $g(\chi)$ denotes the Gauss sum of a Dirichlet character χ, and $L(\chi, z)$ is the L-function attached to χ.

[12]pun intended.

Proof. Compute that

$$G_k^{\psi,\varphi}(\tau) = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)G_k^{rv,s+tv}(\tau)$$

$$= \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)\left(\mathbb{1}_{rv\equiv 0 \bmod N}\sum_{d\equiv s+tv \bmod N}\frac{1}{d^k} + \frac{C_k}{N^k}\sum_{\substack{mn>0\\ n\equiv rv \bmod N}}\operatorname{sgn}(m)m^{k-1}\mu_N^{(s+tv)m}q_N^{mn}\right)$$

$$\underset{n=n'v}{=} \psi(0)\sum_{s=0}^{v-1}\overline{\varphi}(s)\sum_{d\equiv s \bmod v}\frac{1}{d^k} + \frac{C_k}{N^k}\sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\psi(r)\overline{\varphi}(s)\sum_{\substack{mn'>0\\ n'\equiv r \bmod u}}\operatorname{sgn}(m)m^{k-1}\mu_N^{sm}q_u^{mn'}\underbrace{\sum_{t=0}^{u-1}\mu_u^{tm}}_{\mathbb{1}_{u|m}u}.$$

But when $u=1$, ψ is trivial and thus φ and hence $\overline{\varphi}$ are even, so that

$$\sum_{s=0}^{v-1}\overline{\varphi}(s)\sum_{d\equiv s \bmod v}\frac{1}{d^k} = 2L(k,\overline{\varphi}).$$

Consequently, setting also $m=m'u$, one gets

$$G_k^{\psi,\varphi}(\tau) = \mathbb{1}_{u=1}2L(k,\overline{\varphi}) + \frac{C_k}{N^k}\sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\psi(r)\overline{\varphi}(s)\sum_{\substack{m'n'>0\\ n'\equiv r \bmod u}}\operatorname{sgn}(m')m'^{k-1}u^{k-1}\mu_v^{sm'}q^{m'n'u}$$

$$= \mathbb{1}_{u=1}2L(k,\overline{\varphi}) + \frac{C_k}{v^k}\sum_{r=0}^{u-1}\psi(r)\sum_{\substack{m'n'>0\\ n'\equiv r \bmod u}}\operatorname{sgn}(m')m'^{k-1}q^{m'n'}\underbrace{\sum_{s=0}^{v-1}\overline{\varphi}(s)\mu_v^{sm'}}_{g(\overline{\varphi},m')=g(\overline{\varphi})\varphi(m')}$$

$$= \mathbb{1}_{u=1}2L(k,\overline{\varphi}) + \frac{C_k g(\overline{\varphi})}{v^k}\sum_{m'n'>0}\operatorname{sgn}(m')m'^{k-1}\varphi(m')\psi(n')q^{m'n'}$$

$$\underset{(\psi\varphi)(-1)=(-1)^k}{=} \mathbb{1}_{u=1}2L(k,\overline{\varphi}) + \frac{2C_k g(\overline{\varphi})}{v^k}\sum_{m',n'>0}m'^{k-1}\varphi(m')\psi(n')q^{m'n'}$$

$$\underset{n=m'n',m=m'}{=} \mathbb{1}_{u=1}2L(k,\overline{\varphi}) + \frac{2C_k g(\overline{\varphi})}{v^k}\sum_{n=1}^{+\infty}\sum_{m|n}m^{k-1}\varphi(m)\psi(n/m)q^n.$$

It now remains to factor $\frac{C_k g(\overline{\varphi})}{v^k}$ out of the constant term, so as to make $E_k^{\psi,\varphi}$ appear. For even φ, the functional equation (cf. [DS05, section 4.4]) of $L(z,\overline{\varphi})$ reads

$$\pi^{-z/2}\Gamma\left(\frac{z}{2}\right)v^z L(z,\overline{\varphi}) = \pi^{-(1-z)/2}\Gamma\left(\frac{1-z}{2}\right)g(\overline{\varphi})L(1-z,\varphi).$$

Setting $z=k$, one consequently gets that the constant term of $G_k^{\psi,\varphi}$, if any, is

$$\mathbb{1}_{u=1}2L(k,\overline{\varphi}) = \mathbb{1}_{u=1}\frac{2\pi^{k-1/2}\Gamma(\frac{1-k}{2})g(\overline{\varphi})L(1-k,\varphi)}{\Gamma(\frac{k}{2})v^k}.$$

In order to simplify out the Γ's, one first invokes *Euler's reflection formula*

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z},$$

which shows that

$$\Gamma\left(\frac{1-k}{2}\right)\Gamma\left(\frac{k+1}{2}\right) = \frac{\pi}{\sin \pi\frac{k+1}{2}} = \frac{\pi}{\cos \frac{k\pi}{2}},$$

and therefore

$$\frac{\Gamma(\frac{1-k}{2})}{\Gamma(\frac{k}{2})} = \frac{\pi}{\cos \frac{k\pi}{2}\Gamma(\frac{k}{2})\Gamma(\frac{k+1}{2})},$$

and then the *duplication formula*

$$\Gamma(z)\Gamma(z+1/2) = 2^{1-2z}\sqrt{\pi}\Gamma(2z),$$

which yields

$$\frac{\pi}{\cos \frac{k\pi}{2}\Gamma(\frac{k}{2})\Gamma(\frac{k+1}{2})} = \frac{2^{k-1}\sqrt{\pi}}{\cos \frac{k\pi}{2}\Gamma(k)}.$$

In the end, it appears that the constant term of $G_k^{\psi,\varphi}$ is

$$\mathbb{1}_{u=1}\frac{2\pi^{k-1/2}\Gamma(\frac{1-k}{2})g(\overline{\varphi})L(1-k,\varphi)}{\Gamma(\frac{k}{2})v^k} = \mathbb{1}_{u=1}\frac{2^{k-1}2\sqrt{\pi}\pi^{k-1/2}g(\overline{\varphi})L(1-k,\varphi)}{\cos\frac{k\pi}{2}\Gamma(k)v^k}$$

$$= \mathbb{1}_{u=1}\frac{2^k\pi^k g(\overline{\varphi})L(1-k,\varphi)}{(-1)^{k/2}(k-1)!v^k} = \mathbb{1}_{u=1}\frac{C_k g(\overline{\varphi})}{v^k}L(1-k,\varphi).$$

The proof is now complete. □

In order to make the term $L(1-k,\varphi)$ more explicit, introduce the twisted Bernoulli numbers $B_{k,\chi}$, defined by

$$\sum_{a=0}^{n-1}\chi(n)\frac{te^{at}}{e^{nt}-1} = \sum_{k=0}^{+\infty}B_{k,\chi}\frac{t^k}{k!}.$$

where χ is a Dirichlet character modulo n.

Proposition A.2.2.40. *(i) Let $B_k(X)$ denote the Bernoulli polynomials, defined by the generating function*

$$\frac{te^{tX}}{e^t-1} = \sum_{k=0}^{+\infty}B_k(X)\frac{t^k}{k!}.$$

Then the twisted Bernoulli numbers $B_{k,\chi}$ can be computed using the formula

$$B_{k,\chi} = n^{k-1}\sum_{a=0}^{n-1}\chi(a)B_k(a/n).$$

(ii) The values of the L-function attached to χ at non-positive integers is related to the twisted Bernoulli numbers by the formula

$$L(1-k,\chi) = -\frac{B_{k,\chi}}{k}.$$

For a proof, cf. [DS05, section 4.7].

Corollary A.2.2.41.

$$E_k^{\psi,\varphi}(\tau) = -\mathbb{1}_{\psi \text{ trivial}}\frac{B_{k,\varphi}}{k} + 2\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}\psi(n/m)\varphi(m)m^{k-1}\right)q^n.$$

For each pair of Dirichlet characters ψ and φ of respective conductors u and v, the Eisenstein series $E_k^{\psi,\varphi}(\tau)$ lies in $E_k(uv,\psi\varphi)$, so the series $E_k^{\psi,\varphi}(t\tau)$ lies in $E_k(N,\psi\varphi)$ for all $t \in \mathbb{N}$ such that $tuv|N$. One can show (cf. [DS05, theorem 4.5.2]) that the number of triplets (ψ,φ,t) such that $\psi\varphi$ is even and $t\mathfrak{f}_\psi\mathfrak{f}_\varphi|N$, where $\mathfrak{f}_\chi$ denotes the conductor of a character χ, agrees with the number of cusps of $X_1(N)$, which is the dimension of $E_k\big(\Gamma_1(N)\big)$ given by formula A.2.2.10, and that the corresponding series $E_k^{\psi,\varphi}(t\tau)$ form a basis of $E_k\big(\Gamma_1(N)\big)$. This can be summarised into the decomposition

$$E_k\big(\Gamma_1(N)\big) = \bigoplus_{\chi \text{ even}} E_k(N,\chi),$$

$$E_k(N,\chi) = \bigoplus_{\substack{\psi,\varphi\\ \psi\varphi=\chi}}\bigoplus_{t\mathfrak{f}_\psi\mathfrak{f}_\varphi|N}\mathbb{C}E_k^{\psi,\varphi}(t\tau) \qquad (\chi \text{ even}).$$

The case of weight $k = 2$

For $k = 2$, the above definition of the series G_k^v no longer makes sense due to convergence issues. However, this problem may be overcome by forming null-sum linear combinations of such series:

Proposition A.2.2.42. *Let (λ_v) be a family of complex numbers indexed by vectors of $(\mathbb{Z}/N\mathbb{Z})^2$ of order exactly N. If $\sum_v \lambda_v = 0$, it makes sense to define $\sum_v \lambda_v E_2^v$ as*

$$\sum_v \lambda_v E_2^v(\tau) = \frac{1}{N^2}\sum_{c,d\in\mathbb{Z}}\sum_v \frac{\lambda_v}{\left(\frac{c_v\tau+d_v}{N}+c\tau+d\right)^2},$$

where again c_v and d_v stand for lifts to $\mathbb{Z}$ of the coordinates of v. This is a locally normally convergent series of τ.

Proof. A Taylor expansion computation reveals that the fact that $\sum_v \lambda_v = 0$ kills the first term of the Taylor expansion of $\sum_v \frac{\lambda_v}{\left(\frac{c_v\tau+d_v}{N}+c\tau+d\right)^k}$ as $(c,d)\to\infty$. The order of magnitude of this first term was $\frac{1}{\|(c,d)\|^k}$, hence this sum becomes $O\left(\frac{1}{\|(c,d)\|^{k+1}}\right)$, ensuring local normal convergence of the double series even for $k = 2$. □

Remark A.2.2.43. For the same reason, one could even define Eisenstein series of weight $k = 1$ by also requiring that $\sum_v \lambda_v v = 0$, which results in killing the second term of the Taylor expansion of $\sum_v \frac{\lambda_v}{\left(\frac{c_v\tau+d_v}{N}+c\tau+d\right)^k}$. I shall however not need this fact, but I refer the reader to [DS05, section 4.8] for more comments on this question.

One shows just as in the higher weight case that the series $\sum_v \lambda_v E_2^v$ are modular of weight 2 and level $\Gamma(N)$ and that they are orthogonal to the cuspforms.

Say that a vector $v = (\overline{c}_v, \overline{d}_v) \in (\mathbb{Z}/N\mathbb{Z})^2$ represents the cusp $s = \Gamma(N)(-d_v/c_v)$ of $X(N)$, and let $v_1, \cdots, v_{\varepsilon_\infty}$ represent the ε_∞ cusps of $X(N)$. Then for each $0 \leqslant i < \varepsilon_\infty$, the series $E_2^{v_i} - E_2^{v_{\varepsilon_\infty}}$ evaluates to 1 on the cusp corresponding to v_i, to -1 on the cusp corresponding to v_{ε_∞}, and vanishes at the other cusps. These $\varepsilon_\infty - 1$ series are thus linearly independent, hence form a basis of $E_2\big(\Gamma(N)\big)$ since this space has dimension $\varepsilon_\infty - 1$ by the formulae A.2.2.10, and therefore

$$E_2\big(\Gamma(N)\big) = \left\{ \sum_v \lambda_v E_2^v \;\middle|\; \sum_v \lambda_v = 0 \right\}.$$

The series

$$G_2^{\psi,\varphi} = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1} \psi(r)\overline{\varphi}(s) G_2^{rv,s+tv}(\tau)$$

is well defined and lies in $E_2(N, \psi\varphi)$, unless ψ and φ are both trivial. The q-expansion computations carried out in the case $k \geqslant 4$ remain valid for these series, and since the second Bernoulli polynomial is $B_2(X) = X^2 - X + \frac{1}{6}$, one has

$$L(-1,\varphi) = -\frac{B_{2,\varphi}}{2} = -\frac{v}{2}\sum_{a=0}^{v-1}\varphi(a)\left(\left(\frac{a}{v}\right)^2 + \frac{a}{v} - \frac{1}{6}\right) = -\frac{1}{2}\sum_{a=0}^{v-1}\varphi(a)a\left(\frac{a}{v}+1\right)$$

if φ is non-trivial, so that

$$E_2^{\psi,\varphi}(\tau) = -\mathbb{1}_{\psi \text{ trivial}}\frac{1}{2}\sum_{a=0}^{v-1}\varphi(a)a\left(\frac{a}{v}+1\right) + 2\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}\psi(n/m)\varphi(m)m\right)q^n$$

since ψ and φ are forbidden to be both trivial.

Recall the series $E_2 = 1 - 24\sum_{n\geqslant 1}\sigma_1(n)q^n$. This series is not modular, but one can prove that $E_{2,N}(\tau) = E_2(\tau) - NE_2(N\tau)$ lies in $E_2\big(\Gamma_0(N)\big)$. For ψ and φ Dirichlet characters and $t \in \mathbb{N}$, define

$$E_2^{\psi,\varphi,t}(\tau) = \begin{cases} E_2^{\psi,\varphi}(t\tau) & \text{if } \psi \text{ and } \varphi \text{ are not both trivial,} \\ E_{2,t} & \text{if } \psi \text{ and } \varphi \text{ are both trivial.} \end{cases}$$

Then, as is the higher weight case, one has the decomposition

$$E_2\big(\Gamma_1(N)\big) = \bigoplus_{\chi \text{ even}} E_2(N,\chi),$$

$$E_2(N,\chi) = \bigoplus_{\substack{\psi,\varphi\\ \psi\varphi=\chi}} \bigoplus_{\substack{t\mathfrak{f}_\psi\mathfrak{f}_\varphi|N\\ (\psi,\varphi,t)\neq(\mathbb{1},\mathbb{1},1)}} \mathbb{C}E_2^{\psi,\varphi,t} \qquad (\chi \text{ even})$$

for χ even.

Note that the case ψ and φ both trivial and $t = 1$ is excluded, since $E_2^{\psi,\varphi,t} = 0$ then. This translates the fact that

$$\dim E_2\big(\Gamma_1(N)\big) = \varepsilon_\infty - 1 = \dim E_k\big(\Gamma_1(N)\big) - 1 \qquad (k \geqslant 4).$$

No matter whether $k \geqslant 4$ or $k = 2$, the action of W_N on the Eisenstein series $E_k^{\psi,\phi}$ is given by the following formula:

Proposition A.2.2.44. *Let $k \in 2\mathbb{N}$, and let ψ and φ be Dirichlet characters modulo respectively u and v, such that $uv = N$. Then*

$$W_N E_k^{\psi,\phi} = \frac{g(\psi)}{g(\overline{\varphi})}\left(\frac{v}{u}\right)^{k/2}\psi(-1)E_k^{\overline{\phi},\overline{\psi}}.$$

Proof. It is easier to work with the $G_k^{\psi,\varphi}$. First compute that

$$G_k^{\psi,\varphi}(\tau) = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)G_k^{(rv,s+tv)}(\tau) = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\sum_{\substack{(c',d)\in\mathbb{Z}^2\\ c'\equiv rv \bmod N\\ d\equiv s+tv \bmod N}}\frac{\psi(r)\overline{\varphi}(s)}{(c'\tau+d)^k}$$

$$\underset{c'=cv}{=}\sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\sum_{\substack{(c,d)\in\mathbb{Z}^2\\ c\equiv r \bmod u\\ d\equiv s+tv \bmod N}}\frac{\psi(r)\overline{\varphi}(s)}{(cv\tau+d)^k} = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\sum_{\substack{(c,d)\in\mathbb{Z}^2\\ c\equiv r \bmod u\\ d\equiv s+tv \bmod N}}\frac{\psi(c)\overline{\varphi}(d)}{(cv\tau+d)^k}$$

$$= \sum_{(c,d)\in\mathbb{Z}^2}\frac{\psi(c)\overline{\varphi}(d)}{(vc\tau+d)^k}.$$

Using this identity, I can compute $W_N G_k^{\psi,\varphi}$:

$$\begin{aligned}\big(W_N G_k^{\psi,\varphi}\big)(\tau) &= \frac{1}{N^{k/2}\tau^k}\sum_{(c,d)\in\mathbb{Z}^2}\frac{\psi(c)\overline{\varphi}(d)}{\left(\frac{-vc}{N\tau}+d\right)^k} = N^{k/2}\sum_{(c,d)\in\mathbb{Z}^2}\frac{\psi(c)\overline{\varphi}(d)}{(-vc+Nd\tau)^k}\\ &= \frac{N^{k/2}}{v^k}\sum_{(c,d)\in\mathbb{Z}^2}\frac{\overline{\varphi}(d)\psi(c)}{(ud\tau-c)^k} = \left(\frac{u}{v}\right)^{k/2}\sum_{(c',d')\in\mathbb{Z}^2}\frac{\overline{\varphi}(c')\psi(-d')}{(uc'\tau+d')^k}\\ &= \left(\frac{u}{v}\right)^{k/2}\psi(-1)\sum_{(c',d')\in\mathbb{Z}^2}\frac{\overline{\varphi}(c')\psi(d')}{(uc'\tau+d')^k} = \left(\frac{u}{v}\right)^{k/2}\psi(-1)G_k^{\overline{\varphi},\overline{\psi}}(\tau),\end{aligned}$$

whence the identity

$$W_N G_k^{\psi,\varphi} = \left(\frac{u}{v}\right)^{k/2}\psi(-1)G_k^{\overline{\varphi},\overline{\psi}}.$$

It then only remains to use on both sides the formula $G_k^{\psi,\varphi} = \frac{C_k g(\overline{\varphi})}{v^k}E_k^{\psi,\varphi}$ defining $E_k^{\psi,\varphi}$ to complete the proof. □

A.2.3 Modular symbols

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, and view the corresponding modular curve $X(\Gamma)$ as a Riemann surface. Modular symbols, which I shall now introduce, are an explicit realisation of the homology group $H_1\big(X(\Gamma),\mathbb{Z}\big)$ as a Hecke-module. This is very useful, since this explicitness can be spread by duality to spaces of modular forms, which allows to compute these spaces, that is to say, given $B \in \mathbb{N}$, to compute the q-expansion to precision $O(q^B)$ of the elements of a basis of $S_2(\Gamma)$. As an illustration, I shall compute the space $S_2\big(\Gamma_0(11)\big)$ in example A.2.3.12. Note that the ideas presented here can be generalised to higher weights $k \in 2\mathbb{N}$ without much difficulty (cf. [Ste07, chapter 8]), but I shall stick to $k = 2$ here for simplicity.

A.2.3.1 Computing with modular symbols

Let $\mathbb{M}_2$ be the group of *modular symbols*, that is to say the free abelian group on the set of couples $\{\alpha,\beta\}$ of cusps $\alpha,\ \beta \in \mathbb{P}^1\mathbb{Q}$ modulo the relation

$$\{\alpha,\beta\} + \{\beta,\gamma\} + \{\gamma,\alpha\} = 0$$

and modulo any torsion. The couple $\{\alpha,\beta\}$ is meant to be thought of as an oriented path joining α to β in $\mathcal{H}^\bullet$ and defined up to homotopy, as shown on figure A.2.3.1.

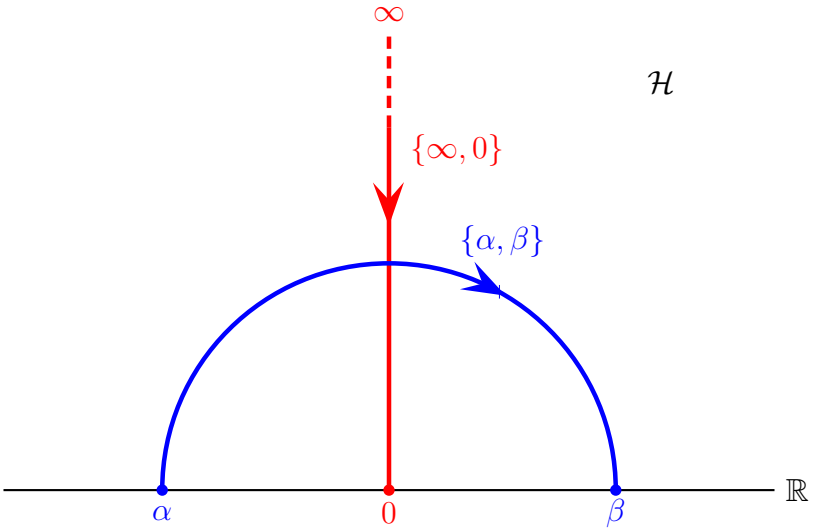


Figure A.2.3.1: Two modular symbols

Remark A.2.3.2. Beware that $\{\alpha,\beta\}$ really denotes the class of the **couple** (α,β) and not the set containing α and β, so that the order between α and β matters (modular symbols represent **oriented** paths). The notation $\{\alpha,\beta\}$ is deceptive, but it is standard.

One extends the action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathbb{P}^1\mathbb{Q}$ by defining

$$\gamma\cdot\{\alpha,\beta\} = \{\gamma\cdot\alpha,\gamma\cdot\beta\} \quad \big(\gamma \in \mathrm{SL}_2(\mathbb{Z}), \alpha,\beta \in \mathbb{P}^1\mathbb{Q}\big).$$

Lemma A.2.3.3. *The group $\mathbb{M}_2$ is generated by the elements $\gamma\cdot\{\infty,0\}$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. I shall actually prove that every modular symbol of the form $\{\alpha, 0\}$ is a sum of symbols of the form $\pm\gamma \cdot \{\infty, 0\}$, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This is enough since every modular symbol $\{\alpha, \beta\}$ can be written as $\{\alpha, 0\} - \{\beta, 0\}$.

If $\alpha = \infty$, then one can take $\gamma = 1$ and the proof is over, so assume that $\alpha \in \mathbb{Q}$. Let $\lfloor \alpha \rfloor = \frac{p_0}{q_0}, \frac{p_1}{q_1}, \cdots, \frac{p_n}{q_n} = \alpha$ be the convergents of the continued fraction expansion of α. Then the theory of continued fractions (cf. for instance [HW08, ch. X, theorem 150]) indicates that $p_{i+1}q_i - p_i q_{i+1} = (-1)^i$ for all $i < n$, and so

$$\begin{aligned} \{\alpha, 0\} &= \left\{\frac{p_n}{q_n}, \frac{p_{n-1}}{q_{n-1}}\right\} + \cdots \left\{\frac{p_1}{q_1}, \frac{p_0}{q_0}\right\} + \{\lfloor \alpha \rfloor, 0\} \\ &= \gamma_{n-1}\{\infty, 0\} + \cdots + \gamma_0\{\infty, 0\} + \gamma'\{\infty, 0\} + \{\infty, 0\}, \end{aligned}$$

where $\gamma_i = \left[\begin{smallmatrix} p_{i+1} & (-1)^i p_i \\ q_{i+1} & (-1)^i q_i \end{smallmatrix}\right]$ and $\gamma' = \left[\begin{smallmatrix} \lfloor \alpha \rfloor & -1 \\ 1 & 0 \end{smallmatrix}\right]$ lie in $\mathrm{SL}_2(\mathbb{Z})$. □

I now fix a level $N \in \mathbb{N}$, and a congruence subgroup $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$.

Definition A.2.3.4. The group $\mathbb{M}_2(\Gamma)$ of *modular symbols* of level Γ is the quotient of $\mathbb{M}_2$ by the action of Γ and modulo any resulting torsion.

Example A.2.3.5. As $\gamma = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma$, one has

$$\{0, 1\} = \{\infty, 1\} - \{\infty, 0\} = \gamma \cdot \{\infty, 0\} - \{\infty, 0\} = 0$$

in $\mathbb{M}_2(\Gamma)$.

One defines an action of the Hecke algebra $\mathbb{T} = \mathbb{T}_{2,N}$ of weight 2 and level N (cf. section A.2.1.2) on $\mathbb{M}_2(\Gamma)$ by the formulae

$$\langle \overline{d} \rangle \{\alpha, \beta\} = \gamma \cdot \{\alpha, \beta\}, \ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N), \ d \equiv \overline{d} \bmod N$$

and

$$T_n\{\alpha, \beta\} = \sum_{\substack{a,d \in \mathbb{N} \\ \gcd(a,N)=1 \\ ad=n \\ 0 \leqslant b < d}} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot \langle a \rangle \{\alpha, \beta\}. \tag{A.2.3.6}$$

By the identification of $S_2(\Gamma)$ with the space $\Omega^1\big(X(\Gamma)\big)$ of holomorphic differential 1-forms on $X(\Gamma)$, one gets an integration pairing

$$\begin{aligned} \mathbb{M}_2(\Gamma) \underset{\mathbb{Z}}{\otimes} S_2(\Gamma) &\longrightarrow \mathbb{C} \\ \{\alpha, \beta\} \otimes f &\longmapsto \big\langle \{\alpha, \beta\}, f \big\rangle = \int_\alpha^\beta f(\tau) \mathrm{d}\tau. \end{aligned} \tag{A.2.3.7}$$

Note that the integral converges since it corresponds to the integration of f, seen as a holomorphic differential 1-form on $X(\Gamma)$, along the projection on $X(\Gamma)$ of a path in $\mathcal{H}^\bullet$ joining α to β (cf. figure A.2.3.1). Furthermore, this pairing is well-defined, since the differential $f(\tau)\mathrm{d}\tau$ is Γ-invariant as $f \in S_2(\Gamma)$ and since $\mathcal{H}^\bullet$ is simply connected. Finally, and this is the key point, this paring is Hecke-equivariant, that is to say

$$\langle Ts, f \rangle = \langle s, Tf \rangle$$

for all $s \in \mathbb{M}_2(\Gamma)$, $f \in S_2(\Gamma)$ and $T \in \mathbb{T}$.

Fix a coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i \in I} \Gamma\gamma_i.$$

According to example A.2.1.3, if $\Gamma = \Gamma_1(N)$ one can take $I = A_N$, the set of vectors in $(\mathbb{Z}/N\mathbb{Z})^2$ of order exactly N, whereas if $\Gamma = \Gamma_0(N)$, one can take $I = \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Lemma A.2.3.3 shows that the group $\mathbb{M}_2(\Gamma)$ is spanned by the modular symbols $[i] = \gamma_i\{\infty, 0\}$, $i \in I$. The symbols $[i]$ are called the *Manin symbols* attached to the coset decomposition above.

One lets $\mathrm{SL}_2(\mathbb{Z})$ act on the **right** on the set of Manin symbols by the rule

$$[i] \cdot \gamma = [j] \quad \text{where } \Gamma\gamma_i\gamma = \Gamma\gamma_j.$$

Let $R = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$ and $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. Then one sees that for all $i \in I$,

$$[i] + [i] \cdot S = \gamma_i \cdot \{\infty, 0\} + \gamma_i S \cdot \{\infty, 0\} = \{\gamma_i \cdot \infty, \gamma_i \cdot 0\} + \{\gamma_i \cdot 0, \gamma_i \cdot \infty\} = 0,$$

and

$$[i] + [i] \cdot R + [i] \cdot R^2 = \{\gamma_i \cdot \infty, \gamma_i \cdot 0\} + \{\gamma_i \cdot 0, \gamma_i \cdot 1\} + \{\gamma_i \cdot 1, \gamma_i \cdot \infty\} = 0.$$

J. Manin proved in [Man72] that these are actually the "only" relations satisfied by the Manin symbols:

Theorem A.2.3.8 (Manin)**.** *The kernel of the natural surjective morphism*

$$\bigoplus_{i \in I} \mathbb{Z}[i] \longrightarrow \mathbb{M}_2(\Gamma)$$

is generated over $\mathbb{Z}$ by the elements $[i] + [i] \cdot S$ and $[i] + [i] \cdot R + [i] \cdot R^2$, $i \in I$.

The proof of this theorem requires some work, cf. [Man72, section 1.7].

From this, one can find a $\mathbb{Z}$-basis of $\mathbb{M}_2(\Gamma)$ (which exists as $\mathbb{Z}$ is principal) in terms on Manin symbols, by performing linear algebra over $\mathbb{Z}$ (cf. [Coh93, section 2.4.3]). The interest of this is that it makes effective computations in $\mathbb{M}_2(\Gamma)$ easy (cf. example A.2.3.12 below for a fully worked-out case).

In order to compute the matrix of a Hecke operator $T_n \in \mathbb{T}$ acting on $\mathbb{M}_2(\Gamma)$ with respect to this basis, it is natural to use formula (A.2.3.6) directly, and to convert the resulting terms into Manin symbols by the process explained in the proof of lemma A.2.3.3. One may, however, compute for each $n \in \mathbb{N}$ a finite set $H_n \subset \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ of matrices, called the *Heilbronn matrices*, such as the action of T_n on Manin symbols is given directly by

$$T_n[i] = \sum_{h \in H_n} [i] \cdot h,$$

which is a more efficient approach (cf. [Cre97, section 2.4] or [Ste07, sections 3.4.2 and 8.3.2] for details).

The modular symbols are meant to represent the homology $H_1\big(X(\Gamma), \mathbb{Z}\big)$ of $X(\Gamma)$, but $\{\alpha, \beta\}$ represents a path from α to β, which projects to a closed loop on $X(\Gamma)$ if and only if the cusps α and β are equivalent under Γ. This justifies the following definition:

Definition A.2.3.9. The subgroup $\mathbb{S}_2(\Gamma)$ of *cuspidal* modular symbols is the kernel of the *boundary morphism*

$$\begin{array}{rccc} \partial\colon & \mathbb{M}_2(\Gamma) & \longrightarrow & \mathbb{Z}[\Gamma\backslash\mathbb{P}^1\mathbb{Q}] \\ & \{\alpha,\beta\} & \longmapsto & \Gamma\beta-\Gamma\alpha, \end{array}$$

where $\mathbb{Z}[\Gamma\backslash\mathbb{P}^1\mathbb{Q}]$ denotes the free abelian group on the set $\Gamma\backslash\mathbb{P}^1\mathbb{Q}$ of cusps of $X(\Gamma)$.

It is clear that the Hecke algebra $\mathbb{T}$ stabilises $\mathbb{S}_2(\Gamma)$. One can prove (cf. [Man72, theorem 1.9]) that $\mathbb{S}_2(\Gamma)$ and $H_1\big(X(\Gamma),\mathbb{Z}\big)$ are isomorphic $\mathbb{T}$-modules as expected; in particular, the $\mathbb{Z}$-rank of $\mathbb{S}_2(\Gamma)$ is twice the genus g of $X(\Gamma)$.

Remark A.2.3.10. As mentioned in the beginning of this section, one can also define the group $\mathbb{S}_k(\Gamma)$ of modular symbols of higher weight $k \in 2\mathbb{N}$ (cf. [Ste07, chapter 8]), which is also free of finite $\mathbb{Z}$-rank and which comes with a natural dual action of the Hecke algebra of weight k. As a consequence, for each congruence subgroup Γ and for each weight $k \in 2\mathbb{N}$, there exists a number field $K_{k,\Gamma}$ such that for all Hecke operator $T \in \mathbb{T}_{k,\Gamma}$, the eigenvalues of T lie in the ring of integers of $K_{k,\Gamma}$.

In order to compute $\mathbb{S}_2(\Gamma)$, one needs a practical criterion for the Γ-equivalence of cusps. J. Cremona gave such a criterion:

Proposition A.2.3.11. *Let p/q and $p'/q' \in \mathbb{P}^1\mathbb{Q}$ be two cusps written in lowest terms (in particular, ∞ must be written $1/0$, and $q, q' \geqslant 0$ in any case), and let $N \in \mathbb{N}$.*

(i) These cusps are equivalent under $\Gamma_1(N)$ if and only if $q \equiv q' \bmod N$ and $p \equiv p' \bmod \gcd(q,N)$.

(ii) Let r, $r' \in \mathbb{Z}$ be such that $pr \equiv 1 \bmod q$ and $p'r' \equiv 1 \bmod q'$. Then these cusps are equivalent under $\Gamma_0(N)$ if and only if $qr' \equiv q'r \bmod \gcd(qq', N)$.

I refer the reader to [Cre92, lemma 3.2] for the proof of the $\Gamma_1(N)$ case, and to [Cre97, proposition 2.2.3] for the proof of the $\Gamma_0(N)$ case.

These criteria allow one to write down the matrix of the boundary morphism ∂ with respect to a basis of Manin symbols (computed by applying theorem A.2.3.8) of $\mathbb{M}_2(\Gamma)$ and to a set of representatives of $\Gamma\backslash\mathbb{P}^1\mathbb{Q}$. Note that in practice, one can construct this set along with the computation of ∂, by testing for equivalence the cusp which is handled with an initially empty list of pairwise inequivalent cusps. From there, one can compute a $\mathbb{Z}$-basis of $\mathbb{S}_2(\Gamma)$ by performing linear algebra over $\mathbb{Z}$, and deduce the genus of $X(\Gamma)$ as half the $\mathbb{Z}$-rank of $\mathbb{S}_2(\Gamma)$ (cf. example A.2.3.12 below).

In what follows, I shall denote by a_n the linear form on $S_2(\Gamma)$

$$\sum_{m=1}^{+\infty} a_m q^m \longmapsto a_n.,$$

and by $\mathbb{T}_C = \mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{C} \subset \mathrm{End}_{\mathbb{C}}\big(S_2(\Gamma)\big)$ denotes the Hecke algebra with scalars extended to $\mathbb{C}$. By lemma A.2.2.30, the pairing

$$\begin{array}{rcl} \mathbb{T}_{\mathbb{C}} \underset{\mathbb{C}}{\otimes} S_2(\Gamma) & \longrightarrow & \mathbb{C} \\ T \otimes f & \longmapsto & a_1(Tf) \end{array}$$

is perfect, so that the map

$$\begin{array}{rccl} \Psi\colon & \mathbb{S}_2(\Gamma) & \longrightarrow & \mathbb{T}_{\mathbb{C}}^{\vee} \\ & f & \longmapsto & \big(T \mapsto a_1(Tf)\big), \end{array}$$

where $\mathbb{T}_C^{\vee} = \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$ denotes the linear dual of $\mathbb{T}_{\mathbb{C}}$, is a $\mathbb{C}$-linear isomorphism. Furthermore, example A.2.2.17 shows that the image of a linear form $\varphi \in \mathbb{T}_{\mathbb{C}}^{\vee}$ by its inverse is

$$\Psi^{-1}(\varphi) = \sum_{n=1}^{+\infty} \varphi(T_n) q^n \in S_2(\Gamma).$$

Now, the computation of the matrices of the Hecke operators T_n acting on $\mathbb{S}_2(\Gamma)$ above yields an explicit embedding

$$M\colon \mathbb{T} \hookrightarrow \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}).$$

Let $a_{i,j}\colon \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}) \longrightarrow \mathbb{Z}$, $1 \leqslant i, j \leqslant 2g$, be the "$(i,j)$-matrix coefficient" linear form. By composing with M, one gets linear forms $a_{i,j} \circ M \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z})$ which span $\mathbb{T}_{\mathbb{C}}^{\vee}$ over $\mathbb{C}$, and so the forms

$$f_{i,j} = \sum_{n=1}^{+\infty} a_{i,j}\big(M(T_n)\big) q^n$$

form an explicit generating family of $S_2(\Gamma)$.

Example A.2.3.12. In order to illustrate all of this, I shall now compute a basis of $S_2\big(\Gamma_0(11)\big)$ to precision $O(q^4)$ explicitly.

By example A.2.1.3, one has the coset decomposition

$$\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{x \in \mathbb{P}^1\mathbb{F}_{11}} \Gamma_0(11)\gamma_x,$$

with $\gamma_x = \left[\begin{smallmatrix} 1 & 0 \\ \widetilde{x} & 1 \end{smallmatrix}\right]$ for $x \in \mathbb{F}_{11}$ and $\widetilde{x}$ the lift to $\mathbb{Z}$ between 0 and 10 of x, and $\gamma_\infty = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. One finds by looking at the bottom row of the matrices $\gamma_x R$ and $\gamma_x S$ that the matrices R and S act on the corresponding Manin symbols $[x]$ by

$$[x] \cdot S = [-1/x],$$

whence the relations

$$\begin{array}{lll} [0] + [\infty] = 0, & [1] + [10] = 0, & [2] + [5] = 0, \\ [3] + [7] = 0, & [4] + [8] = 0, & [6] + [9] = 0, \end{array}$$

and by

$$[x] \cdot R = \left[\frac{-1}{x+1}\right],$$

whence the relations

$$[0]+[10]+[\infty]=0, \qquad [2]+[7]+[4]=0,$$
$$[1]+[5]+[9]=0, \qquad [3]+[8]+[6]=0,$$

from which it follows that the Manin symbols $[0],[2],[4]$ form a $\mathbb{Z}$-basis of $\mathbb{M}_2\big(\Gamma_0(11)\big)$, the other Manin symbols being given by

$$\begin{array}{ccc} [1]=0, & [3]=[2]+[4], & [5]=-[2], \\ [6]=-[2], & [7]=-[2]-[4], & [8]=-[4], \\ [9]=[2], & [10]=0, & [\infty]=-[0]. \end{array}$$

Next, one has $[0]=\{\infty,0\}$, $[2]=\{1/2,0\}$ and $[4]=\{1/4,0\}$, and the cusps $1/2$ and $1/4$ are equivalent to 0 under $\Gamma_0(11)$ by the criterion A.2.3.11(ii) whereas ∞ is not equivalent to 0, so $\mathbb{S}_2\big(\Gamma_0(11)\big)$ is the subgroup of $\mathbb{M}_2\big(\Gamma_0(11)\big)$ generated by $[2]$ and $[4]$. In particular, its $\mathbb{Z}$-rank is 2, so the genus of $X_0(11)$ is $g=1$. It follows that the space $S_2\big(\Gamma_0(11)\big)$ is of dimension 1, so it is generated by a form f. By example A.2.2.23, one may suppose that f is a newform $f=q+O(q^2)$.

In order to compute the q-expansion of f, one must compute the matrices of the Hecke operators acting on $\mathbb{S}_2\big(\Gamma_0(11)\big)$, for instance with respect to the basis $([2],[4])$. I shall do it here by using formula (A.2.3.6) directly. One has $T_1=\mathrm{Id}$ by definition, so the matrix of T_1 is

$$T_2=\begin{bmatrix}1&0\\0&1\end{bmatrix}.$$

Next,

$$T_2[2]=T_2\left\{\frac12,0\right\}=\{1,0\}+\left\{\frac14,0\right\}+\left\{\frac34,\frac12\right\}$$

by formula (A.2.3.6)

$$=\left\{\frac14,0\right\}+\left\{\frac34,1\right\}-\left\{\frac12,0\right\}=[4]+\left[\begin{smallmatrix}3&-1\\4&-1\end{smallmatrix}\right]\cdot\{\infty,0\}-[2]$$

as $\{1,0\}=0$ by example A.2.3.5

$$=[4]+[(4:-1)]-[2]=[4]+[7]-[2]=[4]-[2]-[4]-[2]=-2[2],$$

and

$$\begin{aligned} T_2[4]&=T_2\left\{\frac14,0\right\}=\left\{\frac12,0\right\}+\left\{\frac18,0\right\}+\left\{\frac58,\frac12\right\}=\left\{\frac58,0\right\}+\left\{\frac18,0\right\}\\ &=\left\{\frac58,\frac23\right\}+\left\{\frac23,\frac12\right\}+\left\{\frac12,0\right\}+\left\{\frac18,0\right\}\end{aligned}$$

using the convergents 0, 1/2, 2/3, 5/8 of $\dfrac{5}{8}=0+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac12}}}$

$$\begin{aligned} &=\left[\begin{smallmatrix}5&-2\\8&-3\end{smallmatrix}\right]\cdot\{\infty,0\}+\left[\begin{smallmatrix}2&1\\3&2\end{smallmatrix}\right]\cdot\{\infty,0\}+[2]+[8]=[(8:-3)]+[(3:2)]+[2]+[8]\\ &=[1]+[7]+[2]+[8]=0-[2]-[4]+[2]-[4]=-2[4],\end{aligned}$$

so the matrix of T_2 acting on $\mathbb{S}_2\big(\Gamma_0(11)\big)$ is

$$T_2 = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}.$$

Similarly,

$$\begin{aligned} T_3[2] = T_3\left\{\frac{1}{2},0\right\} &= \left\{\frac{3}{2},0\right\} + \left\{\frac{1}{6},0\right\} + \left\{\frac{1}{2},\frac{1}{3}\right\} + \left\{\frac{5}{6},\frac{2}{3}\right\} \\ &= \left\{\frac{3}{2},1\right\} + \left\{\frac{1}{6},0\right\} + \left\{\frac{1}{2},0\right\} - \left\{\frac{1}{3},0\right\} + \left\{\frac{5}{6},1\right\} - \left\{\frac{2}{3},1\right\} \\ &= \left[\begin{smallmatrix} 3 & 1 \\ 2 & 1 \end{smallmatrix}\right] \cdot \{\infty,0\} + [6] + [2] - [3] + \left[\begin{smallmatrix} 5 & -1 \\ 6 & -1 \end{smallmatrix}\right] \cdot \{\infty,0\} - \left[\begin{smallmatrix} 2 & -1 \\ 3 & -1 \end{smallmatrix}\right] \cdot \{\infty,0\} \\ &= [(2:1)] + [6] + [2] - [3] + [(6:-1)] - [(3:-1)] \\ &= [2] + [6] + [2] - [3] + [5] - [8] = [2] - [2] + [2] - [2] - [4] - [2] + [4] = -[2], \end{aligned}$$

and

$$\begin{aligned} T_3[4] = T_3\left\{\frac{1}{4},0\right\} &= \left\{\frac{3}{4},0\right\} + \left\{\frac{1}{12},0\right\} + \left\{\frac{5}{12},\frac{1}{3}\right\} + \left\{\frac{3}{4},\frac{2}{3}\right\} \\ &= \left\{\frac{3}{4},1\right\} + \left\{\frac{1}{12},0\right\} + \left\{\frac{5}{12},\frac{2}{5}\right\} + \left\{\frac{2}{5},\frac{1}{2}\right\} + \left\{\frac{1}{2},0\right\} - \left\{\frac{1}{3},0\right\} + \left\{\frac{3}{4},\frac{2}{3}\right\} \end{aligned}$$

using the convergents 0, 1/2, 2/5, 5/12 of $\dfrac{5}{12} = 0 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}$

$$\begin{aligned} &= \left[\begin{smallmatrix} 3 & -1 \\ 4 & -1 \end{smallmatrix}\right] \cdot \{\infty,0\} + [12] + \left[\begin{smallmatrix} 5 & 2 \\ 12 & 5 \end{smallmatrix}\right] \cdot \{\infty,0\} + \left[\begin{smallmatrix} 2 & -1 \\ 5 & -2 \end{smallmatrix}\right] \cdot \{\infty,0\} + [2] - [3] + \left[\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right] \cdot \{\infty,0\} \\ &= [(4:-1)] + [12] + [(1:5)] + [(5:-2)] + [2] - [3] + [(4:3)] \\ &= [7] + [1] + [9] + [3] + [2] - [3] + [5] = -[2] - [4] + 0 + [2] + [2] - [2] = -[4], \end{aligned}$$

so the matrix of T_3 acting on $\mathbb{S}_2\big(\Gamma_0(11)\big)$ is

$$T_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The upper-left and lower-right matrix entries both give the form $q - 2q^2 - q^3 + O(q^4)$ whereas the upper-right and lower-left entries both give the 0 form, so finally one concludes that $S_2\big(\Gamma_0(11)\big)$ is generated by the newform

$$f = q - 2q^2 - q^3 + O(q^4).$$

Of course, one may push this computation further so as to get more coefficients of the q-expansion of f.

The interested reader may find examples of similar computations in [Ste07, chapters 3 and 8].

Remark A.2.3.13. One can show (cf. [Cre97, sections 2.1.3 and 2.5]) that the symmetry $\tau \mapsto -\overline{\tau}$ around the vertical axis $i\mathbb{R}$ of $\mathcal{H}^\bullet$ induces an involution on $\mathbb{S}_2(\Gamma)$, and that the corresponding eigenspaces $\mathbb{S}_2(\Gamma)^+$ and $\mathbb{S}_2(\Gamma)^-$ are isomorphic $\mathbb{T}$-modules, which explains why I obtained "twice" the same form in example A.2.3.12 just above. It is therefore possible to work in one of these eigenspaces so as to speed up the computation.

However, even with this trick and the use of Heilbronn matrices, the cost of the computation of the action of the Hecke operator T_p on $\mathbb{S}_2(\Gamma)$ for p prime is more than linear in p (cf. [Ste07, sections 8.3.3 and 8.3.4]), so the cost of the computation of a basis of $S_2(\Gamma)$ to precision $O(q^B)$ with this method is more than quadratic in B. I shall present a practical trick of mine to bring down this complexity to $\widetilde{O}(B)$ for fixed Γ in section B.3.1. Moreover, the goal of this thesis is to describe an algorithm (unfortunately currently impractical) which computes the coefficient a_p of a newform in complexity polynomial in $\log p$, cf. part B.

A.2.3.2 The Manin-Drinfeld theorem

In the discussions above, the non-cuspidal modular symbols (that is to say, the ones corresponding to non-closed paths on $X(\Gamma)$) have been left aside. I shall now examine then more in detail.

Thanks to the integration pairing (A.2.3.7), a modular symbol $\{\alpha, \beta\}$ may be seen as a linear form $\int_\alpha^\beta$ on $S_2(\Gamma) \simeq \Omega^1\big(X(\Gamma)\big)$. Let $S_2(\Gamma)^\vee = \mathrm{Hom}_{\mathbb{C}}\big(S_2(\Gamma), \mathbb{C}\big)$ denote the space of linear forms on $S_2(\Gamma)$. The subgroup $\mathbb{S}_2(\Gamma) \subset \mathbb{M}_2(\Gamma)$ of cuspidal modular symbols corresponds to the homology $H_1\big(X(\Gamma), \mathbb{Z}\big)$ of the modular curve $X(\Gamma)$, and so forms a full-rank lattice in $S_2(\Gamma)^\vee$ by corollary A.1.2.12. It follows that

$$S_2(\Gamma)^\vee = H_1\big(X(\Gamma), \mathbb{Z}\big) \underset{\mathbb{Z}}{\otimes} \mathbb{R},$$

so in particular every modular symbol lies in $H_1\big(X(\Gamma), \mathbb{Z}\big) \underset{\mathbb{Z}}{\otimes} \mathbb{R}$. In other words, if $(\gamma_i)_{1 \leqslant i \leqslant 2g}$ denotes a $\mathbb{Z}$-basis of $H_1\big(X(\Gamma), \mathbb{Z}\big)$, then for every modular symbol $\{\alpha, \beta\} \in \mathbb{M}_2(\Gamma)$, there exists a unique family $(\lambda_i)_{1 \leqslant i \leqslant 2g} \in \mathbb{R}^{2g}$ of real coefficients such that

$$\int_\alpha^\beta = \sum_{i=1}^{2g} \lambda_i \int_{\gamma_i}$$

as linear forms on $S_2(\Gamma)$.

The Manin-Drinfeld theorem, which I now present, asserts that these coefficients λ_i are actually rational.

Theorem A.2.3.14 (Manin-Drinfeld)**.** *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then for all cusps α and β, the modular symbol $\{\alpha, \beta\}$, seen as a linear form on $S_2(\Gamma) = \Omega^1\big(X(\Gamma)\big)$, lies in $H_1\big(X(\Gamma), \mathbb{Z}\big) \otimes \mathbb{Q}$.*

In view of the Abel-Jacobi theorem A.1.2.15, this can be reformulated as follows:

Corollary A.2.3.15. *If $D \in \mathrm{Div}^0\big(X(\Gamma)\big)$ is a null-degree divisor supported by the cusps of $X(\Gamma)$, then the class of D is torsion in $\mathrm{Pic}^0\big(X(\Gamma)\big)$.*

The proof for general Γ may be found in [Lan95, section IV.2]. I shall give a proof here for the case $\Gamma \supseteq \Gamma_1(N)$. This proof is effective, in that given α and β, it explains how to compute the coefficients $\lambda_i \in \mathbb{Q}$ such that

$$\int_\alpha^\beta = \sum_{i=1}^{2g} \lambda_i \int_{\gamma_i} .$$

I shall use this in my main algorithm so as to accelerate the computation of the period lattice of $X_1(N)$, cf. section B.3.2.

Proof. In this proof, I assume that $\Gamma \supseteq \Gamma_1(N)$ for some $N \in \mathbb{N}$. Let $r \in \mathbb{N}$ be a prime such that $r \equiv 1 \bmod N$. Then the diamond operator $\langle r \rangle$ is the identity, so the Hecke operator T_r on $S_2(\Gamma)$ is given by

$$T_r f = \sum_{\gamma \in G_r} f|_2 \gamma = \sum_{\gamma \in G_r} \gamma^* f,$$

where

$$G_r = \left\{ \begin{bmatrix} 1 & b \\ 0 & r \end{bmatrix},\ b \in \mathbb{Z},\ 0 \leqslant b < r \right\} \cup \left\{ \begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} \right\} \subset \mathrm{Mat}_{2\times 2}(\mathbb{Z})$$

and the right-hand side uses the identification of cuspforms in $S_2(\Gamma)$ with differential forms on $X(\Gamma)$. Since clearly $\|f\| = \|\alpha^* f\|$ for all $f \in S_2(\Gamma)$ and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, where $\|\cdot\|$ denotes the hermitian norm attached to the Petersson inner product with respect to the congruence subgroup $\Gamma \cap \alpha^{-1}\Gamma\alpha$, the operator $T_r - \#G_r = T_r - (r+1)$ is invertible on $S_2(\Gamma)$ since an equality $T_r f = (r+1)f$ would imply

$$\left\| \sum_{\gamma \in G_r} \alpha^* f \right\| = \|T_r f\| = \|(r+1)f\| = \sum_{\gamma \in G_r} \|\gamma^* f\|$$

which by euclidian triangle equality means that the vectors $\gamma^* f$ are all equal, so agree with f, so in particular (taking $\gamma = \left[\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right] \in G_r$) one would have $f(\tau) = f(r\tau)$, hence by induction $r^n | \operatorname{ord}_q f$ for all $n \in \mathbb{N}$, whence $f = 0$. By duality, one deduces that the endomorphism $\varphi = T_r - (r+1)$ on $\mathbb{S}_2(\Gamma) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ is invertible.

Besides, since $r \equiv 1 \bmod N$, the criterion A.2.3.11 shows that for all $\alpha \in \mathbb{P}^1\mathbb{Q}$, the cusps α, $r\alpha$ and α/r are equivalent under $\Gamma_1(N)$ and hence under Γ. Since $\left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right] \in \Gamma_1(N)$ for all $b \in \mathbb{Z}$, it follows that for all $\alpha \in \mathbb{P}^1\mathbb{Q}$, the cusps α and $\gamma\alpha$ are equivalent under Γ for all $\gamma \in G_r$, whence

$$\partial\big(T_r - (r+1)\big)\{\alpha, \beta\} = \partial \left(\sum_{\gamma \in G_r} \big(\{\gamma \cdot \alpha, \gamma \cdot \beta\} - \{\alpha, \beta\}\big) \right) = 0,$$

that is to say that the image of the morphism $\psi = T_r - (r+1) \colon \mathbb{M}_2(\Gamma) \longrightarrow \mathbb{M}_2(\Gamma)$ lies in $\mathbb{S}_2(\Gamma)$. One thus gets a morphism $\varphi^{-1} \circ \psi \colon \mathbb{M}_2(\Gamma) \longrightarrow \mathbb{S}_2(\Gamma) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ which induces the identity on $S_2(\Gamma)^\vee$. □

A.3 Galois representations

To conclude this introductory part, I shall now describe the relation between modular forms and Galois representations, and exhibit some of the consequences of this relation on modular forms.

A.3.1 Definitions and first examples

A.3.1.1 Number fields, Galois groups, and representations

To begin with, let me fix some notation. Let L/K be a Galois extension with Galois group G of number fields with integer rings respectively $\mathbb{Z}_K$ and $\mathbb{Z}_L$, let $\mathfrak{p}$ be a prime of K, and let $\mathfrak{P}$ be a prime of L lying above $\mathfrak{p}$. Denote the corresponding residue fields by $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_K/\mathfrak{p}$ and $\mathbb{F}_\mathfrak{P} = \mathbb{Z}_L/\mathfrak{P}$.

The Galois group G acts transitively on the primes of L lying above $\mathfrak{p}$. The stabiliser of $\mathfrak{P}$ is called the *decomposition group* of $\mathfrak{P}$ and is denoted by $D_\mathfrak{P}$. It identifies with the Galois group of the local extension $L_\mathfrak{P}/K_\mathfrak{p}$. Reduction modulo $\mathfrak{P}$ yields a surjective group morphism from $D_\mathfrak{P}$ to the residual Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, which is cyclic of order $f_{\mathfrak{P}/\mathfrak{p}} = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$, generated by the *Frobenius automorphism* $x \mapsto x^{\mathbb{N}\mathfrak{p}}$, where $\mathbb{N}\mathfrak{p} = \#\mathbb{F}_\mathfrak{p}$ is the numerical norm of $\mathfrak{p}$. The kernel of this morphism is the *inertia subgroup* $I_\mathfrak{P}$. It has order $e_{\mathfrak{P}/\mathfrak{p}} = \mathrm{ord}_\mathfrak{P}\,\mathfrak{p}$, and identifies with the inertia subgroup of $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Consequently, the extension L/K is said to be *ramified* at $\mathfrak{P}$ if $I_\mathfrak{P}$ is non-trivial, that is to say if $e_{\mathfrak{P}/\mathfrak{p}} > 1$.

More generally, the so-called *higher inertia subgroups* $I_\mathfrak{P}^{(i)}$ made up of the elements of $D_\mathfrak{P}$ which induce the identity on $\mathbb{Z}_L/\mathfrak{P}^{i+1}$ form a finite decreasing filtration

$$I_\mathfrak{P} = I_\mathfrak{P}^{(0)} \supseteq I_\mathfrak{P}^{(1)} \supseteq I_\mathfrak{P}^{(2)} \supseteq \cdots$$

of $I_\mathfrak{P}$. The normal subgroup $I_\mathfrak{P}^{(1)}$ of $I_\mathfrak{P}$ is called the *wild* inertia subgroup. I shall denote it by $W_\mathfrak{P} = I_\mathfrak{P}^{(1)}$, and the corresponding quotient by $I_\mathfrak{P}^{\mathrm{tame}} = I_\mathfrak{P}/W_\mathfrak{P}$. Picking a uniformiser $\Pi \in \mathbb{Z}_L$ (that is to say $\mathrm{ord}_\mathfrak{P}\,\Pi = 1$) yields injections

$$\begin{array}{ccc} I_\mathfrak{P}^{\mathrm{tame}} & \hookrightarrow & \mathbb{F}_\mathfrak{P}^* \\ \sigma & \longmapsto & \dfrac{\sigma(\Pi)}{\Pi} \bmod \mathfrak{P} \end{array}, \quad \text{and}$$

$$\begin{array}{ccc} I_\mathfrak{P}^{(i)}/I_\mathfrak{P}^{(i+1)} & \hookrightarrow & \mathbb{F}_\mathfrak{P} \\ \sigma & \longmapsto & \dfrac{\sigma(\Pi)-\Pi}{\Pi^i} \bmod \mathfrak{P} \end{array} \qquad (i \geqslant 1),$$

so that $I_\mathfrak{P}^{\mathrm{tame}}$ is abelian and $W_\mathfrak{P}$ is actually the p-Sylow subgroup of $I_\mathfrak{P}$, where $p \in \mathbb{N}$ is the prime number below $\mathfrak{P}$. In particular, $W_\mathfrak{P}$ is non-trivial if and only if $p \,|\, e_{\mathfrak{P}/\mathfrak{p}}$, in which case the extension L/K is said to be *wildly* ramified at $\mathfrak{P}$, and *tamely* ramified (if ramified) else.

An element $\sigma \in D_\mathfrak{P}$ reducing modulo $\mathfrak{P}$ to the Frobenius automorphism of the residual extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is called a *Frobenius element* at $\mathfrak{P}$ and is denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$.

Since G acts transitively on the primes $\mathfrak{P}$ above $\mathfrak{p}$, replacing the prime $\mathfrak{P}$ used in the constructions above by another one amounts to conjugating everything by some

element of G. In particular, the ramification behaviour depends only on $\mathfrak{p}$, and not on $\mathfrak{P}$. I shall write $D_\mathfrak{p}$, $I_\mathfrak{p}$, $W_\mathfrak{p}$, $I_\mathfrak{p}^{(i)}$, and so on to mean $D_\mathfrak{P}$, $I_\mathfrak{P}$, $W_\mathfrak{P}$, $I_\mathfrak{P}^{(i)}$, and so on for some $\mathfrak{P}$ when the choice of this $\mathfrak{P}$ does not matter. In particular, an element $\sigma \in G$ which is a Frobenius element at some $\mathfrak{P}|\mathfrak{p}$ is called a Frobenius element at $\mathfrak{p}$, and in what follows, I shall denote such an element, which is defined only up to conjugacy and inertia, by $\mathrm{Frob}_\mathfrak{p}$, or by $\left(\frac{L/K}{\mathfrak{p}}\right)$ if the field extension in consideration is not clear.

Example A.3.1.1. Let $K = \mathbb{Q}$, and let $L = \mathbb{Q}(\mu_{\ell^n})$ be the $\ell^{n\text{-th}}$ cyclotomic extension, where ℓ is a prime. Let ζ be a primitive $\ell^{n\text{-th}}$ root of 1 in L. The extension L/K is Galois of degree $d = \ell^n(1 - \frac{1}{\ell})$, with Galois group G canonically isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ by letting $a \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$ correspond to $\zeta \mapsto \zeta^a$.

The ring of integers of L is well-known to be $\mathbb{Z}_L = \mathbb{Z}[\zeta]$. The element

$$\epsilon_a = \frac{\zeta^a - 1}{\zeta - 1} = 1 + \zeta + \cdots + \zeta^{a-1}$$

is clearly integral for all $a \in \mathbb{Z}/\ell^n\mathbb{Z}$; furthermore, if a is invertible in $\mathbb{Z}/\ell^n\mathbb{Z}$, then $1/\epsilon_a$ can similarly be expressed as a polynomial in ζ^a and hence in ζ, so that ϵ_a is a unit in $\mathbb{Z}_L^*$ in this case. Since

$$\ell = \prod_{a \in (\mathbb{Z}/\ell^n\mathbb{Z})^*} (1 - \zeta^a) = (1 - \zeta)^d \prod_{a \in (\mathbb{Z}/\ell^n\mathbb{Z})^*} \epsilon_a,$$

the ideal $\mathfrak{l} = \ell\mathbb{Z}$ factors as $\mathfrak{L}^d$, where $\mathfrak{L} = (1 - \zeta)\mathbb{Z}[\zeta]$. In particular, the extension L/K is totally ramified at ℓ, hence $G = I_\ell$ and $\lambda = 1 - \zeta$ is a uniformiser at ℓ.

Since $\mathbb{Z}_L = \mathbb{Z}[\zeta]$, it suffices to look at the Galois action on ζ to determine the higher ramification filtration: an element $\sigma \in G = I_\ell$ lies in $I_\ell^{(i)}$ if and only if $\mathrm{ord}_\lambda\left(\sigma(\zeta) - \zeta\right) \geqslant i + 1$. Let $a \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$ correspond to σ, and let $m = \mathrm{ord}_\ell(a - 1)$, so that $a = 1 + \ell^m u$ for some $u \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$ and

$$\sigma(\zeta) - \zeta = \zeta(\zeta^{a-1} - 1) = \zeta\frac{\zeta^{l^m u} - 1}{\zeta^{l^m} - 1}(\zeta^{l^m} - 1)$$

has the same λ-adic valuation as $\zeta^{l^m} - 1$. Now, by the same reasoning as above, $\zeta^{l^m} - 1$ is a uniformiser at ℓ for the field $E = \mathbb{Q}(\zeta^{\ell^m}) = \mathbb{Q}(\mu_{\ell^{n-m}})$. Since L/K is totally ramified at ℓ, so is L/E, which implies

$$\mathrm{ord}_\lambda(\zeta^{l^m} - 1) = [L\colon E] = \frac{[L : K]}{[E : K]} = \frac{\ell^n(1 - \frac{1}{\ell})}{\ell^{n-m}(1 - \frac{1}{\ell})} = \ell^m.$$

This means that upon identification of $I_\ell = G$ with $(\mathbb{Z}/\ell^n\mathbb{Z})^*$, the higher inertia filtration is

$$\underbrace{G = I_\ell^{(0)}}_{\left(\frac{\mathbb{Z}}{\ell^n\mathbb{Z}}\right)^*} \supsetneq \underbrace{I_\ell^{(1)} = \cdots = I_\ell^{(\ell-1)}}_{\frac{1+\ell\mathbb{Z}}{\ell^n\mathbb{Z}}} \supsetneq \underbrace{I_\ell^{(\ell)} = \cdots = I_\ell^{(\ell^2-1)}}_{\frac{1+\ell^2\mathbb{Z}}{\ell^n\mathbb{Z}}} \supsetneq I_\ell^{(\ell^2)} \cdots$$

Finally, the extension L/K is unramified at other primes $p \neq \ell$ since $\overline{\mathbb{F}}_p$ contains ℓ^n distinct $\ell^{n\text{-th}}$ roots of 1. Since L/K is also abelian, the Frobenius element at $p \neq \ell$ is well-defined, and clearly corresponds to $p \bmod \ell^n \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$.

Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$ containing K, and consider a now possibly infinite extension L of K contained in $\overline{\mathbb{Q}} = \overline{K}$. The extension L/K is Galois if it is a compositum of finite Galois extensions, in which case the group

$$\mathrm{Gal}(L/K) = \varprojlim_{\substack{L \supset E/K \\ \text{finite Galois}}} \mathrm{Gal}(E/K)$$

is endowed with the Krull topology, that is to say the profinite topology, which makes G a compact topological group. In other words, a basis of this topology is made up by the subsets U of $\mathrm{Gal}(L/K)$ of the form $\pi_E^{-1}(A)$ for some finite Galois subextension E/K and some subset A of $\mathrm{Gal}(E/K)$, where π_E denotes the projection $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(E/K)$. In particular, the subgroups $\mathrm{Gal}(L/E)$ for finite Galois subextensions E/K form a basis of compact open neighbourhoods of $\mathrm{Id} \in \mathrm{Gal}(L/K)$. The usual Galois theory extends into a correspondence between subextensions of L/K and *closed* subgroups of $\mathrm{Gal}(L/K)$, for which finite subextensions correspond to finite index subgroups. Moreover, the Cebotarev density theorem implies that Frobenius elements are dense in G.

The above generalises to infinite extensions L/K by seeing them as the compositum of their finite subextensions. In particular, in the case $L = \overline{\mathbb{Q}}$, the group $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is called the *absolute Galois group* of K, and the decomposition subgroup of a prime lying above $\mathfrak{p}$ identifies to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p})$, which can hence be seen as a subgroup of the absolute Galois group of K.

Definition A.3.1.2. Let R be a topological ring, and let $n \in \mathbb{N}$. A *Galois representation of degree n* is a continuous group morphism

$$\rho\colon G_K \longrightarrow \mathrm{GL}_n(R),$$

where $G_K = \mathrm{Gal}(\overline{K}/K)$ denotes the *absolute Galois group* of K.

In the case $n = 1$, a representation

$$\rho\colon G_K \longrightarrow \mathrm{GL}_1(R) = R^*$$

is called a Galois *character*.

Note that I only consider *continuous* Galois representations. In particular, the kernel of such a representation ρ is a closed normal subgroup of G_K, which corresponds to a Galois extension L of K, which I call the field *cut out* by ρ. Its Galois group is $\mathrm{Im}\,\rho$.

The Galois representation ρ is said to be *unramified* at a finite prime $\mathfrak{p}$ of K if ρ is trivial on the inertia subgroup of a prime $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ lying above $\mathfrak{p}$. This does not depend on $\mathfrak{P}$, since all the $\mathfrak{P}$'s are conjugate, and the kernel of ρ is a normal subgroup. Actually, it is clear that ρ is unramified at $\mathfrak{p}$ if and only if the number field L it cuts out is unramified at $\mathfrak{p}$.

Remark A.3.1.3. Although the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ is defined only up to conjugacy and inertia, its image $\rho(\mathrm{Frob}_\mathfrak{p}) \in \mathrm{GL}_n(R)$ lies in a well-defined conjugacy (i.e. similarity) class if ρ is unramified at $\mathfrak{p}$. In particular, it makes sense to refer to the trace, determinant, and characteristic polynomial of $\rho(\mathrm{Frob}_\mathfrak{p})$. I shall even write $\mathrm{tr}\,\mathrm{Frob}_\mathfrak{p}$, $\det \mathrm{Frob}_\mathfrak{p}$, and $\chi_{\mathrm{Frob}_\mathfrak{p}}$ when ρ is clear from the context.

In practice, I shall consider $K = \mathbb{Q}$, $n = 1$ or 2, and three kinds of rings R:

- $R = \mathbb{C}$ endowed with the usual topology, in which case I shall refer to ρ as a complex Galois representation, also known as an Artin representation. This case turns out to be rather uninteresting, since $\mathrm{GL}_n(\mathbb{C})$, unlike $G_{\mathbb{Q}}$, does not have arbitrarily small subgroups[13], so that the image of a complex Galois representation is always finite. In particular, the field cut out by such a representation ρ is a Galois number field, and ρ ramifies at finitely many primes.

- $R = \mathbb{Q}_\ell$ (or a finite extension $K_\mathfrak{l}$ thereof) endowed with the $\mathfrak{l}$-adic topology, in which case I shall refer to ρ as an $\mathfrak{l}$-adic Galois representation. Unlike in the complex case, the profinite topologies of $G_{\mathbb{Q}}$ and $GL_n(K_\mathfrak{l})$ are "compatible", so that there do exist $\mathfrak{l}$-adic Galois representations with infinite image as I shall demonstrate shortly, making this case much more interesting. By compacity of $G_{\mathbb{Q}}$, an $\mathfrak{l}$-adic representation is always conjugate to a representation with values in $\mathrm{GL}_n(\mathbb{Z}_\mathfrak{l})$. In particular, it is tempting to reduce it modulo $\mathfrak{l}$, which leads to the last case.

- $R = \mathbb{F}_\ell$ (or a finite extension $\mathbb{F}_\mathfrak{l}$ thereof) endowed with the discrete topology, in which case I shall refer to ρ as a mod $\mathfrak{l}$ Galois representation. The image of such a complex Galois representation is obviously finite. In particular, the field cut out by such a representation ρ is a Galois number field, and ρ ramifies at finitely many primes. This kind of representation is especially well suited for computational purposes.

Remark A.3.1.4. As mentioned above, every $\mathfrak{l}$-adic Galois representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(K_\mathfrak{l})$$

is conjugate to a representation ρ' with values in $\mathrm{GL}_n(\mathbb{Z}_\mathfrak{l})$, which one can reduce modulo $\mathfrak{l}$ to get a mod $\mathfrak{l}$ Galois representation $\overline{\rho}$ with values in $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$. This representation $\overline{\rho}$ may not not uniquely defined since ρ' may not be not uniquely defined. However, by the Brauer-Nesbitt theorem below, the *semi-simplification* $\overline{\rho}^{\mathrm{ss}}$ of $\overline{\rho}$ over $\overline{\mathbb{F}_\ell}$ is well-defined.

Theorem A.3.1.5 (Brauer-Nesbitt, cf. [Wei03, theorem 7.2.4])**.** *Let G be a finite group, and let*

$$\rho_1, \rho_2\colon G \longrightarrow \mathrm{GL}_n(F)$$

*be two **semi-simple** representations of G of degree n with coefficients in an algebraically closed field F (of any characteristic). These representations are isomorphic if and only if $\rho_1(\sigma)$ has the same characteristic polynomial as $\rho_2(\sigma)$ for all $\sigma \in G$.*

Although $G_{\mathbb{Q}}$ is infinite, this theorem does apply, since both ρ_1 and ρ_2 factor through the finite quotient $\mathrm{Gal}(L_1L_2/\mathbb{Q})$ of $G_{\mathbb{Q}}$, where L_1L_2 denotes the compositum of the Galois number fields L_1 and L_2 cut out respectively by ρ_1 and ρ_2.

In particular, if $\overline{\rho}^{\mathrm{ss}}$ is irreducible over $\overline{\mathbb{F}_\ell}$, then $\overline{\rho} = \overline{\rho}^{\mathrm{ss}}$ is well-defined.

[13]This comes from the fact that the exponential map $\exp\colon \mathfrak{gl}_n(\mathbb{C}) = \mathrm{Mat}_{n\times n}(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ is locally invertible at 0, so that a small enough subgroup of $\mathrm{GL}_n(\mathbb{C})$ would be linearisable, and hence could not stay near 0.

A.3.1.2 Examples

Here are some classical examples of Galois representations.

Example A.3.1.6. Let $\chi\colon (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ be a Dirichlet character. Then the canonical identification of $(\mathbb{Z}/N\mathbb{Z})^*$ with the Galois group $\mathrm{Gal}\left(\mathbb{Q}(\mu_N)/\mathbb{Q}\right)$ of the N^{th} cyclotomic extension allows to see χ as a complex Galois character

$$\chi\colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}(\mu_N)/\mathbb{Q}\right) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\chi} \mathbb{C}^* .$$

The number field it cuts out is $\mathbb{Q}(\mu_N)$ if χ is a primitive Dirichlet character, and a subfield thereof in general. In particular, χ is unramified outside N. For $p \nmid N$, the image of the Frobenius element Frob_p by χ is $\chi(p)$.

Let now $\ell \in \mathbb{N}$ denote a prime number.

Example A.3.1.7. The action of $G_{\mathbb{Q}}$ on the ℓ^{th} roots of unity in $\overline{\mathbb{Q}}$ yields a mod ℓ Galois character

$$\overline{\chi}_\ell\colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right) \xrightarrow{\sim} (\mathbb{Z}/\ell\mathbb{Z})^*$$

called the mod ℓ cyclotomic character. It cuts out the number field $\mathbb{Q}(\mu_\ell)$, and it is ramified only at ℓ. The image of the Frobenius element Frob_p for $p \neq \ell$ is p mod ℓ.

Example A.3.1.8. More generally, the action of $G_{\mathbb{Q}}$ on group μ_{ℓ^∞} of ℓ-power roots of unity in $\overline{\mathbb{Q}}$ yields an ℓ-adic Galois character

$$\chi_\ell\colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right) \xrightarrow{\sim} \mathbb{Z}_\ell^*$$

called the ℓ-adic cyclotomic character, whose reduction modulo ℓ is the mod ℓ cyclotomic character defined just above. It cuts out the number field $\mathbb{Q}(\mu_{\ell^\infty})$, and it is ramified only at ℓ. The image of the Frobenius element Frob_p for $p \neq \ell$ is $p \in \mathbb{Z}_\ell^*$. In particular, χ_ℓ has infinite image.

The following lemma shows the omnipresence of the cyclotomic characters.

Lemma A.3.1.9. *Let $\psi\colon G_{\mathbb{Q}} \longrightarrow \mathbb{F}_\ell^*$ be a Galois character which is unramified outside ℓ. Then ψ is a power of the mod ℓ cyclotomic character $\overline{\chi}_\ell$.*

Proof. If $\ell = 2$, then ψ is trivial and the statement is vacuous. Assume now that $\ell \geqslant 3$, and let L be the field cut out by ψ. Since $\mathbb{F}_\ell^*$ is abelian, so is the image of ψ, so that L is a subfield of the maximal abelian extension of $\mathbb{Q}$, which is the cyclotomic extension $\mathbb{Q}(\mu_\infty)$ by the Kronecker-Weber theorem. Next, since ψ only ramifies at ℓ, the same is true for L, which is thus a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$ since for all $m \in \mathbb{N}$, $\mathbb{Q}(\mu_m)$ is ramified exactly at the primes dividing m. Finally, the order of the image of ψ divides the order $\ell - 1$ of $\mathbb{F}_\ell^*$, hence is prime to ℓ, so that L is a subfield of the field $\mathbb{Q}(\mu_\ell)$ fixed by the ℓ-Sylow subgroup of $\mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right) \simeq \mathbb{Z}_\ell^* \simeq (\mathbb{Z}/\ell\mathbb{Z})^* \times \mathbb{Z}_\ell$. □

In order to give a less obvious example of Galois representation, I shall need the following result (cf. [HS00, theorem C.1.4 and section C.2]):

Theorem A.3.1.10. *Let A be an abelian variety defined over a number field K, let $\mathfrak{p}$ be a prime of K at which A has good reduction, and let $p \in \mathbb{N}$ be the prime number lying below $\mathfrak{p}$. Then for all $n \in \mathbb{N}$ such that $p \nmid n$, the reduction modulo $\mathfrak{p}$ map*

$$A(K) \longrightarrow \overline{A}(\mathbb{F}_{\mathfrak{p}})$$

is injective on the n-torsion $A[n](K)$ of $A(K)$.

Example A.3.1.11. Let E be an elliptic curve defined over $\mathbb{Q}$. The action of $G_{\mathbb{Q}}$ on $E(\overline{\mathbb{Q}})$ commutes with the group law on E since the latter is defined over $\mathbb{Q}$, so that $G_{\mathbb{Q}}$ leaves the ℓ-torsion subgroup $E[\ell]$ of $E(\overline{\mathbb{Q}})$ invariant. Since $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ as a group by A.1.2.16, the action of $G_{\mathbb{Q}}$ on $E[\ell]$ yields a mod ℓ Galois representation

$$\overline{\rho}_{E,\ell} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell),$$

which clearly cuts out the number field $\mathbb{Q}(P, P \in E[\ell])$ generated by the coordinates of the points of $E[\ell]$.

The *conductor* $N \in \mathbb{N}$ of E is an integer which measures the properties of bad reduction of E. In particular, if $p \nmid N$, then E can be reduced modulo p into an elliptic curve $\overline{E}$ defined over $\mathbb{F}_p$. Let $\sigma_p \in \mathrm{End}(\overline{E})$ be the Frobenius endomorphism on $\overline{E}$, and define

$$a_p = p + 1 - \#\overline{E}(\mathbb{F}_p) \in \mathbb{Z}.$$

If the endomorphism $\sigma_p - 1$ of $\overline{E}$ were not separable, then it would factor as $f \circ \sigma_p$ for some $f \in \mathrm{End}(\overline{E})$, but then one would have $1 = (f-1) \circ \sigma_p$, which is absurd since σ_p is not an automorphism (it is of degree $p \neq 1$). Therefore,

$$\#\overline{E}(\mathbb{F}_p) = \#\operatorname{Ker}(\sigma_p - 1) = \deg_{\mathrm{sep}}(\sigma_p - 1) = \deg(\sigma_p - 1),$$

and on the other hand one has

$$[\deg(\sigma_p - 1)]_{\overline{E}} = \widehat{(\sigma_p - 1)}(\sigma_p - 1) = (\widehat{\sigma_p} - 1)(\sigma_p - 1) = \widehat{\sigma_p}\sigma_p - \sigma_p - \widehat{\sigma_p} + 1 = [p]_{\overline{E}} - \sigma_p - \widehat{\sigma_p} + 1$$

in $\mathrm{End}(\overline{E})$, so $[a_p]_{\overline{E}} = \sigma_p + \widehat{\sigma_p}$ and thus $\sigma_p^2 - a_p\sigma_p + p = 0$ on $\overline{E}$. If furthermore $p \neq \ell$, then the right morphism on the commutative diagram

$$\begin{array}{ccc} D_p & \longrightarrow & \mathrm{Aut}(E[\ell]) \\ \downarrow & & \downarrow \wr \\ \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \longrightarrow & \mathrm{Aut}(\overline{E}[\ell]) \end{array} \tag{A.3.1.12}$$

is injective by theorem A.3.1.10, so the image of an element $\sigma \in D_p$ in $\mathrm{Aut}(E[\ell])$ depends only on its image in $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, which proves that $\overline{\rho}_{E,\ell}$ is unramified at p; moreover, the identity $\mathrm{Frob}_p^2 - a_p \mathrm{Frob}_p + p = 0$ stands on $E[\ell]$. Besides, if $P, Q \in E[\ell]$ form an $\mathbb{F}_\ell$-basis of $E[\ell]$ with Weil pairing $\langle P, Q\rangle = \zeta \in \mu_\ell$, then

$$\zeta^p = \mathrm{Frob}_p(\zeta) = \langle \mathrm{Frob}_p(P), \mathrm{Frob}_p(Q)\rangle = \langle P, Q\rangle^{\det \overline{\rho}_{E,\ell}(\mathrm{Frob}_p)}$$

as the Weil pairing on $E[\ell]$, being defined over $\mathbb{Q}$, commutes with the Galois action and as it is an alternate pairing, so that $\det \overline{\rho}_{E,\ell}(\mathrm{Frob}_p) = p \bmod \ell$, and thus the characteristic polynomial of $\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$ is

$$X^2 - a_p X + p \in \mathbb{F}_\ell[X].$$

In particular, the trace of $\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$ is $a_p \bmod \ell$, so the Galois representations $\overline{\rho}_{E,\ell}$ can be used to compute the coefficients a_p, by letting ℓ vary and using Chinese remainders. This is the central idea of Schoof's algorithm [Sch95], and also of the algorithm presented in this dissertation.

More generally, one can consider the action of $G_{\mathbb{Q}}$ on the *ℓ-adic Tate module*

$$\mathrm{Ta}_\ell E = \varprojlim_{n\in\mathbb{N}} E[\ell^n]$$

of E, where the transition maps are multiplication by ℓ. Since $\mathrm{Ta}_\ell E$ is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a group, this yields an ℓ-adic Galois representation

$$\rho_{E,\ell}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$$

which is clearly continuous. The same reasoning as above shows that it is unramified at $p \nmid \ell N$ and that the Frobenius element Frob_p at any unramified p has characteristic polynomial

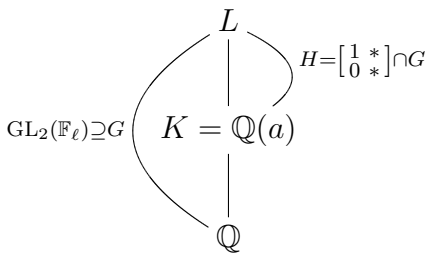
$$X^2 - a_p X + p \in \mathbb{Z}_\ell[X].$$

J.-P. Serre proved in [Ser72] that if E is not a CM elliptic curve, that is to say if $\mathrm{End}(E)$ is reduced to $\mathbb{Z}$, then the image of $\rho_{E,\ell}$ is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (i.e. contains $1 + \ell^n \mathrm{Mat}_{2\times 2}(\mathbb{Z}_\ell)$ for some $n \in \mathbb{N}$) for all ℓ, and is the whole of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for almost all ℓ. In particular, the Galois representations $\rho_{E,\ell}$ all have infinite image.

A.3.2 The Dokchitsers' resolvents

Let $\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$ be a mod ℓ Galois representation, where V is a 2-dimensional vector space over the prime field $\mathbb{F}_\ell$ ($\ell \in \mathbb{N}$ prime). In this section, I address the problem of computing the image by ρ of the Frobenius elements $\mathrm{Frob}_p \in G_{\mathbb{Q}}$, for the primes $p \in \mathbb{N}$ at which ρ is unramified. Of course, this image $\rho(\mathrm{Frob}_p)$ is only defined up to conjugation, so I actually only characterise it in terms of its conjugacy class in $\mathrm{GL}(V) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$.

Let me first explain how I assume ρ to be given. Let $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\rho}$ be the number field cut out by ρ, so that ρ embeds $G = \mathrm{Gal}(L/\mathbb{Q})$ into $\mathrm{GL}(V)$. This yields an action of G on V, and I shall assume that this action is transitive on $V - \{0\}$, which means I exclude the degenerate cases of Galois representations with "small" image. Pick then a point $x_1 \in V$, let $H = \mathrm{Stab}_G x_1 \subsetneq G$ be the stabiliser of x, and let $a \in L$ be a primitive element for the subfield $K = L^H$ of L corresponding to H. The following diagram illustrates the situation:



Then the stabiliser of a in G is exactly H, so that a has $[G\colon H] = \#(V - \{0\}) = \ell^2 - 1$ conjugates. Moreover, since G acts transitively on $V - \{0\}$, the formula

$$a_{\rho(\sigma)(x_1)} = \sigma(a), \quad \sigma \in G$$

yields a well-defined, natural indexation of these conjugates by $V-\{0\}$, for which $a = a_{x_1}$ in particular. Consider now the polynomial

$$F(X) = \prod_{\substack{x\in V\\ x\neq 0}} (X - a_x) \in \mathbb{Q}[X].$$

This polynomial lies in $\mathbb{Q}[X]$ and is irreducible over $\mathbb{Q}$ since G acts transitively on $V-\{0\}$, and L is the splitting field of $F(X)$ in $\overline{\mathbb{Q}}$ since the action of $\mathrm{GL}(V)$ on $V-\{0\}$ is faithful. Furthermore, the action of G on the roots a_x of $F(X)$ corresponds to the natural action of $\mathrm{GL}(V)$ on the points x of $V-\{0\}$. I may (and shall) thus assume that the Galois representation ρ is given as the following data:

- An irreducible polynomial $F(X) \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$,
- its roots in $\mathbb{C}$ (or in $\overline{\mathbb{Q}_p}$ for some prime $p \in \mathbb{N}$),
- an indexation of these roots by $V - \{0\}$, such that the action of $G_{\mathbb{Q}}$ on them corresponds to the ρ-action of $G_{\mathbb{Q}}$ on $V - \{0\}$.

In this framework, Tim and Vladimir Dokchitser's work [Dok10] can be adapted, yielding the following result:

Theorem A.3.2.1. *Let $h(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. For each similarity class $C \subset \mathrm{GL}_2(\mathbb{F}_\ell)$, the resolvent*

$$\Gamma_C(X) = \prod_{g\in C} \left(X - \sum_{\substack{x\in V\\ x\neq 0}} h(a_x) a_{g(x)} \right)$$

lies in $\mathbb{Q}[X]$. Furthermore, these resolvents $\Gamma_C(X)$ are pairwise coprime over $\mathbb{Q}$ for a generic choice of $h(X)$ amongst the polynomials of degree at most $\ell^2 - 2$ with coefficients in $\mathbb{Z}$. Let $p \in \mathbb{N}$ be a prime such that F is p-integral and squarefree modulo p, so that in particular, ρ is unramified at p. Define $u = \mathrm{tr}_{\frac{\mathbb{F}_p[X]}{F(X)}/\mathbb{F}_p} h(\overline{a})\overline{a}^p \in \mathbb{F}_p$, where $\overline{a}$ denotes the class of X in the quotient algebra $\mathbb{F}_p[X]/\big(F(X)\big)$. Then the resolvents Γ_C are also p-integral, and one has the implication

$$\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p) \in C \Longrightarrow \Gamma_C(u) = 0 \bmod p.$$

Proof. If $\mathrm{Im}\,\rho$ is the whole of $\mathrm{GL}(V)$, then this is a direct application of [Dok10, theorem 5.3]. The idea is that if C is the similarity class of $\rho(\mathrm{Frob}_p)$, then each $g \in C$ is the image of a Frobenius element $\left(\frac{L/\mathbb{Q}}{\mathfrak{P}}\right)$ for some ideal $\mathfrak{P}$ of L lying above p, so that

$$\sum_{\substack{x\in V\\ x\neq 0}} h(a_x) a_{g(x)} \equiv \sum_{\substack{x\in V\\ x\neq 0}} h(a_x) a_x^p \bmod \mathfrak{P}.$$

If $\mathrm{Im}\,\rho$ is a strict subgroup of $\mathrm{GL}(V)$, then the method still applies since the similarity classes in $\mathrm{Im}\,\rho$ are unions of conjugacy classes of $\mathrm{Im}\,\rho$, so that the resolvents $\Gamma_C(X)$ are products of resolvents as defined in [Dok10, theorem 5.3]. □

The point of this is that if the resolvents Γ_C are indeed pairwise coprime over $\mathbb{Q}$, and if p is very large, then it is likely that they remain pairwise coprime modulo p, so that $\Gamma_C(u)$ vanishes in $\mathbb{F}_p$ for only one C, which must then be the similarity class of $\rho(\mathrm{Frob}_p)$.

If, however, the resolvents fail to be pairwise coprime modulo p (which can occur only for finitely many p), then $\Gamma_C(u)$ may vanish for several C, so that one cannot tell in which class $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ lies. But at least this is easy to detect, so one is sure never to get a wrong answer, although one may not be able to conclude for certain values of p. Finally, the criterion is

$$\Gamma_C(u) = 0 \text{ and } \Gamma_{C'}(u) \neq 0 \text{ for all } C' \neq C \Longrightarrow \rho(\mathrm{Frob}_p) \in C.$$

To compute the resolvents $\Gamma_C(X)$, one starts by computing the roots a_x, which are already known to some mild accuracy which is enough to tell them apart, to a very high accuracy in $\mathbb{C}$ (or in $\overline{\mathbb{Q}}_p$) by using Newton iteration on the equation $F(a) = 0$. Then, one computes complex (or p-adic) approximations of the resolvents $\Gamma_C(X)$, and finally, one recognises their coefficients as rational numbers by using continued fractions (or rational reconstruction). This is amenable since an *a priori* multiple of their denominators in known beforehand, namely $d^{(\#C)(1+\deg h)}$, where d is a common denominator for the coefficients of $F(X)$.

The practical computation of the resolvents $\Gamma_C(X)$ requires making explicit the partition of $\mathrm{GL}_2(\mathbb{F}_\ell)$ into similarity classes. This is easily done:

Type	Scalar	Split semisimple	Non-split semisimple	Non-semisimple
Class representative	$\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$	$\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$	$\begin{bmatrix} 0 & -n \\ 1 & t \end{bmatrix}$	$\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$
Minimal polynomial	$x - \lambda$	$(x-\lambda)(x-\mu)$	$x^2 - tx + n$ irreducible over $\mathbb{F}_\ell$	$(x-\lambda)^2$
Number of such classes	$\ell - 1$	$\dfrac{(\ell-1)(\ell-2)}{2}$	$\dfrac{\ell(\ell-1)}{2}$	$\ell - 1$
Size of class	1	$\ell(\ell+1)$	$\ell(\ell-1)$	$(\ell+1)(\ell-1)$
Centraliser coset representatives	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} u & 1 \\ 1 & v \end{bmatrix}$, $u, v \in \mathbb{F}_\ell$, $uv \neq 1$, $\begin{bmatrix} w & 0 \\ 1 & 1 \end{bmatrix}$, $w \in \mathbb{F}_\ell^*$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} u+2 & t-vn \\ v & u+vt \end{bmatrix}$, $u, v \in \mathbb{F}_\ell$, $\det \neq 0$	$\begin{bmatrix} 1 & 0 \\ 0 & v \end{bmatrix}$, $\begin{bmatrix} u & v \\ 1 & 0 \end{bmatrix}$, $u \in \mathbb{F}_\ell$, $v \in \mathbb{F}_\ell^*$

Remark A.3.2.2. Note for future reference that the similarity classes of $\mathrm{GL}_2(\mathbb{F}_\ell)$ are represented unambiguously by their minimal polynomial. Giving this minimal

polynomial in factored form over $\mathbb{F}_\ell$ is a clear and compact representation of the similarity classes, which I shall use to present tables of results of my computations, cf. section C.1.

A.3.3 Modular Galois representations

A.3.3.1 Ramanujan congruences and Serre's insight

Recall that Ramanujan's τ function is the multiplicative function defined by

$$\Delta = q\prod_{n=1}^{+\infty}(1-q^n)^{24} = q + \sum_{n=2}^{+\infty}\tau(n)q^n,$$

where $\Delta \in S_{12}(1)$ is the normalised cuspform of level 1 and weight 12. Ramanujan conjectured that this function satisfies congruences modulo certain prime numbers, namely

- $\forall n \in \mathbb{N}$ prime to 2, $\tau(n) \equiv \sigma(n) \bmod 2$,
- $\forall n \in \mathbb{N}$ prime to 3, $\tau(n) \equiv \sigma(n) \bmod 3$,
- $\forall n \in \mathbb{N}$ prime to 5, $\tau(n) \equiv n\sigma(n) \bmod 5$,
- $\forall n \in \mathbb{N}$ prime to 7, $\tau(n) \equiv n\,\sigma_3(n) \bmod 7$,
- $\forall n \in \mathbb{N}$, $\tau(n) \equiv 0 \bmod 23$ if n is not a square modulo 23,
- $\forall n \in \mathbb{N}$, $\tau(n) \equiv \sigma_{11}(n) \bmod 691$,

where $\sigma_k(n) = \sum_{0<d|n} d^k$ and $\sigma = \sigma_1$. These congruences were proved, but, as P. Swinnerton-Dyer points out in [Swi72], the proofs "do little to explain why such congruences occur". Besides, τ does not seem to satisfy any simple congruence modulo other primes.

J.-P. Serre then realised in 1967 (cf. [Ser69]) that this phenomenon would be beautifully explained by the existence, for each prime $\ell \in \mathbb{N}$, of a mod ℓ Galois representation

$$\overline{\rho}_{\Delta,\ell}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell),$$

ramified only at ℓ, and such that the Frobenius element at $p \neq \ell$ has trace $\tau(p) \bmod \ell$. Indeed, the determinant of $\overline{\rho}_{\Delta,\ell}$ would then be a Galois character, hence a power $\overline{\chi}_\ell^k$ of the mod ℓ cyclotomic character according to lemma A.3.1.9. Besides, the representations $\rho_{\Delta,\ell}$ would be likely to be surjective, or at least to have a big image, for all but finitely many ℓ. For these exceptional ℓ, the image would happen to be a small subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so that there would be relations between the trace and the determinant of the matrices in this image. Therefore, for each $p \neq \ell$, from information about $p \bmod \ell$, one could deduce information about the determinant $\det\rho_{\Delta,\ell}(\mathrm{Frob}_p) = \overline{\chi}_\ell^k(\mathrm{Frob}_p) = p^k \bmod \ell$, hence about the trace $\mathrm{tr}\,\rho_{\Delta,\ell}(\mathrm{Frob}_p) = a_p \bmod \ell$; in other words, one would get a congruence relation modulo ℓ on the $\tau(p)$ for $p \neq \ell$, which would spread to the $\tau(n)$ for n prime to ℓ by mutiplicativity of τ. However, for almost all ℓ it would be impossible to get information on $\tau(p) \bmod \ell$ from $p \bmod \ell$ since the image of $\rho_{\Delta,\ell}$ would be (almost) the whole

of $\mathrm{GL}_2(\mathbb{F}_\ell)$, where it is impossible to get information on the trace from information on the determinant. Similar Galois representations should exist for other newforms, not only for Δ.

Example A.3.3.1. For example, the congruence for $\tau(n)$ modulo 7 would stem from the fact that the Galois representation $\overline{\rho}_{\Delta,7}$ is of the form

$$\overline{\rho}_{\Delta,7} \sim \begin{bmatrix} \overline{\chi}_7^b & * \\ 0 & \overline{\chi}_7^a \end{bmatrix}$$

with $a = 1$ and $b = 4$ or vice versa, since then for all $p \neq 7$,

$$\tau(p) \equiv \operatorname{tr} \overline{\rho}_{\Delta,7}(\mathrm{Frob}_p) = \overline{\chi}_7(\mathrm{Frob}_p)^a + \overline{\chi}_7(\mathrm{Frob}_p)^b \equiv p^a + p^b = p + p^4 = p\sigma_3(p) \bmod 7,$$

whence $\tau(n) \equiv n\sigma_3(n) \bmod 7$ for all n prime to 7 by multiplicativity of both sides.

Example A.3.3.2. Similarly, the congruence for $\tau(n)$ modulo 23 would stem from the fact that the matrices in the image of the Galois representation $\overline{\rho}_{\Delta,23}$ are all either diagonal or anti-diagonal in a fixed well-chosen basis. Indeed, this would yield a Galois character

$$\psi \colon G_{\mathbb{Q}} \longrightarrow \pm 1$$

such that for all $\sigma \in G_{\mathbb{Q}}$, $\psi(\sigma) = +1$ when $\overline{\rho}_{\Delta,23}(\sigma)$ is diagonal, and $\psi(\sigma) = -1$ when $\overline{\rho}_{\Delta,23}(\sigma)$ is anti-diagonal. The field K cut out by ψ would then be a quadratic number field (since $\operatorname{Im}\psi$ is of order 2), ramified only at 23 (since it is the case for $\overline{\rho}_{\Delta,23}$), whence $K = \mathbb{Q}(\sqrt{-23})$. Identifying $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{-23})/\mathbb{Q}\right)$ with ± 1, this means that the Galois character ψ would actually be

$$G_{\mathbb{Q}} \xrightarrow{\psi} \!\!\!\!\rightarrow \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-23})/\mathbb{Q}\right) \simeq \pm 1 \,.$$

Therefore, $\psi(\mathrm{Frob}_p) = \left(\frac{-23}{p}\right) = \left(\frac{p}{23}\right)$ for all $p \neq 23$ by quadratic reciprocity. In particular, if p is not a square modulo 23, then $\psi(\mathrm{Frob}_p) = -1$, so that $\overline{\rho}_{\Delta,23}(\mathrm{Frob}_p)$ is anti-diagonal and hence has trace $\tau(p) \bmod 23 = 0$.

J.-P. Serre's insight was proved true four years later by P. Deligne, who constructed the following Galois representations (cf. [Del71]):

Theorem A.3.3.3 (Deligne)**.** *Let*

$$f = q + \sum_{n \geqslant 2} a_n q^n \in S_k(N, \varepsilon)$$

be a newform of weight k, level N, and nebentypus ε. Let $K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$ be the number field generated by the q-expansion coefficients of f. For each prime $\mathfrak{l}$ of K_f, there exists an $\mathfrak{l}$-adic Galois representation

$$\rho_{f,\mathfrak{l}} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{\mathfrak{l}}),$$

which is unramified outside of ℓN (where $\mathbb{Z}_{\mathfrak{l}}$ denotes the $\mathfrak{l}$-adic completion of the integer ring on K_f, and $\ell \in \mathbb{N}$ is the prime number below $\mathfrak{l}$), and by which the Frobenius element Frob_p has characteristic polynomial

$$X^2 - a_p X + \varepsilon(p) p^{k-1} \in \mathbb{Z}_{\mathfrak{l}}[X]$$

for all unramified prime $p \nmid \ell N$.

A.3.3.2 Arithmetic consequences

The existence of Galois representations attached to newforms as described above has tremendous consequences on the arithmetic properties on the q-expansion coefficients of cuspforms.

Example A.3.3.4 ([Ser74])**.** For instance, it is not too difficult to prove that for every cuspform $f = \sum_{n\geqslant 1} a_n q^n$ whose coefficients a_n lie in the integer ring $\mathbb{Z}_K$ of some number field K, and for any ideal $\mathfrak{a}$ of K, the set of $n \in \mathbb{N}$ such that $a_n \not\equiv 0 \bmod \mathfrak{a}$ has density zero, and actually that

$$\#\{n \leqslant x \mid a_n \not\equiv 0 \bmod \mathfrak{a}\} = O(x/\log^{\alpha} x)$$

for some $\alpha > 0$ when $x \to +\infty$.

To see this, suppose first that f is a newform, so that the coefficients a_n are multiplicative. Then, for every prime $\mathfrak{l}$ of K and every $v \in \mathbb{N}$, the Cebotarev density theorem applied to the Galois representation

$$G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{Z}_{\mathfrak{l}}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{Z}_{\mathfrak{l}}/\mathfrak{l}^v\mathbb{Z}_{\mathfrak{l}})$$

indicates that the set $P_{\mathfrak{l},v}$ of primes $p \in \mathbb{N}$ such that $a_p \equiv 0 \bmod \mathfrak{l}^v$ has positive density $\delta_{\mathfrak{l},v} > 0$. Since the coefficients a_n are multiplicative, one then has $a_n \equiv 0 \bmod \mathfrak{l}^v$ for all n such that $p \| n$ for some $p \in P_{\mathfrak{l},v}$. A little analysis then shows that then number of $n \leqslant x$ for which this is not the case is $O(x/\log^{\delta_{\mathfrak{l},v}} x)$.

This extends to cuspforms since every cuspform is a linear combination of newforms up to finitely many coefficients by (A.2.2.28).

Example A.3.3.5. P. Deligne's construction A.3.3.3 also shows that the *Weil conjectures* (cf. [Wei49]) imply the *Ramanujan-Petersson* conjecture, which says that if

$$f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N)\big)$$

is a newform of weight k, then

$$|\sigma(a_p)| \leqslant 2p^{\frac{k-1}{2}} \tag{A.3.3.6}$$

for all $p \in \mathbb{N}$ prime and every embedding σ of $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ into $\mathbb{C}$. For instance, in the case of $f = \Delta$, this would say that $\tau(p) \leqslant 2p^{11/2}$. P. Deligne again proved the Weil conjectures a few years later (cf. [Del74, Del80]), and hence the Ramanujan-Petersson conjecture too. Note that the multiplicativity (A.2.2.20) of the a_n imply that

$$|\sigma(a_n)| \leqslant \sigma_0(n) n^{\frac{k-1}{2}} \tag{A.3.3.7}$$

for all $n \in \mathbb{N}$ and all σ, where $\sigma_0(n)$ denotes the number of positive divisors of n. One has $d(n) = O(n^{\delta})$ for all $\delta > 0$ (cf. for instance [HW08, ch. XVIII, theorem 315]), so by (A.2.2.28) one concludes that for all cuspform f of weight k,

$$a_n(f) = O(n^{\frac{k-1}{2}+\delta})$$

for all $\delta > 0$ when $n \to +\infty$. Note that one can prove by elementary means (cf. [DS05, proof of proposition 5.9.1]) that $a_n(f) = O(n^{k/2})$.

Finally, P. Swinnerton-Dyer proved (cf. [Swi72] or [Ser73]) that for each newform f whose q-expansion coefficients are rational (i.e. lie in $\mathbb{Z}$), there are only finitely many primes $\ell \in \mathbb{N}$ such that the image of the associated mod ℓ Galois representation $\overline{\rho}_{f,\ell}$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, which implies that there exist only finitely many ℓ such that the coefficients of f satisfy Ramanujan-style congruence relations modulo ℓ.

Remark A.3.3.8. According to Maeda's conjecture, for all k, the newforms in $S_k(1)$ form a single Galois orbit, so that in particular a newform has rational coefficients only if the space $S_k(1)$ it lies in has dimension 1. By the dimension formulae given in theorem A.2.2.10, there are only six such newforms: Δ, $E_4\Delta$, $E_6\Delta$, $E_8\Delta$, $E_{10}\Delta$ and $E_{14}\Delta$, of respective weights $k = 12$, 16, 18, 20, 22 and 26. Maeda's conjecture has been tested successfully for all k up to 2000 by D. Farmer and K. James in [FW02].

I now present a sketch of P. Swinnerton-Dyer's proof, following the presentation of [Swi72]. To simplify matters, I assume henceforth that $\ell \geqslant 5$. I shall denote reduction modulo ℓ by a bar, and the weight of f by k_f.

Definition A.3.3.9. A prime $\ell \in \mathbb{N}$ is *exceptional* for f if the image of the associated mod ℓ Galois representation $\overline{\rho}_{f,\ell}$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$.

To begin with, it is natural to wonder what the possible images of a mod ℓ Galois representations are. Define a *Borel subgroup* of $\mathrm{GL}_2(\mathbb{F}_\ell)$ to be a subgroup conjugate to the subgroup of upper triangular matrices, and a *Cartan subgroup* to be a subgroup which is either conjugate to the subgroup of diagonal matrices, in which case it is said to be *split* and is isomorphic to $\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$, or conjugate in $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ to the subgroup of $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ made of matrices of the form $\left[\begin{smallmatrix} a & 0 \\ 0 & a' \end{smallmatrix}\right]$ where $a' = a^\ell$ is the conjugate of a by the Frobenius automorphism $x \mapsto x^\ell$, in which case it is said to be *non-split* and is isomorphic to $\mathbb{F}_{\ell^2}^*$. The normaliser of a Cartan subgroup C either swaps the two eigenlines of C or leaves them invariant, so C has index 2 in it, whereas a Borel subgroup is its own normaliser.

Example A.3.3.10. For instance, the representation $\overline{\rho}_{\Delta,7}$ studied in example A.3.3.1 has values in a Borel subgroup, whereas the representation $\overline{\rho}_{\Delta,23}$ studied in example A.3.3.2 has values in the normaliser of a split Cartan subgroup.

One then has the following classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, due to Dixon:

Proposition A.3.3.11. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. If its order is divisible by ℓ, then G either contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or is contained in a Borel subgroup. Else, letting $\mathrm{P}G$ denote the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$, then either*

(i) *$\mathrm{P}G$ is cyclic, and G is contained in a Cartan subgroup, or*

(ii) *$\mathrm{P}G$ is dihedral, and G is contained in the normaliser of a Cartan subgroup but not in the Cartan subgroup itself, or*

(iii) *$\mathrm{P}G$ is isomorphic to the symmetric group $\mathfrak{S}_4$, or to the alternating group $\mathfrak{A}_4$ or $\mathfrak{A}_5$.*

The proof is fairly standard, cf. [Swi72, lemma 2].

However, some of these subgroups cannot be the image of a $\overline{\rho}_{f,\ell}$.

Lemma A.3.3.12. *Let G be the image of $\overline{\rho}_{f,\ell}$. Then G cannot be contained in a* ***non-split*** *Cartan subgroup, and* PG *cannot be isomorphic to $\mathfrak{A}_4$ nor $\mathfrak{A}_5$.*

Proof. Let $c \in G_{\mathbb{Q}}$ be the complex conjugation corresponding to some embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Then $\overline{\rho}_{f,\ell}(c) \in G$ is an involutory matrix of $\mathrm{GL}_2(\mathbb{F}_\ell)$, of determinant $\det \overline{\rho}_{f,\ell}(c) = \overline{\chi}_\ell^{k_f-1}(c) = (-1)^{k_f-1} = -1$ since k_f is even, so its eigenvalues are 1 and -1. In particular, it cannot lie in a non-split Cartan subgroup.

Consider next the following Galois character

$$G_{\mathbb{Q}} \xrightarrow{\overline{\rho}_{f,\ell}} G \xrightarrow{\det} \mathbb{F}_\ell^* \twoheadrightarrow \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2 \simeq \pm 1 \,.$$
$$\overline{\chi}_\ell^{k_f-1}$$

It is non-trivial again because k_f is even, so G has a subgroup of index 2. But neither $\mathfrak{A}_4$ nor $\mathfrak{A}_5$ do. □

Corollary A.3.3.13. *Let G be the image of $\overline{\rho}_{f,\ell}$. If ℓ is an exceptional prime for f, then either*

(i) G is contained in a Borel subgroup, or

(ii) G is contained in the normaliser of a Cartan subgroup but not in the Cartan subgroup itself, or

(iii) the image PG *of G in* $\mathrm{PGL}_2(F_\ell)$ *is isomorphic to the symmetric group $\mathfrak{S}_4$.*

Indeed, a split Cartan subgroup can be seen as a subgroup of a Borel subgroup.

At this point, it is already apparent that if ℓ is an exceptional prime for f, then the image of $\overline{\rho}_{f,\ell}$ will be small enough for non-trivial relations to exist between the trace and the norm of elements of its image G, whence Ramanujan-like congruences for the coefficients a_n of f. In other words, the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ which do not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$ all turn out to be sufficiently small for Ramanujan-like congruences to exist, which explains Serre's insight [Ser69]. Note that this also limits the kind of congruences which may occur:

Corollary A.3.3.14. *Let ℓ be an exceptional prime for f. Then the three cases listed in the above corollary respectively imply*

(i) There exists an integer a such that $0 \leqslant a < k_f - 1 - a$ and that $a_n \equiv n^a \sigma_{k_f-1-2a}(n)$ for all $n \in \mathbb{N}$ prime to ℓ.

(ii) $a_n \equiv 0$ for all $n \in \mathbb{N}$ which are not a square modulo ℓ.

(iii) For all prime numbers $p \neq \ell$, $\frac{a_p^2}{p^{k_f-1}} \equiv 0,\ 1,$ or $4 \bmod \ell$ if p is a square modulo ℓ, and $\frac{a_p^2}{p^{k_f-1}} \equiv 0$ or $2 \bmod \ell$ else.

Proof. (i) This is a generalisation of example A.3.3.1: by hypothesis, after conjugation by a fixed matrix, the image of $\overline{\rho}_{f,\ell}$ is made up of upper triangular matrices, so that in particular the diagonal entries are Galois characters, hence of the form $\overline{\chi}_\ell^a$ and $\overline{\chi}_\ell^b$ by lemma A.3.1.9. Besides, their product is $\det \overline{\rho}_{f,\ell} = \overline{\chi}_\ell^{k_f-1}$, so that $a+b \equiv k_f - 1 \bmod \ell - 1$. One can assume without loss of generality that $a+b = k_f - 1$, and that $a < b$ (a and b cannot be equal since their sum $k_f - 1$ is odd). Then for all $p \neq \ell$,

$$\begin{aligned} a_p \bmod \ell = \operatorname{tr} \overline{\rho}_{f,\ell}(\mathrm{Frob}_p) &= \overline{\chi}_\ell^a(\mathrm{Frob}_p) + \overline{\chi}_\ell^{k_f-1-a}(\mathrm{Frob}_p) \\ &= p^a + p^{k_f-1-a} = p^a \sigma_{k_f-1-2a}(p), \end{aligned}$$

and this congruence spreads to all $n \in \mathbb{N}$ prime to ℓ by multiplicativity.

(ii) This is a generalisation of example A.3.3.2: by hypothesis, after conjugation by a fixed matrix, the image of $\overline{\rho}_{f,\ell}$ is made up of matrices which are either diagonal or anti-diagonal, which yields a Galois character

$$\psi \colon G_{\mathbb{Q}} \longrightarrow \pm 1$$

such that for all $\sigma \in G_{\mathbb{Q}}$, $\psi(\sigma) = +1$ when $\overline{\rho}_{f,\ell}(\sigma)$ is diagonal, and $\sigma \in G_{\mathbb{Q}}$, $\psi(\sigma) = -1$ when $\overline{\rho}_{f,\ell}(\sigma)$ is anti-diagonal. Since ψ factors through $\overline{\rho}_{f,\ell}$, the number field K it cuts out is contained in the number field cut out by $\overline{\rho}_{f,\ell}$ and so ramifies only at ℓ, and it is a quadratic number field since $\operatorname{Im}\psi$ is of order 2. But there is only one quadratic number field ramified only at ℓ, namely $\mathbb{Q}(\sqrt{\ell^*})$ where $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$, so ψ is actually

$$G_{\mathbb{Q}} \xrightarrow{\psi} \!\!\!\!\rightarrow \mathrm{Gal}\left(\mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}\right) \simeq \pm 1\,.$$

Therefore, $\psi(\mathrm{Frob}_p) = \left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$ for all $p \neq \ell$ by quadratic reciprocity. In particular, if p is not a square modulo ℓ, then $\psi(\mathrm{Frob}_p) = -1$, so that $\overline{\rho}_{f,\ell}(\mathrm{Frob}_p)$ is anti-diagonal and hence has trace $a_p \bmod \ell = 0$. Since the a_n are multiplicative, one therefore also has $a_n \equiv 0 \bmod \ell$ if there exists a prime $p \| n$ which is not a square modulo ℓ, and thus *a fortiori* if n is not a square mod ℓ.

(iii) First observe that the map

$$\phi \colon \begin{array}{ccc} \mathrm{GL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathbb{F}_\ell \\ M & \longmapsto & \frac{(\operatorname{tr} M)^2}{\det M} \end{array}$$

factors through $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Now, the elements of $\mathfrak{S}_4$ are of order $n = 1, 2, 3$ or 4, and a matrix M whose image in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has such order n is killed by a polynomial of the form $(X-a)^n \in \mathbb{F}_\ell[X]$ for some $a \in \mathbb{F}_\ell^*$, which is separable since I assumed $\ell \geqslant 5$. This implies that such a matrix M is semi-simple, hence its image in $\mathrm{PGL}_2(\overline{\mathbb{F}_\ell})$ can be represented by $\left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right]$ for some root of unity $\zeta \in \overline{\mathbb{F}_\ell}$ of exact order n. One then finds that $\phi(M) = 4, 0, 1, 2$, respectively. Besides, a reasoning similar to case (ii) shows that the image of Frob_p lies in $\mathfrak{A}_4$ if and only if p is a square modulo ℓ. In this case, it has order 1, 2 or 3, else, it has order 2 or 4.

□

I shall now effectively prove that each of these cases can happen for only finitely many ℓ. Let

$$E_k = 1 - \frac{2k}{b_k} \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n \in M_k(1)$$

be the Eisenstein series from example A.2.2.5, which can also be normalised as

$$F_k = \frac{b_k}{2k} - \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n \in M_k(1),$$

and also let

$$E_2 = 1 - 24 \sum_{n=1}^{+\infty} \sigma_1(n) q^n.$$

This is **NOT** a modular form, and actually $M_2(1) = \{0\}$. However,

Proposition A.3.3.15 (cf. [Swi72, lemma 3])**.** *Let $\theta = q\frac{\mathrm{d}}{\mathrm{d}q}$ be the operator*

$$\sum_{n=0}^{+\infty} a_n q^n \longmapsto \sum_{n=0}^{+\infty} n a_n q^n$$

on q-series, and let $\partial = 12\theta - kE_2$ be the operator

$$f \longmapsto 12\theta f - kE_2 f$$

for $f \in M_k(1)$. Then for all $k \geqslant 4$, ∂ maps $M_k(1)$ to $M_{k+2}(1)$.

Unfortunately, the operator θ does not necessarily transform modular forms into modular forms since E_2 is not modular. However, the situation is much more pleasant modulo ℓ. To see that, let $M_k^{(\ell)}(1)$ denote the subset of $M_k(1)$ made up of forms whose q-expansion coefficients are all ℓ-integral, in other words, the $\mathbb{Z}_{(\ell)}$-span of the so-called Miller basis of $M_k(1)$ (cf. [Ste07, section 2.3]), where $\mathbb{Z}_{(\ell)}$ denotes the localisation of $\mathbb{Z}$ at ℓ. The Von-Staudt congruences on Bernoulli numbers (cf. [Lan95, theorem X.2.1]) imply that $E_k \in M_k^{(\ell)}(1)$ for all k, and that $F_k \in M_k^{(\ell)}(1)$ except if $(\ell - 1)|2k$; furthermore, one has $E_{\ell-1} \equiv 1 \bmod \ell$ and $E_{\ell+1} \equiv E_2 \bmod \ell$, so E_2 becomes a modular form mod ℓ. The graded algebra

$$M = \bigoplus_{k \geqslant 0} M_k^{(\ell)}(1) = \mathbb{Z}_{(\ell)}[E_4, E_6]$$

comes with the injective morphism $\phi : M \hookrightarrow \mathbb{Z}_{(\ell)}\big[[q]\big]$ provided by q-expansion, which allows to identify M with a $\mathbb{Z}_{(\ell)}$-subalgebra of $\mathbb{Z}_{(\ell)}\big[[q]\big]$. Letting

$$\overline{M}_k(1) = \left\{ \sum_{n=0}^{+\infty} \overline{a_n} q^n \;\middle|\; \sum_{n=0}^{+\infty} a_n q^n \in M_k^{(\ell)}(1) \right\},$$

one gets a morphism of $\mathbb{F}_\ell$ algebras

$$\overline{\phi} \colon \overline{M} = M/\ell M = \sum_{k \geqslant 0} \overline{M}_k^{(\ell)}(1) \longrightarrow \mathbb{F}_\ell\big[[q]\big]$$

which is no longer injective since $E_{\ell-1} \equiv 1 \bmod \ell$. Actually, to quote J.-P. Serre, this is "the only relation" between modular forms modulo ℓ:

Theorem A.3.3.16 (cf. [Swi72, theorem 2(iv)]). *The kernel of $\overline{\phi}$ is the ideal of $\overline{M}$ generated by $\overline{E_{\ell-1}} - 1$.*

In particular, $\overline{M}$ inherits a $\mathbb{Z}/(\ell-1)\mathbb{Z}$-graduation from M. Besides, since $E_{\ell+1} \equiv E_2 \bmod \ell$, one has

$$12\theta\overline{f} = \partial\overline{f} + k\overline{E_2 f} = \overline{E_{\ell-1}\partial f} + k\overline{E_{\ell+1} f} \tag{A.3.3.17}$$

for all $\overline{f} \in \overline{M}_k(1)$, so that θ now preserves modular forms modulo ℓ, and is actually a homogeneous operator of degree 2 on $\overline{M}$.

A graded element $\overline{f}$ of $\overline{M}$ is the sum of reductions modulo ℓ of forms whose weights all agree modulo $\ell - 1$. Multiplying these forms with powers of $E_{\ell-1}$, I can arrange for all of their weights to be equal, so that $\overline{f}$ is the reduction modulo ℓ of a modular form $f \in M_k^{(\ell)}(1)$ whose weight $k \in \mathbb{N}$ reduces modulo $\ell - 1$ to the graduation of $\overline{f}$. The minimal such k is called the *filtration* of $\overline{f}$, and is denoted by $w(\overline{f}) \in \mathbb{N}$. Equation (A.3.3.17) above hints at how the operator θ changes the filtration:

Lemma A.3.3.18. *For every graded element $\overline{f}$ of $\overline{M}$, one has $w(\theta\overline{f}) \leqslant w(\overline{f}) + \ell + 1$, with equality unless $\ell \mid w(\overline{f})$.*

Proof. The first part is clear form equation (A.3.3.17). The second part comes from the fact that the filtration can drop only by getting rid of the $E_{\ell+1}$-part in (A.3.3.17), which can only happen if $k \equiv 0 \bmod \ell$; cf. [Swi72, lemma 5 (ii)] for the details. □

Using this, one can bound effectively the possible exceptional values of ℓ for each of the three cases listed above in corollary A.3.3.14.

Theorem A.3.3.19. *The cases listed in corollary A.3.3.14 can only occur, respectively, if*

(i) $\ell < k_f$ *or* ℓ *divides the numerator of the Bernoulli number* b_{k_f},

(ii) $\ell < 2k_f$,

(iii) for all primes $p \neq \ell$, ℓ *divides either* a_p^2, $a_p^2 - p^{k_f-1}$, $a_p^2 - 2p^{k_f-1}$ *or* $a_p^2 - 4p^{k_f-1}$.

Proof. (i) Possibly after swapping a and $b = k_f - 1 - a$, one is in the situation where there exist integers a and b such that $0 \leqslant a < b < \ell - 1$, $a + b = k_f$, and the q-expansion coefficients a_n of f satisfy

$$\forall n \in \mathbb{N} \text{ prime to } \ell, a_n \equiv n^a \sigma_{b-a}(n) \bmod \ell.$$

This can be rewritten as

$$\theta\overline{f} = \theta^{a+1}\overline{F_{b-a+1}},$$

where an extra θ has been applied on both sides in order to kill the terms whose rank is divisible by ℓ; however, the case $a = 0$, $b = \ell - 2$ must be treated separately since $F_{\ell-1}$ is not ℓ-integral. Now the left hand side has filtration at most $k_f + \ell + 1$ by lemma A.3.3.18; on the other hand, $\overline{F_{b-a+1}}$ clearly has filtration $b - a + 1$, and if $b - a > 1$ one sees by induction on $i \leqslant a + 1$ that the filtration of $\theta^i\overline{F_{b-a+1}}$ is exactly $b - a + 1 + i(\ell + 1)$ because one is in the case of

equality in lemma A.3.3.18 every time. Therefore, leaving the case $b-a=1$ aside,

$$k_f+\ell+1 \geqslant b-a+1+(a+1)(\ell+1),$$

hence $b+a\ell+1 \leqslant k_f$. Assume now that $\ell > k_f$ on the top of that. Then this forces $a=0$, whence

$$\theta\overline{f} = \theta\overline{F_{k_f}}.$$

If $\overline{f}$ and $\overline{F_{k_f}}$ did not agree, then $\overline{f}-\overline{F_{k_f}}$ would have filtration k_f, whence

$$0 = w(0) = w\big(\theta(\overline{f}-\overline{F_{k_f}})\big) = k+\ell+1$$

by lemma A.3.3.18, which is impossible. So f and F_{k_f} agree modulo ℓ, and in particular F_{k_f} has no constant term modulo ℓ, so that ℓ divides the numerator of b_{k_f}. The special cases $b-a=\ell-2$ and $b-a=1$ are dealt with similarly.

(ii) In this case, one has similarly

$$\theta\overline{f} = \theta^{\frac{\ell+1}{2}}\overline{f}.$$

If $\ell > 2k_f$, then $w(\overline{f}) = k_f$ and hence $w(\theta^i\overline{f}) = k_f+i(\ell+1)$ for $i \leqslant \frac{\ell+1}{2}$ by induction since one is every time in the case of equality of lemma A.3.3.18. Comparing weights on both sides then yields

$$k_f+\ell+1 = k_f+\frac{\ell+1}{2}(\ell+1),$$

which is impossible.

(iii) is immediate.

□

This yields a decision process to determine and test all possible exceptional primes ℓ of kind (i) and (ii) for each newform f of level 1 with rational coefficients: test the finitely many possible exceptional values of ℓ, and use the Sturm bound A.2.2.31 to prove an exceptional congruence $\theta\overline{f} = \theta^{a+1}\overline{F_{b-a+1}}$ or $\theta\overline{f} = \theta^{\frac{\ell+1}{2}}\overline{f}$ whenever suspected. On the other hand, exceptional primes of type (iii) are not harder to detect but are harder to prove, since they cannot be translated in terms of the θ operator, so that the Sturm bound does not apply.

Example A.3.3.20. Let me apply this to $f=\Delta$ for instance. Since $k_f=12$,

(i) can only occur for $\ell < 12$ or $\ell = 691$ since $b_{12} = -\frac{691}{2730}$. The Ramanujan congruences for $\tau(n)$ show that the values $\ell = 2,3,5,7$ and 691 are indeed exceptional of this type. On the other hand, $\ell=11$ is not exceptional of type (i), since $\tau(2) = -24$ and there exists no $0 \leqslant a < 6$ such that $2^a + 2^{11-a}$ is congruent to -24 mod 11.

(ii) can only occur for $\ell < 24$. It actually does not for $\ell = 2,3,5,7$ since these are exceptional of type (i) as shown just above, which is incompatible with type (ii). On the other hand, the Ramanujan congruence for $\tau(n)$ modulo 23 shows that $\ell=23$ is indeed exceptional of type (ii). In order to rule out $\ell = 13, 17$ or 19, it suffices to find for each of those ℓ a prime p such that $(\frac{p}{\ell}) = -1$ and $\ell \nmid \tau(p)$. One can take $p=2$ for $\ell = 11$ and 19, and $p=3$ for $\ell = 13$.

f	k_f	Exceptional primes of type (i)	Exceptional primes of type (ii)	Exceptional primes of type (iii)
Δ	12	2, 3, 5, 7, 691	23	-
$E_4\Delta$	16	2, 3, 5, 7, 11, 3617	31	59
$E_6\Delta$	18	2, 3, 5, 7, 11, 13, 43867	-	-
$E_8\Delta$	20	2, 3, 5, 7, 11, 13, 283, 617	-	-
$E_{10}\Delta$	22	2, 3, 5, 7, 13, 17, 131, 593	-	-
$E_{14}\Delta$	26	2, 3, 5, 7, 11, 17, 19, 657931	-	-

Table A.3.3.21: The exceptional primes for the rational newforms of level 1

(iii) Taking $p = 2$ and examining the prime divisors of $\tau(p)^2$, $\tau(p)^2 - p^{11}$, $\tau(p)^2 - 2p^{11}$ and $\tau(p)^2 - 4p^{11}$, one sees that this case can only occur for $\ell = 2, 3, 5, 7, 11, 17$, or 23. Similarly, taking $p = 3$ reveals that this case can only occur for $\ell = 2, 3, 5, 7, 11, 23, 61, 181$, or 359. Taking the intersection, the only possibilities left are $\ell = 2, 3, 5, 7, 11$, or 23, which have already been seen to be of kind (i) or (ii).

Applying this process to all the newforms of level 1 with rational coefficients leads to table A.3.3.21.

Remark A.3.3.22. Fortunately, it turns out that there is only one exceptional prime of type (iii), namely $\ell = 59$ for $E_4\Delta$. P. Swinnerton-Dyer detected it and conjectured that it was exceptional of type (iii) in [Swi72], and this was proved a few years later by K. Haberland (cf. [Hab83, Kapitel 3]).

I can now explain what I meant when I claimed that, unlike for Eisenstein series, there is no simple formula for the coefficients a_n of cuspforms: the Galois representations attached to them generally have non-abelian images, so that the coefficients a_n cannot be computed by using class field theory in the number fields cut out by these representations. On the contrary, it is possible to construct Galois representations attached to Eisenstein series as direct sums of Galois characters. These representations are then reducible and have abelian image, so that class field theory should be able to express the coefficients of Eisenstein series with characters, and indeed the formulae for coefficients of Eisenstein series are based on characters, as I demonstrated in section A.2.2.3.

A.3.3.3 Geometric realisation

Even though there are no such closed formulae for the coefficients a_n of cuspforms, it is still possible to compute these coefficients. One possible approach consists in using modular symbols, as demonstrated in section A.2.3 (cf. example A.2.3.12). Another approach, originally due to J.-M. Couveignes and B. Edixhoven (cf. [CE11]) and which is the central topic of this thesis, is to use the Galois representations attached to newforms, and especially the fact that they allow to recover the coefficient a_p of a newform for p prime as the trace of the image of the Frobenius element Frob_p. One can then deduce the coefficients a_n of this newform thanks to the multiplicativity

relations (A.2.2.20), and hence compute the coefficients a_n of any cuspform by expressing it as a linear combination of forms directly related to newforms of possibly lower level as in (A.2.2.28).

In order to compute such Galois representations, I need to describe them more explicitly so as to get a computational grasp on them, and this is what I shall now do. More precisely, I shall sketch a construction of G. Shimura's (cf. [Shi71, chapter 7]) which corresponds to the case of weight $k = 2$ of theorem A.3.3.3. This construction was later generalised to higher weights by P. Deligne as he proved theorem A.3.3.3, but this generalisation uses advanced algebraic geometry techniques which are not well-suited for computational purposes. On the other hand, the case $k = 2$ is easier to handle thanks to the relationship between the space $S_2(\Gamma)$ of cuspforms of weight 2 and the modular jacobian $\mathrm{Jac}\big(X(\Gamma)\big) = S_2(\Gamma)^\vee / H_1\big(X(\Gamma), \mathbb{Z}\big)$. As a consequence, I shall first sketch Shimura's construction in weight $k = 2$ in elementary terms, and then show how to adapt it to higher weights. The price of this is that I shall only show how to construct the mod ℓ Galois representations attached to higher-weight newforms, instead of the ℓ-adic ones.

The case of weight $k = 2$

To be precise, I shall now sketch the proof of the following theorem:

Theorem A.3.3.23. *Let $f = q + \sum_{n \geqslant 2} a_n q^n \in S_2\big(\Gamma_1(N)\big)$ be a newform of weight 2, let $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ be the number field spanned by its q-expansion coefficients, and let $\mathfrak{l}$ be a prime of degree 1 of K_f lying over a prime $\ell \in \mathbb{N}$ which is prime to the level N and such that the mod $\mathfrak{l}$ Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ attached to $f \bmod \mathfrak{l}$ is not exceptional (that is to say such that its image contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$). Denote by*

$$\overline{\lambda}_{f,\mathfrak{l}} \colon \mathbb{T} \longrightarrow \mathbb{Z}_{K_f} \twoheadrightarrow \mathbb{F}_\mathfrak{l} \simeq \mathbb{F}_\ell$$

the mod $\mathfrak{l}$ eigenvalue system of f, that is to say the ring morphism mapping the Hecke operator T_n to $a_n \bmod \mathfrak{l}$ for all $n \in \mathbb{N}$, where $\mathbb{T} = \mathbb{T}_{2,N}$ is the Hecke algebra of weight 2 and level $\Gamma_1(N)$. Then the $\mathbb{F}_\ell$-subspace

$$V_{f,\mathfrak{l}} = \bigcap_{T \in \mathbb{T}} \mathrm{Ker}\,\big(T - \overline{\lambda}_{f,\mathfrak{l}}(T)\big)_{|J_1(N)[\ell]}$$

of the ℓ-torsion $J_1(N)[\ell]$ of the jacobian $J_1(N)$ of the modular curve $X_1(N)$ is of dimension 2 over $\mathbb{F}_\ell$, is stable under Galois, and the Galois action on its points yields a mod ℓ Galois representation

$$\overline{\rho} \colon G_\mathbb{Q} \longrightarrow \mathrm{GL}(V_{f,\mathfrak{l}}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

which is isomorphic to $\overline{\rho}_{f,\mathfrak{l}}$.

The proof follows the same lines as the study A.3.1.11 of the Galois representation afforded by the torsion of an elliptic curve. The idea is the following (cf. [DDT95, sections 1.6 and 1.7]).

Let $\Lambda = H_1\big(X_1(N), \mathbb{Z}\big)$. As explained in remark A.2.3.13, the involution $\tau \mapsto -\overline{\tau}$ of $\mathcal{H}^\bullet$ induces an involution on Λ and hence splits Λ into two eigen sublattices Λ^+

and Λ^- (note that $\Lambda^+ \oplus \Lambda^-$ will not in general be the whole of Λ, but merely a sublattice of finite index). Then the $\mathbb{Q}$-vector spaces $\Lambda^\pm \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ are both isomorphic as $\mathbb{T}$-modules to $\mathrm{Hom}_{\mathbb{Q}}\big(S_2(\Gamma_1(N),\mathbb{Q}),\mathbb{Q}\big)$, which is a free $\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$-module of rank one by lemma A.2.2.30, where $S_2\big(\Gamma_1(N),\mathbb{Q}\big) = S_2\big(\Gamma_1(N),\mathbb{Z}\big) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$. Therefore $\Lambda \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ is a free $\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$-module of rank 2.

Let now

$$\mathrm{Ta}_\ell\, J_1(N) = \varprojlim_{n\in\mathbb{N}} J_1(N)[\ell^n]$$

be the *Tate module* of $J_1(N)$, where the transition maps are the multiplication by ℓ, and let $V_\ell J_1(N) = \big(\mathrm{Ta}_\ell\, J_1(N)\big) \underset{\mathbb{Z}}{\otimes} \mathbb{Q} = \big(\mathrm{Ta}_\ell\, J_1(N)\big) \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell$. Since $J_1(N)[\ell^n] = \frac{1}{\ell^n}\Lambda/\Lambda$ by the analytic construction of the jacobian (cf. section A.1.2), the above shows that $V_\ell J_1(N)$ is a free $\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell$-module of rank 2. Since $J_1(N)$ is an abelian variety over $\mathbb{Q}$ and since the action of the Hecke operators $T \in \mathbb{T}$ on $J_1(N)$ is also defined over $\mathbb{Q}$, the Galois action commutes with the group law of $J_1(N)$ and with the Hecke action, and thus yields a Galois representation

$$\rho_{N,\ell}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\mathbb{T}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}_\ell}\big(V_\ell J_1(N)\big) \simeq \mathrm{GL}_2\big(\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell\big).$$

Let $p \nmid \ell N$ be a prime number, and let $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ be a Frobenius element at p. I shall now prove that $\rho_{N,\ell}$ is unramified at p and that the characteristic polynomial of $\rho_{N,\ell}(\mathrm{Frob}_p)$ is

$$X^2 - T_p X + p\langle p\rangle \in \big(\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell\big)[X].$$

For all $n \in \mathbb{N}$, the right morphism on the commutative diagram

$$\begin{array}{ccc} D_p & \longrightarrow & \mathrm{Aut}\big(J_1(N)[\ell^n]\big) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \longrightarrow & \mathrm{Aut}\big(J_1(N)_{\mathbb{F}_p}[\ell^n]\big) \end{array} \tag{A.3.3.24}$$

is injective by theorem A.3.1.10, so the image of an element $\sigma \in D_p$ in $\mathrm{Aut}(E[\ell])$ depends only on its image in $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, which proves that $\rho_{N,\ell}$ is unramified at p. Besides, the Eichler-Shimura relation A.2.1.20 says that $\overline{T_p} = \sigma_p + p\overline{\langle p\rangle}\sigma_p^{-1}$ holds in $\mathrm{End}\big(J_1(N)_{\mathbb{F}_p}[\ell^n]\big)$, where σ_p denotes the Frobenius automorphism $x \mapsto x^p$ in characteristic p. Multiplying by σ_p, one finds that σ_p satisfies the relation

$$\sigma_p^2 - \overline{T_p}\sigma_p + p\overline{\langle p\rangle} = 0$$

on $J_1(N)_{\mathbb{F}_p}[\ell^n]$, so Frob_p satisfies the relation

$$\mathrm{Frob}_p^2 - T_p\,\mathrm{Frob}_p + p\langle p\rangle = 0$$

on $J_1(N)[\ell^n]$ since the right morphism on (A.3.3.24) is injective, and hence on $V_\ell J_1(N)$ since $n \in \mathbb{N}$ is arbitrary.

In order to prove that this is the characteristic polynomial of $\rho_{N,\ell}(\mathrm{Frob}_p)$, it suffices to show that the trace of $\rho_{N,\ell}(\mathrm{Frob}_p)$ is T_p. In the beginning of section A.2.1.2,

I constructed the Weil pairing on an elliptic curve, but a similar construction exists on any jacobian, yielding in the present case a Galois-equivariant non-degenerate alternate $\mathbb{Z}/m\mathbb{Z}$-pairing

$$\langle \cdot, \cdot \rangle \colon J_1(N)[m] \wedge J_1(N)[m] \longrightarrow \mu_m$$

for all $m \in \mathbb{N}$. Taking $m = \ell^n$, $n \in \mathbb{N}$, and passing to the limit yields a non-degenerate alternate $\mathbb{Z}_\ell$-pairing

$$\langle \cdot, \cdot \rangle \colon \operatorname{Ta}_\ell J_1(N) \wedge \operatorname{Ta}_\ell J_1(N) \longrightarrow \varprojlim_{n \in \mathbb{N}} \mu_{\ell^n} \simeq \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/\ell^n\mathbb{Z} = \mathbb{Z}_\ell$$

which one extends into a non-degenerate alternate $\mathbb{Q}_\ell$-pairing

$$\langle \cdot, \cdot \rangle \colon V_\ell J_1(N) \wedge V_\ell J_1(N) \longrightarrow \mathbb{Q}_\ell.$$

I mentioned in remark A.2.2.19 that the adjoint of a Hecke operator $T \in \mathbb{T}$ with respect to the Petersson inner product is $W_N T W_N$, and one can show by a proof following the same lines that $W_N T W_N$ is also the adjoint of T with respect to the Weil pairing. Therefore, the pairing

$$[\cdot, \cdot] = \langle \cdot, W_N \cdot \rangle \colon V_\ell J_1(N) \wedge V_\ell J_1(N) \longrightarrow \mathbb{Q}_\ell$$

is a perfect $\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell$-bilinear pairing, so that one has a $\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell$-linear isomorphism

$$\begin{array}{ccc} V_\ell J_1(N) & \longrightarrow & \big(V_\ell J_1(N)\big)^\vee = \operatorname{Hom}_{\mathbb{Q}_\ell}\big(V_\ell J_1(N), \mathbb{Q}_\ell\big) \\ x & \longmapsto & [x, \cdot]. \end{array}$$

It is a general property of the Weil pairing that the adjoint of an isogeny ϕ is the dual isogeny $\widehat{\phi}$. In particular, the adjoint of σ_p on $J_1(N)_{\mathbb{F}_p}$ is $\widehat{\sigma_p} = p\sigma_p^{-1}$, so by theorem A.3.1.10 the adjoint of Frob_p with respect to the Weil pairing $\langle \cdot, \cdot \rangle$ on $V_\ell J_1(N)$ is $p \operatorname{Frob}_p^{-1}$, and hence the adjoint of Frob_p with respect to the modified pairing $[\cdot, \cdot]$ is $pW_N \operatorname{Frob}_p^{-1} W_N$. Since W_N acts on $X_1(N)$ by $(E, P) \mapsto (E/\langle P \rangle, Q + \langle P \rangle)$ where $Q \in E[N]$ is such that the Weil pairing of P and Q on E is a fixed primitive N^{th} root of 1, and since Frob_p raises roots of 1 to the p, one sees that $W_N \operatorname{Frob}_p^{-1} W_N(E, P) = \big(E^{\operatorname{Frob}_p^{-1}}, p \operatorname{Frob}_p^{-1}(P)\big)$, that is to say $W_N \operatorname{Frob}_p^{-1} W_N = \langle p \rangle \operatorname{Frob}_p^{-1}$. It follows that the trace of Frob_p on $V_\ell J_1(N)$ is the same as the trace of $\phi \mapsto \phi \circ (p\langle p \rangle \operatorname{Frob}_p^{-1})$ on $\big(V_\ell J_1(N)\big)^\vee$, whence

$$2 \operatorname{tr} \operatorname{Frob}_p = \operatorname{tr} \operatorname{Frob}_p + \operatorname{tr}(p\langle p \rangle \operatorname{Frob}_p^{-1}) = \operatorname{tr} T_p = 2T_p,$$

where the middle equality stems again from the Eichler-Shimura relation A.2.1.20. This proves that the characteristic polynomial of $\rho_{N,\ell}(\operatorname{Frob}_p)$ is

$$X^2 - T_p X + p\langle p \rangle \in \big(\mathbb{T} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell\big)[X]$$

as announced.

Consider now the annihilator I_f of f in $\mathbb{T}$,

$$I_f = \{T \in \mathbb{T} \mid Tf = 0\},$$

and let $A_f = J_1(N)/I_f$. This is an abelian veriety over $\mathbb{Q}$ of dimension $d = [K_f : \mathbb{Q}]$, which can be described analytically as

$$A_f = S_f^\vee / \Lambda_f,$$

where

$$S_f = \bigoplus_{\sigma\colon K_f \hookrightarrow \overline{\mathbb{Q}}} \mathbb{C} f^\sigma \subset S_2\big(\Gamma_1(N)\big)$$

is the subspace of $S_2\big(\Gamma_1(N)\big)$ spanned over $\mathbb{C}$ by the Galois conjugates of f, and $\Lambda_f = \Lambda / I_f \Lambda$ is the lattice of $S_f^\vee = \mathrm{Hom}_{\mathbb{C}}(S_f, \mathbb{C})$ formed by the periods

$$\int_\gamma, \quad \gamma \in H_1\big(X_1(N), \mathbb{Z}\big).$$

Remark A.3.3.25. By using the decomposition (A.2.2.28) of $S_2\big(\Gamma_1(N)\big)$, one can show that $J_1(N)$ is isogenous to the product

$$\prod_{[f]} A_f^{\sigma_0(N/N_f)},$$

where the product ranges over the $G_{\mathbb{Q}}$-orbits $[f]$ of newforms f of level $N_f | N$, and where $\sigma_0(n)$ denotes the number of positive divisors of n.

By construction, $\mathrm{End}(A_f) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ contains K_f, and a_n acts on A_f as T_n; in particular $\varepsilon(d)$ acts on A_f as $\langle d \rangle$, where ε denotes the nebentypus of f. In other words, the action of $\mathbb{T}$ on A_f factors exactly through I_f, so it follows from the above that

$$V_\ell A_f \overset{\text{def}}{=} (\mathrm{Ta}_\ell\, A_f) \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell \overset{\text{def}}{=} \left(\varprojlim_{n \in \mathbb{N}} A_f[\ell^n] \right) \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell$$

is free of rank 2 over $K_f \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_\ell \simeq \prod_{\mathfrak{l}_i | \ell} K_{f,\mathfrak{l}_i}$, where $K_{f,\mathfrak{l}_i}$ denotes the $\mathfrak{l}_i$-adic completion of K_f and the $\mathfrak{l}_i$ are the primes of K_f lying above ℓ. Therefore, the Galois action on $V_\ell A_f$ yields a Galois representation

$$\rho_{[f],\ell}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2\left(K_f \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_\ell\right) \simeq \prod_{\mathfrak{l}_i | \ell} \mathrm{GL}_2(K_{f,\mathfrak{l}_i})$$

which is unramified at $p \nmid \ell N$ and such that the characteristic polynomial of the image of Frob_p is

$$X^2 - a_p X + p\varepsilon(p) \in \big(K_f \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_\ell\big)[X].$$

In particular, by considering the ℓ-torsion instead of the Tate module, one sees that the Galois action yields a Galois representation

$$\overline{\rho}_{[f],\ell}\colon G_{\mathbb{Q}} \longrightarrow \prod_{\mathfrak{l}_i | \ell} \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}_i})$$

which is unramified at $p \nmid \ell N$ and such that the characteristic polynomial of the image of Frob_p is

$$X^2 - a_p X + p\varepsilon(p) \in \big(\prod_{\mathfrak{l}_i \mid \ell} \mathbb{F}_{\mathfrak{l}_i}\big)[X].$$

Taking the $\overline{\lambda}_{f,\mathfrak{l}}$ eigen subspace of $J_1(N)[\ell]$ amounts to selecting the factor of $\overline{\rho}_{[f],\ell}$ corresponding to f and $\mathfrak{l}$. As the level N was assumed to be prime to ℓ (note that this is the only place where I use this hypothesis in this whole construction of $\overline{\rho}_{f,\mathfrak{l}}$), and since $\overline{\rho}_{f,\mathfrak{l}}$ is irreducible over $\overline{\mathbb{F}_\ell}$ as $\mathfrak{l}$ is not an exceptional prime for f by assumption, [Edi92, theorem 9.2] ensures that $V_{f,\mathfrak{l}}$ is of dimension 2 over $\mathbb{F}_{\mathfrak{l}} \simeq \mathbb{F}_\ell$. As a consequence, the Galois action on it yields a mod ℓ Galois representation $\overline{\rho}$ whose semi-simplification over $\overline{\mathbb{F}_\ell}$ is, by the Brauer-Nesbitt theorem A.3.1.5 and the Cebotarev density theorem, isomorphic to the one of $\overline{\rho}_{f,\mathfrak{l}}$. But since $\overline{\rho}_{f,\mathfrak{l}}$ is irreducible over $\overline{\mathbb{F}_\ell}$, it is equal to its own semi-simplification, and so $\overline{\rho}$ is irreducible and is isomorphic to $\overline{\rho}_{f,\mathfrak{l}}$ as claimed.

The case of higher weight

I shall now explain how the above construction of the mod $\mathfrak{l}$ representation attached to a newform of weight 2 can be extended to newforms of higher weight. More precisely, I shall prove the following result:

Theorem A.3.3.26. *Let $f = q + \sum_{n \geqslant 2} a_n q^n \in S_k(N, \varepsilon)$ be a newform of even weight $k \geqslant 4$ and of level $N \neq 3, 4$, let $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ be the number field spanned by its q-expansion coefficients, and let $\mathfrak{l}$ be prime of degree 1 of K_f such that the mod $\mathfrak{l}$ Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ attached to $f \bmod \mathfrak{l}$ is not exceptional (that is to say such that its image contains $\mathrm{SL}_2(\mathbb{F}_{\mathfrak{l}})$), that $k < \ell$, and that N is prime to ℓ, where $\ell \in \mathbb{N}$ is the prime lying below $\mathfrak{l}$. Denote by*

$$\overline{\lambda}_{f,\mathfrak{l}} \colon \mathbb{T} \longrightarrow \mathbb{Z}_{K_f} \twoheadrightarrow \mathbb{F}_{\mathfrak{l}} \simeq \mathbb{F}_\ell$$

the mod $\mathfrak{l}$ eigenvalue system of f, that is to say the ring morphism mapping the Hecke operator T_n to $a_n \bmod \mathfrak{l}$ for all $n \in \mathbb{N}$, where $\mathbb{T} = \mathbb{T}_{k,N}$ is the Hecke algebra of weight k and level $\Gamma_1(N)$. Consider the $\mathbb{F}_\ell$-subspace

$$V_{f,\mathfrak{l}} = \bigcap_{n=1}^{+\infty} \mathrm{Ker}\left(T_n^{(2,\ell N)} - \overline{\lambda}_{f,\mathfrak{l}}(T_n^{(k,N)})\right)_{|J_1(\ell N)[\ell]}$$

of the ℓ-torsion $J_1(\ell N)[\ell]$ of the jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$, where $T_n^{(w,M)}$ denotes the Hecke operator T_n in weight w and level M. Then $V_{f,\mathfrak{l}}$ is of dimension 2 over $\mathbb{F}_\ell$, is stable under Galois, and the Galois action on its points yields a mod ℓ Galois representation

$$\overline{\rho} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V_{f,\mathfrak{l}}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

which is isomorphic to $\overline{\rho}_{f,\mathfrak{l}}$.

Note that this time I am looking for $\overline{\rho}_{f,\mathfrak{l}}$ in the ℓ-torsion of $J_1(\ell N)$ instead of $J_1(N)$. The reason for this is the following result of B. Gross's (cf. [Gro90, theorem 9.3.2]), which roughly says that I can find a newform f_2 of weight 2 but of higher level ℓN which is congruent to f modulo ℓ:

Proposition A.3.3.27. *Let f be a newform of even weight $k \geqslant 4$ and level $N \neq 3, 4$, let $\mathfrak{l}$ be a prime of the number field $K_f = \mathbb{Q}(a_n, n \geqslant 2)$ spanned by its q-expansion coefficients, and fix an embedding $\sigma\colon \mathbb{F}_{\mathfrak{l}} \hookrightarrow \overline{\mathbb{F}_\ell}$ of $\mathbb{F}_{\mathfrak{l}}$ into a fixed algebraic closure $\overline{\mathbb{F}_\ell}$ of $\mathbb{F}_\ell$. If $k < \ell$ and if N is prime to the prime number $\ell \in \mathbb{N}$ lying below $\mathfrak{l}$, then there exists a newform f_2 of weight 2, level ℓN and nebentypus ε_2, a prime $\mathfrak{l}_2$ of $K_{f_2} = \mathbb{Q}(a_n, n \geqslant 2)$, and an embedding $\sigma_2\colon \mathbb{F}_{\mathfrak{l}_2} \hookrightarrow \overline{\mathbb{F}_\ell}$ such that*

$$\sigma\big(a_n(f) \bmod \mathfrak{l}\big) = \sigma_2\big(a_n(f_2) \bmod \mathfrak{l}_2\big)$$

for all $n \in \mathbb{N}$ and that

$$\sigma_2\big(\varepsilon_2(n) \bmod \mathfrak{l}_2\big) = \sigma\big(n^{k-2}\varepsilon(n) \bmod \mathfrak{l}\big)$$

for all $n \in \mathbb{Z}$.

Let $(f_2, \mathfrak{l}_2)$ be such data corresponding to f and $\mathfrak{l}$ (there is no choice for the embeddings σ as $\mathfrak{l}$ is of degree 1), so that $\overline{\lambda}_{f,\mathfrak{l}}(T_n^{(k,N)}) = a_n(f) \bmod \mathfrak{l} = a_n(f_2) \bmod \mathfrak{l}_2 = \lambda_{f_2,\mathfrak{l}_2}(T_n^{(2,\ell N)})$ for all $n \in \mathbb{N}$, whence

$$\begin{aligned} V_{f,\mathfrak{l}} &= \bigcap_{n=1}^{+\infty} \mathrm{Ker}\left(T_n^{(2,\ell N)} - \overline{\lambda}_{f,\mathfrak{l}}(T_n^{(k,N)})\right)_{|J_1(\ell N)[\ell]} \\ &= \bigcap_{n=1}^{+\infty} \mathrm{Ker}\left(T_n^{(2,\ell N)} - \overline{\lambda}_{f_2,\mathfrak{l}_2}(T_n^{(2,\ell N)})\right)_{|J_1(\ell N)[\ell]} \quad = \quad V_{f_2,\mathfrak{l}_2}. \end{aligned}$$

Although the level ℓN is obviously no longer prime to ℓ, [Edi92, theorem 9.2] still applies thanks to the hypothesis $k < \ell$, and ensures that $V_{f,\mathfrak{l}}$ is of dimension 2 over $\mathbb{F}_\ell$. By the very same reasoning as in the case of weight $k = 2$, one then sees that $V_{f,\mathfrak{l}}$ is invariant under Galois, and moreover that the Galois action on it affords the mod $\mathfrak{l}_2$ Galois representation $\overline{\rho}_{f_2,\mathfrak{l}_2}$ attached to f_2 mod $\mathfrak{l}_2$. In particular, for all $p \nmid \ell N$, this representation is unramified at p, and the characteristic polynomial of the image of Frob_p is

$$X^2 - a_p(f_2)X + p\varepsilon_2(p) \in \mathbb{F}_{\mathfrak{l}_2}[X].$$

The relation between ε_2 and ε implies that it may be rewritten as

$$X^2 - a_p(f)X + p^{k-1}\varepsilon(p) \in \mathbb{F}_{\mathfrak{l}}[X],$$

which is the characteristic polynomial of the image of Frob_p by $\overline{\rho}_{f,\mathfrak{l}}$. The Cebotarev density theorem and the Brauer-Nesbitt theorem A.3.1.5 then imply that $\overline{\rho}_{f,\mathfrak{l}}$, which is irreducible and *a fortiori* semi-simple over $\overline{\mathbb{F}_\ell}$ by hypothesis on $\mathfrak{l}$, is isomorphic to the semi-simplification of $\overline{\rho}_{f_2,\mathfrak{l}_2}$. Therefore, $\overline{\rho}_{f_2,\mathfrak{l}_2}$ is irreducible, hence semi-simple, and so $\overline{\rho}_{f_2,\mathfrak{l}_2}$ and $\overline{\rho}_{f,\mathfrak{l}}$ are isomorphic and the proof of theorem A.3.3.26 is complete.

Remark A.3.3.28. There is no need to actually compute the newform f_2 of weight 2 at any point; its mere existence is enough to justify the above construction A.3.3.26.

A.3.4 The Serre conjecture

As I have illustrated in section A.3.3.2, the mod ℓ Galois representation $\overline{\rho}_{f,\mathfrak{l}}$ attached to a newform $f \in S_k(N,\varepsilon)$ is usually[14] irreducible. It is moreover odd, which means that $\det \overline{\rho}_{f,\mathfrak{l}}(c) = -1$ for all $c \in G_{\mathbb{Q}}$ corresponding to the complex conjugation for some embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$. Indeed, $\det \overline{\rho}_{f,\mathfrak{l}}(c) = \overline{\chi}_\ell(c)^{k-1}\varepsilon(c) = -1$ since k and ε must have the same parity (cf. remark A.2.2.14).

In a famous 1987 article [Ser87], J.-P. Serre conversely conjectured that **every** irreducible and odd mod ℓ Galois representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

is modular, that is to say is isomorphic to $\overline{\rho}_{f,\mathfrak{l}}$ for some newform f and some prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ. Even better, he gave recipes to compute from ρ a weight k_ρ, a level N_ρ and a nebentypus ε_ρ such that there should exist a newform $f \in S_{k_\rho}(N_\rho,\varepsilon_\rho)$ such that $\rho \sim \overline{\rho}_{f,\mathfrak{l}}$ for some $\mathfrak{l}$. I describe these recipes in detail below.

In 2009, C. Khare and J.-P. Wintenberger managed to prove Serre's conjecture, cf. [KW09].

A.3.4.1 The level and the nebentypus

I first introduce the *Artin conductor* of a Galois representation ρ, which is a measure of the ramification of this representation. The level N_ρ attached to ρ by Serre will be a slight modification of the Artin conductor $N(\rho)$ of ρ.

Definition A.3.4.1. Let V be a finite-dimensional vector space over a field F, and

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V)$$

be a Galois representation with finite image. For each prime $p \in \mathbb{N}$, consider the higher ramification subgroups

$$G_{\mathbb{Q}} \supseteq D_p \supseteq I_p = I_p^{(0)} \supseteq I_p^{(1)} \supseteq I_p^{(2)} \supseteq \cdots$$

corresponding to some prime of the number field cut out by ρ and lying above p, and for each $i \geqslant 0$ let $V_p^{(i)} = V^{\rho(I_p^{(i)})}$ denote the subspace on which the higher inertia subgroup $I_p^{(i)}$ acts trivially, so that there is an increasing filtration

$$V^{\rho(I_p)} = V_p^{(0)} \subseteq V_p^{(1)} \subseteq V_p^{(1)} \subseteq \cdots = V$$

with $V_p^{(i)} = V$ for large i. The *Artin conductor* of the Galois representation ρ is then

$$N(\rho) = \prod_p p^{n(\rho,p)},$$

where the integers $n(\rho,p)$ are defined by

$$n(\rho,p) = \sum_{i=0}^{+\infty} \frac{1}{[I_p\colon I_p^{(i)}]} \operatorname{codim}_V V_p^{(i)}.$$

[14] More precisely, one can show that if f is not CM, that is to say if $f \neq f\otimes\chi$ for every non-trivial Dirichlet character χ, then $\overline{\rho}_{f,\mathfrak{l}}$ is exceptional for finitely many $\mathfrak{l}$. Note that a newform of level 1 is never CM by theorem A.2.2.34.

This sum is actually finite, and it is a deep result of Artin's that its value is an integer. As a consequence, $N(\rho)$ is an integer divisible only by the ramified primes.

Example A.3.4.2. Let $\chi\colon (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow F^*$ be a Dirichlet-like character. It can be seen as a Galois character, by composing it with the canonical morphism

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}(\mu_N)/\mathbb{Q}\right) \simeq (\mathbb{Z}/N\mathbb{Z})^*.$$

Assume furthermore that χ is primitive, that is to say that it does not factor through $(\mathbb{Z}/N'\mathbb{Z})^*$ for any strict divisor N' of N. Then the Artin conductor $N(\chi)$ of χ seen as a Galois character is equal to N. In other words, the conductor of a Dirichlet character is the same as the Artin conductor of the corresponding Galois character.

To see this, write $N = \prod_p p^{n_p}$, and see χ as a character on

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_\infty)/\mathbb{Q}\right) \simeq \prod_p \mathbb{Z}_p.$$

Then, since χ is primitive, for each p, χ is trivial on $1 + p^n\mathbb{Z}_p \subset \mathbb{Z}_p$ if and only if $n \geqslant n_p$, which by example A.3.1.1 means that χ is trivial on $I_p^{(i)}$ if and only if $i \geqslant p^{n_p-1}$. Therefore, one finds that

$$n(\chi, p) = \sum_{i=0}^{+\infty} \frac{1}{[I_p\colon I_p^{(i)}]} \mathrm{codim}_F F^{I_p^{(i)}} = \sum_{0\leqslant i<p^{n_p-1}} \frac{1}{[I_p\colon I_p^{(i)}]},$$

which is 0 if $n_p = 0$, and which is

$$1 + \sum_{n=0}^{n_p-2} \sum_{p^n\leqslant i<p^{n+1}} \frac{1}{(p-1)p^n} = 1 + \sum_{n=0}^{n_p-2} 1 = n_p$$

else. Thus $n(\chi, p) = n_p$ in each case, whence $N(\chi) = N$.

Back to the case of a Galois representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell),$$

the level N_ρ is defined to be the *Artin conductor* $N(\rho)$ of ρ stripped from its ℓ-part, in other words

$$N_\rho = \prod_{p\neq\ell} p^{n(\rho,p)}.$$

Example A.3.4.3. In particular, a representation ρ which is ramified only at ℓ comes from a form of level $N_\rho = 1$.

Clearly, the Artin conductor of the Galois character $\det\rho$ divides the one of ρ. Besides, $\det\rho$ is at most tamely ramified at ℓ, since its image, being a finite subgroup of $\overline{\mathbb{F}}_\ell^*$, is of order prime to ℓ, so that it cuts out a Galois number field of degree prime to ℓ. As a consequence, $n(\det\rho, \ell) \leqslant 1$, so that the Artin conductor $N(\det\rho)$ divides ℓN_ρ. Now $\det\rho$, having an finite abelian image, factors through a finite quotient of $\mathrm{Gal}\left(\mathbb{Q}(\mu_\infty)/\mathbb{Q}\right) \simeq \widehat{\mathbb{Z}}$, hence can be seen as a (not necessarily primitive) character modulo ℓN_ρ according to example A.3.4.2. Since ℓ and N_ρ are coprime, $\det\rho$ can be factored into a product $\chi\varepsilon$, where χ is a character modulo ℓ, thus of the form $x \mapsto x^h$ for some $h \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ upon identification of $(\mathbb{Z}/\ell\mathbb{Z})^*$ with $\mathbb{F}_\ell^*$, and ε is a character modulo N_ρ. The nebentypus ε_ρ is then defined to be this ε.

A.3.4.2 The weight

While the level N_ρ is defined by the ramification of ρ away from ℓ, the weight k_ρ is defined by the ramification behaviour of ρ at ℓ. So let $D_\ell \subset G_\mathbb{Q}$ be the decomposition subgroup corresponding to some place of $\overline{\mathbb{Q}}$ lying above ℓ, and let $\rho_\ell = \rho_{|D_\ell}$ be the restriction of ρ to D_ℓ. Since D_ℓ is canonically isomorphic to the absolute Galois group $G_{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$, I shall identify D_ℓ with $G_{\mathbb{Q}_\ell}$ and regard ρ_ℓ as a representation of $G_{\mathbb{Q}_\ell}$.

Let I_ℓ be the inertia subgroup of D_ℓ, and W_ℓ the wild inertia subgroup. Since W_ℓ is a normal pro-ℓ-group of D_ℓ, the following lemma indicates that the semi-simplification of $\rho_{\ell|I_\ell}$ factors through the tame inertia quotient $I_\ell^{\text{tame}} = I_\ell/W_\ell$.

Lemma A.3.4.4. *Let $\rho\colon G \longrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ be a **semi-simple** continuous representation of a compact group G, and let $H \trianglelefteq G$ be a normal pro-ℓ-subgroup of G. Then ρ is trivial on H.*

Proof. I can assume without loss of generality that ρ is simple. Since G is compact, there exists a finite subextension $\mathbb{F} \subset \overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$ such that the image of ρ is contained in $\mathrm{GL}_n(\mathbb{F})$. Let V^H be the subspace of $V = \mathbb{F}^n$ on which H acts trivially. This subspace is stable under G since H is normal in G, so it is either $\{0\}$ or all V since V is simple. Now

$$\#(V - \{0\}) = \sum_{\Omega \in G\backslash(V-\{0\})} \#\Omega = \#(V^H - \{0\}) + \sum_{i\in I} \#(G/\operatorname{Stab}_G x_i)$$

where $(x_i)_{i\in I}$ is a system of representatives of $G\backslash(V - V^H)$, so $\#(V^H - \{0\}) \neq 0$ since ℓ divides $\sum_{i\in I} \#(G/\operatorname{Stab}_G x_i)$ but not $\#(V - \{0\})$. Therefore $V^H = V$. □

Actually, since I_ℓ^{tame} is abelian, the semi-simplification of $\rho_{\ell|I_\ell}$ is the direct sum $\varphi \oplus \varphi'$ of two tamely ramified characters φ and φ' of I_ℓ. Therefore, up to equivalence, the restriction of ρ_ℓ to the inertia is

$$\rho_{\ell|I_\ell} \sim \begin{bmatrix} \varphi & \xi \\ 0 & \varphi' \end{bmatrix}$$

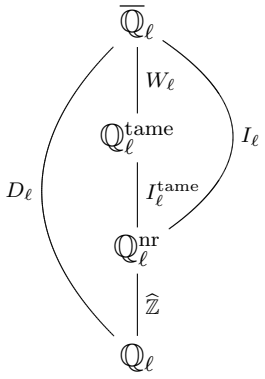
for some function $\xi\colon I_\ell \longrightarrow \overline{\mathbb{F}}_\ell$. Besides,

$$\rho_{\ell|W_\ell} \sim \begin{bmatrix} 1 & \xi \\ 0 & 1 \end{bmatrix}$$

since φ and φ' are tamely ramified, so that $\xi_{|W_\ell}$ is an additive character.

In order to proceed further, one must examine what φ and φ' look like. Fix an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$, and let $\mathbb{Q}_\ell^{\text{nr}}$ and $\mathbb{Q}_\ell^{\text{tame}}$ be respectively the maximal unramified and the maximal tamely ramified subextension of $\mathbb{Q}_\ell$ in $\overline{\mathbb{Q}}_\ell$. One has the

following diagram of Galois groups:



In particular I_ℓ^{tame} identifies canonically with $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{tame}}/\mathbb{Q}_\ell^{\mathrm{nr}})$. Now

$$\mathbb{Q}_\ell^{\mathrm{tame}} = \bigcup_{\substack{n\in\mathbb{N}\\ \gcd(n,\ell)=1}} \mathbb{Q}_\ell^{\mathrm{nr}}(\sqrt[n]{\ell}),$$

and since $\overline{\mathbb{F}}_\ell$ contains the n^{th} roots of 1 for all $n \in \mathbb{N}^*$ prime to ℓ, Kummer theory yields a canonical isomorphism

$$\begin{array}{rccc} \theta_n : & \mathrm{Gal}\left(\mathbb{Q}_\ell^{\mathrm{nr}}(\sqrt[n]{\ell})/\mathbb{Q}_\ell^{\mathrm{nr}}\right) & \xrightarrow{\sim} & \mu_n \\ & \sigma & \longmapsto & \frac{\sigma(\sqrt[n]{\ell})}{\sqrt[n]{\ell}} \end{array},$$

whence an isomorphism

$$\theta\colon I_\ell^{\mathrm{tame}} \xrightarrow{\sim} \varprojlim_{\substack{n\in\mathbb{N}\\ \gcd(n,\ell)=1}} \mu_n,$$

where the transition morphism from μ_{mn} to μ_n consists in raising to the m^{th} power.

Again since $\overline{\mathbb{F}}_\ell^*$ contains the n^{th} roots of 1 for all $n \in \mathbb{N}$ prime to ℓ, one has canonically

$$\mathrm{Hom}\left(\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{nr}}(\sqrt[n]{\ell})/\mathbb{Q}_\ell^{\mathrm{nr}}), \overline{\mathbb{F}}_\ell^*\right) \simeq \mathrm{Hom}(\mu_n, \overline{\mathbb{F}}_\ell^*) \simeq \mathbb{Z}/n\mathbb{Z} \simeq \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$$

for such n, whence a canonical isomorphism

$$\theta^\vee\colon \mathrm{Hom}(I_\ell^{\mathrm{tame}}, \overline{\mathbb{F}}_\ell^*) \xrightarrow{\sim} \bigcup_{\substack{n\in\mathbb{N}\\ \gcd(n,\ell)=1}} \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z} = \mathbb{Z}_{(\ell)}/\mathbb{Z}$$

called the *invariant*, where $\mathbb{Z}_{(\ell)}$ denotes the localisation of $\mathbb{Z}$ at the prime ideal $\ell\mathbb{Z}$.

Example A.3.4.5. The morphisms θ_n defined above for $n \in \mathbb{N}$ prime to ℓ can be seen as $\overline{\mathbb{F}}_\ell^*$-valued characters on I_ℓ^{tame}, of respective invariants $\frac{1}{n}$ mod $\mathbb{Z}$.

Besides, since the integers of the form $\ell^n - 1$, $n \in \mathbb{N}$ are cofinal amongst the integers prime to ℓ ordered by divisibility, one actually has

$$I_\ell^{\mathrm{tame}} \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{F}_{\ell^n}^*,$$

where the transition maps are the relative norms.

Definition A.3.4.6. A character $\chi\colon I_\ell^{\mathrm{tame}} \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{F}_{\ell^n}^* \longrightarrow \mathbb{F}_\ell^*$ is said to be of *level* $n \in \mathbb{N}$ if it factors through $\mathbb{F}_{\ell^n}^*$ but not through $\mathbb{F}_{\ell^m}^*$ for any $m < n$. In other words, χ is of level n if its invariant $\theta^\vee(\chi)$ is of the form $\frac{a}{p^n-1}$ and n is the minimal integer with this property.

For each $m \in \mathbb{N}$, the composition of the projection

$$I_\ell^{\mathrm{tame}} \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{F}_{\ell^n}^* \twoheadrightarrow \mathbb{F}_{\ell^m}^*$$

with the m field embeddings of $\mathbb{F}_{\ell^m}$ into $\overline{\mathbb{F}}_\ell$ yield m characters

$$\theta_{\ell^m-1},\ \theta_{\ell^m-1}^{\ell},\ \theta_{\ell^m-1}^{\ell^2},\ \cdots,\ \theta_{\ell^m-1}^{\ell^{m-1}}$$

from I_ℓ^{tame} to $\overline{\mathbb{F}}_\ell^*$, called the *fundamental characters* of level m. Their respective invariants are

$$\frac{1}{\ell^m-1} \bmod \mathbb{Z},\ \frac{\ell}{\ell^m-1} \bmod \mathbb{Z},\ \frac{\ell^2}{\ell^m-1} \bmod \mathbb{Z},\ \cdots,\ \frac{\ell^{m-1}}{\ell^m-1} \bmod \mathbb{Z}.$$

Example A.3.4.7. The fundamental character $\theta_{\ell-1}$ of level 1 is none other than the restriction to I_ℓ of the mod ℓ cyclotomic character $\overline{\chi}_\ell$. Indeed, letting $\lambda = \sqrt[\ell-1]{\ell}$ be a uniformiser for $K = \mathbb{Q}_\ell^{\mathrm{nr}}(\sqrt[\ell-1]{\ell})$, one has

$$\frac{(1+\lambda T)^\ell - 1}{\lambda\ell} = \frac{(\lambda T)^\ell}{\lambda\ell} + \sum_{i=1}^{\ell-1} \frac{1}{\ell}\binom{\ell}{i}\lambda^{i-1}T^i \equiv T^\ell + T \bmod \lambda,$$

so that by the Hensel lemma K contains the ℓ^{th} roots of 1, which are of the form $\zeta = 1+a\lambda+O(\lambda^2)$ where a is a root of $T^\ell+T$ in $\mathbb{Q}_\ell^{\mathrm{nr}}$. Then, for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_\ell^{\mathrm{nr}})$, one has

$$\sigma(\zeta) = \zeta^{\overline{\chi}_\ell(\sigma)} = 1 + \overline{\chi}_\ell(\sigma)a\lambda + O(\lambda^2)$$

by definition of $\overline{\chi}_\ell$ on the one hand, and

$$\sigma(\zeta) = 1 + a\sigma(\lambda) + O(\lambda^2) = 1 + a\theta_{\ell-1}(\sigma)\lambda + O(\lambda^2)$$

by definition of $\theta_{\ell-1}$ on the other hand.

In particular, the invariant of the mod ℓ cyclotomic character (or rather of its restriction to I_ℓ^{tame}) is $\frac{1}{\ell-1}$.

Lemma A.3.4.8. *Let $\phi \in D_\ell$ be a Frobenius element at ℓ. Then, for all $\sigma \in I_\ell^{\mathrm{tame}}$, one has $\phi\sigma\phi^{-1} = \sigma^\ell$ in I_ℓ^{tame}.*

Proof. Since θ is an isomorphism, it suffices to check that $\theta_n(\phi\sigma\phi^{-1}) = \theta_n(\sigma)^\ell$ for all $n \in \mathbb{N}$ prime to ℓ. So let $n \in \mathbb{N}$ be prime to ℓ, let $\zeta \in \mu_n$ be such that $\phi^{-1}(\sqrt[n]{\ell}) = \zeta\sqrt[n]{\ell}$, and let

$$\eta = \theta_n(\sigma) = \frac{\sigma(\sqrt[n]{\ell})}{\sqrt[n]{\ell}} \in \mu_n.$$

Then, since $\zeta \in \mathbb{Q}_\ell^{\mathrm{nr}}$,

$$\theta_n(\phi\sigma\phi^{-1}) = \frac{\phi\sigma\phi^{-1}(\sqrt[n]{\ell})}{\sqrt[n]{\ell}} = \frac{\phi\sigma(\zeta\sqrt[n]{\ell})}{\sqrt[n]{\ell}} = \frac{\phi(\zeta\eta\sqrt[n]{\ell})}{\sqrt[n]{\ell}} = \frac{\phi(\eta)\sqrt[n]{\ell}}{\sqrt[n]{\ell}} = \eta^\ell.$$

□

By this lemma, the two representations $\varphi^\ell \oplus \varphi'^\ell$ and $\varphi \oplus \varphi'$ are conjugate, so that the pair $\{\varphi, \varphi'\}$ is stable under the ℓ^{th} power map. This means that either ϕ and ϕ' are both of level 1, or that ϕ is of level 2 and $\varphi' = \varphi^\ell$ is its conjugate.

In the level 2 case, the representation $\rho_{\ell|I_\ell}$ is semisimple: if it were not, then ρ_ℓ would not be semisimple either since the proindex of I_ℓ in D_ℓ is prime to ℓ, so that D_ℓ would act on a stable line of $\overline{\mathbb{F}}_\ell^2$ by a character $\Phi \in \mathrm{Hom}(D_\ell, \mathbb{F}_\ell^*)$. Such a character Φ cuts out a subextension of a cyclotomic extension of $\mathbb{Q}_\ell$ by the local Kronecker-Weber theorem, so must be a power of the mod ℓ cyclotomic character $\overline{\chi}_\ell$, so that its restriction to I_ℓ is of level at most 1 by example A.3.4.7; on the other hand, this restriction is either φ or φ', a contradiction. The function ξ is thus trivial, and

$$\rho_{\ell|I_\ell} \sim \begin{bmatrix} \varphi & 0 \\ 0 & \varphi' \end{bmatrix} = \varphi \oplus \varphi'$$

is tamely ramified. Let $\theta^\vee(\varphi) = \frac{a\ell+b}{\ell^2-1}$ be the invariant of φ where $0 \leqslant a, b < \ell$ are integers, so that $\varphi = \theta_{\ell^2-1}^{a\ell+b}$, and that $\varphi' = \varphi^\ell$ has invariant $b\ell + a$. The integers a and b cannot be equal since $\theta_{\ell^2-1}^{a\ell+a} = \theta_{\ell-1}^a = \overline{\chi}_\ell^a$ is of level 1, so that I may assume that $a < b$ since φ and φ' play symmetric roles. The weight k_ρ is then defined to be

$$k_\rho = 1 + a\ell + b$$

in this case.

In the level 1 case, the characters φ and φ' are powers of the restriction to I_ℓ of the mod ℓ cyclotomic character by example A.3.4.7, so that

$$\rho_{\ell|I_\ell} \sim \begin{bmatrix} \overline{\chi}_\ell^a & \xi \\ 0 & \overline{\chi}_\ell^b \end{bmatrix}$$

for some integers $0 \leqslant a, b \leqslant \ell - 2$. If $a \not\equiv b + 1 \bmod \ell - 1$, then the weight k_ρ is defined to be

$$k_\rho = 1 + \min(a, b)\ell + \max(a, b).$$

If $a \equiv b + 1 \bmod \ell - 1$, the definition of k_ρ is more delicate: let $K = \mathbb{Q}_\ell^{\text{nr}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$, so that $\rho_{\ell|I_\ell}$, seen as a representation of $I_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/K)$, cuts out a finite Galois extension L of K, and let L_{tame} denote the maximal tamely ramified subextension of L. Since $\rho_{\ell|I_\ell}$ takes values in the group of upper triangular matrices, one may compose it with the morphism

$$\begin{bmatrix} x & * \\ 0 & y \end{bmatrix} \longmapsto x/y$$

to get the representation $\overline{\chi}_\ell^a/\overline{\chi}_\ell^b = \overline{\chi}_\ell$ of I_ℓ, which proves that L contains $K(\mu_\ell)$, a tamely ramified extension of K. Besides, the restriction of ρ_ℓ to $\mathrm{Gal}\left(L/K(\mu_\ell)\right)$ is $\left[\begin{smallmatrix} 1 & \xi \\ 0 & 1 \end{smallmatrix}\right]$ and so is given by the additive character ξ, so $L/K(\mu_\ell)$ is totally wild and so $K(\mu_\ell) = L_{\text{tame}}$. The extension L/L_{tame} is thus a Kummer extension, so that

$$L = L_{\text{tame}}(y_1, \cdots, y_r)$$

for some r such that $[L : L_{\text{tame}}] = \ell^r$ and some $y_i \in L$ such that $x_i = y_i^\ell \in L_{\text{tame}}^*$, and one has an isomorphism

$$\begin{array}{rccc} \Phi\colon & \mathrm{Gal}(L/L_{\text{tame}}) & \xrightarrow[\xi]{\sim} & \mathbb{F}_{\ell^r} \simeq \mu_\ell^r \\ & \sigma & \longmapsto & \left(\dfrac{\sigma(y_i)}{y_i}\right)_{1 \leqslant i \leqslant r} \end{array}.$$

Let $\sigma \in \mathrm{Gal}(L/L_{\mathrm{tame}})$, and let $\tau \in \mathrm{Gal}(L/K)$ restrict to a generator of $\mathrm{Gal}(L_{\mathrm{tame}}/K)$. The identity

$$\begin{bmatrix} x^{b+1} & t \\ 0 & x^b \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x^{b+1} & t \\ 0 & x^b \end{bmatrix}^{-1} = \begin{bmatrix} 1 & xy \\ 0 & 1 \end{bmatrix}$$

shows that $\Phi(\tau\sigma\tau^{-1}) = \tau\big(\Phi(\sigma)\big)$ where the right-hand-side means the Galois action of τ on μ_ℓ, so

$$\tau\left(\frac{\sigma(\tau^{-1}y_i)}{\tau^{-1}y_i}\right) = \frac{\tau\sigma\tau^{-1}y_i}{y_i} = \tau\left(\frac{\sigma(y_i)}{y_i}\right)$$

and hence $\frac{\tau^{-1}y_i}{y_i}$ is fixed by σ whence lies in L_{tame}, so that the x_i may actually be chosen in K. Assuming that they are, one says that ρ_ℓ is *peu ramifiée* if $\mathrm{ord}_\ell\, x_i \equiv 0 \bmod \ell$ for all i (in other words, if the x_i may be chosen to be *units* of K), and one defines

$$k_\rho = 1 + \min(a,b)\ell + \max(a,b),$$

else, one says that ρ_ℓ is *très ramifiée*, and one defines

$$k_\rho = \begin{cases} 1 + \min(a,b)\ell + \max(a,b) + \ell - 1 & \text{if } \ell \geqslant 3, \\ 4 & \text{if } \ell = 2. \end{cases}$$

Remark A.3.4.9. One can check that $\det \rho_{|I_\ell} = \overline{\chi}_\ell^{k_\rho - 1}$ in each case, which is necessary since the mod ℓ Galois representation $\overline{\rho}_{f,\ell}$ attached to a newform $f \in S_k(N,\varepsilon)$ has determinant $\det \overline{\rho}_{f,\ell} = \overline{\chi}_\ell^{k-1}\varepsilon$, and ε is unramified at ℓ if N is prime to ℓ.

For instance, in the case where φ and φ' are of level 2, one has

$$\det \rho = \varphi\varphi' = \theta_{\ell^2-1}^{a\ell+b}\theta_{\ell^2-1}^{b\ell+a} = \theta_{\ell^2-1}^{(a+b)(\ell+1)} = \theta_{\ell-1}^{a+b} = \overline{\chi}_\ell^{a+b},$$

and $k_\rho - 1 = 1 + a\ell + b - 1 \equiv a + b \bmod \ell - 1$.

A.3.4.3 Statement of the Serre conjecture

Now that I have explained the definition of the level, nebentypus and weight, I can finally state the Serre conjecture in detail:

Theorem A.3.4.10 (Serre, Khare, Wintenberger)**.** *Let*

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$$

be a mod ℓ Galois representation. If ρ is irreducible and odd, then there exists an eigenform

$$f \in S_{k_\rho}(N_\rho, \varepsilon_\rho),$$

where k_ρ, N_ρ and ε_ρ are defined as above, and a prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ lying above ℓ, such that ρ is isomorphic to the Galois representation $\rho_{f,\mathfrak{l}}$ attached to f modulo $\mathfrak{l}$.

The Serre conjecture will be an invaluable tool to prove the results of my computations, cf. the section C.2. In order to demonstrate its power, I shall conclude by sketching how it implies Fermat's last theorem for $\ell \geqslant 5$:

Example A.3.4.11 (Fermat's last theorem)**.** Let a, b, $c \in \mathbb{Z}$ be integers such that

$$a^\ell + b^\ell + c^\ell = 0.$$

Then $abc = 0$. Indeed, assume that $abc \neq 0$. Up to permutation and renormalisation, one can then assume that a, b and c are coprime, that b is even, and that $a \equiv -1 \bmod 4$.

Let $A = a^\ell$, $B = b^\ell$, and $C = c^\ell$, and consider the elliptic curve E defined over $\mathbb{Q}$ by the equation

$$y^2 = x(x - A)(x + B).$$

For each odd prime p, this curve has bad reduction if and only if $p|ABC$, in which case it has multiplicative reduction. The change of variables

$$x = 4X, \quad y = 8Y + 4X$$

transforms the equation of E into

$$Y^2 + XY = X^3 + \frac{B - 1 - A}{4}X^2 - \frac{AB}{16}X$$

whose coefficients are integral since $A \equiv -1 \bmod 4$ and $B \equiv 0 \bmod 32$. Reduction modulo $p = 2$ yields

$$Y^2 + XY = X^3 + X^2 \quad \text{or} \quad X^3$$

depending whether $A \equiv -1$ or $3 \bmod 8$, so that E has multiplicative reduction at $p = 2$. Finally E has everywhere either good or multiplicative reduction, so that it is semi-stable, of conductor

$$N_E = \prod_{p|2ABC} p = \prod_{p|ABC} p.$$

Furthermore, the first equation is minimal at every $p \neq 2$, whereas the second one is minimal at $p = 2$, so that the discriminant of E is

$$\Delta_E = \frac{(ABC)^2}{2^8}.$$

Consider now the mod ℓ Galois representation

$$\rho_{E,\ell} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

afforded by the Galois action on $E[\ell]$, as in example A.3.1.11. Its determinant is the mod ℓ cyclotomic character $\overline{\chi}_\ell$, so that this representation is odd. It is also irreducible. Indeed, if it were not, the curve E would have a subgroup X of order ℓ which is stable under $G_{\mathbb{Q}}$, so that one would have

$$\rho_{E,\ell} \sim \begin{bmatrix} \varphi & * \\ 0 & \varphi' \end{bmatrix}.$$

The action of $G_{\mathbb{Q}}$ on X would be given by the mod ℓ Galois character φ, and since E is semi-stable, by [Ser72, p. 307, lemme 6], one of the Galois characters φ, φ' would be trivial whereas the other one would be a power of $\overline{\chi}_\ell$. Since $\varphi\varphi' = \det \rho_{E,\ell} = \overline{\chi}_\ell$, the character φ would be either trivial or equal to $\overline{\chi}_\ell$. After possibly replacing E with its quotient E/X, one may assume that φ is trivial. Then the points in X would be $\mathbb{Q}$-rational, so that $E(\mathbb{Q})_{\text{tors}}$ would be of order at least $2^2\ell \geqslant 20$ since the 4 points in $E[2]$ are $\mathbb{Q}$-rational, which would contradict Mazur's bounds A.2.1.18.

The Galois representation $\rho_{E,\ell}$ is thus odd and irreducible, so that the Serre conjecture A.3.4.10 applies. J.-P. Serre then shows (cf. [Ser87, §4.1 and 4.2]) that as E is semi-stable, the Artin conductor of $\rho_{E,\ell}$ is

$$N(\rho_{E,\ell}) = \prod_{\substack{p\neq\ell \\ \ell\nmid \mathrm{ord}_p(\Delta_E)}} p = 2,$$

so that its level is also $N_{\rho_{E,\ell}} = 2$; besides, he computes that its weight is also $k_{\rho_{E,\ell}} = 2$. But $S_2\big(\Gamma_1(2)\big) = \{0\}$, a contradiction.

J.-P. Serre also notes in [Ser87, théorème 4] that his conjecture also implies the *modularity conjecture* for elliptic curves over $\mathbb{Q}$, a.k.a the Taniyama-Shimura-Weil conjecture.

Part B

Computing modular Galois representations

Computers are like Old Testament gods; lots of rules and no mercy.

— Joseph Campbell, *The Hero's Journey*

I now present the heart of my thesis: an algorithm, based on original ideas from J.-M. Couveignes and B. Edixhoven (cf. [CE11]), to compute the mod $\mathfrak{l}$ Galois representation[1] $\rho_{f,\mathfrak{l}}$ attached to a newform $f \in S_k(N)$ of even weight modulo a prime $\mathfrak{l}$ of degree 1. By this, I mean that the algorithm which I describe here first computes an irreducible polynomial $F(X) \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$ whose decomposition field in $\overline{\mathbb{Q}}$ is the number field L cut out by $\rho_{f,\mathfrak{l}}$ and such that the Galois action on its roots mimics the $\rho_{f,\mathfrak{l}}$-action on $\mathbb{F}_\mathfrak{l}^2 - \{0\}$, and then it gives an efficient recipe to compute the similarity class of the image in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ of the Frobenius element at almost every prime $p \in \mathbb{N}$.

Apart from making $\rho_{f,\mathfrak{l}}$ explicit, the main interest of this algorithm is that it allows to compute the coefficients a_p of f modulo $\mathfrak{l}$ as the trace of the image of the Frobenius element at p. For fixed f and $\mathfrak{l}$, this yields a method to compute a_p mod $\mathfrak{l}$ using only $\widetilde{O}(\log^2 p)$ bit operations. In theory, one can then use Chinese remainders to compute a_p from its reduction modulo sufficiently many primes $\mathfrak{l}$, yielding an algorithm to compute a_p in time polynomial in $\log p$, whereas the algorithm based on modular symbols (cf. example A.2.3.12) requires at least $\widetilde{O}(p)$ bit operations. Unfortunately, the complexity of my algorithm with respect to ℓ, although polynomial, is too bad for this to be practical.

The idea consists in catching $\rho_{f,\mathfrak{l}}$ in the ℓ-torsion of $J_1(\ell N)$, as explained in theorem A.3.3.26. In order to simplify the exposition, I shall assume that the newform f is of level $N = 1$, so that I am working in prime level ℓ and I do not have to worry about the old part in $\Omega^1\big(X_1(\ell)\big) = S_2(\ell)$ (cf. example A.2.2.23). The algorithm presented here can however be easily extended to newforms of higher level N, provided

[1] This representation was denoted by $\overline{\rho}_{f,\mathfrak{l}}$ in the previous part, but I shall drop the bar from now on, for the sake of readability.

that N is square-free and is prime to ℓ. In order not to have to deal with degenerate cases, I shall also assume that the prime $\mathfrak{l}$ is not exceptional in the sense of definition A.3.3.9, so that the image of $\rho_{f,\mathfrak{l}}$ contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ and is thus

$$\mathrm{Im}\,\rho_{f,\mathfrak{l}} = \left\{ g \in \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}) \;\middle|\; \det g \in \mathbb{F}_\mathfrak{l}^{*(k-1)} \right\}$$

since the determinant of $\rho_{f,\mathfrak{l}}$ is the $(k-1)^{\text{th}}$ power of the mod ℓ cyclotomic character $\overline{\chi}_\ell$.

Finally, I shall assume that $\ell > k$, so that theorem A.3.3.26 applies. In particular, the genus $g = \frac{(\ell-5)(\ell-7)}{24}$ of $X_1(\ell)$ is then non-zero.

B.1 Overview of the algorithm

It is immediate to compute the ℓ-torsion of $J_1(\ell)$ in the analytic model $\mathbb{C}^g/\Lambda$ (cf. section A.1.2), whereas it is easier to write down a Galois-equivariant function to $\overline{\mathbb{Q}}$ on the algebraic model $\mathrm{Pic}^0\left(X_1(\ell)_{\overline{\mathbb{Q}}}\right)$, as shown on figure B.1.0.1. Therefore, I shall start by computing the analytic model, and switch to the algebraic model at some point.

Algebraic model	$\xrightarrow{\text{Abel-Jacobi}}$	Analytic model
$\mathrm{Pic}^0\left(X_1(\ell)_{\mathbb{C}}\right)$	$\dashleftarrow$	$\mathbb{C}^g/\Lambda$
Easy to evaluate points		Easy torsion

Figure B.1.0.1: Switching between two models of $J_1(\ell)$

The first task consists in computing a high-precision complex approximation of the period lattice Λ of $X_1(\ell)$, which I do by integrating term-by-term the q-expansions of a basis $(\omega_i)_{1\leqslant i\leqslant g}$ of cuspforms of weight 2 along modular symbols. In order to get a very accurate result, this requires q-expanding the ω_i to high precision, which I show how to do quickly below. Then, since the action of the Hecke algebra on modular symbols is known, I deduce an analytic representation of the ℓ-torsion subspace

$$V_{f,\mathfrak{l}} = \bigcap_{n=1}^{+\infty} \mathrm{Ker}\left(T_n - a_n(f) \bmod \mathfrak{l}\right)\Big|_{J_1(\ell)[\ell]} \subset J_1(\ell)[\ell] = (\mathbb{C}^g/\Lambda)[\ell] = \left(\frac{1}{\ell}\Lambda\right)/\Lambda$$

which affords $\rho_{f,\mathfrak{l}}$ by theorem A.3.3.26, where T_n denotes the Hecke operator in weight 2 and level ℓ.

Next, by locally inverting the Abel-Jacobi map $\jmath$, I find divisors D_1, D_2 in $\mathrm{Div}^0\left(X_1(\ell)\right)$ such that $\jmath(D_1) = x_1$ and $\jmath(D_2) = x_2$, where x_1 and x_2 are two ℓ-torsion points on $J_1(\ell)$ forming a basis of the two-dimensional $\mathbb{F}_\ell$-subspace $V_{f,\mathfrak{l}} \subset J_1(\ell)[\ell]$. This is done as follows:

I pick g points $(P_j)_{1\leqslant j\leqslant g}$ on $X_1(\ell)$, and, using Newton iteration, I compute another g points $(P'_j)_{1\leqslant j\leqslant g}$ with P'_j close to P_j such that

$$\sum_{j=1}^{g} \left(\int_{P_j}^{P'_j} \omega_i(\tau)\mathrm{d}\tau \right)_{1\leqslant i\leqslant g} = \frac{\widetilde{x_1}}{2^m},$$

where $\widetilde{x_1}$ is a lift of x_1 to $\mathbb{C}^g$, $m \in \mathbb{N}$ is large enough for Newton iteration to converge, and the integrals are taken along paths joining P_j to P'_j and staying inside some coordinate disk. Thus, I get the divisor

$$D_1^{(m)} = \sum_{j=1}^{g} (P'_j - P_j)$$

which satisfies $\jmath(2^m D_1^{(m)}) = x_1$. Then, using K. Khuri-Makdisi's algorithms (cf. section A.1.3) to compute in $\mathrm{Pic}^0\big(X_1(\ell)\big)$, I double m times the divisor class of $D_1^{(m)}$, which yields an ℓ-torsion divisor D_1 representing x_1. I apply the same process another time so as to get another ℓ-torsion divisor D_2 representing x_2.

This way, I find ℓ-torsion divisors using only integrals along short paths which stay well inside the convergence disks. Therefore, I have far fewer precision problems than with J. Bosman's method [Bos07].

I now have two ℓ-torsion divisors D_1 and D_2 whose images by the Abel-Jacobi map form a basis of the ℓ-torsion subspace $V_{f,\mathfrak{l}}$. I then compute all the divisors

$$D_{a,b} \sim aD_1 + bD_2, \quad a, b \in \mathbb{F}_\ell$$

up to equivalence, yielding a collection of ℓ^2 divisors corresponding to the ℓ^2 points of $V_{f,\mathfrak{l}}$. Finally, I evaluate a well-chosen Galois-equivariant map $\alpha\colon V_{f,\mathfrak{l}} \longrightarrow \overline{\mathbb{Q}}$ in these points. The polynomial

$$F(X) = \prod_{\substack{a,b\in\mathbb{F}_\ell \\ (a,b)\neq(0,0)}} \big(X - \alpha(D_{a,b})\big)$$

then lies in $\mathbb{Q}[X]$, and I can identify its coefficients by using continued fractions. This polynomial encodes the Galois representation $\rho_{f,\mathfrak{l}}$, in that its splitting field L over $\mathbb{Q}$ is the number field cut out by the representation $\rho_{f,\mathfrak{l}}$, and $\mathrm{Gal}(L/\mathbb{Q})$ acts on its roots $\alpha(D_{a,b})$ just like $\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $(a, b) \in \mathbb{F}_\ell^2$.

My final task is to describe the image of Frobenius elements by this representation. For this, I adapt T. and V. Dokchitser's work [Dok10] (cf. section A.3.2) to get resolvents

$$\Gamma_C(X) \in \mathbb{Q}[X], \quad C \text{ similarity class of } \mathrm{GL}_2(\mathbb{F}_\ell)$$

such that for almost all rational primes p,

$$\rho_{f,\mathfrak{l}}\left(\mathrm{Frob}_p\right) \in C \iff \Gamma_C\big(\mathrm{tr}_{A_p/\mathbb{F}_p}\, a^p\, h(a)\big) = 0 \bmod p,$$

where a denotes the class of X in $A_p = \mathbb{F}_p[X]/\big(F(X)\big)$ and $h \in \mathbb{Z}[X]$ is a polynomial. I furthermore present two tricks to reduce the amount of computations required at this step.

I can then use these resolvents to compute the coefficients a_p of the q-expansion of f modulo $\mathfrak{l}$, as

$$a_p \bmod \mathfrak{l} = \mathrm{tr}\, \rho_{f,\mathfrak{l}}\left(\mathrm{Frob}_p\right).$$

I shall now explain how to use K. Khuri-Makdisi's algorithms on $X_1(\ell)$, after what I shall give a detailed description of all the steps of my algorithm.

B.2 Computing in $J_1(\ell)$

B.2.1 Arithmetic in the jacobian $J_1(\ell)$

In order to efficiently compute in the jacobian $J_1(\ell)$, I adapt K. Khuri-Makdisi's algorithms (cf. section A.1.3). This requires choosing an effective divisor D_0 of degree $d_0 \geqslant 2g+1$ for which I know how to compute the associated Riemann-Roch space

$$V = H^0\big(X_1(\ell), 3D_0\big).$$

I then represent a divisor class $x \in J_1(\ell)$ by the subspace

$$W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V$$

where D is an effective divisor of degree d_0 such that the class of $D - D_0$ is x. In particular, $0 \in J_1(\ell)$ can be represented by

$$W_0 = H^0\big(X_1(\ell), 2D_0\big) \subset V.$$

I shall also want D_0 to be defined over $\mathbb{Q}$, so that $(W_D)^\sigma$ represents D^σ for all $\sigma \in \operatorname{Aut}\mathbb{C}$.

Let me first give an overview of how to find such a divisor D_0. My strategy consists in choosing $D_0 = K + c_1 + c_2 + c_3$, where K is an effective canonical divisor defined over $\mathbb{Q}$ and the c_i are $\mathbb{Q}$-rational cusps. In particular I set $d_0 = 2g+1$ exactly, the minimum to ensure the correctness of K. Khuri-Makdisi's method.

First, I compute the $(g+2)$-dimensional space

$$V_2 = H^0\big(X_1(\ell), \Omega^1(c_1 + c_2 + c_3)\big).$$

This space is the direct sum of all the cusp forms of weight 2 and of the scalar multiples of the Eisenstein series $e_{1,2}$ and $e_{1,3}$ of weight 2 vanishing at all cusps except respectively c_1 and c_2 for $e_{1,2}$ and except c_1 and c_3 for $e_{1,3}$, so that

$$V_2 = S_2\big(\Gamma_1(\ell), \mathbb{C}\big) \oplus \mathbb{C}e_{1,2} \oplus \mathbb{C}e_{1,3} \subset M_2\big(\Gamma_1(\ell), \mathbb{C}\big). \tag{B.2.1.1}$$

The point of this is that by picking a cusp form $f_0 \in S_2\big(\Gamma_0(\ell), \mathbb{Q}\big)$ defined over $\mathbb{Q}$, one obtains a Galois-equivariant isomorphism

$$\begin{array}{ccc} V_2 & \xrightarrow{\sim} & H^0\big(X_1(\ell), K + c_1 + c_2 + c_3\big) \\ f & \longmapsto & \dfrac{f}{f_0} \end{array},$$

where K is the divisor of the differential 1-form over $X_1(\ell)$ associated to the cuspform f_0, which is indeed an effective canonical divisor. Now, by theorem A.1.3.5, the map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & H^0\big(X_1(\ell), 3(K + c_1 + c_2 + c_3)\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & \dfrac{f_1 f_2 f_3}{f_0^3} \end{array}$$

is surjective. I may thus choose V to be the image of the multiplication map

$$\begin{array}{ccc} V_2^{\otimes 3} & \longrightarrow & M_6\big(\Gamma_1(\ell), \mathbb{C}\big) \\ f_1 \otimes f_2 \otimes f_3 & \longmapsto & f_1 f_2 f_3 \end{array}.$$

In this framework, the subspace W_0 representing $0 \in J_1(\ell)$ is the image of the map

$$\begin{array}{ccc} V_2^{\otimes 2} & \longrightarrow & M_6\big(\Gamma_1(\ell),\mathbb{C}\big) \\ f_1 \otimes f_2 & \longmapsto & f_1 f_2 f_0 \end{array}.$$

From now on, I shall identify weight-6 modular form spaces with the corresponding modular function spaces obtained by dividing by f_0^3, without explicitly mentioning it.

I represent weight-6 forms by their q-expansions at each cusp. To compute these q-expansions, I start from the q-expansion at ∞, and apply the Fricke involution and diamond operators in order to reach all the other cusps, as explained below. I could also have represented forms by their q-expansions at ∞ only, but I surmise that using q-expansions at various cusps ensures better numerical stability. Also I shall later need to be able to evaluate the forms at various points of the modular curve, so it is better to know the q-expansions at various places.

The modular curve $X_0(\ell)$ has exactly two cusps, namely $\Gamma_0(\ell)\cdot\infty$ and $\Gamma_0(\ell)\cdot 0$, whereas the modular curve I am interested in, $X_1(\ell)$, has exactly $\ell-1$ cusps, half of which lie above $\Gamma_0(\ell)\cdot\infty$ while the other half lie above $\Gamma_0(\ell)\cdot 0$ (cf. example A.2.1.13). I call the former "cusps above ∞" and the latter "cusps above 0". The cusps above 0 are all rational, whereas the cusps above ∞ make up a single Galois orbit. Now, the diamond operators $\langle d\rangle$, $d \in (\mathbb{Z}/\ell\mathbb{Z})^*$, which correspond to the action of the quotient group $\Gamma_0(\ell)/\Gamma_1(\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^*$, map the cusp $\Gamma_1(\ell)\cdot\infty$ onto the cusps above ∞, and the cusp $\Gamma_1(\ell)\cdot 0$ onto the cusps above 0. Moreover, the Fricke operator W_ℓ swaps $\Gamma_1(\ell)\cdot\infty$ and $\Gamma_1(\ell)\cdot 0$. I know how the Fricke operator acts on newforms of weight 2 by theorem A.2.2.33, and on Eisenstein series by proposition A.2.2.44. Besides, all the forms I am dealing with have a nebentypus, so that the action of a diamond operator $\langle d\rangle$ on their q-expansions is very easy to compute: it boils down to multiplying by the value $\varepsilon(d)$ of their nebentypus at d. Using these two kinds of operators, I thus get the q-expansions of the newforms and of the Eisenstein series at all cusps from their q-expansions at ∞.

B.2.2 Finding the appropriate Eisenstein series

I shall now explain how to construct Eisenstein series $e_{1,2}$ and $e_{1,3}$ such that (B.2.1.1) holds. As explained in section A.2.2.3, the Eisenstein subspace $E_2\big(\Gamma_1(N)\big)$ of $M_2\big(\Gamma_1(N)\big)$ has a basis formed by the Eisenstein series

$$G_2^{\psi,\varphi}(t\tau) = \sum_{r=0}^{u-1}\sum_{s=0}^{v-1}\sum_{t=0}^{u-1}\psi(r)\overline{\varphi}(s)\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c\equiv rv \bmod N \\ d\equiv s+tv \bmod N}}\frac{1}{(ct\tau+d)^2},$$

where $t \in \mathbb{N}$ and ψ and φ are Dirichlet characters not both trivial, of the same parity, and of respective conductors u and v such that $tuv|N$, along with the

$$G_2(\tau) - tG_2(t\tau), \quad \text{where} \quad G_2(\tau) = \sum_{c\in\mathbb{Z}}\sum_{\substack{d\in\mathbb{Z} \\ (c,d)\neq(0,0)}}\frac{1}{(c\tau+d)^2} \text{ and } 1 < t|N.$$

Their q-expansions at ∞ are given by

$$E_2^{\psi,\varphi}(\tau) = -\mathbb{1}_{u=1}\frac{1}{2}\sum_{a=0}^{v-1}\varphi(a)a\left(\frac{a}{v}+1\right) + 2\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}\psi(n/m)\varphi(m)m\right)q^n,$$

where $\mathbb{1}_{u=1}$ is 1 if $u=1$ and 0 else, $E_2^{\psi,\varphi}$ is the normalisation of $G_2^{\psi,\varphi}$ defined by the relation

$$G_2^{\psi,\varphi} = \frac{-4\pi^2 g(\overline{\varphi})}{v^2}E_2^{\psi,\varphi},$$

and where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character, and

$$E_2(\tau) = 1 - 24\sum_{n=1}^{+\infty}\left(\sum_{\substack{m>0\\ m|n}}m\right)q^n, \quad G_2 = \frac{\pi^2}{3}E_2.$$

Also, $G_2^{\psi,\varphi}(t\tau) \in E_2\big(\Gamma_1(N), \psi\varphi\big)$ has nebentypus $\psi\varphi$, where $\psi\varphi$ is seen as a Dirichlet character modulo N, whereas $G_2(\tau) - tG_2(t\tau)$ has trivial nebentypus. In what follows, I shall not use the $G_2(\tau) - tG_2(t\tau)$ at all.

In the case when $N = \ell$ is prime, one is left with only two cases, namely $G_2^{\chi,1}$ and $G_2^{1,\chi}$, where χ is a non-trivial even Dirichlet character modulo ℓ. Both have nebentypus χ, and $G_2^{\chi,1}$ vanishes at ∞ while $G_2^{1,\chi}$ does not (cf. section A.2.2.3).

I construct the Eisenstein series $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$ and of the $E_2^{1,\chi}$, because they have nicer q-expansions than their G-counterparts. First, I choose the cusps c_1, c_2 and c_3 to be $c_1 = \Gamma_1(\ell)\cdot 0$, $c_2 = \langle 2\rangle c_1$, and $c_3 = \langle 3\rangle c_1$, which are all $\mathbb{Q}$-rational. They are also all distinct since $\ell \geqslant 13$. The form $f_0 \in S_2\big(\Gamma_0(\ell), \mathbb{Q}\big)$ is defined over $\mathbb{Q}$ because its q-expansion at the $\mathbb{Q}$-rational cusp $\Gamma_1(\ell)\cdot 0$ has rational coefficients, so its divisor K is defined over $\mathbb{Q}$, and so is my divisor $D_0 = K + c_1 + c_2 + c_3$. Next, according to formula A.2.2.44, one has

$$W_\ell E_2^{\chi,1} = \frac{g(\chi)}{\ell}E_2^{1,\overline{\chi}} \qquad \text{and} \qquad W_\ell E_2^{1,\chi} = \frac{\ell}{g(\overline{\chi})}E_2^{\overline{\chi},1},$$

from which one reads that $E_2^{\chi,1}$ vanishes at the cusps above ∞ but not at the cusps above 0, whereas $E_2^{1,\chi}$ has the opposite behaviour. Consequently, I can construct $e_{1,2}$ and $e_{1,3}$ as linear combinations of the $E_2^{\chi,1}$ only. It then follows easily from the orthogonality relations between Dirichlet characters that the Eisenstein series

$$e_{1,2} = \sum_{\substack{\chi \text{ even}\\ \chi\neq 1}} \frac{1-\chi(2)}{g(\chi)\displaystyle\sum_{a=0}^{\ell-1}\overline{\chi}(a)a\left(\frac{a}{\ell}+1\right)}E_2^{\chi,1}$$

and

$$e_{1,3} = \sum_{\substack{\chi \text{ even}\\ \chi\neq 1}} \frac{1-\chi(3)}{g(\chi)\displaystyle\sum_{a=0}^{\ell-1}\overline{\chi}(a)a\left(\frac{a}{\ell}+1\right)}E_2^{\chi,1}$$

are the ones which I am looking for, that is to say that $e_{1,2}$ vanishes at all cusps except c_1 and c_2, and $e_{1,3}$ vanishes at all cusps except c_1 and c_3.

Finally, I need to compute the q-expansions of $e_{1,2}$ and of $e_{1,3}$ at each of the cusps of $X_1(\ell)$, so as to be able to use them in K. Khuri-Makdisi's algorithms. Although these series are probably not eigenseries, this is not a problem, as it is still easy to compute the action of the Fricke involution and of the diamond operators on them simply by linearity, and thus to deduce their q-expansions at each of the cusps.

B.3 Detailed description of the algorithm

I first show in subsection B.3.1 how to quickly compute a huge number of terms of the q-expansion at infinity of the cuspforms of weight 2 and level ℓ, and next, in B.3.2, how to efficiently compute the period lattice of $X_1(\ell)$ to high precision using these q-expansions. After this, I show in B.3.3 how to compute a basis of the eigenplane $V_{f,\mathfrak{l}} \subset J_1(\ell)[\ell]$. Finally, I explain in B.3.4 how to construct a well-behaved function on the jacobian $J_1(\ell)$ and how to evaluate it at the ℓ-torsion divisors, and I conclude by describing in B.3.5 an efficient recipe to computing the image of the Frobenius elements by the Galois representation $\rho_{f,\mathfrak{l}}$.

B.3.1 Expanding the cuspforms of weight 2 to high precision

I need to compute the q-expansion of the newforms of weight 2 in order to compute the period lattice of the modular curve. Classical methods based on modular symbols (cf. example A.2.3.12) can be used to compute a moderate number of terms of these q-expansions. However, I shall need to compute the periods with very high accuracy, which requires knowing a very large number of coefficients in these q-expansions. As using classical methods for this, although possible, would be too slow, I present a new method to quickly compute a huge number of such coefficients. It proceeds roughly as follows:

- First, I compute a moderate number of coefficients of the q-expansion of each cuspform ω by using the classical method based on modular symbols.
- Then, I use these coefficients to determine a polynomial equation relating a modular function depending on ω to the modular invariant j (cf. example A.2.2.5), whose q-expansion is easy to compute, even to very high accuracy.
- Finally, I use Newton iteration on this equation between q-series to compute a huge number of coefficients of the modular function depending on ω, and from this I deduce the ones of ω.

Moreover, I perform all of these computations modulo some prime p, so as to prevent intermediate coefficient growth from slowing down the process.

More precisely, to compute these q-expansions to the precision $O(q^B)$, I first compute a generator of the Hecke algebra $\mathbb{T}_{2,\ell} \otimes_{\mathbb{Z}} \mathbb{Q}$, by picking a Hecke operator and testing whether it is a $\mathbb{Q}$-algebra generator. This is easy as it amounts to check whether its eigenvalues on $S_2\big(\Gamma_1(\ell)\big)$ are all distinct. One can for instance proceed as follows: starting with $n = 2$, first check whether T_n is a generator, if not then try a few combinations of small integers λ_m and check whether $T_n + \sum_{m=2}^{n-1} \lambda_m T_m$ is a generator, and if still not, increase n by 1 and start again. In practise, it appears that for $11 \leqslant \ell \leqslant 31$, at least one of T_2 and T_3 is a $\mathbb{Q}$-algebra generator.

Let $\mathcal{B} = \bigsqcup_\varepsilon \mathcal{B}_\varepsilon$ be a basis of $S_2\big(\Gamma_1(\ell)\big)$ corresponding to the decomposition

$$S_2\big(\Gamma_1(\ell)\big) = \bigoplus_\varepsilon S_2\big(\Gamma_1(\ell), \varepsilon\big),$$

where ε ranges over the even characters modulo ℓ, and $\mathcal{B}_\varepsilon$ is a basis of $S_2(\varepsilon)$ consisting in forms which are not necessarily eigenforms[2], but which are normalised, and whose q-expansion coefficients lie among the integers $\mathbb{Z}_K$ of the common cyclotomic field $K = \mathbb{Q}\left(\zeta_{(\ell-1)/2}\right)$. To make it easier to reduce mod p and lift back to K, I require p to split completely in K. Also, p should be chosen large enough for reduction mod p of the coefficients to be faithful. Deligne's bounds (A.3.3.7) state that if $q + \sum_{n\geqslant 2} a_n q^n$ is a newform of weight 2, then $|\sigma(a_n)| \leqslant \sigma_0(n)\sqrt{n}$ for all $n \in \mathbb{N}$ and for every embedding σ of $\overline{\mathbb{Q}}$ into $\mathbb{C}$, where $\sigma_0(n)$ denotes the number of positive divisors of n. These bounds may not apply to the forms in the bases $\mathcal{B}_\varepsilon$ since they are not eigenforms, but using the $\mathbb{Q}$-generator of the Hecke algebra computed above, I can compute for each ε a change of basis matrix from the basis $\mathcal{B}_\varepsilon$ to a basis of eigenforms, then deduce from Deligne's bound a bound on the complex embeddings of the B first coefficients of the forms of $\mathcal{B}_\varepsilon$, and finally compute a bound on the coefficients of these coefficients seen as polynomials in $\zeta_{(\ell-1)/2}$. I then choose $p \neq \ell$ to be the smallest rational prime greater than twice this bound and such that $p \equiv 1 \bmod (\ell-1)/2$. Then the $(\ell-1)/2$-th cyclotomic polynomial splits completely over $\mathbb{F}_p$, and, letting a_i denote lifts to $\mathbb{Z}$ of its roots in $\mathbb{F}_p$, the prime p splits completely in K into $\prod_i \mathfrak{p}_i$, where $\mathfrak{p}_i = \big(p, \zeta_{(\ell-1)/2} - a_i\big)$.

Next, I compute the forms

$$E_4 = 1 + 240\sum_{n=1}^{+\infty} \sigma_3(n) q^n,\ E_6 = 1 - 540\sum_{n=1}^{+\infty} \sigma_5(n) q^n,\ \text{and } u = \frac{1}{j} = \frac{E_4^3 - E_6^2}{1728 E_6^2}$$

in $\mathbb{F}_p[[q]]$, as well as $\mathrm{d}j$ in $q^{-2}\mathbb{F}_p[[q]]\mathrm{d}q$, to precision $O(q^B)$.

I can then compute the q-expansions of the forms ω with trivial nebentypus $\varepsilon = \mathbb{1}$ in $\mathcal{B}_{\mathbb{1}}$ as follows. Such a form ω has q-coefficients in $\mathbb{Z}$. Consider the form $v = \frac{\omega \mathrm{d}q}{q\mathrm{d}j} \in \mathbb{Z}[[q]]$. It has weight 0, so it is a rational function on $X_1(\ell)$, which actually descends to a rational function on $X_0(\ell)$ because $\varepsilon = \mathbb{1}$. I claim that its degree there is at most $2g_0 + \ell + 1$, where g_0 denotes the genus of $X_0(\ell)$. Indeed, its degree is at most the number of zeroes of the 1-form $\omega\frac{\mathrm{d}q}{q}$ plus the number of poles of the 1-form $\mathrm{d}j$. On the one hand, $\omega\frac{\mathrm{d}q}{q}$ has exactly $2g_0 - 2$ zeroes as it is regular. On the other hand, as $\mathrm{d}j$ has a double pole at the cusp on $X(1)$, it has a

[2]If I used a basis made up of eigenforms, the common number field containing the Fourier coefficients of all these forms could be much larger.

pole of order $e_c + 1$ at each cusp c of $X_0(\ell)$, where e_c is the ramification index of c. Summing over the two cusps of $X_0(\ell)$, one thus sees that $\mathrm{d}j$ has $\ell+3$ poles on $X_0(\ell)$, hence my claim on the degree of v. Besides, u has degree exactly $\ell+1$ on $X_0(\ell)$. Consequently, there exists an irreducible polynomial $\Phi(U,V) \in \mathbb{F}_p[U,V]$ of degree at most $2g_0+\ell+1$ in U and exactly $\ell+1$ in V such that $\Phi(u,v) \equiv 0 \bmod p$. I compute such a polynomial by coefficient identification in $\mathbb{F}_p[[q]]$, using a moderately precise q-expansion of ω computed by classical algorithms, along with linear algebra over $\mathbb{F}_p$. Then, by Newton iteration, I can compute $v \bmod p$, and hence $\omega \bmod p$, to the precision $O(q^B)$, and finally lift the coefficients of ω back to $\mathbb{Z}$.

Now that the forms with trivial nebentypus are dealt with, I can compute the q-expansions of the forms ω with nontrivial nebentypus ε as follows. Let $\omega_0 \in \mathcal{B}_{\mathbb{1}}$ be one of the g_0 forms[3] with trivial nebentypus whose q-expansion I have just computed. Then $\frac{\omega}{\omega_0}$ is a rational function on $X_1(\ell)$ with nebentypus ε. I could thus proceed to find an equation Φ as previously by reasoning on $X_1(\ell)$ instead of $X_0(\ell)$, but this would lead to very high degrees and hence would be too slow. Instead, notice that if r denotes the order of ε, then $v = \left(\frac{\omega}{\omega_0}\right)^r$ has trivial nebentypus, so descends to a function on $X_0(\ell)$, of degree at most $\frac{(2g_1-2)r}{(\ell-1)/2}$, where $g_1 = g$ denotes the genus of $X_1(\ell)$, because it has degree at most $(2g_1-2)r$ over $X_1(\ell)$. I can thus compute as previously for each $\mathfrak{p}_i$ an irreducible polynomial $\Phi(U,V) \in \mathbb{F}_p[U,V]$ of degree at most $\frac{(2g-2)r}{(\ell-1)/2}$ in U and exactly $\ell+1$ in V such that $\Phi(u,v) \equiv 0 \bmod \mathfrak{p}_\mathfrak{i}$. Next, I use Newton iteration as before to compute $v \bmod \mathfrak{p}_\mathfrak{i}$, then take the r^{th} root to recover $\omega \bmod \mathfrak{p}_\mathfrak{i}$, and finally lift back to K by Chinese remainders.

Finally, I apply the change of basis matrices from $\mathcal{B}_\varepsilon$ to the basis of eigenforms which I computed in the beginning to the q-expansions of the forms which I have just computed, so as to get the q-expansions of the newforms.

For large B, this method is faster than the one based one modular symbols:

Theorem B.3.1.1. *For fixed prime level ℓ, the number of bit operations required to compute the q-expansion of the newforms in $S_2\big(\Gamma_1(\ell)\big)$ to precision $O(q^B)$ with the algorithm described above is quasi-linear in B.*

In comparison, the bit complexity of the classical algorithm based on modular symbols is at least quadratic in B, cf. remark A.2.3.13.

Proof. First notice that for fixed level ℓ, the change of basis matrices from the bases $\mathcal{B}_\varepsilon$ to the eigenforms are fixed, and so is the common field $K = \mathbb{Q}\left(\zeta_{(\ell-1)/2}\right)$. Consequently, there exists some $C > 0$ not depending on B such that the coefficients of $\zeta_{(\ell-1)/2}$ in the coefficients up to q^B of the forms in the bases $\mathcal{B}_\varepsilon$ are bounded by $M = C \sup_{n<B} \sigma_0(n)\sqrt{n}$. One has $M = O(B)$, because $\sigma_0(n) = O(n^\delta)$ for every $\delta > 0$, cf. for instance [HW08, ch. XVIII, theorem 315]. If B is large enough, then M will be large too, so that by the prime number theorem for arithmetic

[3]Here, the method breaks down for $\ell = 13$. Indeed, this is the only case in which $g_0 = 0$ (remember that I supposed $\ell \geqslant 11$), so that there is no such form in this case. So, in this special case $\ell = 13$, classical methods to expand the forms should be used instead. This is not a big problem, as this is a "small" case (g is only 2), so little accuracy in the q-expansions is needed to compute the Galois representation, and classical methods based on modular symbols can be used in this case.

progressions (cf. for instance [Sop10]), I can assume that there exists a prime number $p \equiv 1 \bmod (\ell-1)/2$ lying between $2M$ and, say, $3M$. I can find such a p in $O(B \log B \log\log B)$ bit operations thanks to the sieve of Eratosthenes (cf. the proof of [GG99, theorem 18.10 part ii]). Then arithmetic operations in the residue field $\mathbb{F}_p$ will require $O(\log B)$ bit operations. Next, E_4 and E_6 can be computed mod p to precision $O(q^B)$ in $O(B \log B \log\log B)$ bit operations by using again the sieve of Eratosthenes, and u and $\mathrm{d}j$ can be computed in $\mathbb{F}_p\big[[q]\big]$ to accuracy $O(q^B)$ in $O(B \log B)$ operations in $\mathbb{F}_p$ by using fast series arithmetic. As ℓ is fixed, computing the short q-expansions and finding the equations Φ, which are of fixed degree, takes fixed time. Then, each Newton iteration takes $O(B \log B)$ operations in $\mathbb{F}_p$ thanks to fast arithmetic, and reaching precision $O(q^B)$ requires $O(\log B)$ such iterations. Finally, the coefficients can be lifted back to K since $p > 2M$, and each such lift requires $O(\log B)$ bit operations, so lifting the forms requires $O(B \log B)$ bit operations, hence the result. □

B.3.2 Computing the periods of $X_1(\ell)$

Computing the period lattice Λ amounts, by the Manin-Drinfeld theorem A.2.3.14, to compute integrals of newforms ω of weight 2 along modular symbols, such as

$$\int_\infty^0 \omega(\tau)\mathrm{d}\tau.$$

These integrals can be computed by integrating q-expansions term by term. However, the integration path must be split so that the resulting series converges. Furthermore, to increase the convergence speed, I need the path ends to lie well-inside the convergence disks.

To reduce the number of integrals which I compute, I use the adjointness property of the Hecke operators with respect to the integration pairing between modular symbols and cuspforms, so that it is enough for me to compute the periods along a $\mathbb{T}_{2,\ell}$-generating family of cycles, where $\mathbb{T}_{2,\ell}$ denotes the Hecke algebra of weight 2 and level ℓ. In general, the modular symbol $\{\infty, 0\}$ alone does not span the rational homology of the modular curve, even over the Hecke algebra, so I introduce other modular symbols, the *twisted winding elements* w_p, defined (cf. [CE11, section 6.3]) for $p \neq \ell$ prime or $p = 1$ as

$$w_p = \sum_{a \bmod p} \epsilon_p(a) \left\{\infty, \frac{a}{p}\right\} \in \mathbb{M}_2\big(\Gamma_1(\ell)\big),$$

where $\epsilon_p = \left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol at p, which I define to be 1 if $p = 1$ for convenience.

By the Manin-Drinfeld theorem A.2.3.14, each basis element γ_j of $H_1\big(X_1(\ell)(\mathbb{C}), \mathbb{Z}\big)$, seen as a linear form on $S_2\big(\Gamma_1(\ell)\big)$, may be written as a $\mathbb{T}_{2,\ell} \otimes \mathbb{Q}$-linear combination

$$\gamma_j = \sum_p T_{j,p} w_p, \quad T_{j,p} \in \mathbb{T}_{2,\ell} \otimes \mathbb{Q}.$$

I can then compute the periods by using the adjointness property of the integration pairing with respect to Hecke operators as follows:

$$\int_{\gamma_j}\omega(\tau)\mathrm{d}\tau=\int_{\sum_p T_{j,p}w_p}\omega(\tau)\mathrm{d}\tau=\sum_p\int_{w_p}(T_{j,p}\omega)(\tau)\mathrm{d}\tau=\sum_p\lambda_{j,p}\int_{w_p}\omega(\tau)\mathrm{d}\tau,$$

where $\lambda_{j,p}\in\mathbb{C}$ denotes the eigenvalue of the newform ω for the Hecke operator $T_{j,p}$. Consequently, all I need is to compute the integrals $\int_{w_p}\omega(\tau)\mathrm{d}\tau$.

The Fricke involution W_ℓ transforms the form $\omega(\tau)$ into $\frac{1}{\ell\tau^2}\omega\left(\frac{-1}{\ell\tau}\right)$. It is useful for my purpose because it can be used to map a point τ with small imaginary part to $\frac{-1}{\ell\tau}$, which may have a much larger imaginary part and hence significantly accelerae the convergence of q-series. Formula A.2.2.33 asserts that if

$$\omega=q+\sum_{n\geqslant 2}a_nq^n\in S_2\big(\Gamma_1(\ell),\varepsilon\big)$$

is a newform of weight 2, level ℓ and nebentypus ε, then $W_\ell\omega$ is the eigenform of weight 2, level ℓ and conjugate nebentypus $\overline{\varepsilon}$ defined by

$$W_\ell\omega=\lambda_\ell(\omega)\left(q+\sum_{n\geqslant 2}\overline{a_n}q^n\right),$$

where $\lambda_\ell(\omega)$ is given by

$$\lambda_\ell(\omega)=\begin{cases}-\overline{a_\ell} & \text{if } \varepsilon \text{ is trivial,}\\ \dfrac{g(\varepsilon)\overline{a_\ell}}{\ell} & \text{if } \varepsilon \text{ is nontrivial,}\end{cases}$$

where $g(\cdot)$ denotes the Gauss sum of a Dirichlet character. Moreover, according to theorem A.2.2.34, if χ is a Dirichlet character modulo $p\neq\ell$, then

$$\omega\otimes\chi=\sum_{n\geqslant 1}a_n\chi(n)q^n$$

is a cuspform of level ℓp^2, and

$$W_{\ell p^2}(\omega\otimes\chi)=\frac{g(\chi)}{g(\overline{\chi})}\varepsilon(p)\chi(-\ell)\cdot(W_\ell\omega)\otimes\overline{\chi}.$$

An easy computation shows that

$$\sum_{a \bmod p}\overline{\chi}(a)\omega(\tau+a/p)=g(\overline{\chi})(\omega\otimes\chi)(\tau).$$

This yields the formula

$$\begin{aligned}\int_{w_p}\omega(\tau)\mathrm{d}\tau&=g(\epsilon_p)\int_\infty^0(\omega\otimes\epsilon_p)(\tau)\mathrm{d}\tau\\&=g(\epsilon_p)\left(\int_\infty^{\frac{i}{p\sqrt{\ell}}}(\omega\otimes\epsilon_p)(\tau)\mathrm{d}\tau+\int_{\frac{i}{p\sqrt{\ell}}}^0(\omega\otimes\epsilon_p)(\tau)\mathrm{d}\tau\right)\\&=g(\epsilon_p)\left(\int_\infty^{\frac{i}{p\sqrt{\ell}}}(\omega\otimes\epsilon_p)(\tau)\mathrm{d}\tau-\int_\infty^{\frac{i}{p\sqrt{\ell}}}W_{\ell p^2}(\omega\otimes\epsilon_p)(\tau)\mathrm{d}\tau\right)\\&=\frac{g(\epsilon_p)}{2\pi i}\sum_{n=1}^{+\infty}\big(a_n-\varepsilon(p)\epsilon_p(-\ell)\lambda_\ell(\omega)\overline{a_n}\big)\frac{\epsilon_p(n)}{n}\left(e^{-\frac{2\pi}{p\sqrt{\ell}}}\right)^n,\end{aligned}$$

which allows me to compute the integral of a newform along a twisted winding element, and thus to finally compute the period lattice of the modular curve $X_1(\ell)$.

I sum power series at $q = e^{-\frac{2\pi}{p\sqrt{\ell}}}$ for primes p, and such a q has small enough modulus to achieve fast convergence. I have indeed checked that $p \leqslant 3$ is very often sufficient for the w_p to span the rational homology of the modular curve over $\mathbb{T}_{2,\ell}$, and $p \leqslant 7$ is enough for all levels $\ell \leqslant 61$, except for $\ell = 37$ in which case I had to go up to $p = 19$.

B.3.3 Computing an ℓ-torsion basis

My goal is to find null-degree divisors D_1 and D_2 representing a basis of the eigenplane

$$V_{f,\mathfrak{l}} = \bigcap_{T \in \mathbb{T}_{2,\ell}} \mathrm{Ker}\left(T - [\mu_{f,\mathfrak{l}}(T)]\right) \subset J_1(\ell)[\ell],$$

where $\mu_{f,\mathfrak{l}}(T_p) = a_p \bmod \mathfrak{l}$ (cf. section A.3.3.3). The period lattice Λ which I have just computed yields an analytic model $J_1(\ell)(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$, and in particular the ℓ-torsion subgroup $J_1(\ell)[\ell](\mathbb{C})$ is represented by $\frac{1}{\ell}\Lambda/\Lambda$. The action of the Hecke algebra $\mathbb{T}_{2,\ell}$ on $\mathbb{S}_2\big(\Gamma_1(\ell)\big)$, and hence on Λ and on $\frac{1}{\ell}\Lambda/\Lambda$, is known explicitly (cf. section A.2.3). As a consequence, I can compute the subspace of $\frac{1}{\ell}\Lambda/\Lambda$ representing $V_{f,\mathfrak{l}}$ as

$$\bigcap_{T \in \mathcal{T}} \mathrm{Ker}\left(T - [\mu_{f,\mathfrak{l}}(T)]\right)\big|_{\frac{1}{\ell}\Lambda/\Lambda} \qquad (\star)$$

by starting with $\mathcal{T} = \emptyset$ and successively adjoining T_2, T_3, etc. to $\mathcal{T}$ until the dimension of the intersection $(\star)$ drops to 2. Proposition A.2.2.32 implies that the Hecke operators T_n for $n \leqslant \frac{\ell^2-1}{6}$ span $\mathbb{T}_{2,\ell}$ as a $\mathbb{Z}$-module, so that should not take too long (it is enough that $\mathcal{T}$ span $\mathbb{T}_{2,\ell}$ as a $\mathbb{Z}_{(\ell)}$-algebra). Actually, in practice, it turns out that it is enough to consider T_2 and T_3, so this is very fast.

I can thus express the vectors x_1, x_2 making up an $\mathbb{F}_\ell$-basis of $V_{f,\mathfrak{l}}$ as points in $\mathbb{C}^g/\Lambda$. I fix g points $P'_1, \cdots, P'_g \in X_1(\ell)(\mathbb{C})$, and for each $k \in \{1, 2\}$, I lift x_k to $\widetilde{x_k} \in \mathbb{C}^g$, then I use Newton iteration to compute g points $P'_1, \cdots, P'_g \in X_1(\ell)(\mathbb{C})$, with each P'_j close to P_j, such that

$$\sum_{j=1}^{g} \left(\int_{P_j}^{P'_j} \omega_i(\tau) \mathrm{d}\tau \right)_{1 \leqslant i \leqslant g} = \frac{\widetilde{x_k}}{2^m}. \qquad (\star\star)$$

Here $m \in \mathbb{N}$ is an integer, and I introduced the 2^m factor so as to help the Newton iteration scheme to converge by ensuring that for each j, P'_j stays well-inside the coordinate disk containing P_j (see below). The integral from P_j to P'_j is understood to be along a path which stays inside this disk, so that the left-hand side of $(\star\star)$ is well-defined in $\mathbb{C}^g$.

If the effective divisor $P_1 + \cdots + P_g \in \mathrm{Eff}^g\left(X_1(\ell)\right)$ is not special, then the map

$$(P'_1, \cdots, P'_g) \longmapsto \sum_{j=1}^{g} \left(\int_{P_j}^{P'_j} \omega_i(\tau) \mathrm{d}\tau \right)_{1 \leqslant i \leqslant g}$$

is a local diffeomorphism at $(P'_1, \cdots, P'_g) = (P_1, \cdots, P_g)$, so for m large enough, the equation $(\star\star)$ in $(P'_1, \cdots, P'_g)$ has a unique solution in a neigbourhood of $(P_1, \cdots, P_g)$, which will lie in the convergence domain of the Newton iteration scheme if m is large enough. In practice I use $m \approx 10$.

More precisely, I first pick g (not necessarily distinct) cusps c_1, $\cdots$, c_g. For each of these cusps, there is an analytic map, the "q-coordinate" around c_j

$$\kappa_j \colon \mathbb{E} \longrightarrow X_1(\ell)(\mathbb{C})$$

where $\mathbb{E}$ stands for the open unit disk in $\mathbb{C}$, which maps 0 to the cusp c_j and which is a local diffeomorphism. Next, I choose g complex numbers q_1, $\cdots$, q_g of small moduli, and I let $P_j = \kappa_j(q_j)$, which is thus close to the cusp c_j. Consider another vector of g small complex numbers δ_1, $\cdots$, δ_g. The goal is to adjust this vector so that $(\star\star)$ be satisfied with $P'_j = \kappa_j(q_j + \delta_j)$. In a nutshell, the overall map I apply Newton iteration to is

$$\begin{array}{ccccccc} U & \xrightarrow{\prod \kappa_j} & X_1(\ell)^g & \longrightarrow & \operatorname{Div}^0 X_1(\ell) & \longrightarrow & \mathbb{C}^g \\ (\delta_j)_{1\leqslant j\leqslant g} & \longmapsto & (P'_j)_{1\leqslant j\leqslant g} & \longmapsto & \displaystyle\sum_{j=1}^{g}(P'_j - P_j) & \longmapsto & \displaystyle\sum_{j=1}^{g}\left(\int_{P_j}^{P'_j}\omega_i(\tau)\mathrm{d}\tau\right)_{1\leqslant j\leqslant g} \end{array},$$

where U is a neighbourhood of $0 \in \mathbb{E}^g$ such that $(q_j + \delta_j)_{1\leqslant j\leqslant g}$ remains in $\mathbb{E}^g$ for all $(\delta_j)_{1\leqslant j\leqslant g} \in U$. The differential of this map is given by the newforms ω_i themselves evaluated at the P'_j, so using this map for Newton iteration presents no difficulty.

Once this is done, I need to double the divisor class of

$$D_k^{(m)} = \sum_{j=1}^{g}(P'_j - P_j)$$

m times by using K. Khuri-Makdisi's algorithms, so as to get a divisor representing x_k. This is however not so immediate, since these algorithms only deal with divisors of the form $D - D_0$, where D is an effective divisor of degree d_0, D_0 and d_0 being defined in the beginning of the section B.2.1. To work around this, I fix what I call a *padding divisor*, that is to say an effective divisor C of degree $d_0 - g = g + 1$, then I feed the divisors $\sum_{j=1}^{g} P'_j + C - D_0$ and $\sum_{j=1}^{g} P_j + C - D_0$ (which are indeed of the form $D - D_0$) to K. Khuri-Makdisi's algorithms, and finally I use these algorithms to subtract these two divisor classes. Feeding a divisor $D - D_0$ to K. Khuri-Makdis's algorithms is easy: it amounts to computing the subspace $W_D = H^0\big(X_1(\ell), 3D_0 - D\big)$ of $V = H^0\big(X_1(\ell), 3D_0\big)$ consisting of functions of V which vanish at D. I do so by evaluating the q-series in the basis of V at the points of D and by doing linear algebra. Since I shall thus have to evaluate q-series at C, it proves convenient to choose a divisor C supported by cusps, hence the notation C.

Finally, once the divisor $D_k^{(m)}$ is processed, I apply Khuri-Makdisi's chord algorithm A.1.3.12 on it, yielding $(-2)^m[D_k^{(m)}] = \pm x_k$. The $\pm$ sign is not a problem, because I get a basis $(\pm x_1, \pm x_2)$ for $V_{f,\mathfrak{l}}$ no matter what the signs are, and this is all I actually need.

B.3.4 Evaluating the torsion divisors

I must construct a Galois-equivariant function $\alpha \in \mathbb{Q}\big(J_1(\ell)\big)$ which can be efficiently evaluated at every point $x \in V_{f,\mathfrak{l}}$ given in Khuri-Makdisi form. I shall then evaluate α in each non-zero point of $V_{f,\mathfrak{l}}$, and form the polynomial

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

which encodes the Galois representation $\rho_{f,\mathfrak{l}}$. In order to recognise its coefficients as rational numbers, I compute the continued fraction expansion of each of them until I find a huge term. Clearly, the lower the height of $F(X)$ the better, as it requires performing all the computations described above with less precision in $\mathbb{C}$ in order to be able to identify the coefficients. This means that I should use an evaluation function α which is arithmetically well-behaved. In order to try to quantify this, I may look at the class of its divisor of poles (or zeroes) in the Néron-Severi group of $J_1(\ell)$; I expect that the "smaller" this class is, the better the arithmetic behaviour of α will be.

The approach used in [CE11], [Bos07] and [ZJ13] consists in selecting a rational function ξ on $X_1(\ell)$ which is defined over $\mathbb{Q}$, and extending it to $J_1(\ell)$ by

$$\begin{array}{rccc} \Xi\colon & J_1(\ell) & \dashrightarrow & \mathbb{C} \\ & \left[\sum_{i=1}^{g} P_i - gO\right] & \longmapsto & \sum_{i=1}^{g} \xi(P_i), \end{array}$$

where g denotes the genus of $X_1(\ell)$ and $O \in X_1(\ell)(\mathbb{Q})$ is an origin for the Abel-Jacobi map. Indeed, by the Riemann-Roch theorem A.1.1.33(v), each divisor class $x \in \mathrm{Pic}^0\big(X_1(\ell)\big)$ can be written as $[E_x - \Omega]$, where Ω is a fixed divisor of degree g and E_x is an effective divisor of degree g which is unique for generic x, so this does define a rational function on $J_1(\ell)$, which is defined over $\mathbb{Q}$ since O and ξ are. The divisor of the poles of this function is

$$(\Xi)_\infty = \sum_{Q \text{ pole of } \xi} \tau^*_{[Q-O]}\Theta,$$

where τ_x denotes the translation by x map on $J_1(\ell)$ and Θ is the theta divisor on $J_1(\ell)$ attached to the Abel-Jacobi map with origin O. Thus $(\Xi)_\infty$ is the sum of $\deg \xi$ translates of Θ. If I am to let this function Ξ play the role of α, then I want it to be be arithmetically well-behaved, so that I should take a ξ with degree as low as possible. However, this degree is by definition at least the gonality of $X_1(\ell)$, which is roughly proportional to g (cf. [Abr96, remark 0.2]), so this method becomes less and less effective as the genus grows.

For this reason, I introduce a radically different method, which can be used to construct a function $\alpha \in \mathbb{Q}\big(\mathrm{Jac}(X)\big)$ on the jacobian of any algebraic curve X. Let g be the genus of X. As previously, every point $x \in \mathrm{Jac}(X)$ can be written as $[E_x - gO]$, where E_x is an effective divisor of degree g on X which is generically

unique, and $O \in X$ is a fixed point. Let Π be a fixed divisor on X of degree $2g$. Then, again by the Riemann-Roch theorem A.1.1.33(v), the space $H^0(X, \Pi - E_x)$ is generically 1-dimensional over $\mathbb{C}$, say spanned by $t_x \in \mathbb{C}(X)$. The divisor of t_x is of the form $(t_x) = -\Pi + E_x + R_x$, where R_x is a residual effective divisor of degree g on X, which is the image of E_x by the reflection

$$\begin{array}{rccc} R_\Pi\colon & \mathrm{Pic}^g(X) & \longrightarrow & \mathrm{Pic}^g(X) \\ & [E] & \longmapsto & [\Pi - E]. \end{array}$$

Let A and B be two points on X disjoint from the support of Π. I can then define

$$\begin{array}{rccc} \alpha\colon & \mathrm{Jac}(X) & \dashrightarrow & \mathbb{C} \\ & x & \longmapsto & \frac{t_x(A)}{t_x(B)}. \end{array}$$

This map is well-defined only on a Zariski-dense subset of $\mathrm{Jac}(X)$ because of the genericity assumptions, and it is defined over $\mathbb{Q}$ if X, Π, A, B and O are. Moreover, it is much better-behaved than the function Ξ used in the classical approach:

Theorem B.3.4.1. *The divisor of poles of α is the sum of only two translates of the Θ divisor.*

Proof. The function α has a pole at $x \in \mathrm{Jac}(X)$ if and only if $[E_x - gO]$ or $[R_x - gO]$ are on the support of $\tau^*_{[B-O]}\Theta$. But $[R_x - gO]$ is the image of $[E_x - gO]$ by the involution $R_\Pi = \tau_{[\Pi - 2gO]} \circ [-1]$ defined above, and $[-1]^*\Theta = \tau^*_{\mathcal{K}}\Theta$ is the translate of Θ by the image $\mathcal{K}$ of the canonical class, cf. [HS00, theorem A.8.2.1.i]. □

This is even in some sense optimal, since by the Riemann-Roch theorem for abelian varieties (cf. [HS00, theorem A.5.3.3]), no non-constant function on $\mathrm{Jac}(X)$ has a single translate of Θ as divisor of poles, whereas the Néron-Severi group of the jacobian of a generic curve is infinite cyclic and spanned by Θ.

In order to make this practical on the modular curve $X_1(\ell)$, there is a difficulty which must be overcome: In K. Khuri-Makdisi's algorithms, a divisor class $x \in J_1(\ell)$ is represented by a subspace $W_D = H^0\big(X_1(\ell), 3D_0 - D\big) \subset V$, where D is an effective divisor of degree $d_0 = 2g + 1$ such that $[D - D_0] = x$, but such a D is far from being unique — by the Riemann-Roch theorem A.1.1.33(i), there is a whole $(g+1)$-dimensional projective space of them ! Thus, the first thing to do is to rigidify the representation W_D of x into a representation which depends on x only. To do this, I compute the sub-subspace

$$W_{D,\mathrm{red}} = H^0\big(X_1(\ell), 3D_0 - D - C_1\big) \subset W_D,$$

where C_1 is a fixed effective divisor of degree $d_1 = 2d_0 - g$, so that $W_{D,\mathrm{red}}$ will generically be 1-dimensional by the Riemann-Roch theorem A.1.1.33(v). Let $s_D \in V$ be such that $W_{D,\mathrm{red}} = \mathbb{C}s_D$. Its divisor is of the form

$$\mathrm{div}(s_D) = -3D_0 + D + C_1 + E_D,$$

where E_D is some effective divisor of degree g. Again by the Riemann-Roch theorem A.1.1.33(iv), E_D is generically alone in its linear equivalence class. But on the other

hand, if W_D and $W_{D'}$ both represent the same point $x \in J_1(\ell)(\mathbb{C})$, then $D \sim D'$, so that $E_D \sim E_{D'}$ as D_0 and C_1 are fixed. Consequently, one generically has $E_D = E_{D'}$, which shows that E_D only depends on x and not on D, so that the process $W_D \mapsto E_D$ is the rigidification which I am looking for. I then use a trick *à la* Khuri-Makdisi: I first compute

$$s_D \cdot V = \{s_D v,\ v \in V\} = H^0\big(X_1(\ell), 6D_0 - D - C_1 - E_D\big)$$

by using the "multiply-by-function" block A.1.3.7, after which I compute

$$H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big) = \{v \in V \mid vW_D \subset s_D \cdot V\}$$

by using the "subtract" block A.1.3.8. Next, I fix another effective divisor C_2 of degree $d_2 = d_0 + 1 - g$, so that the subspace $H^0\big(X_1(\ell), 3D_0 - C_1 - C_2 - E_D\big)$ of the previously computed space $H^0\big(X_1(\ell), 3D_0 - C_1 - E_D\big)$ is generically one-dimensional. Letting $\Pi = 3D_0 - C_1 - C_2$, I thus have computed a function $t_D \in \mathbb{C}\big(X_1(\ell)\big)$ such that

$$\mathbb{C}t_D = H^0\big(X_1(\ell), \Pi - E_D\big),$$

as wanted. This allows me to compute the map α, which is defined over $\mathbb{Q}$ as long as C_1, C_2, A and B are. As in the previous section, it proves convenient to choose the divisors C_1 and C_2 to be supported by cusps, so that the q-series can be evaluated effortlessly, hence the notation C_1 and C_2.

Evaluating α on $V_{f,\mathfrak{l}}$, I may thus hope to get a defining polynomial $F(X)$ of logarithmic height $g/2$ times less than if I had used the classical approach. A numerical comparison of these two methods may be found in [DvHZ14, table 2 p.8].

Table B.3.4.2 below, which compares the genus $g = \frac{(\ell-5)(\ell-7)}{24}$ of the modular curves $X_1(\ell)$ to the rough number h of decimal digits in the common denominator of the polynomials $F(X)$ associated to newforms of level $N = 1$ (cf. the Tables section below) which I computed using the algorithm currently being described, seems to indicate that the heuristic performance of my method is $h \approx g^{2.5}$.

ℓ	g	h
11	1	0
13	2	5
17	5	50
19	7	150
23	12	500
29	22	1800
31	26	2500

Table B.3.4.2: Comparison of the size h of coefficients of $F(X)$ (computed with my method) with the genus g of $X_1(\ell)$

B.3.5 Finding the Frobenius elements

After evaluating a suitable function in the torsion divisors representing the points of $V_{f,\mathfrak{l}} \setminus \{0\}$, I have thus got a polynomial $F(X) \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$ whose decomposition field is the field L fixed by the kernel of the Galois representation. It is thus a Galois number field, and its Galois group over $\mathbb{Q}$ is embedded by the representation $\rho_{f,\mathfrak{l}}$ into $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$. I would now like to know the image of the Frobenius elements Frob_p in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$, especially so as to get the value of the coefficients a_p of f modulo $\mathfrak{l}$ by looking at the trace.

The roots $\alpha(x)$, $x \in V_{f,\mathfrak{l}} - \{0\}$ of $F(X)$ come by construction with an indexing by $V_{f,\mathfrak{l}} - \{0\}$ such that the Galois action of $G_\mathbb{Q}$ on them corresponds to its $\rho_{f,\mathfrak{l}}$-action on the indices, so that I am perfectly poised to use the Dokchitsers' method described in section A.3.2.

This allows me to determine the similarity class of $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ for almost all primes $p \in \mathbb{N}$. It fails only if $F(X)$ is not integral or not squarefree modulo p, or if two resolvents $\Gamma_C(X)$ (defined in section A.3.2) do not remain coprime when reduced modulo p. However, the primary goal of my computations is to find the coefficients a_p of the q-expansion of f modulo $\mathfrak{l}$, and as naive methods compute a_p for small p in almost no time, the only case I am really interested in is the case of extremely large (if not titanic) p, for which failure is extremely unlikely. The only thing to do is to find a polynomial $h(X) \in \mathbb{Z}[X]$ such that the resolvents $\Gamma_C(X)$ are pairwise coprime over $\mathbb{Q}$, and in practise either $h(X) = X^2$ or $h(X) = X^3$ works.

Once the resolvents are computed, it is easy to deduce what $\rho_{f,\mathfrak{l}}(\mathrm{Frob}_p)$ is similar to, and hence to compute the coefficients a_p of f modulo $\mathfrak{l}$.

B.3.5.1 The quotient representation trick

Unfortunately, these computations, although simple, can be rather slow because they require performing operations on very high precision approximations of certain complex numbers, due to the large height of the coefficients of $F(X)$. For instance, for $\ell = 29$, about 5 million decimal digits after the decimal point are required to compute the resolvents, so that the computation is almost intractable.

For this reason, I present a simple trick, which in most cases allows to sharply reduce the amount of computations needed. The key is that I have not yet used the fact that I know in advance what the determinant of the image of the Frobenius element Frob_p is, namely $\varepsilon(p)p^{k-1} \bmod \mathfrak{l}$, where k and ε denote respectively the weight and the nebentypus of the newform f.

The idea is then to compute a *quotient* representation, that is to say the representation $\rho_{f,\mathfrak{l}}$ composed with the projection map from $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ onto one its quotient groups. The coarser the quotient, the smaller the computation, so one should use a quotient just fine enough to be able to lift correctly an element back to $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ provided that the determinant of the lift is known. For instance, $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$ is slightly too coarse, because the knowledge of the image of a matrix in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$ and of its determinant only determines this matrix up to sign. This is the very reason why J. Bosman, for computing only the projective Galois representation in [Bos07], determined the coefficients a_p of f only up to sign. However, some intermediate quotients between GL_2 and PGL_2 will do:

Lemma B.3.5.1. *Embed $\mathbb{F}_\ell^*$ into $\mathrm{GL}_2(\mathbb{F}_\ell)$ by $\lambda \mapsto \left[\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right]$. Let S be a subgroup of $\mathbb{F}_\ell^*$, and let $\pi\colon \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S$ be the projection morphism. Then the group morphism*

$$\begin{array}{rccc}\phi\colon & \mathrm{GL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S \times \mathbb{F}_\ell^* \\ & g & \longmapsto & \big(\pi(g), \det(g)\big)\end{array}$$

is injective if and only if $-1 \notin S$.

Proof. Let $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$. If $g \in \operatorname{Ker}\phi$, then in particular $g \in \operatorname{Ker}\pi$, so that there exists a scalar $s \in S$ such that $g = \left[\begin{smallmatrix}s & 0\\ 0 & s\end{smallmatrix}\right]$. Since also $\det g = 1$, one has $s^2 = 1$, hence $s = \pm 1$. The result follows. □

In the light of this result, I let S to be the largest subgroup of $\mathbb{F}_\ell^*$ such that $-1 \notin S$. This is the subgroup made up of the elements of odd order in $\mathbb{F}_\ell^*$, that is to say, the $2'$-subgroup of $\mathbb{F}_\ell^*$. If $\ell - 1 = 2^r m$ with r, $m \in \mathbb{N}$ and m odd, its order is $\#S = m$.

Let the associated quotient Galois representation be

$$\rho_{f,\mathfrak{l}}^S\colon G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \xrightarrow{\pi} \mathrm{GL}_2(\mathbb{F}_\ell)/S.$$

Then the image of the morphism $\rho_{f,\mathfrak{l}}^S \times \overline{\chi}_\ell^{k-1}$ is contained in the image of ϕ, so the map

$$\varrho\colon G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}^S \times \overline{\chi}_\ell^{k-1}} \mathrm{GL}_2(\mathbb{F}_\ell)/S \times \mathbb{F}_\ell^* \xrightarrow{\phi^{-1}} \mathrm{GL}_2(\mathbb{F}_\ell)$$

is well-defined, and agrees with $\rho_{f,\mathfrak{l}}$.

To compute the linear representation $\rho_{f,\mathfrak{l}}$, it is therefore enough to compute the quotient representation $\rho_{f,\mathfrak{l}}^S$. This amounts to describing the Galois action on the quotient space $V_{f,\mathfrak{l}}/S$. I thus begin by computing a polynomial $F^S(X) \in \mathbb{Q}[X]$ corresponding to the action of $G_{\mathbb{Q}}$ on $V_{f,\mathfrak{l}}/S$, by tracing the roots $\alpha(x)$, $0 \neq x \in V_{f,\mathfrak{l}}$ of $F(X)$ along their orbits under S:

$$F^S(X) = \prod_{\substack{Sx \in V_{f,\mathfrak{l}}/S \\ x \neq 0}} \left(X - \sum_{s \in S} \alpha(sx) \right).$$

This new polynomial has roughly the same height as the original $F(X)$, but its degree is $\#S$ times smaller.

Next, I compute a resolvent $\Gamma_{\overline{C}}(X)$ for each conjugacy class $\overline{C}$ of $\mathrm{GL}_2(\mathbb{F}_\ell)/S$. As the subgroup S of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is central, these conjugacy classes are easy to describe:

Lemma B.3.5.2. *Let $\pi\colon \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S$ denote the projection map, let $\overline{g} \in \mathrm{GL}_2(\mathbb{F}_\ell)/S$, and let $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\pi(g) = \overline{g}$. Then π induces a bijection*

$$\begin{array}{rccc}\pi_g\colon & \textit{Conjugacy class of } g & \xrightarrow{\sim} & \textit{Conjugacy class of } \overline{g} \\ & hgh^{-1} & \longmapsto & \pi(hgh^{-1}).\end{array}$$

Proof. It is clear that the image of the conjugacy class of g by π is exactly the conjugacy class of $\overline{g}$, so that π_g is well-defined and surjective. To show that π_g is also injective, let h_1, $h_2 \in \mathrm{GL}_2(\mathbb{F}_\ell)$ such that $\pi(h_1 g h_1^{-1}) = \pi(h_2 g h_2^{-1})$, that is to say

such that $h_1 g h_1^{-1} = s h_2 g h_2^{-1}$ for some $s \in S$. I must prove that $h_1 g h_1^{-1} = h_2 g h_2^{-1}$. By taking determinants, one sees that $\det s = 1$. As s is scalar, this implies $s = \pm 1$. Since $-1 \notin S$, one concludes that $s = 1$, and therefore $h_1 g h_1^{-1} = h_2 g h_2^{-1}$. □

A resolvent $\Gamma_{\overline{C}}(X)$ has therefore exactly the same degree as (each of) the corresponding $\Gamma_C(X)$, so I still have to use the same very high precision in $\mathbb{C}$ to compute it. However, I now have $\#S$ times less such resolvents to compute. Furthermore, the roots $\sum_{i=1}^{n} h(a_i)\sigma(a_i)$ of these resolvents actually take $(\#S)^2$ less time to compute, since they are defined by sums $\#S$ times shorter and there are $\#S$ times less of them.

Using these resolvents $\Gamma_{\overline{C}}(X)$, I can then determine the conjugacy class of the image of the Frobenius element Frob_p in $\mathrm{GL}_2(\mathbb{F}_\ell)/S$ as above, and since $-1 \notin S$, I can deduce the similarity class of the image of the Frobenius element in $\mathrm{GL}_2(\mathbb{F}_\ell)$ using the fact that its determinant is $p^{k-1} \bmod \ell$. Consequently, with this trick, I can still compute the linear representation $\rho_{f,\mathfrak{l}}$, saving a factor $(\#S)^2$ in the computation of the roots of the resolvents, and a factor $\#S$ in their expansion and in the identification of their coefficients as rational numbers.

Since

$$\#S = m = \frac{\ell - 1}{2^{\mathrm{ord}_2(\ell-1)}},$$

this prevents this final step of the Galois representation computation from being the slowest one, as explained in section B.4.

B.3.5.2 Reducing the polynomials

The biggest problem is that the coefficients of the polynomial $F(X)$ tend to have larger and larger height as ℓ grows. More precisely, table B.3.4.2 seems to indicate that this logarithmic height grows as $g^{2.5}$. While this is rather harmless for $l \leqslant 17$ (that is to say $g \leqslant 5$), it makes the Dokchitsers' method intractable as soon as $\ell \geqslant 29$, even with the quotient representation trick. It is thus necessary to reduce this polynomial, that is to say to compute another polynomial whose rupture field is isomorphic to the rupture field of $F(X)$ but whose coefficients are much nicer. An algorithm to perform this task based on LLL lattice reduction is described in [Coh93, section 4.4.2] and implemented in [Pari/GP] under the name `polred`. Unfortunately, the polynomial $F(X)$ has degree $\ell^2 - 1$ and tends to have ugly coefficients, and this is too much for `polred` to be practical, even for small values of ℓ.

On the other hand, it would be possible to apply the `polred` algorithm to the polynomial

$$F^{\mathrm{proj}}(X) = \prod_{W \in \mathbb{P}V_{f,\mathfrak{l}}} \left(X - \sum_{\substack{x \in W \\ x \neq 0}} \alpha(x) \right) \in \mathbb{Q}[X]$$

whose splitting field is the number field L^{proj} cut out by the *projective* Galois representation

$$\rho_{f,\mathfrak{l}}^{\mathrm{proj}} \colon\ G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)\ ,$$

but this representation does not contain enough information to recover the values of $a_p \bmod \mathfrak{l}$.

However, I have just explained above that working with $F^{\mathrm{proj}}(X)$ is not enough to recover the values of $a_p \bmod \mathfrak{l}$, whereas working with $F^S(X)$ is. If the degree and height of $F^S(X)$ are not too large, then I can apply the `polred` algorithm to it directly. Write $\ell - 1 = 2^r m$. Since $\#S = m$, the degree of $F^S(X)$ is $2^r(\ell+1)$, so I can `polred` it directly in the cases $\ell = 19$ or 23, but the cases $\ell = 29$ or 31 remain impractical.

For these remaining cases, Bill Allombert suggested to me that one can still reduce $F^S(X)$ in several steps, as I now explain. Since $\mathbb{F}_\ell^*$ is cyclic, there is a filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $[S_i : S_{i+1}] = 2$ for all i, namely

$$S_i = \mathrm{Im}\begin{pmatrix} \mathbb{F}_\ell^* & \longrightarrow & \mathbb{F}_\ell^* \\ x & \longmapsto & x^{2^i} \end{pmatrix}.$$

For each i, let

$$F_i(X) = \prod_{\substack{S_i x \in V_{f,\mathfrak{l}}/S_i \\ x \neq 0}} \left(X - \sum_{s \in S_i} \alpha(sx) \right) \in \mathbb{Q}[X],$$

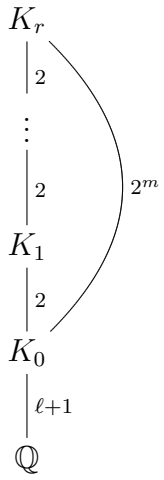
$$K_i = \mathbb{Q}[X]/F_i(X),$$

and let L_i be the Galois closure of K_i, that is to say the number field cut out by the quotient representation

$$\rho_{f,\mathfrak{l}}^{S_i} \colon\ G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i\ .$$

In particular, one has $\rho_{f,\mathfrak{l}}^{S_0} = \rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, $L_0 = L^{\mathrm{proj}}$, and I am looking for a nice model of K_r.

The fields K_i fit in an extension tower



and the trick is to `polred` the polynomials $F_i(X)$ along this tower recursively from bottom up, as I now explain.

First, I apply directly the `polred` algorithm to $F_0(X) = F^{\mathrm{proj}}(X)$. Since the degree of this polynomial is only $\ell + 1$, this is amenable, as mentioned above.

I then proceed by induction. Assuming that I have managed to reduce $F_i(X)$, I have a nice model for $K_i = \mathbb{Q}[X]/F_i(X)$, so I can factor $F_{i+1}(X)$ in $K_i[X]$. Since the extension $K_{i+1} = \mathbb{Q}[X]/F_{i+1}(X)$ is quadratic over K_i, there must be at least one factor of degree 2. Let $G_{i+1}(X)$ be one of those, and let $\Delta_i \in K_i$ be its discriminant, so that

$$K_{i+1} \simeq K_i[X]/G_{i+1}(X) \simeq K_i\big(\sqrt{\Delta_i}\big).$$

In order to complete the induction, all I have to do is to strip Δ_i from the largest square factor I can find, say $\Delta_i = A_i^2\delta_i$ with $A_i, \delta_i \in K_i$ and δ_i as small as possible. Indeed, I then have $K_{i+1} = K_i\big(\sqrt{\delta_i}\big)$, and actually even $K_{i+1} = \mathbb{Q}\big(\sqrt{\delta_i}\big)$ unless I am very unlucky[4], so that if $\chi_i(X) \in \mathbb{Q}[X]$ is the characteristic polynomial of δ_i, then one has

$$K_{i+1} \simeq \mathbb{Q}[X]/\chi_i(X^2),$$

and so $\chi_i(X^2)$ is a reduced version of F_{i+1}. If its degree and coefficients are not too big, I can even apply the `polred` algorithm to this polynomial in order to further reduce it, which is what I do in practice since it makes the next step of the induction faster.

In order to decompose Δ_i into $A_i^2\delta_i$, I would like to factor Δ_i in K_i, but even if K_i were principal, this would not be amenable whatsoever. I can however consider the ideal generated by Δ_i in K_i, and remove its ℓ-part. The fractional ideal $\mathfrak{B}_i$ which I obtain must then be a perfect square, since K_{i+1} is unramified outside ℓ (since L is), and the very efficient `idealsqrt` script from [BS14] can explicitly factor it into $\mathfrak{B}_i = \mathfrak{A}_i^2$. If A_i denotes an element in $\mathfrak{A}_i$ close to being a generator of $\mathfrak{A}_i$ (that is to say of norm not much bigger than the norm of A_i), or even an actual generator if amenable, then $\delta_i = \Delta_i/A_i^2$ must be small, so this does the trick.

B.4 Complexity analysis

The most time-consuming part of the computation of the polynomial $F(X) \in \mathbb{Q}[X]$ defining the representation is the arithmetic in the jacobian $J_1(\ell)$. To perform these operations, K. Khuri-Makdisi's algorithms rely on linear algebra on matrices of size $O(g) \times O(g)$; as $g = \frac{(\ell-5)(\ell-7)}{24} = O(\ell^2)$, and since my algorithm computes $O(\ell^2)$ ℓ-torsion points in the jacobian, this implies a complexity of $O(\ell^8)$ operations in $\mathbb{C}$ to compute the Galois representation.

Let h be the logarithmic height of $F(X)$, so that computing $F(X)$ with my algorithm requires a precision of $O(h)$ bits in $\mathbb{C}$. Then the complexity of my method to find $F(X)$ is $\widetilde{O}(\ell^8 h)$ bit operations. The experiments which I have run (cf. table B.3.4.2) seem to indicate that h is $O(g^{5/2}) = O(\ell^5)$, but I do not try to refine this estimate, because I do not know a proven sharp[5] bound on h.

[4]The case $K_{i+1} \supsetneq \mathbb{Q}\big(\sqrt{\delta_i}\big)$ has never happened to me in practice. Should it happen, it can be corrected by multiplying δ_i by the square of an (hopefully small) element in K_i.

[5]B. Edixhoven and R. de Jong proved the bound $h = O(\ell^{16})$ in [CE11, theorem 11.7.6], but that seems really pessimistic compared to table B.3.4.2, and it is completely impractical to use ℓ^{16} bits of precision in $\mathbb{C}$, even in the small genus cases: even all the hard drives in Bordeaux university put together would barely be enough to store just one complex number with such an insane accuracy.

Next, if I did not use the quotient representation trick (cf. section B.3.5.1), computing a root $\sum_x h(a_x)a_{g(x)}$ of a Dokchitsers' resolvent $\Gamma_C(X)$ would require $O(\deg F) = O(\ell^2)$ operations in $\mathbb{C}$. As there is one such root for each $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$, computing all these roots would require $O(\ell^6)$ operations in $\mathbb{C}$. Then, computing a resolvent $\Gamma_C(X)$ from its roots would require $\widetilde{O}\big(\deg \Gamma_C(X)\big) = \widetilde{O}(\ell^2)$ operations in $\mathbb{C}$ using a fast Fourier transform. As there are $O(\ell^2)$ similarity classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$, computing all the resolvents $\Gamma_C(X)$ from their roots would require $\widetilde{O}(\ell^4)$ operations in $\mathbb{C}$. Thus the overall computation of all the resolvents would require $O(\ell^6)$ operations in $\mathbb{C}$, the slow part being the computation of their roots. The precision in $\mathbb{C}$ I would have to work at for this is $O(\ell^2 h)$, so that the total complexity of the computation of the resolvents $\Gamma_C(X)$ would be $\widetilde{O}(\ell^8 h)$ bit operations, which is the same as the rest of the computation.

However, with the quotient representation trick, computing the resolvent roots $\sum_x h(a_x)a_{g(x)}$ requires only $O(\ell^6/|S|^2) = O(\ell^4\ell_2^2)$ operations in $\mathbb{C}$, where $\ell_2 = 2^r$ is the 2-primary part of $\ell - 1$, and then computing the resolvents $\Gamma_{\overline{C}}(X)$ from these roots takes only $\widetilde{O}(\ell^4/|S|) = \widetilde{O}(\ell^3\ell_2)$ operations in $\mathbb{C}$. Therefore, computing the resolvents $\Gamma_{\overline{C}}(X)$ overall requires $\widetilde{O}(\ell^6\ell_2^2 h)$ bit operations, since the precision in $\mathbb{C}$ I have to work at is still $O(\ell^2 h)$. So, for instance, the use of this trick allows me to reduce the complexity of the computation of the resolvents $\Gamma_{\overline{C}}(X)$ by a factor ℓ^2 if I restrict to the primes $\ell \equiv -1 \bmod 4$. Note that restricting to such ℓ does not worsen the complexity of the computation of coefficients a_p of f by Chinese remainders. On the other hand, in the worst cases $\ell = 2^\lambda + 1$ for some $\lambda \in \mathbb{N}$, this trick unfortunately does not help at all.

Although its use sharply reduces the computational effort for large ℓ, I shall not try to quantify here the impact of the quadratic tower reduction trick presented in section B.3.5.2, as I do not know the complexity of the `idealsqrt` script from [BS14].

Finally, once the polynomial $F(X)$ and the resolvents $\Gamma_{\overline{C}}(X)$ are computed for some fixed f and $\mathfrak{l}$, then the element $h(\overline{a})\overline{a}^p$ can be computed in the $\mathbb{F}_p$-algebra $\mathbb{F}_p[\overline{a}] = \mathbb{F}_p[X]/F(X)$ in $O(\log p)$ operations in $\mathbb{F}_p$ by a square-and-multiply approach, and computing its trace u to $\mathbb{F}_p$ and evaluating the resolvents $\Gamma_{\overline{C}}(X)$ at u requires $O(1)$ operations in $\mathbb{F}_p$. Since each arithmetic operation in $\mathbb{F}_p$ can be performed in $\widetilde{O}(\log p)$ bit operations thanks to fast arithmetic, the coefficient a_p of f can be determined modulo $\mathfrak{l}$ in only $\widetilde{O}(\log^2 p)$ bit operations. It is therefore possible to compute $a_p \bmod \mathfrak{l}$ for titanic primes p having thousands of decimal digits, cf. the tables in section C.1.

The practical computation times achieved by my algorithm are indicated in table C.1.0.1 below.

Part C

Tables and proof of the computation results

Alors ?

— Jean-Marc Couveignes

C.1 Tables

I have computed all the Galois representations $\rho_{f,\mathfrak{l}}$ attached to the newforms $f \in S_k(1)$ of level $N = 1$ and of weight k modulo the non-exceptional[1] primes $\mathfrak{l}$ of degree 1 and lying above the rational primes ℓ ranging from $k+1$ to 31, along with the much easier case of the Galois representation $\rho_{\Delta,11}$ attached to Δ mod 11 and which is afforded by the 11-torsion of the elliptic curve $X_1(11)$ as a warm-up.

According to Maeda's conjecture, for each weight k there is only one newform in $S_k(1)$ up to $G_{\mathbb{Q}}$-conjugation. This conjecture has been verified in [FW02] for k up to 2000, and since I work with newforms of level 1 and weight k up to only 30 (because of the condition $k < \ell$), I may denote without ambiguity one of the newforms in $S_k(1)$ by f_k, and the coefficients of its q-expansion at infinity by $\tau_k(n)$. Then, for each k, the newform f_k and the sequence $\big(\tau_k(n)\big)_{n\geqslant 2}$ are well-defined up to $G_{\mathbb{Q}}$-action, and the newforms in $S_k(1)$ are the $G_{\mathbb{Q}}$-conjugates of

$$f_k = q + \sum_{n=2}^{+\infty} \tau_k(n) q^n.$$

Thus for instance $f_{12} = \Delta$, $\tau_{12} = \tau$ is Ramanujan's τ-function,

$$f_{16} = E_4\Delta = q + \sum_{n=2}^{+\infty} \tau_{16}(n) q^n$$

is the only newform of level 1 and weight 16, and so on. Although I would have liked to treat other similar cases, the only newform with non-rational coefficients for

[1] In the sense of definition A.3.3.9

which I have computed the attached Galois representation was f_{24}, for which I have computed the Galois representations only modulo the primes lying above $\ell = 31$, due to the conditions that $\mathfrak{l}$ be of degree 1 and that $k < \ell$.

For each Galois representation $\rho_{f,\mathfrak{l}}$, I denote by L the number field it cuts out, and I give the image of the Frobenius element $\left(\frac{L/\mathbb{Q}}{p}\right)$ at p for the 40 first primes p above 10^{1000}. Since these p are unramified, these Frobenius elements are well-defined up to conjugacy, so their images are well-defined up to similarity. I represent a similarity class in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ by its *minimal* polynomial in factored form over $\mathbb{F}_\mathfrak{l}$, as explained in remark A.3.2.2.

I carried out my computations on the PlaFRIM experimental testbed of the Bordeaux university. The softwares used were [SAGE] for the main part of the computation, and [Pari/GP] for the polynomial reduction.

For each ℓ, I indicate in table C.1.0.1 below the precision in $\mathbb{C}$ (in bits) at which I chose to perform the computations (it had to be at least twice the height of the coefficients of the output polynomial $F(X)$ describing the field cut out by the representation), as well as the typical execution times of the various steps of the algorithm:

- the human time taken by the computation of the period lattice of $X_1(\ell)$ (cf. section B.3.2), including the q-expansion of the cuspforms of weight 2 (cf. section B.3.1), along with the necessary precision of the q-series so as to achieve the required accuracy in $\mathbb{C}$ (this depends strongly on the largest p for which I need to consider the twisted winding element w_p),
- the human time needed to initialise K. Khuri-Makdisi's algorithm to compute in $J_1(\ell)$, that is to say to compute the q-expansion of the Eisenstein series $e_{1,2}$ and $e_{1,3}$ (cf. section B.2.2) and the multiplication of the weight 2 modular forms into weight 4 and weight 6 (cf. section B.2.1),
- the CPU time required to perform one group operation in $J_1(\ell)$,
- the CPU time spent in Newton iterations in order to approximate an ℓ-torsion divisor (cf. section B.3.3),
- the CPU time required to evaluate my Galois-equivariant function $\alpha\colon J_1(\ell) \dashrightarrow \overline{\mathbb{Q}}$ (cf. section B.3.4) at one point of $J_1(\ell)$,
- the CPU time required to reduce the polynomial describing the number field cut out by the Galois representation (cf. section B.3.5.2),
- the human time required to compute one of the Dokchitsers' resolvent $\Gamma_{\overline{C}}(X)$ (cf. sections A.3.2 and B.3.5.1),
- and finally the total human time taken to compute the Galois representation, from scratch to the Dokchitsers' resolvents (note that in practise, the period computations and the Makdisi initialisation are run only once for each ℓ and then re-used for each newform f of weight $k \leqslant \ell$ and each prime $\mathfrak{l}$ lying above ℓ).

By CPU time, I mean the human time that would be required if I did not use any parallelisation.

Level ℓ	11	13	17^2	19	23	29	31
Genus g	1	2	5	7	12	22	26
Precision in $\mathbb{C}$	700b	800b	1.2kb	1.5kb	5kb	15kb	30kb
q-precision of series	736	959	1.6k	5k	8k	26k	129k
Periods of $X_1(\ell)$	6s	88s	83s	6m	22m	2d	6d
Makdisi initialisation	13s	13s	16s	4.5m	10m	11h	10h[3]
One operation in $J_1(\ell)$	1s	2s	24s	80s	15m	6h	1d
Newton iterations	1s	2s	14s	1m	7m	31h	2d
Evaluation in $J_1(\ell)[\ell]$	1s	2s	15s	36s	6m	3h	12h
`polred`[4]	10s	30s	-	5m	3h	1d	5d
Resolvents $\Gamma_{\overline{C}}(X)$	6s	34s	1m	34s	26s	3m	1m
Total time	<1m	3m	30m	40m	10h	6d	12d

Table C.1.0.1: Parameters and times of the computations

Once the resolvents $\Gamma_{\overline{C}}(X)$ are computed, the time required to compute the trace of the Frobenius element at p is essentially independent of ℓ for large p; it is about 30 minutes for $p \approx 10^{1000}$.

The results are the following:

[2]The case $\ell = 17$ is somehow special since it is the case where the quotient representation trick does not help. I have not tried to reduce the polynomials computed by my algorithm in this case, and I have proceeded directly to the computation of the resolvents, so the algorithm I use is slightly different.

[3]Due to an exaggerated memory usage to store the Fourier coefficients of the series, I split my code to initialise K. Khuri-Makidisi's algorithms into several substeps, and I used the occasion the partly-rewrite it and parallelise it, whence the better time than for $\ell = 29$.

[4]For $\ell < 23$, the coefficents of the polynomial $F(X)$ computed by my algorithm were not too ugly, so I applied [Pari/GP]'s `polred` algorithm directly on the polynomial $F^S(X)$ defining the quotient representation. It is only for $\ell = 29$ and 31 that I deemed it necessary to used the step-by-step reduction process described in section B.3.5.2.

$\ell = 11$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p)$ mod 11
$10^{1000} + 453$	$(x-9)(x-4)$	2
$10^{1000} + 1357$	$(x-8)(x-2)$	10
$10^{1000} + 2713$	$x^2 + x + 8$	10
$10^{1000} + 4351$	$(x-6)(x-3)$	9
$10^{1000} + 5733$	$x^2 + 3x + 3$	8
$10^{1000} + 7383$	$x^2 + 3x + 3$	8
$10^{1000} + 10401$	$(x-8)(x-5)$	2
$10^{1000} + 11979$	$x^2 + 1$	0
$10^{1000} + 17557$	$(x-10)(x-9)$	8
$10^{1000} + 21567$	$x^2 + 10x + 8$	1
$10^{1000} + 22273$	$(x-9)(x-6)$	4
$10^{1000} + 24493$	$(x-8)(x-1)$	9
$10^{1000} + 25947$	$(x-9)(x-6)$	4
$10^{1000} + 27057$	$x^2 + 4x + 9$	7
$10^{1000} + 29737$	$(x-9)(x-3)$	1
$10^{1000} + 41599$	$x^2 + 9$	0
$10^{1000} + 43789$	$x^2 + 6x + 10$	5
$10^{1000} + 46227$	$(x-7)(x-4)$	0
$10^{1000} + 46339$	$(x-8)(x-1)$	9
$10^{1000} + 52423$	$(x-3)^2$	6
$10^{1000} + 55831$	$x^2 + 10x + 7$	1
$10^{1000} + 57867$	$(x-8)(x-1)$	9
$10^{1000} + 59743$	$(x-3)(x-1)$	4
$10^{1000} + 61053$	$(x-9)^2$	7
$10^{1000} + 61353$	$x^2 + x + 7$	10
$10^{1000} + 63729$	$x^2 + x + 7$	10
$10^{1000} + 64047$	$(x-3)(x-2)$	5
$10^{1000} + 64749$	$(x-10)(x-7)$	6
$10^{1000} + 68139$	$x^2 + 2x + 6$	9
$10^{1000} + 68367$	$(x-3)(x-1)$	4
$10^{1000} + 70897$	$(x-10)(x-8)$	7
$10^{1000} + 72237$	$(x-4)(x-3)$	7
$10^{1000} + 77611$	$(x-8)(x-5)$	2
$10^{1000} + 78199$	$(x-6)(x-2)$	8
$10^{1000} + 79237$	$(x-5)(x-1)$	6
$10^{1000} + 79767$	$x^2 + 4x + 7$	7
$10^{1000} + 82767$	$x^2 + 2x + 4$	9
$10^{1000} + 93559$	$(x-4)^2$	8
$10^{1000} + 95107$	$(x-10)(x-9)$	8
$10^{1000} + 100003$	$(x-9)(x-4)$	2

$\ell = 13$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p)$ mod 13
$10^{1000} + 453$	$x^2 + 3x + 1$	10
$10^{1000} + 1357$	$(x - 10)(x - 7)$	4
$10^{1000} + 2713$	$x^2 + 12x + 12$	1
$10^{1000} + 4351$	$x^2 + x + 12$	12
$10^{1000} + 5733$	$(x - 12)(x - 4)$	3
$10^{1000} + 7383$	$x^2 + 6x + 7$	7
$10^{1000} + 10401$	$(x - 5)(x - 2)$	7
$10^{1000} + 11979$	$(x - 9)^2$	5
$10^{1000} + 17557$	$x^2 + 6x + 4$	7
$10^{1000} + 21567$	$x^2 + 5x + 9$	8
$10^{1000} + 22273$	$(x - 10)(x - 8)$	5
$10^{1000} + 24493$	$x^2 + 8x + 10$	5
$10^{1000} + 25947$	$x^2 + 10x + 7$	3
$10^{1000} + 27057$	$(x - 7)(x - 4)$	11
$10^{1000} + 29737$	$x^2 + x + 3$	12
$10^{1000} + 41599$	$(x - 11)(x - 3)$	1
$10^{1000} + 43789$	$(x - 10)(x - 7)$	4
$10^{1000} + 46227$	$x^2 + 10x + 7$	3
$10^{1000} + 46339$	$(x - 8)(x - 7)$	2
$10^{1000} + 52423$	$(x - 10)(x - 3)$	0
$10^{1000} + 55831$	$(x - 4)(x - 3)$	7
$10^{1000} + 57867$	$(x - 2)(x - 1)$	3
$10^{1000} + 59743$	$x^2 + 6$	0
$10^{1000} + 61053$	$x^2 + x + 5$	12
$10^{1000} + 61353$	$(x - 11)(x - 5)$	3
$10^{1000} + 63729$	$(x - 11)(x - 1)$	12
$10^{1000} + 64047$	$(x - 10)(x - 9)$	6
$10^{1000} + 64749$	$(x - 4)(x - 3)$	7
$10^{1000} + 68139$	$x^2 + 6x + 3$	7
$10^{1000} + 68367$	$(x - 7)(x - 5)$	12
$10^{1000} + 70897$	$(x - 12)(x - 7)$	6
$10^{1000} + 72237$	$x^2 + 11x + 12$	2
$10^{1000} + 77611$	$x^2 + 5x + 10$	8
$10^{1000} + 78199$	$(x - 7)(x - 4)$	11
$10^{1000} + 79237$	$(x - 4)(x - 2)$	6
$10^{1000} + 79767$	$x^2 + 7x + 7$	6
$10^{1000} + 82767$	$x^2 + 9x + 12$	4
$10^{1000} + 93559$	$x^2 + 8x + 1$	5
$10^{1000} + 95107$	$x^2 + 10x + 7$	3
$10^{1000} + 100003$	$x^2 + 6x + 4$	7

$\ell = 17$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 17$
$10^{1000} + 453$	$x^2 + 3$	0
$10^{1000} + 1357$	$(x - 15)^2$	13
$10^{1000} + 2713$	$(x - 14)(x - 12)$	9
$10^{1000} + 4351$	$(x - 10)(x - 6)$	16
$10^{1000} + 5733$	$(x - 6)(x - 4)$	10
$10^{1000} + 7383$	$(x - 15)(x - 2)$	0
$10^{1000} + 10401$	$(x - 7)(x - 3)$	10
$10^{1000} + 11979$	$x^2 + 6x + 3$	11
$10^{1000} + 17557$	$x^2 + 11x + 6$	6
$10^{1000} + 21567$	$x^2 + 16x + 3$	1
$10^{1000} + 22273$	$x^2 + 16x + 8$	1
$10^{1000} + 24493$	$x^2 + 8x + 6$	9
$10^{1000} + 25947$	$x^2 + 2x + 13$	15
$10^{1000} + 27057$	$(x - 16)(x - 2)$	1
$10^{1000} + 29737$	$x^2 + 5x + 7$	12
$10^{1000} + 41599$	$x^2 + 6x + 16$	11
$10^{1000} + 43789$	$(x - 11)(x - 5)$	16
$10^{1000} + 46227$	$x^2 + 4x + 7$	13
$10^{1000} + 46339$	$(x - 14)(x - 10)$	7
$10^{1000} + 52423$	$(x - 16)(x - 5)$	4
$10^{1000} + 55831$	$x^2 + 14x + 8$	3
$10^{1000} + 57867$	$x^2 + 8x + 9$	9
$10^{1000} + 59743$	$(x - 14)(x - 7)$	4
$10^{1000} + 61053$	$x^2 + 15x + 11$	2
$10^{1000} + 61353$	$x^2 + 6x + 16$	11
$10^{1000} + 63729$	$x^2 + 6$	0
$10^{1000} + 64047$	$x^2 + 7x + 14$	10
$10^{1000} + 64749$	$(x - 6)(x - 1)$	7
$10^{1000} + 68139$	$(x - 11)(x - 10)$	4
$10^{1000} + 68367$	$(x - 16)(x - 2)$	1
$10^{1000} + 70897$	$x^2 + 5x + 5$	12
$10^{1000} + 72237$	$x^2 + 7$	0
$10^{1000} + 77611$	$x^2 + 15x + 11$	2
$10^{1000} + 78199$	$(x - 16)(x - 8)$	7
$10^{1000} + 79237$	$(x - 10)(x - 5)$	15
$10^{1000} + 79767$	$(x - 8)(x - 1)$	9
$10^{1000} + 82767$	$x^2 + 16x + 3$	1
$10^{1000} + 93559$	$x^2 + 5x + 14$	12
$10^{1000} + 95107$	$(x - 11)^2$	5
$10^{1000} + 100003$	$(x - 14)(x - 5)$	2

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 17
$10^{1000} + 453$	$x^2 + 5x + 12$	12
$10^{1000} + 1357$	$x^2 + 3x + 4$	14
$10^{1000} + 2713$	$x^2 + 8x + 2$	9
$10^{1000} + 4351$	$x^2 + 14x + 8$	3
$10^{1000} + 5733$	$x^2 + 11x + 6$	6
$10^{1000} + 7383$	$(x - 8)^2$	16
$10^{1000} + 10401$	$(x - 16)(x - 13)$	12
$10^{1000} + 11979$	$(x - 9)(x - 7)$	16
$10^{1000} + 17557$	$(x - 5)(x - 2)$	7
$10^{1000} + 21567$	$x^2 + 12x + 12$	5
$10^{1000} + 22273$	$x^2 + 13x + 9$	4
$10^{1000} + 24493$	$x^2 + 10$	0
$10^{1000} + 25947$	$(x - 16)(x - 4)$	3
$10^{1000} + 27057$	$(x - 10)(x - 7)$	0
$10^{1000} + 29737$	$x^2 + 9x + 6$	8
$10^{1000} + 41599$	$x^2 + 4x + 16$	13
$10^{1000} + 43789$	$(x - 4)(x - 1)$	5
$10^{1000} + 46227$	$(x - 12)(x - 9)$	4
$10^{1000} + 46339$	$x^2 + 15x + 4$	2
$10^{1000} + 52423$	$(x - 11)(x - 9)$	3
$10^{1000} + 55831$	$x^2 + 9x + 9$	8
$10^{1000} + 57867$	$x^2 + 12x + 8$	5
$10^{1000} + 59743$	$(x - 8)^2$	16
$10^{1000} + 61053$	$(x - 15)(x - 5)$	3
$10^{1000} + 61353$	$x^2 + 16x + 16$	1
$10^{1000} + 63729$	$x^2 + 14x + 10$	3
$10^{1000} + 64047$	$x^2 + 12x + 5$	5
$10^{1000} + 64749$	$x^2 + 10$	0
$10^{1000} + 68139$	$(x - 10)(x - 6)$	16
$10^{1000} + 68367$	$x^2 + 8x + 2$	9
$10^{1000} + 70897$	$(x - 16)(x - 14)$	13
$10^{1000} + 72237$	$(x - 13)(x - 7)$	3
$10^{1000} + 77611$	$(x - 6)(x - 4)$	10
$10^{1000} + 78199$	$(x - 8)(x - 1)$	9
$10^{1000} + 79237$	$x^2 + 13x + 16$	4
$10^{1000} + 79767$	$x^2 + 4x + 9$	13
$10^{1000} + 82767$	$x^2 + 5x + 12$	12
$10^{1000} + 93559$	$x^2 + 5$	0
$10^{1000} + 95107$	$(x - 7)^2$	14
$10^{1000} + 100003$	$(x - 10)^2$	3

$\ell = 19$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p)$ mod 19
$10^{1000} + 453$	$(x-15)(x-10)$	6
$10^{1000} + 1357$	$(x-17)^2$	15
$10^{1000} + 2713$	$(x-11)(x-4)$	15
$10^{1000} + 4351$	$(x-6)(x-4)$	10
$10^{1000} + 5733$	$(x-16)(x-1)$	17
$10^{1000} + 7383$	$(x-1)^2$	2
$10^{1000} + 10401$	$x^2 + 11x + 4$	8
$10^{1000} + 11979$	$(x-16)(x-13)$	10
$10^{1000} + 17557$	$x^2 + 8x + 14$	11
$10^{1000} + 21567$	$(x-11)^2$	3
$10^{1000} + 22273$	$(x-13)(x-1)$	14
$10^{1000} + 24493$	$(x-14)(x-10)$	5
$10^{1000} + 25947$	$x^2 + 14x + 15$	5
$10^{1000} + 27057$	$(x-10)(x-9)$	0
$10^{1000} + 29737$	$x^2 + 12x + 7$	7
$10^{1000} + 41599$	$(x-18)(x-15)$	14
$10^{1000} + 43789$	$(x-13)(x-11)$	5
$10^{1000} + 46227$	$x^2 + 5$	0
$10^{1000} + 46339$	$x^2 + x + 11$	18
$10^{1000} + 52423$	$x^2 + 7x + 7$	12
$10^{1000} + 55831$	$(x-16)(x-13)$	10
$10^{1000} + 57867$	$(x-17)(x-2)$	0
$10^{1000} + 59743$	$x^2 + 5x + 9$	14
$10^{1000} + 61053$	$x^2 + 9x + 3$	10
$10^{1000} + 61353$	$(x-14)(x-10)$	5
$10^{1000} + 63729$	$x^2 + 15x + 8$	4
$10^{1000} + 64047$	$(x-6)(x-5)$	11
$10^{1000} + 64749$	$(x-13)^2$	7
$10^{1000} + 68139$	$x^2 + 15x + 13$	4
$10^{1000} + 68367$	$(x-14)(x-5)$	0
$10^{1000} + 70897$	$(x-18)(x-15)$	14
$10^{1000} + 72237$	$(x-10)(x-5)$	15
$10^{1000} + 77611$	$x^2 + 13x + 6$	6
$10^{1000} + 78199$	$(x-15)^2$	11
$10^{1000} + 79237$	$x^2 + 12x + 9$	7
$10^{1000} + 79767$	$x^2 + 13x + 13$	6
$10^{1000} + 82767$	$x^2 + 3x + 8$	16
$10^{1000} + 93559$	$x^2 + 4x + 8$	15
$10^{1000} + 95107$	$x^2 + 13x + 15$	6
$10^{1000} + 100003$	$x^2 + 5x + 3$	14

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 19
$10^{1000} + 453$	$(x-15)(x-2)$	17
$10^{1000} + 1357$	$(x-18)(x-12)$	11
$10^{1000} + 2713$	$x^2 + 6x + 7$	13
$10^{1000} + 4351$	$x^2 + 9x + 11$	10
$10^{1000} + 5733$	$(x-17)(x-4)$	2
$10^{1000} + 7383$	$x^2 + 5x + 1$	14
$10^{1000} + 10401$	$x^2 + 13x + 7$	6
$10^{1000} + 11979$	$(x-16)(x-13)$	10
$10^{1000} + 17557$	$(x-9)(x-3)$	12
$10^{1000} + 21567$	$x^2 + 5x + 1$	14
$10^{1000} + 22273$	$(x-17)(x-13)$	11
$10^{1000} + 24493$	$(x-17)(x-9)$	7
$10^{1000} + 25947$	$(x-18)(x-7)$	6
$10^{1000} + 27057$	$x^2 + 5x + 8$	14
$10^{1000} + 29737$	$(x-13)(x-3)$	16
$10^{1000} + 41599$	$x^2 + 7x + 7$	12
$10^{1000} + 43789$	$x^2 + 9x + 12$	10
$10^{1000} + 46227$	$x^2 + 16x + 11$	3
$10^{1000} + 46339$	$(x-17)(x-9)$	7
$10^{1000} + 52423$	$(x-15)(x-14)$	10
$10^{1000} + 55831$	$(x-14)(x-4)$	18
$10^{1000} + 57867$	$x^2 + 18x + 12$	1
$10^{1000} + 59743$	$x^2 + 7$	0
$10^{1000} + 61053$	$(x-17)(x-15)$	13
$10^{1000} + 61353$	$(x-10)(x-2)$	12
$10^{1000} + 63729$	$x^2 + 16x + 18$	3
$10^{1000} + 64047$	$(x-10)(x-2)$	12
$10^{1000} + 64749$	$x^2 + 10x + 11$	9
$10^{1000} + 68139$	$(x-10)(x-5)$	15
$10^{1000} + 68367$	$(x-18)(x-7)$	6
$10^{1000} + 70897$	$x^2 + 6x + 7$	13
$10^{1000} + 72237$	$x^2 + 6x + 18$	13
$10^{1000} + 77611$	$x^2 + 13x + 7$	6
$10^{1000} + 78199$	$(x-7)^2$	14
$10^{1000} + 79237$	$(x-14)(x-10)$	5
$10^{1000} + 79767$	$(x-12)(x-1)$	13
$10^{1000} + 82767$	$(x-16)(x-13)$	10
$10^{1000} + 93559$	$x^2 + 2x + 18$	17
$10^{1000} + 95107$	$x^2 + 18x + 12$	1
$10^{1000} + 100003$	$(x-14)(x-6)$	1

$\ell = 23$

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 23
$10^{1000} + 453$	$(x-15)(x-5)$	20
$10^{1000} + 1357$	$(x-19)(x-15)$	11
$10^{1000} + 2713$	$x^2 + 11x + 21$	12
$10^{1000} + 4351$	$x^2 + 7x + 11$	16
$10^{1000} + 5733$	$(x-18)(x-14)$	9
$10^{1000} + 7383$	$(x-13)(x-6)$	19
$10^{1000} + 10401$	$x^2 + 4x + 7$	19
$10^{1000} + 11979$	$(x-15)(x-7)$	22
$10^{1000} + 17557$	$x^2 + 8x + 1$	15
$10^{1000} + 21567$	$x^2 + 8x + 6$	15
$10^{1000} + 22273$	$(x-17)(x-5)$	22
$10^{1000} + 24493$	$(x-8)(x-5)$	13
$10^{1000} + 25947$	$(x-21)(x-13)$	11
$10^{1000} + 27057$	$(x-8)(x-2)$	10
$10^{1000} + 29737$	$x^2 + 12x + 17$	11
$10^{1000} + 41599$	$(x-20)(x-7)$	4
$10^{1000} + 43789$	$(x-15)^2$	7
$10^{1000} + 46227$	$(x-9)(x-2)$	11
$10^{1000} + 46339$	$(x-22)(x-18)$	17
$10^{1000} + 52423$	$(x-19)(x-6)$	2
$10^{1000} + 55831$	$x^2 + 4x + 12$	19
$10^{1000} + 57867$	$x^2 + 16x + 21$	7
$10^{1000} + 59743$	$(x-7)(x-6)$	13
$10^{1000} + 61053$	$x^2 + 21x + 3$	2
$10^{1000} + 61353$	$(x-11)(x-8)$	19
$10^{1000} + 63729$	$x^2 + 5x + 13$	18
$10^{1000} + 64047$	$(x-22)(x-21)$	20
$10^{1000} + 64749$	$x^2 + 16x + 11$	7
$10^{1000} + 68139$	$(x-18)(x-3)$	21
$10^{1000} + 68367$	$x^2 + 2x + 3$	21
$10^{1000} + 70897$	$x^2 + 21x + 3$	2
$10^{1000} + 72237$	$x^2 + 14x + 5$	9
$10^{1000} + 77611$	$x^2 + 14x + 16$	9
$10^{1000} + 78199$	$x^2 + 6x + 21$	17
$10^{1000} + 79237$	$x^2 + 9x + 4$	14
$10^{1000} + 79767$	$x^2 + 15x + 20$	8
$10^{1000} + 82767$	$(x-8)(x-1)$	9
$10^{1000} + 93559$	$x^2 + x + 10$	22
$10^{1000} + 95107$	$(x-15)(x-11)$	3
$10^{1000} + 100003$	$(x-14)(x-13)$	4

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p)$ mod 23
$10^{1000} + 453$	$(x-18)(x-4)$	22
$10^{1000} + 1357$	$x^2 + 10x + 4$	13
$10^{1000} + 2713$	$x^2 + 13x + 10$	10
$10^{1000} + 4351$	$(x-6)(x-5)$	11
$10^{1000} + 5733$	$x^2 + x + 22$	22
$10^{1000} + 7383$	$(x-20)(x-14)$	11
$10^{1000} + 10401$	$(x-7)(x-4)$	11
$10^{1000} + 11979$	$(x-11)(x-5)$	16
$10^{1000} + 17557$	$x^2 + 7x + 1$	16
$10^{1000} + 21567$	$(x-15)(x-14)$	6
$10^{1000} + 22273$	$x^2 + 22x + 18$	1
$10^{1000} + 24493$	$(x-15)(x-9)$	1
$10^{1000} + 25947$	$(x-7)(x-3)$	10
$10^{1000} + 27057$	$x^2 + 5x + 18$	18
$10^{1000} + 29737$	$x^2 + 5x + 20$	18
$10^{1000} + 41599$	$(x-13)(x-1)$	14
$10^{1000} + 43789$	$x^2 + 8x + 6$	15
$10^{1000} + 46227$	$x^2 + 4x + 6$	19
$10^{1000} + 46339$	$(x-18)(x-15)$	10
$10^{1000} + 52423$	$x^2 + 15x + 22$	8
$10^{1000} + 55831$	$(x-17)(x-5)$	22
$10^{1000} + 57867$	$x^2 + 22x + 10$	1
$10^{1000} + 59743$	$x^2 + 13x + 15$	10
$10^{1000} + 61053$	$(x-20)(x-7)$	4
$10^{1000} + 61353$	$(x-15)(x-1)$	16
$10^{1000} + 63729$	$x^2 + 9$	0
$10^{1000} + 64047$	$(x-17)^2$	11
$10^{1000} + 64749$	$x^2 + 22x + 7$	1
$10^{1000} + 68139$	$(x-9)^2$	18
$10^{1000} + 68367$	$x^2 + 8x + 2$	15
$10^{1000} + 70897$	$(x-2)(x-1)$	3
$10^{1000} + 72237$	$(x-17)(x-1)$	18
$10^{1000} + 77611$	$(x-19)(x-7)$	3
$10^{1000} + 78199$	$(x-17)(x-6)$	0
$10^{1000} + 79237$	$x^2 + 4x + 8$	19
$10^{1000} + 79767$	$x^2 + 11x + 21$	12
$10^{1000} + 82767$	$x^2 + x + 12$	22
$10^{1000} + 93559$	$(x-10)(x-6)$	16
$10^{1000} + 95107$	$x^2 + 13x + 8$	10
$10^{1000} + 100003$	$(x-14)(x-4)$	18

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 23
$10^{1000}+453$	$x^2+5x+13$	18
$10^{1000}+1357$	$x^2+22x+12$	1
$10^{1000}+2713$	$x^2+11x+19$	12
$10^{1000}+4351$	$(x-22)(x-6)$	5
$10^{1000}+5733$	$x^2+22x+22$	1
$10^{1000}+7383$	$(x-15)(x-10)$	2
$10^{1000}+10401$	$x^2+13x+20$	10
$10^{1000}+11979$	$x^2+10x+8$	13
$10^{1000}+17557$	$(x-16)(x-13)$	6
$10^{1000}+21567$	$(x-18)(x-2)$	20
$10^{1000}+22273$	$(x-22)(x-20)$	19
$10^{1000}+24493$	$(x-11)(x-3)$	14
$10^{1000}+25947$	$x^2+18x+14$	5
$10^{1000}+27057$	$x^2+16x+3$	7
$10^{1000}+29737$	$x^2+22x+10$	1
$10^{1000}+41599$	$(x-22)(x-19)$	18
$10^{1000}+43789$	x^2+2	0
$10^{1000}+46227$	$(x-14)(x-10)$	1
$10^{1000}+46339$	$(x-18)(x-5)$	0
$10^{1000}+52423$	$(x-21)(x-12)$	10
$10^{1000}+55831$	$(x-21)(x-20)$	18
$10^{1000}+57867$	$(x-22)(x-4)$	3
$10^{1000}+59743$	$(x-11)(x-9)$	20
$10^{1000}+61053$	x^2+9x+9	14
$10^{1000}+61353$	$(x-22)(x-16)$	15
$10^{1000}+63729$	$x^2+19x+8$	4
$10^{1000}+64047$	$(x-18)(x-13)$	8
$10^{1000}+64749$	$(x-21)(x-3)$	1
$10^{1000}+68139$	$(x-18)(x-1)$	19
$10^{1000}+68367$	x^2+x+9	22
$10^{1000}+70897$	$x^2+21x+9$	2
$10^{1000}+72237$	$(x-11)(x-4)$	15
$10^{1000}+77611$	$(x-15)(x-14)$	6
$10^{1000}+78199$	$(x-17)(x-16)$	10
$10^{1000}+79237$	$x^2+5x+16$	18
$10^{1000}+79767$	$x^2+18x+14$	5
$10^{1000}+82767$	$(x-11)(x-10)$	21
$10^{1000}+93559$	$x^2+6x+15$	17
$10^{1000}+95107$	$(x-19)^2$	15
$10^{1000}+100003$	$x^2+15x+19$	8

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p)$ mod 23
$10^{1000} + 453$	$(x-19)(x-7)$	3
$10^{1000} + 1357$	$x^2 + 13$	0
$10^{1000} + 2713$	$x^2 + 8x + 20$	15
$10^{1000} + 4351$	$(x-16)(x-11)$	4
$10^{1000} + 5733$	$x^2 + 19x + 22$	4
$10^{1000} + 7383$	$(x-19)(x-14)$	10
$10^{1000} + 10401$	$(x-16)(x-5)$	21
$10^{1000} + 11979$	$(x-17)(x-15)$	9
$10^{1000} + 17557$	$(x-19)(x-17)$	13
$10^{1000} + 21567$	$(x-19)(x-7)$	3
$10^{1000} + 22273$	$x^2 + 14x + 12$	9
$10^{1000} + 24493$	$(x-7)(x-4)$	11
$10^{1000} + 25947$	$x^2 + 4x + 17$	19
$10^{1000} + 27057$	$x^2 + 3x + 12$	20
$10^{1000} + 29737$	$x^2 + 5x + 5$	18
$10^{1000} + 41599$	$(x-7)^2$	14
$10^{1000} + 43789$	$x^2 + 18x + 16$	5
$10^{1000} + 46227$	$x^2 + 19x + 16$	4
$10^{1000} + 46339$	$x^2 + 22x + 7$	1
$10^{1000} + 52423$	$(x-22)(x-1)$	0
$10^{1000} + 55831$	$x^2 + 12x + 8$	11
$10^{1000} + 57867$	$(x-17)(x-12)$	6
$10^{1000} + 59743$	$(x-21)(x-16)$	14
$10^{1000} + 61053$	$x^2 + 4x + 6$	19
$10^{1000} + 61353$	$(x-19)(x-8)$	4
$10^{1000} + 63729$	$(x-5)^2$	10
$10^{1000} + 64047$	$(x-12)(x-6)$	18
$10^{1000} + 64749$	$(x-13)(x-10)$	0
$10^{1000} + 68139$	$(x-21)^2$	19
$10^{1000} + 68367$	$(x-19)(x-10)$	6
$10^{1000} + 70897$	$x^2 + 14x + 6$	9
$10^{1000} + 72237$	$(x-20)(x-13)$	10
$10^{1000} + 77611$	$(x-4)(x-3)$	7
$10^{1000} + 78199$	$(x-14)(x-8)$	22
$10^{1000} + 79237$	$x^2 + 20x + 9$	3
$10^{1000} + 79767$	$x^2 + 8x + 17$	15
$10^{1000} + 82767$	$x^2 + 16x + 4$	7
$10^{1000} + 93559$	$(x-14)(x-13)$	4
$10^{1000} + 95107$	$(x-3)^2$	6
$10^{1000} + 100003$	$(x-19)(x-18)$	14

$\ell = 29$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 29$
$10^{1000} + 453$	$x^2 + 8x + 24$	21
$10^{1000} + 1357$	$x^2 + 21x + 1$	8
$10^{1000} + 2713$	$x^2 + 18x + 20$	11
$10^{1000} + 4351$	$x^2 + 3$	0
$10^{1000} + 5733$	$(x - 20)(x - 2)$	22
$10^{1000} + 7383$	$(x - 19)(x - 10)$	0
$10^{1000} + 10401$	$(x - 7)(x - 2)$	9
$10^{1000} + 11979$	$x^2 + 22x + 22$	7
$10^{1000} + 17557$	$x^2 + 27$	0
$10^{1000} + 21567$	$(x - 23)(x - 3)$	26
$10^{1000} + 22273$	$x^2 + 15x + 3$	14
$10^{1000} + 24493$	$x^2 + 25x + 16$	4
$10^{1000} + 25947$	$(x - 27)(x - 15)$	13
$10^{1000} + 27057$	$x^2 + 22x + 23$	7
$10^{1000} + 29737$	$(x - 23)(x - 10)$	4
$10^{1000} + 41599$	$(x - 13)(x - 5)$	18
$10^{1000} + 43789$	$(x - 18)(x - 15)$	4
$10^{1000} + 46227$	$x^2 + 7x + 3$	22
$10^{1000} + 46339$	$(x - 26)(x - 8)$	5
$10^{1000} + 52423$	$(x - 17)(x - 16)$	4
$10^{1000} + 55831$	$x^2 + 21x + 4$	8
$10^{1000} + 57867$	$(x - 13)(x - 11)$	24
$10^{1000} + 59743$	$x^2 + 24x + 2$	5
$10^{1000} + 61053$	$x^2 + 18x + 21$	11
$10^{1000} + 61353$	$(x - 24)(x - 1)$	25
$10^{1000} + 63729$	$(x - 20)(x - 1)$	21
$10^{1000} + 64047$	$x^2 + 14x + 6$	15
$10^{1000} + 64749$	$x^2 + 14x + 28$	15
$10^{1000} + 68139$	$(x - 12)(x - 2)$	14
$10^{1000} + 68367$	$x^2 + 26x + 26$	3
$10^{1000} + 70897$	$x^2 + 12x + 28$	17
$10^{1000} + 72237$	$x^2 + 27x + 13$	2
$10^{1000} + 77611$	$(x - 14)(x - 13)$	27
$10^{1000} + 78199$	$(x - 17)(x - 14)$	2
$10^{1000} + 79237$	$x^2 + 28x + 25$	1
$10^{1000} + 79767$	$x^2 + 13x + 16$	16
$10^{1000} + 82767$	$(x - 27)(x - 13)$	11
$10^{1000} + 93559$	$x^2 + 13x + 17$	16
$10^{1000} + 95107$	$(x - 25)(x - 24)$	20
$10^{1000} + 100003$	$(x - 26)(x - 13)$	10

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 29
$10^{1000}+453$	$x^2+16x+25$	13
$10^{1000}+1357$	x^2+9x+1	20
$10^{1000}+2713$	$(x-23)(x-1)$	24
$10^{1000}+4351$	$x^2+18x+21$	11
$10^{1000}+5733$	$(x-22)(x-8)$	1
$10^{1000}+7383$	x^2+x+24	28
$10^{1000}+10401$	$(x-17)(x-7)$	24
$10^{1000}+11979$	$x^2+26x+9$	3
$10^{1000}+17557$	$(x-27)(x-24)$	22
$10^{1000}+21567$	$(x-16)(x-11)$	27
$10^{1000}+22273$	$(x-27)(x-4)$	2
$10^{1000}+24493$	$(x-25)(x-23)$	19
$10^{1000}+25947$	$(x-17)^2$	5
$10^{1000}+27057$	$x^2+22x+7$	7
$10^{1000}+29737$	x^2+10	0
$10^{1000}+41599$	$x^2+2x+20$	27
$10^{1000}+43789$	$x^2+19x+6$	10
$10^{1000}+46227$	$(x-24)(x-19)$	14
$10^{1000}+46339$	$x^2+17x+4$	12
$10^{1000}+52423$	$(x-26)(x-9)$	6
$10^{1000}+55831$	$(x-17)(x-11)$	28
$10^{1000}+57867$	$(x-27)(x-24)$	22
$10^{1000}+59743$	$x^2+28x+19$	1
$10^{1000}+61053$	$(x-21)(x-20)$	12
$10^{1000}+61353$	$x^2+13x+25$	16
$10^{1000}+63729$	$(x-28)(x-6)$	5
$10^{1000}+64047$	$(x-23)(x-6)$	0
$10^{1000}+64749$	$(x-24)(x-6)$	1
$10^{1000}+68139$	$(x-24)^2$	19
$10^{1000}+68367$	$(x-26)(x-7)$	4
$10^{1000}+70897$	$x^2+15x+28$	14
$10^{1000}+72237$	$(x-28)(x-24)$	23
$10^{1000}+77611$	$x^2+19x+15$	10
$10^{1000}+78199$	$(x-10)(x-8)$	18
$10^{1000}+79237$	$(x-25)^2$	21
$10^{1000}+79767$	$x^2+17x+24$	12
$10^{1000}+82767$	$x^2+6x+21$	23
$10^{1000}+93559$	$(x-24)(x-14)$	9
$10^{1000}+95107$	$x^2+6x+23$	23
$10^{1000}+100003$	$(x-26)(x-6)$	3

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p)$ mod 29
$10^{1000} + 453$	$x^2 + 13x + 23$	16
$10^{1000} + 1357$	$(x - 22)(x - 4)$	26
$10^{1000} + 2713$	$x^2 + 16x + 16$	13
$10^{1000} + 4351$	$(x - 23)(x - 8)$	2
$10^{1000} + 5733$	$(x - 16)(x - 15)$	2
$10^{1000} + 7383$	$(x - 13)(x - 6)$	19
$10^{1000} + 10401$	$x^2 + 27x + 27$	2
$10^{1000} + 11979$	$x^2 + 10x + 4$	19
$10^{1000} + 17557$	$x^2 + 19x + 14$	10
$10^{1000} + 21567$	$(x - 27)(x - 25)$	23
$10^{1000} + 22273$	$(x - 27)(x - 24)$	22
$10^{1000} + 24493$	$x^2 + 6x + 20$	23
$10^{1000} + 25947$	$(x - 21)(x - 11)$	3
$10^{1000} + 27057$	$x^2 + 23x + 24$	6
$10^{1000} + 29737$	$(x - 23)(x - 17)$	11
$10^{1000} + 41599$	$(x - 18)(x - 3)$	21
$10^{1000} + 43789$	$x^2 + 8x + 13$	21
$10^{1000} + 46227$	$(x - 14)(x - 9)$	23
$10^{1000} + 46339$	$(x - 18)(x - 10)$	28
$10^{1000} + 52423$	$(x - 16)(x - 15)$	2
$10^{1000} + 55831$	$x^2 + 22x + 22$	7
$10^{1000} + 57867$	$x^2 + 13x + 14$	16
$10^{1000} + 59743$	$(x - 22)(x - 2)$	24
$10^{1000} + 61053$	$x^2 + 8x + 18$	21
$10^{1000} + 61353$	$(x - 11)(x - 10)$	21
$10^{1000} + 63729$	$(x - 12)(x - 11)$	23
$10^{1000} + 64047$	$(x - 23)(x - 4)$	27
$10^{1000} + 64749$	$(x - 19)(x - 3)$	22
$10^{1000} + 68139$	$x^2 + 4x + 23$	25
$10^{1000} + 68367$	$(x - 15)(x - 9)$	24
$10^{1000} + 70897$	$(x - 25)(x - 22)$	18
$10^{1000} + 72237$	$(x - 18)(x - 15)$	4
$10^{1000} + 77611$	$(x - 25)(x - 19)$	15
$10^{1000} + 78199$	$(x - 19)(x - 14)$	4
$10^{1000} + 79237$	$(x - 19)(x - 8)$	27
$10^{1000} + 79767$	$(x - 17)(x - 8)$	25
$10^{1000} + 82767$	$(x - 27)(x - 24)$	22
$10^{1000} + 93559$	$(x - 11)(x - 9)$	20
$10^{1000} + 95107$	$x^2 + 24x + 16$	5
$10^{1000} + 100003$	$x^2 + 7x + 26$	22

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 29
$10^{1000} + 453$	$x^2 + 23x + 20$	6
$10^{1000} + 1357$	$x^2 + 25x + 1$	4
$10^{1000} + 2713$	$x^2 + 25x + 25$	4
$10^{1000} + 4351$	$(x - 25)(x - 14)$	10
$10^{1000} + 5733$	$x^2 + 27x + 3$	2
$10^{1000} + 7383$	$x^2 + 28x + 7$	1
$10^{1000} + 10401$	$(x - 22)(x - 15)$	8
$10^{1000} + 11979$	$(x - 9)(x - 7)$	16
$10^{1000} + 17557$	$x^2 + 28x + 8$	1
$10^{1000} + 21567$	$(x - 17)(x - 7)$	24
$10^{1000} + 22273$	$x^2 + 14x + 2$	15
$10^{1000} + 24493$	$(x - 18)(x - 2)$	20
$10^{1000} + 25947$	$x^2 + 2x + 28$	27
$10^{1000} + 27057$	$(x - 19)(x - 10)$	0
$10^{1000} + 29737$	$x^2 + 8x + 8$	21
$10^{1000} + 41599$	$x^2 + x + 24$	28
$10^{1000} + 43789$	$(x - 13)(x - 7)$	20
$10^{1000} + 46227$	$(x - 10)(x - 6)$	16
$10^{1000} + 46339$	$(x - 22)(x - 7)$	0
$10^{1000} + 52423$	$x^2 + 15x + 3$	14
$10^{1000} + 55831$	$(x - 19)(x - 11)$	1
$10^{1000} + 57867$	$(x - 11)(x - 6)$	17
$10^{1000} + 59743$	$(x - 18)(x - 6)$	24
$10^{1000} + 61053$	$x^2 + 2x + 19$	27
$10^{1000} + 61353$	$(x - 28)(x - 9)$	8
$10^{1000} + 63729$	$x^2 + 16x + 25$	13
$10^{1000} + 64047$	$x^2 + 5x + 13$	24
$10^{1000} + 64749$	$x^2 + 15x + 28$	14
$10^{1000} + 68139$	$(x - 25)(x - 24)$	20
$10^{1000} + 68367$	$(x - 22)(x - 21)$	14
$10^{1000} + 70897$	$(x - 7)(x - 4)$	11
$10^{1000} + 72237$	$(x - 27)(x - 18)$	16
$10^{1000} + 77611$	$(x - 17)(x - 4)$	21
$10^{1000} + 78199$	$x^2 + 8x + 13$	21
$10^{1000} + 79237$	$(x - 17)(x - 15)$	3
$10^{1000} + 79767$	$(x - 24)(x - 16)$	11
$10^{1000} + 82767$	$x^2 + 15x + 2$	14
$10^{1000} + 93559$	$(x - 23)(x - 2)$	25
$10^{1000} + 95107$	$x^2 + 5x + 25$	24
$10^{1000} + 100003$	$x^2 + 13x + 14$	16

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p)$ mod 29
$10^{1000} + 453$	$(x-17)(x-12)$	0
$10^{1000} + 1357$	$x^2 + 8x + 1$	21
$10^{1000} + 2713$	$(x-6)(x-5)$	11
$10^{1000} + 4351$	$(x-20)(x-18)$	9
$10^{1000} + 5733$	$(x-4)(x-3)$	7
$10^{1000} + 7383$	$(x-17)(x-12)$	0
$10^{1000} + 10401$	$x^2 + 4x + 12$	25
$10^{1000} + 11979$	$(x-19)(x-3)$	22
$10^{1000} + 17557$	$x^2 + 15x + 17$	14
$10^{1000} + 21567$	$x^2 + x + 12$	28
$10^{1000} + 22273$	$(x-28)(x-17)$	16
$10^{1000} + 24493$	$(x-27)(x-14)$	12
$10^{1000} + 25947$	$(x-18)(x-8)$	26
$10^{1000} + 27057$	$x^2 + 9x + 1$	20
$10^{1000} + 29737$	$(x-13)(x-8)$	21
$10^{1000} + 41599$	$(x-10)(x-3)$	13
$10^{1000} + 43789$	$(x-21)(x-11)$	3
$10^{1000} + 46227$	$(x-20)(x-18)$	9
$10^{1000} + 46339$	$(x-24)(x-6)$	1
$10^{1000} + 52423$	$x^2 + 14x + 12$	15
$10^{1000} + 55831$	$(x-16)(x-9)$	25
$10^{1000} + 57867$	$(x-20)(x-11)$	2
$10^{1000} + 59743$	$(x-4)(x-3)$	7
$10^{1000} + 61053$	$x^2 + 11x + 12$	18
$10^{1000} + 61353$	$(x-22)(x-4)$	26
$10^{1000} + 63729$	$(x-1)^2$	2
$10^{1000} + 64047$	$(x-21)(x-11)$	3
$10^{1000} + 64749$	$(x-19)(x-3)$	22
$10^{1000} + 68139$	$x^2 + 20x + 1$	9
$10^{1000} + 68367$	$(x-18)(x-9)$	27
$10^{1000} + 70897$	$(x-7)(x-4)$	11
$10^{1000} + 72237$	$x^2 + 2x + 28$	27
$10^{1000} + 77611$	$(x-15)(x-5)$	20
$10^{1000} + 78199$	$(x-12)^2$	24
$10^{1000} + 79237$	$x^2 + 24x + 1$	5
$10^{1000} + 79767$	$(x-11)(x-8)$	19
$10^{1000} + 82767$	$x^2 + 26x + 12$	3
$10^{1000} + 93559$	$(x-20)(x-18)$	9
$10^{1000} + 95107$	$x^2 + 8x + 1$	21
$10^{1000} + 100003$	$(x-10)(x-7)$	17

$$f_{26} = E_{14}\Delta = \sum_{n=1}^{+\infty} \tau_{26}(n) q^n = q - 48q^2 - 195804q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{26}(p)$ mod 29
$10^{1000} + 453$	$(x-16)^2$	3
$10^{1000} + 1357$	$x^2 + 24x + 1$	5
$10^{1000} + 2713$	$x^2 + 27x + 20$	2
$10^{1000} + 4351$	$x^2 + 8x + 26$	21
$10^{1000} + 5733$	$x^2 + 14x + 18$	15
$10^{1000} + 7383$	$(x-9)(x-5)$	14
$10^{1000} + 10401$	$x^2 + 4x + 15$	25
$10^{1000} + 11979$	$(x-15)^2$	1
$10^{1000} + 17557$	$(x-16)(x-11)$	27
$10^{1000} + 21567$	$(x-27)(x-20)$	18
$10^{1000} + 22273$	$(x-27)(x-16)$	14
$10^{1000} + 24493$	$x^2 + 9x + 16$	20
$10^{1000} + 25947$	$x^2 + 20x + 28$	9
$10^{1000} + 27057$	$(x-9)^2$	18
$10^{1000} + 29737$	$(x-2)(x-1)$	3
$10^{1000} + 41599$	$(x-25)(x-20)$	16
$10^{1000} + 43789$	$(x-9)(x-1)$	10
$10^{1000} + 46227$	$(x-21)(x-4)$	25
$10^{1000} + 46339$	$(x-28)(x-24)$	23
$10^{1000} + 52423$	$x^2 + 27x + 18$	2
$10^{1000} + 55831$	$x^2 + 11x + 4$	18
$10^{1000} + 57867$	$(x-23)(x-19)$	13
$10^{1000} + 59743$	$x^2 + 16x + 27$	13
$10^{1000} + 61053$	$x^2 + 8x + 8$	21
$10^{1000} + 61353$	$(x-24)(x-1)$	25
$10^{1000} + 63729$	$x^2 + 27x + 20$	2
$10^{1000} + 64047$	$(x-25)(x-13)$	9
$10^{1000} + 64749$	$(x-23)(x-5)$	28
$10^{1000} + 68139$	$(x-18)(x-11)$	0
$10^{1000} + 68367$	$(x-24)(x-11)$	6
$10^{1000} + 70897$	$x^2 + 27x + 28$	2
$10^{1000} + 72237$	$(x-28)(x-16)$	15
$10^{1000} + 77611$	$x^2 + 4x + 21$	25
$10^{1000} + 78199$	$(x-21)^2$	13
$10^{1000} + 79237$	$(x-27)(x-2)$	0
$10^{1000} + 79767$	$x^2 + 24x + 16$	5
$10^{1000} + 82767$	$(x-13)(x-2)$	15
$10^{1000} + 93559$	$(x-16)(x-8)$	24
$10^{1000} + 95107$	$x^2 + 7x + 20$	22
$10^{1000} + 100003$	$(x-26)(x-16)$	13

$\ell = 31$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p)$ mod 31
$10^{1000} + 453$	$(x-30)(x-20)$	19
$10^{1000} + 1357$	$x^2 + 18x + 29$	13
$10^{1000} + 2713$	$x^2 + 27x + 12$	4
$10^{1000} + 4351$	$(x-4)^2$	8
$10^{1000} + 5733$	$(x-21)(x-8)$	29
$10^{1000} + 7383$	$(x-13)(x-11)$	24
$10^{1000} + 10401$	$(x-22)(x-9)$	0
$10^{1000} + 11979$	$(x-7)(x-4)$	11
$10^{1000} + 17557$	$(x-27)^2$	23
$10^{1000} + 21567$	$x^2 + 20x + 27$	11
$10^{1000} + 22273$	$x^2 + 9x + 7$	22
$10^{1000} + 24493$	$x^2 + 27x + 8$	4
$10^{1000} + 25947$	$x^2 + 19x + 25$	12
$10^{1000} + 27057$	$x^2 + 8x + 30$	23
$10^{1000} + 29737$	$(x-17)(x-2)$	19
$10^{1000} + 41599$	$x^2 + x + 2$	30
$10^{1000} + 43789$	$(x-12)(x-4)$	16
$10^{1000} + 46227$	$(x-13)(x-9)$	22
$10^{1000} + 46339$	$x^2 + 28x + 30$	3
$10^{1000} + 52423$	$(x-24)(x-6)$	30
$10^{1000} + 55831$	$(x-30)(x-6)$	5
$10^{1000} + 57867$	$(x-23)(x-7)$	30
$10^{1000} + 59743$	$(x-26)(x-20)$	15
$10^{1000} + 61053$	$x^2 + 10x + 10$	21
$10^{1000} + 61353$	$(x-30)(x-17)$	16
$10^{1000} + 63729$	$(x-20)(x-3)$	23
$10^{1000} + 64047$	$x^2 + 2x + 26$	29
$10^{1000} + 64749$	$x^2 + 13x + 6$	18
$10^{1000} + 68139$	$x^2 + 21x + 26$	10
$10^{1000} + 68367$	$x^2 + 22x + 22$	9
$10^{1000} + 70897$	$x^2 + 8x + 25$	23
$10^{1000} + 72237$	$(x-29)(x-5)$	3
$10^{1000} + 77611$	$x^2 + 20x + 23$	11
$10^{1000} + 78199$	$x^2 + 24x + 17$	7
$10^{1000} + 79237$	$(x-21)(x-16)$	6
$10^{1000} + 79767$	$(x-21)(x-11)$	1
$10^{1000} + 82767$	$(x-8)^2$	16
$10^{1000} + 93559$	$x^2 + 8x + 26$	23
$10^{1000} + 95107$	$x^2 + 9x + 4$	22
$10^{1000} + 100003$	$x^2 + 30x + 2$	1

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p)$ mod 31
$10^{1000} + 453$	$x^2 + 10x + 13$	21
$10^{1000} + 1357$	$(x - 25)(x - 11)$	5
$10^{1000} + 2713$	$x^2 + x + 24$	30
$10^{1000} + 4351$	$(x - 20)(x - 19)$	8
$10^{1000} + 5733$	$x^2 + 17x + 22$	14
$10^{1000} + 7383$	$x^2 + 24x + 7$	7
$10^{1000} + 10401$	$x^2 + 24x + 24$	7
$10^{1000} + 11979$	$(x - 13)^2$	26
$10^{1000} + 17557$	$(x - 22)(x - 6)$	28
$10^{1000} + 21567$	$(x - 5)(x - 3)$	8
$10^{1000} + 22273$	$x^2 + 5x + 28$	26
$10^{1000} + 24493$	$(x - 22)(x - 17)$	8
$10^{1000} + 25947$	$x^2 + 25x + 25$	6
$10^{1000} + 27057$	$(x - 19)(x - 13)$	1
$10^{1000} + 29737$	$x^2 + 29x + 17$	2
$10^{1000} + 41599$	$(x - 7)(x - 5)$	12
$10^{1000} + 43789$	$x^2 + 10x + 12$	21
$10^{1000} + 46227$	$(x - 22)(x - 10)$	1
$10^{1000} + 46339$	$x^2 + 8x + 30$	23
$10^{1000} + 52423$	$(x - 17)(x - 12)$	29
$10^{1000} + 55831$	$x^2 + 9x + 25$	22
$10^{1000} + 57867$	$x^2 + 25x + 6$	6
$10^{1000} + 59743$	$(x - 26)(x - 18)$	13
$10^{1000} + 61053$	$x^2 + 23x + 20$	8
$10^{1000} + 61353$	$(x - 16)(x - 7)$	23
$10^{1000} + 63729$	$x^2 + 21x + 27$	10
$10^{1000} + 64047$	$x^2 + 20x + 26$	11
$10^{1000} + 64749$	$(x - 11)(x - 9)$	20
$10^{1000} + 68139$	$(x - 30)(x - 5)$	4
$10^{1000} + 68367$	$(x - 20)(x - 15)$	4
$10^{1000} + 70897$	$(x - 30)(x - 6)$	5
$10^{1000} + 72237$	$(x - 15)(x - 9)$	24
$10^{1000} + 77611$	$(x - 17)(x - 9)$	26
$10^{1000} + 78199$	$(x - 17)(x - 8)$	25
$10^{1000} + 79237$	$(x - 27)(x - 9)$	5
$10^{1000} + 79767$	$x^2 + 2x + 19$	29
$10^{1000} + 82767$	$(x - 18)(x - 14)$	1
$10^{1000} + 93559$	$(x - 15)(x - 10)$	25
$10^{1000} + 95107$	$(x - 8)(x - 2)$	10
$10^{1000} + 100003$	$(x - 2)^2$	4

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 31
$10^{1000}+453$	$(x-21)(x-20)$	10
$10^{1000}+1357$	$x^2+29x+15$	2
$10^{1000}+2713$	$(x-25)(x-3)$	28
$10^{1000}+4351$	x^2+x+2	30
$10^{1000}+5733$	$x^2+21x+12$	10
$10^{1000}+7383$	$x^2+30x+18$	1
$10^{1000}+10401$	$x^2+10x+13$	21
$10^{1000}+11979$	$(x-5)(x-2)$	7
$10^{1000}+17557$	$(x-23)^2$	15
$10^{1000}+21567$	$(x-16)(x-15)$	0
$10^{1000}+22273$	$(x-8)(x-5)$	13
$10^{1000}+24493$	$(x-28)(x-9)$	6
$10^{1000}+25947$	$(x-9)(x-4)$	13
$10^{1000}+27057$	$(x-6)(x-5)$	11
$10^{1000}+29737$	$x^2+16x+21$	15
$10^{1000}+41599$	$(x-27)^2$	23
$10^{1000}+43789$	$x^2+6x+11$	25
$10^{1000}+46227$	$x^2+21x+22$	10
$10^{1000}+46339$	$x^2+24x+30$	7
$10^{1000}+52423$	$x^2+12x+14$	19
$10^{1000}+55831$	x^2+7x+5	24
$10^{1000}+57867$	$(x-28)(x-12)$	9
$10^{1000}+59743$	$(x-29)(x-20)$	18
$10^{1000}+61053$	$x^2+26x+28$	5
$10^{1000}+61353$	$(x-29)(x-21)$	19
$10^{1000}+63729$	$x^2+29x+15$	2
$10^{1000}+64047$	$x^2+16x+6$	15
$10^{1000}+64749$	$(x-23)(x-20)$	12
$10^{1000}+68139$	$(x-11)(x-9)$	20
$10^{1000}+68367$	$x^2+24x+24$	7
$10^{1000}+70897$	x^2+7x+5	24
$10^{1000}+72237$	$(x-16)(x-6)$	22
$10^{1000}+77611$	x^2+x+27	30
$10^{1000}+78199$	$x^2+16x+11$	15
$10^{1000}+79237$	$(x-17)(x-4)$	21
$10^{1000}+79767$	$x^2+23x+20$	8
$10^{1000}+82767$	$(x-25)(x-18)$	12
$10^{1000}+93559$	$x^2+18x+6$	13
$10^{1000}+95107$	$x^2+26x+8$	5
$10^{1000}+100003$	$x^2+9x+16$	22

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p)$ mod 31
$10^{1000} + 453$	$(x-27)(x-1)$	28
$10^{1000} + 1357$	$(x-30)(x-2)$	1
$10^{1000} + 2713$	$x^2 + 4x + 29$	27
$10^{1000} + 4351$	$(x-22)(x-12)$	3
$10^{1000} + 5733$	$x^2 + 28x + 15$	3
$10^{1000} + 7383$	$x^2 + 12x + 2$	19
$10^{1000} + 10401$	$(x-22)(x-14)$	5
$10^{1000} + 11979$	$x^2 + 13x + 16$	18
$10^{1000} + 17557$	$x^2 + 6x + 16$	25
$10^{1000} + 21567$	$(x-27)(x-1)$	28
$10^{1000} + 22273$	$(x-21)(x-12)$	2
$10^{1000} + 24493$	$(x-22)(x-6)$	28
$10^{1000} + 25947$	$x^2 + 23x + 1$	8
$10^{1000} + 27057$	$(x-20)(x-17)$	6
$10^{1000} + 29737$	$(x-11)(x-7)$	18
$10^{1000} + 41599$	$(x-18)(x-7)$	25
$10^{1000} + 43789$	$(x-17)(x-5)$	22
$10^{1000} + 46227$	$x^2 + 16x + 27$	15
$10^{1000} + 46339$	$(x-14)(x-11)$	25
$10^{1000} + 52423$	$x^2 + 15x + 4$	16
$10^{1000} + 55831$	$x^2 + 22x + 1$	9
$10^{1000} + 57867$	$(x-20)(x-17)$	6
$10^{1000} + 59743$	$x^2 + 25x + 27$	6
$10^{1000} + 61053$	$(x-2)(x-1)$	3
$10^{1000} + 61353$	$(x-16)^2$	1
$10^{1000} + 63729$	$x^2 + 6x + 29$	25
$10^{1000} + 64047$	$(x-24)(x-9)$	2
$10^{1000} + 64749$	$x^2 + 5x + 30$	26
$10^{1000} + 68139$	$(x-29)(x-16)$	14
$10^{1000} + 68367$	$x^2 + 12x + 23$	19
$10^{1000} + 70897$	$(x-13)(x-12)$	25
$10^{1000} + 72237$	$(x-10)(x-6)$	16
$10^{1000} + 77611$	$(x-17)(x-5)$	22
$10^{1000} + 78199$	$x^2 + 17x + 23$	14
$10^{1000} + 79237$	$(x-18)(x-12)$	30
$10^{1000} + 79767$	$(x-25)(x-9)$	3
$10^{1000} + 82767$	$(x-18)(x-7)$	25
$10^{1000} + 93559$	$x^2 + 7x + 30$	24
$10^{1000} + 95107$	$x^2 + 3x + 4$	28
$10^{1000} + 100003$	$x^2 + 18x + 2$	13

$$f_{24} = \sum_{n=1}^{+\infty} \tau_{24}(n) q^n = q + 24(22+\alpha)q^2 + 36(4731 - 32\alpha)q^3 + O(q^4), \quad \alpha = \frac{1+\sqrt{144169}}{2}$$

Here I use slightly different notations: f_{24} is the newform of level 1 and of lowest weight to have irrational coefficients, that is to say for which $K_f \neq \mathbb{Q}$. Indeed in this case $K_{f_{24}} = \mathbb{Q}(\sqrt{144169})$ is the quadratic field with integer ring $\mathbb{Z}_{K_{f_{24}}} = \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{144169}}{2}$, and (prime) discriminant 144169. The prime 29 is inert in this field, so I could not compute the representation modulo 29 attached to this form; on the contrary, the prime 31 splits into $(31) = \mathfrak{l}_5\mathfrak{l}_{27}$, where $\mathfrak{l}_5 = (31, \alpha - 5)$ and $\mathfrak{l}_{27} = (31, \alpha - 27)$. Instead of presenting the results for the Galois representations attached to f_{24} modulo $\mathfrak{l}_5$ and $\mathfrak{l}_{27}$ separately, it is more interesting to present them together, since I can then compute the coefficients $\tau_{24}(p)$ mod $31\mathbb{Z}[\alpha]$ by putting together the information coming from both representations and using Chinese remainders. This is what I do in the table below, where I denote by L_5 (respectively L_{27}) the number field cut out by the representation modulo $\mathfrak{l}_5$ (respectively $\mathfrak{l}_{27}$) attached to f_{24}.

p	Similarity class of $\left(\frac{L_5/\mathbb{Q}}{p}\right)$	Similarity class of $\left(\frac{L_{27}/\mathbb{Q}}{p}\right)$	$\tau_{24}(p) \bmod 31\mathbb{Z}[\alpha]$
$10^{1000}+453$	$x^2+26x+21$	$(x-20)(x-15)$	$1+7\alpha$
$10^{1000}+1357$	$(x-18)(x-3)$	$(x-25)(x-22)$	$1+4\alpha$
$10^{1000}+2713$	$(x-24)(x-2)$	$(x-29)(x-7)$	$4+23\alpha$
$10^{1000}+4351$	$(x-17)(x-13)$	$(x-11)(x-6)$	$9+29\alpha$
$10^{1000}+5733$	$(x-19)(x-12)$	$(x-15)(x-9)$	$3+18\alpha$
$10^{1000}+7383$	$x^2+4x+14$	$(x-7)(x-2)$	$17+2\alpha$
$10^{1000}+10401$	$(x-22)(x-5)$	$x^2+24x+17$	$9+16\alpha$
$10^{1000}+11979$	$x^2+17x+7$	$x^2+19x+7$	$6+14\alpha$
$10^{1000}+17557$	$(x-26)(x-24)$	$(x-17)(x-13)$	$1+16\alpha$
$10^{1000}+21567$	$x^2+6x+29$	$x^2+2x+29$	$10+3\alpha$
$10^{1000}+22273$	$x^2+10x+19$	$(x-16)(x-7)$	$29+17\alpha$
$10^{1000}+24493$	$(x-22)(x-12)$	$(x-25)(x-18)$	$8+30\alpha$
$10^{1000}+25947$	$(x-15)(x-12)$	$(x-24)(x-23)$	$14+15\alpha$
$10^{1000}+27057$	$x^2+10x+30$	$(x-26)(x-25)$	$17+7\alpha$
$10^{1000}+29737$	$x^2+3x+24$	$x^2+13x+24$	$19+8\alpha$
$10^{1000}+41599$	$x^2+11x+8$	$x^2+27x+8$	$18+19\alpha$
$10^{1000}+43789$	$x^2+14x+3$	x^2+7x+3	$14+13\alpha$
$10^{1000}+46227$	$x^2+15x+12$	$x^2+4x+12$	$29+16\alpha$
$10^{1000}+46339$	$(x-24)(x-9)$	$x^2+5x+30$	$5+18\alpha$
$10^{1000}+52423$	$(x-10)(x-1)$	$x^2+16x+10$	$27+3\alpha$
$10^{1000}+55831$	$x^2+7x+25$	$(x-28)(x-2)$	$17+20\alpha$
$10^{1000}+57867$	$x^2+12x+6$	x^2+6x+6	$12+20\alpha$
$10^{1000}+59743$	$x^2+16x+12$	$(x-21)(x-5)$	$28+16\alpha$
$10^{1000}+61053$	$(x-18)(x-16)$	$x^2+15x+9$	$24+2\alpha$
$10^{1000}+61353$	$(x-26)(x-13)$	$x^2+30x+28$	$11+18\alpha$
$10^{1000}+63729$	$x^2+4x+23$	$(x-18)(x-3)$	$3+11\alpha$
$10^{1000}+64047$	$(x-19)(x-3)$	$(x-13)(x-2)$	$25+18\alpha$
$10^{1000}+64749$	$(x-13)(x-10)$	$(x-17)(x-4)$	$15+14\alpha$
$10^{1000}+68139$	$x^2+2x+26$	$(x-19)(x-3)$	$1+18\alpha$
$10^{1000}+68367$	$(x-22)(x-2)$	$x^2+21x+13$	$30+5\alpha$
$10^{1000}+70897$	$x^2+8x+25$	$(x-26)^2$	$15+14\alpha$
$10^{1000}+72237$	$(x-11)(x-2)$	$(x-12)(x-7)$	$6+20\alpha$
$10^{1000}+77611$	$x^2+5x+15$	$x^2+28x+15$	$27+6\alpha$
$10^{1000}+78199$	$(x-30)(x-28)$	$(x-25)(x-15)$	$17+2\alpha$
$10^{1000}+79237$	$x^2+10x+26$	$(x-27)(x-9)$	$19+19\alpha$
$10^{1000}+79767$	$(x-15)(x-6)$	$(x-7)(x-4)$	$12+8\alpha$
$10^{1000}+82767$	$(x-13)(x-3)$	$(x-24)(x-21)$	$8+14\alpha$
$10^{1000}+93559$	$(x-15)(x-10)$	$x^2+8x+26$	$17+14\alpha$
$10^{1000}+95107$	$(x-28)(x-20)$	$(x-18)(x-7)$	$18+6\alpha$
$10^{1000}+100003$	$x^2+21x+8$	$(x-10)(x-7)$	$7+13\alpha$

$$f_{26} = E_{14}\Delta = \sum_{n=1}^{+\infty} \tau_{26}(n)q^n = q - 48q^2 - 195804q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{26}(p)$ mod 31
$10^{1000} + 453$	$(x-3)(x-2)$	5
$10^{1000} + 1357$	$(x-23)(x-4)$	27
$10^{1000} + 2713$	$x^2 + 13x + 26$	18
$10^{1000} + 4351$	$(x-13)(x-12)$	25
$10^{1000} + 5733$	$(x-6)(x-1)$	7
$10^{1000} + 7383$	$x^2 + 27x + 5$	4
$10^{1000} + 10401$	$x^2 + 21x + 26$	10
$10^{1000} + 11979$	$(x-27)(x-22)$	18
$10^{1000} + 17557$	$(x-17)(x-11)$	28
$10^{1000} + 21567$	$(x-27)(x-8)$	4
$10^{1000} + 22273$	$x^2 + 2x + 5$	29
$10^{1000} + 24493$	$(x-9)(x-7)$	16
$10^{1000} + 25947$	$(x-20)(x-8)$	28
$10^{1000} + 27057$	$(x-18)(x-12)$	30
$10^{1000} + 29737$	$(x-25)(x-6)$	0
$10^{1000} + 41599$	$x^2 + 23x + 1$	8
$10^{1000} + 43789$	$x^2 + 8x + 26$	23
$10^{1000} + 46227$	$x^2 + 10x + 26$	21
$10^{1000} + 46339$	$x^2 + 22x + 30$	9
$10^{1000} + 52423$	$(x-22)(x-11)$	2
$10^{1000} + 55831$	$x^2 + 17x + 5$	14
$10^{1000} + 57867$	$(x-28)(x-12)$	9
$10^{1000} + 59743$	$x^2 + x + 26$	30
$10^{1000} + 61053$	$(x-5)^2$	10
$10^{1000} + 61353$	$x^2 + 2x + 5$	29
$10^{1000} + 63729$	$(x-29)(x-16)$	14
$10^{1000} + 64047$	$(x-3)(x-2)$	5
$10^{1000} + 64749$	$(x-29)(x-18)$	16
$10^{1000} + 68139$	$x^2 + 27x + 6$	4
$10^{1000} + 68367$	$(x-6)(x-1)$	7
$10^{1000} + 70897$	$x^2 + 24x + 5$	7
$10^{1000} + 72237$	$(x-23)(x-7)$	30
$10^{1000} + 77611$	$x^2 + 8x + 30$	23
$10^{1000} + 78199$	$(x-30)(x-5)$	4
$10^{1000} + 79237$	$(x-11)(x-9)$	20
$10^{1000} + 79767$	$x^2 + 24x + 5$	7
$10^{1000} + 82767$	$x^2 + 20x + 1$	11
$10^{1000} + 93559$	$x^2 + 19x + 6$	12
$10^{1000} + 95107$	$(x-29)(x-15)$	13
$10^{1000} + 100003$	$(x-19)(x-18)$	6

C.2 Certifying the polynomials

The results presented above rely on the identification by continued fractions of rational numbers given in approximate form as floating-point numbers. In order to certify these results, it is thus necessary to make sure that the number fields cut out by the representations as well as the Galois action on them have been correctly identified.

For this, a first possibility consists in proving bounds on the height of the rational numbers the algorithm will have to identify, and then to certify that the continued fraction identification process is correct, for instance by running the computation with high enough precision in $\mathbb{C}$ and controlling the round-off errors all along. Although it is indeed possible to bound the height of the rational numbers which will have to be identified by using Arakelov theory (cf. [CE11, theorem 11.7.6]), this approach (especially the round-off error control in the linear algebra steps in K. Khuri-Makdisi's algorithms) seems ominously tedious, and I have not attempted to follow it.

I deemed it much better to first run the computations in order to obtain unproven results, and then to prove these results. I explain in this section how this can be done in the case of a newform f of level $N = 1$.

C.2.1 Sanity checks

Before attempting to prove the results, it is comforting to perform a few easy checks so as to ensure that these results seem correct beyond reasonable doubt. Namely,

- By theorem A.3.3.3, the number field L cut out by the Galois representation $\rho_{f,\mathfrak{l}}$ attached to a newform $f \in S_k(1)$ is ramified only at ℓ. Therefore, one can check that the discriminant of the polynomial $F(X) \in \mathbb{Q}[X]$ is of the form

$$\pm \ell^n M^2$$

  for some $M \in \mathbb{Q}^*$. Better, one can compute the maximal order of the field $K = \mathbb{Q}[X]/F(X)$ whose Galois closure is L and check that its discriminant is, up to sign, a power of ℓ. Since a number field ramifies at the same primes as its Galois closure, this proves that the decomposition field L of $F(X)$ is ramified only at ℓ.

- Since Galois representations $\rho_{f,\mathfrak{l}}$ attached to modular forms are odd, the image of complex conjugation by these representations is an involutive matrix in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ of determinant -1, hence similar to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ if $\ell \geqslant 2$. This means that the polynomial $F(X)$ of degree $\ell^2 - 1$ computed by the algorithm should have exactly $\ell - 1$ roots in $\mathbb{R}$, which can be checked numerically, and that the sign of its discriminant should be $(-1)^{\ell(\ell-1)/2}$, which can be checked exactly.

- The fact that the resolvents $\Gamma_C(X)$ computed by the Dokchitsers' method seem to have integer (and not just complex) coefficients as expected hints that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so that the number field L is indeed a number field cut out by a Galois representation.

- The fact that the polynomials $F^S(X)$ computed by regrouping the roots of $F(X)$ along their S-orbits for the various subgroups $S \subseteq \mathbb{F}_\ell^*$ considered during the polynomial reduction process (cf. section B.3.5.2) seem to have rational coefficients with common denominator dividing the one of $F(X)$ also hints that the coefficients of these polynomials have been correctly identified as rational numbers, that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and that the Galois action on the root of $F(X)$ is the expected one.

- Finally, one can check that the values $a_p \bmod \mathfrak{l}$ obtained by the algorithm for a few small primes p are correct, by comparing them with the ones computed by "classical" methods based on modular symbols (cf. example A.2.3.12).

C.2.2 Proving the polynomials

I shall now present a method to formally prove that the polynomials computed by my algorithm define the number fields cut out by the corresponding Galois representations. It proceeds from the bottom up, in that it consists in first proving the correctness of the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, then the correctness of the quotient Galois representation $\rho_{f,\mathfrak{l}}^{S}$ where S gradually shifts from the whole of $\mathbb{F}_\mathfrak{l}^*$ to the maximal subgroup of $\mathbb{F}_\mathfrak{l}^*$ not containing -1. In each case, I first prove that I am actually dealing with a Galois representation of the correct kind, which amounts to proving that the Galois group of the polynomial defining the representation is the correct one, and then I prove that the representation is the correct one, that is to say that it is modular and comes from the correct newform.

I shall assume that it has been checked that the polynomials $F^{\mathrm{proj}}(X)$ and $F^S(X)$ computed by my algorithm and reduced as in section B.3.5.2 are irreducible over $\mathbb{Q}$.

C.2.2.1 Proving the projective representation

I begin with the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, which ought to be defined by the monic polynomial $F^{\mathrm{proj}}(X) \in \mathbb{Z}[X]$ of degree $\ell+1$ obtained by the `polred` algorithm (cf. section B.3.5.2). Recall that I denote its splitting field in $\mathbb{C}$ by L^{proj}.

Proving the Galois group

The first thing to do is to make sure that this polynomial does define a projective Galois representation, by proving that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ is isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Since I am dealing with forms of level $N=1$, hence of trivial nebentypus ε, and of even weight, the determinant of the associated mod $\mathfrak{l}$ Galois representations $\rho_{f,\mathfrak{l}}$ are odd powers of the cyclotomic character mod ℓ, and so there are matrices with non-square determinant in the image of each of these representations, so that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ should actually be the whole of $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

The roots a_x, $x \in \mathbb{P}^1\mathbb{F}_\ell$ of $F^{\mathrm{proj}}(X)$ in $\mathbb{C}$ computed by my algorithm are by construction indexed by $\mathbb{P}^1\mathbb{F}_\ell$. Consider the resolvent polynomial

$$R_4^{\mathrm{proj}}(X) = \prod_{\substack{x_1,x_2,x_3,x_4 \in \mathbb{P}^1\mathbb{F}_\ell \\ \text{pairwise distinct}}} \big(X - (\lambda_1 a_{x_1} + \lambda_2 a_{x_2} + \lambda_3 a_{x_3} + \lambda_4 a_{x_4})\big) \in \mathbb{Z}[X],$$

where $\lambda_1, \cdots, \lambda_4 \in \mathbb{Z}$ are fixed integer parameters chosen so that $R_4^{\mathrm{proj}}(X)$ is squarefree.

Recall that the *composed sum* of two polynomials f and $g \in \mathbb{Q}[X]$ is

$$f \oplus g = \prod_{f(\alpha)=g(\beta)=0} \big(X - (\alpha+\beta)\big),$$

where the product runs over the roots α of f and β of g in $\overline{\mathbb{Q}}$ counted with multiplicity. As explained in [BFSS06], it can be computed with quasilinear complexity as follows:

Define, for monic $f \in \mathbb{Q}[X]$, the *exponential Newton sum generating series* of f by

$$H(f) = \sum_{n=0}^{+\infty} \frac{\nu_n(f)}{n!} T^n \in \mathbb{Q}\big[[T]\big],$$

where the $\nu_n(f)$ are the *Newton sums* of f,

$$\nu_n(f) = \sum_{f(\alpha)=0} \alpha^n,$$

the sum running over the roots α of f in $\overline{\mathbb{Q}}$ counted with multiplicity. Then for $B \geqslant \deg f$, the conversion between f and $H(f) \bmod T^B$ can be performed in $\widetilde{O}(B)$ bit operations, by using fast power series arithmetic and the formulae

$$\sum_{n=0}^{\infty} \nu_n(f) T^n = \sum_{f(\alpha)=0} \frac{1}{1-\alpha T} = \frac{\mathrm{rev}(f')}{\mathrm{rev}(f)}$$

in the one way, and

$$\mathrm{rev}(f) = \exp\left(-\sum_{n=1}^{\infty} \frac{\nu_n}{n} T^n\right)$$

in the other way, where $\mathrm{rev}(f) = X^{\deg f} f(1/X)$ denotes the reverse of a polynomial f. Since furthermore

$$H(f \oplus g) = H(f) H(g)$$

for any two polynomials f and g in $\mathbb{Q}[X]$, this yields a quasilinear method to symbolically compute composed sums, and hence the resolvent $R_4^{\mathrm{proj}}(X)$.

Once I have computed the resolvent $R_4^{\mathrm{proj}}(X)$ symbolically, I compute numerically a complex approximation of the factor

$$R_x(X) = \prod_{\substack{x_1,x_2,x_3,x_4 \in \mathbb{P}^1\mathbb{F}_\ell \\ \text{pairwise distinct} \\ [x_1,x_2,x_3,x_4]=x}} \big(X - (\lambda_1 a_{x_1} + \lambda_2 a_{x_2} + \lambda_3 a_{x_3} + \lambda_4 a_{x_4})\big) \in \mathbb{C}[X]$$

for each $x \in \mathbb{P}^1\mathbb{F}_\ell - \{\infty, 0, 1\}$, where $[x_1, x_2, x_3, x_4] = \frac{x_3-x_1}{x_3-x_2}\frac{x_4-x_2}{x_4-x_1} \in \mathbb{P}^1\mathbb{F}_\ell$ denotes the cross-ratio (a.k.a. anharmonic ratio) of the x_i, and check that this approximation seems to lie in $\mathbb{Z}[X]$. I then check that the polynomials $R_x(X)$ all divide $R_4^{\mathrm{proj}}(X)$ in $\mathbb{Z}[X]$.

This proves that the action of $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ on the ordered quadruplets of roots of $F^{\mathrm{proj}}(X)$ preserves the cross-ratio, which implies that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acting on the roots a_x, $x \in \mathbb{P}^1\mathbb{F}_\ell$ of $F^{\mathrm{proj}}(X)$ in the same way as $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acts on $\mathbb{P}^1\mathbb{F}_\ell$.

Correctness of the projective representation

Now that I have made sure that the Galois action on the roots of $F^{\mathrm{proj}}(X)$ does define a projective representation

$$\rho^{\mathrm{proj}}\colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q}) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)\ ,$$

I prove that this representation is isomorphic to $\rho^{\mathrm{proj}}_{f,\mathfrak{l}}$ as expected. For this, I use the following theorem from [Bos07]:

Theorem C.2.2.1. *Let $\pi\colon G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an projective mod ℓ Galois representation. Let $H \subset \mathrm{PGL}_2(\mathbb{F}_\ell)$ be the stabiliser of a point of $\mathbb{P}^1\mathbb{F}_\ell$, and let $K = \overline{\mathbb{Q}}^{\pi^{-1}(H)}$ be the corresponding number field. If the number field L cut out by π is not totally real and if there exists an integer k such that*

$$\mathrm{Disc}\, K = \pm\ell^{k+\ell-2},$$

then there exists a newform $f \in S_k(1)$ and a prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ such that

$$\pi \sim \rho^{proj}_{f,\mathfrak{l}}.$$

Proof. This is [Bos07]. The idea is that the projective representation π can be lifted to a linear representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

which, just like π, is irreducible and ramifies only at ℓ. Furthermore, the image of the complex conjugation (corresponding to some embedding of L into $\mathbb{C}$) by ρ has order at most 2, so is similar to either $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$ or $\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$, but the first two are impossible since they reduce to the identity in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and L is not totally real, which proves that ρ is odd. Serre's conjecture A.3.4.10 then applies and shows that $\rho \sim \rho_{f,\mathfrak{l}}$ for some newform $f \in S_{k_\rho}(N_\rho, \varepsilon_\rho)$ and some prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ. Then $N_\rho = 1$ by example A.3.4.3, so that ε_ρ is trivial. Next, if the lift ρ is chosen so that k_ρ is minimal, then [MT03, theorem 3] gives a formula for the ℓ-adic valuation of the discriminant of the Galois number field cut out by ρ, which by J. Bosman's work boils down to

$$\mathrm{Disc}\, K = \pm\ell^{k_\rho+\ell-2}.$$

□

Thus, in order to prove that $\rho^{\mathrm{proj}} \sim \rho^{\mathrm{proj}}_{f,\mathfrak{l}}$, all I have to do is check that not all the roots of $F^{\mathrm{proj}}(X)$ are real, which can be done by using Sturm's method (cf. [Lan02, chapter XI, theorem 2.7]), and that the discriminant of the rupture field $K^{\mathrm{proj}} = \mathbb{Q}[X]/F^{\mathrm{proj}}(X)$ is $\pm\ell^{k+\ell-2}$, which is a piece of cake for [Pari/GP].

Except in the case $\ell = 31, k = 24$, this concludes in all the cases I have computed since $\dim S_k(1) = 1$ so that there is only one possibility for f, and its coefficients are rational so that the choice of $\mathfrak{l}$ does not matter. In the special case $\ell = 31, k = 24$, I still know that ρ^{proj} is equivalent to either $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_5}$ or its conjugate $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_{27}}$. I order to tell which, I pick a small prime $p \in \mathbb{N}$ which does not divide $\mathrm{Disc}\, F^{\mathrm{proj}}(X)$ (in particular $p \neq \ell$), and such that $\tau_{24}(p) \equiv 0 \bmod \mathfrak{l}_5$ but $\tau_{24}(p) \not\equiv 0 \bmod \mathfrak{l}_{27}$ (the opposite would

do too). Since an element of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is of order 2 if and only if it has trace 0, looking at the factorisation of $F^{\mathrm{proj}}(X)$ mod p allows me to tell $\mathfrak{l}_5$ and $\mathfrak{l}_{27}$ apart: if $F^{\mathrm{proj}}(X)$ splits into linear and quadratic factors in $\mathbb{F}_p[X]$, then it is associated to $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_5}$, else it is associated to $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_{27}}$.

In particular, this implies that the Galois group $\mathrm{Gal}(L_0/\mathbb{Q})$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ (whereas I had only proved that it was isomorphic to a transitive subgroup thereof until now).

C.2.2.2 Proof of the polynomial $F^S(X)$

I now move on to the polynomial $F^S(X)$ defining the quotient representation. Write $\ell - 1 = 2^r m$ with m odd, and recall from section B.3.5.2 that I considered the filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $[S_i : S_{i+1}] = 2$ for all i, so that

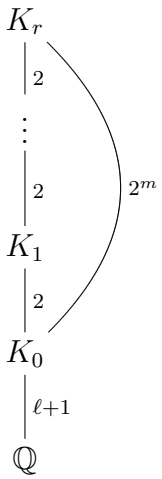
$$S_i = \mathrm{Im}\begin{pmatrix} \mathbb{F}_\ell^* & \longrightarrow & \mathbb{F}_\ell^* \\ x & \longmapsto & x^{2^i} \end{pmatrix},$$

and I computed polynomials $F_i(X) \in \mathbb{Z}[X]$ such that the Galois action on the roots of $F_i(X)$ is supposed to yield the quotient Galois representation

$$\rho^{S_i}_{f,\mathfrak{l}}\colon\ G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i\ .$$

Let $K_i = \mathbb{Q}[X]/F_i(X)$ be the rupture field of $F_i(X)$, and L_i be its Galois closure, which is thus supposed to be the number field cut out by ρ^{S_i}. I have just proved above that it is the case for $i = 0$.

For each $i < r$, the extension K_{i+1}/K_i is quadratic by construction, generated by the square root of some primitive element δ_i of K_i, so that the fields K_i fit in an extension tower



Let $\ell^* = (-1)^{(\ell-1)/2}\ell$, so that $\mathbb{Q}(\sqrt{\ell^*})$ is the unique quadratic number field which ramifies only at ℓ, and consider the following assertions:

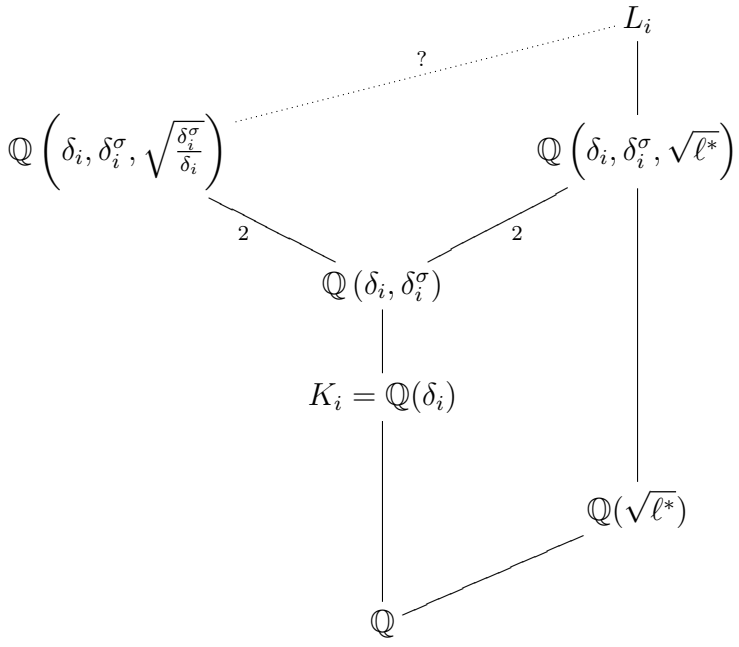
(A1) The polynomials $F_i(X)$ are irreducible in $\mathbb{Q}[X]$, and their decomposition fields L_i ramify only at ℓ.

(A2) For each i, let $\Delta_i(X) \in \mathbb{Z}[X]$ be the monic minimal polynomial of δ_i over $\mathbb{Q}$, and let
$$Q_i(X) = \frac{\mathrm{Res}_Y\big(\Delta_i(Y), \Delta_i(XY)\big)}{(X-1)^{2^i(\ell+1)}} \in \mathbb{Z}[X].$$
Then $Q_i(X)$ is irreducible over $\mathbb{Q}$ and even over $\mathbb{Q}(\sqrt{\ell^*})$, but $Q_i(X^2)$ splits into two factors of equal degrees over $\mathbb{Q}(\sqrt{\ell^*})$.

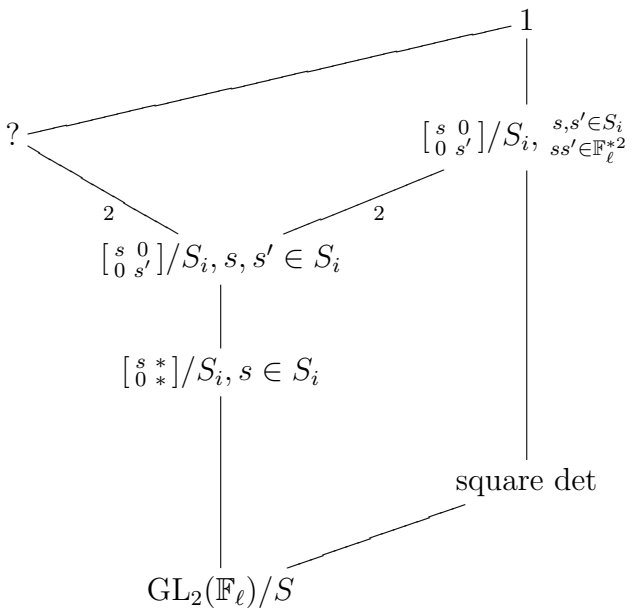
These assertions can be proved easily with [Pari/GP]. For (A1), it suffices to check that the discriminant of the rupture field K_i of $F_i(X)$ is of the form $\pm\ell^n$ for some $n \in \mathbb{N}$. For (A2), note that for any $f = \prod_{i=1}^n (X - \alpha_i)$ such that $f(0) \neq 0$,
$$\mathrm{Res}_Y\big(f(Y), f(XY)\big) = (-1)^n f(0) \prod_{i,j} \left(X - \frac{\alpha_i}{\alpha_j}\right),$$
so that
$$\frac{\mathrm{Res}_Y\big(f(Y), f(XY)\big)}{(X-1)^n} = (-1)^n f(0) \prod_{i \neq j} \left(X - \frac{\alpha_i}{\alpha_j}\right),$$
which shows that $Q_i(X)$ is indeed a polynomial.

I shall now prove that if these assertions hold, then for all $i \leqslant r$, L_i is the number field cut out by $\rho_{f,\mathfrak{l}}^{S_i}$.

To begin with, I shall prove that $\mathrm{Gal}(L_i/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. Since $K_{i+1} = K_i(\sqrt{\delta_i})$, one has
$$L_{i+1} = L_i\big(\sqrt{\delta_i^\sigma}, \sigma \in \mathrm{Gal}(L_i/\mathbb{Q})\big).$$
I first claim that actually $L_{i+1} = L_i(\sqrt{\delta_i})$, that is to say that $\frac{\delta_i^\sigma}{\delta_i}$ is a square in L_i for all $\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})$. To see this, note that since $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has a quotient $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell)$ of order 2, the field $L_i \supset L_0$ has a quadratic subfield, which can only be $\mathbb{Q}(\sqrt{\ell^*})$ since L_i ramifies only at ℓ by (A1). Consider the extension diagram



Assume for now that the extensions marked with a 2 are indeed quadratic and not trivial. If L_i **were** the number field cut out by $\rho_{f,\mathfrak{l}}^{S_i}$, then the corresponding Galois subgroup diagram would be



and since the group

$$\left\{ \begin{bmatrix} s & 0 \\ 0 & s' \end{bmatrix} /S_i,\ s, s' \in S_i \right\} \simeq \mathbb{F}_\ell^*/S_i$$

is cyclic, it has only one subgroup of index 2, so that these two quadratic extensions should agree.

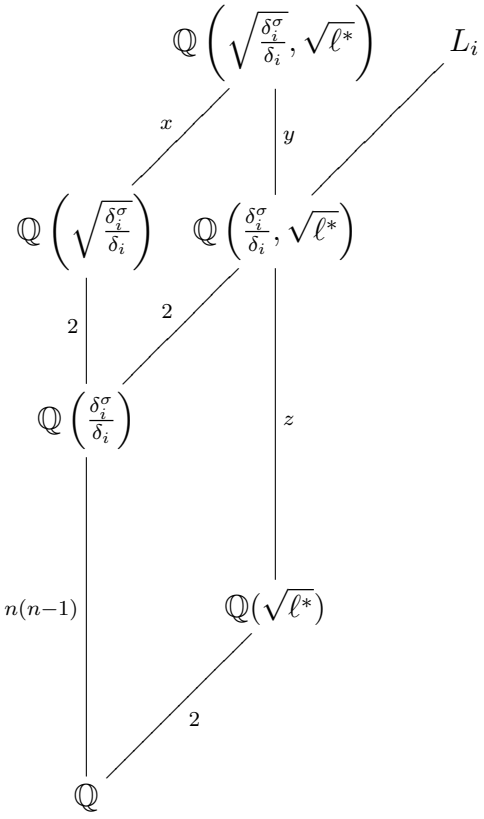
Now, back to the proof, letting $n = 2^i(\ell+1) = [K_i\colon \mathbb{Q}]$, then

$$[\mathbb{Q}(\delta_i, \delta_i^\sigma) : \mathbb{Q}] = [\mathbb{Q}(\delta_i, \delta_i^\sigma) : \mathbb{Q}(\delta_i)][\mathbb{Q}(\delta_i) : \mathbb{Q}] \leqslant (n-1)n,$$

whereas

$$\left[\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right) : \mathbb{Q}\right] = \deg Q_i(X) = (n-1)n$$

since $Q_i(X)$ is irreducible over $\mathbb{Q}$ by (A2), so that $\mathbb{Q}(\delta_i, \delta_i^\sigma) = \mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$. Furthermore, the extension $\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}, \sqrt{\ell^*}\right)/\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ is not trivial since $Q_i(X)$ is irreducible over $\mathbb{Q}(\sqrt{\ell^*})$ by (A2). I may also assume that the extension $\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right)/\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ is not trivial, since the proof that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ is over if it is. The two extensions marked with a 2 in the extension tower above are thus non-trivial, hence quadratic, so that one has the extension diagram



where the labels denote the degrees. By looking at the bottom parallelogram, one sees that $z = n(n-1)$, so that $x = y$ by looking at the top parallelogram. Now since $Q_i(X^2)$ splits into two factors of degrees $n(n-1)$ over $\mathbb{Q}(\sqrt{\ell^*})$ by (A2), one has

$$\left[\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}, \sqrt{\ell^*}\right) : \mathbb{Q}(\sqrt{\ell^*})\right] = n(n-1),$$

so that $y = 1$, whence $x = 1$. Therefore

$$\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right) = \mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}, \sqrt{\ell^*}\right) = \mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}, \sqrt{\ell^*}\right) \subset L_i,$$

so that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ as I claimed.

As a consequence, $L_{i+1} = L_i(\sqrt{\delta_i})$ and $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_i/\mathbb{Q})$ by $\mathbb{Z}/2\mathbb{Z}$, which is necessarily central since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial.

Recall now that given a group G and a G-module M, the extensions of G by M such that the conjugation action of lifts of elements of G on M corresponds to the G-module structure on M are classified by the cohomology group $H^2(G, M)$, the class of the cocycle $\beta\colon G \times G \longrightarrow M$ corresponding to the set $M \times G$ endowed with the group law

$$(m, g) \cdot (m', g') = \big(m + g \cdot m' + \beta(g, g'), gg'\big).$$

Example C.2.2.2. Consider an extension

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

of a group G by $\mathbb{Z}/2\mathbb{Z}$. The G-action on $\mathbb{Z}/2\mathbb{Z}$ is necessarily trivial since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial, so this extension is necessarily central. Let $\beta\colon G\times G \longrightarrow \mathbb{Z}/2\mathbb{Z}$ be a cocycle representing the corresponding cohomology class, and let $g \in G$ be an element of G of order 2. Then the lifts of g in $\widetilde{G}$ are the (x, g), $x \in \mathbb{Z}/2\mathbb{Z}$, and one computes that

$$(x, g) \cdot (x, g) = \big(x + x + \beta(g, g), g^2\big) = \big(\beta(g, g), 1\big)$$

in $\widetilde{G}$. Therefore, the lifts of g have order 2 if $\beta(g, g) = 0$, but have order 4 if $\beta(g, g) = 1$.

Furthermore (cf. [Kar87, theorem 2.1.19]), if M is a trivial G-module, there is a split exact sequence of abelian groups

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M) \xhookrightarrow{\ \phi\ } H^2(G, M) \underset{\longleftarrow}{\overset{\psi}{\rightleftarrows}} \mathrm{Hom}\left(\widehat{M}, H^2(G, \mathbb{C}^*)\right) \longrightarrow 0 \quad \text{(C.2.2.3)}$$

where $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M)$ classifies the abelian extensions of the abelianised G^{ab} of G by M, $\widehat{M} = \mathrm{Hom}(M, \mathbb{C}^*)$ is the group of complex-valued characters on M, $H^2(G, \mathbb{C}^*)$ (with trivial G-action on $\mathbb{C}^*$) is the so-called *Schur multiplier* of G, and ψ maps the class of the cocycle $\beta \in H^2(G, M)$ to the *transgression map* (not to be confused with a trace)

$$\begin{array}{rccc} \mathrm{Tra}_\beta\colon & \widehat{M} & \longrightarrow & H^2(G, \mathbb{C}^*) \\ & \chi & \longmapsto & \chi \circ \beta \end{array}$$

associated to the class of β. Besides, the Schur multiplier $H^2(G, \mathbb{C}^*)$ is trivial if G is cyclic (cf. [Kar87, proposition 2.1.1.(ii)]), and for each central extension $\widetilde{G}$ of G by M, the subgroup $M \cap D\widetilde{G}$ of $\widetilde{G}$ is isomorphic to the image of Tra_β, where $\beta \in H^2(G, M)$ is the cohomology class corresponding to $\widetilde{G}$, and $D\widetilde{G}$ denotes the commutator subgroup of $\widetilde{G}$ (cf. [Kar87, proposition 2.1.7]).

Applying this to the group $G = \mathrm{PGL}_2(\mathbb{F}_\ell)$ and the trivial G-module $M = \mathbb{Z}/2^i\mathbb{Z}$ yields the following result (cf. [Que95]):

Theorem C.2.2.4. *Let $i \in \mathbb{N}$.*

(i) $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, *so that there are four central extensions of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$ *by* $\mathbb{Z}/2^i\mathbb{Z}$.

(ii) These extensions are

- *the trivial extension* $\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, *corresponding to the trivial cohomology class* $\beta_0 \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$,
- *the group* $2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, *whose associated cohomology class* $\beta_{\mathrm{det}} \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ *is the inflation of the non-trivial element of*
$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}$$
(in other words, $\beta_{\mathrm{det}}(g, g')$ *is non-zero if and only if neither* g *nor* g' *lie in* $\mathrm{PSL}_2(\mathbb{F}_\ell)$*),*
- *the group* $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$, *with associated cohomology class* $\beta_- \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$, *defined for* $i = 1$ *as*
$$2_-\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathrm{SL}_2(\mathbb{F}_\ell) \sqcup \begin{bmatrix} \sqrt{\varepsilon} & 0 \\ 0 & 1/\sqrt{\varepsilon} \end{bmatrix} \mathrm{SL}_2(\mathbb{F}_\ell) \subset \mathrm{SL}_2(\mathbb{F}_{\ell^2})$$
where ε *denotes a generator of* $\mathbb{F}_\ell^*$, *and which* $i \geqslant 2$ *corresponds the image of the cohomology class of* $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ *by the map*
$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2\mathbb{Z}\big) \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$$
induced by the embedding of $\mathbb{Z}/2\mathbb{Z}$ *into* $\mathbb{Z}/2^i\mathbb{Z}$,
- *and the group* $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$, *whose associated cohomology class* β_+ *is the sum in* $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ *of* β_{det} *and of* β_-.

(iii) Let $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ *be an element of order 2, and let* β_0, β_{det}, β_- *and* β_+ *be normalised cocycles (that is to say* $\beta(1, h) = \beta(h, 1) = 0$ *for all* $h \in \mathrm{PGL}_2(\mathbb{F}_\ell)$*) representing the cohomology classes of these four extensions. If* $i = 1$, *then their value at* (g, g) *does not depend on the choice of these cocycles, and are*

- $\beta_0(g, g) = 0 \ \forall g$,
- $\beta_{\mathrm{det}}(g, g) = \begin{cases} 0, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 1, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell), \end{cases}$
- $\beta_-(g, g) = 1 \ \forall g$,
- $\beta_+(g, g) = \begin{cases} 1, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 0, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell). \end{cases}$

(iv) For $i \geqslant 2$, *the abelianisations of these extensions are*

- $\big(\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
- $\big(2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^{i+1}\mathbb{Z}$,
- $\big(2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^{i-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
- $\big(2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^i\mathbb{Z}$.

Proof. I shall only give the idea of the proof here, and refer the reader to [Que95, proposition 2.4 and lemma 3.2].

(i) On the one hand, the abelianised of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathbb{Z}/2\mathbb{Z}$, so that

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, \mathbb{Z}/2^i\mathbb{Z}) \simeq \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, the Schur multiplier $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (cf. [Que95, proposition 2.3]). The result then follows from the split exact sequence (C.2.2.3).

(ii) Consider again the exact sequence (C.2.2.3). Then β_{det} lies in the image of ϕ since it is inflated from $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}$. On the other hand, for $i = 1$, β_- does not lie in $\mathrm{Im}\,\phi$, for if it did, then the associated transgression map would be trivial, so that the commutator subgroup of $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ would meet the kernel $\pm\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ of the extension trivially, which is clearly not the case since $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$ is a commutator in $\mathrm{SL}_2(\mathbb{F}_\ell) \subset 2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$. For $i \geqslant 2$, the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 2_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}/2^i\mathbb{Z} & \longrightarrow & 2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1
\end{array}$$

shows that $\mathbb{Z}/2^i\mathbb{Z}$ still intersects the commutator subgroup of $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ non-trivially, so that β_- does not lie in $\mathrm{Im}\,\phi$ either. The extensions $2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ thus represent different non-trivial cohomology classes in $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, hence the result.

(iii) It is a general fact (cf. [Que95, lemma 3.1] that the image at (g, g) of a normalised cocycle representing an extension of a group G by $\mathbb{Z}/2\mathbb{Z}$ only depends on the cohomology class of this cocycle in $H^2(G, \mathbb{Z}/2\mathbb{Z})$.

- The case of the trivial extension is obvious since the zero cohomology class is represented by the zero cocycle.
- The case of β_{det} follows from its very definition.
- Since it is a subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$, the group $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ has only one element of order 2, namely the central element $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$. In particular, no element $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order 2 remains of order 2 when lifted to $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$, and the result follows by example C.2.2.2.
- The case of β_+ follows since one may take $\beta_+ = \beta_{\mathrm{det}} + \beta_-$.

(iv) Again, the case of the trivial extension is clear. In the other cases, the result follows from the fact that the intersection of $\mathbb{Z}/2^i\mathbb{Z}$ with the commutator subgroup of the extension is isomorphic to the image of transgression map

$$\mathrm{Tra}_\beta \colon \widehat{\mathbb{Z}/2^i\mathbb{Z}} \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq \mathbb{Z}/2\mathbb{Z},$$

which is trivial in the case of β_{det} and non-trivial in the case of β_- and β_+. □

I shall now prove that $\mathrm{Gal}(L_r/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. I first deal with the first extension L_1/L_0 in the quadratic tower $L_r/\cdots/L_0$. The Galois group $\mathrm{Gal}(L_1/\mathbb{Q})$ is a (necessarily central) extension of $\mathrm{Gal}(L_0/\mathbb{Q})$, which is isomorphic by $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ since L_0 is the number field cut out by $\rho_{f,\mathfrak{l}}$. Let β be a normalised cocycle representing the cohomology class corresponding to this extension. According to theorem C.2.2.4(ii), $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic either to $\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$, and β is correspondingly cohomologous to β_0, $\beta_{\det}$, β_- or β_+.

If $\mathrm{Gal}(L_1/\mathbb{Q})$ were the trivial extension $\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$, then L_1 would have a subextension L_1^{ab} with Galois group isomorphic to

$$\bigl(\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)\bigr)^{\mathrm{ab}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

and hence three distinct quadratic subfields, which is impossible since L_1 is ramified only at ℓ by (A1), yet there is only one quadratic number field which ramifies only at ℓ, namely $\mathbb{Q}(\sqrt{\ell^*})$.

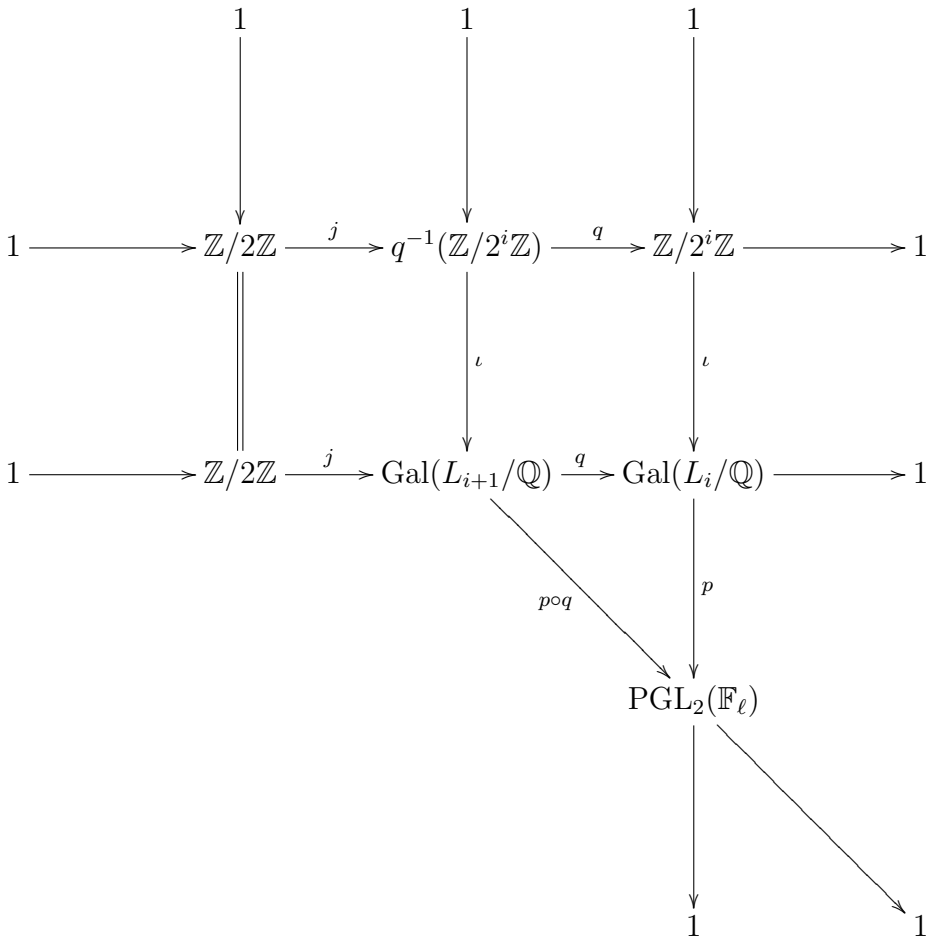
Let now $\tau_1\in\mathrm{Gal}(L_1/\mathbb{Q})$ be the complex conjugation relative to some embedding of L_1 into $\mathbb{C}$. It induces an element $\tau_0\in\mathrm{Gal}(L_0/\mathbb{Q})$, which is not the identity since its image by $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ is conjugate to $g=\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]\in\mathrm{PGL}_2(\mathbb{F}_\ell)$. In particular, τ_1 is not trivial either, so it has order 2. Therefore τ_0 has a lift to $\mathrm{Gal}(L_1/\mathbb{Q})$ of order 2, so that $\beta(g,g)=0$ by example C.2.2.2. Theorem C.2.2.4(iii) then only leaves one possibility: if $\ell\equiv 1 \bmod 4$, then $g\in\mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to β_+, so $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic to $2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$, whereas if $\ell\equiv -1 \bmod 4$, then $g\notin\mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to $\beta_{\det}$, so $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic to $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Now let L_1' be the number field cut out by $\rho_{f,\mathfrak{l}}^{S_1}$, which is supposed to be isomorphic to L_1. Then L_1' is also a quadratic extension of L_0 and is also only ramified at ℓ, so that the same reasoning applies and shows that $\mathrm{Gal}(L_1'/\mathbb{Q})$ is isomorphic to $2_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell\equiv 1 \bmod 4$ and to $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell\equiv 1 \bmod 4$. On the other hand, it is isomorphic to $\mathrm{Im}\,\rho_{f,\mathfrak{l}}^{S_1}\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ since the determinant of $\rho_{f,\mathfrak{l}}$ is an odd power of the mod ℓ cyclotomic character, so that in each case

$$\mathrm{Gal}(L_1/\mathbb{Q})\simeq\mathrm{Gal}(L_1'/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_1.$$

If $\ell\equiv -1 \bmod 4$, then $r=1$, so that the proof that $\mathrm{Gal}(L_r/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ is over. I shall therefore concentrate on the case $\ell\equiv 1 \bmod 4$ from now on. I shall first prove by induction on i that $\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathbb{F}_\ell^*/S_i\simeq\mathbb{Z}/2^i\mathbb{Z}$. Note that I have just proved above that this is the case for $i=1$.

Let $1 \leqslant i < r$. By induction hypothesis, there is a commutative diagram



whose middle row and right column are exact. A diagram chase then reveals that the top row and the diagonal short sequence

$$1 \longrightarrow q^{-1}(\mathbb{Z}/2^i\mathbb{Z}) \xrightarrow{\iota} \mathrm{Gal}(L_{i+1}/\mathbb{Q}) \xrightarrow{p\circ q} \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

are exact, so that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $q^{-1}(\mathbb{Z}/2^i\mathbb{Z})$, which itself is an extension of $\mathbb{Z}/2^i\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$, which is necessarily central since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial.

Now $H^2(\mathbb{Z}/2^i\mathbb{Z}, \mathbb{C}^*) = \{0\}$ since $\mathbb{Z}/2^i\mathbb{Z}$ is cyclic, so the extensions of of $\mathbb{Z}/2^i\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$ are all abelian by the exact sequence (C.2.2.3), so that $q^{-1}(\mathbb{Z}/2^i\mathbb{Z}) = \mathrm{Gal}(L_{i+1}/L_0)$ is isomorphic either to $\mathbb{Z}/2^{i+1}\mathbb{Z}$ or to $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. I shall now prove that the latter is impossible.

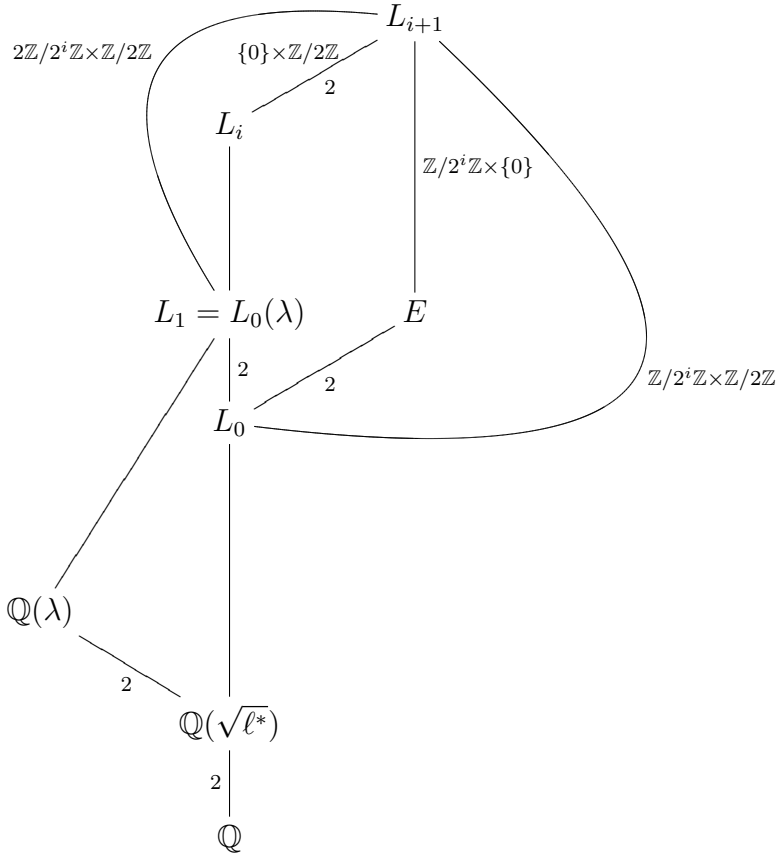
Since $\ell \equiv 1 \bmod 4$, $S_1^2 = \mathbb{F}_\ell^{*4}$ is a strict subgroup of $S_1 = \mathbb{F}_\ell^{*2}$. The determinant induces a surjective morphism

$$\mathrm{Gal}(L_1/\mathbb{Q}) \xrightarrow[\sim]{\rho_{f,\mathfrak{l}}^{S_1}} \mathrm{GL}_2(\mathbb{F}_\ell)/S_1 \xrightarrow{\det} \mathbb{F}_\ell^*/S_1^2 = \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*4} \simeq \mathbb{Z}/4\mathbb{Z},$$

so that L_1 has a quartic subfield. This subfield is abelian, hence is a subfield of the cyclotomic extension $\mathbb{Q}(\mu_\infty)$, and ramifies only at ℓ since L_1 ramifies only at ℓ by (A1), so is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$. Since

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right) \simeq \mathbb{Z}_\ell^* = \mathbb{F}_\ell^* \times (1 + \ell\mathbb{Z}_\ell) \simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}_\ell$$

has only one quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (it does exist since $\ell \equiv 1 \bmod 4$), this quartic subfield is unique, and I shall denote a primitive element of it by λ. This λ thus lies in L_1, but it cannot lie in L_0 since the maximal abelian subextension of L_0 has Galois group $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ (and hence is $\mathbb{Q}(\sqrt{\ell^*})$). Since $\mathbb{Q}(\lambda)$ is a quadratic extension of $\mathbb{Q}(\sqrt{\ell^*}) \subset L_0$ and L_1 is a quadratic extension of L_0, one has $L_1 = L_0(\lambda)$. Now if $\mathrm{Gal}(L_{i+1}/L_0)$ were isomorphic to $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then, letting E be the subfield of L_{i+1} fixed by $\mathbb{Z}/2^i\mathbb{Z} \times \{0\}$, one would have the extension tower



The extensions E/L_0 and L_1/L_0 are both quadratic subextensions of L_{i+1}/L_0, but they are distinct since they correspond respectively to the distinct subgroups $\mathbb{Z}/2^i\mathbb{Z} \times \{0\}$ and $2\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of $\mathrm{Gal}(L_{i+1}/L_0) = \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On the other hand, the field E is a quadratic extension of L_0 which is ramified only at ℓ since L_{i+1} is by (A1), so the same reasoning as above shows that its Galois group is $\mathrm{Gal}(E/\mathbb{Q}) \simeq 2_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ since $\ell \equiv 1 \bmod 4$, so that it has a quartic subfield, which can only be $\mathbb{Q}(\lambda)$. But then $E \supseteq L_0(\lambda) = L_1$, hence $E = L_1$ since they are both quadratic extensions of L_0, a contradiction. This shows that $\mathrm{Gal}(L_{i+1}/L_0)$ cannot be isomorphic to $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so must be isomorphic to $\mathbb{Z}/2^{i+1}\mathbb{Z}$. It follows that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathrm{Gal}(L_{i+1}/L_0) \simeq \mathbb{Z}/2^{i+1}\mathbb{Z}$, and the induction is complete.

I shall now prove by induction on i that this extension is central. Note that it is true for $i = 1$, since every extension by $\mathbb{Z}/2\mathbb{Z}$ is central since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial. Let $i \geqslant 2$, and assume on the contrary that the extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

is not central. Since $\mathrm{Aut}(\mathbb{Z}/2^i\mathbb{Z}) \simeq (\mathbb{Z}/2^i\mathbb{Z})^*$ is abelian, the morphism $\mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{Aut}(\mathbb{Z}/2^i\mathbb{Z})$ expressing the conjugation action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{Z}/2^i\mathbb{Z}$ factors through $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathbb{Z}/2\mathbb{Z}$, so that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially whereas there exists an involution ϕ of $\mathbb{Z}/2^i\mathbb{Z}$ such that $g \cdot x = \phi(x)$ for all $g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $x \in \mathbb{Z}/2^i\mathbb{Z}$. By induction hypothesis, this involution induces the identity on $\mathbb{Z}/2^{i-1}\mathbb{Z}$, so it must be $x \mapsto (1+2^{i-1})x$.

There is thus only one possible non-trivial action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. In order to compute $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ for this non-trivial action, I use the *inflation-restriction exact sequence*:

Lemma C.2.2.5. *Let $q \in \mathbb{N}$, let G be a group, let $H \lhd G$ be a normal subgroup of G, and let M be a G-module. If $H^j(H, A) = 0$ for all $1 \leqslant j \leqslant q-1$, then the sequence*

$$0 \longrightarrow H^q(G/H, M^H) \xrightarrow{\mathrm{Infl}} H^q(G, M) \xrightarrow{\mathrm{Res}} H^q(H, M)$$

is exact.

For a proof, see for instance [Ser62, chapter VII §6 proposition 5]. As $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, one has

$$H^1\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) = \mathrm{Hom}\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) = 0$$

since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple, so that lemma C.2.2.5 applies and yields the exact sequence

$$0 \longrightarrow H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) \xrightarrow{\mathrm{Infl}} H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \xrightarrow{\mathrm{Res}} H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big). \tag{C.2.2.6}$$

On the one hand, since $\mathbb{Z}/2\mathbb{Z} = \{1, \varepsilon\}$ is cyclic, the groups $H^q(\mathbb{Z}/2\mathbb{Z}, M)$ are the cohomology groups of the complex

$$0 \longrightarrow M \xrightarrow{\varepsilon-1} M \xrightarrow{\varepsilon+1} M \xrightarrow{\varepsilon-1} M \xrightarrow{\varepsilon+1} \cdots$$

for any $\mathbb{Z}/2\mathbb{Z}$-module M (cf. [Lan02, chapter XX exercise 16]). In particular,

$$H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) = \frac{\mathrm{Ker}(\varepsilon-1)}{\mathrm{Im}(\varepsilon+1)} = \frac{(\mathbb{Z}/2^i\mathbb{Z})[2^{i-1}]}{(2+2^{i-1})(\mathbb{Z}/2^i\mathbb{Z})} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}, & i = 2, \\ 0, & i \geqslant 3. \end{cases}$$

On the other hand, as $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, the group $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ can be computed by using the split exact sequence (C.2.2.3). As $\mathrm{PSL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \{1\}$ since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple, and as the Schur multiplier is

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq \mathbb{Z}/2\mathbb{Z}$$

(Steinberg, cf. [Kar87, theorem 7.1.1.(ii)]), it results that

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Let $2^i\mathrm{PSL}_2(\mathbb{F}_\ell)$ denote the non-trivial extension. One has

$$2\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_\ell),$$

and the non-trivial element of $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2^i\mathbb{Z}\big)$ is the image of the non-trivial element $\gamma_{\mathrm{SL}_2}\in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2\mathbb{Z}\big)$ corresponding to $\mathrm{SL}_2(\mathbb{F}_\ell)$ by the map

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2\mathbb{Z}\big)\longrightarrow H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2^i\mathbb{Z}\big)$$

induced by the embedding of $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}/2^i\mathbb{Z}$.

Consider the inflation-restriction exact sequence (C.2.2.6), and let

$$\beta\in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell),\mathbb{Z}/2^i\mathbb{Z}\big)$$

be the cohomology class corresponding to the extension

$$0\longrightarrow\mathbb{Z}/2^i\mathbb{Z}\longrightarrow\mathrm{Gal}(L_i/\mathbb{Q})\longrightarrow\mathrm{PGL}_2(\mathbb{F}_\ell)\longrightarrow 1.$$

If $\gamma=\mathrm{Res}\,\beta\in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2^i\mathbb{Z}\big)$ were trivial, then $\beta=\mathrm{Infl}\,\alpha$ would be the inflation of some $\alpha\in H^2\big(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2^i\mathbb{Z}\big)$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic to the fibred product (a.k.a. pullback) $G_\alpha\underset{\mathbb{Z}/2\mathbb{Z}}{\times}\mathrm{PGL}_2(\mathbb{F}_\ell)$, where G_α is the group extension

$$0\longrightarrow\mathbb{Z}/2^i\mathbb{Z}\longrightarrow G_\alpha\longrightarrow\mathbb{Z}/2\mathbb{Z}\longrightarrow 0$$

corresponding to α. Actually, if $i\geqslant 3$, then $\beta=\mathrm{Infl}\,\alpha$ would be trivial since $H^2\big(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2^i\mathbb{Z}\big)=0$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic to the semi-direct product

$$\mathbb{Z}/2^i\mathbb{Z}\rtimes\mathrm{PGL}_2(\mathbb{F}_\ell),$$

whereas if $i=2$, then $H^2\big(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2^i\mathbb{Z}\big)\simeq\mathbb{Z}/2\mathbb{Z}$, so that $\mathrm{Gal}(L_2/\mathbb{Q})$ would be isomorphic either to $\mathbb{Z}/4\mathbb{Z}\rtimes\mathrm{PGL}_2(\mathbb{F}_\ell)$ or to $Q_8\underset{\mathbb{Z}/2\mathbb{Z}}{\times}\mathrm{PGL}_2(\mathbb{F}_\ell)$, where Q_8, the quaternionic group $\{\pm1,\pm i,\pm j,\pm k\}$, is the extension

$$0\longrightarrow\mathbb{Z}/4\mathbb{Z}\longrightarrow Q_8\longrightarrow\mathbb{Z}/2\mathbb{Z}\longrightarrow 0$$

corresponding to the non-trivial element of $H^2(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/4\mathbb{Z})$. However, since the abelianisations

$$\Big(\mathbb{Z}/2^i\mathbb{Z}\rtimes\mathrm{PGL}_2(\mathbb{F}_\ell)\Big)^{\mathrm{ab}}\simeq\mathbb{Z}/2^{i-1}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

and

$$\big(Q_8\underset{\mathbb{Z}/2\mathbb{Z}}{\times}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

have 2-rank 2, this is impossible, since L_i ramifies only at ℓ by (A1) and there is only one quadratic number field which ramifies only at ℓ, namely $\mathbb{Q}(\sqrt{\ell^*})$.

It follows that $\gamma=\mathrm{Res}\,\beta\in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2^i\mathbb{Z}\big)$ cannot be trivial, so it must be $\gamma_{\mathrm{SL}_2}\in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell),\mathbb{Z}/2\mathbb{Z}\big)$ followed by the embedding of $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}/2^i\mathbb{Z}$. Let $g=\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]\in\mathrm{PGL}_2(\mathbb{F}_\ell)$. As $\ell\equiv 1\bmod 4$, g lies in $\mathrm{PSL}_2(\mathbb{F}_\ell)$, and since the only element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$, g cannot be lifted to an element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that $\gamma_{\mathrm{SL}_2}(g,g)\neq 0$ by example C.2.2.2. On the other hand, since g is the image of the complex conjugation (with respect to some embedding of L_0 into $\mathbb{C}$) by the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, it must lift to an element of order 2 of $\mathrm{Gal}(L_i/\mathbb{Q})$, which is contradictory: in the extension $\mathrm{Gal}(L_i/\mathbb{Q})$, seen as the set $\mathbb{Z}/2^i\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$ endowed with the group law

$$(x_1,g_1)\cdot(x_2,g_2)=\big(x_1+g_1\cdot x_2+\beta(g_1,g_2),g_1g_2\big),$$

one computes that

$$(x,g)\cdot(x,g) = \big(x + g\cdot x + \beta(g,g), g^2\big) = \big(\beta(g,g), 1\big)$$

as $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, so $\beta(g,g)$ must be zero, but $\beta(g,g) = \gamma_{\mathrm{SL}_2}(g,g) \neq 0$ since $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$.

It is therefore impossible that the extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

be not central, which completes the induction.

In particular, $\mathrm{Gal}(L_r/\mathbb{Q})$ is a central extension of $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathrm{Gal}(L_r/L_0) \simeq \mathbb{Z}/2^r\mathbb{Z}$, so that it is isomorphic either to $\mathbb{Z}/2^r\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^r_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^r_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ by theorem C.2.2.4(ii). Let L_r^{ab} be the maximal subfield of L_r which is abelian over $\mathbb{Q}$. Then its Galois group is the abelianised of $\mathrm{Gal}(L_r/\mathbb{Q})$, which is thus respectively isomorphic to $\mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2^{r+1}\mathbb{Z}$, $\mathbb{Z}/2^{r-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2^r\mathbb{Z}$ by theorem C.2.2.4(iv). This allows to exclude $\mathbb{Z}/2^r\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^r_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ since L_r, which ramifies only at ℓ by (A1), can only have one quadratic subfield, namely $\mathbb{Q}(\sqrt{\ell^*})$. Furthermore, since L_r^{ab} is abelian and ramifies only at ℓ, it is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$, so that its Galois group $\mathrm{Gal}(L_r/\mathbb{Q})^{\mathrm{ab}}$ is a quotient of

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right) \simeq \mathbb{Z}_\ell^* \simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}_\ell.$$

In particular, this quotient cannot be isomorphic to $\mathbb{Z}/2^{r+1}\mathbb{Z}$ since $\ell - 1 = 2^r m$, m odd, so $\mathrm{Gal}(L_r/\mathbb{Q})$ cannot be isomorphic to $2^r_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$ either. It must therefore be isomorphic to $2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell)$. Besides, the same reasoning applies to the number field cut out by the quotient Galois representation $\rho_{f,\mathfrak{l}}^{S_r}$, whose Galois group is isomorphic to the image of $\rho_{f,\mathfrak{l}}^{S_r}$, which is the whole of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ since the determinant of $\rho_{f,\mathfrak{l}}$ is an odd power of the mod ℓ cyclotomic character. Therefore, $\mathrm{Gal}(L_r/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$.

Remark C.2.2.7. From there, one can go back down the quadratic tower $L_r/\cdots/L_0$ and see that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. Besides, it is easy to see that the abelianised of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ is $\mathbb{F}_\ell^*/S_i^2$, the projection being induced by the determinant. Since $S_i^2 = S_{i+1} \subsetneq S_i$ for $i < r$ whereas $S_r^2 = S_r$ as $-1 \notin S_r$, theorem C.2.2.4(iv) leads to the unified formula

$$\mathrm{Gal}(L_i/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \simeq \begin{cases} \mathrm{PGL}_2(\mathbb{F}_\ell), & i = 0, \\ 2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell), & 0 < i < r, \\ 2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell), & i = r, \end{cases}$$

which is valid for $\ell \equiv 1 \bmod 4$ and for $\ell \equiv -1 \bmod 4$ as well, and which allows to identify for each i the extension $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ amongst the ones listed in theorem C.2.2.4(ii).

It follows that there exists a quotient Galois representation

$$\rho^{S_r} : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(L_r/\mathbb{Q}) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_\ell)/S_r$$

which cuts out the field L_r and whose projectivisation

$$G_{\mathbb{Q}} \xrightarrow{\rho^{S_r}} \mathrm{GL}_2(\mathbb{F}_\ell)/S_r \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$$

is isomorphic to $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$. This representation ρ^{S_r} is therefore a twist $\rho_{f,\mathfrak{l}}^{S_r} \otimes \psi$ of $\rho_{f,\mathfrak{l}}^{S_r}$ by a Galois character

$$\psi\colon G_{\mathbb{Q}} \longrightarrow \mathbb{F}_\ell^*/S_r.$$

The number field cut out by ψ is abelian and, since it is contained in L_r, it ramifies only at ℓ by (A1), so it is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$. Besides, its Galois group is isomorphic to the image of ψ, whose order is prime to ℓ, so that this field is a subfield of $\mathbb{Q}(\mu_\ell)$, which is also contained L_r^{ab}. Since $\mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right) \simeq \mathbb{Z}/(\ell-1)\mathbb{Z}$ is cyclic and since the order of $\mathrm{Im}\,\psi \subset \mathbb{F}_\ell^*/S_r$ divides the order of $\mathrm{Gal}(L_r^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{F}_\ell^*/S_r$, the number field cut out by ψ is contained in L_r^{ab}. The kernel of the quotient representation $\rho \sim \rho_{f,\mathfrak{l}}^{S_r} \otimes \psi$ therefore agrees with the kernel of $\rho_{f,\mathfrak{l}}^{S_r}$, which completes the proof of the fact that the decomposition field of the polynomial $F_r(X)$ computed by my algorithm is the number field cut out by $\rho_{f,\mathfrak{l}}^{S_r}$.

Remark C.2.2.8. Since the linear Galois representation $\rho_{f,\mathfrak{l}}$ can be recovered from the quotient Galois representation $\rho_{f,\mathfrak{l}}^{S_r}$ and the mod ℓ cyclotomic character $\overline{\chi}_\ell$ as

$$\rho_{f,\mathfrak{l}}\colon G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}^{S_r} \times \overline{\chi}_\ell^{k-1}} \mathrm{GL}_2(\mathbb{F}_\ell)/S_r \times \mathbb{F}_\ell^* \xrightarrow{\phi^{-1}} \mathrm{GL}_2(\mathbb{F}_\ell)$$

where

$$\begin{array}{rccc} \phi\colon & \mathrm{GL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S \times \mathbb{F}_\ell^* \\ & g & \longmapsto & \big(\pi(g), \det(g)\big) \end{array}$$

(cf. section B.3.5.1), the number field L cut out by the linear representation $\rho_{f,\mathfrak{l}}$ is the compositum of the number field L_r cut out by $\rho_{f,\mathfrak{l}}^{S_r}$ and of the number field $E \subseteq \mathbb{Q}(\mu_\ell)$ cut out by $\overline{\chi}_\ell^{k-1}$. This yields an easy method to compute a nice monic polynomial in $\mathbb{Z}[X]$ whose decomposition field is L: using [Pari/GP], first compute a polynomial defining the subcyclotomic field E by using the `polsubcyclo` function, then apply the `polcompositum` function to $F_r(X)$ and to this polynomial.

This is useful since the polynomial $F(X)$ computed by my algorithm is usually too big to be reduced, even by the methods presented in section B.3.5.2.

Bibliography

[Abr96] Abramovich, Dan, **A linear lower bound on the gonality of modular curves**. Internat. Math. Res. Notices 1996, no. 20, 1005–1011.

[AG90] Allgower, Eugene L.; Georg, Kurt, **Introduction to numerical continuation methods**. Reprint of the 1990 edition [Springer-Verlag, Berlin; MR1059455 (92a:65165)]. Classics in Applied Mathematics, 45. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2003. xxvi+388 pp. ISBN:0-89871-544-X.

[Asa76] Asai, Tetsuya, **On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution**. J. Math. Soc. Japan 28 (1976), no. 1, pp. 48–61.

[AL78] Atkin, A. O. L.; Li, Wen Ch'ing Winnie, **Twists of newforms and pseudo-eigenvalues of W-operators**. Invent. Math. 48 (1978), no. 3, 221–243.

[BS14] Belabas, Karim; Simon, Denis, **Ideal power detection over number fields**. In preparation. Personal communication.

[Bos07] Bosman, Johan, **On the computation of Galois representations associated to level one modular forms**. arXiv:0710.1237

[Bos89] Bost, Jean-Benoît, **Introduction to compact Riemann surfaces, Jacobians, and abelian varieties**. In **From number theory to physics** (Les Houches, 1989), pp. 64–211, Springer, Berlin, 1992.

[BFSS06] Bostan, Alin; Flajolet, Philippe; Salvy, Bruno; Schost, Éric, **Fast computation of special resultants**. Journal of Symbolic Computation 41, 1 (2006), pp. 1–29.

[Coh93] Cohen, Henri, **A course in computational algebraic number theory**. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993. xii+534 pp. ISBN: 3-540-55640-0.

[CE11] **Computational aspects of modular forms and Galois representations**. Edited by Bas Edixhoven and Jean-Marc Couveignes, with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.

[Cre92] Cremona, John E., **Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction**. Math. Proc. Cambridge Philos. Soc. 111 (1992), no. 2, pp. 199–218.

[Cre97] Cremona, John E., **Algorithms for modular elliptic curves**. Second edition. Cambridge University Press, Cambridge, 1997. vi+376 pp. ISBN : 0-521-59820-6.

[DDT95] Darmon, Henri; Diamond, Fred; Taylor, Richard, **Fermat's last theorem**. Current developments in mathematics, 1995 (Cambridge, MA), pp. 1–154, Int. Press, Cambridge, MA, 1994.

[Del71] Deligne, Pierre, **Formes modulaires et représentations l-adiques**. Séminaire Bourbaki vol. 1968/69 Exposés 347–363, Lecture Notes in Mathematics, 179, Berlin, New York, Springer-Verlag, ISBN : 978-3-540-05356-9.

[Del74] Deligne, Pierre, **La conjecture de Weil I**. Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), pp. 273–307.

[Del80] Deligne, Pierre, **La conjecture de Weil II**. Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), pp. 137–252.

[Dem97] Demmel, James W., **Applied numerical algebra**. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1997. xii+419 pp. ISBN: 0-89871-389-7.

[DvHZ14] Maarten Derickx, Mark van Hoeij, Jinxiang Zeng, **Computing Galois representations and equations for modular curves $X_H(\ell)$**. Version 2 of the arXiv.org preprint `http://arxiv.org/abs/1312.6819`.

[DS05] Diamond, Fred; Shurman, Jerry, **A first course in modular forms**. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. ISBN: 0-387-23229-X.

[Dok10] Dokchitser, Tim and Vladimir, **Identifying Frobenius elements in Galois groups**. September 2010 preprint, to appear in Algebra and Number Theory.

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

[FW02] Farmer, D. W.; James, K., **The irreducibility of some level 1 Hecke polynomials**. Mathematics of Computation, Vol. 71, No. 239 (Jul., 2002), pp. 1263–1270.

[Fly90] Flynn, E. V., **The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field**. Math. Proc. Camb. Phil. Soc. 107 (1990), 425–441.

[GG99] von zur Gathen, Joachim; Gerhard, Jürgen, **Modern computer algebra**. Cambridge University Press, New York, 1999. xiv+753 pp. ISBN: 0-521-64176-4.

[GH78] Griffiths, Phillip; Harris, Joseph, **Principles of algebraic geometry**. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York, 1978. xii+813 pp. ISBN: 0-471-32792-1.

[Gro90] Gross, Benedict H., **A tameness criterion for Galois representations associated to modular forms (mod p)**. Duke Math. J. 61 (1990), no. 2, 445–517.

[Hab83] Haberland, Klaus, **Perioden von Modulformen einer Variabler und Gruppencohomologie III**. Math. Nachr. 112 (1983), pp. 297–315.

[HW08] Hardy, G. H.; Wright, E. M., **An introduction to the theory of numbers**. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp. ISBN: 978-0-19-921986-5.

[Har77] Hartshorne, Robin, **Algebraic geometry**. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN: 0-387-90244-9.

[HS00] Hindry, Marc; Silverman, Joseph H., **Diophantine geometry - An introduction**. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1.

[Igu59] Igusa, Jun-ichi, **Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves.** Amer. J. Math. 81 1959 pp. 453–476.

[Kar87] Karpilovsky, Gregory, **The Schur multiplier**. London Mathematical Society Monographs. New Series, 2. The Clarendon Press, Oxford University Press, New York, 1987. x+302 pp. ISBN: 0-19-853554-6.

[KW09] Khare, Chandrashekhar; Wintenberger, Jean-Pierre, **Serre's modularity conjecture (I and II)**. Inventiones Mathematicae 178 (3), pp. 485–504 and 505–586.

[KM04] Khuri-Makdisi, Kamal, **Linear algebra algorithms for divisors on an algebraic curve**. Math. Comp. 73 (2004), no. 245, 333–357.

[KM07] Khuri-Makdisi, Kamal, **Asymptotically fast group operations on Jacobians of general curves**. Math. Comp. 76 (2007), no. 260, 2213–2239.

[Lan95] Lang, Serge, **Introduction to modular forms**. Grundlehren der Mathematischen Wissenschaften, 222. Springer-Verlag, Berlin, 1995. x+261 pp. ISBN: 3-540-07833-9.

[Lan02] Lang, Serge, **Algebra**. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X.

[Liu02] Liu, Qing, **Algebraic geometry and arithmetic curves**. Translated from the French by Reinie Erné. Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002. xvi+576 pp. ISBN: 0-19-850284-2.

[Man72] Manin, Ju. I., **Parabolic points and zeta functions of modular curves**. Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), pp. 19–66.

[Maz78] Mazur, Barry, **Rational isogenies of prime degree**. Invent. Math. 44 (1978), no. 2, pp. 129–162.

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

[Mil12] Milne, James S., **Jacobian varieties**. `www.jmilne.org/math/xnotes/JVs.pdf`

[MT03] Moon, Hyunsuk; Taguchi, Yuichiro, **Refinement of Tates discriminant bound and non-existence theorems for mod p Galois representations**. Doc. Math. Extra Vol. (2003), 641–654.

[Pari/GP] **PARI/GP**, version 2.6.0. `http://pari.math.u-bordeaux.fr/`

[Que95] Quer, Jordi, **Liftings of projective 2-dimensional Galois representations and embedding problems**. Journal of Algebra, volume 171, issue 2, 15 January 1995, pp. 541–566.

[RW14] Rebolledo, Marusia; Wuthrich, Christian, **A moduli interpretation for the non-split Cartan modular curve**. arXiv preprint available at `http://arxiv.org/abs/1402.3498`.

[SAGE] **SAGE mathematics software**, version 5.3. `http://sagemath.org/`

[Sch95] Schoof, René, **Counting points on elliptic curves over finite fields**. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). J. Théor. Nombres Bordeaux 7 (1995), no. 1, 219–254.

[Ser62] Serre, Jean-Pierre, **Corps locaux**. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII Actualités Sci. Indust., No. 1296. Hermann, Paris 1962 243 pp. English translation available as [Ser62en].

[Ser62en] Serre, Jean-Pierre, **Local fields**. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. viii+241 pp. ISBN: 0-387-90424-7.

[Ser69] Serre, Jean-Pierre, **Une interprétation des congruences relatives à la fonction τ de Ramanujan**. 1969 Séminaire Delange-Pisot-Poitou: 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14 17 pp. Secrétariat mathématique, Paris.

[Ser70] Serre, Jean-Pierre, **Cours d'arithmétique**. Collection SUP: "Le Mathématicien", Presses Universitaires de France, Paris 1970. 188 pp. English translation available as [Ser70en].

[Ser70en] Serre, Jean-Pierre, **A course in arithmetic**. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. viii+115 pp.

[Ser72] Serre, Jean-Pierre, **Propriétés galoisiennes des points d'ordre fini des courbes elliptiques**. Invent. Math. 15 (1972), no. 4, 259–331.

[Ser73] Serre, Jean-Pierre, **Congruences et formes modulaires** [d'après H. P. F. Swinnerton-Dyer]. Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, pp. 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[Ser74] Serre, Jean-Pierre, **Divisibilité des coefficients des formes modulaires de poids entier**. C. R. Acad. Sci. Paris Sér. A 279 (1974), pp. 679–682.

[Ser87] Serre, Jean-Pierre, **Sur les représentations modulaires de degré 2 de** $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. 54 (1987), no. 1, 179–230.

[Shi71] Shimura, Goro, **Introduction to the arithmetic theory of automorphic functions**. Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. xiv+267 pp.

[Sop10] Soprounov, Ivan, **A short proof of the Prime Number Theorem for arithmetic progressions**. 2010 preprint available at http://academic.csuohio.edu/soprunov_i/pdf/primes.pdf

[Ste07] Stein, William, **Modular forms, a computational approach**. With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007. xvi+268 pp. ISBN: 978-0-8218-3960-7; 0-8218-3960-8.

[Stu87] Sturm, Jacob, **On the congruence of modular forms**. Number theory (New York, 1984–1985), pp. 275–280, Lecture Notes in Math., 1240, Springer, Berlin, 1987.

[Swi72] Swinnerton-Dyer, H. P. F., **On ℓ-adic representations and congruences for coefficients of modular forms**. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[Wei49] Weil, André, **Numbers of solutions of equations in finite fields**. Bull. Amer. Math. Soc. 55, (1949). pp. 497–508.

[Wei03] Weintraub, Steven H, **Representation theory of finite groups: algebra and arithmetic**. Graduate Studies in Mathematics, 59. American Mathematical Society, 2003. 212 pp. ISBN: 978-0-8218-3222-6; 0-8218-3222-0.

[ZJ13] Zeng, Jinxiang; Yin, Linsheng, **On the computation of coefficients of modular forms: the reduction modulo p approach**. arXiv:1211.1124

Résumé

J.-P. Serre a conjecturé à la fin des années 60 et P. Deligne a prouvé au début des années 70 que pour toute newform $f = q + \sum_{n\geqslant 2} a_n q^n \in S_k(N,\varepsilon)$, $k \geqslant 2$, et tout premier $\mathfrak{l}$ du corps de nombres $K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$, il existe une représentation galoisienne $\mathfrak{l}$-adique $\rho_{f,\mathfrak{l}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$ qui est non-ramifiée en dehors de ℓN et telle que le polynôme caractéristique du Frobenius en $p \nmid \ell N$ est $X^2 - a_p X + \varepsilon(p)p^{k-1}$. Après réduction modulo $\mathfrak{l}$ et semi-simplification, on obtient une représentation galoisienne $\overline{\rho}_{f,\mathfrak{l}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$ modulo $\mathfrak{l}$, non-ramifiée en dehors de ℓN et telle que le polynôme caractéristique du Frobenius en $p \nmid \ell N$ est $X^2 - a_p X + \varepsilon(p)p^{k-1} \bmod \mathfrak{l}$, d'où un moyen de calcul rapide de $a_p \bmod \mathfrak{l}$ pour p gigantesque.

L'objet de cette thèse est l'étude et l'implémentation d'un algorithme reposant sur cette idée (initialement due à J.-M. Couveignes and B. Edixhoven), qui calcule les coefficients a_p modulo $\mathfrak{l}$ en calculant d'abord cette représentation modulo $\mathfrak{l}$, en s'appuyant sur le fait que pour $k < \ell$, cette représentation est réalisée dans la ℓ-torsion de la jacobienne de la courbe modulaire $X_1(\ell N)$.

Grâce à plusieurs améliorations, telles que l'utilisation des méthodes de K. Khuri-Makdisi pour calculer dans la jacobienne modulaire $J_1(\ell N)$ ou la construction d'une fonction $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$ au bon comportement arithmétique, cet algorithme est très efficace, ainsi qu'illustré par des tables de coefficients. Cette thèse se conclut par la présentation d'une méthode permettant de prouver formellement que les résultats de ces calculs sont corrects.

Mots clés: Formes modulaires, représentations galoisiennes, conjecture de modularité de Serre, jacobiennes modulaires, algorithme rapide.

Summary

It was conjectured in the late 60's by J.-P. Serre and proved in the early 70's by P. Deligne that to each newform $f = q + \sum_{n\geqslant 2} a_n q^n \in S_k(N,\varepsilon)$, $k \geqslant 2$, and each prime $\mathfrak{l}$ of the number field $K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$, is attached an $\mathfrak{l}$-adic Galois representation $\rho_{f,\mathfrak{l}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$, which is unramified outside ℓN and such the characteristic polynomial of the Frobenius element at $p \nmid \ell N$ is $X^2 - a_p X + \varepsilon(p)p^{k-1}$. Reducing modulo $\mathfrak{l}$ and semi-simplifying, one gets a mod $\mathfrak{l}$ Galois representation $\overline{\rho}_{f,\mathfrak{l}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$, which is unramified outside ℓN and such that the characteristic polynomial of the Frobenius element at $p \nmid \ell N$ is $X^2 - a_p X + \varepsilon(p)p^{k-1} \bmod \mathfrak{l}$. In particular, its trace is $a_p \bmod \mathfrak{l}$, which gives a quick way to compute $a_p \bmod \mathfrak{l}$ for huge p.

The goal of this thesis is to study and implement an algorithm based on this idea (originally due to J.-M. Couveignes and B. Edixhoven) which computes the coefficients a_p modulo $\mathfrak{l}$ by computing the mod $\mathfrak{l}$ Galois representation first, relying on the fact that if $k < \ell$, this representation shows up in the ℓ-torsion of the jacobian of the modular curve $X_1(\ell N)$.

Thanks to several improvements, such as the use of K. Khuri-Makdisi's methods to compute in the modular Jacobian $J_1(\ell N)$ or the construction of an arithmetically well-behaved function $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$, this algorithm performs very well, as illustrated by tables of coefficients. This thesis ends by the presentation of a method to formally prove that the output of the algorithm is correct.

Key words: Modular forms, Galois representations, Serre's modularity conjecture, modular jacobians, fast algorithm.