Université de Bordeaux
École doctorale mathématiques et informatique

Habilitation à diriger des recherches

Spécialité : mathématiques pures

Hecke operators in algorithmic number theory

Aurel PAGE

Soutenance publique le 3 juin 2025 devant le jury :

Cécile Armana	Univ. M. et L. Pasteur	Examinatrice
Christine Bachoc	Univ. de Bordeaux	Examinatrice
Wouter Castryck	KU Leuven	Examinateur
Tim Dokchitser	Univ. of Bristol	Rapporteur
David Kohel	Aix-Marseille Univ.	Rapporteur
John Voight	Univ. of Sydney	Rapporteur

στην Νεφέλη, τον Μηνά, και τον Φοίβο

Contents

Foreword

This HDR manuscript presents my research work since the end of my PhD, as well as some work that my PhD students Jean Kieffer and Fabrice Étienne did under my supervision. This is an exposition of results: the proofs are sketched or omitted, as all the details are contained in the full articles. In order to give (perhaps artificially) some coherence to the document, I chose Hecke operators as a theme for the manuscript, since they arise in several different forms in my research work. This means that some of my papers are not presented or only briefly mentioned, since they did not really fit that theme. I hope the coauthors of those papers will forgive me for not presenting the beautiful mathematics we did together!

Acknowledgements

I would like to thank all my coauthors for the great joy and excitement that doing mathematics together has brought me. I also thank my PhD students for trusting me with their supervision, and for the many enriching conversations we had. I feel grateful towards everyone that supported me during all those years, especially John Cremona who hired me as a postdoc, and Nicolas Bergeron who was very generous with his advice and always showed strong support; he is dearly missed.

I would like to thank Bill Allombert, Karim Belabas and Henri Cohen, for introducing me to the wonderful Pari/GP software a long time ago, for the many rich discussions on its development, and now for trusting me with part of the responsibility of taking care of it.

The research presented in this manuscript was done first at the Mathematics Department of the University of Warwick until August 2017, and then in the Inria teams Lfant and Canari at the Insitut de Mathématiques de Bordeaux. I would like to thank these institutions for providing a great research environment, and all the colleagues with whom I had many friendly discussions, mathematical or otherwise.

I would like to express my gratitude towards Tim Dokchitser, David Kohel and John Voight for agreeing to write a report on this manuscript, as well as Cécile Armana, Christine Bachoc and Wouter Castryck, for accepting to be part of my jury, all on rather short notice.

Et finalement, un grand merci à mes amis et à ma famille!

Part 1

Introduction

Notations and conventions

The cardinality of a finite set X will be written $\#X$. For p a prime number, we will write $\mathbb{Z}_p$ the ring of p-adic integers and $\mathbb{Z}_{(p)}$ the localisation of $\mathbb{Z}$ at p. When G is a group and $X \subset G$, we denote $\langle X \rangle$ the subgroup generated by X. Rings are assumed to be associative but not necessarily commutative. Let R be a ring. When W is an R-module and $X \subset W$, we denote $\langle X \rangle_R$ the sub-R-module generated by X. All R-modules are assumed to be finitely generated unless specified otherwise. When f, g are positive functions, we will use the big O notation $f = O(g)$ and we will write $f = \tilde{O}(g)$ for $f = g \cdot (\log(2+g)^{O(1)})$.

1. A short history of Hecke operators

In 1916, Ramanujan [Ram16] considered the following series

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

After computing the values of $\tau(n)$ for $1 \leq n \leq 30$, he proposed the following conjecture[1]:

$$\tau(mn) = \tau(m)\tau(n) \text{ whenever } \gcd(m, n) = 1 \tag{1.1}$$

and

$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}) \tag{1.2}$$

for every prime number p and every $r \geq 1$.

In 1917, this conjecture was proved by Mordell [Mor17], using the *modularity* property of Δ: for $z \in \mathbb{C}$ with $\mathrm{Im}(z) > 0$, let $\Delta(z)$ denote the sum of the series above where $q = \exp(2\pi i z)$; then we have

$$\Delta(z+1) = \Delta(z) \text{ and } \Delta(-1/z) = z^{12}\Delta(z). \tag{1.3}$$

In fact, he works with a slightly different form of the Δ function, namely

$$f(\omega_1, \omega_2) = \Big(\frac{2\pi}{\omega_2}\Big)^{12} \Delta\Big(\frac{\omega_1}{\omega_2}\Big)$$

where $\omega_1, \omega_2 \in \mathbb{C}$ satisfy $\mathrm{Im}(\omega_1/\omega_2) > 0$, where the modularity property now becomes invariance under every change of basis

$$(\omega_1, \omega_2) \mapsto (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$$

for every $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$. For every prime number p, Mordell introduces a new function

$$\varphi(\omega_1, \omega_2) = f(p\omega_1, \omega_2) + f(\omega_1, p\omega_2) + \cdots + f(\omega_1 + (p-1)\omega_2, p\omega_2)$$

where he calls the changes of variables "the reduced substitutions of order p", i.e. the changes of basis by the matrices

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \dots \begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix},$$

[1] He also conjectured the famous and much more difficult bound $\tau(p)^2 \leq 4p^{11}$.

which we would now call the matrices of determinant p in Hermite normal form [Her51, Section II.]. He writes that it is a well-known fact that φ is again modular, citing Hurwitz and Weber. He then shows that this implies that φ is a scalar multiple of f, i.e.

$$\varphi = Qf$$

for some $Q \in \mathbb{C}$. Finally, he proves Ramanujan's conjecture using this property for various p. He saw the potential for generalisation of the method but dismissed it, writing "We should however have to consider now invariants of a sub-group of the modular group, and it seems hardly worth while to go into details." Mordell's paper does not seem to have attracted much attention for the next 20 years.

In 1937, Hecke [Hec37a,Hec37b] introduced a general method to prove properties similar to (1.1) and (1.2) for certain modular forms F (i.e. functions satisfying a generalisation of (1.3), where 12 is replaced by an integer k called the weight). For every integer n, Hecke defines an operator T_n by[2]

$$F|T_n = n^{k-1} \sum_{\substack{a\cdot d=n \\ b \bmod d, d>0}} F\Big(\frac{az+b}{d}\Big) d^{-k},$$

also writing them as coming from the action of the matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ of determinant n and covering all classes up to left multiplication by $\mathrm{SL}_2(\mathbb{Z})$ exactly once, and emphasising the role of the finitely many cosets of the subgroup $\mathrm{SL}_2(\mathbb{Z}) \cap M\,\mathrm{SL}_2(\mathbb{Z})M^{-1}$ in $\mathrm{SL}_2(\mathbb{Z})$ where $M = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$. He shows that $F|T_n$ is again a modular form, and he proves a general identity satisfied by his operators[3]:

$$T(n)T(m) = \sum_{d|n,m} T\Big(\frac{nm}{d^2}\Big) d^{k-1}.$$

From the commutativity of his operators, he deduces that they admit a basis of common eigenvectors F and that for such forms, which satsify $F|T_n = c_n F$ for some $c_n \in \mathbb{C}$, the eigenvalues c_n satisfy identities similar to (1.1) and (1.2). We immediately see that Hecke's method is a general version of Mordell's argument. However, after noting that his results imply Ramanujan's conjecture as a special case, he writes "Dieses Resultat ist für Δ von Ramanujan empirisch vermutet und, wie ich inzwischen festgestellt habe, im Jahre 1917 von Herrn Mordell bewiesen worden." i.e. "This result was empirically conjectured for Δ by Ramanujan and, as I have discovered in the meantime, was proved by Mordell in 1917". It therefore seems that Hecke was not aware of Mordell's paper before his own work.

[2]We restrict to level 1 for simplicity.

[3]The change of notation from T_n to $T(n)$ is Hecke's.

In 1959, Shimura [Shi59, §7], who was studying discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$ more general than $\mathrm{SL}_2(\mathbb{Z})$, introduces a new abstract construction, for which he credits "une idée de A. Weil". Starting from an arbitrary group $\mathfrak{G}$ and a subgroup G, he defines

$$\tilde{G} = \{\rho \in \mathfrak{G} \mid G \cap \rho^{-1}G\rho \text{ has finite index both in } G \text{ and in } \rho^{-1}G\rho\},$$

which is a subgroup of $\mathfrak{G}$ containing G, which we would now call the commensurator of G in $\mathfrak{G}$. He then defines a ring structure on the group $\mathfrak{A}$ of finite formal linear combinations of double cosets $G\rho G$ for $\rho \in \tilde{G}$, which we would now write $\mathbb{Z}[G\backslash\tilde{G}/G]$ and call an abstract Hecke ring; he proves that his multiplication is associative by embedding $\mathfrak{A}$ into the endomorphism ring of the permutation module $\mathbb{Z}[\mathfrak{G}/G]$. Finally, he specialises to $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{R})$ and constructs actions of his algebra $\mathfrak{A}$ via what he calls *Hecke operators*, on spaces of modular forms, cohomology groups of G, and abelian varieties attached to modular curves. Although he does not write it explicitly, it is very clear that he had in mind Hecke's operators T_n for $\rho = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$; however he does not refer to commutativity properties. The structure of some abstract Hecke rings was investigated by Iwahori [Iwa64], who emphasised the relation to endomorphisms of permutation modules, expressed as induced from the trivial representation. Iwahori writes that this relation "seems to be well-known". He was right: in 1951 Mackey [Mac51] had already described homomorphisms between induced representations in terms of double cosets. Shimura's construction gradually percolated into group theory, and eventually appeared outside of a number theoretic context (for example [RW70,Yos83]).

In 1960, Tamagawa [Tam60] independently introduced a topological version of Shimura's construction. Inspired by Gel'fand's theory of spherical functions [Gel50] and Selberg's work on the trace formula [Sel56], which take place in real Lie groups, he proposes the following version: starting from G a locally compact group and U a compact subgroup, he defines $L(G, U)$ to be the space of complex-valued continuous functions on G with compact support and that are bi-U-invariant. This bi-invariance is equivalent to saying that the functions are constant on double cosets UgU. However, contrary to Shimura's ring $\mathfrak{A}$ that only contains finite linear combinations of double cosets and has a unit element, Tamagawa's functions can a priori be supported on infinitely many cosets and his algebra $L(G, U)$ may not contain a unit element. He defines multiplication by convolution, making the associativity property immediate. He emphasises the importance of commutativity of his algebra $L(G, U)$ but does not refer to endomorphisms of induced representations. Tamagawa does not mention Hecke operators, but he clearly has p-adic and adélic groups in mind since he studies restricted direct products of groups and points to future applications in number theory. This is confirmed by his next paper [Tam63], where

he uses $L(G,U)$ for p-adic and adélic groups G, and explicitly refers to Hecke and Shimura. He also thanks "Professor Shimura for some valuable suggestions about" his section on Hecke algebras.

The adélic version of the Hecke algebra became a standard in automorphic forms theory in the 1960s, and was for instance used in Jacquet and Langlands's book [JL70] where they generalise Hecke's theory to arbitrary number fields. In the adélic version, the tensor product decomposition over primes of the Hecke algebra replaces Hecke's relations for coprime integers that lead to (1.1), and Satake's isomorphism [Sat62,Sat63] between the local Hecke algebra at a prime and a polynomial ring replaces Hecke's relations for prime powers that lead to (1.2).

2. Finite groups

In this section, G denotes a finite group. When R is a commutative ring, we write $R[G]$ the corresponding group ring.

2.1. Permutation modules and Hecke operators. For every G-set X and every commutative ring R we write $R[X]$ the corresponding permutation $R[G]$-module; for every $x \in X$ we write $[x]$ the corresponding element of $R[X]$.

Let U be a subgroup of G. We write

$$N_U = \sum_{u \in U} u \in \mathbb{Z}[G]$$

which is called the *norm element of* U. For every $\mathbb{Z}[G]$-module W, denote

$$W^U = \{w \in W \mid u \cdot w = w \text{ for all } u \in U\}$$

the set of U-fixed points; for every $w \in W$, we have $N_U \cdot w \in W^U$. We have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/U], W) \cong W^U$$

given by $\varphi \mapsto \varphi([1 \cdot U])$. In other words, the $\mathbb{Z}[G]$-module $\mathbb{Z}[G/U]$ represents the functor of fixed points $W \mapsto W^U$. In particular, if U' is another subgroup of G, we get an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/U], \mathbb{Z}[G/U']) \cong \mathbb{Z}[G/U']^U \cong \mathbb{Z}[U\backslash G/U'].$$

In particular, the abelian group $\mathbb{Z}[U\backslash G/U]$ inherits from from the endomorphism ring $\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/U])$ the structure of a ring called the *Hecke ring* of (G,U). More generally, for all subgroups U, U', U'' of G, we obtain a composition law

$$\mathbb{Z}[U\backslash G/U'] \otimes \mathbb{Z}[U'\backslash G/U''] \longrightarrow \mathbb{Z}[U\backslash G/U''],$$

and the elements of $\mathbb{Z}[U\backslash G/U']$ are also called *Hecke operators*. By the representability property above (or unravelling the isomorphisms

above), to every $T \in \mathbb{Z}[U\backslash G/U']$ and every $\mathbb{Z}[G]$-module W we can attach a map

$$T\colon W^{U'} \longrightarrow W^U,$$

in a way compatible with the composition laws; such maps T are also called *Hecke operators*. There is a linear map $\mathbb{Z}[U\backslash G/U'] \to \mathbb{Z}[U'\backslash G/U]$ given by $UgU' \mapsto U'g^{-1}U$, which we denote by $T \mapsto T^*$. We have $(T^*)^* = T$, and $(TT')^* = T'^*T^*$ whenever the product makes sense.

More generally, let X be a finite G-set. By decomposing X into orbits we get an isomorphism of G-sets

$$X \cong \bigsqcup_{i=1}^{n} G/U_i$$

for some subgroups U_i of G, and correspondingly an isomorphism of $\mathbb{Z}[G]$-modules

$$\mathbb{Z}[X] \cong \bigoplus_{i=1}^{n} \mathbb{Z}[G/U_i].$$

For every G-set Z (finite or infinite) we write

$$Z^X = \mathrm{Hom}_G(X, Z),$$

so that we have a bijection

$$Z^X \cong \prod_{i=1}^{n} Z^{U_i}.$$

In particular, if W is a $\mathbb{Z}[G]$-module, we have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[X], W) \cong W^X$$

given by restriction to X. If Y is another finite G-set, we also call *Hecke operator* every element $T \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[X], \mathbb{Z}[Y])$, and the induced linear map

$$T\colon W^Y \longrightarrow W^X.$$

These can be decomposed as sums of Hecke operators corresponding to double cosets of subgroups.

2.2. Brauer relations. The *Burnside group*[4] $\Omega(G)$ of G is the group of finite formal linear combinations $\sum_i a_i X_i$ of finite G-sets X_i and $a_i \in \mathbb{Z}$, modulo all relations of the form $(X \sqcup Y) - (X + Y)$ for finite G-sets X, Y and of the form $X - Y$ for isomorphic G-sets $X \cong Y$. Every element of $\Omega(G)$ can be written $X - Y$ for G-sets X and Y. When U is a subgroup of G, we also abbreviate $U \in \Omega(G)$ to mean $G/U \in \Omega(G)$.

Let R be a commutative ring, and $\Theta = X - Y \in \Omega(G)$. We say that Θ is an $R[G]$-*relation* if there is an isomorphism of $R[G]$-modules

$$R[X] \cong R[Y].$$

[4]It is in fact a ring, but we will not need this extra structure.

LEMMA 2.1. *Let $\Theta \in \Omega(G)$. Let p be a prime number that does not divide $\#G$. The following are equivalent:*

(1) *Θ is a $\mathbb{Q}[G]$-relation;*
(2) *Θ is a $\mathbb{C}[G]$-relation;*
(3) *Θ is an $\mathbb{F}_p[G]$-relation.*

When these conditions are satisfied, we also say that Θ is a *Brauer relation* [Bra51].

LEMMA 2.2. *Let $\Theta \in \Omega(G)$. Let p be a prime number. The following are equivalent:*

(1) *Θ is an $\mathbb{F}_p[G]$-relation;*
(2) *Θ is a $\mathbb{Z}_p[G]$-relation;*
(3) *Θ is a $\mathbb{Z}_{(p)}[G]$-relation.*

Let $\Theta = X - Y \in \Omega(G)$ be a Brauer relation. By definition there exist Hecke operators

$$T\colon \mathbb{Z}[X] \longrightarrow \mathbb{Z}[Y] \text{ and } T'\colon \mathbb{Z}[Y] \longrightarrow \mathbb{Z}[X]$$

and an integer $d \in \mathbb{Z}_{>0}$ such that

$$TT' = d \cdot \mathrm{Id} \text{ and } T'T = d \cdot \mathrm{Id}\,.$$

If Θ is a $\mathbb{Z}_{(p)}[G]$-relation, then we may assume that p does not divide d. If Θ is a $\mathbb{Z}[G]$-relation, then we may assume that $d = 1$.

2.3. Regulator constants. Let W be a $\mathbb{Q}[G]$-module, let $\langle \cdot, \cdot \rangle$ be a $\mathbb{Q}$-bilinear, G-invariant, non-degenerate $\mathbb{R}$-valued pairing, and let $\Theta = \sum_i n_i U_i$ be a $\mathbb{Q}[G]$-relation. The *regulator constant* of W with respect to Θ is defined to be

$$\mathcal{C}_\Theta(W) = \prod_i \det\left(\frac{1}{\#U_i}\langle \cdot, \cdot \rangle \mid W^{U_i}\right)^{n_i} \in \mathbb{R}^\times/(\mathbb{Q}^\times)^2,$$

where the determinant is computed with respect to any $\mathbb{Q}$-basis of W^{U_i}.

THEOREM 2.3 (Theorem 2.17 in [DD09]). *The value of $\mathcal{C}_\Theta(W)$ is independent of the pairing $\langle \cdot, \cdot \rangle$ and belongs to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.*

PROOF. We give our proof using Hecke operators, as in [P10, Section 2.2]. Write $\Theta = X - Y$ for G-sets X, Y, so that we have

$$\mathcal{C}_\Theta(W) = \frac{\det(\langle \cdot, \cdot \rangle_X \mid W^X)}{\det(\langle \cdot, \cdot \rangle_Y \mid W^Y)}$$

where $\langle \cdot, \cdot \rangle_X, \langle \cdot, \cdot \rangle_Y$ are given on their direct summands W^{U_i} by $\frac{1}{\#U_i}\langle \cdot, \cdot \rangle$. Let

$$T\colon \mathbb{Z}[X] \longrightarrow \mathbb{Z}[Y]$$

be a Hecke operator that is invertible over $\mathbb{Q}$. We obtain two isomorphisms of vector spaces

$$T\colon W^Y \to W^X \text{ and } T^*\colon W^X \to W^Y.$$

Moreover, T and T^* are adjoint with respect to $\langle\cdot,\cdot\rangle_X$ and $\langle\cdot,\cdot\rangle_Y$. In other words, we have a commutative diagram

$$\begin{array}{ccc} W^Y \otimes \mathbb{R} & \xrightarrow{T} & W^X \otimes \mathbb{R} \\ {\scriptstyle \langle\cdot,\cdot\rangle_Y}\downarrow & & \downarrow{\scriptstyle \langle\cdot,\cdot\rangle_X} \\ \mathrm{Hom}(W^Y, \mathbb{R}) & \xrightarrow{T^*} & \mathrm{Hom}(W^X, \mathbb{R}). \end{array}$$

Fixing $\mathbb{Q}$-bases of W^X and W^Y, we obtain

$$\frac{\det(\langle\cdot,\cdot\rangle_X)}{\det(\langle\cdot,\cdot\rangle_Y)} = \frac{\det T^*}{\det T}. \tag{2.1}$$

The left hand side is $\mathcal{C}_\Theta(W)$, and the right hand side does not depend on $\langle\cdot,\cdot\rangle$ and is visibly rational, proving the result. □

2.4. Galois theory. An *étale F-algebra* is a finite product of finite separable extensions of F. We recall Galois theory for étale algebras. Let $\widetilde{F}/F$ be a Galois extension with Galois group G. For every finite G-set X there is a ring structure on $\widetilde{F}^X$ given by pointwise multiplication of G-equivariant maps. This induces an equivalence of categories

$$\begin{array}{rcl} \{\text{étale } F\text{-algebras}\} & \longleftrightarrow & \{\text{finite } G\text{-sets}\} \\ L & \longmapsto & \mathrm{Hom}_{F\text{-alg}}(L, \widetilde{F}) \\ \widetilde{F}^X & \longmapsfrom & X \end{array}$$

In this equivalence of categories, the decomposition as a product of fields corresponds to the decomposition of a G-set into orbits. If the étale algebras L_1, L_2 correspond to X_1, X_2 respectively, then the direct product $L_1 \times L_2$ corresponds to the disjoint union $X_1 \sqcup X_2$ and the tensor product $L_1 \otimes_F L_2$ corresponds to the product $X_1 \times X_2$.

Now assume that L_1, L_2 are fields. A *compositum* of L_1 and L_2 is a triple (C, ι_1, ι_2) where C/F is a field extension, $\iota_i \colon L_i \to C$ are F-algebra morphisms and C is generated by $\iota_1(L_1)$ and $\iota_2(L_2)$. In other words, a compositum is a field generated by L_1 and L_2 but we also record the exact maps. The compositums of L_1 and L_2 are exactly the field quotients of $L_1 \otimes_F L_2$. For $i = 1, 2$, let U_i be a subgroup of G such that G/U_i corresponds to L_i. Then the compositums of L_1 and L_2 correspond to the G-orbits on $G/U_1 \times G/U_2$, i.e. to the elements of $U_1 \backslash G / U_2$.

We will sometimes refer to infinite Galois theory. In that case, $\bar{F}$ will denote a separable closure of F and $\mathcal{G}_F = \mathrm{Gal}(\bar{F}/F)$ will be its absolute Galois group equipped with its profinite topology.

3. Algebraic number theory

3.1. Notations. Let F be a number field, i.e. a finite extension of $\mathbb{Q}$. The *signature* of F is the pair (r_1, r_2) where r_1 is the number of real embeddings of fields $F \hookrightarrow \mathbb{R}$, and r_2 is the number of conjugate

pairs of nonreal complex embeddings $F \hookrightarrow \mathbb{C}$. We write $\mathbb{Z}_F$ for the ring of integers of F and Δ_F its discriminant. Let $\mathrm{Cl}(F)$ denote the class group, $\mathrm{Reg}(F)$ the regulator, and $w(F)$ the number of roots of unity in F. We write $\mathrm{N}(\mathfrak{a}) = \#(\mathbb{Z}_F/\mathfrak{a})$ for the norm of a nonzero ideal $\mathfrak{a} \leq \mathbb{Z}_F$.

For every prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$, we write $F_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of F with ring of integers $\mathbb{Z}_\mathfrak{p}$, and $v_\mathfrak{p}\colon F_\mathfrak{p} \to \mathbb{Z} \cup \{\infty\}$ the $\mathfrak{p}$-adic valuation; let $\mathbb{F}_\mathfrak{p} = \mathbb{Z}_F/\mathfrak{p}$ denote the residue field. For every set $\mathcal{S}$ of prime ideals of $\mathbb{Z}_F$, we write

$$\mathbb{Z}_{F,\mathcal{S}} = \{x \in F \mid v_\mathfrak{p}(x) \geq 0 \text{ for every } \mathfrak{p} \notin \mathcal{S}\}$$

the ring of $\mathcal{S}$-integers in F; its unit group $\mathbb{Z}_{F,\mathcal{S}}^\times$ is called the group of $\mathcal{S}$-units of F. When $\mathcal{S} \subset \mathbb{Z}$ is a set of prime numbers, we use the shortcut $\mathbb{Z}_{F,\mathcal{S}} = \mathbb{Z}_{F,\mathcal{S}'}$ where $\mathcal{S}'$ is the set of all prime ideals of $\mathbb{Z}_F$ above the prime numbers in $\mathcal{S}$.

The Dedekind zeta function

$$\zeta(F,s) = \sum_{\mathfrak{a} \leq \mathbb{Z}_F} \mathrm{N}(\mathfrak{a})^{-s},$$

where the sum ranges over nonzero ideals of $\mathbb{Z}_F$, converges for $\mathrm{Re}(s) > 1$, admits a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$, and satisfies the functional equation

$$\Lambda(F,s) = \Lambda(F,1-s)$$

where

$$\Lambda(F,s) = |\Delta_F|^{s/2}\Gamma_\mathbb{R}(s)^{r_1}\Gamma_\mathbb{C}(s)^{r_2}\zeta(F,s)$$

and

$$\Gamma_\mathbb{R}(s) = \pi^{-s/2}\Gamma(s) \text{ and } \Gamma_\mathbb{C}(s) = \Gamma_\mathbb{R}(s)\Gamma_\mathbb{R}(s+1),$$

and the analytic class number formula

$$\mathrm{Res}_{s=1}\,\zeta(F,s) = \frac{2^{r_1}(2\pi)^{r_2}h(F)\,\mathrm{Reg}(F)}{|\Delta_F|^{1/2}w(F)},$$

or equivalently

$$\zeta(F,s) = -\frac{h(F)\,\mathrm{Reg}(F)}{w(F)}s^{r_1+r_2-1} + O(s^{r_1+r_2}) \tag{3.1}$$

as $s \to 0$.

One of the most important conjectures in number theory is the Riemann hypothesis, including its generalisations to various L-functions.

Conjecture 3.1 (Generalised Riemann hypothesis for $\zeta(F,s)$). Every zero ρ of $\zeta(F,s)$ that lies in the critical strip $0 \leq \mathrm{Re}(\rho) \leq 1$ actually lies on the vertical line $\mathrm{Re}(\rho) = \frac{1}{2}$.

We will abbreviate "generalised Riemann hypothesis" to "GRH".

We write $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $x \mapsto x^*$ its canonical involution, which is the identity on the $\mathbb{R}$ factors and complex conjugation on the $\mathbb{C}$ factors. The $\mathbb{R}$-algebra $F_{\mathbb{R}}$ has a canonical Euclidean structure given by $\langle x, y\rangle = \mathrm{Tr}_{F_{\mathbb{R}}/\mathbb{R}}(xy^*)$.

Let $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}_p$ be the profinite completion of $\mathbb{Z}$. We write $\hat{\mathbb{Z}}_F = \mathbb{Z}_F \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ and $\hat{F} = F \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \cong \prod'_{\mathfrak{p}} F_{\mathfrak{p}}$ the ring of finite adèles of F, and $\mathbb{A}_F = \hat{F} \times F_{\mathbb{R}}$ the ring of adèles of F. A *Hecke character* Ψ is a continuous character of $F^\times \backslash \mathbb{A}_F^\times$. There is an attached L-function $L(\Psi, s)$ which is conjectured to satisfy the Riemann hypothesis.

A *modulus* $\mathfrak{M}$ is a pair $(\mathfrak{M}_f, \mathfrak{M}_\infty)$ where $\mathfrak{M}_f$ is a nonzero ideal of $\mathbb{Z}_F$ and $\mathfrak{M}_\infty$ is a subset of the set of real embeddings of F. Let $U(\mathfrak{M}_f) \subset \hat{\mathbb{Z}}_F^\times$ be the open subgroup of elements congruent to $1 \bmod \mathfrak{M}_f$ and let $U(\mathfrak{M}_\infty) \subset F_{\mathbb{R}}^\times$ the subgroup of elements that are positive at all $\sigma \in \mathfrak{M}_\infty$. Then the *ray class group* $\mathrm{Cl}(F, \mathfrak{M}) = F \backslash \mathbb{A}_F^\times / U(\mathfrak{M}_f) U(\mathfrak{M}_\infty)$ is a finite group.

3.2. Computation of class groups. One of the most important problem in algorithmic number theory is the following.

Problem 3.2. Given the ring of integers $\mathbb{Z}_F$ of a number field F, compute its class group $\mathrm{Cl}(F)$ and unit group $\mathbb{Z}_F^\times$.

We add the ring of integers to the input to separate the problem of computing $\mathbb{Z}_F$, which is related to factorisation [BL94], from the one we really want to focus on. Computing the torsion subgroup of $\mathbb{Z}_F^\times$, in other words the group of roots of unity, is easy (see for instance [LS17, Proposition 3.5] for a polynomial time algorithm, see also [Mol10]).

The following algorithm, due to Buchmann [Buc90], assumes the validity of GRH for $\zeta(L, s)$ for every abelian unramified extension L/F.

Algorithm 3.3 (Buchmann). Assume GRH.

- Input: a number field F and its ring of integers $\mathbb{Z}_F$.
- Output: the structure of the class group $\mathrm{Cl}(F)$ and a basis of the unit group $\mathbb{Z}_F^\times$.

(1) Choose $X \geq 4(\log |\Delta_F|)^2$.
(2) Let $\mathcal{S}$ be the set of all prime ideals in $\mathbb{Z}_F$ of norm at most X.
(3) Compute an approximation $\widetilde{hR}$ of $h(F)\,\mathrm{Reg}(F)$ up to a factor $\sqrt{2}$.
(4) $h_0 \leftarrow \infty, R_0 \leftarrow \infty$
(5) $B \leftarrow \emptyset, B' \leftarrow \emptyset$
(6) While $h_0 R_0 > \widetilde{hR}$:
  (a) Generate random elements $x \in \mathbb{Z}_F$ until $x \in \mathbb{Z}_{F,\mathcal{S}}^\times$.
  (b) $B' \leftarrow B' \cup \{x\}$
  (c) Let $v_{\mathcal{S}} \colon \langle B' \rangle \to \mathbb{Z}^{\mathcal{S}}$ be given by $b \mapsto (v_{\mathfrak{p}}(b))_{\mathfrak{p} \in \mathcal{S}}$.

(d) $C \leftarrow \mathbb{Z}^{\mathcal{S}}/\operatorname{im}(v_{\mathcal{S}})$
(e) $B \leftarrow$ basis of $\ker(v_{\mathcal{S}})$
(f) $R_0 \leftarrow \operatorname{Reg}(B)$
(g) $h_0 \leftarrow \#C$
(7) Return C, B

The GRH is used to guarantee that the classes of primes in $\mathcal{S}$ generate $\operatorname{Cl}(F)$ and that a low-precision approximation $\widetilde{hR}$ can be computed efficiently. The correctness relies on the fact that in this case, we have

$$\operatorname{Cl}(F) \cong \mathbb{Z}^{\mathcal{S}}/v_{\mathcal{S}}(\mathbb{Z}_{F,\mathcal{S}}^{\times}).$$

There are various ways of adjusting the bound X and generating random elements to improve the probability of finding enough $\mathcal{S}$-units, but the fundamental problem is that we do not have a very good strategy for this step.

QUESTION 3.4. Can we generate "random" $\mathcal{S}$-units in F efficiently?

3.3. Selmer groups. A different class of groups that bear some resemblance with class groups are Selmer groups. They were introduced in the context of descent on elliptic curves [Sil86, Section X.4] but also play an important role in understanding special values of L-functions [Kol89,Kol90,BK90] and in the theory of deformations of Galois representations [Maz89]. They already have algorithmic applications: of course effective descent on elliptic curves [SS04] but also effective class field theory [Coh00, Section 5].

First, for L an arbitrary field with absolute Galois group $\mathcal{G}_L$ and W a $\mathbb{Z}[\mathcal{G}_L]$-module, we use the usual notation from Galois cohomology:

$$H^i(L, W) = H^i(\mathcal{G}_L, W).$$

Let W be a $\mathbb{Z}[\mathcal{G}_F]$-module.

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$, and let $F_{\mathfrak{p}}^{\mathrm{ur}}/F_{\mathfrak{p}}$ be the maximal unramified extension. Define

$$H^1_{\mathrm{ur}}(F_{\mathfrak{p}}, W) = \ker(\mathrm{Res}\colon H^1(F_{\mathfrak{p}}, W) \to H^1(F_{\mathfrak{p}}^{\mathrm{ur}}, W)).$$

A *Selmer structure* $\mathcal{F}$ is a collection $(\mathcal{F}_{\mathfrak{p}})_{\mathfrak{p}}$ indexed by prime ideals of $\mathbb{Z}_F$, where

- for every $\mathfrak{p}$, the group $\mathcal{F}_{\mathfrak{p}}$ is a subgroup of $H^1(F_{\mathfrak{p}}, W)$, and
- for all but finitely many $\mathfrak{p}$, we have $\mathcal{F}_{\mathfrak{p}} = H^1_{\mathrm{ur}}(F_{\mathfrak{p}}, W)$.

The corresponding *Selmer group* is the subgroup $H^1_{\mathcal{F}}(F, W) \subset H^1(F, W)$ of classes that land in the local subgroup $\mathcal{F}_{\mathfrak{p}}$ everywhere locally:

$$H^1_{\mathcal{F}}(F, W) = \ker\left(H^1(F, W) \to \prod_{\mathfrak{p}} \frac{H^1(F_{\mathfrak{p}}, W)}{\mathcal{F}_{\mathfrak{p}}}\right).$$

EXAMPLE 3.5. Let $n \in \mathbb{Z}_{\geq 2}$ and consider $W = \mu_n = \mu_n(\bar{F})$. For every field L, we have an isomorphism $H^1(L, \mu_n) \cong (L^{\times})/(L^{\times})^n$.

In addition, for every prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$ whose residue characteristic does not divide n, we have $H^1_{\mathrm{ur}}(F_\mathfrak{p}, \mu_n) \cong (\mathbb{Z}_\mathfrak{p}^\times)/(\mathbb{Z}_\mathfrak{p}^\times)^n$.

Define, for every prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$:

$$\mathcal{F}_\mathfrak{p} = (\mathbb{Z}_\mathfrak{p}^\times)/(\mathbb{Z}_\mathfrak{p}^\times)^n.$$

Then we get

$$H^1_\mathcal{F}(F, \mu_n) \cong \{x \in F^\times \mid v_\mathfrak{p}(x) \equiv 0 \bmod n \text{ for all } \mathfrak{p}\}/(F^\times)^n.$$

Every element of this Selmer group, seen as an element of $F^\times$, generate an ideal that is an n-th power; we therefore have a well-defined map $x \mapsto \sqrt[n]{x\mathbb{Z}_F}$, which gives an exact sequence

$$1 \to \mathbb{Z}_F^\times/(\mathbb{Z}_F^\times)^n \to H^1_\mathcal{F}(F, \mu_n) \to \mathrm{Cl}(F)[n] \to 1.$$

This is one way of seeing that Selmer groups are closely related to class groups.

Given the usefulness of Selmer groups and the fact that they are analogous to class groups, it is important to find efficient algorithms for the following generalisation of Problem 3.2.

Problem 3.6. Given a number field F, a finite $\mathcal{G}_F$-module W and a Selmer structure $\mathcal{F}$, compute $H^1_\mathcal{F}(F, W)$.

In fact, the problem is also interesting for H^2.

4. Arithmetic manifolds

4.1. Manifolds. Unless otherwise specified, by *manifold* we always mean an orientable Riemannian manifold. Similarly all our orbifolds will be orientable Riemannian (recall that an *orbifold* is defined similarly to a manifold but locally modelled on $\mathbb{R}^n/G$ where G is a finite group, see [Car19,Gor12] for general references); we will freely refer to homology, differential forms, spectrum, etc. for orbifolds. An orbifold is *closed* if it is compact without boundary. If M_1, M_2 are manifolds, we write $M_1 \# M_2$ their connected sum. We write $\mathbb{S}^n$ for the n-sphere and $\mathbb{D}^2$ for the 2-disc. We write $\mathcal{H}^n$ for the hyperbolic n-space, which is the unique simply connected manifold of constant curvature -1. A concrete model for hyperbolic 2-space is $\mathcal{H}^2 = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ with the metric $\frac{dx^2+dy^2}{y^2}$ where $\tau = x+iy \in \mathcal{H}^2$; its group of orientation-preserving isometries is $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{PGL}_2(\mathbb{R})^+$ with the action by linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + b},$$

and we have

$$\mathcal{H}^2 \cong \mathrm{PSL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \cong \mathrm{PGL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}).$$

The group of orientation-preserving isometries of $\mathcal{H}^3$ is $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{PSL}_2(\mathbb{C})$ and we have

$$\mathcal{H}^3 \cong \mathrm{PSL}_2(\mathbb{C})/\mathrm{PSU}_2(\mathbb{C}).$$

An orbifold is *hyperbolic* if it is of the form $\Gamma\backslash\mathcal{H}^n$ where Γ is a discrete subgroup of $\mathrm{Isom}(\mathcal{H}^n)$.

Let M be an orbifold. For all $i \geq 0$, the Riemannian metric induces a Euclidean norm on $H_i(M,\mathbb{R})$. The i-th *regulator* of M is

$$\mathrm{Reg}_i(M) = \mathrm{vol}\left(\frac{H_i(M,\mathbb{R})}{H_i(M,\mathbb{Z})}\right).$$

Let $d = \dim(M)$; we have $\mathrm{Reg}_i(M) = \mathrm{Reg}_{d-i}(M)^{-1}$ for all $i \geq 0$, and $\mathrm{Reg}_d(M) = \mathrm{vol}(M)^{1/2}$. See [Rai21] for a survey of regulators of hyperbolic manifolds.

4.2. Arithmetic groups and Hecke operators. Let $\mathbb{G} \subset \mathrm{GL}_n$ be a linear algebraic group over a number field F, and assume that $\mathbb{G}$ is *reductive*, i.e. it has no nontrivial connected normal unipotent subgroup. Examples include $\mathrm{GL}_n, \mathrm{SL}_n, \mathrm{Sp}_{2g}$, and $A^\times$ where A is a central simple algebra over F. Let $G = \mathbb{G}(F_\mathbb{R})$, let $K \subset G$ be a maximal compact subgroup, and let Z be the identity component of largest $\mathbb{Q}$-split torus in the center of $\mathbb{G}$. Concretely, $Z = 1$ if $\mathbb{G}$ is semisimple (e.g. $\mathrm{SL}_n, \mathrm{Sp}_{2g}$), and $Z = \mathbb{R}_{>0}$ if $\mathbb{G} = A^\times$ as above. The *symmetric space* attached to $\mathbb{G}$ is the manifold

$$\mathcal{X} = G/KZ.$$

Two subgroups Γ_1, Γ_2 of G are *commensurable* if $\Gamma_1 \cap \Gamma_2$ has finite index in both Γ_1 and Γ_2. An *arithmetic group* in G is a subgroup $\Gamma \subset G$ that is commensurable with $\mathbb{G}(\mathbb{Z}_F)$, which is defined as $\mathbb{G}(F) \cap \mathrm{GL}_n(\mathbb{Z}_F)$. Arithmetic groups are discrete subgroups of G and of G/Z. The associated *arithmetic orbifold* is the quotient

$$M = M(\Gamma) = \Gamma\backslash\mathcal{X}.$$

By a theorem of Borel and Harish-Chandra [BHC62], the orbifold M has finite volume; it is compact in the case $\mathbb{G} = D^\times$ where D is a division algebra. Let $g \in \mathbb{G}(F)$. Then the group $g\Gamma g^{-1}$ is commensurable with Γ, so we have two finite covering maps

$$\pi_1 \colon M(\Gamma \cap g^{-1}\Gamma g) \longrightarrow M(\Gamma)$$

and

$$\pi_2 \colon M(\Gamma \cap g^{-1}\Gamma g) \cong M(g\Gamma g^{-1} \cap \Gamma) \longrightarrow M(\Gamma).$$

The *Hecke operator* $T_g = \pi_2 \circ \pi_1^*$ defines a correspondence (i.e. it sends a point to a formal sum of points) $M(\Gamma) \to M(\Gamma)$ that only depends on the double coset $\Gamma g \Gamma$; in particular in acts on abelian groups functorially attached to M: homology, functions, differential forms, etc. The *degree* $\deg(T_g)$ of the Hecke operator T_g is the degree of the covering π_1.

More generally, let $U \subset \mathbb{G}(\hat{F})$ be a compact open subgroup. The associated *adélic double quotient* is

$$\mathcal{M} = \mathcal{M}(U) = \mathbb{G}(F)\backslash\mathbb{G}(\mathbb{A}_F)/UKZ.$$

The orbifold $\mathcal{M}$ can be disconnected, and it is a disjoint union of finitely many arithmetic orbifolds as above:

$$\mathcal{M}(U) = \bigsqcup_{c\in\mathbb{G}(F)\backslash\mathbb{G}(\hat{F})/U} \Gamma_c\backslash\mathcal{X},$$

where $\Gamma_c = \mathbb{G}(F) \cap cUc^{-1}$. Let $\delta \in \mathbb{G}(\hat{F})$. Then $\delta U\delta^{-1}$ is also open in $\mathbb{G}(\hat{F})$, so we have two finite covering maps

$$\pi_1 \colon \mathcal{M}(U \cap \delta^{-1}U\delta) \longrightarrow \mathcal{M}(U)$$

and

$$\pi_2 \colon \mathcal{M}(U \cap \delta^{-1}U\delta) \cong \mathcal{M}(\delta U\delta^{-1} \cap U) \longrightarrow \mathcal{M}(U).$$

The *Hecke operator* $T_\delta = \pi_2 \circ \pi_1^*$ defines a correspondence $\mathcal{M}(U) \to \mathcal{M}(U)$ that only depends on the double coset $U\delta U$. The *Hecke algebra* is the ring $\mathbb{Z}[U\backslash\mathbb{G}(\hat{F})/U]$ with a ring structure compatible with the action of Hecke operators. The *degree* $\deg(T_\delta)$ of the Hecke operator T_δ is the degree of the covering π_1. When $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}_F$ such that there is an isomorphism $\mathbb{G}(F_\mathfrak{p}) \cong \mathrm{GL}_n(F_\mathfrak{p})$, we write $T_\mathfrak{p}$ for the Hecke operator T_δ where δ has component 1 at every prime other than $\mathfrak{p}$ and $\delta_\mathfrak{p}$ is the diagonal matrix

$$\delta_\mathfrak{p} = \begin{pmatrix} \pi & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

where π is a uniformiser of $F_\mathfrak{p}$.

5. Can you hear the shape of a drum?

5.1. Original problem. In 1966, Kac [Kac66] popularised the study of isospectrality problems by asking his famous question *"Can one hear the shape of a drum?"*. The idea is that you should start with a compact domain of the plane, and construct a drum with that shape. If you hit the drum, it vibrates and produces sound: Kac's question is whether this sound determines the shape, i.e. whether it determines the plane domain up to isometry. To simplify the analysis and make the problem more mathematically natural, we only take into account the vibrating frequencies of the drum, which are completely determined by the eigenvalues of the Laplace operator

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

acting on the functions on the plane domain with boundary conditions. We will actually replace plane domains by compact Riemannian orbifolds of arbitrary dimension but without boundary. From the Riemannian metric, such an orbifold M is equipped with a Laplace operator Δ acting on the space $L^2(M)$ of functions, and in fact for every $i \geq 0$ with a Hodge–Laplace operator Δ on the space $\Omega^i(M)$ of differential i-forms, and this operator has a discrete spectrum. We then say that two orbifolds M_1 and M_2 are i-isospectral if the spectra of Δ on $\Omega^i(M_1)$ and $\Omega^i(M_2)$ agree with multiplicity. We abbreviate "0-isospectral" as "isospectral". In this context, Kac's question becomes: *are isospectral orbifolds necessarily isometric?* Then answer is easily seen to be *yes* in dimension 1, but was already known to be *no* in general by a construction of 16-dimensional flat tori by Milnor [Mil64] in 1964. A breakthrough came from Vignéras [Vig80] who gave a beautiful arithmetic construction showing that the answer is again *no* in every dimension ≥ 2. Sunada [Sun85] then proposed a flexible construction of isospectral manifolds from group theory, that was since then applied to construct a plethora of examples. Finally, Gordon, Webb and Wolpert [GWW92] managed to construct isospectral, nonisometric plane domains, settling Kac's original question. The question is still open if one restricts to plane domains with smooth boundary.

5.2. Refined questions. Despite the resolution of the initial question, there are many interesting variants and refinements, and the area has been very active since the 1980s. We present some of these questions.

First, the question has emerged of how general the constructions of Sunada and Vignéras are. To be more precise, we give the statement of Sunada's theorem.

THEOREM 5.1 (Sunada). *Let G be a finite group, let M be a manifold with a free G-action, and let U_1, U_2 be subgroups such that there is an isomorphism of $\mathbb{C}[G]$-modules*

$$\mathbb{C}[G/U_1] \cong \mathbb{C}[G/U_2]. \tag{5.1}$$

Then for all $i \geq 0$, the manifolds M/U_1 and M/U_2 are i-isospectral.

If the condition (5.1) is satisfied, we say that (G, U_1, U_2) form a *Gassmann* triple [Gaß26], a special case of Brauer relation (see Section 2.2). We can generalise this condition to infinite groups as follows.

DEFINITION 5.2. Let G be a Lie group acting on a Riemannian manifold M by isometries, and let Γ_1, Γ_2 be discrete subgroups that act properly discontinuously on M and such that $\Gamma_i \backslash M$ is compact for $i = 1, 2$. We say that Γ_1 and Γ_2 are *representation equivalent* if

there exists an isomorphism of unitary representations of G

$$L^2(\Gamma_1\backslash G) \cong L^2(\Gamma_2\backslash G)$$

DeTurck and Gordon [DG89, Theorem 1.16 and Remark 1.18] proved the following generalisation of Sunada's criterion.

THEOREM 5.3 (DeTurck–Gordon). *If Γ_1 and Γ_2 are representation equivalent, then for all $i \geq 0$, the quotients $\Gamma_1\backslash M$ and $\Gamma_2\backslash M$ are i-isospectral.*

It turns out that the examples constructed by Vignéras are in fact representation-equivalent (this makes sense as Vignéras's manifolds are arithmetic manifolds, see Sections 4.2 and 12.1), which has led Vignéras's method to be sometimes considered as a special case of Sunada's. However, we should note that while it is very easy to check whether a triple (G, U_1, U_2) is a Gassmann triple, it is often nontrivial to prove representation equivalence.

Another perspective is that representation equivalence is a very strong version of isospectrality, and from this point of view a natural follow-up question is to compare these different versions. The following question was raised by Pesce [Pes95] and Wolf [Wol01].

QUESTION 5.4. Does i-isospectrality for all $i \geq 0$ imply representation equivalence?

This open question seems especially interesting in the case of hyperbolic manifolds, being highlighted by Rajan [Raj10, § 4.1], Linowitz and Voight [LV15, Remark 2.6], and [LL24, Question 8.11]. For hyperbolic manifolds of arbitrary dimension, Pesce [Pes95] proved that a notion called *strong isospectrality* implies representation equivalence. Conversely, Question 5.4 has a positive answer for hyperbolic surfaces, and in fact Doyle and Rossetti [DR11] proved that it even holds for hyperbolic 2-orbifolds. This has led them to conjecture [DR11, § 12] that it holds for hyperbolic orbifolds of arbitrary dimension. Another variant is as follows.

QUESTION 5.5. Does i-isospectrality for some set of indices i imply j-isospectrality for another j?

Gordon [Gor86] constructed pairs of manifolds that are isospectral but not 1-isospectral. Lauret and Linowitz [LL24, Question 8.10] recently asked whether hyperbolic examples exist. In fact, Lauret, Miatello and Rossetti [LMR15] have constructed spherical examples; they write that hyperbolic examples should also exist but that "their construction seems much more difficult".

In a different direction, it is natural to ask whether we can relate the functions themselves instead of only the eigenvalues.

QUESTION 5.6. When M_1, M_2 are i-isospectral, can we construct explicit isomorphisms

$$T\colon \Omega^i(M_1)_{\Delta=\lambda} \longrightarrow \Omega^i(M_2)_{\Delta=\lambda}$$

that realise the isospectrality?

This is known to be possible in Sunada's construction [Gor09, § 2.2] (see also the proof of Proposition 7.10). Bérard [Bér92,Bér93] coined the term *transplantation operator* for a map T as above, and gave a general construction in the context of representation equivalence, which therefore applies to Vignéras's examples, but his maps are in fact induced by an isomorphism

$$T\colon L^2(\Gamma_1\backslash G) \longrightarrow L^2(\Gamma_2\backslash G)$$

and are not explicit.

Another natural question is to determine, for various invariants of Riemannian manifolds, whether they are isospectral invariants. The following list is far from exhaustive.

- Dimension: *yes*.
- Volume: *yes*.
- Total scalar curvature, and generally heat invariants: *yes*.
- Betti numbers: *yes* from all-i-isospectrality (tautologically) but *no* in general; related to Question 5.5.
- Real cohomology ring: *no*, see [LMR13] in dimensions ≥ 7 and [Ten21] in dimension 3.

The first two are obtained from Weyl's law:

$$\sum_{\lambda<X} \dim(\Omega^i(M)_{\Delta=\lambda}) \sim_{X\to\infty} C(d)\binom{d}{i}\operatorname{vol}(M)X^{d/2},$$

where $d = \dim(M)$ and $C(d)$ is some function of the dimension.

In a different direction, we would like to measure the complexity of isospectral pairs. For spaces of constant curvature, we can use the volume as a measure of complexity. For spherical manifolds, we look for the pair with the largest volume [ÁL24]. For Riemann surfaces, we can equivalently look for the pair with the smallest genus; examples are known in genus 4 and higher [BT87], and it is believed that genus 2 is not possible. Linowitz and Voight [LV15] prove some bounds on the smallest possible genus that can be obtained from Vignéras's construction. For hyperbolic 3-manifolds, Maclachlan and Reid [MR03, Section 12.4] lament (prior to the work of Linowitz and Voight) that "we do not have any estimates on the smallest volume of a pair of isospectral but non-isometric hyperbolic 3-manifolds".

QUESTION 5.7. What is the smallest volume of a pair of isospectral, non isometric 3-orbifolds?

There are of course natural variants, considering i-isospectrality or manifolds. Linowitz and Voight [LV15] provide an orbifold pair of volume $2.8340\ldots$ and a manifold pair of volume $51.024566\ldots$ and prove some minimality results among a class of arithmetic examples. This should be compared with the minimal volume of a hyperbolic 3-orbifold [CF86,GM09,MM12] namely $0.03905\ldots$ and that of a hyperbolic 3-manifold [CFJR01,GMM09,GMM11] namely $0.9427\ldots$. In particular, since the smallest index $[G : U_i]$ in a Gassmann triple is 7 (see for instance [Per77, Theorem 3]), the volume of an isospectral pair of 3-orbifolds arising from Sunada's construction must be at least $7 \cdot 0.03905 > 0.2733$.

Another interesting question is how similar the spectra of non-isospectral manifolds can be.

QUESTION 5.8. Let $d \geq 1$. What is the supremum of the exponents α such that if M_1, M_2 are d-manifolds satisfying

$$\sum_{\lambda<X} |\dim(\Omega^i(M_1)_{\Delta=\lambda}) - \dim(\Omega^i(M_2)_{\Delta=\lambda})| = o(X^\alpha)$$

then M_1 and M_2 are i-isospectral?

By Weyl's law, this supremum belongs to $[0, d/2]$. It was proved by Elstrodt, Grunewald and Mennicke [EGM98, Section 5.3 Theorem 3.3] for hyperbolic 3-manifolds, and then by Bhagwat and Rajan [BR11] for hyperbolic manifolds of any dimension, that if finitely many eigenvalues differ then the manifolds are isospectral. Kelmer [Kel14] then proved that $\alpha = 1/2$ satisfies this property. He guesses that his exponent is probably not optimal, and that the correct exponent might even be $\alpha = d/2$.

There are many other interesting problems and results in this area, see [Sch94,Gor00,GPS05,Gor09,LL24,MR24] for surveys.

6. Post-quantum cryptography

6.1. Cryptography and quantum algorithms. Public-key cryptography [DH76] relies on difficult mathematical problems to build cryptographic protocols. More precisely, one needs a computational problem that is easy to solve in one direction, and difficult in another, or that is difficult in general but easy given extra information. Here are some classical examples.

PROBLEM 6.1 (FACTOR). Given an integer N, compute the prime factors of N.

This problem underlies the security of the RSA cryptosystem [RSA78].

PROBLEM 6.2 (DISCRETELOGARITHM). Given two elements g, h of a finite abelian group G with the promise that $h \in \langle g \rangle$, compute an integer a such that $h = g^a$.

This problem was originally considered in the multiplicative group of a finite field [DH76]. We now have subexponential algorithms to solve it in this case [JOP14]. Considered in the group points of an elliptic curve over a finite field, it underlies the security of the ECDSA cryptosystem.

Quantum computation is an abstract model of computation inspired by the properties of quantum mechanics, that we are trying to realise by concrete physical devices. This model has the same set of computable functions as a Turing machine, but possibly not with the same time complexity, depending on the problem. Concretely, this means that quantum computers can be simulated by classical computers, although with exponentially higher space and time complexity, but that quantum computers may be able to solve some problems faster than classical ones. Shor [Sho97] proved the following.

THEOREM 6.3 (Shor). *There exist polynomial time quantum algorithms to solve* FACTOR *(Problem 6.1) and* DISCRETELOGARITHM *(Problem 6.2).*

This creates a threat on classical cryptography, and it is difficult to estimate how far in the future this threat could materialise (if at all). This motivated the emergence of *post-quantum cryptography*: the design of cryptographic protocols that can be run on a classical computer, but that are believed to be difficult to break, even with a quantum computer. Several families of computational problems have been proposed:

- lattices,
- isogenies,
- codes,
- multivariate polynomial systems,
- etc.

At least, the proposed problems should not be solved efficiently by known quantum algorithms, but ideally we would like strong evidence that they cannot be, and this is difficult: it is hard to prove that a computational problem is hard. A first step in this direction is to prove reductions between problems.

DEFINITION 6.4. We say that *Problem A reduces to Problem B in polynomial time*, written $A \leq B$, if there exists a probabilistic algorithm that, given access to an oracle solving Problem B, solves Problem A in expected polynomial time. We say that *Problem A is equivalent to Problem B*, written $A \asymp B$, if $A \leq B$ and $B \leq A$.

Note that this is a weak notion of reduction: the algorithm is allowed make several calls to the oracle on different inputs (not necessarily a fixed number), the inputs of these calls can depend on the results of the previous calls, and the algorithm can make any polynomial amount of computation with the outputs of those calls. However,

if $A \leq B$ and there is a polynomial time algorithm solving B, then there exists a polynomial time algorithm to solve A.

6.2. Lattices. A *lattice* is a discrete subgroup of a Euclidean vector space V, equivalently the group generated by an independent subset $b_1, \ldots, b_n$ of V; in particular a lattice is a free $\mathbb{Z}$-module of finite rank n. The *covolume* $\mathrm{covol}(\Lambda)$ (also often called *determinant* or *volume*) of a lattice Λ is its covolume in the real vector space it spans. There are several post-quantum cryptosystems based on lattice problems, see [dBvW25] for a recent survey.

The first fondamental computational problem on lattices is the shortest vector problem.

Problem 6.5 (SVP). Given a lattice Λ, compute a shortest nonzero vector $v \in \Lambda$.

We define the successive minima of a lattice.

Definition 6.6. Let Λ be a lattice of rank n. For each $1 \leq i \leq n$ we define

$$\lambda_i(\Lambda) = \min\{\lambda : \dim_{\mathbb{Q}} \langle v \in \Lambda \mid \|v\| \leq \lambda \rangle_{\mathbb{Q}} \geq i\}.$$

In particular $\lambda_1(\Lambda)$ is the length of a shortest nonzero vector in Λ. A useful relaxation of SVP is its approximate version.

Problem 6.7 (γ-SVP). Given a lattice Λ, compute a nonzero vector $v \in \Lambda$ such that $\|v\| \leq \gamma \lambda_1(\Lambda)$.

Thus SVP is the same as 1-SVP. We know several algorithms to solve γ-SVP:

- The LLL algorithm [LLL82] solves $\exp(O(n))$-SVP in polynomial time.
- Sieving algorithms [ASD18] solve $O(1)$-SVP in time $\exp(O(n))$.
- The BKZ algorithm [Sch87,LN25] is parametrised by a block size β and solves $\exp(O(n/\beta))$-SVP in dimension n by making polynomially many calls to an $O(1)$-SVP oracle in dimension β.

For instance, setting $\beta = \sqrt{n}$ we get an algorithm for $\exp(O(\sqrt{n}))$-SVP running in time $\exp(O(\sqrt{n}))$; setting $\beta = \log(n)$ we get a polynomial time algorithm for $\exp(O(n/\log(n)))$-SVP, which is a better approximation factor than LLL.

On the other hand, the problem γ-SVP:

- is NP-hard when $\gamma = O(1)$ and slightly above;
- is in NP$\cap$co-NP when $\gamma = \sqrt{n}$ (and therefore probably not NP-hard);
- underlies the security of cryptographic protocols for $\gamma = n^{O(1)}$.

One problem for constructing reductions is that γ-SVP forces the algorithm to see the difference between lattices that have a very short vector from generic ones. Indeed, by Minkowski's theorem we have

$$\lambda_1(\Lambda) \leq \sqrt{n}\,\mathrm{covol}(\Lambda)^{1/n},$$

and for random lattices we indeed have $\lambda_1(\Lambda) \approx \sqrt{n/(2\pi e)}\,\mathrm{covol}(\Lambda)^{1/n}$ with high probability, but for fixed covolume the shortest vector can be arbitrarily small. This motivates the following variant.

Problem 6.8 (γ-HSVP). Given a lattice Λ, compute a nonzero vector $v \in \Lambda$ such that $\|v\| \leq \gamma\,\mathrm{covol}(\Lambda)^{1/n}$.

By Minkowski's theorem, for all γ we have the obvious reduction

$$\gamma\sqrt{n}\text{-HSVP} \leq \gamma\text{-SVP}.$$

In practice, cryptosystems use structured lattices to allow faster computations, smaller sizes and additional cryptographic functionalities. A common type of structure is that of a module lattice.

Definition 6.9. Let F be a number field. A *$\mathbb{Z}_F$-module lattice* (or *module lattice* when F is implicit) is a lattice Λ equipped with an action of $\mathbb{Z}_F$ such that

$$\langle av, w\rangle = \langle v, a^* w\rangle$$

for all $v, w \in \Lambda$ and $a \in \mathbb{Z}_F$, where $a \mapsto a^*$ denotes the canonical involution $F_{\mathbb{R}} \to F_{\mathbb{R}}$. The *rank* of a module lattice is its rank as a projective $\mathbb{Z}_F$-module.

This raises the following question.

Question 6.10. Are lattice problems significantly easier on module lattices than on unstructured lattices?

There are indeed significantly better algorithms for rank 1 module lattices [PMHS19,CDW21], but so far not in higher rank.

6.3. Isogenies. We are going to consider a class of problems consisting in finding isogenies between given elliptic curves over finite fields, subject to certain restrictions. However, it is easy to find such isogenies if they have low degree, so we will need to be able to represent isogenies of large degree. There are several possible representations (for instance as a chain of isogenies of low degree) but for the purpose of constructing reductions it is better not to specify a particular representation.

Definition 6.11 (Efficient representation). Let $\mathcal{A}$ be an algorithm, and let $\varphi\colon E \to E'$ be an isogeny over a finite field $\mathbb{F}_q$. An *efficient representation* of φ (with respect to $\mathcal{A}$) is data $D_\varphi \in \{0,1\}^*$ such that

- $D_\varphi \in \{0,1\}^*$ has size polynomial in $\log(\deg(\varphi))$ and $\log q$, and

- on input D_φ and $P \in E(\mathbb{F}_{q^k})$, the algorithm $\mathcal{A}$ returns $\varphi(P)$, and runs in polynomial time in $\log(\deg(\varphi))$, $\log q$, and k.

The algorithm $\mathcal{A}$ will be left implicit. Now recall that there are two types of elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p: *ordinary* and *supersingular*. For us, the most important difference is:

- If $E/\mathbb{F}_q$ is ordinary, then $\mathrm{End}(E)$ is an order in a quadratic imaginary field.
- If $E/\mathbb{F}_q$ is supersingular, then $\mathrm{End}(E)$ is a maximal order in the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞.

The first cryptosystem based on isogeny problems was proposed by Couveignes [Cou97] and rediscovered later by Rostovtsev and Stolbunov [RS06], and is based on ordinary curves. It is inefficient but served as inspiration to many other ones.

In the sequel we will mostly use supersingular curves. We will use the notation $\mathrm{SS}(p)$ to denote the category with

- objects: supersingular elliptic curves over $\overline{\mathbb{F}}_p$;
- morphisms: algebraic group morphisms.

There are approximately $p/12$ supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism.

The first cryptosystem based on supersingular isogenies is the Charles–Lauter–Goren hash function [CLG09]. It uses a public $E \in \mathrm{SS}(p)$ and a small prime ℓ; an input binary string $s \in \{0,1\}^*$ is then converted to a path of ℓ-isogenies where at each intermediate curve E_i, the bit s_i determines (in a public way) which outgoing isogeny should be taken. The hash of the string s is the j-invariant of the end curve E' of the path $E \to E'$. Clearly, if one can find preimages of this hash function, then one can solve the following problem.

Problem 6.12 (ℓ-isog). Given two supersingular curves $E, E' \in \mathrm{SS}(p)$, compute an isogeny $E \to E'$ of degree a power of ℓ.

Moreover, if one can find collisions for the CGL hash function, then from the two paths $\varphi\colon E \to E'$ and $\psi\colon E \to E'$ one can create an endomorphism $\hat{\psi} \circ \varphi \in \mathrm{End}(E)$. One can show that this creates a non-scalar endomorphism. Therefore, if one can find collisions, then one can solve the following problem.

Problem 6.13 (OneEnd). Given a supersingular curve $E \in \mathrm{SS}(p)$, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

We have the following easy reduction (by generating a random path and computing a second path to the same endpoint).

$$\text{OneEnd} \leq \ell\text{-isog}.$$

The first cryptosystem that really got isogeny-based cryptography off the ground was the key exchange protocal SIDH proposed by Jao

and De Feo [JDF11,DFJP14]. Its underlying problem was to find an ℓ-isogeny path as in ℓ-ISOG, but given the action of the secret isogeny on a basis of N-torsion points for some integer N coprime to ℓ.

In light of the relation between supersingular isogenies and quaternion algebras (which can be made precise in the form of Deuring's correspondence, see Theorem 11.5), it is natural to study the problem analogous to ℓ-ISOG in quaternion algebras. This was done in [KLPT14], in which Kohel, Lauter, Petit and Tignol described a heuristic polynomial time algorithm (known as the KLPT algorithm) that, given a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ and a right $\mathcal{O}$-ideal J, computes $x \in B_{p,\infty}$ such that xJ has ℓ-power norm. This made it clear that the following problem was important.

PROBLEM 6.14 (ENDRING). Given a supersingular curve $E \in \mathrm{SS}(p)$, compute a basis $\alpha_1, \dots, \alpha_4$ of $\mathrm{End}(E)$.

Tautologically we have

$$\textsc{OneEnd} \leq \textsc{EndRing}.$$

Using the KLPT algorithm, De Feo, Kohel, Leroux, Petit and Wesolowski proposed a signature scheme called SQISIGN [DFKL$^+$20]. They studied its security, and in particular its soundness naturally reduces to the ONEEND problem.

THEOREM 6.15 (Theorem 1 in [DFKL$^+$20]). *If* ONEEND *is hard then* SQISIGN *is sound.*

In 2022, SIDH was broken by Castryck and Decru [CD23,MMP$^+$23, Rob23]. This made SQISIGN the new flagship of isogeny-based cryptography, but also made it clear that a better understanding of the relative security of the various isogeny problems was necessary. The attack was using the torsion point information in a crucial way, and people remained confident in the difficulty of ENDRING and ℓ-ISOG. But what about ONEEND, which is a priori weaker than each of them?

As a first step towards this better understanding, Wesolowski [Wes22] provided a variant of the KLPT algorithm that he proved to be correct under GRH, and deduced the following equivalence.

THEOREM 6.16 ([Wes22]). *We have* ENDRING $\asymp \ell$-ISOG.

In parallel, many cryptosystem were proposed based on *oriented* supersingular elliptic curves (i.e. given with the extra data of an embedding of a fixed quadratic order R in its endomorphism ring). They are closer in spirit to the original Couveignes cryptosystem: first CSIDH [CLM$^+$18], then CSI-Fish [BKV19], OSIDH [CK20] which was partially broken [DDF22], SCALLOP [FFK$^+$23] and others. One recurring problem with those constructions was the inability to efficiently compute the isogeny action of $\mathrm{Cl}(R)$ on the corresponding set of elliptic curves, for arbitrary input ideals (only smooth ideals could be handled).

Together with Damien Robert, I designed Clapotis [P9] [P15], an algorithm to compute this action in polynomial time for arbitrary input ideals. I also took part in a proposed variant, PEARL-SCALLOP [P11], which interpolates between CSI-Fish and SCALLOP. These works do not fit in the theme of this manuscript, so I will not describe them in detail.

Part 2

Hecke operators of finite groups

7. Can you hear torsion homology?

7.1. Number fields and 3-manifolds. Sunada was led to his discovery of a construction of isospectral manifolds [Sun85] by an analogy with a number-theoretic construction. In fact, as was first pointed out by Mazur in his "knots and primes" philosophy, the analogy between manifolds and number fields becomes especially strong in dimension 3 since rings of integers of number fields satisfy a 3-dimensional Poincaré duality [Maz73]. The property of number fields analogous to isospectrality is arithmetic equivalence.

DEFINITION 7.1. Two number fields F_1 and F_2 are *arithmetically equivalent* if

$$\zeta(F_1, s) = \zeta(F_2, s).$$

Of course, this is equivalent to the property that almost all unramified primes split in the same way in the two fields. This analogy is most visible when isospectrality is expressed using spectral zeta functions.

DEFINITION 7.2. Let M be a closed manifold and let $i \geq 0$. The i-th *spectral zeta function* of M is defined by

$$\zeta_i(M, s) = \sum_{\lambda > 0} \lambda^{-s},$$

where the sum is taken over the positive spectrum of the Laplace operator acting on i-forms, taken with multiplicity.

This sum converges for $\mathrm{Re}(s) > \frac{\dim(M)}{2}$ and the spectral zeta function admits a meromorphic extension to $\mathbb{C}$ with finitely many poles, all simple ([MP49,See67], see also [Ros97, Section 5.1]). If two manifolds M_1 and M_2 are i-isospectral then $\zeta_i(M_1, s) = \zeta_i(M_2, s)$.

Similarly to the case of isospectral manifolds, it is natural to ask which invariants of a number field F are determined by the Dedekind zeta function. The following are:

- the degree, and more precisely the signature (r_1, r_2);
- the discriminant;
- the Galois closure;
- the largest subfield that is Galois over $\mathbb{Q}$;
- the number of roots of unity;
- the product $h(F) \cdot \mathrm{Reg}(F)$,

where the last statement follows from the analytic class number formula (3.1). It is therefore natural to ask whether $h(F)$ and $\mathrm{Reg}(F)$ are separately determined by $\zeta(F, s)$. This turns out to be false.

EXAMPLE 7.3 ([dSP94]). Let $F_1 = \mathbb{Q}(\sqrt[8]{-15})$ and $F_2 = \mathbb{Q}(\sqrt[8]{-240})$. Then $\zeta(F_1, s) = \zeta(F_2, s)$, but their class groups are

$$\mathrm{Cl}(F_1) \cong C_8 \times C_2 \text{ and } \mathrm{Cl}(F_2) \cong C_8$$

and their regulators are

$$\mathrm{Reg}(F_1) \approx 66.316 \text{ and } \mathrm{Reg}(F_2) \approx 132.63.$$

One is therefore led to ask which primes can occur in $h(F_1)/h(F_2) = \mathrm{Reg}(F_2)/\mathrm{Reg}(F_1)$ for arithmetically equivalent number fields F_1, F_2. The following is expected to hold [dS98].

Conjecture 7.4. For every prime number p, there exists arithmetically equivalent number fields F_1, F_2 such that $v_p(h(F_1)) \neq v_p(h(F_2))$.

This conjecture is known to be true for a finite number of primes p, by finding examples, but is open in general. Spectral zeta functions admit a special value formula analogous to the analytic class number formula, the Cheeger–Müller formula [RS71,Che79,Mül78,Mül93] (see also the expositions in [BV13, Section 2] and [Rai21, Section 1]). For simplicity we only state its consequence for isospectral manifolds.

Theorem 7.5. *Let M_1, M_2 be isospectral closed manifolds of dimension d. Then*

$$\prod_{i=0}^{d} \left(\frac{\mathrm{Reg}_i(M_1)}{\#H_i(M_1,\mathbb{Z})_{\mathrm{tors}}} \right)^{(-1)^i} = \prod_{i=0}^{d} \left(\frac{\mathrm{Reg}_i(M_2)}{\#H_i(M_2,\mathbb{Z})_{\mathrm{tors}}} \right)^{(-1)^i}.$$

When the dimension d is even, both products actually equal 1 and we learn nothing. When d is odd, we obtain that the real number

$$\prod_{i=0}^{\frac{d-1}{2}} \frac{\mathrm{Reg}_i(M_1)^2}{\mathrm{Reg}_i(M_2)^2}$$

is in fact a rational number. This is interesting, especially considering that the regulators are typically transcendental numbers! Any arithmetician immediately wants to ask the following question.

Question 7.6. When M_1, M_2 are i-isospectral, does it follow that the real number $\frac{\mathrm{Reg}_i(M_1)^2}{\mathrm{Reg}_i(M_2)^2}$ is rational?

We do not know the answer in general, but we have obtained results in the cases of the Sunada construction (Corollary 7.14) and the Vignéras construction (Section 12.5). In dimension 3, Theorem 7.5 specialises as follows.

Corollary 7.7. *Let M_1, M_2 be isospectral closed 3-manifolds. Then*

$$\frac{\#H_1(M_1,\mathbb{Z})_{\mathrm{tors}}}{\mathrm{Reg}_1(M_1)^2} = \frac{\#H_1(M_2,\mathbb{Z})_{\mathrm{tors}}}{\mathrm{Reg}_1(M_2)^2}.$$

This is reminiscent of the case of number fields, especially with the terms written $\#H_1(M,\mathbb{Z})_{\mathrm{tors}} \cdot \mathrm{Reg}_2(M)^2$, but notice the square, which is an important difference. In analogy with Conjecture 7.4, we may ask the following question.

QUESTION 7.8. Let p be a prime number. Does there exist isospectral 3-manifolds M_1, M_2 such that

$$v_p(\#H_1(M_1,\mathbb{Z})_{\text{tors}}) \neq v_p(\#H_1(M_2,\mathbb{Z})_{\text{tors}})?$$

However, contrary to the open case of number fields, we answer this question positively for all p as a special case of Theorem 7.19. In fact, this was already known to be false in dimension 2 and true in every dimension ≥ 4, so the 3-dimensional case is the most interesting one.

7.2. Brauer relations, torsion and regulators. It is convenient to place Sunada's construction in the setting of Brauer relations (Section 2.2).

DEFINITION 7.9. Let G be a finite group and M a closed manifold equipped with a free G-action. Let X be a finite G-set, and write

$$X \cong \bigsqcup_{i=1}^{n} G/U_i$$

for some subgroups U_i of G. Define the possibly disconnected manifold

$$M/X = \bigsqcup_{i=1}^{n} M/U_i.$$

We then have the following possibly possibly disconnected extension of Sunada's theorem, replacing Gassmann's triples by Brauer relations.

PROPOSITION 7.10. *Let G be a finite group and M a closed manifold equipped with a free G-action. Let $\Theta = X - Y$ be a $\mathbb{Q}[G]$-relation. Then the manifolds M/X and M/Y are i-isospectral for all $i \geq 0$.*

PROOF. Let $i \geq 0$. First note that for every finite G-set Z, we have

$$\Omega^i(M/Z) \cong \Omega^i(M)^Z,$$

where the isomorphism commutes with the Laplace operator, so that for every $\lambda \in \mathbb{R}$, we have

$$\Omega^i(M/Z)_{\Delta=\lambda} \cong \Omega^i(M)^Z_{\Delta=\lambda}.$$

Let

$$T\colon \mathbb{C}[X] \to \mathbb{C}[Y] \text{ and } T'\colon \mathbb{C}[Y] \to \mathbb{C}[X]$$

be inverse isomorphisms of $\mathbb{C}[G]$-modules. They induce, for every $i \geq 0$ and λ, Hecke operators that are inverse isomorphisms (cf. Section 2.1)

$$\Omega^i(M)^X_{\Delta=\lambda} \cong \Omega^i(M)^Y_{\Delta=\lambda}.$$

The dimensions of $\Omega^i(M/X)_{\Delta=\lambda}$ and $\Omega^i(M/Y)_{\Delta=\lambda}$ are therefore the same for every i and λ, i.e. M/X and M/Y are i-isospectral for all i. □

We also introduce the following convenient notation.

NOTATION 7.11. let G be a finite group. Let f be a function on the set of isomorphism classes of finite G-sets, valued in an abelian group, that respects disjoint unions in the sense that $f(X \sqcup Y) = f(X)f(Y)$ for every X, Y. Then we extend f to the Burnside group by setting $f(X - Y) = f(X)/f(Y)$.

For instance, for a Brauer relation $\Theta = X - Y$, we will write

$$\mathrm{Reg}_i(M/\Theta) = \frac{\mathrm{Reg}_i(M/X)}{\mathrm{Reg}_i(M/Y)}, \text{ etc.}$$

In this context, we easily obtain some control over the primes that can appear in $\#H_i(M/\Theta, \mathbb{Z})_{\mathrm{tors}}$.

PROPOSITION 7.12 (Theorem 3.5 in [P1]). *Let M be a closed manifold with a free G-action, and let $\Theta = X - Y$ be a $\mathbb{Z}_p[G]$-relation. Then for all $i \geq 0$ we have*

$$H_i(M/X, \mathbb{Z}_p) \cong H_i(M/Y, \mathbb{Z}_p).$$

In particular we have $v_p(\#H_i(M/\Theta, \mathbb{Z})_{\mathrm{tors}}) = 0$.

PROOF. Since they are short, we give two proofs.

First proof: for every subgroup U of G we have

$$H_i(M/U, \mathbb{Z}_p) \cong H_i(M/G, \mathbb{Z}_p[G/U]).$$

By additivity we get

$$H_i(M/X, \mathbb{Z}_p) \cong H_i(M/G, \mathbb{Z}_p[X]) \cong H_i(M/G, \mathbb{Z}_p[Y]) \cong H_i(M/X, \mathbb{Z}_p).$$

Second proof: by Lemma 2.2, Θ is a $\mathbb{Z}_{(p)}[G]$-relation. Therefore, there exists Hecke operators

$$T\colon \mathbb{Z}[X] \to \mathbb{Z}[Y] \text{ and } T'\colon \mathbb{Z}[Y] \to \mathbb{Z}[X]$$

whose compositions are homotheties $d \cdot \mathrm{Id}$ with $v_p(d) = 0$. Since $U \mapsto H_i(M/U, \mathbb{Z}_p)$ is a Mackey functor (a formalism allowing us to construct actions of Hecke operators [Yos83] more generally than on fixed points), we obtain induced maps

$$T\colon H_i(M/Y, \mathbb{Z}) \to H_i(M/X, \mathbb{Z}) \text{ and } T'\colon H_i(M/X, \mathbb{Z}) \to H_i(M/Y, \mathbb{Z})$$

that are isomorphisms over $\mathbb{Z}_p$.

□

The second proof is not really shorter than the first, especially if one writes down all the details of "homology is a Mackey functor", but it gives an explicit isomorphism. Importantly, this point of view will also be useful in the analysis of the Vignéras construction (see Section 12.6). Proposition 7.12 is useful to exclude primes from appearing in $\#H_1(M/\Theta, \mathbb{Z})_{\mathrm{tors}}$, but we also want to force primes to appear. This turns out to be easier to do by using regulators and applying the Cheeger–Müller formula, via the theory of regulator constants (see Section 2.3).

PROPOSITION 7.13 (Theorem 3.11 in [P1]). *Let M be a closed manifold with a free G-action, and let Θ be a $\mathbb{Q}[G]$-relation. Then for all $i \geq 0$ we have*

$$\mathrm{Reg}_i(M/\Theta)^2 \equiv \mathcal{C}_\Theta(H_i(M,\mathbb{Q})) \bmod (\mathbb{Q}^\times)^2.$$

As a corollary, we obtain a positive answer to Question 7.6 for i-isospectral manifolds obtained from Sunada's construction.

COROLLARY 7.14. *Let M be a closed manifold with a free G-action, and let $\Theta = X - Y$ be a $\mathbb{Q}[G]$-relation. Then for all $i \geq 0$ we have*

$$\frac{\mathrm{Reg}_i(M/X)^2}{\mathrm{Reg}_i(M/Y)^2} \in \mathbb{Q}^\times.$$

PROOF. Apply Proposition 7.13 and Theorem 2.3. □

7.3. Equivariant surgery. In order to apply Proposition 7.13 to Question 7.8, we need a supply of Brauer relations with interesting regulator constants.

EXAMPLE 7.15 (Proposition 4.2 in [P1]). Let p be an odd prime, let $G = \mathrm{GL}_2(\mathbb{F}_p)$, and let $U, U' \leq B \leq G$ be the following subgroups:

$$B = \begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}, U = \begin{pmatrix} (\mathbb{F}_p^\times)^2 & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}, U' = \begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & (\mathbb{F}_p^\times)^2 \end{pmatrix}.$$

Then we have isomorphisms of $\mathbb{Q}[G]$-modules

$$\mathbb{Q}[G/U] \cong \mathbb{Q}[G/B] \oplus W \cong \mathbb{Q}[G/U'],$$

where W is a simple $\mathbb{Q}[G]$-module (in fact W remains simple over $\mathbb{C}$: it is a principal series representation attached to the nontrivial quadratic character of $\mathbb{F}_p^\times$); in particular, the linear combination $\Theta = U - U'$ is a $\mathbb{Q}[G]$-relation. In addition, Θ is a $\mathbb{Z}_q[G]$-relation for every prime $q \neq p$, and we have

$$\mathcal{C}_\Theta(W) \equiv p \bmod (\mathbb{Q}^\times)^2.$$

EXAMPLE 7.16. Let $G = \mathbb{Z}/8\mathbb{Z} \rtimes (\mathbb{Z}/8\mathbb{Z})^\times$, and let $U, U' \leq B \leq G$ be the following subgroups:

$$B = 4\mathbb{Z}/8\mathbb{Z} \rtimes (\mathbb{Z}/8\mathbb{Z})^\times, U = 0 \times (\mathbb{Z}/8\mathbb{Z})^\times, U' = 4\mathbb{Z}/8\mathbb{Z} \times \langle -1 \rangle.$$

Then we have isomorphisms of $\mathbb{Q}[G]$-modules

$$\mathbb{Q}[G/U] \cong \mathbb{Q}[G/B] \oplus W \cong \mathbb{Q}[G/U'],$$

where W is a simple $\mathbb{Q}[G]$-module; in particular, the linear combination $\Theta = U - U'$ is a $\mathbb{Q}[G]$-relation. In addition, Θ is a $\mathbb{Z}_q[G]$-relation for every prime $q \neq 2$, and we have

$$\mathcal{C}_\Theta(W) \equiv 2 \bmod (\mathbb{Q}^\times)^2.$$

From these examples, we can solve Question 7.8 if we can exhibit, for certain finite groups G and $\mathbb{Q}[G]$-modules W, a closed 3-manifold with a free G-action whose first homology is isomorphic to G. In [P2], we prove that this is possible for every G and every W!

THEOREM 7.17 (Theorem 3.8 in [P2]). *Let G be a finite group, and let W be a finitely generated $\mathbb{Q}[G]$-module. Then there exists a closed hyperbolic non-arithmetic 3-manifold M with a free G-action such that the $\mathbb{Q}[G]$-module $H_1(M, \mathbb{Q})$ is isomorphic to W.*

PROOF SKETCH. Our proof is inspired by the work of Cooper and Long [CL00], in which they prove Theorem 7.17 for $W = 0$. The steps are the following:

(1) construct a 3-manifold M with a free G action, without any control on $H_1(M, \mathbb{Q})$;
(2) from any 3-manifold M with a free G-action, construct M' that has an extra regular module in its homology, i.e. $H_1(M', \mathbb{Q}) \cong H_1(M, \mathbb{Q}) \oplus \mathbb{Q}[G]$;
(3) from any 3-manifold M with a free G-action with a decomposition $H_1(M, \mathbb{Q}) \cong \mathbb{Q}[G] \oplus V$ and a $\mathbb{Q}[G]$-submodule P of $\mathbb{Q}[G]$, construct M' that replaces the regular summand by P, i.e. $H_1(M', \mathbb{Q}) \cong P \oplus V$;
(4) from any 3-manifold M with a free G-action, construct M' with $H_1(M', \mathbb{Q}) \cong H_1(M, \mathbb{Q})$ such that M' is hyperbolic and non-arithmetic.

It is clear that by repeated application of those steps, we obtain Theorem 7.17.

Step 1 is simple: start with a 3-manifold M' whose fundamental group surjects onto the free group Free_2 on two generators, for instance the connected sum $M' = (\mathbb{S}^1 \times \mathbb{S}^2)\#(\mathbb{S}^1 \times \mathbb{S}^2)$. Let r be such that G can be generated by r elements. Let M'' be a finite covering of M' such that $\pi_1(M'')$ surjects onto Free_r. Then there exists a surjection $\pi_1(M'') \to G$; the corresponding covering $M \to M''$ is a G-covering, so that G acts freely on M.

We accomplish steps 2, 3 and 4 by performing G-equivariant Dehn surgery on the manifolds. However, step 2 can be explained simply: the G-equivariant connected sum

$$M' = M\#(G \times \mathbb{S}^1 \times \mathbb{S}^2)$$

is suitable since $H_1(G \times \mathbb{S}^1 \times \mathbb{S}^2, \mathbb{Q}) \cong \mathbb{Q}[G]$. Dehn surgery is the following process:

- Drilling: choose a simple closed curve γ and a tubular neighborhood T of γ, which is a solid torus $\mathbb{S}^1 \times \mathbb{D}^2$. Remove the interior of T to obtain a manifold with torus boundary.
- Filling: glue back a solid torus to the torus boundary by a diffeomorphism of ∂T.

In our application, we perform drilling and filling G-equivariantly, so as to preserve the G-action. The effect of G-equivariant Dehn surgery on the first homology is as follows (see [2, Lemma 3.2]):

- Drilling: this adds a quotient of $\mathbb{Q}[G]$ to the first homology, corresponding to the fact that the class of $\partial\mathbb{D}^2$ might no longer be trivial once the disk is removed, and similarly for its G-orbit.
- Filling: this kills a quotient of $\mathbb{Q}[G]$, as the curve on which the disk $\mathbb{D}^2$ gets glued becomes trivial in homology, and similarly for its G-orbit.

The precise modules that are created and killed by Dehn surgery can be controlled by prescribing the surgery coefficients from the coefficients of some idempotent $e \in \mathbb{Q}[G]$; this is the step where our work is more precise than that of Cooper and Long. In this process, the image e^* of e under the canonical involution $x = \sum_g x_g g \mapsto x^* = \sum_g x_g g^{-1}$ of $\mathbb{Q}[G]$ appears naturally, along with the following algebraic property: for every idempotent $e \in \mathbb{Q}[G]$, we have $\mathbb{Q}[G] = \mathbb{Q}[G]e + \mathbb{Q}[G](1 - e^*)$ [2, Proposition 1.5].

Finally, step 4 is an application of Thurston's hyperbolic Dehn surgery theorem [Thu22, Theorem 5.8.2]. The non-arithmeticity is not stated in [P2], but it can be imposed using the fact that there are only finitely many arithmetic hyperbolic 3-manifolds of volume bounded above [Bor81, Theorem 8.2]. □

In Theorem 7.17 we have determined all the $\mathbb{Q}[G]$-modules that can occur as the first homology of a 3-manifold with free G-action. The following question seems harder (recall that a $\mathbb{Z}[G]$-*lattice* is a $\mathbb{Z}[G]$-module that is finite free over $\mathbb{Z}$).

QUESTION 7.18. Which $\mathbb{Z}[G]$-lattices can be realised as $H_1(M, \mathbb{Z})_{\text{free}}$ for some closed hyperbolic 3-manifold M with a free G-action?

We finally return to spectral geometry, settling Question 7.8.

THEOREM 7.19 (Theorem 5.14 in [P2]). *Let $\mathcal{S}$ be a finite set of prime numbers. Then there exists closed connected non-arithmetic manifolds M_1 and M_2 that are 0- and 1-isospectral with respect to hyperbolic metrics and such that*

(1) *for all $p \in \mathcal{S}$ we have*

$$\#H_1(M_1, \mathbb{Z})[p^\infty] \neq \#H_1(M_2, \mathbb{Z})[p^\infty];$$

(2) *for all primes $q \notin \mathcal{S}$ we have an isomorphism of abelian groups*

$$H_1(M_1, \mathbb{Z})[q^\infty] \cong H_1(M_2, \mathbb{Z})[q^\infty].$$

It is clear that Theorem 7.19 for $\mathcal{S} = \{p\}$ follows from the combination of Theorem 7.17, Proposition 7.12, the Cheeger–Müller formula,

Proposition 7.13 and Examples 7.15 and 7.16. The general case is obtained by taking suitable products of the groups from these examples.

In light of this success, it is natural to ask whether the techniques can be adapted to the case of number fields (Conjecture 7.4). Unfortunately, this seems difficult for several reasons. First, number fields are much more rigid than manifolds, and we do not currently have an analogue of Dehn surgery for number fields. One way this manifests is that there is very little flexibility for the $\mathbb{Q}[G]$-module analogous to $H_1(M,\mathbb{Q})$, namely $\mathbb{Z}_F^\times \otimes \mathbb{Q}$ for a Galois extension $F/\mathbb{Q}$ with Galois group G: it is isomorphic to $\mathbb{Q}[G/\langle c\rangle] \ominus \mathbb{Q}$ where $c \in G$ is a complex conjugation. In addition, while the ratio of torsion homology sizes is related to the regulator constant, the ratio of class numbers is related to the square of the regulator constant, but regulator constants of $\mathbb{Q}[G]$-modules are only well-defined up to squares, so this gives no information; to obtain useful information with this method, one would have to control the $\mathbb{Z}[G]$-module structure of the units (or at least the $\mathbb{Z}_p[G]$-module structure for some primes p), which is much harder.

8. Computing class groups

8.1. From Brauer relations to norm relations. We have algorithms to compute class groups, but it often happens, especially in large degree number fields, that those algorithms do not terminate in reasonable time. A natural idea is then to extract partial information with other techniques. Brauer relations can provide this kind of information. For instance, let F be a number field with Galois closure $\widetilde{F}$ having Galois group G, let $\Theta = \sum_i n_i U_i$ be a $\mathbb{Q}[G]$-relation with $n_i \neq 0$, and let $F_i = \widetilde{F}^{U_i}$ for all i. Then we have

$$\prod_i \zeta(F_i, s)^{n_i} = 1,$$

and by the analytic class number formula we get

$$\prod_i \left(\frac{h(F_i)\operatorname{Reg}(F_i)}{w(F_i)}\right)^{n_i} = 1,$$

which was the motivation for Brauer's work [Bra51]. If we can find such a relation Θ where F appears as one of the F_i and all the other F_i are easier than F (for instance, in this situation the degree is often a good proxy for the difficulty of the class group and unit computation), then we can obtain the product $h(F)\operatorname{Reg}(F)$. We can sometimes obtain more precise information about the class groups.

Theorem 8.1 (Corollary 1.4 and Proposition 2.2 in [Bol97]). *Let p be a prime number and assume that Θ is a $\mathbb{Z}_p[G]$-relation. Then we*

have an isomorphism of abelian groups

$$\bigoplus_{n_i>0} \mathrm{Cl}(F_i)[p^\infty]^{n_i} \cong \bigoplus_{n_i<0} \mathrm{Cl}(F_i)[p^\infty]^{-n_i}.$$

However, even when we have a useful Brauer relation, there is often one or more primes p for which one cannot apply Theorem 8.1. A solution appeared for the special case of multiquadratic fields (compositums of quadratic extensions) in the work of Biasse and van Vredendaal [BVV19], generalising work [BBdV+17] on the related problem of recovering a short generator of an ideal. These papers used subfields, saturation techniques, as well as a seemingly ad hoc identity coming from the work of Wada [Wad66]: in the group ring of $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$ we have

$$2 = (1+\sigma) + (1+\tau) - \sigma(1+\sigma\tau) = N_{\langle\sigma\rangle} + N_{\langle\tau\rangle} - \sigma N_{\langle\sigma\tau\rangle}, \tag{8.1}$$

where we recall the notation $N_H = \sum_{h\in H} h \in \mathbb{Q}[G]$. Note that the group $C_2 \times C_2$ also has a Brauer relation, namely

$$\Theta = 1 + 2G - \langle\sigma\rangle - \langle\tau\rangle - \langle\sigma\tau\rangle,$$

i.e. we have an isomorphism

$$\mathbb{Q}[G] \oplus \mathbb{Q}[G/G]^2 \cong \mathbb{Q}[G/\langle\sigma\rangle] \oplus \mathbb{Q}[G/\langle\tau\rangle] \oplus \mathbb{Q}[G/\langle\sigma\tau\rangle],$$

but the identity (8.1) seems to be of a different nature, as it has coefficients from the group ring $\mathbb{Z}[G]$ rather than only scalars. This motivates the following definition.

Definition 8.2 (Definition 2.1 (2) in [P5]). Let G be a finite group, and let $\mathcal{U}$ be a set of nontrivial subgroups of G. A *norm relation with respect to* $\mathcal{U}$ is an identity of the form

$$d = \sum_{i=1}^{n} a_i N_{U_i} b_i, \tag{8.2}$$

for some integer $d > 0$, subgroups $U_i \in \mathcal{U}$ and coefficients $a_i, b_i \in \mathbb{Z}[G]$. We omit the mention of $\mathcal{U}$ when it is the set of all nontrivial subgroups of G.

Remark 8.3. We allow repetitions in the U_i, so the definition is less restrictive than identities of the form

$$d = \sum_{U\in\mathcal{U}} a_U N_U b_U.$$

Of course, we designed the definition so that the identity (8.1) is a norm relation. There are many other examples.

Example 8.4. Let $G = C_3 \times C_3 = \langle u, v \rangle$. We have the norm relation

$$3 = N_{\langle u\rangle} + N_{\langle v\rangle} + N_{\langle uv\rangle} - (u + uv)N_{\langle u^2v\rangle}.$$

This relation was introduced by Parry [Par77] and was used in [LPS20].

EXAMPLE 8.5. Let p be a prime number, and let $G = C_p \times C_p$. Then we have the norm relation

$$p = -N_G + \sum_{C \leq G, \#C = p} N_C.$$

Indeed, every nontrivial element of G has order p, there are $p + 1$ subgroups of order p, and every nontrivial element of G is contained in exactly one of them.

EXAMPLE 8.6. Let p be a prime number and q a prime number dividing $p - 1$. Let $G = C_p \rtimes C_q$ be a nonabelian semidirect product. Then we have the norm relation

$$p = -N_G + N_{C_p} + \sum_{C \leq G, \#C = q} N_C.$$

Indeed, every nontrivial element of G has order p or q, there is a unique subgroup of order p, there are p subgroups of order q, and every nontrivial element is contained in exactly one subgroup of prime order.

The usefulness of norm relations is demonstrated by the following simple lemma.

LEMMA 8.7 (Proposition 3.1 in [P5]). *Let G be a finite group and let W be a $\mathbb{Z}[G]$-module. Assume G admits a norm relation (8.2). Then the exponent of the quotient $W/\sum_{i=1}^{n} a_i W^{U_i}$ is finite and divides d.*

PROOF. Let $w \in W$. Then

$$d \cdot w = \Big(\sum_{i=1}^{n} a_i N_{U_i} b_i\Big) w = \sum_{i=1}^{n} a_i (N_{U_i} b_i w) \in \sum_{i=1}^{n} a_i W^{U_i}.$$

□

Applied to an $\mathcal{S}$-unit group W, this means that we can recover W from the W^{U_i}, which are $\mathcal{S}$-unit groups of the corresponding fixed fields, and extractions of d-th roots. Following [P12], we will generalise this fact before the actual algorithmic applications, and Lemma 8.7 is given here for the purpose of illustration and comparison.

At this point, it is not clear whether the existence of norm relations is a coincidence or something systematic. To make progress, we reformulate this existence in representation-theoretic language.

PROPOSITION 8.8 (Proposition 2.10 in [P5]). *Let G be a finite group and $\mathcal{U}$ a set of nontrivial subgroups of G. The following are equivalent:*

1. *there exists a norm relation with respect to $\mathcal{U}$;*
2. *in $\mathbb{Q}[G]$, the two-sided ideal generated by the N_U for $U \in \mathcal{U}$ equals $\mathbb{Q}[G]$;*
3. *for every simple $\mathbb{Q}[G]$-module W, there exists $U \in \mathcal{U}$ such that $W^U \neq 0$;*

(4) *for every simple* $\mathbb{C}[G]$*-module* W*, there exists* $U \in \mathcal{U}$ *such that* $W^U \neq 0$*.*

PROOF SKETCH. Use the fact that for every $U \leq G$, the idempotent $\frac{1}{\#U} N_U$ acts on every $\mathbb{Q}[G]$-module W as a projector onto W^U. □

First, using Proposition 8.8, we can easily test the existence of norm relations by character theory. Second, because of the existence of an invariant Hermitian product on every complex representation of a finite group, this relates the existence of norm relations to the well-studied problem of fixed-point free actions on spheres. Using this relation and in particular the work of Wolf [Wol67] we obtain a necessary and sufficient condition for the existence of norm relations.

THEOREM 8.9 (Theorem 2.11 in [P5]). *Let* G *be a finite group. The group* G *admits a norm relation if and only if it contains*

- *a non-cyclic subgroup of order* pq *where* p *and* q *are (not necessarily distinct) primes, or*
- *a subgroup isomorphic to* $\mathrm{SL}_2(\mathbb{F}_p)$ *where* $p = 2^{2^k} + 1$ *is a Fermat prime with* $k > 1$*.*

This theorem says that many groups have norm relations: informally, every group that is "far from cyclic" admits norm relations. More precisely, the groups that do not admit norm relations are also known as *freely representable groups*; such groups are very constrained and are classified, see [Wal13,Ait21]. It is instructive to compare Theorem 8.9 with the following theorem of Funakura.

THEOREM 8.10 (Funakura, Theorem 9 in [Fun78]). *Let* G *be a finite group. The group* G *admits a Brauer relation with a nonzero coefficients of* $\mathbb{Q}[G]$ *if and only if* G *contains a non-cyclic subgroup of order* pq *where* p *and* q *are (not necessarily distinct) primes.*

In light of these theorems, we see that

- $G = \mathrm{SL}_2(\mathbb{F}_5)$ does not admit a norm relation.
- $G = \mathrm{SL}_2(\mathbb{F}_{17})$ admits a norm relation, but no Brauer relation involving $\mathbb{Q}[G]$.

8.2. Generalising further. In [P5], we develop algorithms based on the above notion of norm relations. However, this notion is only useful in Galois extensions, and only takes advantage of subfields (in fact, intermediate fields in the Galois extension). There are many interesting number fields that do not have automorphisms, and one may naturally wonder whether auxiliary fields that are not subfields could also be used. This was fully resolved by Étienne in [P12], so we first present his generalisation before explaining the resulting algorithms. For this purpose, we will apply some more representation-theoretic massage. The following terminology is convenient.

DEFINITION 8.11. Let G be a finite group and let V, W be $\mathbb{Q}[G]$-modules. We say that V *covers* W, written $V \succ W$, if

$$V \cdot \mathrm{Hom}_{\mathbb{Q}[G]}(V, W) = W,$$

where the left hand side means $\sum_{f \in \mathrm{Hom}_{\mathbb{Q}[G]}(V,W)} f(V)$.

The relation $\succ$ is transitive, and we have the following easy characterisation (see also [CR81, Lemma 37.10]).

PROPOSITION 8.12. *Let G be a finite group and let V, W be finitely generated $\mathbb{Q}[G]$-modules. The following are equivalent.*

1. *$V \succ W$;*
2. *there exists $n \geq 0$ and a surjection of $\mathbb{Q}[G]$-modules $V^n \to W$;*
3. *for every simple $\mathbb{Q}[G]$-module π, we have*

$$\mathrm{Hom}_{\mathbb{Q}[G]}(\pi, W) \neq 0 \Longrightarrow \mathrm{Hom}_{\mathbb{Q}[G]}(\pi, V) \neq 0.$$

From Proposition 8.8 we obtain another characterisation of the existence of norm relations.

COROLLARY 8.13. *Let G be a finite group and $\mathcal{U}$ a set of nontrivial subgroups of G. Define the G-set $X = \bigsqcup_{U \in \mathcal{U}} G/U$. Then there exists a norm relation with respect to $\mathcal{U}$ if and only if $\mathbb{Q}[X] \succ \mathbb{Q}[G]$.*

This motivates the following definition.

DEFINITION 8.14. Let G be a finite group, $H \leq G$ a subgroup and $\mathcal{U}$ a set of subgroups of G. Define the G-set $X = \bigsqcup_{U \in \mathcal{U}} G/U$. We say that G *admits a norm relation with respect to* $(\mathcal{U}, H)$ if

$$\mathbb{Q}[X] \succ \mathbb{Q}[G/H].$$

In [P12], Étienne proves an analogue of Proposition 8.8 in this setting, and gives an equivalent definition with norm elements. However, in my opinion, his work shows that this is really the correct definition (and maybe that the "norm relation" terminology should be replaced).

It would be very nice to have an analogue of Theorem 8.9 for this generalised setting. However, the extra dependence on H makes the existence a simple criterion unlikely, in addition to the fact that such relations are mostly useful when the index of all subgroups $U \in \mathcal{U}$ is smaller than that of H. On the other hand, Brauer relations are completely classified [BD15,BD14], so maybe we should instead hope for a general classification.

QUESTION 8.15. Can one classify (in a sense to be defined) norm relations in the sense of Definition 8.14?

The integer d in (8.2) controls which d-th roots will be needed, and more generally how much information is lost by using a norm relation and needs to be recovered. It is therefore important to give bounds on this number. In the original setting, we proved that one can always

take $d \mid (\#G)^3$ [P5, Theorem 2.20]. In the general setting, we have the following result.

THEOREM 8.16 (Theorem 2.16 in [P12]). *Let G be a finite group, $H \leq G$ a subgroup and $\mathcal{U}$ a set of subgroups of G, and assume that G admits a norm relation with respect to $(\mathcal{U}, H)$. Then there exists $n \geq 0$ and Hecke operators*

$$T\colon \mathbb{Z}[X]^n \to \mathbb{Z}[G/H] \text{ and } T'\colon \mathbb{Z}[G/H] \to \mathbb{Z}[X]^n$$

such that $T \circ T' = d\,\mathrm{Id}$ where $d \in \mathbb{Z}$ divides $(\#G)^2$.

PROOF SKETCH. The existence of d without the divisibility property follows from the fact that $\mathbb{Q}[G]$-modules are semisimple, so that one can construct a right inverse of T. The divisibility property is local, so we can work with $\mathbb{Z}_p[G]$-modules. Since maximal orders over $\mathbb{Z}_p$ behave almost like semisimple algebras, we would get a right inverse for lattices over such an order. Taking into account the discrepancy between $\mathbb{Z}_p[G]$ and a maximal order yields the $(\#G)^2$ factor. □

Now we can generalise Lemma 8.7.

LEMMA 8.17. *Let G be a finite group and W a $\mathbb{Z}[G]$-module, and let X, Y be G-sets. Assume that there exists Hecke operators*

$$T\colon \mathbb{Z}[X] \to \mathbb{Z}[Y] \text{ and } T'\colon \mathbb{Z}[Y] \to \mathbb{Z}[X]$$

such that $T \circ T' = d\,\mathrm{Id}$ where $d \in \mathbb{Z}_{>0}$. Then the exponent of the quotient $W^Y/T(W^X)$ is finite and divides d.

PROOF. Let $w \in W^Y$. Then

$$d \cdot w = T(T'(w)) \in T(W^X).$$

□

8.3. Algorithms. In order to make use of this tool in the context of class groups, we need to be able to detect d-th powers efficiently. There is a standard method for doing this (known as Adleman's characters [Adl91] in the context of the number field sieve), namely reducing modulo prime ideals $\mathfrak{p}$ and using explicit maps $\mathbb{F}_\mathfrak{p}^\times/(\mathbb{F}_\mathfrak{p}^\times)^d \to \mathbb{Z}/d\mathbb{Z}$: if an element is a d-th power then it must be in the kernel of all those maps. A common heuristic is that if you use enough prime ideals, then d-th powers will be correctly detected. Whether this is the case when you use all prime ideals is the topic of the Grunwald–Wang theorem [AT09, Chapter X]. In order to obtain a fully proven algorithm, we proved an effective version of the Grunwald–Wang theorem.

THEOREM 8.18 (Theorem 4.11 in [P5]). *Assume GRH.*

Let $d = p^r$ with p prime number and $r \geq 1$. Let F be a number field of degree n, and $L = F(\zeta_d)$. Let $\mathcal{S}$ be a finite set of prime ideals of F, let $M_\mathcal{S} = \prod_{\mathfrak{p}\in\mathcal{S}} \mathrm{N}(\mathfrak{p})$, and let $\mathcal{S}_p = \mathcal{S} \cup \{\mathfrak{p} \mid p\}$. Let

$$c_0 = 18d^2 \left(2\log|\Delta_F| + 6n\log d + \log M_\mathcal{S}\right)^2.$$

Let $\mathcal{T}$ be the set of prime ideals $\mathfrak{p}$ of F such that

- $\mathfrak{p} \notin \mathcal{S}_p$,
- $\mathfrak{p}$ *has residue degree* 1,
- $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod p$, *and*
- $\mathrm{N}(\mathfrak{p}) \leq c_0$.

Let $\alpha \in F^\times$ be such that all the valuations of α at prime ideals $\mathfrak{p} \notin \mathcal{S}_p$ are divisible by d and such that for every $\mathfrak{p} \in \mathcal{T}$, the image of α in $F_\mathfrak{p}^\times$ is a d-th power. Then $\alpha \in (L^\times)^d$. If in addition L/F is cyclic, then $\alpha \in (F^\times)^d$.

Proof sketch. In L, studying whether α is a d-th power amounts to studying the behaviour of the abelian extension $L(\alpha^{1/d})/L$. After bounding the conductor of this extension, the first part of the result is reduced to bounding the first prime ideal $\mathfrak{P}$ such that $\chi(\mathfrak{P}) \neq 1$ for ray class group characters χ, for which we use [Bac90].

In the second part one needs to descend from L to F. Since L/F is also abelian, the usual proof of the Grunwald–Wang theorem can be made effective in the same way. This step is rather subtle: it is the step where the original version of our theorem was incorrect, so that we had to publish an erratum. □

The final ingredient we need for the algorithm is an efficient way to compute the action of Hecke operators. This was not necessary in [P5] since we only used subfields, in other words the only Hecke operators that appeared were the inclusion maps and the action of automorphisms, but it is necessary in the general case. Étienne solved this by working out a beautiful interpretation of Hecke operators in terms of compositums (see also Section 2.4).

Proposition 8.19 (Proposition 1.13 and Theorem 1.18 in [P12]). *Let F, L be subfields of a Galois field $\widetilde{F}$ with Galois group G, respectively fixed by subgroups H, U of G. There is a natural bijection*

$$U\backslash G/H \longleftrightarrow \{\textit{compositums } C \textit{ of } F \textit{ and } L\}$$

such that for every $HgU \in U\backslash G/H$ with corresponding compositum C, the action of the Hecke operator

$$T = T_{UgH} \colon L^\times = (\widetilde{F}^\times)^U \longrightarrow F^\times = (\widetilde{F}^\times)^H$$

is given by

$$T(x) = \mathrm{N}_{C/F}(\iota(x))$$

where $\iota \colon L \hookrightarrow C$ is the structural inclusion map.

We will write T_C the Hecke operator corresponding to the compositum C. The point of this interpretation is that since every compositum of F and L is a quotient of $F \otimes L$, it has degree bounded by $[F : \mathbb{Q}][L : \mathbb{Q}]$, which is small enough to allow for polynomial time

algorithms. We can finally describe the main algorithm of this work; it is a generalisation of [P5, Algorithm 4.16].

ALGORITHM 8.20 (Algorithm 4.3 in [P12]). Assume that the finite group G admits a norm relation with respect to a pair $(\mathcal{U}, H)$.

- Input: a number field F, a finite set of prime numbers $\mathcal{S}$, and for each $U \in \mathcal{U}$, the field $L = \widetilde{F}^U$ and a $\mathbb{Z}$-basis B_L of $\mathbb{Z}_{L,\mathcal{S}}^\times$.
- Output: a $\mathbb{Z}$-basis of $\mathbb{Z}_{F,\mathcal{S}}^\times$.

(1) Let $B = \bigcup_L \bigcup_C T_C(B_L)$ where C ranges over compositums of F and L.
(2) Let $\Lambda \subset \mathbb{Z}_{F,\mathcal{S}}^\times$ be the subgroup generated by B.
(3) For prime $p = 2$ to n:
  (a) $v \leftarrow 2 \cdot \lfloor \frac{n}{p-1} \rfloor$
  (b) $\Lambda_p \leftarrow \Lambda$.
  (c) Repeat v times: $\Lambda_p \leftarrow \Lambda_p \cdot (\Lambda_p \cap (F^\times)^p)^{1/p}$.
(4) $\Lambda \leftarrow \prod_{2 \le p \le n} \Lambda_p$ (product in $\mathbb{Z}_{F,\mathcal{S}}^\times$).
(5) Return a basis of Λ.

The results collected above (Lemma 8.17, Theorem 8.18, and Proposition 8.19) allowed us to prove that this algorithm runs in polynomial time.

THEOREM 8.21 (Theorem 4.4 in [P12], generalising Theorem 4.18 in [P5]). *Assume GRH. Let G be a finite group, $H \subset G$ a subgroup, and $\mathcal{U}$ a set of subgroups of G. Assume that the group G admits a norm relation with respect to a pair $(\mathcal{U}, H)$. Then Algorithm 8.20 is a deterministic polynomial time algorithm that, on input of*

- *a number field F whose Galois closure has Galois group G,*
- *a finite set of prime numbers $\mathcal{S}$,*
- *for each $U \in \mathcal{U}$, the field $L = \widetilde{F}^U$ and a $\mathbb{Z}$-basis B_L of $\mathbb{Z}_{L,\mathcal{S}}^\times$,*

returns a $\mathbb{Z}$-basis of $\mathbb{Z}_{F,\mathcal{S}}^\times$.

This gives a satisfactory answer to Problem 3.2 and Question 3.4 when the method applies. In most applications, we know the auxiliary fields L because of the structure of the original problem. However, from a theoretical point of view, it is frustrating that we do not know how to compute these fields efficiently (recall that we do not know how to compute the Galois group of the Galois closure in polynomial time).

QUESTION 8.22. Can one determine the existence of a norm relation and compute the auxiliary fields L from the data of F only in polynomial time?

From the group of $\mathcal{S}$-units where $\mathcal{S}$ is taken large enough to generate the class group, we can obtain $\mathrm{Cl}(F)$. We have implemented this algorithm and it beats Buchmann's algorithm in many cases, but we can do even better: we can take shortcuts as long as we can certify the

result in the end. This is what I did in my GP implementation [P6]; which is restricted to the abelian case, enabling a more detailed analysis and in particular the determination of optimal relations to be used [P5, Theorem 2.28]. The algorithm is described in detail in [P5, Algorithm 4.23] and also allows for unconditional computations using [P5, Proposition 4.28]. Before giving examples of computations performed with this implementation, let us examine the gain in time complexity that we can hope for with these techniques. The complexity of usual techniques (for fixed root discriminant) in terms of the degree n is approximately

$$\exp(c \cdot n^{\alpha})$$

where c is constant, $0 < \alpha < 1$ for computations under GRH, and $\alpha = 1$ for unconditional computations.

For the sake of comparison, implementations of Buchmann's algorithm conditional on GRH are currently able to compute class groups of number fields of degree slightly above 100.

EXAMPLE 8.23. Let $F = \mathbb{Q}(\zeta_{6552})$ which has Galois group over $\mathbb{Q}$ isomorphic to $C_{12} \times C_6^2 \times C_2^2$, degree 1728 and discriminant $2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$. Our GP implementation computes in 4.2 hours on a laptop that, assuming GRH, the class group of F is isomorphic to

$$\begin{aligned}
&C_e \times C_{1239033466476506902449634984179843551476216834003 20} \\
&\times C_{582777587574759236929319232 0} \times C_{2098524198141572423040} \\
&\times C_{33847164486154393920} \times C_{7383876252480} \times C_{101148989760}^2 \\
&\times C_{50574494880}^2 \times C_{276363360}^5 \times C_{7469280}^2 \times C_{3734640}^8 \times C_{196560}^2 \\
&\times C_{98280} \times C_{32760}^4 \times C_{6552}^{26} \times C_{3276}^2 \times C_{252} \times C_{84}^3 \times C_{12}^{29} \times C_6^8 \times C_2^{11}
\end{aligned}$$

where

$$\begin{aligned}
e \;=\; & 3493800297067370591042482235653196928838975486383928 5 \\
& 6641627842662891732318286799812329621077189995594165 7 \\
& 4436185909021455016573455555887058972994901315067596 8 \\
& 232635365760,
\end{aligned}$$

and that $h_{6552}^{+} = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13$. Our algorithm uses a relation with $d = 1$ involving 62 subfields of degree at most 192. The computations in those subfields recursively uses relations with d supported at a single prime (2 or 3), involving a total of 672 subfields of degree at most 12.

Finally, we certified some new values of class numbers of cyclotomic fields.

THEOREM 8.24 (Theorem 4.29 in [P5]). *The class numbers and class groups in Table 1 are correct.*

TABLE 1. Class numbers of cyclotomic fields $\mathbb{Q}(\zeta_f)$

f conductor, $\varphi(f)$ degree, h^+ plus part of class number, r_2 2-rank of class group, r_3 3-rank of class group, T_1 time for the conditional computation, T_2 time to unconditionally certify the computation.

f	$\varphi(f)$	h^+	r_2	r_3	T_1	T_2	f	$\varphi(f)$	h^+	r_2	r_3	T_1	T_2
255	128	1	1	1	1 min	3 h	624	192	1	3	4	2.5 min	28 min
272	128	2	4	2	1 min	8 h	720	192	1	3	4	2.5 min	24 min
320	128	1	0	2	25 s	13 h	780	192	1	18	1	6.5 min	6.5 min
340	128	1	3	0	1 min	8 h	840	192	1	6	4	6 min	2 min
408	128	2	5	2	3 min	21 min	455	288	1	14	3	4 min	9 h
480	128	1	3	4	43 s	4 s	585	288	1	7	4	4 min	10.5 h
273	144	1	9	2	34 s	5.5 min	728	288	20	17	14	3 min	2 h
315	144	1	4	2	20 s	4.5 min	936	288	16	11	11	2.5 min	2.5 h
364	144	1	6	5	25 s	11 min	1008	288	16	13	10	2.5 min	5.5 h
456	144	1	1	3	1.5 min	8 h	1092	288	1	24	7	3 min	1 h
468	144	1	3	6	25 s	12 min	1260	288	1	14	7	2.5 min	2 h
504	144	4	9	6	16 s	2 s	1560	384	8	40	5	2 h	3.5 h
520	192	4	18	3	6.5 min	16 min	1680	384	1	12	8	1 h	8 h
560	192	1	3	5	2.5 min	18 min	2520	576	208	38	15	40 min	43 h

In order to keep the table small, we did not include fields for which the class number was already known unconditionally. According to Miller [Mil14], the largest conductor for which the class number of a cyclotomic field has been computed unconditionally was 420 prior to our work; we raise this record to 2520. Note that our methods are not restricted to cyclotomic fields, but these number fields provide a family of examples to which they often apply and that are of general interest. Our proof of Theorem 8.24 does not use special properties of cyclotomic fields other than their Galois group; it would be interesting to combine them with special cyclotomic techniques.

9. Computing Selmer groups

Let $\mathbb{G}$ be a commutative algebraic group over a field F of characteristic 0. We also denote $\mathbb{G}$ the $\mathcal{G}_F$-module $\mathbb{G}(\bar{F})$. Let $n \in \mathbb{Z}_{\geq 2}$, and assume that multiplication by n is surjective on $\mathbb{G}$. The short exact sequence of $\mathcal{G}_F$-modules

$$1 \longrightarrow \mathbb{G}[n] \longrightarrow \mathbb{G} \xrightarrow{[n]} \mathbb{G} \longrightarrow 1$$

induces the Kummer exact sequence

$$1 \longrightarrow \mathbb{G}(F)/[n]\mathbb{G}(F) \longrightarrow H^1(F, \mathbb{G}[n]) \to H^1(F, \mathbb{G}). \tag{9.1}$$

There are two important families of connected such $\mathbb{G}$:

- tori, which are affine, and

- abelian varieties, which are projective.

There are important differences in the behaviour of (9.1) in these two cases. For instance, consider the case of a quasi-split torus, i.e. $\mathbb{G} = \mathrm{Res}_{L/F}\,\mathbb{G}_{\mathrm{m}}$ for some finite extension L/F. Then

$$H^1(F,\mathbb{G}) = H^1(F,\mathrm{Res}_{L/F}\,\mathbb{G}_{\mathrm{m}}) = H^1(L,\mathbb{G}_{\mathrm{m}}) = 1$$

by Hilbert's Theorem 90, and $\mathbb{G}(F) = L^\times$. The Kummer sequence therefore becomes an isomorphism

$$H^1(F,\mathbb{G}[n]) \cong L^\times/(L^\times)^n.$$

Algorithmically, this manifests itself by the fact that we can use the rational points $\mathbb{G}(F)$ to get a grasp on $H^1(F,\mathbb{G}[n])$.

On the other hand, consider the case where $\mathbb{G}$ is an abelian variety and F a number field. Then the Kummer map is not surjective, and one adds further local restrictions to get instead an embedding into a Selmer group

$$1 \longrightarrow \mathbb{G}(F)/[n]\mathbb{G}(F) \longrightarrow H^1_{\mathcal{F}}(F,\mathbb{G}[n]).$$

Algorithmically, we now use the Selmer group $H^1_{\mathcal{F}}(F,\mathbb{G}[n])$ to get a grasp on the group $\mathbb{G}(F)$ of rational points. The reason we are able to compute $H^1_{\mathcal{F}}(F,\mathbb{G}[n])$ is that since $\mathbb{G}[n]$ is finite, we can relate it to the easier case of tori. The general idea of the present work is to apply this strategy to Selmer groups of arbitrary finite $\mathcal{G}_F$-modules.

In the rest of this section, F will be a number field and W a finite $\mathcal{G}_F$-module. There are various notions of duality for Galois modules; we need the following one.

Definition 9.1. The *dual* V^* of a $\mathcal{G}_F$-module V is [5]

$$V^* = \mathrm{Hom}(V,\bar{F}^\times).$$

Example 9.2. Let $n \geq 1$ be such that $W = W[n]$. Then

$$W^* = \mathrm{Hom}(W,\bar{F}^\times) = \mathrm{Hom}(W,\mu_n),$$

so W^* is the usual linear dual $\mathrm{Hom}(W,\mathbb{Z}/n\mathbb{Z})$ with the Galois action twisted by the mod n cyclotomic character.

Example 9.3. Let L/F be a finite extension and let $P = \mathbb{Z}[\mathcal{G}_F/\mathcal{G}_L]$ be the corresponding permutation module. Then

$$(P^*)^{\mathcal{G}_F} = \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}_F]}(\mathbb{Z}[\mathcal{G}_F/\mathcal{G}_L],\bar{F}^\times) = (\bar{F}^\times)^{\mathcal{G}_L} = L^\times.$$

More generally, let X be a finite $\mathcal{G}_F$-set and let $P = \mathbb{Z}[X]$ be the corresponding permutation module. Then

$$(P^*)^{\mathcal{G}_F} = \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}_F]}(\mathbb{Z}[X],\bar{F}^\times) = (\bar{F}^\times)^X = (\bar{F}^X)^\times,$$

and P^* is the quasi-split torus corresponding to X.

[5] From the point of view of group schemes, this is the Cartier dual.

The textbook way of defining group cohomology is to take a free resolution, then fixed points, and finally the homology of the resulting complex. Free modules over an absolute Galois group are not computationally tractable, but as we will see, a resolution by quasi-split tori is sufficient. Assume that we have a resolution of W^* by permutation modules, i.e. an exact sequence

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow W^* \longrightarrow 1$$

where $P_i = \mathbb{Z}[X_i]$ is the permutation module associated with a finite $\mathcal{G}_F$-set X_i. Taking duals, we obtain a resolution

$$1 \longrightarrow W \longrightarrow I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \cdots$$

where $I_i = P_i^*$ is the quasi-split torus corresponding to X_i. Denote $L_i = \bar{F}^{X_i}$ the corresponding étale algebra. The vanishing of $H^1(F, I_0)$ implies the following.

Proposition 9.4 (Proposition 2.4 in [P13]). *We have*

$$H^1(F, W) \cong \frac{\ker(L_1^\times \to L_2^\times)}{\mathrm{im}(L_0^\times \to L_1^\times)}.$$

In other words, $H^1(F, W)$ is the H^1 of the complex

$$1 \longrightarrow L_0^\times \longrightarrow L_1^\times \longrightarrow L_2^\times \longrightarrow \cdots$$

Example 9.5. Let $W = \mu_n$. Then $W^* = \mathbb{Z}/n\mathbb{Z}$. We have the resolution

$$1 \longrightarrow \mathbb{Z} \xrightarrow{[n]} \mathbb{Z} \longrightarrow W^* \longrightarrow 1$$

by the permutation modules with $X_0 = X_1 = \{\cdot\}$ and $X_2 = \emptyset$. The isomorphism of Proposition 9.4 becomes

$$H^1(F, \mu_n) \cong \frac{\ker(F^\times \to 1)}{\mathrm{im}(F^\times \xrightarrow{[n]} F^\times)} = F^\times/(F^\times)^n,$$

which is the usual description of this cohomology group.

A resolution by permutation modules always exists and can be computed easily as follows (see [P13, Algorithm 4.2]). Let V be an arbitrary finitely generated discrete $\mathbb{Z}[\mathcal{G}_F]$-module and let $B \subset V$ be a finite subset. Then the orbit $X = \mathcal{G}_F \cdot B$ is a finite $\mathcal{G}_F$-set and we have a natural morphism of $\mathbb{Z}[\mathcal{G}_F]$-modules

$$\mathbb{Z}[X] \to V$$

extending the inclusion $X \subset V$. If we take B to be a generating set of V, then the resulting morphism $\mathbb{Z}[X] \to V$ is surjective. Applying this to $V = W^*$ we get $X = X_0$, then to $V = \ker(\mathbb{Z}[X_0] \to W^*)$ we get $X = X_1$, etc. In addition, the maps appearing in Proposition 9.4 are Hecke operators that can be computed via compositums by Proposition 8.19.

Now that we have a nice representation of the full cohomology group $H^1(F,W)$, we want to find Selmer groups inside. This is done by replacing the full multiplicative groups by $\mathcal{S}$-units.

DEFINITION 9.6 (Definition 3.1 in [P13]). Let $\mathcal{S}$ be a finite set of prime numbers. Define

$$H^1_{\mathcal{S}}(F,W) = \frac{\ker(\mathbb{Z}^\times_{L_1,\mathcal{S}} \to \mathbb{Z}^\times_{L_2,\mathcal{S}})}{\mathrm{im}(\mathbb{Z}^\times_{L_0,\mathcal{S}} \to \mathbb{Z}^\times_{L_1,\mathcal{S}})}.$$

The isomorphism of Proposition 9.4 is compatible with restriction maps: if L/F is an extension, we get an induced morphism $\mathcal{G}_L \to \mathcal{G}_F$ and a corresponding restriction map

$$H^1(F,W) \to H^1(L,W),$$

and the isomorphism is compatible with the natural maps

$$L_i^\times \to (L_i \otimes_F L)^\times.$$

This compatibility in the special cases F_v/F and F_v^{ur}/F_v, and the ramification properties of Kummer extensions allowed Étienne to prove the following result.

PROPOSITION 9.7 (Propositions 3.7 and 3.8 in [P13]). *Assume that the set $\mathcal{S}$ contains all prime divisors of $\#W$ and that $\mathrm{Cl}(L_0)$ is generated by the set of prime ideals of L_0 above primes in $\mathcal{S}$. Define a Selmer structure $\mathcal{F}$ by*

- *$\mathcal{F}_v = H^1(F_v,W)$ for v above a prime in $\mathcal{S}$, and*
- *$\mathcal{F}_v = H^1_{\mathrm{ur}}(F_v,W)$ otherwise.*

Then we have an isomorphism

$$H^1_{\mathcal{F}}(F,W) \cong H^1_{\mathcal{S}}(F,W).$$

This immediately yields the following algorithm to compute arbitrary Selmer groups.

ALGORITHM 9.8.

- Input: étale algebras L_0, L_1, L_2 and Hecke operators giving the initial segment $L_0^\times \to L_1^\times \to L_2^\times$ from a resolution of W, a finite set of primes $\mathcal{S}$ satisfying the hypotheses of Proposition 9.7, for each v above a prime of $\mathcal{S}$, a subgroup $\mathcal{F}_v \subset H^1(F_v,W)$, and a basis of each $\mathbb{Z}^\times_{L_i,\mathcal{S}}$.
- Output: the structure and a basis of the Selmer group $H^1_{\mathcal{F}}(F,W)$ in $H^1(F,W)$.

(1) Compute $H^1_{\mathcal{S}}(F,W)$ by linear algebra.
(2) Compute the kernel H of the map

$$H^1_{\mathcal{S}}(F,W) \to \bigoplus_{v|p\in\mathcal{S}} \frac{H^1(F_v,W)}{\mathcal{F}_v}$$

by linear algebra.

(3) Return H.

This reduces the computation of arbitrary Selmer groups to the problem of computing units and class groups in the number fields appearing in the resolution. In fact, with a bit of care we can avoid computing them in L_2.

Selmer groups are so important that I think an implementation of such a general algorithm would be very useful. Due to lack of time, we have not implemented our algorithms yet. However, I think it could be worth trying to improve the algorithms before implementing them. Indeed, let us think about the algebras L_i for $W = \mathbb{F}_p^2$ and where the Galois image is the full $\mathrm{GL}_2(\mathbb{F}_p)$. Then L_0 will be a field of degree $p^2 - 1 \approx p^2$ over F, and L_1 will be the full Galois closure of L_0/F, of degree $\approx p^4$. We can use norm relations to ease the computation of the class group and units of this field: this reduces the problem to fields of degree $\approx p^3$, but it would be better if L_0 were sufficient. I believe that this should be possible, by using a resolution by permutation modules over $\mathbb{Z}/n\mathbb{Z}$ instead of $\mathbb{Z}$ (where W has exponent n); the dual resolution will then have pieces of the form $\mathrm{Res}_{L/F}\,\mu_n$. Tracking the exact sequences becomes more complicated, but apart from parasite terms, it relates $H^1(F, W)$ to $L_0^\times/(L_0^\times)^n$, and hopefully a Selmer group can be extracted from $\mathcal{S}$-units in L_0.

Part 3

Hecke operators and isogenies

10. Reconstructing isogenies

A landmark in the algorithmic theory of elliptic curves over finite fields was Schoof's polynomial time point counting algorithm [Sch85, Sch95]: his idea was to compute the trace of the Frobenius endomorphism $\pi \in \mathrm{End}(E)$ by computing its action on $E[\ell]$ for many small primes ℓ. The algorithm was improved by Elkies and Atkin, leading to a practical algorithm known as the SEA algorithm. Elkies's improvement [Elk98] decreases the asymptotic complexity as follows: if ℓ is chosen such that E admits a rational ℓ-isogeny φ, then we can compute the action of π on the kernel $E[\varphi]$ instead, decreasing the degree of the polynomials involved. However, while it is easy to detect whether E admits an ℓ-isogeny with modular polynomials, it is a non-trivial task to compute the kernel $E[\varphi]$, or equivalently to compute the isogeny $\varphi\colon E \to E'$: this is Elkies's *isogeny reconstruction algorithm*, at the heart of Elkies's improvement. Schoof's algorithm was generalised to genus 2 curves [GS12,GKS11,BGLG$^+$17], but not Elkies's improvement, due to the lack of an isogeny reconstruction algorithm. The goal of our work [P4] is to describe such an algorithm.

10.1. Elkies's algorithm. We first recall Elkies's isogeny reconstruction algorithm [Elk98, Section 3] (see also [Sch95, Section 7]). For simplicity we assume that we are working over a field of large enough characteristic. We are given an integer $\ell \geq 2$ and two elliptic curves E, E' such that there exists an ℓ-isogeny $\varphi\colon E \to E'$. The first remark is that the curves are given by Weierstrass equations

$$E : y^2 = x^3 + Ax + B$$

and similarly for E'. However, such equations are not unique; we can make a change of variables $(x, y) \mapsto (x/u^2, y/u^3)$, which changes (A, B) to (u^4A, u^6B). In order to reconstruct the map $E \to E'$, we would like to fix a particular equation. Note that a choice of equation determines a basis of the 1-forms on E, namely $\omega = \frac{dx}{y}$ and similarly ω' on E'. The isogeny φ induces a linear map between the 1-dimensional spaces of 1-forms, so there exists a constant c such that $\varphi^*\omega' = c\omega$. Elkies calls the isogeny *normalised* if $c = 1$, i.e. if $\varphi^*\omega' = \omega$. There is always a Weierstrass equation for E' making the isogeny normalised, and we would like to find this equation. Elkies's idea is to use *derivatives* of modular functions. First note that for $\tau \in \mathcal{H}^2$, the standard elliptic curve $E(\tau) = \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ has equation

$$y^2 = x^3 - \frac{E_4(\tau)}{48}x + \frac{E_6(\tau)}{864}.$$

Define, for $\tau \in \mathcal{H}^2$,

$$j'(\tau) = \frac{1}{2\pi i}\frac{\partial}{\partial \tau}j(\tau) = q\frac{\partial}{\partial q}j(q).$$

Then j' is a weakly modular function of weight 2, and we have

$$\frac{j'(\tau)}{j(\tau)} = -\frac{E_6(\tau)}{E_4(\tau)}.$$

Algebraically, j depends only on E but j' depends on a pair (E, ω), i.e. on a curve equation; we will write $j(E)$ and $j'(E, \omega)$. We have

$$\frac{j'(E,\omega)}{j(E)} = -\frac{E_6(E,\omega)}{E_4(E,\omega)}.$$

From this identity, we see that if we know $j(E)$ and $j'(E, \omega)$, then we can write a Weierstrass equation for (E, ω), and conversely. Now enter the modular polynomial. We have

$$\Phi_\ell(j(\tau), j(\ell\tau)) = 0,$$

and by differentiating we obtain

$$j'(\tau)\frac{\partial}{\partial X}\Phi_\ell(j(\tau), j(\ell\tau)) + \ell j'(\ell\tau)\frac{\partial}{\partial Y}\Phi_\ell(j(\tau), j(\ell\tau)) = 0.$$

Since the standard isogeny $E(\tau) \to E(\ell\tau)$ is normalised, and by a lifting argument, we also have algebraically

(10.1)

$$j'(E,\omega)\frac{\partial}{\partial X}\Phi_\ell(j(E), j(E')) + \ell j'(E',\omega')\frac{\partial}{\partial Y}\Phi_\ell(j(E), j(E')) = 0,$$

whenever the ℓ-isogeny $\varphi\colon (E, \omega) \to (E', \omega')$ is normalised. Now, if we fix a Weierstrass equation for E, this determines (E, ω) and therefore $j'(E, \omega)$, and from Equation (10.1) we obtain $j'(E', \omega')$ (unless the partial derivative vanishes, which is generically not the case) and from there we obtain a normalised equation for E'.

Finally, the normalisation identity $\varphi^*\omega' = \omega$ gives a differential equation satisfied by the expression of φ in terms of a local parameter at 0 on E; solving this differential equation yields a power series that may be reconstructed into a rational expression for the isogeny φ.

10.2. Isogeny reconstruction and Hecke correspondences. We propose the following reformulation of Elkies's algorithm. Consider the moduli space $\mathcal{A}_g$ of principally polarised abelian varieties A of dimension g, and $\mathcal{A}_g(\ell)$ be the corresponding moduli space with level structure given by a kernel C of an ℓ-isogeny from A (they are both arithmetic orbifolds for Sp_{2g} as in Section 4.2). We have a map

$$\Phi_\ell = (\Phi_{\ell,1}, \Phi_{\ell,2})\colon \mathcal{A}_g(\ell) \to \mathcal{A}_g \times \mathcal{A}_g$$

given by $(A, C) \mapsto (A, A/C)$. The image of Φ_ℓ is the *Hecke correspondence*, the algebraic incarnation of the Hecke operator. Now let $\varphi\colon A \to A'$ be an ℓ-isogeny, so that there is a corresponding point on $\mathcal{A}_g(\ell)$, and $(A, A') \in \mathcal{A}_g \times \mathcal{A}_g$ lies on the Hecke correspondence.

The problem of finding a normalised form of the isogeny amounts to understanding the *tangent map*

$$d\varphi\colon T_0(A) \to T_0(A')$$

of the isogeny $\varphi\colon A \to A'$. For instance, we would like to know its matrix on fixed bases of $T_0(A)$ and $T_0(A')$. On the other hand, we have a more direct access to the *deformation map*

$$\mathcal{D}(\varphi)\colon T_A(\mathcal{A}_g) \longrightarrow T_{A'}(\mathcal{A}_g)$$

defined by $d\Phi_{\ell,2} \circ d\Phi_{\ell,1}^{-1}$ (in other words, the derivative of the Hecke operator $\mathcal{A}_g \to \mathcal{A}_g$ locally around $A \mapsto A'$). The crucial point is that there is a close relationship between $d\varphi$ and $\mathcal{D}(\varphi)$.

Before giving the general identity, let us rewrite the dimension 1 case from this point of view. Let $\varphi\colon E \to E'$ be an ℓ-isogeny. Picking bases of the tangent spaces at hand, we have

$$d\varphi = c^{-1} \text{ where } \varphi^*\omega' = c\omega$$

and

$$\mathcal{D}(\varphi) = \frac{\frac{\partial}{\partial Y}\Phi_\ell(j(E), j(E'))}{\frac{\partial}{\partial X}\Phi_\ell(j(E), j(E'))}.$$

Now Equation (10.1) in the case of normalised isogenies becomes, in the general case,

$$\ell\mathcal{D}(\varphi) = -\frac{j'(E,\omega)}{j'(E',\omega')}(d\varphi)^2.$$

This can be generalised using the *Kodaira–Spencer isomorphism* ([KS58], see also [And17, §1.3]), which is a canonical isomorphism

$$T_A(\mathcal{A}_g) \cong \operatorname{Sym}^2 T_0(A).$$

The dimensions nicely match up: $\dim A = g$ and $\dim \mathcal{A}_g = \binom{g}{2}!$ We prove, when we choose the right bases for this isomorphism, the following identity.

Proposition 10.1 (Propositions 3.19 and 4.19 in [P4]). *We have*

$$\operatorname{Sym}^2(d\varphi) = \ell\mathcal{D}(\varphi).$$

As in dimension 1, this is first proved over $\mathbb{C}$, which in turn implies that this is true algebraically; Damien replaced the lifting argument by a nice stacky argument.

This leads to the following Elkies-type meta-algorithm:

(1) Compute the deformation map $\mathcal{D}(\varphi)$ by differentiating modular equations.
(2) Compute the tangent map $d\varphi$ from an explicit version of the Kodaira–Spencer isomorphism.
(3) Compute a power series expansion of φ by solving a differential system in the formal group of A.
(4) Reconstuct φ as a tuple of rational functions.

10.3. Algorithm in genus 2. We turned this meta-algorithm into an actual algorithm (this was Kieffer's work at the beginning of his PhD). The ingredients are as follows.

- A generic abelian surface A is represented as the Jacobian of a genus 2 hyperelliptic curve. A curve equation corresponds to a choice of basis of the 1-forms on A (see [P4, Corollary 3.3]).
- The j-invariant is replaced by Igusa invariants (with Mestre's algorithm [Mes91] to construct a curve from its invariants), and the modular polynomial by 3 modular equations in 4 variables (see [P4, Section 2.6]).
- The explicit Kodaira–Spencer isomorphism is obtained by relating covariants of the curve equation to vector-valued Siegel modular forms; more precisely, Kieffer identified the derivatives of the Igusa invariants as explicit covariants (therefore having an explicit expression in terms of the coefficients of the curve equation): this is [P4, Theorem 3.14].
- The reconstruction via power series is done by restriction to the curve, so that the differential system is still univariate (see [P4, Section 5]). Similar methods appear, also in genus 2, in [CE15] and [CMSV19]. The differential system is solved efficiently by Newton iteration as in [BMSS08].

THEOREM 10.2 (Theorem 1.1 in [P4]). *Let A, A' be generic ℓ-isogenous abelian surfaces over a field of characteristic large enough. Our algorithm [P4, Algorithm 6.1] computes an isogeny $\varphi\colon A \to A'$ as a rational map, using $\tilde{O}(\ell)$ elementary operations, $O(1)$ square roots in an extension of the base field of degree $O(1)$, and $O(1)$ evaluations of the derivatives of the modular equations of level ℓ.*

Returning to the point-counting problem, the current algorithms to evaluate modular polynomials are not good enough for the Elkies-type method to yield faster point-counting on generic genus 2 curves. However, our work also covers the case of Hilbert modular surfaces, and the approach should lead to concrete speedups in the case of genus 2 curves with real multiplication. This is the subject of recent work by Kieffer [Kie20,Kie22].

11. Hardness of isogeny problems

In the context of isogeny based cryptography (see Section 6.3), the isogeny we are looking for have very large degree, which changes the nature of the problem. The relative difficulty of various isogeny problems was studied from a heuristic point of view in [EHL+18]; in particular the relation between OneEnd (Problem 6.13) and EndRing (Problem 6.14). The basic naive idea to reduce EndRing to OneEnd is to call the oracle repeatedly.

Algorithm 11.1. Relative to an oracle $\mathbf{O}_{\text{OneEnd}}$.

- Input: $E \in \mathrm{SS}(p)$
- Output: $\mathrm{End}(E)$

(1) $\Lambda \leftarrow \mathbb{Z}$
(2) While $\Lambda \neq \mathrm{End}(E)$ do $\Lambda \leftarrow \Lambda + \mathbb{Z} \cdot \mathbf{O}_{\text{OneEnd}}(E)$
(3) Return Λ.

Remark 11.2. We can actually test whether Λ equals $\mathrm{End}(E)$: this ring is equipped with a positive definite quadratic form $(\varphi, \psi) \mapsto \mathrm{Tr}(\hat{\varphi}\psi)$ whose discriminant is known; since at every step we have $\Lambda \subset \mathrm{End}(E)$ we have equality if and only if the discriminant is correct.

An immediately visible problem with Algorithm 11.1 is that the output of $\mathbf{O}_{\text{OneEnd}}$ could be constant on E! There is therefore no guarantee that the algorithm will terminate. An simple attempt to fix this problem is to randomise the curve on which the oracle is called, using the property proved by Pizer [Piz90] that the the endpoints of long ℓ-isogeny paths in $\mathrm{SS}(p)$ are almost equidistributed.

Algorithm 11.3. Relative to an oracle $\mathbf{O}_{\text{OneEnd}}$.

- Input: $E \in \mathrm{SS}(p)$
- Output: $\mathrm{End}(E)$

(1) $\Lambda \leftarrow \mathbb{Z}$
(2) While $\Lambda \neq \mathrm{End}(E)$ do
  (a) Let $\varphi\colon E \to E'$ be a long random ℓ-isogeny path.
  (b) $\alpha \leftarrow \mathbf{O}_{\text{OneEnd}}(E')$
  (c) $\Lambda \leftarrow \Lambda + \mathbb{Z} \cdot \hat{\varphi}\alpha\varphi$
(3) Return Λ.

At least Algorithm 11.3 has a chance of producing distinct endomorphisms. In [EHL+18] it was proposed as a heuristic that Algorithm 11.3 quickly terminates. This is however not true: for instance there could exist and integer $N \geq 2$ such that for every $E' \in \mathrm{SS}(p)$, the endomorphism $\mathbf{O}_{\text{OneEnd}}(E')$ belongs to $\mathbb{Z} + N\,\mathrm{End}(E')$. This would force $\Lambda \subset \mathbb{Z} + N\,\mathrm{End}(E)$, so that Algorithm 11.3 would never terminate. We could hope instead (but we would have to prove it!) that Λ always quickly stabilises to some suborder of the form $\mathbb{Z} + N\,\mathrm{End}(E)$; but one can also see that such termination can be made exponentially slow if the oracle uses several different congruences with varying probabilities. In this type of study, one should think of the oracle as being adversarial, forced to give a valid output but doing its best to make our intended use fail!

In order to fix Algorithm 11.3, we have to understand the distribution of the generated endomorphisms.

Question 11.4. What is the distribution of $\hat{\varphi}\alpha\varphi \in \mathrm{End}(E)$, where the φ are random long ℓ-isogeny paths from E to various endpoints E', and $\alpha \in \mathrm{End}(E')$ are drawn from a fixed distribution?

This question seems much too general to have a nice answer. We were however able to obtain sufficient information for our desired application. This required a powerful generalisation of Pizer's theorem, which we developed in [P8], using Deuring's correspondence and relating isogeny walks to properties of Hecke operators on spaces of quaternionic automorphic forms.

Fix a base curve $E_0 \in \mathrm{SS}(p)$, and let $\mathcal{O} = \mathrm{End}(E_0)$ and $B = \mathcal{O} \otimes \mathbb{Q}$. Let $\mathrm{Mod}(\mathcal{O})$ be the category with

- objects: projective right $\mathcal{O}$-modules of rank 1;
- morphisms: right $\mathcal{O}$-module homomorphisms.

We then have the classical Deuring correspondence, formulated categorically (see [Koh96, Theorem 45] and [Voi21, Theorem 42.3.2]).

THEOREM 11.5 (Deuring correspondence). *The associations* $E \mapsto \mathrm{Hom}(E_0, E)$ *and* $(\varphi\colon E \to E') \mapsto (\psi \mapsto \varphi\psi)$ *define an equivalence of categories*

$$\mathrm{SS}(p) \longrightarrow \mathrm{Mod}(\mathcal{O}).$$

Our approach of Question 11.4 consists in seeing each step of the ℓ-isogeny random walk as an operator on the space of distributions on pairs (E', α) with $\alpha \in \mathrm{End}(E')$, modifying the distribution at each step. We found that it was convenient to use the following (simple and classical) categorical construction.

DEFINITION 11.6. Let $\mathcal{C}$ be a category and $\mathcal{F}\colon \mathcal{C} \to \mathrm{Sets}$ be a functor. The *category of elements* $\mathrm{El}(\mathcal{F})$ is the category with

- objects: pairs (c, x) where $c \in \mathcal{C}$ and $x \in \mathcal{F}(c)$;
- morphisms $(c, x) \to (c', x')$: morphisms $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$ such that $\mathcal{F}(f)(x) = x'$.

This captures exactly the intuitive notion of "objects in $\mathcal{C}$ with extra data", where the morphisms from $\mathcal{C}$ can be used to transport this data. However, in most cases not every isogeny can transport the type of data we want, so it is useful to restrict the degrees of isogenies that can appear.

DEFINITION 11.7. Let $\mathcal{S}$ be a set of prime numbers. Let $\mathrm{SS}_{\mathcal{S}}(p)$ denote the category with

- objects: supersingular elliptic curves over $\overline{\mathbb{F}}_p$;
- morphisms $\mathrm{Hom}_{\mathcal{S}}(E, E')$: isogenies with degree a product of the primes in $\mathcal{S}$.

Another important insight is that the sets $\mathrm{End}(E')$ are too large for the relevant distributions to converge (for instance, the degrees of the endomorphisms grow as we transport them). It is however sufficient to collect information about endomorphisms modulo N for various N, leading to the following crucial example.

EXAMPLE 11.8. Let $N \geq 1$ be an integer and let $\mathcal{S}$ be the set of primes not dividing N. Let $\mathrm{End}\,/N$ denote the functor $\mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ defined by

- $(\mathrm{End}\,/N)(E) = \mathrm{End}(E)/N\,\mathrm{End}(E)$;
- for $\varphi\colon E \to E'$, the map $(\mathrm{End}\,/N)(\varphi)$ is $\alpha \mapsto \varphi\alpha\hat{\varphi}$.

Our results are expressed in terms of isogeny graphs of elliptic curves with extra structure. Such graphs have been studied a lot in the context of supersingular isogenies, including with extra structure [Arp24]. However, the graphs were typically considered only had edges corresponding to isogenies of a single degree ℓ. Our graphs include all isogenies together, only keeping the degree as a label; this leads to better structural properties.

DEFINITION 11.9 (Definition 3.4 in [P8]). Let $\mathcal{F}\colon \mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ be a functor with $\mathcal{F}(E)$ finite for all E. We define the graph $\mathbf{G}_{\mathcal{F}}$ with:

- vertices: isomorphism classes of objects in $\mathrm{El}(\mathcal{F})$;
- edges: let $(E, x) \in \mathrm{El}(\mathcal{F})$; edges from (E, x) are isogenies $\varphi \in \mathrm{Hom}_{\mathcal{S}}(E, E')$ modulo automorphisms of $(E', \mathcal{F}(\varphi)(x))$.

Let $L^2(\mathbf{G}_{\mathcal{F}})$ be the space of complex-valued functions on the set of vertices of $\mathbf{G}_{\mathcal{F}}$, and define

$$\langle F, G\rangle = \sum_{(E,x)\in\mathbf{G}_{\mathcal{F}}} \frac{F(E,x)\overline{G(E,x)}}{\#\,\mathrm{Aut}(E,x)} \text{ for } F, G \in L^2(\mathbf{G}_{\mathcal{F}}).$$

For every prime ℓ, we define the adjacency operator A_ℓ on $L^2(\mathbf{G}_{\mathcal{F}})$ by

$$A_\ell F(E,x) = \sum_{(E,x)\to(E',x')} F(E',x'),$$

where the sum runs over edges of degree ℓ leaving (E, x).

In order to relate these graphs to Hecke operators, we introduced the corresponding quaternionic categories, using an adélic formulation. Let $\hat{\mathcal{O}} = \mathcal{O} \otimes \hat{\mathbb{Z}}$ be the profinite completion of $\mathcal{O}$ and $\hat{B} = \hat{\mathcal{O}} \otimes \mathbb{Q}$. For every open subgroup $U \leq \hat{\mathcal{O}}^\times$ we defined a category $\mathrm{Cosets}_{\mathcal{S}}(U)$ [P8, Definition 3.22] in such a way that the associated graph has vertex set the adélic double quotient (see Section 4.2)

$$B^\times \backslash \hat{B}^\times / U,$$

and so that the adjacency operator A_ℓ becomes a Hecke operator. For simplicity of the exposition we do not give the full definition here, but we simply remark that the main difficulty of this part of the work was to find the correct definition of the category $\mathrm{Cosets}_{\mathcal{S}}(U)$.

Not every functor $\mathcal{F}\colon \mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ is related to these adélic categories; we need the following kind of N-adic continuity property.

DEFINITION 11.10 (Definition 3.7 in [P8]). Let $\mathcal{F}\colon \mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ be a functor and $N \geq 1$ an integer. We say that $\mathcal{F}$ *satisfies the* (mod N)*-congruence property* if for every $E \in \mathrm{SS}(p)$ and every $\varphi, \psi \in \mathrm{End}_{\mathcal{S}}(E)$ such that $\varphi - \psi \in N\,\mathrm{End}(E)$, we have $\mathcal{F}(\varphi) = \mathcal{F}(\psi)$.

For instance, it is easy to see that the functor $\mathrm{End}\,/N$ from Example 11.8 has the (mod N)-congruence property. In every example we considered, this property was easy to check. Using this notion, we obtain the following augmented Deuring correspondence.

THEOREM 11.11 (Theorem 3.27 and Proposition 3.24 in [P8]). *Let p be a prime number and let $N \geq 1$ be an integer. Let $\mathcal{S}$ be a set of primes that do not divide N, such that $\mathcal{S}$ contains at least one prime different from p and generates $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $\mathcal{F}\colon \mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ be a functor satisfying the* (mod N)*-congruence property and such that all sets $\mathcal{F}(E)$ are finite. Then there exist open subgroups U_i of $\hat{\mathcal{O}}^\times$ and an equivalence of categories*

$$\mathrm{El}(\mathcal{F}) \longrightarrow \bigsqcup_i \mathrm{Cosets}_{\mathcal{S}}(U_i).$$

PROOF SKETCH. In order to prove this theorem, we first use the classical Deuring correspondence (Theorem 11.5) to replace $\mathcal{F}$ by a functor defined on $\mathrm{Cosets}_{\mathcal{S}}(\hat{\mathcal{O}}^\times)$. We then construct, for each open subgroup $U \leq \hat{\mathcal{O}}^\times$, other such functors $\mathcal{F}_U$ in such a way that $\mathrm{El}(\mathcal{F}_U) \cong \mathrm{Cosets}_{\mathcal{S}}(U)$. This reduces the theorem to proving an isomorphism of functors $\mathcal{F} \cong \bigsqcup_i \mathcal{F}_{U_i}$.

(1) We prove that the congruence property implies that for every morphism f, the map $\mathcal{F}(f)$ is a bijection.
(2) We extend the congruence property to all morphisms (as opposed to only endomorphisms).
(3) We use strong approximation to construct an action of $\hat{B}^\times$ on the disjoint union of all targets of $\mathcal{F}$; the stabilisers of the various orbits under $\hat{\mathcal{O}}^\times$ on one set $\mathcal{F}(x)$ then yield open subgroups $U_i \leq \hat{\mathcal{O}}^\times$.
(4) From this action and careful adélic manipulations, we extend this orbit decomposition to the desired isomorphism of functors.

□

Our augmented Deuring correspondence provides a direct relationship between isogeny graphs with extra structure and quaternionic automorphic forms. From the Jacquet–Langlands correspondence [JL70, Theorem 14.4] and Deligne's bounds on the coefficients of classical modular forms [Del73, Theorem 8.2], we obtained the following general equidistribution theorem.

THEOREM 11.12 (Theorem 3.10 in [P8]). *Let p be a prime number and let $N \geq 1$ be an integer. Let $\mathcal{S}$ be a set of primes that do not divide N, such that $\mathcal{S}$ generates $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $\mathcal{F}\colon \mathrm{SS}_{\mathcal{S}}(p) \to \mathrm{Sets}$ be a functor satisfying the* (mod N)*-congruence property and such that all sets $\mathcal{F}(E)$ are finite.*

Then, for every $\ell \in \mathcal{S}$ different from p, the adjacency operator A_ℓ is a normal operator on $L^2(\mathbf{G}_{\mathcal{F}})$ which stabilises the following subspaces:

- *$L^2_{\deg}(\mathbf{G}_{\mathcal{F}})$, the subspace of functions that are constant on every connected component of the graph $\mathbf{G}^1_{\mathcal{F}}$ obtained from $\mathbf{G}_{\mathcal{F}}$ by keeping only the edges of degree* $1 \bmod N$*. The operator norm of A_ℓ on $L^2_{\deg}(\mathbf{G}_{\mathcal{F}})$ is $\ell + 1$.*
- *$L^2_0(\mathbf{G}_{\mathcal{F}})$, the orthogonal complement of $L^2_{\deg}(\mathbf{G}_{\mathcal{F}})$. The operator norm of A_ℓ on $L^2_0(\mathbf{G}_{\mathcal{F}})$ is at most $2\sqrt{\ell}$.*

In other words, the averaging operator $A'_\ell = \frac{1}{\ell+1}A_\ell$ makes functions rapidly converge to the subspace $L^2_{\deg}(\mathbf{G}_{\mathcal{F}})$, a space that is easy to understand (see [P8, Proposition 3.11]). To see why this is an equidistribution result, one should think of a probability distribution over the vertices of $\mathbf{G}_{\mathcal{F}}$ as being represented by its density function in $L^2(\mathbf{G}_{\mathcal{F}})$: assuming for simplicity that $L^2_{\deg}(\mathbf{G}_{\mathcal{F}})$ only contains constant functions, Theorem 11.12 says that random walks in the graph make any initial distribution converge to the uniform distribution. A similar equidistribution theorem was proved in [CL23], but ours is more flexible.

Applying Theorem 11.12 in the special case of $\mathcal{F} = \mathrm{End}\,/N$, we obtain the following partial answer to Question 11.4.

COROLLARY 11.13 (Theorem 4.2 in [P8]). *Let $N \geq 1$ be an integer. With the notation of Question 11.4, the distribution of $\hat{\varphi}\alpha\varphi$ is almost (with a quantifiable statistical distance) invariant by conjugation under the degree* 1 *subgroup of* $(\mathrm{End}(E)/N\,\mathrm{End}(E))^\times$.

One can even be more precise (see [P8, Sections A.4 and A.5]), but this is sufficient for our application. Note the following additional properties

- The only subgroups of $\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$ containing $\mathbb{Z}$ that are invariant under conjugation by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ are those of the form $\mathbb{Z} + M\,\mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$ for some integer M: this follows from the irreducibility of the adjoint representation of SL_2 over finite fields, together with Nakayama's lemma.
- The fact that Corollary 11.13 holds for all integers contains a statement of independence between the prime factors.

This allowed us to design a version of Algorithm 11.3 that provably works.

ALGORITHM 11.14 (Algorithm 5 in [P8]). Relative to an oracle $\mathbf{O}_{\text{OneEnd}}$.

- Input: $E \in \mathrm{SS}(p)$

- Output: $\mathrm{End}(E)$

(1) $\Lambda \leftarrow \mathbb{Z}$
(2) While $\Lambda \neq \mathrm{End}(E)$ do
  (a) Let $\varphi\colon E \to E'$ be a long random 2-isogeny path.
  (b) $\alpha \leftarrow \mathbf{O}_{\textsc{OneEnd}}(E')$
  (c) $\alpha \leftarrow 2\alpha - \mathrm{Tr}(\alpha)$
  (d) Divide α as much as possible by 2 and by known factors of $\mathrm{disc}(\Lambda)$.
  (e) $\Lambda \leftarrow \Lambda + \mathbb{Z} \cdot \hat{\varphi}\alpha\varphi$
  (f) The first time Λ has rank 4, replace it with its 2-saturation, i.e. the largest $\Lambda \subset \Lambda' \subset \mathrm{End}(E)$ such that $[\Lambda' : \Lambda]$ is a power of 2.
  (g) Update a partial factorisation of $\mathrm{disc}(\Lambda)$.
(3) Return Λ.

Note that Step 2d is nontrivial. The fact that such divisions can be performed efficiently is a byproduct of the attacks on SIDH (see [Rob22]). Our preparatory work yields the following final result.

Theorem 11.15 (Theorem 7.2 of [P8]). *Algorithm 11.14 gives a reduction* EndRing $\leq$ OneEnd.

This result greatly cleaned up the landscape of supersingular isogeny problems. Complemented with variants of the Clapoti algorithm [P9], this lead to a better understanding of many of the problems underlying supersingular isogeny based cryptography; see [MW25] for the most recent such results. A concrete consequence is the following.

Corollary 11.16 (Theorems 8.1 and 8.2 of [P8]). *If* EndRing *is hard, then:*

- *the CGL hash function is collision resistant, and*
- *the* SQISign *identification protocol is sound.*

Another nice consequence is a new unconditional algorithm for solving EndRing, by using a simple birthday paradox algorithm for solving OneEnd.

Corollary 11.17 (Theorem 8.7 of [P8]). *There exists a probabilistic algorithm solving* EndRing *in time* $\tilde{O}(\sqrt{p})$.

Before our work, the best unconditional algorithm was due to Kohel [Koh96, Theorem 75] and was running in time $\tilde{O}(p)$; algorithms with complexity $\tilde{O}(\sqrt{p})$ were known heuristically first, and then under GRH [FIK+25, Theorem 5.5].

Part 4

Hecke operators of arithmetic manifolds

12. Can you hear representation equivalence?

12.1. Vignéras's construction and Hecke operators. Despite the success of Sunada's construction of isospectral manifolds for its flexibility, Vignéras's construction remains of great interest, especially to number theorists. Her construction goes as follows.

Let F be a number field and D a division quaternion division algebra over F. We assume that at least one infinite place of F is unramified in D. Let $\mathcal{O}_1$ be a maximal order in D. The reduced norm induces a bijection between the classes of right $\mathcal{O}_1$-ideals and the ray class group $C = \mathrm{Cl}(\mathfrak{M}_\infty)$ where $\mathfrak{M}_\infty$ is the set of real places of F that ramify in D. This induces a bijection between conjugacy classes of maximal orders and the quotient C_{iso} of C by the classes of squares and of the prime ideals of $\mathbb{Z}_F$ that ramify in D. For each $c \in C_{\mathrm{iso}}$, we choose a maximal order $\mathcal{O}_c$ in the corresponding class and let $\Gamma_c = \mathcal{O}_c^\times/\mathbb{Z}_F^\times$. Let $\mathcal{X} \cong (\mathcal{H}^2)^s \times (\mathcal{H}^3)^{r_2}$ and $G = \mathrm{PGL}_2(\mathbb{R})^s \times \mathrm{PGL}_2(\mathbb{C})^{r_2}$, where s is the number of real places of F that split in D. Finally, for $c \in C_{\mathrm{iso}}$, define the closed orbifold $M_c = \Gamma_c\backslash\mathcal{X}$. Vignéras's theorem [6] is the following.

THEOREM 12.1 (Theorem 7 and Application in [Vig80]). *Assume that at least one prime ideal of $\mathbb{Z}_F$ ramifies in D. Then all the subgroups Γ_c of G are representation equivalent, and all the orbifolds M_c are isospectral.*

There is a visible subtlety: an extra condition is used to ensure the isospectrality of the orbifolds M_c. This condition arises as follows: Vignéras uses the trace formula to relate conjugacy classes in Γ_c to the representation $L^2(\Gamma_c\backslash G)$, and controls the conjugacy classes by studying which quadratic orders $R/\mathbb{Z}_F$ embed in $\mathcal{O}_c$. Vignéras's extra condition ensures that every quadratic order that embeds in some $\mathcal{O}_c$ automatically embeds in all of them. The trace formula has been the main method to study the isospectrality of Vignéras's orbifolds, and this embedding phenomenon was coined *selectivity* (see for instance [CF99,LV15,Lin15] and [Voi21, Chapter 31]). An alternative method was described by Rajan [Raj07], using the Labesse–Langlands multiplicity formula [LL79]. All of these methods either prove representation equivalence or nothing at all, therefore providing no insight into Questions 5.4 and 5.5; and only relate the spectra but not the functions (see Question 5.6).

In [P10], we propose a new perspective on Vignéras's construction, based on Hecke operators. Our isospectrality criteria distinguish between isospectrality, i-isospectrality and representation equivalence. Moreover, our technique also applies to the study of integral homology,

[6] Technically she works with the subgroups of reduced norm 1 instead of the full unit groups.

which was our original motivation. In order to present our method, we restrict to the case $C \cong C_{\text{iso}} \cong C_2$ for simplicity; by class field theory this class group corresponds to a quadratic extension L/F. Consider some finitely generated groups or vector spaces $\mathcal{F}(\Gamma_c)$ attached to the components, which we would like to be isomorphic: $\Omega^i(M_c)_{\Delta=\lambda}$ or $H^i(M_c, W)$ or some isotypical piece of $L^2(\Gamma_c\backslash G)$. Let $C = \{1, c\}$. We would like to exhibit an isomorphism

$$\mathcal{F}(\Gamma_1) \cong \mathcal{F}(\Gamma_c).$$

Our idea is to use the Hecke operators acting on the full arithmetic manifold

$$\mathcal{M} = M_1 \sqcup M_c.$$

These Hecke operators are indexed by prime ideals $\mathfrak{p}$ of $\mathbb{Z}_F$, and their action is compatible with the classes in C: if the class of $\mathfrak{p}$ in C is trivial, then $T_\mathfrak{p}$ stabilises both components and therefore acts on $\mathcal{F}(\Gamma_1)$ and $\mathcal{F}(\Gamma_c)$ separately; if the class of $\mathfrak{p}$ in C is nontrivial, then $T_\mathfrak{p}$ induces maps

$$T_\mathfrak{p} \colon \mathcal{F}(\Gamma_1) \longrightarrow \mathcal{F}(\Gamma_c) \text{ and } T_\mathfrak{p} \colon \mathcal{F}(\Gamma_c) \longrightarrow \mathcal{F}(\Gamma_1).$$

We therefore have a large supply of candidates for isomorphisms. How could these maps all fail to be invertible? One possibility is that there is a single element $v \in \mathcal{F}(\Gamma_1)$ that is annihilated by $T_\mathfrak{p}$ for all $\mathfrak{p}$ that swap the components. A priori invertibility could fail in more complicated ways, but we actually show that this is the only possible obstruction. Writing $\chi \colon C \to \{\pm 1\}$ the nontrivial character, this means that the corresponding system $(a_\mathfrak{p})$ of eigenvalues of Hecke operators satisfies

$$a_\mathfrak{p} = a_\mathfrak{p}\chi(\mathfrak{p}) \text{ for all } \mathfrak{p}.$$

This is reminiscent of CM elliptic curves or modular forms. In the cases of interest for isospectrality, the theory of automorphic induction ([Lan80], see also [GH24, Theorem 13.4.2]) implies that there exists a Hecke character Ψ of L giving rise to the eigenvalues $(a_\mathfrak{p})$. We examine precisely the conditions that must be satisfied by Ψ depending on the particular choice of $\mathcal{F}$ to arrive at our isospectrality criteria. Since the existence of the character Ψ does not necessarily prevent isospectrality but only prevents our method from proving isospectrality, we do not call them "obstruction characters" or "bad characters" but *shady characters*. Our criteria have the following form, for various instanciations of $*$.

THEOREM$\langle * \rangle$ 12.2 (Theorem D in [P10]). *At least one of the following holds:*

(1) *There exists a $*$-shady character of L;*
(2) *Γ_1 and Γ_c are $*$-isospectral.*

There are notions of i-shady character for each $i \geq 0$, and a notion of L^2-shady character, where L^2-isospectrality means representation equivalence. Existence or absence of shady characters can be checked by computation using the algorithms of [P7] that Pascal Molin and I designed and implemented in PARI/GP [The23]. This allowed us to construct interesting examples, which we present in the next sections, by testing many number fields enumerated by Voight for [LV15] and which can be found in the LMFDB [LMF25]. In addition, our Hecke operators realising isospectrality can be seen as transplantation maps, providing another answer to Question 5.6 for Vignéras orbifolds. Our method can be seen as being dual to the trace formula and selectivity method:

- we study the spectrum and identify certain eigenvalues, coming from shady characters, whose absence implies isospectrality;
- with the trace formula, one studies the length spectrum and identifies certain conjugacy classes, coming from selective orders, whose absence implies isospectrality.

It would be interesting to see whether our refined criteria have an equivalent in the language of selectivity.

12.2. Isospectrality and representation equivalence. We apply our criteria to a first example. Let $F = \mathbb{Q}(\alpha)$ where $\alpha^4 - \alpha^3 + \alpha^2 + 4\alpha - 4 = 0$, which is also the field $\mathbb{Q}(\sqrt{-10 - 14\sqrt{5}})$. The field F is the unique number field of discriminant -1375 and signature $(2, 1)$ (LMFDB `4.2.1375.1`). Let D be the unique quaternion division algebra ramified at every real place and no finite place of F. We have $C \cong C_{\mathrm{iso}} \cong C_2$, which therefore has a single non-trivial character χ, corresponding to the quadratic extension $L = F(\zeta_{10})$. Let $C = \{1, c\}$. We have

$$\mathrm{vol}(M_1) = \mathrm{vol}(M_c) = \frac{1375^{3/2}\zeta_F(2)}{2^8\pi^6} = 0.2510654\ldots.$$

The maximal cyclic subgroups of Γ_1 have order 2, 3 or 5, the maximal cyclic subgroups of Γ_c have order 2, 3 or 10, and we have

$$H_1(\Gamma_1, \mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \quad \text{and} \quad H_1(\Gamma_c, \mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

By [LV15, Theorem C], the groups Γ_1 and Γ_c are not representation equivalent. We prove by computation (see [P10, Example 7.4]) that there is no i-shady character of L for any $i \geq 0$. This implies that the orbifolds M_1 and M_c are i-isospectral for all $i \geq 0$.

THEOREM 12.3 (Theorem A in [P10]). *There exists a pair of closed hyperbolic 3-orbifolds with volume* $0.251\ldots$ *that are i-isospectral for all i, but not representation equivalent.*

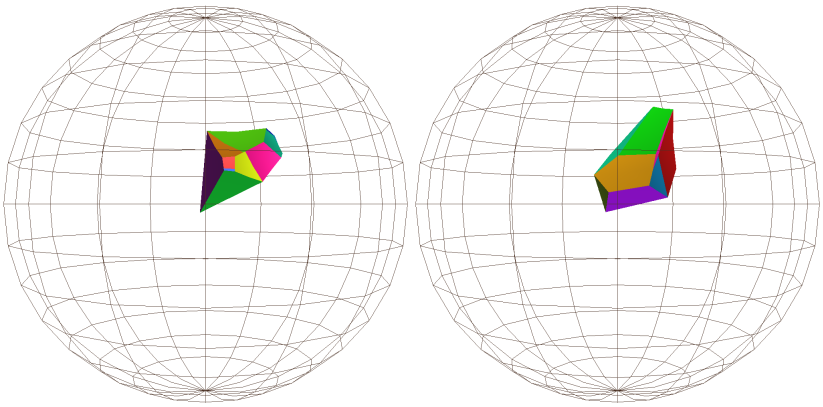

FIGURE 1. Isospectral and 1-isospectral but not representation equivalent 3-orbifolds (volume ≈ 0.251)

This answers Question 5.4 negatively for hyperbolic 3-orbifolds, contrary to the expectation of Doyle and Rossetti. In addition, the volume of this pair is very small, making it a good candidate for Question 5.7 in the case of i-isospectrality for all i. Indeed, as explained in the discussion following this question, the Sunada construction can achieve volume 0.2733 at best. In addition, by [Ada91], the first accumulation point of volumes of hyperbolic 3-orbifolds is $0.30521\ldots$, so there are finitely many hyperbolic 3-orbifolds of volume less than 0.251. Another measure of the low complexity of this example is that the underlying topological space of both M_1 and M_c is the 3-sphere $\mathbb{S}^3$, which is the simplest 3-manifold.

12.3. Isospectrality and 1-isospectrality. Consider the number field $F = \mathbb{Q}(\alpha)$ where $\alpha^4 - 3\alpha^2 - 2\alpha + 1 = 0$. This is the unique field of discriminant -1328 and signature $(2, 1)$ (LMFDB `4.2.1328.1`). Let D be the unique quaternion division algebra ramified at every real place and no finite place of F. We have $C \cong C_{\text{iso}} \cong C_2$, which therefore has a single non-trivial character χ, corresponding to the quadratic extension $L = F(\zeta_4)$. Let $C = \{1, c\}$. We have

$$\text{vol}(M_1) = \text{vol}(M_c) = \frac{1328^{3/2}\zeta_F(2)}{2^8\pi^6} = 0.2461808\ldots.$$

The maximal cyclic subgroups of both Γ_1 and Γ_c have order 2, 3 or 4, and we have

$$H_1(\Gamma_1, \mathbb{Z}) \cong H_1(\Gamma_c, \mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

We prove by computation (see [P10, Example 7.6]) that there is no 0-shady character of L. This implies that the orbifolds M_1 and M_c are isospectral. On the other hand, there exist 1-shady characters of L, and we prove that there there is a Laplace eigenvalue approximately $30.2167\ldots$ on $\Omega^1(M_1 \sqcup M_c)$ that appears with odd multiplicity, forcing M_1 and M_c to be non-1-isospectral.

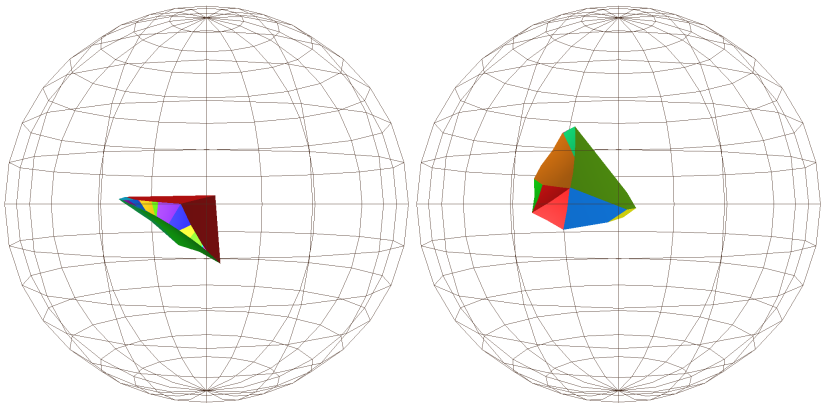

FIGURE 2. Isospectral but not 1-isospectral 3-orbifolds (volume ≈ 0.246)

THEOREM 12.4 (Theorem B in [P10]). *There exists a pair of closed hyperbolic 3-orbifolds with volume* $0.246\ldots$ *that are isospectral, but not 1-isospectral.*

This partially answers Question 5.5 in the case of hyperbolic 3-orbifolds, leaving open the possibility that 1-isospectrality implies 0-isospectrality. The same remarks on the small volume as for the previous example apply to this one, again making it a good candidate for Question 5.7.

12.4. Density of bad eigenvalues. A byproduct of our method is that since Hecke characters are easy to count, it provides an upper bound on the number of eigenvalues whose multiplicity in M_1 and M_c can differ. We prove the following bound.

THEOREM 12.5 (Theorem C in [P10]). *Consider the 3-dimensional case, where* $\mathcal{X} = \mathcal{H}^3$ *i.e.* $(s, r_2) = (0, 1)$. *There exists a constant* $a > 0$ *such that for all* $i \geq 0$ *and for all* $X > 0$ *we have*

$$\sum_{\lambda<X} |\dim(\Omega^i(M_1)_{\Delta=\lambda}) - \dim(\Omega^i(M_c)_{\Delta=\lambda})| \leq aX^{1/2}.$$

In other words, Vignéras's pairs of orbifolds, even when they are not isospectral, are always "almost isospectral", in the sense that there is a vanishing proportion of eigenvalues whose multiplicities differ. In particular, since there exist Vignéras pairs that are not isospectral, we have $\alpha \leq 1/2$ in Question 5.8 for hyperbolic 3-manifolds. Combined with Kelmer's theorem [Kel14, Theorem 1], this answers Question 5.8 completely for hyperbolic 3-manifolds: the supremum is $1/2$, contrary to Kelmer's expectation. It would be interesting to examine the sharpness of Kelmer's threshold for the length spectrum from the point of view of selectivity.

12.5. Regulators. Our Hecke operators method also applies to the integral homology. Indeed, by Hodge's theorem and Matsushima's formula ([Mat67], see also [BC05, §1.2]), automorphic forms allow us to detect the existence of an invertible Hecke operator

$$T\colon H_i(M_1,\mathbb{R}) \longrightarrow H_i(M_c,\mathbb{R})$$

This operator has an adjoint

$$T^*\colon H_i(M_c,\mathbb{R}) \longrightarrow H_i(M_1,\mathbb{R})$$

for the inner product induced by the Riemannian metric. However, the adjoint T^* is also a Hecke operator, so both these Hecke operators preserve the integral homology: we get adjoint maps

$$T\colon H_i(M_1,\mathbb{Z}) \longrightarrow H_i(M_c,\mathbb{Z}) \text{ and } T^*\colon H_i(M_c,\mathbb{Z}) \longrightarrow H_i(M_1,\mathbb{Z}).$$

As in our proof of Theorem 2.3 (see (2.1)), we obtain that

$$\frac{\operatorname{Reg}_i(M_1)^2}{\operatorname{Reg}_i(M_c)^2} = \frac{\det T^*}{\det T}.$$

Inspired by the theory of regulator constants (see [DD09] and Section 2.3), we develop an abstract theory of regulator constants for graded modules [P10, Sections 3.2 and 3.3] from identities of this form, although it is maybe not as complete as the one for finite groups. We obtain a version of Theorem 12.2 for $* = H^\bullet$ where the meaning of $H^\bullet$-isospectrality is:

- M_1 and M_c have the same Betti numbers, and
- for all $i \geq 0$ the ratio $\operatorname{Reg}_i(M_1)^2/\operatorname{Reg}_i(M_c)^2$ is rational.

This provides a partial answer to Question 7.6 in the setting of the Vignéras construction. Interestingly, $H^\bullet$-shady characters are much more restricted than i-shady characters; for instance they are algebraic Hecke characters, whereas general i-shady characters are transcendental. This means that we can prove rationality of regulator ratios even when the orbifolds are not isospectral!

Consider the following example. Let $F = \mathbb{Q}(\alpha)$ where $\alpha^4 - 2\alpha^3 + 7\alpha^2 - 6\alpha - 3 = 0$. The field F is a number field of discriminant -10224 and signature $(2,1)$ (LMFDB `4.2.10224.2`). Let D be the unique quaternion division algebra ramified at every real place and no finite place of F. We have $C \cong C_{\text{iso}} \cong C_2$, which therefore has a single non-trivial character χ, corresponding to the quadratic extension $L = F(\zeta_{12})$. Let $C = \{1, c\}$. We have

$$\operatorname{vol}(M_1) = \operatorname{vol}(M_c) = \frac{10224^{3/2}\zeta_F(2)}{2^8\pi^6} = 5.902455\ldots.$$

The maximal cyclic subgroups of Γ_1 have order 2, 3, 4 or 12, and the maximal cyclic subgroups of Γ_c have order 2 or 3.

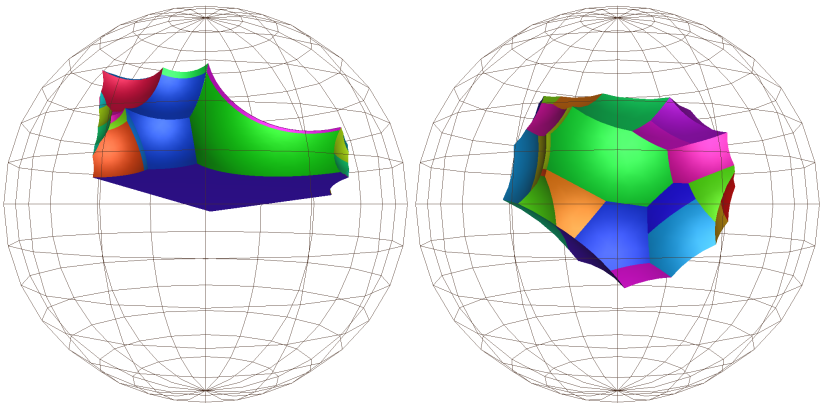

FIGURE 3. Non-isospectral 3-orbifolds with both Betti numbers 1 and with rational regulator square quotient (volume ≈ 5.902)

By the same odd multiplicity argument as before, we prove that M_1 and M_c are neither isospectral not 1-isospectral. However, there is no $H^\bullet$-shady character of L, so we have

$$\frac{\operatorname{Reg}_1(M_1)^2}{\operatorname{Reg}_1(M_c)^2} \in \mathbb{Q}^\times,$$

and the Betti numbers of M_1 and M_c are equal. In fact, we have

$$H_1(\Gamma_1, \mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z} \quad \text{and} \quad H_1(\Gamma_c, \mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z},$$

and in particular both first Betti numbers are 1, so the rationality of the ratio of regulators is a non-trivial statement. Moreover, since the orbifolds are not isospectral, the Cheeger–Müller theorem does not say anything about this rationality.

THEOREM 12.6 (Theorem E in [P10]). *There exists a pair of closed hyperbolic 3-orbifolds M_1, M_c with volume 5.902... that are not isospectral, nor 1-isospectral, and for which* $\dim H_1(M_1, \mathbb{Q}) = \dim H_1(M_c, \mathbb{Q}) = 1$, *yet* $\operatorname{Reg}_1(M_1)^2 / \operatorname{Reg}_1(M_c)^2$ *is rational.*

12.6. Torsion homology and Galois representations. Finally, our method even applies to torsion homology. However, this is conditional to a plausible conjecture ([P10, Conjecture 6.5], a variant of [Ash92], [CG18, Conjecture B], and [CV19, Conjecture 2.2.5]) on the existence of mod p Galois representations attached to torsion classes in the homology of the arithmetic orbifolds we are considering. Fix a prime number $p > 2$, and suppose we want to compare the p-power torsion homology of the two orbifolds. Following our method, we look for a Hecke operator

$$T \colon H_i(M_1, \mathbb{Z}_p) \longrightarrow H_i(M_c, \mathbb{Z}_p)$$

that is invertible over $\mathbb{Z}_p$. By dévissage, if this fails to exist then there exists a mod p system of eigenvalues $(a_\mathfrak{p})$ for the Hecke operators such

that such that

$$a_{\mathfrak{p}} = a_{\mathfrak{p}}\chi(\mathfrak{p}) \text{ for all } \mathfrak{p}.$$

But now, torsion homology is not directly related to automorphic forms, so we cannot use automorphic induction. Instead, we assume that there exists a semisimple Galois representation

$$\rho\colon \mathcal{G}_F \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

such that $\operatorname{Tr}\rho(\mathrm{Frob}_{\mathfrak{p}}) = a_{\mathfrak{p}}$ for almost all $\mathfrak{p}$, and satisfying other expected local properties. The self-twist condition implies

$$\rho \otimes \chi \cong \rho,$$

and this is well-known to imply (since $p \neq 2$) the existence of a character $\psi\colon \mathcal{G}_L \to \bar{\mathbb{F}}_p^{\times}$ such that

$$\rho \cong \mathrm{Ind}_{\mathcal{G}_F/\mathcal{G}_L}\,\psi.$$

By class field theory, the Galois character ψ corresponds to a mod p character Ψ of a ray class group, and again one can analyse the properties that Ψ should satisfy. We obtain a version of Theorem 12.2 for $* = \mathbb{Z}_p$, where the meaning of $\mathbb{Z}_p$-isospectrality is:

- for all $i \geq 0$, $H_i(M_1, \mathbb{Z}_p) \cong H_i(M_c, \mathbb{Z}_p)$, and
- for all $i \geq 0$, we have $\operatorname{Reg}_i(M_1)^2 / \operatorname{Reg}_i(M_c)^2 \in \mathbb{Z}_{(p)}^{\times}$.

Note that $\mathbb{Z}_p$-isospectrality is stronger than $H^\bullet$-isospectrality; correspondingly, every $H^\bullet$-shady character gives rise to a $\mathbb{Z}_p$-shady character for all p. Conversely, if there is no $H^\bullet$-shady character, then there is a computable finite set of primes $\mathcal{S}$ such that there is no $\mathbb{Z}_p$-shady character for $p \notin \mathcal{S}$ (see [P10, Theorem H]). This set of primes plays, in the context of the Vignéras construction, the role of the set of prime divisors of $\#G$ in the context of the Sunada construction with a finite group G.

Although the conjecture that we use has been proved in some cases (see [Sch15] for the first such result and [CN23] for the most recent developments), it would be nice to be able to bypass Galois representations to get an unconditional result. This would require the following special case of torsion functoriality, which could be very hard.

Question 12.7. Can we prove the existence of mod p automorphic induction? Can we characterise it in terms of self-twists?

Torsion analogues of phenomena from the Langlands programme have recently been of great interest, for instance the Jacquet–Langlands correspondence [CV19] or cyclic base-change [TV16]. Our results can also be interpreted as a such a phenomenon, namely a torsion analogue of the Labesse–Langlands multiplicity formula [LL79]. The Langlands programme postulates the existence of a compact group $\mathcal{L}_F$, which is an extension of $\mathcal{G}_F$, and conjectures that to each cuspidal automorphic

representation Π of $D^\times$, one should be able to attach a continuous irreducible representation, called a *Langlands parameter*,

$$\rho = \rho_\Pi \colon \mathcal{L}_F \longrightarrow \mathrm{GL}_2(\mathbb{C}),$$

such that $\rho_\Pi \cong \rho_{\Pi'}$ if and only if $\Pi \cong \Pi'$. Concretely, each such Π contributes to the spectrum of

$$\mathcal{M} = \bigsqcup_{c \in C} M_c,$$

i.e. of one or several of the components. In contrast, to each cuspidal automorphic representation Π of the kernel $\mathrm{SL}_1(D)$ of the reduced norm, one should be able to attach an irreducible Langlands parameter

$$\rho \colon \mathcal{L}_F \longrightarrow \mathrm{PGL}_2(\mathbb{C}),$$

but several non-isomorphic Π can have isomorphic parameters ρ: they form an L-packet. The difference between the several Π manifests itself by the fact that they may not have fixed points under the same subgroups, and they may not all have the same multiplicity in the space of automorphic forms for $\mathrm{SL}_1(D)$. Concretely, each such Π contributes to the spectrum of a connected orbifold $\mathrm{SL}_1(\mathcal{O}_c)\backslash\mathcal{X}$, which is closely related to the component $M_c = \mathcal{O}_c^\times\backslash\mathcal{X}$. However, the following result of Labesse and Langlands [LL79, Proposition 7.2] implies that most ρ contribute equally to the spectrum of all of these orbifolds.

Theorem 12.8 (Labesse–Langlands). *Suppose $\rho \colon \mathcal{L}_F \to \mathrm{PGL}_2(\mathbb{C})$ is not induced from a character of an index 2 subgroup. Then the automorphic multiplicity of every Π in the L-packet of ρ is the same.*

The relation with isospectrality was noticed by Rajan [Raj07] who used it to reprove isospectrality results generalising Vignéras's. Returning to torsion homology, let $\mathbb{T}$ denote the algebra generated by all Hecke operators $T_\mathfrak{p}$ and $\mathbb{T}_1$ the subalgebra generated by the operators $T_\mathfrak{p}$ that stabilise the components, corresponding to primes $\mathfrak{p}$ with trivial class in C. To each system of eigenvalues $(a_\mathfrak{p})$ of the Hecke algebra $\mathbb{T}$ occurring in $H_1(\mathcal{M}, \mathbb{F}_p)$ should correspond a continuous semisimple Galois representation

$$\rho \colon \mathcal{G}_F \longrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

such that $\operatorname{Tr}\rho(\mathrm{Frob}_\mathfrak{p}) = a_\mathfrak{p}$ for almost all $\mathfrak{p}$. The restriction of the eigenvalue system to $\mathbb{T}_1$ does not completely determine ρ, but it completely determines its projectivisation

$$P\rho \colon \mathcal{G}_F \longrightarrow \mathrm{PGL}_2(\bar{\mathbb{F}}_p).$$

Our result is that if $P\rho$ is not induced from $\mathcal{G}_L$, then we have an isomorphism of $\mathbb{T}_1$-modules

$$H_i(M_1, \mathbb{Z}_p)_\mathfrak{m} \cong H_i(M_c, \mathbb{Z}_p)_\mathfrak{m}$$

where $\mathfrak{m}$ is the maximal ideal of $\mathbb{T}_1$ generated by p and the $T_\mathfrak{p} - a_\mathfrak{p}$. This is analogous to Theorem 12.8. However, more generally Labesse

and Langlands give, in terms of the Langlands parameter, a formula for the multiplicity of Π. This leads to the following interesting question.

QUESTION 12.9. Can one formulate a torsion analogue of the full Labesse–Langlands multiplicity formula? More precisely, from the properties of the Galois representations ρ, can one predict the ratio

$$\frac{\#H_i(M_1, \mathbb{Z}_p)_{\mathrm{tors}}}{\#H_i(M_c, \mathbb{Z}_p)_{\mathrm{tors}}}$$

or the p-adic valuation of the ratio

$$\frac{\mathrm{Reg}_i(M_1)^2}{\mathrm{Reg}_i(M_c)^2}?$$

Can one prove it?

13. Hardness of lattice problems

When studying the hardness of a computational problem A, we usually mean "does there exist an efficient algorithm that solves A on all instances?"; this is the *worst-case* complexity of the problem: a problem is hard in this sense if there exists some instance that is hard. However, for cryptographic applications, what we really need is a problem that is hard when instances are picked at random with respect to a certain distribution (think about the instance as a secret key, which needs to be generated at random from a large set). Therefore, one needs to consider the question "does there exist and algorithm that solves A efficiently most of the time on random instances?"; this is the *average-case* complexity of the problem (see [BT06] for a survey with precise definitions). A priori, it may happen that a problem is hard in the worst case (there exists hard instances) but easy on average (most instances are easy). Again, as for worst-case complexity, it is hard to prove that a computational problem is hard on average, but we can prove reductions. More precisely, assume we can design an algorithm that uses an oracle for A that works on most random inputs, and uses calls to that oracle to solve A in an arbitrary instance. Then A is no easier on average than in the worst case: this is a *worst-case to average-case reduction*. The goal of our work [P14] is to prove such a result for certain short vector problems for module lattices (Definition 6.9) of fixed rank r. Such a result was obtained by de Boer, Ducas, Pellet-Mary and Wesolowski in the rank 1 case [dBDPMW20]. It was suggested in [DK22] that a generalisation might be possible. In the exposition of our results, we assume that r is fixed and $|\Delta_F| \leq [F : \mathbb{Q}]^{O([F:\mathbb{Q}])}$, to simplify the statements.

13.1. Geometry of the space of module lattices. We gave an abstract definition of module lattices (Definition 6.9) but it turns out that all such lattices of rank r can be embedded in $F_{\mathbb{R}}^r$. By choosing a

pseudo-basis (see [Coh00, Section 1.4.1]), we obtain that the space of module lattices is the adélic double quotient (see Section 4.2)

$$\mathcal{M} = \mathrm{GL}_r(F) \backslash \mathrm{GL}_r(\mathbb{A}_F) / \prod_{\mathfrak{p}} \mathrm{GL}_r(\mathbb{Z}_{\mathfrak{p}}) \times \mathrm{U}_n(F_{\mathbb{R}}) \mathbb{R}_{>0} = \bigsqcup_{\mathfrak{a} \in \mathrm{Cl}(F)} \Gamma_{\mathfrak{a}} \backslash \mathcal{X}$$

where

$$\mathcal{X} = \mathrm{GL}_r(F_{\mathbb{R}}) / \mathrm{U}_n(F_{\mathbb{R}}) \mathbb{R}_{>0}$$

and

$$\Gamma_{\mathfrak{a}} = \mathrm{Aut}_{\mathbb{Z}_F}(\mathbb{Z}_F^{r-1} \oplus \mathfrak{a}).$$

In particular, there is a natural measure on $\mathcal{M}$ coming from the Haar measure on $\mathrm{GL}_r(F_{\mathbb{R}})$; since the total measure of $\mathcal{M}$ is finite, we normalise it to be a probability measure. This gives a meaning to the notion of a "uniformly random module lattice", but this is not quite suitable for notions of average-case complexity: computers cannot represent arbitrary real numbers, so we need to discretise this probability distribution and prove that we can efficiently sample from it. The discretisation is a technical part of [P14] that we omit here, but the samplability will follow from the techniques presented below.

The space $\mathcal{M}$ has finite volume, but when $r > 1$ it is not compact. Its large scale geometry is related to the shape of the corresponding lattices: the largest, compact part ("the bulk") consists of lattices that are balanced in the sense that they do not have very short vectors compared to their covolume; there are thin parts attached to the bulk, consisting of lattices that are imbalanced; as $\lambda_1(\Lambda)/\operatorname{covol}(\Lambda)^{1/n} \to 0$, the lattice Λ goes to infinity ("the cusps").

Our general strategy is to use the well-known equidistribution of Hecke orbits [GM03,COU01] in $\mathcal{M}$. The basic idea is the following: from a lattice Λ, take a random sublattice Λ' of fixed index. If $v \in \Lambda'$ is a solution to γ-HSVP in Λ', then it is a solution of $[\Lambda : \Lambda']^{1/n}\gamma$-HSVP in Λ. Moreover, as the index grows, there are more and more possible sublattices, which therefore have a chance of being equidistributed in $\mathcal{M}$. If this happens for moderately large index, then we obtain a worst-case to average-case reduction for HSVP with a moderately large blowup in the approximation factor γ. In fact, this operation is precisely reflected by the action of Hecke operators (see Section 4.2): the Hecke operator $T_{\mathfrak{p}}$ sends a lattice Λ to the formal sum of its sublattices Λ' such that $\Lambda/\Lambda' \cong \mathbb{F}_{\mathfrak{p}}$.

However, we cannot hope the equidistribution to happen for a small index $[\Lambda : \Lambda']$ if Λ is very imbalanced: indeed, if $v \in \Lambda$ is a vector that is very short compared to $\operatorname{covol}(\Lambda)^{1/n}$, then the sublattice Λ' contains the vector $[\Lambda : \Lambda']v$ whereas its covolume is larger than that of Λ, so Λ' is still imbalanced if the index is moderately large, preventing equidistribution. Concretely, this means that we are not able to prove a worst-case to average-case reduction for HSVP in the entire space $\mathcal{M}$. However, a slightly different problem is better behaved for imbalanced

lattices: the Short Independent Vectors Problem (recall Definition 6.6 of the successive minima $\lambda_i(\Lambda)$).

PROBLEM 13.1 (γ-SIVP). Given a lattice Λ, compute independent vectors $v_1, \ldots, v_n \in \Lambda$ such that $\|v_i\| \leq \gamma \lambda_n(\Lambda)$.

We will need to treat lattices differently depending on their balancedness. We use the following measure.

DEFINITION 13.2. Let Λ be a module lattice of rank r. For each integer $1 \leq i \leq r$ we define

$$\lambda_i^F(\Lambda) = \min\{\lambda : \dim_F \langle v \in \Lambda \mid \|v\| \leq \lambda \rangle_F \geq i\}.$$

We define the *imbalance factor*

$$\alpha_F(\Lambda) = \frac{\lambda_r^F(\Lambda)}{\lambda_1^F(\Lambda)} \geq 1.$$

Our technique will distinguish three regions of $\mathcal{M}$. We carefully choose bounds

- $\alpha_{bf} \in n^{O(1)}$, and
- $\alpha_{fc} \in 2^{O(n)}$,

and we define

- the *bulk of* $\mathcal{M}$ to be the set of Λ such that
$$\alpha_F(\Lambda) \leq \alpha_{bf};$$
- the *flares of* $\mathcal{M}$ to be the set of Λ such that
$$\alpha_{bf} < \alpha_F(\Lambda) \leq \alpha_{fc};$$
- the *cuspidal region of* $\mathcal{M}$ (sometimes abbreviated as the *cusps*, although technically the cusps are at infinity) to be the set of Λ such that
$$\alpha_{fc} < \alpha_F(\Lambda).$$

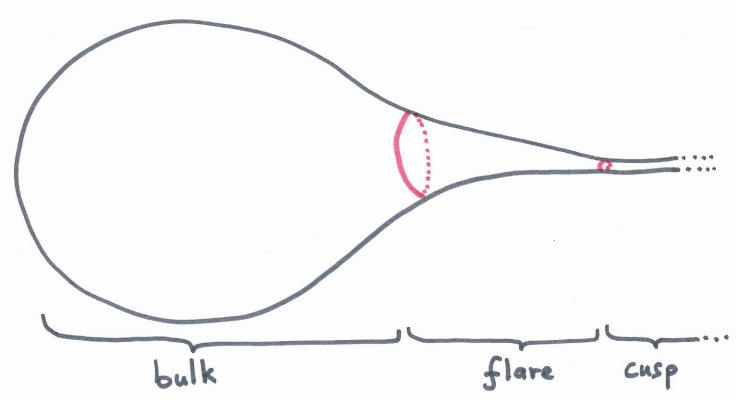

FIGURE 4. Regions of the space $\mathcal{M}$

13.2. Self-reduction in the bulk. We now give more details about our technique. Let $f_\Lambda \colon \mathcal{M} \to \mathbb{R}_{\geq 0}$ be a bounded, compactly supported function such that $\int_{\mathcal{M}} f_\Lambda = 1$, which we see as the density of a probability distribution. In our application f_Λ will need to be tightly concentrated around the input lattice Λ, so that drawing a random lattice according to f_Λ yields lattices that are close to Λ. Let $\bar{T} = \frac{1}{\deg(T_\mathfrak{p})} T_\mathfrak{p}$ denote the Hecke operator normalised to be an averaging operator, so that $\bar{T}\mathbf{1} = \mathbf{1}$. We would like $\bar{T} f_\Lambda$ to be very close to the uniform distribution, which has density function the constant function $\mathbf{1}$, in other words we would like to make the L^1 norm $\|\bar{T} f_\Lambda - \mathbf{1}\|_1$ (also known as the statistical distance) very small. The Hecke operator is self-adjoint, so it stabilises the orthogonal complement $L^2_0(\mathcal{M})$ of $\mathbb{C} \cdot \mathbf{1}$. Let λ be the operator norm of $\bar{T}$ acting on $L^2_0(\mathcal{M})$. Then we have

$$\|\bar{T} f_\Lambda - \mathbf{1}\|_1 \leq \|\bar{T} f_\Lambda - \mathbf{1}\|_2 = \|\bar{T}(f_\Lambda - \mathbf{1})\|_2 \leq \lambda \|f_\Lambda\|_2 \text{ since } \langle f_\Lambda - \mathbf{1}, \mathbf{1} \rangle = 0.$$

If we can estimate the norm $\|f_\Lambda\|_2$ and if we can make λ very small by using a prime ideal $\mathfrak{p}$ of large norm, then we can indeed make the distance $\|\bar{T} f_\Lambda - \mathbf{1}\|_1$. Unfortunately, we always have $\lambda = 1$! This is due to the determinant map

$$\mathcal{M} \xrightarrow{\det} \mathcal{M}_1$$

to the space $\mathcal{M}_1$ of rank 1 module lattices. Let $L^2_{\det}(\mathcal{M}) \subset L^2(\mathcal{M})$ denote the subspace of functions that are pulled back from $L^2(\mathcal{M}_1)$. Because GL_1 is commutative, $\mathcal{M}_1$ is in fact a group (also known as the Arakelov class group) and its spectral decomposition comes from Hecke characters, so that every eigenvalue of $\bar{T}$ on $L^2_{\det}(\mathcal{M})$ has absolute value 1. However, this is the only obstruction: by inspecting the spectral decomposition of $L^2(\mathcal{M})$ (see [GH24, Section 10]) and known bounds towards the generalised Ramanujan conjecture (see [BB13] for a survey), we have the following bound.

Proposition 13.3. *The operator norm of $T_\mathfrak{p}$ acting on the orthogonal complement of $L^2_{\det}(\mathcal{M})$ is at most $O(\mathrm{N}(\mathfrak{p})^{-3/8})$.*

In addition, the bad eigenvalues of $L^2_{\det}(\mathcal{M})$ can be dealt with by the techniques of [dBDPMW20]: by averaging over all primes with norm up to some bound B (assuming GRH for L-functions of Hecke characters) and using a smooth function f_Λ.

The next ingredient is a bound on $\|f_\Lambda\|_2$. We construct our function f_Λ as follows: start from a function

$$f \colon \mathcal{X} \longrightarrow \mathbb{R}_{\geq 0}$$

and project it via

$$\mathcal{X} \longrightarrow \Gamma_\mathfrak{a} \backslash \mathcal{X}$$

to a component, centering it around Λ, to yield f_Λ. The norm bound uses the following ingredients. First we need some integral formulas and bounds from [P3]. Then we need to take into account the blowup in L^2 norm incurred by the possible overlap between f and its $\Gamma_{\mathfrak{a}}$-translates; this amounts to counting almost-automorphisms of Λ, which we reduce to counting vectors in Λ in various balls. The more imbalanced Λ is, the more almost-automorphisms it has. Putting these ingredients together yields the following bound.

PROPOSITION 13.4 ([P14]). *We have*

$$\|f_\Lambda\|_2 \leq (n\,\alpha_F(\Lambda))^{O(n)}.$$

To use this f_Λ in the reduction, we explain in [P14] how to sample from the distribution with density f_Λ. This leads to the following algorithm.

ALGORITHM 13.5. Relative to an oracle $\mathbf{O}_{\text{avgHSVP}}$.

- Input: a lattice Λ in the bulk of $\mathcal{M}$.
- Output: a vector $v \in \Lambda$.

(1) Draw a random metric on Λ according to f_Λ, yielding a new lattice Λ'.
(2) Draw a random prime $\mathfrak{p}$ of norm $\leq B$ and a random sublattice $\Lambda'' \subset \Lambda'$ with $\Lambda'/\Lambda'' \cong \mathbb{F}_{\mathfrak{p}}$.
(3) $v \leftarrow \mathbf{O}_{\text{avgHSVP}}(\Lambda'')$
(4) Return v.

We obtain the following worst-case average-case reduction for HSVP, that applies to balanced lattices.

THEOREM 13.6 ([P14]). *Assume GRH. Algorithm 13.5 gives a polynomial time reduction from $n^{O(1)}\gamma$-HSVP restricted to the bulk of $\mathcal{M}$ to average γ-HSVP.*

However, for imbalanced lattices our technique cannot yield a good reduction for HSVP, so we need an analogue of this result for SIVP. For that purpose we prove that random lattices in $\mathcal{M}$ are balanced with high probability. We use the notion of *semistable* and *unstable* lattices due to Grayson [Gra84], which is a notion of balanceness based on volume of sublattices instead of length of vectors. We prove that:

- semistable lattices belong to the bulk of $\mathcal{M}$ (i.e. are balanced in our sense); and
- the volume of the set of unstable lattices is very close to 0 (we adapt computations of Thunder [Thu98] and Shapira and Weiss [SW14]).

We can therefore consider the obvious analogue of Algorithm 13.5 for SIVP.

ALGORITHM 13.7. Relative to an oracle $\mathbf{O}_{\text{avgSIVP}}$.

- Input: a lattice Λ in the bulk of $\mathcal{M}$.
- Output: independent vectors $v_1, \dots, v_n \in \Lambda$.

(1) Draw a random metric on Λ according to f_Λ, yielding a new lattice Λ'.
(2) Draw a random prime $\mathfrak{p}$ of norm $\leq B$ and a random sublattice $\Lambda'' \subset \Lambda'$ with $\Lambda'/\Lambda'' \cong \mathbb{F}_\mathfrak{p}$.
(3) $v_1, \dots, v_n \leftarrow \mathbf{O}_{\text{AVGSIVP}}(\Lambda'')$
(4) Return $v_1, \dots, v_n$.

We obtain the following analogue of Theorem 13.6 for SIVP.

THEOREM 13.8 ([P14]). *Assume GRH. Algorithm 13.7 gives a polynomial time reduction from $n^{O(1)}\gamma$-SIVP restricted to the bulk of $\mathcal{M}$ to average γ-SIVP.*

13.3. Rebalancing lattices: from the flares to the bulk. In the flares, the lattices are imbalanced, but not sufficiently to be able to find the gaps in polynomial time. Our reduction instead guesses the size of the gaps, and uses specially crafted Hecke operators to rebalance those gaps.

ALGORITHM 13.9. Relative to an oracle $\mathbf{O}_{\text{AVGSIVP}}$.

- Input: a lattice Λ in the bulk or the flares of $\mathcal{M}$.
- Output: independent vectors $v_1, \dots, v_n \in \Lambda$.

(1) $v_1, \dots, v_n \leftarrow$ an LLL-reduced basis of Λ
(2) For all integer tuples $(t_1, \dots, t_{r-1})$ such that $1 \leq 2^{t_i} \leq \alpha_{fc}$:
  (a) $\Lambda' \leftarrow \Lambda$
  (b) For $i = 1$ to $r-1$:
    - Let p be a prime number such that $p \approx 2^{t_i}$.
    - Let $\Lambda'' \subset \Lambda'$ be a random sublattice such that $\Lambda'/\Lambda'' \cong (\mathbb{Z}_F/p\mathbb{Z}_F)^i$
    - $\Lambda' \leftarrow \Lambda''$
  (c) $v'_1, \dots, v'_n \leftarrow$ output of Algorithm 13.7 on Λ'
  (d) If $\max_i \|v'_i\| < \max_i \|v_i\|$ then: $v_1, \dots, v_n \leftarrow v'_1, \dots, v'_n$
(3) Return $v_1, \dots, v_n$.

We are able to prove that at least one of the lattices Λ' belongs to the bulk of $\mathcal{M}$, namely the one where the 2^{t_i} are closest to $\lambda^F_{i+1}(\Lambda)/\lambda^F_i(\Lambda)$, and that $\lambda_n(\Lambda')$ is not too much larger than $\lambda_n(\Lambda)$. Note the use of the Hecke operator $T_{p,\dots,p}$ (i times), where $p\mathbb{Z}_F$ is not necessarily a prime ideal, to rebalance the i-th gap. This gives the following reduction.

THEOREM 13.10 ([P14]). *Assume GRH. Algorithm 13.9 gives a polynomial time reduction from $n^{O(1)}\gamma$-SIVP restricted to the union of the bulk and the flares of $\mathcal{M}$ to average γ-SIVP.*

13.4. Cutting cusps: from cuspidal regions to flares. Our definition of the cuspidal region is designed so that the gaps of lattices

in such regions are so large that they can be detected by the LLL algorithm, and can therefore be broken into lower rank pieces. In order to obtain a self-reduction in rank r, we complement these lower rank lattices while being careful not to create a new large gap.

ALGORITHM 13.11. Relative to an oracle $\mathbf{O}_{\text{AVGSIVP}}$.

- Input: a lattice Λ in $\mathcal{M}$.
- Output: independent vectors $v_1, \ldots, v_n \in \Lambda$.

(1) $d \leftarrow [F : \mathbb{Q}]$
(2) $v_1, \ldots, v_n \leftarrow$ an LLL-reduced basis of Λ
(3) Let $r_1 + \cdots + r_t = r$ be the partition of r corresponding to gaps in the (v_i) that are larger than $2^{O(n)}$.
(4) $\Lambda_{\text{prev}} \leftarrow 0$
(5) For $j = 1$ to t:
  (a) $R_j \leftarrow r_1 + \cdots + r_j$
  (b) $\Lambda_1 \leftarrow \Lambda \cap \langle v_1, \ldots, v_{dR_j} \rangle_F$ *(Λ_1 has rank R_j)*
  (c) $\Lambda_2 \leftarrow \Lambda_1 / \Lambda_{\text{prev}}$ *(Λ_2 has rank r_j)*
  (d) $\Lambda_3 \leftarrow \Lambda_2 \oplus (\text{covol}(\Lambda_2)^{1/(dr_j)} \mathbb{Z}_F)^{r - r_j}$ *(Λ_3 has rank r)*
  (e) $w_1, \ldots, w_n \leftarrow$ output of Algorithm 13.9 on Λ_3
  (f) Project $w_1, \ldots, w_n \in \Lambda_3$ orthogonally onto Λ_2, and extract independent vectors $w'_1, \ldots w'_{dr_j} \in \Lambda_2$.
  (g) Lift $w'_1, \ldots w'_{dr_j}$ to $v_{dR_{j-1}+1}, \ldots, v_{dR_j} \in \Lambda$.
  (h) $\Lambda_{\text{prev}} \leftarrow \Lambda_1$
(6) Return $v_1, \ldots, v_n$.

The careful design of the lattices Λ_3 forces them to belong to the flares or bulk of $\mathcal{M}$, finally giving our main result.

THEOREM 13.12 ([P14]). *Assume GRH. Algorithm 13.11 gives a polynomial time reduction from $n^{O(1)}\gamma$-SIVP to average γ-SIVP for module lattices.*

In this exposition we hid the dependence on r in the big O notation; in [P14] we make this dependence explicit although our intended application is for fixed r. The outcome is that the bounds in the reduction are exponential in r, making them very weak as $r \to \infty$. It would be very interesting to strengthen the method so that it gives good bounds even when $r \to \infty$, for instance in the case $F = \mathbb{Q}$ (unstructured lattices). At present this seems quite difficult.

List of presented works

This list contains publications, preprints, software, and papers written under my supervision, in chronological order.

[P1] Alex Bartel and Aurel Page. Torsion homology and regulators of isospectral manifolds. *J. Topol.*, 9(4):1237–1256, 2016. `https://arxiv.org/abs/1601.06821`.

[P2] Alex Bartel and Aurel Page. Group representations in the homology of 3-manifolds. *Comment. Math. Helv.*, 94(1):67–88, 2019. `https://arxiv.org/abs/1605.04866`.

[P3] Christian Maire and Aurel Page. Codes from unit groups of division algebras over number fields. *Math. Z.*, 298(1-2):327–348, 2021. `https://inria.hal.science/hal-01770396`.

[P4] Jean Kieffer, Aurel Page, and Damien Robert. Computing isogenies from modular equations in genus two. *J. Algebra*, 666:331–386, 2025. `https://inria.hal.science/hal-02436133`.

[P5] Jean-François Biasse, Claus Fieker, Tommy Hofmann, and Aurel Page. Norm relations and computational problems in number fields. *J. Lond. Math. Soc., II. Ser.*, 105(4):2373–2414, 2022. `https://arxiv.org/abs/2002.12332`.

[P6] Aurel Page. `abelianbnf`, September 2020. `https://inria.hal.science/hal-02961482`.

[P7] Pascal Molin and Aurel Page. Computing groups of Hecke characters. *Res. Number Theory*, 8(4):26, 2022. Id/No 91. `https://inria.hal.science/hal-03795267`.

[P8] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. In *Advances in cryptology – EUROCRYPT 2024. 43rd annual international conference on the theory and applications of cryptographic techniques, Zurich, Switzerland, May 26–30, 2024. Proceedings. Part VI*, pages 388–417. Cham: Springer, 2024. `https://inria.hal.science/hal-04209824`.

[P9] Aurel Page and Damien Robert. Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Paper 2023/1766, 2023. `https://eprint.iacr.org/2023/1766`.

[P10] Alex Bartel and Aurel Page. Vignéras orbifolds: isospectrality, regulators, and torsion homology. Preprint, arXiv:2407.07240

[math.NT] (2024), 2024. https://arxiv.org/abs/2407.07240.

[P11] Bill Allombert, Jean-François Biasse, Jonathan Komada Eriksen, Péter Kutas, Chris Leonardi, Aurel Page, Renate Scheidler, and Márton Tot Bagi. PEARL-SCALLOP: Parameter Extension Applicable in Real-Life SCALLOP. Cryptology ePrint Archive, Paper 2024/1744, 2024. https://eprint.iacr.org/2024/1744.

[P12] Fabrice Étienne. Computing class groups by induction with generalised norm relations. Preprint, arXiv:2411.13124 [math.NT] (2024), 2024. https://arxiv.org/abs/2411.13124.

[P13] Fabrice Étienne. An algorithm to compute Selmer groups via resolutions by permutation modules. Preprint, arXiv:2504.13506 [math.NT] (2025), 2025. https://arxiv.org/abs/2504.13506.

[P14] Koen de Boer, Aurel Page, Radu Toma, and Benjamin Wesolowski. Random self-reducibility of SIVP for module lattices of fixed rank. In preparation, 2025.

[P15] Aurel Page and Damien Robert. Clapotis: Evaluating the isogeny class group action in polynomial time. In preparation, 2025.

Bibliography

[Ada91] Colin C. Adams, *Limit volumes of hyperbolic three-orbifolds*, J. Differ. Geom. **34** (1991), no. 1, 115–141 (English).

[Adl91] Leonard M Adleman, *Factoring numbers using singular integers*, Proceedings of the twenty-third annual ACM symposium on Theory of computing, 1991, pp. 64–71.

[Ait21] Wayne Aitken, *Report on Freely Representable Groups*, Preprint, arXiv:2102.00559 [math.GR] (2021), 2021.

[ÁL24] Alfredo Álzaga and Emilio A. Lauret, *Isospectral spherical space forms and orbifolds of highest volume*, Preprint, arXiv:2409.02213 [math.DG] (2024), 2024.

[And17] Yves André, *On the Kodaira-Spencer map of abelian schemes*, Ann. Sc. Norm. Super. Pisa, Cl. Sci. (5) **17** (2017), no. 4, 1397–1416 (English).

[Arp24] Sarah Arpin, *Adding level structure to supersingular elliptic curve isogeny graphs*, J. Théor. Nombres Bordx. **36** (2024), no. 2, 405–443 (English).

[ASD18] Divesh Aggarwal and Noah Stephens-Davidowitz, *Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP)*, 1st symposium on simplicity in algorithms. SOSA 2018, January 7–10, 2018, New Orleans, LA, USA. Co-located with the 29th ACM-SIAM symposium on discrete algorithms (SODA 2018), Wadern: Schloss Dagstuhl – Leibniz Zentrum für Informatik, 2018, Id/No 12, p. 19 (English).

[Ash92] Avner Ash, *Galois representations attached to mod p cohomology of $GL(n, \mathbb{Z})$*, Duke Math. J. **65** (1992), no. 2, 235–255 (English).

[AT09] Emil Artin and John Tate, *Class field theory*, reprint of the 1990 2nd ed. ed., Providence, RI: AMS Chelsea Publishing, 2009 (English).

[Bac90] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comput. **55** (1990), no. 191, 355–380 (English).

[BB13] Valentin Blomer and Farrell Brumley, *The role of the Ramanujan conjecture in analytic number theory*, Bull. Am. Math. Soc., New Ser. **50** (2013), no. 2, 267–320

(English).

[BBdV+17] Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal, *Short generators without quantum computers: The case of multiquadratics*, Advances in Cryptology – EUROCRYPT 2017 (Cham) (Jean-Sébastien Coron and Jesper Buus Nielsen, eds.), Springer International Publishing, 2017, pp. 27–59.

[BC05] Nicolas Bergeron and Laurent Clozel, *Spectre automorphe des variétés hyperboliques et applications topologiques*, Astérisque, vol. 303, Paris: Société Mathématique de France, 2005 (French).

[BD14] Alex Bartel and Tim Dokchitser, *Brauer relations in finite groups. II: Quasi-elementary groups of order p^aq*, J. Group Theory **17** (2014), no. 3, 381–393 (English).

[BD15] ———, *Brauer relations in finite groups*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 10, 2473–2512 (English).

[Bér92] Pierre Bérard, *Transplantation and isospectrality. I*, Math. Ann. **292** (1992), no. 3, 547–560 (French).

[Bér93] ———, *Transplantation et isospectralité. II. (Transplantation and isospectrality. II)*, J. Lond. Math. Soc., II. Ser. **48** (1993), no. 3, 565–576 (French).

[BGLG+17] Sean Ballentine, Aurore Guillevic, Elisa Lorenzo García, Chloe Martindale, Maike Massierer, Benjamin Smith, and Jaap Top, *Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication*, Algebraic geometry for coding theory and cryptography, IPAM, Los Angeles, CA, USA, February 2016, Cham: Springer, 2017, pp. 63–94 (English).

[BHC62] Armand Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. Math. (2) **75** (1962), 485–535 (English).

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Collect. Artic. in Honor of the 60th Birthday of A. Grothendieck. Vol. I, Prog. Math. 86, 333-400 (1990)., 1990.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren, *CSI-FiSh: efficient isogeny based signatures through class group computations*, Advances in cryptology – ASIACRYPT 2019. 25th international conference on the theory and application of cryptology and information security, Kobe, Japan, December 8–12, 2019.

Proceedings. Part I, Cham: Springer, 2019, pp. 227–247 (English).

[BL94] J. A. Buchmann and H. W. jun. Lenstra, *Approximating rings of integers in number fields*, J. Théor. Nombres Bordx. **6** (1994), no. 2, 221–260 (English).

[BMSS08] A. Bostan, F. Morain, B. Salvy, and É. Schost, *Fast algorithms for computing isogenies between elliptic curves*, Math. Comput. **77** (2008), no. 263, 1755–1778 (English).

[Bol97] Robert Boltje, *Class group relations from Burnside ring idempotents*, J. Number Theory **66** (1997), no. 2, 291–305 (English).

[Bor81] A. Borel, *Commensurability classes and volumes of hyperbolic* 3*-manifolds*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **8** (1981), no. 1, 1–33.

[BR11] Chandrasheel Bhagwat and C. S. Rajan, *On a spectral analog of the strong multiplicity one theorem*, Int. Math. Res. Not. **2011** (2011), no. 18, 4059–4073 (English).

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

[BT87] Robert Brooks and Richard Tse, *Isospectral surfaces of small genus*, Nagoya Math. J. **107** (1987), 13–24 (English).

[BT06] Andrej Bogdanov and Luca Trevisan, *Average-case complexity*, Found. Trends Theor. Comput. Sci. **2** (2006), no. 1, 111 (English).

[Buc90] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Sémin. Théor. Nombres, Paris/Fr. 1988-89, Prog. Math. 91, 27-41 (1990)., 1990.

[BV13] Nicolas Bergeron and Akshay Venkatesh, *The asymptotic growth of torsion homology for arithmetic groups*, J. Inst. Math. Jussieu **12** (2013), no. 2, 391–447 (English).

[BVV19] Jean-François Biasse and Christine Van Vredendaal, *Fast multiquadratic S-unit computation and application to the calculation of class groups*, ANTS XIII. Proceedings of the thirteenth algorithmic number theory symposium, University of Wisconsin-Madison, WI, USA, July 16–20, 2018, Berkeley, CA: Mathematical Sciences Publishers (MSP), 2019, pp. 103–118 (English).

[Car19] Francisco C. Caramello, *Introduction to orbifolds*, Preprint, arXiv:1909.08699 [math.DG] (2019), 2019.

[CD23] Wouter Castryck and Thomas Decru, *An efficient key recovery attack on SIDH*, Advances in cryptology – EUROCRYPT 2023. 42nd annual international conference on the theory and applications of cryptographic techniques, Lyon, France, April 23–27, 2023. Proceedings. Part V, Cham: Springer, 2023, pp. 423–447 (English).

[CDW21] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski, *Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time*, J. ACM **68** (2021), no. 2, 26 (English), Id/No 8.

[CE15] Jean-Marc Couveignes and Tony Ezome, *Computing functions on Jacobians and their quotients*, LMS J. Comput. Math. **18** (2015), 555–577 (English).

[CF86] Ted Chinburg and Eduardo Friedman, *The smallest arithmetic hyperbolic three-orbifold*, Invent. Math. **86** (1986), 507–527 (English).

[CF99] ———, *An embedding theorem for quaternion algebras*, J. Lond. Math. Soc., II. Ser. **60** (1999), no. 1 (English).

[CFJR01] Ted Chinburg, Eduardo Friedman, Kerry. N. Jones, and Alan W. Reid, *The arithmetic hyperbolic* 3*-manifold of smallest volume*, Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser. **30** (2001), no. 1, 1–40 (English).

[CG18] Frank Calegari and David Geraghty, *Modularity lifting beyond the Taylor-Wiles method*, Invent. Math. **211** (2018), no. 1, 297–433 (English).

[Che79] Jeff Cheeger, *Analytic torsion and the heat equation*, Ann. Math. (2) **109** (1979), 259–322 (English).

[CK20] Leonardo Colò and David Kohel, *Orienting supersingular isogeny graphs*, J. Math. Cryptol. **14** (2020), 414–437 (English).

[CL00] D. Cooper and D. D. Long, *Free actions of finite groups on rational homology 3-spheres*, Topology Appl. **101** (2000), no. 2, 143–148 (English).

[CL23] Giulio Codogni and Guido Lido, *Spectral Theory of Isogeny Graphs*, Preprint, arXiv:2308.13913 [math.NT] (2023), 2023.

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology **22** (2009), no. 1, 93–113 (English).

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *CSIDH: an efficient post-quantum commutative group action*, Advances in cryptology – ASIACRYPT 2018. 24th international conference on the theory and application of cryptology and

information security, Brisbane, QLD, Australia, December 2–6, 2018. Proceedings. Part III, Cham: Springer, 2018, pp. 395–427 (English).

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comput. **88** (2019), no. 317, 1303–1339 (English).

[CN23] Ana Caraiani and James Newton, *On the modularity of elliptic curves over imaginary quadratic fields*, Preprint, arXiv:2301.10509 [math.NT] (2023), 2023.

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Grad. Texts Math., vol. 193, New York, NY: Springer, 2000 (English).

[Cou97] Jean-Marc Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive, Paper 2006/291, 1997.

[COU01] Laurent Clozel, Hee Oh, and Emmanuel Ullmo, *Hecke operators and equidistribution of Hecke points*, Invent. Math. **144** (2001), no. 2, 327–351 (English).

[CR81] Charles W. Curtis and Irving Reiner, *Methods of representation theory, with applications to finite groups and orders. Vol. I*, Pure and Applied Mathematics. A Wiley-Interscience Publication. New York etc.: John Wiley & Sons. XXI, 819 p. £ 40.70 (1981)., 1981.

[CV19] Frank Calegari and Akshay Venkatesh, *A torsion Jacquet-Langlands correspondence*, Astérisque, vol. 409, Paris: Société Mathématique de France (SMF), 2019 (English).

[dBDPMW20] Koen de Boer, Léo Ducas, Alice Pellet-Mary, and Benjamin Wesolowski, *Random self-reducibility of ideal-SVP via Arakelov random walks*, Advances in cryptology – CRYPTO 2020. 40th annual international cryptology conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020. Proceedings. Part II, Cham: Springer, 2020, pp. 243–273 (English).

[dBvW25] Koen de Boer and Wessel van Woerden, *Lattice-based cryptography: A survey on the security of the lattice-based NIST finalists*, Cryptology ePrint Archive, Paper 2025/304, 2025.

[DD09] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71 (English).

[DDF22] Pierrick Dartois and Luca De Feo, *On the security of OSIDH*, Public-key cryptography – PKC 2022. 25th IACR international conference on practice and theory

of public-key cryptography, virtual event, March 8–11, 2022. Proceedings. Part I, Cham: Springer, 2022, pp. 52–81 (English).

[Del73] Pierre Deligne, *La conjecture de Weil. I*, Publ. Math., Inst. Hautes Étud. Sci. **43** (1973), 273–307 (French).

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), no. 3, 209–247 (English).

[DFKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski, *SQISign: compact post-quantum signatures from quaternions and isogenies*, Advances in cryptology – ASIACRYPT 2020. 26th international conference on the theory and application of cryptology and information security, Daejeon, South Korea, December 7–11, 2020. Proceedings. Part I, Cham: Springer, 2020, pp. 64–93 (English).

[DG89] Dennis M. DeTurck and Carolyn S. Gordon, *Isospectral deformations. II: Trace formulas, metrics, and potentials*, Commun. Pure Appl. Math. **42** (1989), no. 8, 1067–1095 (English).

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **22** (1976), 644–654 (English).

[DK22] Samed Düzlü and Juliane Krämer, *Application of automorphic forms to lattice problems*, J. Math. Cryptol. **16** (2022), 156–197 (English).

[DR11] Peter G. Doyle and Juan Pablo Rossetti, *Laplace-isospectral hyperbolic 2-orbifolds are representation-equivalent*, Preprint, arXiv:1103.4372 [math.DG] (2011), 2011.

[dS98] Bart de Smit, *Generating arithmetically equivalent number fields with elliptic curves*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 392–399.

[dSP94] Bart de Smit and Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 2, 213–215.

[EGM98] J. Elstrodt, F. Grunewald, and J. Mennicke, *Groups acting on hyperbolic space. Harmonic analysis and number theory*, Springer Monogr. Math., Berlin: Springer, 1998 (English).

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit, *Supersingular isogeny graphs and endomorphism rings: reductions*

and solutions, Advances in cryptology – EUROCRYPT 2018. 37th annual international conference on the theory and applications of cryptographic techniques, Tel Aviv, Israel, April 29 – May 3, 2018. Proceedings. Part III, Cham: Springer, 2018, pp. 329–368 (English).

[Elk98] Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory. Proceedings of a conference in honor of A. O. L. Atkin, Chicago, IL, USA, September 1995, Providence, RI: American Mathematical Society, 1998, pp. 21–76 (English).

[FFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski, *SCALLOP: scaling the CSI-FiSh*, Public-key cryptography – PKC 2023. 26th IACR international conference on practice and theory of public-key cryptography, Atlanta, GA, USA, May 7–10, 2023. Proceedings. Part I, Cham: Springer, 2023, pp. 345–375 (English).

[FIK+25] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam, *Computing supersingular endomorphism rings using inseparable endomorphisms*, J. Algebra **668** (2025), 145–189 (English).

[Fun78] Takeo Funakura, *On Artin's theorem of induced characters*, Comment. Math. Univ. St. Pauli **27** (1978), 51–58 (English).

[Gaß26] F. Gaßmann, *Bemerkung zur vorstehenden Arbeit von Hurwitz über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppen.*, Math. Z. **25** (1926), 661–675 (German).

[Gel50] I. M. Gel'fand, *Spherical functions in symmetric Riemann spaces*, Doklady Akad. Nauk SSSR (N.S.) **70** (1950), 5–8. MR 33832

[GH24] Jayce R. Getz and Heekyoung Hahn, *An introduction to automorphic representations. With a view toward trace formulae*, Grad. Texts Math., vol. 300, Cham: Springer, 2024 (English).

[GKS11] Pierrick Gaudry, David Kohel, and Benjamin Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology – ASIACRYPT 2011. 17th international conference on the theory and application of cryptology and information security, Seoul, South Korea, December 4–8, 2011. Proceedings, Berlin:

Springer, 2011, pp. 504–519 (English).

[GM03] Daniel Goldstein and Andrew Mayer, *On the equidistribution of Hecke points*, Forum Math. **15** (2003), no. 2, 165–189 (English).

[GM09] Frederick W. Gehring and Gaven J. Martin, *Minimal co-volume hyperbolic lattices. I: The spherical points of a Kleinian group*, Ann. Math. (2) **170** (2009), no. 1, 123–161 (English).

[GMM09] David Gabai, Robert Meyerhoff, and Peter Milley, *Minimum volume cusped hyperbolic three-manifolds*, J. Am. Math. Soc. **22** (2009), no. 4, 1157–1215 (English).

[GMM11] ———, *Mom technology and volumes of hyperbolic 3-manifolds*, Comment. Math. Helv. **86** (2011), no. 1, 145–188 (English).

[Gor86] Carolyn S. Gordon, *Riemannian manifolds isospectral on functions but not on 1-forms*, J. Differ. Geom. **24** (1986), 79–96 (English).

[Gor00] ———, *Survey of isospectral manifolds*, Handbook of differential geometry. Vol. I, Amsterdam: North-Holland, 2000, pp. 747–778 (English).

[Gor09] Carolyn Gordon, *Sunada's isospectrality technique: two decades later*, Spectral analysis in geometry and number theory. International conference on the occasion of Toshikazu Sunada's 60th birthday, August 6–10, 2007, Providence, RI: American Mathematical Society (AMS), 2009, pp. 45–58 (English).

[Gor12] ———, *Orbifolds and their spectra*, Spectral geometry. Based on the international conference, Dartmouth, NH, USA, July 19–23, 2010, Providence, RI: American Mathematical Society (AMS), 2012, pp. 49–71 (English).

[GPS05] Carolyn Gordon, Peter Perry, and Dorothee Schueth, *Isospectral and isoscattering manifolds: a survey of techniques and examples*, Geometry, spectral theory, groups, and dynamics. Proceedings in memory of Robert Brooks, Haifa, Israel, December 29, 2003–January 2, 2004, January 5–9, 2004, Providence, RI: American Mathematical Society (AMS); Ramat Gan: Bar-Ilan University, 2005, pp. 157–179 (English).

[Gra84] Daniel R. Grayson, *Reduction theory using semistability*, Comment. Math. Helv. **59** (1984), 600–634 (English).

[GS12] Pierrick Gaudry and Éric Schost, *Genus 2 point counting over prime fields*, J. Symb. Comput. **47** (2012), no. 4, 368–400 (English).

[GWW92] C. Gordon, D. Webb, and S. Wolpert, *Isospectral plane domains and surfaces via Riemannian orbifolds*, Invent. Math. **110** (1992), no. 1, 1–22 (English).

[Hec37a] E. Hecke, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. I*, Math. Ann. **114** (1937), 1–28 (German).

[Hec37b] _____, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. II*, Math. Ann. **114** (1937), 316–351 (German).

[Her51] Ch. Hermite, *Sur l'introduction des variables continues dans la théorie des nombres.*, J. Reine Angew. Math. **41** (1851), 191–216 (French).

[Iwa64] Nagayoshi Iwahori, *On the structure of a Hecke ring of a Chevalley group over a finite field*, J. Fac. Sci., Univ. Tokyo, Sect. I **10** (1964), 215–236 (English).

[JDF11] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-quantum cryptography. 4th international workshop, PQCrypto 2011, Taipei, Taiwan, November 29–December 2, 2011. Proceedings, Berlin: Springer, 2011, pp. 19–34 (English).

[JL70] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lect. Notes Math., vol. 114, Springer, Cham, 1970 (English).

[JOP14] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot, *The past, evolving present, and future of the discrete logarithm*, Open problems in mathematics and computational science. Based on the presentations at the conference, Istanbul, Turkey, September 18–20, 2013, Cham: Springer, 2014, pp. 5–36 (English).

[Kac66] Mark Kac, *Can one hear the shape of a drum?*, Am. Math. Mon. **73** (1966), 1–23 (English).

[Kel14] Dubi Kelmer, *A refinement of strong multiplicity one for spectra of hyperbolic manifolds*, Trans. Am. Math. Soc. **366** (2014), no. 11, 5925–5961 (English).

[Kie20] Jean Kieffer, *Evaluating modular equations for abelian surfaces*, Preprint, arXiv:2010.10094 [math.NT] (2020), 2020.

[Kie22] _____, *Counting points on abelian surfaces over finite fields with Elkies's method*, Preprint, arXiv:2203.02009 [math.NT] (2022), 2022.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol, *On the quaternion ℓ-isogeny path problem*, LMS J. Comput. Math. **17A** (2014), 418–432 (English).

[Koh96] David Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

[Kol89] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Sha(E,\mathbb{Q})$ for a subclass of Weil curves*, Math. USSR, Izv. **32** (1989), no. 3, 523–541 (English).

[Kol90] ———, *Euler systems*, The Grothendieck Festschrift, Collect. Artic. in Honor of the 60th Birthday of A. Grothendieck. Vol. II, Prog. Math. 87, 435-483 (1990)., 1990.

[KS58] Kunihiko Kodaira and D. C. Spencer, *On deformations of complex analytic structures. I*, Ann. Math. (2) **67** (1958), 328–401 (English).

[Lan80] Robert P. Langlands, *Base change for* GL(2), Ann. Math. Stud., vol. 96, Princeton University Press, Princeton, NJ, 1980 (English).

[Lin15] Benjamin Linowitz, *Selective orders in central simple algebras and isospectral families of arithmetic manifolds*, Manuscr. Math. **147** (2015), no. 3-4, 399–413 (English).

[LL79] J.-P. Labesse and R. P. Langlands, *L-indistinguishability for SL(2)*, Can. J. Math. **31** (1979), 726–785 (English).

[LL24] Emilio A. Lauret and Benjamin Linowitz, *The spectral geometry of hyperbolic and spherical manifolds: analogies and open problems*, New York J. Math. **30** (2024), 682–721 (English).

[LLL82] A. K. Lenstra, H. W. jun. Lenstra, and László Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534 (English).

[LMF25] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2025.

[LMR13] Emilio A. Lauret, Roberto J. Miatello, and Juan P. Rossetti, *Strongly isospectral manifolds with nonisomorphic cohomology rings*, Rev. Mat. Iberoam. **29** (2013), no. 2, 611–634 (English).

[LMR15] E. A. Lauret, R. J. Miatello, and J. P. Rossetti, *Representation equivalence and p-spectrum of constant curvature space forms*, J. Geom. Anal. **25** (2015), no. 1, 564–591 (English).

[LN25] Jianwei Li and Phong Q. Nguyen, *A complete analysis of the BKZ lattice reduction algorithm*, J. Cryptology **38** (2025), no. 1, 58 (English), Id/No 12.

[LPS20] Andrea Lesavourey, Thomas Plantard, and Willy Susilo, *Short principal ideal problem in multicubic fields*, J. Math. Cryptol. **14** (2020), 359–392 (English).

[LS17] H. W. jun. Lenstra and A. Silverberg, *Roots of unity in orders*, Found. Comput. Math. **17** (2017), no. 3, 851–877 (English).

[LV15] Benjamin Linowitz and John Voight, *Small isospectral and nonisometric orbifolds of dimension 2 and 3*, Math. Z. **281** (2015), no. 1-2, 523–569 (English).

[Mac51] George W. Mackey, *On induced representations of groups*, Am. J. Math. **73** (1951), 576–592 (English).

[Mat67] Yozô Matsushima, *A formula for the Betti numbers of compact locally symmetric Riemannian manifolds*, J. Differ. Geom. **1** (1967), 99–109 (English).

[Maz73] Barry Mazur, *Notes on étale cohomology of number fields*, Ann. Sci. École Norm. Sup. (4) **6** (1973), 521–552 (1974).

[Maz89] B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$, Proc. Workshop, Berkeley/CA (USA) 1987, Publ., Math. Sci. Res. Inst. 16, 385-437 (1989)., 1989.

[Mes91] Jean-François Mestre, *Construction of genus 2 curves starting from their moduli*, Effective methods in algebraic geometry, Proc. Symp., Castiglioncello/Italy 1990, Prog. Math. 94, 313-334 (1991)., 1991.

[Mil64] John W. Milnor, *Eigenvalues of the Laplace operator on certain manifolds*, Proc. Natl. Acad. Sci. USA **51** (1964), 542 (English).

[Mil14] J. C. Miller, *Class numbers of real cyclotomic fields of composite conductor*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 404–417.

[MM12] Timothy H. Marshall and Gaven J. Martin, *Minimal co-volume hyperbolic lattices. II: Simple torsion in a Kleinian group*, Ann. Math. (2) **176** (2012), no. 1, 261–301 (English).

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski, *A direct key recovery attack on SIDH*, Advances in cryptology – EUROCRYPT 2023. 42nd annual international conference on the theory and applications of cryptographic techniques, Lyon, France, April 23–27, 2023. Proceedings. Part V, Cham: Springer, 2023, pp. 448–471 (English).

[Mol10] Pascal Molin, *On the calculation of roots of unity in a number field*, unpublished, 2010, available from `https://webusers.imj-prg.fr/~pascal.molin/pdf/nfunitroots.pdf`.

[Mor17] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions.*, Proc. Camb. Philos. Soc.

19 (1917), 117–124 (English).

[MP49] S. Minakshisundaram and Åke Pleijel, *Some properties of the Eigenfunctions of the Laplace-operator on Riemannian manifolds*, Can. J. Math. **1** (1949), 242–256 (English).

[MR03] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Grad. Texts Math., vol. 219, New York, NY: Springer, 2003 (English).

[MR24] Gustav Mårdby and Julie Rowlett, *112 years of listening to Riemannian manifolds*, Preprint, arXiv:2406.18369 [math.SP] (2024), 2024.

[Mül78] Werner Müller, *Analytic torsion and R-torsion of Riemannian manifolds*, Adv. Math. **28** (1978), 233–305 (English).

[Mül93] ———, *Analytic torsion and R-torsion for unimodular representations*, J. Am. Math. Soc. **6** (1993), no. 3, 721–753 (English).

[MW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski, *Unconditional foundations for supersingular isogeny-based cryptography*, arXiv preprint arXiv:2502.17010 (2025).

[Par77] Charles J. Parry, *Class number formulae for bicubic fields*, Ill. J. Math. **21** (1977), 148–163 (English).

[Per77] Robert Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$*, J. Number Theory **9** (1977), 342–360 (English).

[Pes95] Hubert Pesce, *Strongly isospectral hyperbolic and elliptic manifolds*, J. Funct. Anal. **134** (1995), no. 2, 363–391 (French).

[Piz90] Arnold K. Pizer, *Ramanujan graphs and Hecke operators*, Bull. Am. Math. Soc., New Ser. **23** (1990), no. 1, 127–137 (English).

[PMHS19] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé, *Approx-SVP in ideal lattices with pre-processing*, Advances in cryptology – EUROCRYPT 2019. 38th annual international conference on the theory and applications of cryptographic techniques, Darmstadt, Germany, May 19–23, 2019. Proceedings. Part II, Cham: Springer, 2019, pp. 685–716 (English).

[Rai21] Jean Raimbault, *Analytic torsion, regulators and arithmetic hyperbolic manifolds*, Arithmetic L-functions and differential geometric methods. Regulators IV, May 2016, Paris, Cham: Birkhäuser, 2021, pp. 179–212 (English).

[Raj07] C. S. Rajan, *On isospectral arithmetical spaces*, Am. J. Math. **129** (2007), no. 3, 791–806 (English).

[Raj10] Conjeeveram S. Rajan, *Some questions on spectrum and arithmetic of locally symmetric spaces*, Algebraic and arithmetic structures of moduli spaces. Proceedings of the conference, Sapporo, Japan, September 2007, Tokyo: Mathematical Society of Japan (MSJ), 2010, pp. 137–157 (English).

[Ram16] Srinivasa Ramanujan, *On certain arithmetical functions*, Trans. Camb. Philos. Soc. **22** (1916), 159–184 (English).

[Rob22] Damien Robert, *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*, Cryptology ePrint Archive, Paper 2022/1704, 2022.

[Rob23] Damien Robert, *Breaking SIDH in polynomial time*, Advances in cryptology – EUROCRYPT 2023. 42nd annual international conference on the theory and applications of cryptographic techniques, Lyon, France, April 23–27, 2023. Proceedings. Part V, Cham: Springer, 2023, pp. 472–503 (English).

[Ros97] Steven Rosenberg, *The Laplacian on a Riemannian manifold. An introduction to analysis on manifolds*, Lond. Math. Soc. Stud. Texts, vol. 31, Cambridge: Cambridge University Press, 1997 (English).

[RS71] D. B. Ray and I. M. Singer, *R-torsion and the Laplacian on Riemannian manifolds*, Adv. Math. **7** (1971), 145–210 (English).

[RS06] Alexander Rostovtsev and Anton Stolbunov, *PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES*, Cryptology ePrint Archive, Paper 2006/145, 2006.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21** (1978), 120–126 (English).

[RW70] Y. H. Rhie and G. Whaples, *Hecke operators in cohomology of groups*, J. Math. Soc. Japan **22** (1970), 431–442 (English).

[Sat62] Ichirô Satake, *On spherical functions over p-adic fields*, Proc. Japan Acad. **38** (1962), 422–425 (English).

[Sat63] ———, *Theory of spherical functions on reductive algebraic groups over p-adic fields*, Publ. Math., Inst. Hautes Étud. Sci. **18** (1963), 229–293 (English).

[Sch85] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comput. **44** (1985), 483–494 (English).

[Sch87] C. P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theor. Comput. Sci. **53** (1987), 201–224 (English).

[Sch94] Dorothee Schueth, *Isospectral, non-isometric Riemannian manifolds*, Proceedings of the winter school on geometry and physics, Zdíkov, Czech Republic, January 1993, Palermo: Circolo Matematico di Palermo, 1994, pp. 207–231 (English).

[Sch95] René Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordx. **7** (1995), no. 1, 219–254 (English).

[Sch15] Peter Scholze, *On torsion in the cohomology of locally symmetric varieties*, Ann. Math. (2) **182** (2015), no. 3, 945–1066 (English).

[See67] R. T. Seeley, *Complex powers of an elliptic operator*, Proc. Sympos. Pure Math. 10, 288-307 (1967)., 1967.

[Sel56] Atle Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc., New Ser. **20** (1956), 47–87 (English).

[Shi59] Goro Shimura, *On integrals attached to automorphic forms*, J. Math. Soc. Japan **11** (1959), 291–311 (French).

[Sho97] Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509 (English).

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math., vol. 106, Springer, Cham, 1986 (English).

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve.*, Trans. Am. Math. Soc. **356** (2004), no. 3, 1209–1231 (English).

[Sun85] Toshikazu Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. (2) **121** (1985), no. 1, 169–186.

[SW14] Uri Shapira and Barak Weiss, *A volume estimate for the set of stable lattices*, C. R., Math., Acad. Sci. Paris **352** (2014), no. 11, 875–879 (English).

[Tam60] T. Tamagawa, *On Selberg's trace formula*, J. Fac. Sci., Univ. Tokyo, Sect. I **8** (1960), 363–386 (English).

[Tam63] Tsuneo Tamagawa, *On the ζ-functions of a division algebra*, Ann. Math. (2) **77** (1963), 387–405 (English).

[Ten21] Anda Tenie, *Strongly isospectral hyperbolic 3-manifolds with nonisomorphic rational cohomology rings*, Preprint, arXiv:2111.11454 [math.GT] (2021), 2021.

[The23] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.15.4*, 2023, available from `http://pari.math.u-bordeaux.fr/`.

[Thu98] Jeffrey Lin Thunder, *Higher-dimensional analogs of Hermite's constant*, Mich. Math. J. **45** (1998), no. 2, 301–314 (English).

[Thu22] William P. Thurston, *The geometry and topology of three-manifolds. Vol. IV*, American Mathematical Society, Providence, RI, [2022] ©2022, Edited and with a preface by Steven P. Kerckhoff and a chapter by J. W. Milnor.

[TV16] David Treumann and Akshay Venkatesh, *Functoriality, Smith theory, and the Brauer homomorphism*, Ann. Math. (2) **183** (2016), no. 1, 177–228 (English).

[Vig80] Marie-France Vignéras, *Isospectral and non-isometric Riemannian manifolds*, Ann. Math. (2) **112** (1980), 21–32 (French).

[Voi21] John Voight, *Quaternion algebras*, Grad. Texts Math., vol. 288, Cham: Springer, 2021 (English).

[Wad66] Hideo Wada, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci., Univ. Tokyo, Sect. I **13** (1966), 201–209 (English).

[Wal13] C. T. C. Wall, *On the structure of finite groups with periodic cohomology.*, Lie groups: structure, actions, and representations. In honor of Joseph A. Wolf on the occasion of his 75th birthday, New York, NY: Birkhäuser/Springer, 2013, pp. 381–413 (English).

[Wes22] Benjamin Wesolowski, *The supersingular isogeny path and endomorphism ring problems are equivalent*, FOCS 2021-62nd Annual IEEE Symposium on Foundations of Computer Science, 2022.

[Wol67] J. A. Wolf, *Spaces of constant curvature*, New York-St. Louis-San Francisco-Toronto-London-Sydney: McGraw-Hill Book Comp. XV, 408 p. (1967)., 1967.

[Wol01] Joseph A. Wolf, *Isospectrality for spherical space forms*, Result. Math. **40** (2001), no. 1-4, 321–338 (English).

[Yos83] Tomoyuki Yoshida, *On G-functors. II: Hecke operators and G-functors*, J. Math. Soc. Japan **35** (1983), 179–190 (English).