ARITHMETIC EQUIVALENCE AND ISOSPECTRALITY

ANDREW V. SUTHERLAND

ABSTRACT. In these lecture notes we give an introduction to the theory of *arithmetic equivalence*, a notion originally introduced in a number theoretic setting to refer to number fields with the same zeta function. Gassmann established a direct relationship between arithmetic equivalence and a purely group theoretic notion of equivalence that has since been exploited in several other areas of mathematics, most notably in the spectral theory of Riemannian manifolds by Sunada. We will explicate these results and discuss some applications and generalizations.

1. An introduction to arithmetic equivalence and isospectrality

Let K be a number field (a finite extension of $\mathbf{Q}$), and let $\mathcal{O}_K$ be its ring of integers (the integral closure of $\mathbf{Z}$ in K). The *Dedekind zeta function* of K is defined by the Dirichlet series

$$\zeta_K(s) := \sum_{I \subseteq \mathcal{O}_K} N(I)^{-s} = \prod_{p} (1 - N(\mathfrak{p})^{-s})^{-1}$$

where the sum ranges over nonzero $\mathcal{O}_K$-ideals, the product ranges over nonzero prime ideals, and $N(I) := [\mathcal{O}_K : I]$ is the absolute norm. For $K = \mathbf{Q}$ the Dedekind zeta function $\zeta_{\mathbf{Q}}(s)$ is simply the Riemann zeta function $\zeta(s) := \sum_{n \geq 1} n^{-s}$. As with the Riemann zeta function, the Dirichlet series (and corresponding Euler product) defining the Dedekind zeta function converges absolutely and uniformly to a nonzero holomorphic function on $\mathrm{Re}(s) > 1$, and $\zeta_K(s)$ extends to a meromorphic function on $\mathbf{C}$ and satisfies a functional equation, as shown by Hecke [25].

The Dedekind zeta function encodes many features of the number field K: it has a simple pole at $s = 1$ whose residue is intimately related to several invariants of K, including its class number, and as with the Riemann zeta function, the zeros of $\zeta_K(s)$ are intimately related to the distribution of prime ideals in $\mathcal{O}_K$. There is also a natural generalization of the Riemann hypothesis, which states that all zeros of $\zeta_K(s)$ that are not on the real line lie on the vertical line $\mathrm{Re}(s) = 1/2$.

It is thus natural to ask the following question: to what extent does $\zeta_K(s)$ determine the field K? Number fields with the same Dedekind zeta function are said to be *arithmetically equivalent*, and our question amounts to asking whether arithmetically equivalent number fields are necessarily isomorphic, and if not, how "non isomorphic" can they be?

Let us begin by considering two numbers fields K_1 and K_2. Let $L/\mathbf{Q}$ be a finite Galois extension containing both K_1 and K_2 (the compositum of their Galois closures, for example). Let $G := \mathrm{Gal}(L/\mathbf{Q})$, and let $H_1 := \mathrm{Gal}(L/K_1) \leq G$ and $H_2 := \mathrm{Gal}(L/K_2) \leq G$, so that $K_1 = L^{H_1}$ and $K_2 = L^{H_2}$. In 1925 Fritz Gassmann [17] made the remarkable observation that the arithmetic equivalence of K_1 and K_2 (or lack thereof) is completely determined by a simple relationship between $H_1, H_2 \leq G$.

Definition 1.1. Let H_1, H_2 be subgroups of a finite group G. We say that H_1 and H_2 are *Gassmann equivalent* (or *almost conjugate*) and call (G, H_1, H_2) a *Gassmann triple* if there is a bijection of set $H_1 \longleftrightarrow H_2$ that preserves G-conjugacy. Equivalently, for all $g \in G$ we have

$$\#(H_1 \cap g^G) = \#(H_2 \cap g^G),$$

where g^G is the G-conjugacy class of g. This defines an equivalence relation on the subgroups of G.

If $H_1, H_2 \le G$ are conjugate then (G, H_1, H_2) is obviously a Gassmann triple; we are interested in *non-trivial* Gassmann triples, those in which H_1 and H_2 are not G-conjugate.

Example 1.2. Let p be prime and consider the following subgroups of $G := \mathbf{GL}_2(\mathbf{F}_p)$:

$$H_1 := \left\{ \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbf{F}_p) \right\} \qquad\qquad H_2 := \left\{ \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbf{F}_p) \right\}$$

The bijection $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \longleftrightarrow \left(\begin{smallmatrix} d & b \\ 0 & a \end{smallmatrix}\right)$ preserves G-conjugacy, so (G, H_1, H_2) is a Gassmann triple. For $p > 2$ the subgroups H_1 and H_2 are not conjugate in G; the since the elements H_1 have a common 1-eigenspace (under the left-action of G on column vectors), but this is not true of H_2.

In the previous example the Gassmann equivalent subgroups H_1 and H_2 are isomorphic, and in fact one can embed G in a larger group G' in which H_1 and H_2 are G'-conjugate. If (G, H_1, H_2) is a Gassmann triple, then H_1 and H_2 necessarily have the same cardinality (there is a bijection between them). The order of a group element is determined by its conjugacy class, so H_1 and H_2 must also have the same *order statistics*, which for any finite group H we define as the integer function

$$\begin{aligned} \phi_H \colon \mathbf{Z} &\to \mathbf{Z} \\ e &\mapsto \#\{h \in H : |h| = e\}; \end{aligned}$$

note that ϕ_H depends only on the isomorphism class of H as an abstract group. If H_1 and H_2 are Gassmann equivalent (as subgroups of some G), then $\phi_{H_1} = \phi_{H_2}$. For any particular G the converse need not hold, but if we work in the category of abstract groups, and give ourselves the freedom to choose G, compatibility of order statistics is the only constraint.

Theorem 1.3. *Let H_1 and H_2 be finite groups. There exists a Gassmann triple (G, H_1', H_2') with $H_1' \simeq H_1$ and $H_2' \simeq H_2$ if and only if H_1 and H_2 have the same order statistics $\phi_{H_1} = \phi_{H_2}$.*

Proof. As noted above, the forward implication is immediate. For the reverse, assume $\phi_{H_1} = \phi_{H_2}$, let $n := \#H_1 = \#H_2$, let $G := S_n$ be the symmetric group on n-letters, and for $i = 1, 2$ let $H_i' \le G$ be the left regular permutation representation of H_i. Each $h \in H_i'$ is a permutation consisting of $n/|h|$ cycles of length $|h|$. Thus $h_1 \in H_1'$ and $h_2 \in H_2'$ are conjugate in G if and only if they have the same order. Any bijection $H_1 \longleftrightarrow H_2$ that preserves element orders thus preserves G-conjugacy, and since H_1' and H_2' have the same order statistics, such a bijection exists. $\square$

Abelian groups with the same order statistics are necessarily isomorphic, but this is not true in general; the smallest examples of group $H_1 \not\simeq H_2$ with the same order statistics have order 16 (the groups with GAP [16] identifiers $\langle 16, 10\rangle$ and $\langle 16, 13\rangle$ are an example). The following example provides an infinite family of non-isomorphic pairs of groups with the same order statistics from which we can construct Gassmann triples via Theorem 1.3 above.

Example 1.4. Following [32], let p be an odd prime and let

$$H_1 := (\mathbf{Z}/p\mathbf{Z})^3 \qquad \text{and} \qquad H_2 := \left\{ \left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right) \in \mathbf{SL}_3(\mathbf{F}_p) \right\}.$$

These groups are non-isomorphic, since H_1 is abelian and the Heisenberg group H_2 is not, but they both contain $p^3 - 1$ elements of order p and one element of order 1; thus $\phi_{H_1} = \phi_{H_2}$. As in the proof of Theorem 1.3, we can embed H_1 and H_2 in $G := S_{p^3}$ to obtain a Gassmann triple (G, H_1, H_2) (in fact, we can embed them in a subgroup $G \le S_{p^3}$ of order p^6). We also note that $n \ge 2$, the products $H_1^i \times H_2^{n-i}$ for $0 < i < n$ are nonisomorphic and have the same order statistics (they are all p-groups of exponent p). Thus for every integer $n \ge 2$ and every odd prime p, the symmetric group $S_{p^{3n}}$ contains n pairwise non-isomorphic Gassmann equivalent subgroups of order p^{3n}.

We now state Gassmann's main result [17], which can also be found in [9, Ex. 6.4] and [40, Thm. 1].

Theorem 1.5 (Gassmann, 1925). *Subfields K_1 and K_2 of a finite Galois extension $L/\mathbf{Q}$ are arithmetically equivalent if and only if the subgroups* $\mathrm{Gal}(L/K_1)$ *and* $\mathrm{Gal}(L/K_2)$ *of* $\mathrm{Gal}(L/\mathbf{Q})$ *are Gassmann equivalent.*

We will prove this theorem in the next lecture. Note the number fields $K_1, K_2 \subseteq L$ in Gassmann's theorem are isomorphic if and only if $H_1 := \mathrm{Gal}(L/K_1)$ and $H_2 := \mathrm{Gal}(L/K_2)$ conjugate in $G := \mathrm{Gal}(L/\mathbf{Q})$. Thus given any non-trivial Gassmann triple (G, H_1, H_2), provided we can realize G as $\mathrm{Gal}(L/\mathbf{Q})$ for some Galois extension $L/\mathbf{Q}$, we can construct non-isomorphic arithmetically equivalent number fields $K_1 := L^{H_1}$ and $K_2 := L^{H_2}$, and every non-trivial example of arithmetically equivalent number fields arises in this way. Every symmetric group can certainly be realized as the Galois group of a number field, so Example 1.4 already provides many examples, but the degree of the number fields involved may be very large. Below we give another example that involves extensions of lower degree.

Example 1.6. For $G = \mathbf{GL}_2(\mathbf{F}_p)$ we can explicitly construct $L/\mathbf{Q}$ with $\mathrm{Gal}(L/\mathbf{Q}) = G$ using the p-torsion field of an elliptic curve, as exploited in [12], for example. If $E/\mathbf{Q}$ is an elliptic curve (which we recall is an abelian variety of dimension one), the field $\mathbf{Q}(E[p])$ generated by the coordinates of its p-torsion points in $\overline{\mathbf{Q}}$ is a Galois extension of $\mathbf{Q}$ whose Galois group is isomorphic to a subgroup of

$$\mathrm{Aut}(E[p]) \simeq \mathrm{Aut}(\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{GL}_2(\mathbf{F}_p)$$

By Serre's open image theorem [44], for elliptic curves $E/\mathbf{Q}$ without complex multiplication we will have $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \simeq \mathbf{GL}_2(\mathbf{F}_p)$ for all but finitely many primes p, and in fact for almost all $E/\mathbf{Q}$ this will be true for *every* prime p, as shown in [28]. The elliptic curve $y^2 + y = x^3 - x$ with Cremona label `37a1` is an example; more than a million others can be found in the *L-functions and modular forms database*. If we now take H_1 and H_2 as in Example 1.2, we obtain arithmetically equivalent non-isomorphic number fields $K_1 := \mathbf{Q}(E[p])^{H_1}$ and $K_2 := \mathbf{Q}(E[p])^{H_2}$ of degree $p^2 - 1$. For $p = 3$ we have $p^2 - 1 = 8$, which is nearly the best possible (the smallest degree in which one finds arithmetically equivalent non-isomorphic number fields is 7, as shown in [3]).

1.1. **Hearing the shape of a drum.** One can attach zeta functions to many other mathematical objects. Let us now consider the case of a *Riemannian manifold* M, a smooth manifold equipped with a Riemannian metric g. Recall that a smooth manifold (of dimension n) is a second countable Hausdorff space equipped with an atlas of charts $\varphi_U \colon U \to \mathbf{R}^n$ indexed by an open cover $\mathfrak{U}$ such that each chart defines a homeomorphism and the transition maps $\varphi_U \circ \varphi_V^{-1} \colon \varphi(U \cap V) \to \varphi_V(U \cap V)$ on overlapping charts are (infinitely differentiable) diffeomorphisms. We use $C^\infty(M)$ to denote the $\mathbf{R}$-algebra of *smooth functions* $f : M \to \mathbf{R}$, those for which $f \circ \varphi_U^{-1}$ is infinitely differentiable for all $U \in \mathfrak{U}$.

The Riemannian metric g is a symmetric positive definite $(0,2)$-tensor field,[1] which we may view as a smoothly varying inner product $\langle \cdot, \cdot \rangle_g$ on the tangent spaces T_x; here T_x is the n-dimensional $\mathbf{R}$-vector space of $\mathbf{R}$-linear maps $v \colon C^\infty(M) \to \mathbf{R}$ that satisfy $v(fg) = f(x)v(g) + v(f)g(x)$ for all $f, g \in C^\infty(M)$; these are *derivations* of $C^\infty(M)$ at x (the tangent space can also be defined using isomorphism classes of curves through x). The disjoint union $T(M) := \sqcup_{x \in M} T_x$ is the *tangent bundle* of M; it has a natural structure as a smooth manifold of dimension $2n$ equipped with a smooth projection $T(M) \to M$ whose fibers are tangent spaces. The *cotangent bundle* $T^*(M)$ is similarly defined using the dual spaces T_x^*. We now define the following:

[1] We follow the (mostly) standard convention that a (p,q)-tensor field is p-contravariant and q-covariant, meaning that its elements can be viewed as smoothly-varying multi-linear functions $(T_x^*)^p \times (T_x)^q \to \mathbf{R}$, or as smoothly varying elements of $(T_x)^{\otimes p} \otimes (T_x^*)^{\otimes q}$, where T_x is the tangent space at $x \in M$ and T_x^* is the cotangent space.

- $\mathcal{T}(M)$ is the $C^\infty(M)$-module of smooth sections of $T(M)$.
  Elements of $\mathcal{T}(M)$ are $(1,0)$-tensor fields (vector fields), equivalently, derivations of $C^\infty(M)$, which can be viewed as functions $C^\infty(M) \to C^\infty(M)$ corresponding to directional derivatives.
- $\mathcal{T}^*(M)$ is the $C^\infty(M)$-module of smooth sections of $T^*(M)$.
  Elements of $\mathcal{T}^*(M)$ are $(0,1)$-tensor fields, also known as differential 1-forms, and can be viewed as functions $\mathcal{T}(M) \to C^\infty(M)$; for any $f \in C^\infty(M)$, the map $df: X \mapsto X(f)$ lies in $\mathcal{T}^*(M)$.

The metric g can be viewed as a symmetric $C^\infty(M)$-bilinear map $\mathcal{T}(M) \times \mathcal{T}(M) \to C^\infty(M)$. It uniquely determines an isomorphism $\flat\colon \mathcal{T}(M) \to \mathcal{T}^*(M)$ via $X^\flat := (Y \mapsto \langle X, Y\rangle_g)$, which together with its inverse $\sharp\colon \mathcal{T}^*(M) \to \mathcal{T}(M)$ is known as a *musical isomorphism*.

We also have the *Levi-Civita connection* $\nabla\colon \mathcal{T}(M) \times \mathcal{T}(M) \to \mathcal{T}(M)$, the unique torsion-free affine connection compatible with g. This means that for all $f \in C^\infty(M)$ and $X, Y, Z \in \mathcal{T}(M)$ we have

- $\nabla(fX, Y) = f\nabla(X, Y)$ and $\nabla(X, fY) = X(f)Y + f\nabla(X, Y)$ (affine connection),
- $\nabla(X, Y) - \nabla(Y, X) = XY - YX$ (torsion free),
- $X(g(Y, Z)) = g(\nabla(X, Y), Z) + g(Y, \nabla(X, Z))$ (compatible with g).

Note that while ∇ is $\mathbf{R}$-bilinear, it is $C^\infty(M)$-linear only in the first argument. We can alternatively view the Levi-Civita connection as a $C^\infty(M)$-linear map

$$\begin{aligned} \mathcal{T}(M) &\to (\mathcal{T}(M) \to \mathcal{T}(M)) \\ X &\mapsto \nabla_X := (Y \mapsto \nabla(X, Y)). \end{aligned}$$

We define the *trace* of a $C^\infty(M)$-linear map $\mathcal{T}(M) \to \mathcal{T}(M)$ as the function in $C^\infty(M)$ obtained by taking the trace of the linear map on the tangent space at each point. We now define the $\mathbf{R}$-linear operators

$$\begin{aligned} \mathrm{grad}\colon C^\infty(M) &\to \mathcal{T}(M) & \qquad \mathrm{div}\colon \mathcal{T}(M) &\to C^\infty(M) \\ f &\mapsto df^\sharp & X &\mapsto \mathrm{tr}(\nabla_X), \end{aligned}$$

and our main object of interest, the *Laplace-Beltrami operator*

$$\begin{aligned} \Delta_M\colon C^\infty(M) &\to C^\infty(M) \\ f &\mapsto -\mathrm{div}\,\mathrm{grad}\, f \qquad \text{(note the sign).} \end{aligned}$$

All of the operators we have defined intrinsically depend on the metric g, even though we do not highlight this dependence in our notation. Whenever we refer to a Riemannian manifold M we understand that it is equipped with a Riemannian metric (some authors write (M, g) to emphasize the the metric, but we view g is baked into the definition of M).

Theorem 1.7. *Let M be a compact connected Riemannian manifold. The eigenspaces of Δ_M all have finite dimension, and the corresponding eigenvalues form a countable discrete sequence of non-negative real numbers. If we enumerate the eigenvalues with multiplicity as*

$$0 = \lambda_0 < \lambda_1 \le \lambda_2 \le \cdots$$

then there exists an orthonormal sequence of $C^\infty(M)$ functions $\{1 = f_0, f_1, f_2, \ldots\}$ with $\Delta_M f_i = \lambda_i f_i$ that contains a basis for every eigenspace and generates a dense subspace of $L^2(M)$ in the L^2-norm topology.

Proof. See [2, pp. 54-55] for a sketch of the proof (with references to further details). □

The ordered sequence of **nonzero** eigenvalues of Δ_M (listed with multiplicity) is the *eigenvalue spectrum* of M, denoted $\lambda(M)$. Riemannian manifolds with the same spectrum are said to be *isospectral*.

Definition 1.8. Let M be a compact connected Riemannian manifold of dimension n with eigenvalue spectrum $\lambda(M) = (\lambda_i)_{i\geq 1}$. The (Minakshisundaram-Pleijel) *zeta function* of M is defined by the generalized Dirichlet series

$$\zeta_M(s) = \sum_{i\geq 1} \lambda_i^{-s},$$

which converges absolutely and uniformly to a holomorphic function on some right half plane and has a meromorphic continuation to $\mathbf{C}$ that is holomorphic except for simple poles at integers $1, \ldots, n/2$ if n is even and half integers $n/2, n/2-1, \ldots$ if n is odd [34].

Lemma 1.9. *Let M_1 and M_2 be compact connected Riemannian manifolds. Then $\lambda(M_1) = \lambda(M_2)$ if and only if $\zeta_{M_1}(s) = \zeta_{M_2}(s)$.*

Proof. The forward implication is obvious. For the reverse, suppose $\zeta_{M_1}(s) = \zeta_{M_2}(s)$ but $\lambda(M_1) \neq \lambda(M_2)$. Without loss of generality we may assume that there is a positive integer j such that $\lambda_i(M_1) = \lambda_i(M_2)$ for $1 \leq i < j$ and $\lambda_j(M_1) > \lambda_j(M_2)$. Note that this implies $\lambda_j(M_1) > \lambda_i(M_2)$ for all $i \geq j$. Let n_j be the multiplicity of $\lambda_j(M_1)$ in $\lambda(M_1)$ and let σ be the maximum of the abscissa of convergence for the generalized Dirichlet series defining $\zeta_{M_1}(s)$ and $\zeta_{M_2}(s)$. We have

$$\zeta_{M_1}(t) - \zeta_{M_2}(t) \sim n_j \lambda_j(M_1)^{-t}$$

as $t \geq \sigma$ tends to infinity along the real line, but this contradicts $\zeta_{M_1}(s) = \zeta_{M_2}(s)$. $\square$

Example 1.10. Let S^1 be the unit circle in $\mathbf{R}^2$. Then $\lambda(S^1) = \{n^2 : n \geq 1 \text{ with multiplicity } 2\}$ and we have $\zeta_{S^1}(s) = \sum_{n\geq 1} 2n^{-2s} = 2\zeta(2s)$, where $\zeta(s) := \sum_{n\geq 1} n^{-s}$ is the Riemann zeta function.

Definition 1.11. A (full) *lattice* Λ in $\mathbf{R}^n$ is the $\mathbf{Z}$-span of a basis for $\mathbf{R}^n$, the *dual lattice* is defined by

$$\Lambda^* := \{v \in \mathbf{R}^n : \langle v, w\rangle \in \mathbf{Z} \text{ for all } w \in \Lambda\},$$

where $\langle \cdot, \cdot \rangle$ is the Euclidean inner product (dot product). We say that Λ is

- *integral* if $\langle v, w\rangle \in \mathbf{Z}$ for all $v, w \in \Lambda$ (equivalently, $\Lambda \subseteq \Lambda^*$);
- *even* if $\langle v, w\rangle \in 2\mathbf{Z}$ for all $v, w \in \Lambda$ (implies integral);
- *unimodular* if Λ has covolume $\mu(\mathbf{R}^n/\Lambda) = 1$;
- *self dual* if $\Lambda = \Lambda^*$ (equivalently, Λ is integral and unimodular).

Two lattices in $\mathbf{R}^n$ are *isomorphic* if they are related by an orthogonal linear transformation.

Definition 1.12. Let Λ be a lattice in $\mathbf{R}^n$. The *theta series* of Λ is defined by the formal q-series

$$\Theta_\Lambda(q) := \sum_{v\in\Lambda} q^{\langle v,v\rangle/2},$$

If we substitute $q = e^{-2\pi s}$ we obtain a holomorphic function on $\mathrm{Re}(s) > 0$. The *zeta function* of Λ is

$$\zeta_\Lambda(s) := \sum_{v\in\Lambda-\{0\}} \langle v, v\rangle^{-s},$$

which can be derived from Θ_Λ by taking a Mellin transform:

$$\zeta_\Lambda(s) = \pi^s \Gamma(s)^{-1} \int_0^\infty \Theta_\Lambda(e^{-2\pi t}) - 1) t^{s-1} dt.$$

This formula can be inverted using the inverse Mellin transform, thus ζ_Λ and Θ_Λ determine each other.

Example 1.13. Let $M := \mathbf{R}^n/\Lambda$ be the torus defined by a lattice Λ in $\mathbf{R}^n$ equipped with the flat metric (here "flat" means zero curvature; this is not the metric induced by the standard embedding in $\mathbf{R}^{n+1}$). The eigenvalue spectrum of M is

$$\lambda(M) = \{4\pi^2\langle v, v\rangle : \text{nonzero } v \in \Lambda^*\},$$

with corresponding eigenfunctions are $\{e^{2\pi i\langle v,x\rangle} : \text{nonzero } v \in \Lambda^*\}$. If Λ is self-dual then

$$\zeta_M(s) = \sum_{v\in\Lambda-\{0\}} (4\pi^2\langle v, v\rangle)^{-s} = \zeta_{2\pi\Lambda}(s),$$

which we note is determined by (and determines) $\Theta_\Lambda(q)$, since $\Theta_{2\pi\Lambda}(q) = \Theta_\Lambda(4\pi^2 q)$.

Example 1.14. For integers $n \geq 3$ the lattice D_n is defined by

$$D_n := \{(a_1, \ldots, a_n) \in \mathbf{Z}^n : a_1 + \cdots a_n \equiv 0 \bmod 2\};$$

it is an even lattice but is not self-dual. For even integers $n \geq 4$ we define the lattice

$$D_n^+ := D_n \cup (D_n + h),$$

where $h = (\frac{1}{2}, \ldots, \frac{1}{2})$, which is even and self-dual for n divisible by 4 (in fact $D_4^+ \simeq \mathbf{Z}^4$).

The lattice D_8^+ is more commonly known as E_8; up to isomorphism it is the unique even self-dual lattice of dimension 8. In dimension 16 there are two even self-dual lattices (up to isomorphism): $E_8 \oplus E_8$ and D_{16}^+. As shown by Witt [55], these non-isomorphic lattices have the same theta series. This follows from the fact that the theta series of even self-dual lattices of dimension n correspond to a modular form of weight $n/2$. More precisely for any such lattice, the function

$$\theta_\Lambda(\tau) := \Theta_\Lambda(e^{2\pi i\tau})$$

satisfies:

- $\theta_\Lambda(\tau)$ is holomorphic on the upper half plane $\mathrm{Im}(\tau) > 0$;
- $\theta_\Lambda(\tau + 1) = \theta_\Lambda(\tau)$ and $\theta_\Lambda(-1/\tau) = \tau^{n/2}\theta_\Lambda(\tau)$;
- $\theta_\Lambda(\tau)$ remains bounded as $\mathrm{Im}\,\tau \to \infty$ in the strip $0 \leq \mathrm{Re}(\tau) < 1$.

This implies that $\theta_\Lambda(\tau)$ is a modular form of weight $n/2$ for the full modular group $\mathbf{SL}_2(\mathbf{Z})$. For $n = 16$ the space of (new) modular forms of weight $n/2 = 8$ for $\mathbf{SL}_2(\mathbf{Z})$ has dimension 1, so the q-series of any two such modular forms differ only by a scalar; the q-series defining $\theta_\Lambda(\tau)$ has constant coefficient 1, so there is only one possible theta series for an even self-dual lattice of dimension 16. It follows that the corresponding flat tori have the same zeta function

$$\zeta_{\mathbf{R}^{16}/E_8\oplus E_8}(s) = \zeta_{\mathbf{R}^{16}/D_{16}^+}(s),$$

as observed by Milnor [36] in 1964.

In 1966 Mark Kac famously asked "Can one hear the shape of a drum?" [29]. Kac was asking whether the eigenvalue spectrum of a compact Riemannian manifold M in the Euclidean plane determines M up to isomorphism (for manifolds with boundary one restricts to functions with vanishing normal derivative at the boundary when considering the eigenvalue spectrum). It was already known that isospectral manifolds need not be isomorphic in general, as noted in Example 1.14. Twenty-five years later Gordon, Webb, and Wolpert [21] negatively answered Kac's question by extending a general method for constructing non-isomorphic isospectral manifolds that was introduced by Sunada in the mid 1980s. Sunada's result makes essential use of Gassmann triples.

1.2. **Riemannian coverings.** We now work in the category of smooth connected manifolds whose morphisms are smooth maps (they induce C^∞-maps of Euclidean spaces locally).

A *smooth cover* (or *smooth covering*) is a surjective morphism $\pi\colon M \to X$ of smooth connected manifolds that is a local diffeomorphism: every point in X has an open neighborhood U such that each connected component of $\pi^{-1}(U)$ is mapped diffeomorphically onto U by π. Smooth covers preserve dimension and are unramified. The composition of smooth covers is a smooth cover, as is the identity map, so for each $n \geq 1$ we have a subcategory of smooth covers of smooth connected manifolds of dimension n; if we fix the base X we obtain the category of smooth covering spaces of X.

A smooth cover $\pi\colon M \to X$ is called a *universal cover* if M is simply connected. It has the universal property that every smooth cover $\psi\colon N \to X$ admits a smooth cover $\phi\colon M \to N$ such that $\pi = \psi \circ \phi$, equivalently, the universal cover is an initial object in the category of covering spaces of X. Connected manifolds are path connected, and this implies that every connected smooth manifold has a universal cover, which is unique up to isomorphism.

The fibers of a smooth cover $\pi\colon M \to X$ all have the same cardinality, which we denote $\deg \pi$. If this cardinality is finite we say that π is *finite*, in which case M is compact if and only if X is.

Given a smooth cover $\pi\colon M \to X$, a *deck transformation* (or *covering transformation*) is an automorphism of M that fixes π, in other words, a diffeomorphism $\phi\colon M \to M$ such that $\pi \circ \phi = \pi$. The deck transformations of π form a subgroup $\mathrm{Deck}(\pi)$ of the automorphism group $\mathrm{Aut}(M)$. If π is the universal cover, then $\mathrm{Deck}(\pi)$ is isomorphic to the fundamental group $\pi_1(X)$ (which is independent of the base point because M is path connected). Every smooth cover $\pi\colon M \to X$ induces an embedding $\pi_1(M) \hookrightarrow \pi_1(X)$ of fundamental groups via post-composition. The action of $\mathrm{Deck}(\pi)$ on M is free and properly discontinuous, which means that every point in M has an open neighborhood whose $\mathrm{Deck}(\pi)$-translates are disjoint. This implies that the quotient space $M/\mathrm{Deck}(\pi)$ is a smooth manifold (in particular, it is Hausdorff), and the projection map $M \to M/\mathrm{Deck}(\pi)$ is a smooth cover. Similar comments apply to any subgroup of $\mathrm{Deck}(\pi)$.

The group $\mathrm{Deck}(\pi)$ acts freely on the fibers of π, so $\#\,\mathrm{Deck}(\pi) \leq \deg \pi$, and if π is finite then so is $\mathrm{Deck}(\pi)$. If the action of $\mathrm{Deck}(\pi)$ on the fibers of π is transitive (which need not hold in general) then it is necessarily simply transitive (equivalently, regular), and the following equivalent conditions hold:

- each fiber of π is a $\mathrm{Deck}(\pi)$-torsor;
- M is a homogeneous space for $\mathrm{Deck}(\pi)$;
- $M/\mathrm{Deck}(\pi) \simeq X$;
- the embedding $\pi_1(M) \hookrightarrow \pi_1(X)$ induced by π has normal image in $\pi_1(X)$.

Smooth covers that satisfy these equivalent conditions are said to be *normal* (or *regular*, or *Galois*).

Now suppose $\pi\colon M \to X$ is a normal smooth cover. For each subgroup $H \leq \mathrm{Deck}(\pi)$, the projection map $M \to M/H$ is a normal smooth cover with Deck transformation group H. Associated to any inclusion of subgroups $H \leq G \leq \mathrm{Deck}(\pi)$, we have a smooth cover $\pi_{H,G}\colon M/H \to M/G$ that sends each H-orbit in M to the G-orbit in which it lies. The projection map $\pi_G\colon M \to M/G$ is equal to the composition $\pi_{H,G} \circ \pi_H$, where $\pi_H = \pi_{1,H}$ is the projection map $M \to M/H$.

When $G = \mathrm{Deck}(\pi)$ we have $M/G \simeq X$, since π is normal. We then view $\pi_{H,G}\colon M/H \to M/G = X$ as a smooth cover of X that is an *intermediate cover* of π, meaning that $\pi = \pi_{H,G} \circ \pi_H$; the smooth cover $\pi_{H,G}$ is normal if and only if H is a normal in $G = \mathrm{Deck}(\pi)$. If H_1 and H_2 are conjugate subgroups of $\mathrm{Deck}(\pi)$ then the quotients M/H_1 and M/H_2 are diffeomorphic. We thus have a "Galois correspondence" that is directly analogous to a Galois extension of fields.

field extensions	smooth covers
L/K	$\pi\colon M \to X$
Galois	normal
finite	finite
$[L:K]$	$\deg \pi$
$\mathrm{Gal}(L/K)$	$\mathrm{Deck}(\pi)$
L^H/K	$\pi_H\colon M/H \to X$
L^{H_1}/L^{H_2}	$\pi_{H_1,H_2}\colon M/H_1 \to M/H_2$

TABLE 1. Dictionary between Galois field extensions and normal smooth covers

For a Riemannian manifold X, a *Riemannian covering* of X is a smooth cover $\pi\colon M \to X$ that is also a local isometry of Riemannian manifolds; this means that if g and h are the metrics on X and M respectively then for every $q \in M$ and every $X, Y \in T_qM$ we have

$$h_q(X,Y) = g_{\pi(q)}(\pi_* X, \pi_* Y). \tag{1}$$

This condition uniquely determines h, and the metric $\pi^* g$ defined by the RHS of (1) is a Riemannian metric on M. It follows that any smooth covering $\pi\colon M \to X$ of a Riemannian manifold X can be viewed as a Riemannian covering by equipping M with the metric $\pi^* g$, and this is the only possible choice. Note that the metric $\pi^* g$ is invariant under the action of $\mathrm{Deck}(\pi)$ (since π is), which ensures that every deck transformation is an isometry. So $\mathrm{Deck}(M) \subseteq \mathrm{Aut}(M)$, and for every subgroup $H \le \mathrm{Deck}(\pi)$ the quotient M/H is a Riemannian manifold, and the projection $M \to M/H$ is a Riemannian covering.

1.3. **Isospectral manifolds.** We can now state the theorem of Sunada, which extends Theorem 1.5 to the setting of Riemannian manifolds in one direction [47, Thm. 1].

Theorem 1.15 (Sunada, 1985)**.** *Let $\pi\colon M \to X$ be a finite normal Riemannian covering of a compact connected Riemannian manifold X and let $G := \mathrm{Deck}(\pi)$. For any Gassmann triple (G, H_1, H_2) the Riemannian manifolds M/H_1 and M/H_2 are isospectral.*

In contrast to the situation with number fields, it may happen that non-conjugate subgroups H_1 and H_2 give rise to isomorphic (meaning isometric) Riemannian manifolds. In general M/H_1 and M/H_2 will be isometric if and only if H_1 and H_2 are conjugate as subgroups of the full isometry group $\mathrm{Aut}(M)$, but this group may be much larger than G (and difficult to compute). One way to ensure that M/H_1 and M/H_2 are non-isometric is to use non-isomorphic subgroups H_1 and H_2. As noted by Sunada, every finite group G arises as the fundamental group of a compact connected smooth manifold of dimension 4; see [46, §9.4.2]. Theorem 1.3 implies that we can construct isospectral 4-manifolds using any two non-isomorphic groups H_1 and H_2 with the same order statistics, such as $H_1 = (\mathbf{Z}/p\mathbf{Z})^3$ and H_2 the Heisenberg group of order p^3, as in Example 1.4.

Another family of Riemannian manifolds considered by Sunada are *Riemann surfaces*, which are connected complex manifolds of dimension 1, hence real manifolds of dimension 2. Riemann surfaces are smooth manifolds, so to make them Riemannian manifolds we must equip them with a metric; a standard choice is to give them constant negative curvature, and for Riemann surfaces that arise as quotients of the hyperbolic upper half plane by a *Fuchsian group*, a discrete subgroup of $\mathbf{SL}_2(\mathbf{R})$ acting on the upper half plane via fractional linear transformations, this is the natural choice. More generally, there is an equivalence of categories between connected compact Riemann surfaces and smooth projective curves (algebraic varieties of dimension one) over **C**; given a smooth projective curve over a number field, we can obtain a connected compact Riemann surface by embedding our number field in **C**.

Prasad and Rajan [41] consider the case of a smooth projective curve X over an arbitrary fields k equipped with an action by a finite group G and prove a result directly analogous to Sunada's theorem: for any Gassmann triple (G,H,H') the curves X/H_1 and X/H_2 have isogenous Jacobians. When k is a finite field or number field, this amounts to saying that X/H_1 and X/H_2 have the same zeta function (or L-function); we will discuss this result further in a Lecture 3.

1.4. **Isospectral graphs.** There is a discrete analog of Sunada's theorem for graphs. Let us consider the case of a finite undirected graph $\Gamma=(V,E)$, where E is a finite multiset of unordered pairs of elements of V (multiple edges between vertices are allowed; when we enumerate edges we do so with multiplicity). Let $\mathbf{R}(V)$ and $\mathbf{R}(E)$ denote the $\mathbf{R}$-vector spaces of real valued functions on V and the set of edges in E (without multiplicity). The *coboundary operator* ∇ is the linear map $\nabla\colon \mathbf{R}(V)\to\mathbf{R}(E)$ defined by

$$(\nabla f)(\{v,w\}) := f(v)-f(w),$$

which can be viewed as a discrete analog of the gradient. Its transpose $\nabla^{\mathsf{T}}\colon \mathbf{R}(E)\to\mathbf{R}(V)$ is defined by

$$(\nabla^{\mathsf{T}} g)(v) := \sum_{\{v,w\}\in E} g(\{v,w\}),$$

and can viewed as a discrete analog of divergence. The *discrete Laplace operator* $\Delta_\Gamma\colon \mathbf{R}(V)\to\mathbf{R}(V)$ is the composition $\Delta_\Gamma := \nabla^{\mathsf{T}}\nabla$, acting on $f\in\mathbf{R}(V)$ via

$$(\Delta_\Gamma f)(x) := \sum_{\{v,w\}\in E} (f(v)-f(w));$$

note that the sum enumerates edges with multiplicity, and that self-loops (edges of the form $\{x,x\}$) make no contribution. The eigenvalues of Δ_Γ are the eigenvalues of the matrix $D-A$, where D is the *degree matrix* of Γ, and A is its *adjacency matrix*. If we index the vertices as $V=\{v_1,\ldots,v_n\}$, then D is the diagonal matrix with D_{ii} equal to the number of edges incident to v_i (with multiplicity) and A_{ij} is the symmetric matrix with A_{ij} equal to the multiplicity of $\{v_i,v_j\}$ in E (zero if $\{v_i,v_j\}\notin E$).

The eigenvalues of Δ_Γ are real and nonnegative; the eigenvalue 0 occurs with multiplicity equal to the number of connected components of Γ. If we let $0<\lambda_1\le\ldots\le\lambda_r$ denote the nonzero eigenvalues of Δ_Γ (with multiplicity), the *spectral zeta function* of Γ is defined by

$$\zeta_\Gamma(s) := \sum_{1\le i\le r} \lambda_i^{-s}.$$

These definitions readily extend to countably infinite graphs of bounded degree (including lattices) by replacing $\mathbf{R}(V)$ with a suitable Hilbert space of functions (typically a reproducing kernel Hilbert space), and can be generalized further to locally finite weighted directed graphs; see [48]. We should note that there are many other zeta functions of graphs that one may define, and equality of one type of zeta function does not always imply equality of another; see [11] for a survey if this topic.

An automorphism of Γ is a permutation $\varphi\colon V\to V$ that fixes E; this means that $E=\{\{\varphi(x),\varphi(y)\}:\{x,y\}\in E\}$. The set of automorphisms of Γ form a subgroup $\mathrm{Aut}(\Gamma)$ of the group of permutations of V. For any subgroup $H\le\mathrm{Aut}(\Gamma)$, the *quotient* graph Γ/H is the graph whose vertex set consists of H-orbits $[x]$ of $x\in V$ with the multiset of edges $\{\{[x],[y]\}:\{x,y\}\in E\}$.

The following analog of Sunada's theorem appears in [22].

Theorem 1.16. *Let Γ be a finite connected graph and let H_1 and H_2 be subgroups of $G:=\mathrm{Aut}(\Gamma)$ whose non-trivial elements have no fixed points. If (G,H_1,H_2) is a Gassmann triple then $\zeta_{\Gamma/H_1}(s)=\zeta_{\Gamma/H_2}(s)$.*

The converse is not true in general, but for k-regular graphs one can obtain a biconditional by introducing some additional structure; see [5, Cor. 0.1]. As with Sunada's theorem, non-conjugate H_1 and H_2 may yield isomorphic Γ/H_1 and Γ/H_2. The assumption that the non-trivial elements of H_1 and H_2 contain no fixed points is stronger than necessary. If Γ is a simple graph, the quotient graphs Γ/H_i need not be simple. We can remove self-loops, since these do not impact the spectral zeta function, and as explained in [22], one can modify Γ in a way that does not change its spectral zeta function or its automorphism group so that the quotient graphs Γ/H_i will be simple and still have the same spectral zeta functions.

2. Arithmetically equivalent number fields

Let $L/\mathbf{Q}$ be a finite Galois extension with $G := \mathrm{Gal}(L/\mathbf{Q})$, let H_1 and H_2 be subgroups of L, and let $K_1 := L^{H_1}$ and $K_2 := L^{H_2}$ be the corresponding fixed fields. Our main goal for this lecture is to prove Gassmann's theorem, which states that the fields K_1 and K_2 are arithmetically equivalent if and only if H_1 and H_2 are Gassmann equivalent (as subgroups of G). We begin by reviewing some standard facts about the decomposition of primes in number fields; for further background and proofs see any standard reference for algebraic number theory (such as [39]), or these lecture notes.

2.1. **Decomposition of primes.** Let K be a number field of degree $n := [K : \mathbf{Q}]$. Recall that the ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain, an integrally closed noetherian domain of Krull dimension one. This means that every nonzero ideal of $\mathcal{O}_K$ can be uniquely factored into nonzero prime ideals. In particular, for each prime number p we have a factorization of $\mathcal{O}_K$-ideals

$$p\mathcal{O}_K = \prod_{\mathfrak{p}|p\mathcal{O}_K} \mathfrak{p}^{e_\mathfrak{p}},$$

where $e_\mathfrak{p} \in \mathbf{Z}_{>1}$ is the *ramification index of* $\mathfrak{p}$ (note that $\mathfrak{p}|p$ if and only if $p = \mathfrak{p} \cap \mathbf{Z}$, so the ramification index $e_\mathfrak{p}$ is uniquely determined by $\mathfrak{p}$). Henceforth we may use $\mathfrak{p}|p$ as shorthand for $\mathfrak{p}|p\mathcal{O}_K$ and say that $\mathfrak{p}$ *lies above p* whenever $\mathcal{O}_K$ is clear from context. We also define the *residue field degree* (or *inertia degree*) as the degree of the residue field $\mathbf{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ as an extension of $\mathbf{F}_p \simeq \mathbf{Z}/p\mathbf{Z}$. The ramification indices and residue field degrees are related by the equation

$$n = [K : \mathbf{Q}] = [\mathcal{O}_K/p\mathcal{O}_K : \mathbf{Z}/p\mathbf{Z}] = \sum_{\mathfrak{p}|p} [\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}} : \mathbf{Z}/p\mathbf{Z}] = \sum_{p|p} e_\mathfrak{p}[\mathbf{F}_\mathfrak{p} : \mathbf{F}_p] = \sum_{\mathfrak{p}|p} e_\mathfrak{p} f_\mathfrak{p}.$$

For all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ we have $e_\mathfrak{p} = 1$, in which case we say that $\mathfrak{p}$ is *unramified*. Indeed, we can have $e_\mathfrak{p} > 1$ only when $\mathfrak{p}$ lies above a prime p that divides the *discriminant* $\operatorname{disc}\mathcal{O}_K$, which can be computed using any $\mathbf{Z}$-basis $e_1, \ldots e_n$ for $\mathcal{O}_K$ via

$$\operatorname{disc}\mathcal{O}_K := \operatorname{disc}(e_1, \ldots, e_n) = \det[\operatorname{tr}(e_i e_j)]_{ij} \in \mathbf{Z},$$

where $\operatorname{tr}\colon K \to \mathbf{Q}$ is defined on $\alpha \in K$ as the trace of the multiplication-by-α map (as a transformation of the $\mathbf{Q}$-vector space $K \simeq \mathbf{Q}^n$). The extension $K/\mathbf{Q}$ is separable, so by the primitive element theorem, $K = \mathbf{Q}[x]/(f(x))$ for some monic irreducible $f \in \mathbf{Z}[x]$, and we may write $K = \mathbf{Q}(\alpha)$, where α is the image of x in $\mathbf{Q}[x]/(f(x))$. The discriminant of f is related to the discriminant of $\mathcal{O}_K$ via

$$\operatorname{disc}(f) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \operatorname{disc}\mathcal{O}_K.$$

If one can choose $f \in \mathbf{Z}[x]$ so that $|\operatorname{disc}(f)| = |\operatorname{disc}\mathcal{O}_K|$ one says that K is *monogenic*; for most number fields this is not possible. For primes that do not divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, the following theorem allows us to completely determine the factorization of $p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e_\mathfrak{p}}$, as well as the residue field degrees $f_\mathfrak{p}$. This theorem has many applications, so we state it in greater generality than we need.

Theorem 2.1 (DEDEKIND-KUMMER THEOREM). *Let A be a Dedekind domain with fraction field K, let L/K be a finite separable extension, and let B be the integral closure of A in L. Let $L = K(\alpha)$ with $\alpha \in B$, let $f \in A[x]$ be the minimal polynomial of α, let $\mathfrak{p}$ be a nonzero prime ideal of A such that the $\mathfrak{p}A[\alpha]$ is coprime to $\{a \in A[\alpha] : aB \subseteq A[\alpha]\}$, let $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$ be the irreducible factorization of the reduction of f in $(A/\mathfrak{p})[x]$, with $f_1, \ldots, f_r \in A[x]$ monic, and define the B-ideals $\mathfrak{q}_i := (\mathfrak{p}, f_i(\alpha))$. Then*

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

is the unique factorization of $\mathfrak{p}B$ into prime ideals of B and $[B/\mathfrak{q}_i : A/\mathfrak{p}] = \deg f_i$.

The ideal $\{a \in A[\alpha] : aB \subseteq A[\alpha]\}$ in the Dedekind-Kummer theorem is the *conductor* of the order $A[\alpha]$ in B; it is the largest B-ideal that is also an A-ideal. When $A = \mathbf{Z}$ this ideal divides the index $[B : A[\alpha]]$. We now observe that primes $p \nmid \operatorname{disc}(f)$ are unramified and satisfy the hypothesis of the theorem. In this case the reduction of f modulo p is squarefree and the degrees of the irreducible factors of $\bar{f}$ are precisely the residue field degrees $f_{\mathfrak{p}}$ of the primes $\mathfrak{p}|p$. Indeed, the étale algebra $\mathbf{F}_p[x]/(\bar{f}(x))$ decomposes as

$$\frac{\mathbf{F}_p[x]}{(\bar{f}(x))} \simeq \frac{\mathbf{F}_p[x]}{(\bar{f}_1(x))} \times \cdots \times \frac{\mathbf{F}_p[x]}{(\bar{f}_r(x))} \simeq \mathbf{F}_{\mathfrak{p}_1} \times \cdots \times \mathbf{F}_{\mathfrak{p}_r}.$$

We now want to consider the splitting field of $f(x)$, which is a finite Galois extension L of $\mathbf{Q}$ that contains K. For each prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ we have the *decomposition group*

$$D_{\mathfrak{q}} := \{\sigma \in \operatorname{Gal}(L/\mathbf{Q}) : \sigma(\mathfrak{q}) = \mathfrak{q}\} \subseteq \operatorname{Gal}(L/\mathbf{Q}),$$

and an exact sequence

$$1 \longrightarrow I_{\mathfrak{q}} \longrightarrow D_{\mathfrak{q}} \stackrel{\sigma \mapsto \bar{\sigma}}{\longrightarrow} \operatorname{Gal}(\mathbf{F}_{\mathfrak{q}}/\mathbf{F}_p) \longrightarrow 1,$$

where $p = \mathfrak{q} \cap \mathbf{Z}$ and the $\bar{\sigma} \in \operatorname{Gal}(\mathbf{F}_{\mathfrak{q}}/\mathbf{F}_p)$ is defined by $\bar{\alpha} \mapsto \overline{\sigma(\alpha)}$. If $\mathfrak{q}$ is unramified the *inertia subgroup* $I_{\mathfrak{q}}$ is trivial and $D_{\mathfrak{q}} \simeq \operatorname{Gal}(\mathbf{F}_q/\mathbf{F}_p)$. In this case we define the *Frobenius element* $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}} \subseteq \operatorname{Gal}(L/\mathbf{Q})$ as the unique element for which $\bar{\sigma}_{\mathfrak{q}}$ is the p-power Frobenius $a \mapsto a^p$, which is a canonical generator for the cyclic group $\operatorname{Gal}(\mathbf{F}_{\mathfrak{q}}/\mathbf{F}_p)$.

The Galois group $\operatorname{Gal}(L/\mathbf{Q})$ has a natural permutation representation of degree n given by its action on the roots of $f(x)$ (all of which lie in L). For unramified primes p, the Frobenius elements $\sigma_{\mathfrak{q}}$ of the primes $\mathfrak{q}|p\mathcal{O}_L$ are conjugate permutations with cycle type $(f_{\mathfrak{p}_1}, \ldots f_{\mathfrak{p}_r})$, where $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ is the prime factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$. We can also realize this permutation representation as the action of $G := \operatorname{Gal}(L/\mathbf{Q})$ on the coset space $H\backslash G := \{Hg : g \in G\}$ (viewed as a G-set). If we let $C_{\mathfrak{q}} := \langle \sigma_{\mathfrak{q}} \rangle$ by the cyclic subgroup of G generated by the Frobenius element $\sigma_{\mathfrak{q}}$, we can read off the cycle type of the action of $\sigma_{\mathfrak{q}}$ from the double coset decomposition

$$G = Hg_1C_{\mathfrak{q}} \sqcup \cdots \sqcup Hg_rC_{\mathfrak{q}}.$$

For a suitable ordering of the g_i we will have $[Hg_iC_{\mathfrak{q}} : Hg_i] = f_{\mathfrak{p}_i}$, and we can view the double coset decomposition as a partition of the right-coset space $H\backslash G$ into blocks of size $f_{\mathfrak{p}_1}, \ldots, f_{\mathfrak{p}_r}$.

To sum up, given a number field $K = \mathbf{Q}[x]/(f(x))$ with Galois closure L and $H := \operatorname{Gal}(L/K)$, for each prime $p \nmid \operatorname{disc}(f)$ we can describe the decomposition of p in the extension $K/\mathbf{Q}$ in four equivalent ways:

- the factorization $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in $\mathcal{O}_K$, with residue field degrees $(f_{\mathfrak{p}_1}, \ldots, f_{\mathfrak{p}_r})$;
- the factorization $\bar{f} = \bar{f}_1 \cdots \bar{f}_r$ of f in $\mathbf{F}_p[x]$, with degrees $(\deg \bar{f}_1, \ldots, \deg \bar{f}_r)$;
- for $\mathfrak{q}|p\mathcal{O}_L$, the permutation representation of $\sigma_{\mathfrak{q}}$ in S_n, with cycle type $(n_1, \ldots, n_r)$;
- for $\mathfrak{q}|p\mathcal{O}_L$, the double coset partition of G with block sizes $([Hg_1C_{\mathfrak{q}} : Hg_1], \ldots, [Hg_rC_{\mathfrak{q}} : Hg_r])$.

When suitably ordered these tuples of integers all coincide and sum to $n = [K : \mathbf{Q}]$; we have

$$(f_{\mathfrak{p}_1}, \ldots, f_{\mathfrak{p}_r}) = (\deg f_1, \ldots, \deg f_r) = (n_1, \ldots, n_r) = ([Hg_1C_{\mathfrak{q}} : Hg_1], \ldots, [Hg_rC_{\mathfrak{q}} : Hg_r]).$$

For each $p \nmid \operatorname{disc}(f)$ we thus have a partition of the integer n that we call the *decomposition type* of p in the extension $K/\mathbf{Q}$. For $p | \operatorname{disc}(f)$ we define the decomposition type to be the sequence of residue field degrees in non-decreasing order (which will be a partition of n if p is unramified but not otherwise).

The decomposition type of every prime $p \nmid \operatorname{disc}(f)$ is the cycle type of some $\sigma \in \operatorname{Gal}(L/\mathbf{Q})$ acting on the roots of $f(x)$. One might ask whether every cycle type in the permutation representation of $\operatorname{Gal}(L/\mathbf{Q})$ arises as the decomposition type of such a prime p. This follows from a theorem of Frobenius.

Theorem 2.2 (Frobenius density theorem). *Let $K = \mathbf{Q}[x]/(f(x))$ be a number field with Galois closure L. For each tuple of integers $(n_1, \ldots, n_r)$, the density of primes p with this decomposition type is equal to the proportion of elements of* $\operatorname{Gal}(L/\mathbf{Q})$ *that have this cycle type in the permutation representation on the roots of $f(x)$.*

There are several ways to interpret the word "density" in Frobenius' theorem, all of which imply that every cycle type of an element of G arises as the decomposition type of infinitely many primes, which is all that we will use. Frobenius originally proved his theorem using the notion of *polar density*, and the generalization of his theorem by Chebotarev in his 1922 thesis used *Dirichlet density*; work of Hecke [25] that actually predates Chebotarev's result implies that in both cases one can use *natural density*. The natural density of a set of primes S is defined as

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{p \le x : p \in S\}}{\#\{p \le x\}},$$

whenever this limit exists, where p ranges over primes.

We conclude this section by observing that replacing the Galois closure L of K with any finite Galois extension $L/\mathbf{Q}$ that contains K changes none of the discussion above, and Theorem 2.2 still holds in this context. The group $G := \operatorname{Gal}(L/\mathbf{Q})$ becomes larger, but so does $H = \operatorname{Gal}(L/K)$, and $[G : H]$ is unchanged. The right coset space $H\backslash G$ still has the same cardinality, and the corresponding permutation representation of G does not change, other than having a larger kernel. In particular, double coset decompositions still correspond to cycle types of permutations of roots of a defining polynomial for K.

2.2. **The Dedekind zeta function.** Recall that the Dedekind zeta function of a number field K is

$$\zeta_K(x) := \sum_I N(I)^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

where I ranges over nonzero $\mathcal{O}_K$-ideals and $\mathfrak{p}$ ranges over nonzero prime $\mathcal{O}_K$-ideals; the sum and product converge absolutely on $\operatorname{Re}(s) > 1$. Let $D_K := \operatorname{disc} \mathcal{O}_K$ be the discriminant of the number field K, and let r_1 and r_2 denote the number of real and complex places of K; these correspond to equivalence classes of archimedean absolute values on K and can be defined as the unique integers for which we have an isomorphism of $\mathbf{R}$-algebras

$$K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^{r_1} \otimes \mathbf{C}^{r_2},$$

and we note that $r_1 + 2r_2 = n := [K : \mathbf{Q}]$, since the LHS is an $\mathbf{R}$-vector space of dimension n. Associated to the real and complex places of K we have Γ-*factors*

$$\Gamma_{\mathbf{R}}(s) := \pi^{-s/2}\Gamma(\tfrac{s}{2}) \qquad \text{and} \qquad \Gamma_{\mathbf{C}}(s) := 2(2\pi)^{-s}\Gamma(s),$$

where $\Gamma(s) := \int_0^\infty t^{s-1} e^{-s} dt$. We now define the *completed Dedekind zeta function* as

$$Z_K(s) := |D_K|^{s/2} \Gamma_{\mathbf{R}}(s)^{r_1} \Gamma_{\mathbf{C}}(s)^{r_2} \zeta_K(s).$$

One should think of the Γ-factors as Euler factors for the archimedean places that are missing from the Euler product of $\zeta_K(x)$. As shown by Hecke [25], the completed Dedekind zeta function $Z_K(s)$ extends to a meromorphic function on $\mathbf{C}$ that satisfies the *functional equation*

$$Z_K(s) = Z_K(1-s).$$

The existence of this functional equation imposes a certain rigidity on the Dedekind zeta function that has several implications. For our purposes the most important of these is that $Z_K(s)$ and $\zeta_K(s)$ are both completely determined by any partial product that includes all but finitely many of the factors in the Euler product for $\zeta_K(s)$. To prove this we first note the following purely analytic result.

Lemma 2.3. *Let $1 < c_1 \le c_2 \le \cdots c_m$ and $1 < d_1 \le d_2 \cdots \le d_n$ be real numbers, and define*

$$f(s) := \prod_{i=1}^{m}(1 - c_i^{-s}), \qquad g(s) := \prod_{j=1}^{n}(1 - d_j^{-s}) \qquad h(s) = \frac{f(s)}{g(s)}$$

Let $\phi(s)$ be a meromorphic function with no zeros or poles at any zero or pole of $h(s)$. Suppose that

$$h(s) = \phi(s)h(1-s).$$

Then $f(s) = g(s)$ and $\phi(s) = 1$.

Proof. The functions f and g have no poles. The zeros of f are $\{2\pi i k/\log c_i : k \in \mathbf{Z}\}$ and the zeros of g are $\{2\pi i k/\log d_j : k \in \mathbf{Z}\}$. Every zero of h must be a zero of f (since g has no poles) and not a zero of ϕ (by hypothesis), and cannot be zero of $h(1-s)$ because $f(s)$ and $f(1-s)$ have no common zeros (the zeros of $f(s)$ lies on $\mathrm{Re}(s) = 0$ while those of $f(1-s)$ lie on $\mathrm{Re}(s) = 1$). But this contradicts the hypothesis $h(s) = \phi(s)h(1-s)$, so h must not have any zeros.

Similarly, every pole of h must be a zero of g but not a pole of ϕ or of $h(1-s)$, so h has no poles. It follows that f and g have the same zeros, with the same multiplicities, and therefore the sequences $c_1, \ldots, c_m$ and $d_1, \ldots, d_n$ coincide. It follows that $f = g$, which implies $h = 1$ and $\phi = 1$. □

Corollary 2.4. *Let K_1 and K_2 be number fields and suppose that for all but finitely many primes p we have*

$$\prod_{\mathfrak{p}|p\mathcal{O}_{K_1}} (1 - N(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}|p\mathcal{O}_{K_2}} (1 - N(\mathfrak{p})^{-s}).$$

Then $\zeta_{K_1}(s) = \zeta_{K_2}(s)$ and $Z_{K_1}(s) = Z_{K_2}(s)$, and the number fields K_1 and K_2 have the same degree, discriminant, and numbers of real and complex places.

Proof. Let S be the finite set of primes for which the hypothesis of the corollary does not hold. For any prime ideal $\mathfrak{p}$ of either $\mathcal{O}_{K_1}$ or $\mathcal{O}_{K_2}$, the norm $N(\mathfrak{p})$ is a power of the prime $p := \mathfrak{p} \cap \mathbf{Z}$ (which is a real number greater than 1), and the set of norms of prime ideals $\mathfrak{p}$ that lie above a prime $p \in X$ is disjoint from the set of norms of prime ideals that lie above a prime $p \notin S$. We also note that the ratio Z_{K_1}/Z_{K_2} satisfies the functional equation, We may thus apply Lemma 2.3 with

$$f(s) := \prod_{\substack{\mathfrak{p}|p\mathcal{O}_{K_1} \\ p \in S}} (1 - N(\mathfrak{p})^{-s}), \qquad g(s) := \prod_{\substack{\mathfrak{p}|p\mathcal{O}_{K_2} \\ p \in S}} (1 - N(\mathfrak{p})^{-s}), \qquad \phi(s) := \frac{Z_{K_1}(s)Z_{K_2}(1-s)\zeta_{K_2}(s)\zeta_{K_1}(1-s)}{Z_{K_2}(s)Z_{K_1}(1-s)\zeta_{K_1}(s)\zeta_{K_2}(1-s)}$$

shows that $\zeta_{K_1}(s) = \zeta_{K_2}(s)$ and $Z_{K_1}(s)Z_{K_1}(1-s) = Z_{K_2}(s)Z_{K_2}(1-s)$, which implies $Z_{K_1}(s)^2 = Z_{K_2}(s)^2$, by the functional equation. Let r_{11} and r_{21} be the numbers of real and complex places of K_1 and similarly define r_{21} and r_{22} as the numbers of real and complex places of K_2. Noting that $\Gamma_{\mathbf{R}}(1) = 1$ and $\Gamma_{\mathbf{C}}(1) = \pi^{-1}$, evaluating $Z_{K_1}(s)^2/Z_{K_2}(s)^2$ as $s \to 1^+$ yields

$$|D_{K_1}|^{-1}\pi^{-2r_{21}} = |D_{K_2}|^{-1}\pi^{-2r_{22}},$$

which implies $r_{21} = r_{22}$ and $|D_{K_1}| = |D_{K_2}|$, since π is transcendental and the discriminants are integers. Noting that $\Gamma_{\mathbf{R}}(2) = \pi^{-1}$, if we now evaluate $Z_{K_1}(s)^2/Z_{K_2}(s)^2$ at $s = 2$ we obtain $\pi^{-2r_{11}} = \pi^{-2r_{21}}$ and therefore $r_{21} = r_{22}$, which implies $Z_{K_1}(s) = Z_{K_2}(s)$. Since K_1 and K_2 have the same number of real and complex places, they have the same degree, and since the sign of the discriminant of a number field is determined by the parity of the number of complex places (see [4]), we also have $D_{K_1} = D_{K_2}$. □

Corollary 2.4 is a very special case of what is known as a *multiplicity one theorem*: for L-functions that satisfy a certain list of properties, including the existence of a functional equation and an Euler product, if the Euler products agree at all but finitely many factors then the L-functions must coincide.

Definition 2.5. The *polynomial Selberg class* $\mathcal{S}^{\mathrm{p}}$ consists of Dirichlet series $L(s) := \sum_{n\ge 1} a_n n^{-s}$ for which:

(1) the series converges absolutely on $\mathrm{Re}(s) > 1$;
(2) $(s-1)^m L(s)$ is holomorphic on $\mathbf{C}$ for some $m \in \mathbf{Z}$, and $|L(s)| = O(\exp(|s|^\kappa))$ for some $\kappa > 0$;
(3) for some $\gamma(s) := Q^s \prod_{i=1}^r \Gamma(\lambda_i s + \mu_i)$ and ε the completed L-function $\tilde{L}(s) := \gamma(s)L(s)$ satisfies

$$\tilde{L}(s) = \varepsilon\overline{\tilde{L}(1-\bar{s})},$$

with $Q > 0$, $\lambda_i > 0$, $\mathrm{Re}(\mu_i) \ge 0$, and $|\varepsilon| = 1$. Define $\deg L := 2\sum_{i=1}^r \lambda_i$;
(4) $a_1 = 1$ and $a_n = O(n^\epsilon)$ for all $\epsilon > 0$;
(5) we have an Euler product $L(s) = \prod_p L_p(p^{-s})^{-1}$, with $L_p(T) \in 1 + \mathbf{C}[T]$ of degree at most $\deg L$.

Provided one renormalizes as required to make $\mathrm{Re}(s) = 1/2$ the axis of symmetry for the functional equation, the polynomial Selberg class is known to include:

(1) Dirichlet L-functions $L(s,\chi) := \sum_{n\ge 1} \chi(n)n^{-s}$ of Dirichlet characters $\chi\colon \mathbf{Z} \to \mathbf{C}$;
(2) Dedekind zeta functions $\zeta_K(s)$ of number fields K;
(3) Hecke L-functions $L(s,\chi) := \sum_I \chi(I)N(I)^{-s}$ associated to an idele class character χ;
(4) Artin L-functions $L(s,\rho) = \prod_{\mathfrak{p}} \det(I - N(\mathfrak{p})^{-s}\rho_{|V^{I_\mathfrak{q}}}(\mathrm{Frob}_\mathfrak{q}))^{-1}$ associated to an Artin representation $\rho\colon\ \mathrm{Gal}(L/K) \to \mathbf{GL}(V)$ of a Galois extension of number fields L/K;
(5) Modular L-functions $L(f,s) := \sum_{n\ge 1} a_n n^{-s}$ associated to modular forms $f \in S_k(\Gamma_1(N))$;
(6) Elliptic curve L-functions $L(E,s) := \prod_p L_p(p^{-s})$ associated to an elliptic curve $E/\mathbf{Q}$.

The last two examples are special cases of automorphic L-functions and motivic L-functions, respectively. Under the Langlands program, all motivic L-functions are expected to arise as automorphic L-functions; this is known for elliptic curve L-functions over $\mathbf{Q}$ thanks to the modularity theorem. Automorphic L-functions are all conjectured to lie in the Selberg class $\mathcal{S}$, which generalizes the polynomial Selberg class $\mathcal{S}^{\mathrm{p}}$ by allowing a more general notion of an "Euler product". Motivic L-functions, which include L-functions of abelian varieties over number fields and Hasse-Weil zeta functions of arithmetic schemes are all conjectured to lie in $\mathcal{S}^{\mathrm{p}}$.

We can now state the strong multiplicity one theorem for $\mathcal{S}^{\mathrm{p}}$, due to Kaczorowski and Perelli [30].

Theorem 2.6 (Kaczorowski-Perelli, 2001)**.** *If $A(s) := \sum_{n\ge 1} a_n n^{-s}$ and $B(s) := \sum_{n\ge 1} a_n n^{-s}$ both lie in $\mathcal{S}^{\mathrm{p}}$ and $a_p = b_p$ for all but finitely many primes p then $A(s) = B(s)$.*

2.3. **Proof of Gassmann's theorem.** For a subgroup H of a finite group G we use $\chi_H\colon G\to\mathbf{Z}$ to denote the character of the permutation representation given by the G-set $H\backslash G$; in other words χ_H is the trace of the induced representation 1_H^G, and we have

$$\chi_H(\sigma) := \#\{H\tau\in H\backslash G : H\tau\sigma = H\tau\}.$$

Lemma 2.7. *Subgroups H_1 and H_2 of a finite group G are Gassmann equivalent if and only if $\chi_{H_1}=\chi_{H_2}$.*

Proof. Let $\sigma^G := \{\tau\sigma\tau^{-1} : \tau\in G\}$ denote the conjugacy class of $\sigma\in G$, and for any subgroup $H\le G$ let $\psi_H\colon G\to\mathbf{Z}$ be the class function $\psi_H(\sigma) := \#(H\cap\sigma^G)$. By definition, H_1 and H_2 are Gassmann equivalent if and only if $\psi_{H_1}=\psi_{H_2}$. It suffices to show that $\chi_H=\phi_H\psi_H$ for some class function $\phi_H\colon G\to\mathbf{Q}^\times$ (we then also have $\psi_H=\chi_H/\phi_H$). We now observe that for any $\sigma\in G$ we have

$$\psi_H(\sigma)\#G_\sigma = \#\{\tau\in G : \tau\sigma\tau^{-1}\in H\} = \#\{\tau\in G : H\tau\sigma = H\tau\} = \chi_H(\sigma)\#H,$$

where G_σ is the centralizer of σ in G. The first equality follows from the fact that G_σ is the stabilizer of the G-action on σ^G (via conjugation), and the second follows from the fact that the map $\tau\mapsto H\tau$ is a $\#H$-to-one. We now define $\phi_H(\sigma) := \#G_\sigma/\#H$ and the lemma follows. $\square$

Theorem 2.8. *Let K_1 and K_2 be number fields. Let L any Galois number field containing K_1 and K_2, let $G:=\mathrm{Gal}(L/\mathbf{Q})$, and define $H_2 := \mathrm{Gal}(L/K_1)$ and $H_2 := \mathrm{Gal}(L/K_2)$. The following are equivalent:*

- (i) *K_1 and K_2 are arithmetically equivalent;*
- (ii) *All but finitely many primes p have the same decomposition type in K_1 and K_2;*
- (iii) *(G,H_1,H_2) is a Gassmann triple.*

Proof. **(i) ⇒ (ii)**: For $n\ge 1$ let a_n be the number of $\mathcal{O}_{K_1}$-ideals of norm n, so that $\zeta_{K_1}(s)=\sum_{n\ge1}a_nn^{-s}$, and similarly define b_n so that $\zeta_{K_2}(s)=\sum_{n\ge1}b_nn^{-s}$. By (i) we have

$$\sum_{n\ge1}a_nn^{-s}=\sum_{n\ge1}b_nn^{-s}$$

for all $\mathrm{Re}(s)>1$, and for $s\to\infty$ we obtain $a_1=b_1$. After subtracting $a_1=b_1$ from both sides and multiplying by 2^s we can similarly show $a_2=b_2$. Continuing in this fashion we obtain $a_n=b_n$ for all $n\ge1$. For any prime ideal $\mathfrak{p}$ in the ring of integers of a number field, for $p:=\mathfrak{p}\cap\mathbf{Z}$ we have

$$N(\mathfrak{p}) = [\mathcal{O}_K:\mathfrak{p}] = \#\mathbf{F}_\mathfrak{p} = (\#\mathbf{F}_p)^{[\mathbf{F}_\mathfrak{p}:\mathbf{F}_p]} = p^{f_\mathfrak{p}},$$

where $f_\mathfrak{p} := [\mathbf{F}_\mathfrak{p}:\mathbf{F}_p]$ is the residue field degree. It follows that a_p is the number of prime ideals $\mathfrak{p}|p\mathcal{O}_K$ with $f_\mathfrak{p}=1$. This implies that $a_{p^2}-\binom{a_p}{2}-a_p$ is the number of prime ideals $\mathfrak{p}|p\mathcal{O}_K$ with $f_\mathfrak{p}=2$, and in general, the number of prime ideals $p|p\mathcal{O}_K$ with $f_\mathfrak{p}=m$ is a polynomial in $a_p,a_{p^2},\ldots,a_{p^{m-1}}$ with coefficients in $\mathbf{Q}$. Thus for every prime number p, the decomposition type of p in K_1 is determined by the integers $a_n=b_n$ and therefore coincides with its decomposition type in K_2, and (ii) follows.

(ii) ⇒ (iii): By the Frobenius density theorem, the cycle type of every $\sigma\in G$ in the permutation representation $[H_1\backslash G]$ is determined by the decomposition type of the infinitely many primes p for which σ is the Frobenius element of some prime ideal $\mathfrak{q}|p\mathcal{O}_L$, and the same applies for the permutation representation $[H_2\backslash G]$. By (ii), every $\sigma\in G$ has the same cycle type in the permutation representations $[H_1\backslash G]$ and $[H_2\backslash G]$. In particular, each $\sigma\in G$ fixes the same number of right cosets of H_1 and H_2. Thus $\chi_{H_1}=\chi_{H_2}$, and (iii) follows from Lemma 2.7.

(iii) ⇒ (ii): By Lemma 2.7, (iii) implies $\chi_{H_1}=\chi_{H_2}$, so every $\sigma\in G$ has the same cycle type in the permutation representations $[H_1\backslash G]$ and $[H_2\backslash G]$ (note that the set $\{\chi_{H_1}(\sigma^n) : n\in\mathbf{Z}\}$ determines the cycle type of σ). All but finitely many primes p are unramified in both K_1 and K_2, and the decomposition type of these primes is determined by the cycle type of $\sigma_{\mathfrak{q}}$ for any $\mathfrak{q}|p\mathcal{O}_L$; thus (ii) holds.

(ii) ⇒ (i): By (ii), for all but finitely many primes p we have the same sequence of residue field degrees $(f_{\mathfrak{p}_1},\ldots,f_{\mathfrak{p}_r})$ for primes $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ dividing $\mathfrak{p}\mathcal{O}_{K_1}$, and for primes $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ dividing $p\mathcal{O}_{K_2}$ (with the same value of r in both cases). It follows that for all but finitely many primes p we have

$$\prod_{\mathfrak{p}|p\mathcal{O}_{K_1}}(1-N(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}|p\mathcal{O}_{K_2}}(1-N(\mathfrak{p})^{-s}).$$

Corollary 2.4 implies (i). □

Recall that for a subgroup $H \le G$, the *normal core* of H is the intersection of its G-conjugates, equivalently, the largest subgroup of H that is normal in G, and the *normal closure* of H is the union of its G-conjugates, equivalently, the smallest normal subgroup of G containing H. For a number field $K/\mathbf{Q}$, the normal core of K is the largest subfield of K that is a normal extension of $\mathbf{Q}$; if $L/\mathbf{Q}$ is a finite Galois extension containing K with $G := \mathrm{Gal}(L/\mathbf{Q})$ and $H := \mathrm{Gal}(L/K)$, the normal core of K is the fixed field of the normal closure of of H in G and the normal closure of K (its Galois closure) is the fixed field of the normal core of H.

Corollary 2.9. *Let K_1 and K_2 be arithmetically equivalent number fields. Then K_1 and K_2 have the same normal closure, normal core, degree, discriminant, and numbers of real and complex places. Moreover, the unit groups $\mathcal{O}_{K_1}^\times$ and $\mathcal{O}_{K_2}^\times$ are isomorphic as finitely generated abelian groups; in particular, they have the same rank and contain the same roots of unity.*

Proof. Let G be the Galois group of the compositum of the Galois closures of K_1, K_2, and let $H_1, H_2 \le G$ be the subgroups of G with fixed fields K_1, K_2 (resp.). The Galois closure L of K_1 is the fixed field of the normal core of H_1 in G (the intersection of all its G-conjugates), and similarly for H_2. By Theorem 2.8, the subgroups H_1 and H_2 are Gassmann equivalent, and they thus intersect every conjugacy class of elements of G with the same cardinality. But the normal cores of H_1 and H_2 are both stable under G-conjugation, hence unions of conjugacy classes, so they and their fixed fields must coincide, so L is also the Galois closure of K_2. The normal closure of H_1 is the union of all the G-conjugacy classes that intersect H_1, and similarly for H_2, so H_1 and H_2 have the same normal closure and it follows that K_1 and K_2 have the same normal core.

The rest of the corollary follows immediately from Theorem 2.8 and Corollary 2.4 except for the statement about roots of unity, since Dirichlet's unit theorem (see below) implies that the rank of the unit group is determined by the numbers of real and complex places. The roots of unity in K_1 generate a Galois extension of $\mathbf{Q}$ which must lie in the normal core of K_1, and therefore also in the normal core of K_2. Similarly, every root of unity in K_2 lies in the normal core of K_1, and it follows that K_1 and K_2 contain exactly the same roots of unity. □

Let K be a number field with r_1 real places and r_2 complex places, so that

$$K_{\mathbf{R}} := K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^{r_1} \times \mathbf{C}^{r_2},$$

and let $K_{\mathbf{R}}^\times \simeq (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2}$ denote the unit group of the ring $K_{\mathbf{R}}$. We now define the map

$$\begin{aligned}\mathrm{Log}\colon K_{\mathbf{R}}^\times &\to \mathbf{R}^{r_1+r_2}\\ (x_v) &\mapsto (\log\|x_v\|_v),\end{aligned}$$

where v ranges over the archimedean places of K and $\|\ \|_v$ denotes the *normalized absolute value* on K_v, the completion of K with respect to the (equivalence class of the) absolute value v. For $K_v \simeq \mathbf{R}$ the normalized absolute value is just the usual absolute value on $\mathbf{R}$, and for $K_v \simeq \mathbf{C}$ it is the square of the usual absolute value on $\mathbf{C}$ (which is not an absolute value because the triangle inequality fails, but is a multiplicative function $\mathbf{C} \to \mathbf{R}$). It follows from the product formula for K that elements of $\mathcal{O}_K \hookrightarrow K_{\mathbf{R}}^{\times}$ are mapped by Log into the *trace zero hyperplane*

$$\mathbf{R}_0^{r_1+r_2} := \{\mathbf{x} \in \mathbf{R}^{r+s} : \sum \mathbf{x}_i = 0\} \simeq \mathbf{R}^{r_1+r_2-1}.$$

The torsion subgroup of the unit group $\mathcal{O}_K^{\times}$ consists of the roots of unity $\mu_K := \{x^n = 1 : x \in K, n \in \mathbf{Z}_{>0}\}$, and we have an exact sequence of abelian groups

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^{\times} \xrightarrow{\text{Log}} \mathbf{R}_0^{r_1+r_2} \longrightarrow \mathbf{R}_0^{r_1+r_2}/\operatorname{Log}(\mathcal{O}_K^{\times}) \longrightarrow 1$$

Theorem 2.10 (Dirichlet's unit theorem). *Let K be a number field with r_1 real places and s_1 complex places. Then $\operatorname{Log}(\mathcal{O}_K^{\times})$ is a lattice in $\mathbf{R}_0^{r_1+r_s}$ and $\mathcal{O}_K^{\times} \simeq \mu_K \times \mathbf{Z}^{r_1+r_2-1}$.*

Recall that $\zeta_K(s)$ has a simple pole at $s = 1$. The residue of this pole can be computed using the *analytic class number formula*, which involves several of the arithmetic invariants of K that we have already seen, along with the *regulator* R_K and the class number h_K. The regulator is the covolume of $\operatorname{Log}(\mathcal{O}_K^{\times})$ in $\mathbf{R}_0^{r_1+r_2}$, and the class number is the cardinality of the *ideal class group* of $\mathcal{O}_K$, the group of nonzero fractional ideals of $\mathcal{O}_K$ (finitely generated $\mathcal{O}_K$-submodules of K) modulo its subgroup of principal fractional ideals.

Theorem 2.11 (Analytic class number formula). *Let K be a number field with r_1 real places and r_2 complex places. Then*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\#\mu_K |D_K|^{1/2}}.$$

Corollary 2.9 implies that for arithmetically equivalent number fields K_1 and K_2, all of the invariants in the analytic class number formula coincide, except possibly the class number and regulator, and in any case we always have

$$h_{K_1} R_{K_1} = h_{K_2} R_{K_2}.$$

One might then ask whether $h_{K_1} = h_{K_2}$ necessarily holds; the answer is no, as we will see in Lecture 4.

We also know that for arithmetically equivalent number fields K_1 and K_2, for every prime number p the sequence of residue field degrees $f_{\mathfrak{p}_1} \le \cdots \le f_{\mathfrak{p}_r}$ for the primes $\mathfrak{p}_i$ of $\mathcal{O}_{K_1}$ that lie above p coincides with the corresponding sequence of residue field degrees for primes $\mathfrak{p}_i$ of $\mathcal{O}_{K_2}$ that lie above p. One might then ask whether the same holds for the ramification indices $e_{\mathfrak{p}_i}$; here again the answer is no, and we will see examples of this in Lecture 4.

3. Isospectral Riemannian manifolds

We are now ready to prove Sunada's theorem. The proof we give here is a simplification of Sunada's argument due to Buser [7, §11] (c.f. [19, Thm. 4.3A]). Sunada's original argument is already quite simple, but Buser observed that by considering each eigenspace individually one can work entirely with finite dimensional linear representations, rather than working with a trace class operator on an (infinite dimensional) Hilbert space as Sunada does.

Theorem 3.1 (Sunada's Theorem). *Let X be a compact connected Riemannian manifold, let $\pi\colon M \to X$ be a finite normal Riemannian covering, let (G, H_1, H_2) be a Gassmann triple with $G = \operatorname{Deck}(\pi)$, and let $M_1 := M/H_1$ and $M_2 := M/H_2$. Then $\zeta_{M_1}(s) = \zeta_{M_2}(s)$.*

Proof. Let $\pi_i \colon M \to M_i$ be the projection map. Suppose $f \in C^\infty(M_i)$ is an eigenfunction for Δ_{M_i}, say $\Delta_{M_i}(f) = \lambda f$. Then $f \circ \pi_i$ is an H_i-invariant function in $C^\infty(M)$ and

$$\Delta_M(f \circ \pi_i) = \Delta_{M_i}(f) \circ \pi_i = (\lambda f) \circ \pi_i = \lambda(f \circ \pi_i).$$

The first equality follows from the fact that every point $P \in M$ has an open neighborhood U on which $\pi_i \colon U \to \pi_i(U)$ is an isometry, which means that $\Delta_M(f(\pi_i(P)) = \Delta_{M_i}(f)(\pi_i(P))$ for all $P \in U$. Thus every eigenfunction of Δ_{M_i} pulls back to an H_i-invariant eigenfunction of Δ_M with the same eigenvalue. Conversely, if $f \in C^\infty(M)$ is an eigenfunction of Δ_M that is H-invariant, then it induces an eigenfunction of Δ_{M_i} with the same eigenvalue (by the same argument).

Now let λ be any nonzero eigenvalue of Δ_M and let V_λ be the corresponding eigenspace, which has finite dimension equal to the multiplicity of λ in $\lambda(M)$. The multiplicity of λ as an eigenvalue of Δ_{M_i} is the dimension of the subspace $V_\lambda^{H_i}$ of H_i-invariant functions (which may be zero).

The Laplace-Beltrami operator commutes with isometries, so the eigenspaces of Δ_M are G-invariant subspaces of $C^\infty(M)$. For each eigenvalue λ of Δ_M we thus have a linear representation

$$\rho_\lambda \colon G \to \mathbf{GL}(V_\lambda)$$

given by the action of G on V_λ. The linear transformation $\phi_{\lambda,i} \colon V_\lambda \to V_\lambda$ defined by

$$\phi_{\lambda,i} := \frac{1}{\#H_i} \sum_{\sigma \in H_i} \rho_\lambda(\sigma)$$

is idempotent (i.e., $\phi_{\lambda,i}^2 = \phi_{\lambda,i}$) with image $V_\lambda^{H_i}$. It defines a projection $V_\lambda \to V_\lambda^{H_i}$, and we have

$$\dim V^{H_i} = \operatorname{tr} \phi_{\lambda,i} = \frac{1}{\#H_i} \sum_{\sigma \in H_i} \operatorname{tr} \rho_\lambda(\sigma).$$

We now observe that $\#H_1 = \#H_2$ and $\operatorname{tr} \rho_\lambda(\sigma)$ depends only on the conjugacy class of σ in G, so $\dim V_\lambda^{H_1} = \dim V_\lambda^{H_2}$. This holds for every $\lambda \in \lambda(M)$, so $\lambda(M_1) = \lambda(M_2)$ and $\zeta_{M_1}(s) = \zeta_{M_2}(s)$. $\square$

We now want to describe an alternative method for constructing isospectral manifolds due to Vignéras that uses quotients of Lie groups. Vignéras' method predates Sunada's and is not as general, but as we shall see, there is a representation-theoretic thread that underlies them both. We begin by reviewing some background material on arithmetic subgroups of Lie groups.

3.1. **Lattices in locally compact groups.** Recall that a (real) Lie group G is a smooth manifold that is also a topological group (with smooth group operations). We include the case of finite groups, viewed as 0-dimensional manifolds with the discrete topology. Lie groups are locally compact groups (topological groups that are locally compact Hausdorff spaces), and are thus equipped with left and right Haar measures.

Definition 3.2. Let X be a locally compact Hausdorff space The *Borel σ-algebra* $\Sigma(X)$ is the collection of subsets of X generated by open and closed sets under countable unions and intersections; its elements are said to be *measurable*. A function $f : X \to Y$ is *measurable* if $f^{-1}(S) \in \Sigma(X)$ for all $S \in \Sigma(Y)$. A *Borel measure* on X is a countably additive function

$$\mu \colon \Sigma \to \mathbf{R}_{\geq 0} \cup \{\infty\}$$

A *Radon measure* on X is a Borel measure μ on X such that

- $\mu(S) < \infty$ if S is compact (locally finite, since X is locally compact);
- $\mu(S) = \inf\{\mu(U) : S \subseteq U, U \text{ open}\}$ (outer regular);

- $\mu(S) = \sup\{\mu(C) : C \subseteq S, C \text{ compact}\}$ (inner regular).

A Radon measure μ is *finite* if $\mu(X) < \infty$.

In any topological group G, left multiplication, right multiplication, and conjugation by a fixed element are homeomorphisms $G \to G$, as is the map $g \mapsto g^{-1}$. Homeomorphisms preserve measurability (which depends only on $\Sigma(G)$), but need not preserve measure (which depends on $\mu\colon \Sigma(G) \to \mathbf{R}^{\times}_{>0}$).

Definition 3.3. Let G be a locally compact group with a nonzero Radon measure μ. We call μ a *left* (resp. *right*) *Haar measure* if we have $\mu(gS) = \mu(S)$ (resp. $\mu(Sg) = \mu(S)$) for all $g \in G$ and $S \in \Sigma(G)$. In other words, a left/right Haar measure is a nonzero Radon measure invariant under left/right translation.

If μ is a Haar measure on G, so is $c\mu$ for any $c \in \mathbf{R}_{>0}$ (where $c\infty := \infty$).

Theorem 3.4 (Cartan, Weil)**.** *Let G be a locally compact group. Then G admits left and right Haar measures, each of which is unique up to a constant factor.*

Proof. See [8, 53] for the original proofs, or see [31] for a more modern treatment. □

Lemma 3.5. *Let G be a locally compact group equipped with a left or right Haar measure. Every open set in G has nonzero measure and every element of G has an open neighborhood with finite nonzero measure.*

Proof. Let μ be a left (resp. right) Haar measure on G and let $U \subseteq G$ be an open set. For any compact $C \subseteq G$ the left (resp. right) translates of U form an open cover of C, which implies that C lies in a finite union of sets with measure $\mu(U)$. If $\mu(U) = 0$ then $\mu(C) = 0$ for all compact $C \subseteq G$, in which case $\mu(S) = 0$ for all $S \in \Sigma(G)$, by inner regularity, which is a contradiction (Haar measures are nonzero Radon measures), so $\mu(U) > 0$. Every $g \in G$ has a compact neighborhood C which contains an open neighborhood U (since G is locally compact), and $0 < \mu(U) \leq \mu(C) < \infty$, by local finiteness. □

Definition 3.6. Let G be a locally compact group with a left Haar measure μ and let S be an open set of finite measure. The *Haar modulus* (or *modular function*) of G is the continuous group homomorphism[2]

$$\begin{aligned} \delta_G\colon G &\to \mathbf{R}^{\times}_{>0} \\ g &\mapsto \frac{\mu(Sg)}{\mu(S)}. \end{aligned}$$

Note that $\mu(\bullet g)$ is a left Haar measure. The uniqueness of left Haar measures up to scaling implies that δ_G is well-defined: $\mu(Sg) < \infty$ for all $g \in G$, and δ_G does not depend on the choice of S. It follows that δ_G is a group homomorphism, since for any $g, h \in G$ we have

$$\delta_G(gh) = \frac{\mu(Sgh)}{\mu(S)} = \frac{\mu(Sgh)}{\mu(Sg)}\frac{\mu(Sg)}{\mu(S)} = \frac{\mu(Sh)}{\mu(S)}\frac{\mu(Sg)}{\mu(S)} = \delta_G(g)\delta_G(h),$$

since replacing S with Sg does not change δ_G. For any $\epsilon > 0$, by inner and outer regularity we can choose $S' \subseteq C \subseteq S$ with S' open and C compact so that $1 - \epsilon < \mu(S')/\mu(S) \leq \mu(S)/\mu(S') < 1 + \epsilon$. For each $x \in C$ there is an open neighborhood V_x of the identity such that $xV_x \subseteq S$. If we take V to be the intersection of the V_x that arise in a finite subcover of the open cover $\{xV_x : x \in C\}$ of C, then $S'V \subseteq CV \subseteq S$ and $S' \subseteq C \subseteq SV^{-1}$. For all g in the open neighborhood $V \cap V^{-1}$ of the identity we have

$$(1 - \epsilon) < \frac{\mu(S')}{\mu(S)} \leq \frac{\mu(Sg)}{\mu(S)} = \delta_G(g) = \frac{\mu(S'g)}{\mu(S')} \leq \frac{\mu(S)}{\mu(S')} < (1 + \epsilon).$$

[2]The function δ_G is usually denoted Δ_G, but we want to avoid any potential confusion with the Laplace-Beltrami operator.

Thus δ_G is continuous at the identity, and by continuity of the group operation, continuous everywhere. The left and right Haar measures of G are equivalent if and only if $\delta_G = 1$, in which case G is *unimodular*. In general, for any $S \in \Sigma(G)$ we have $\mu(Sg) = \Delta_G(g)\mu(S)$ (but note that both sides may be infinite).

The center of G clearly lies in the kernel of δ_G, as does its commutator subgroup and all torsion elements (since $\mathbf{R}^{\times}_{>0}$ is abelian and torsion free). This implies that $\mathbf{SL}_n(\mathbf{R})$ and $\mathbf{GL}_n(\mathbf{R})$ are unimodular, as are all groups generated by torsion elements, including all finite groups. Compact groups are unimodular, since δ_G is continuous and the only compact subgroup of $\mathbf{R}^{\times}_{>0}$ is the trivial group, as are countable discrete groups (the counting measure is a left and right Haar measure), and abelian groups. For $n > 1$ the subgroup of upper triangular matrices in $\mathbf{GL}_n(\mathbf{R})$ is an example of locally compact group that is not unimodular.

If H is a closed subgroup of a locally compact group G then the left coset space G/H is a locally compact Hausdorff space equipped with a continuous G-action given by left translation.

Definition 3.7. Let H be a closed subgroup of a locally compact group G. A *left Haar measure* μ on G/H is a Radon measure with $\mu(gS) = \mu(S)$ for $g \in G$ and $S \subseteq \Sigma(G/H)$; if $\mu(G/H) < \infty$ then μ is *finite*.

Recall that discrete subgroups of topological groups are closed.

Definition 3.8. A *lattice* in a locally compact group G is a discrete subgroup Γ for which G/Γ admits a finite left Haar measure (note the finiteness condition).

We shall be interested in the case where G is a Lie group, in which case the topology on G is second countable (we included this condition in our definition of a real manifold, but even without it, Lie groups with countably many connected components are still second countable).

Lemma 3.9. *Let Γ be a discrete subgroup of a second countable locally compact group G. Then Γ is countable and G/Γ has a measurable set of unique coset representatives with nonzero measure.*

Proof. Let $\pi\colon G \to G/\Gamma$ be the projection map. Let U be an open neighborhood of the identity $1 \in G$ such that $U \cap \Gamma = \{1\}$, let $A \times B$ be the inverse image of U under the multiplication map $G \times G \to G$, with $A, B \subseteq G$ open, and let $V := (A \cap B)^{-1} \cap (A \cap B)$. Then V is an open neighborhood of the identity with $V^{-1}V \cap \Gamma = \{1\}$. For any $g \in G$ the restriction of π to gV is injective, since for $v_1, v_2 \in V$, if $\pi(gv_1) = \pi(gv_2)$ then $gv_1\gamma_1 = gv_2\gamma_2$ for some $\gamma_1, \gamma_2 \in \Gamma$ and then $\gamma_2\gamma_1^{-1} = v_2^{-1}v_1 \in V^{-1}V \cap \Gamma = \{1\}$.

Let $\{U_n\}_{n\geq 1}$ be a countable subcover of $\{gV : g \in G\}$ (second countable implies Lindelöf); then π restricts to an injective map on each U_n and Γ is countable. Now let $F_1 := U_1$ and for $n > 1$ define

$$F_n := U_n - U_n \cap \pi^{-1}(\pi(U_1 \cup \cdots \cup U_{n-1})).$$

Then π restricts to an injective map on each $F_n \subseteq U_n$ and the images $\pi(F_m)$ and $\pi(F_n)$ are disjoint for $m \neq n$, since $\pi(F_n) = \pi(U_n) - \pi(U_n) \cap (\pi(F_1) \cup \cdots \cup \pi(F_{n-1}))$. Now let $F := \bigcup_{n\geq 1} F_n$. The restriction of π to F is injective, and it also surjective, since $\pi(F) = \pi(\cup_{n\geq 1} U_n) = \pi(G)$. Thus F is a set of unique representatives, and it is measurable, since each F_n is (note that $\pi^{-1}(\pi(U)) = U\Gamma$ is open for any open $U \subseteq G$). The measure of F is clearly nonzero, since it contains the open set U_1. □

A set of unique coset representatives for G/Γ is called a *strict fundamental domain*.

Lemma 3.10. *Let Γ be a discrete subgroup of a second countable locally compact group G. Then G/Γ admits a left Haar measure if and only if $\Delta_G(\Gamma) = \{1\}$.*

Proof. Let $\pi\colon G \to G/\Gamma$ be the quotient map, let F be a measurable strict fundamental domain for G/Γ as in Lemma 3.9, and let ν be a left Haar measure on G. For $S \in \Sigma(G/\Gamma)$ we define

$$\mu(S) := \nu(F \cap \pi^{-1}(S)).$$

For any $g \in G$, the left G-invariance of ν implies

$$\mu(gS) = \nu(F \cap \pi^{-1}(gS)) = \nu(F \cap g\pi^{-1}(S)) = \nu(g^{-1}F \cap \pi^{-1}(S)) = \nu(F' \cap T),$$

where $F' := g^{-1}F$ and $T := \pi^{-1}(S)$. Now F' is also a measurable strict fundamental domain for G/Γ, thus $G = F'\Gamma = F\Gamma$, and $T\Gamma = T$. If $\Delta_G(\Gamma) = \{1\}$ then ν is Γ-right invariant and

$$\mu(gS) = \nu(G \cap F' \cap T) = \sum_{\gamma\in\Gamma} \nu(F\gamma \cap F' \cap T) = \sum_{\gamma\in\Gamma} \nu(F \cap F'\gamma^{-1} \cap T) = \nu(F \cap G \cap T) = \mu(S),$$

implying that μ is a left G-invariant. The function μ is a nonzero Radon measure on G/Γ, since ν restricts to a nonzero Radon measure on F (because F is measurable and G is second countable, hence σ-compact). It follows that μ is a left Haar measure on G/Γ.

Conversely, given a left Haar measure μ on G/Γ, for any $S \in \Sigma(G)$ we may define

$$\nu(S) := \sum_{\gamma\in\Gamma} \mu(\pi(F\gamma \cap S)).$$

The left Haar measure μ on G/Γ lifts to a nonzero Radon measure on each of the measurable strict fundamental domains $F\gamma$, which form a countable partition of G. It follows that ν is a nonzero Radon measure on G. The left G-invariance of μ implies that ν is a left Haar measure, and we note that ν is right Γ-invariant, since π is; it follows that $\Delta_G(\Gamma) = \{1\}$. $\square$

Corollary 3.11. *Let Γ be a lattice in a second countable locally compact group G. Then G is unimodular*

Proof. Let μ be a finite left Haar measure on G/Γ. By Lemma 3.10, the lattice Γ lies in the kernel of $\Delta_G\colon G \to \mathbf{R}^\times_{>0}$, thus Δ_G factors through the corresponding map $G/\Gamma \to \mathbf{R}^\times_{>0}$ induced by μ. It follows that $\Delta_G(G)$ has bounded image in $\mathbf{R}^\times_{>0}$, since μ is finite, but the only bounded subgroup of $\mathbf{R}^\times_{>0}$ is $\{1\}$. Therefore $\Delta_G(G) = \{1\}$, which means that G is unimodular. $\square$

Lemma 3.12. *Let G be a second countable locally compact group with a discrete cocompact subgroup Γ. Then Γ is a lattice.*

Proof. Let $\pi\colon G \to G/\Gamma$ be the projection map and let C be the closure of the measurable strict fundamental domain F for G/Γ given by Lemma 3.9. Then C is compact: if $\{U_n\}$ is an open cover of C, we can assume the sets $\pi(U_n)$ are distinct (if $\pi(U_i) = \pi(U_j)$ then $U_i \cap F = U_j \cap F$ and this implies $U_i \cap C = U_j \cap C$, in which case we can remove U_j from our open cover); taking a finite subcover of the open cover $\{\pi(U_n)\}$ of G/Γ then determines a finite subcover of the open cover $\{U_n\}$ of C.

Let ν be a left Haar measure on G. We have $\nu(F) \le \nu(C) < \infty$, since C is compact, and we also have $\nu(F^{-1}) \le \nu(C^{-1}) < \infty$, since the homeomorphism $g \mapsto g^{-1}$ preserves compactness. The map $g\Gamma \mapsto \Gamma g^{-1}$ is a homeomorphism of the left and right coset spaces G/Γ and $\Gamma\backslash G$, thus $\Gamma\backslash G$ is compact and F^{-1} is a measurable strict fundamental domain for $\Gamma\backslash G$.

Let $\phi\colon G \to \Gamma\backslash G$ be the projection map and define $\mu\colon \Sigma(\Gamma\backslash G) \to \mathbf{R}^\times_{>0}$ by $\mu(S) := \nu(F^{-1} \cap \phi^{-1}(S)$; as in the proof of Lemma 3.10, the Radon measure ν restricts to a radon measure on F^{-1} (because F^{-1} is second countable and G is σ-compact), thus μ is a nonzero Radon measure. For any $\gamma \in \Gamma$ we have

$$\mu(S) = \nu(F^{-1} \cap \phi^{-1}(S)) = \nu(\gamma^{-1}F^{-1} \cap \gamma^{-1}\phi^{-1}(S)) = \nu((\gamma F)^{-1} \cap \phi^{-1}(S)),$$

since ν is left G-invariant and $\phi^{-1}(S)$ is left Γ-invariant. It follows that replacing F with γF does not change the definition of μ. For all $\gamma \in \Gamma$ and $S \in \Sigma(\Gamma\backslash G)$ we have

$$\mu(S\gamma) = \nu(F^{-1} \cap \phi^{-1}(S\gamma)) = \nu(F^{-1}\gamma^{-1}\gamma \cap \phi^{-1}(S)\gamma) = \nu((\gamma F)^{-1} \cap \phi^{-1}(S))\Delta_G(\gamma) = \mu(S)\Delta_G(\gamma).$$

For $S = \Gamma\backslash G$ we have $S\gamma = S$, and therefore

$$\nu(F^{-1}) = \nu(F^{-1} \cap G) = \nu(F^{-1} \cap \phi^{-1}(\Gamma\backslash G)) = \mu(\Gamma\backslash G) = \mu(\Gamma\backslash G\gamma) = \mu(\Gamma\backslash G)\Delta_G(\gamma) = \nu(F^{-1})\Delta_G(\gamma),$$

so $\Delta_G(\gamma) = 1$, since $\nu(F^{-1})$ is finite. Therefore $\Delta_G(\Gamma) = \{1\}$ and we may apply Lemma 3.10. □

Cocompact lattices are said to be *uniform*.

Example 3.13. Not all lattices are uniform; $\mathbf{SL}_2(\mathbf{Z}) \subseteq \mathbf{SL}_2(\mathbf{R})$ is an important example. The subgroup $\mathbf{SL}_2(\mathbf{Z})$ is clearly discrete, and $\mathbf{SL}_2(\mathbf{R})$ is unimodular, so by Lemma 3.10, $\mathbf{SL}_2(\mathbf{Z})$ is a lattice in $\mathbf{SL}_2(\mathbf{R})$, but it is not cocompact (the image of the diagonal subgroup of $\mathbf{SL}_2(\mathbf{R})$ in the quotient is unbounded).

Remark 3.14. We defined the notion of a lattice in terms of left Haar measures and left coset spaces, but we could have instead used right Haar measures and right coset spaces; Lemmas 3.9, 3.10, 3.12 still hold, and the proofs are the same (*mutatis mutandi*). As implied by Corollary 3.11, it makes no difference whether we work with left or right Haar measures: in a locally compact group G that contains a lattice Γ every left Haar measure is also a right Haar measure.[3] In situations where we view Γ as acting on G (rather than the other way around), it will be more natural to work with the right coset space $\Gamma\backslash G$.

3.2. **Representation equivalent subgroups.** In this section we follow the treatment in [19, §4].

Let Γ be a uniform lattice in a Lie group G. The Lie group G is an orientable smooth manifold and thus admits a Riemannian metric and an associated Riemannian volume form that defines a Haar measure; we can use this volume form to integrate any compactly supported smooth function against the Haar measure. The lattice Γ then acts on the Riemannian manifold G via isometries (freely and properly discontinuously), and the quotient space $\Gamma\backslash G$ is a compact Riemannian manifold that is locally isometric to G. We shall use $d\mu$ and μ to denote the Riemannian volume form and corresponding measure on $\Gamma\backslash G$; the measure μ is a nonzero Radon measure that is invariant under the right G-action $\Gamma x \mapsto \Gamma x g$. Note that we do not assume that G is connected; we allow G to be finite (and totally disconnected), in which case we have a Riemannian manifold of dimension zero and μ is the counting measure.

For each $\alpha \in G$ we have a measure preserving right translation operator

$$\begin{aligned} R_{\Gamma,\alpha} \colon \Gamma\backslash G &\to \Gamma\backslash G \\ \Gamma x &\mapsto \Gamma x\alpha. \end{aligned}$$

Let $L^2(\Gamma\backslash G)$ be the Hilbert space of measurable functions on the compact space $\Gamma\backslash G$; it consists of all functions $f : \Gamma\backslash G \to \mathbf{C}$ for which $f^{-1}(S) \in \Sigma(\Gamma\backslash g)$ for all $S \subseteq \Sigma(\mathbf{C})$. The space $L^2(\Gamma\backslash G)$ is a complex vector space equipped with the inner product

$$\langle f, g\rangle := \int_{\Gamma\backslash G} f(x)\bar{g}(x)d\mu(x),$$

and is complete with respect to the metric induced by the norm $\|f\| := \sqrt{\langle f, f\rangle}$ (this is what it means to be a Hilbert space). We may now associate to Γ the linear representation

$$\begin{aligned} \rho_\Gamma \colon G &\to \mathbf{GL}(L^2(\Gamma\backslash G)) \\ \alpha &\mapsto (f \mapsto f \circ R_{\Gamma,\alpha}) \end{aligned}$$

[3]We proved this only in the case that G is second countable, but it holds for all locally compact G; see [13, Thm. 9.16].

The representation ρ_Γ is *unitary*, meaning that each $\rho_\Gamma(g)$ is an automorphism of $L^2(\Gamma\backslash G)$, an invertible linear transformation that preserves inner products. Indeed, for $f, g \in L^2(\Gamma\backslash G)$ and $\alpha \in G$ we have

$$\langle \rho_\Gamma(\alpha)(f), \rho_\Gamma(\alpha)(g)\rangle = \langle f \circ R_{\Gamma,\alpha}, g \circ R_{\Gamma,\alpha}\rangle = \int_{\Gamma\backslash G} f(x\alpha)\bar{g}(x\alpha)d\mu(x) = \int_{\Gamma\backslash G} f(x)\bar{g}(x)d\mu(x) = \langle f, g\rangle,$$

where we have used $d\mu(x) = d\mu(x\alpha)$ (because μ is right G-invariant) to get the third equality.

If $n := [G:\Gamma]$ is finite (as when G is finite, for example), then $L^2(\Gamma\backslash G) \simeq \mathbf{C}^n$, since a function $\Gamma\backslash G$ is simply a list of n complex numbers (all functions are measurable under the counting measure). In this finite setting if we represent $\rho_\Gamma(\alpha)$ in terms of the standard orthonormal basis for $\mathbf{C}^n$, we get a permutation matrix (which we note is unitary); in other words, ρ_Γ is the linear representation corresponding to the permutation representation of G given by its action on the set of right cosets $[\Gamma\backslash G]$.

Definition 3.15. Let G be a Lie group. Two uniform lattices Γ_1, Γ_2 in G are *representation equivalent* if there exists an isomorphism of Hilbert spaces $T: L^2(\Gamma_1\backslash G) \xrightarrow{\sim} L^2(\Gamma_2\backslash G)$ such that

$$T \circ \rho_{\Gamma_1}(\alpha) = \rho_{\Gamma_2}(\alpha) \circ T$$

for all $\alpha \in G$. The unitary isomorphism T is called an *intertwining operator*.

Proposition 3.16. *Let Γ_1, Γ_2 be subgroups of a finite Lie group G. Then Γ_1 and Γ_2 are Gassmann equivalent if and only if they are representation equivalent.*

Proof. We can assume that Γ_1 and Γ_2 have the same index n in G (otherwise they are clearly neither Gassmann equivalent nor representation equivalent). As noted above, if we take standard orthonormal bases for $L^2(\Gamma_1\backslash G) \simeq \mathbf{C}^n$ and $L^2(\Gamma_2\backslash G) \simeq \mathbf{C}^n$ then the linear representations ρ_{Γ_1} and ρ_{Γ_2} coincide with the permutation representations given by the action of G on the coset spaces $[\Gamma_1\backslash G]$ and $[\Gamma_2\backslash G]$. By Lemma 2.7, the subgroups Γ_1 and Γ_2 are Gassmann equivalent if and only if the permutation characters χ_{Γ_1} and χ_{Γ_2} coincides, which occurs if and only if the corresponding linear representations ρ_{Γ_1} and ρ_{Γ_2} are equivalent (see [45, p. 16], for example), in which case they must be unitarily equivalent, by Lemma 3.17, in which case Γ_1 and Γ_2 are representation equivalent. □

Lemma 3.17. *Let $\sigma, \tau: G \to \mathbf{GL}_n(\mathbf{C})$ be unitary representations of a group G. If σ and τ are equivalent then they are unitarily equivalent. More precisely if $T \in \mathbf{GL}_n(\mathbf{C})$ satisfies $T\sigma(\alpha) = \tau(\alpha)T$ for all $\alpha \in G$ then so does the unitary operator U in its polar decomposition $T = UP$, with P hermitian positive definite.*

Proof. For $\alpha \in G$ we have $T\sigma(\alpha) = \tau(\alpha)T$ and $\sigma(\alpha^{-1})T^* = T^*\tau(\alpha^{-1})$, since $\sigma(\alpha)^* = \sigma(\alpha)^{-1} = \sigma(\alpha^{-1})$ (and similarly for τ), and therefore $\sigma(\alpha)T^* = T^*\tau(\alpha)$ for all $\alpha \in G$. We then have

$$T^*T\sigma(\alpha) = T^*\tau(\alpha)T = \sigma(\alpha)T^*T,$$

thus $T^*T = (UP)^*UP = P^2$ commutes with $\sigma(\alpha)$ for all $\alpha \in G$. The operator $\sigma(\alpha)P$ is normal, since

$$(\sigma(\alpha)P)^*(\sigma(\alpha)P) = P\sigma(\alpha)^*\sigma(\alpha)P = P^2 = P^2\sigma(\alpha)\sigma(\alpha)^* = \sigma(\alpha)P^2\sigma(\alpha)^* = (\sigma(\alpha)P)(\sigma(\alpha)P)^*,$$

which implies that the components of its unique polar decomposition (which are $\sigma(\alpha)$ and P) commute with each other; see [43, 12.35], for example. So for all $\alpha \in G$ we have $\sigma(\alpha)P = P\sigma(\alpha)$, and therefore $U\sigma(\alpha)P = UP\sigma(\alpha) = \tau(\alpha)UP$, so $U\sigma(\alpha) = \tau(\alpha)U$ as desired. □

We now continue in our earlier setting: G is a Lie group containing a uniform lattice Γ equipped with a G-invariant Riemannian metric whose volume form is a Haar measure (G is unimodular, so it is both a left and a right Haar measure). For every $\alpha \in G$ the left translation map $L_\alpha: G \to$ defined by $x \mapsto \alpha x$ is an isometry, and the natural projection $G \to \Gamma\backslash G$ is a Riemannian covering (which need not be finite, since G is not necessarily compact, even though $\Gamma\backslash G$ is). Each of the isometries L_α of G induces a local isometry of the compact Riemannian manifold $\Gamma\backslash G$ (but unlike the right translation operator $R_{\Gamma,\alpha}$, the local isometry induced by L_α need not be an isometry of $\Gamma\backslash G$). This allows us to associate to any left-invariant vector field in $\mathfrak{T}(G)$ a corresponding vector field in $\mathfrak{T}(\Gamma\backslash G)$.

A key feature of Riemannian manifolds that are Lie groups with an invariant metric is that they admit an *orthonormal global frame*, a set of left-invariant vector fields that provide a smoothly varying orthonormal basis for each tangent space. Indeed, if we fix an orthonormal basis for the tangent space of the identity we can use the left G-action to define a corresponding set of (smooth) vector fields (to get an orthonormal basis for the tangent space at $\alpha \in G$ multiply each basis element on the left by α). We can identify the space of left-invariant vector fields on G with its Lie algebra $\mathfrak{g}$, and the Lie-theoretic exponential map $\exp\colon \mathfrak{g} \to G$ is the same as the exponential map $\exp\colon T(G) \to G$ on the tangent bundle of the Riemannian manifold G (because we have a G-invariant metric).

Theorem 3.18. *Let Γ_1, Γ_2 be uniform lattices in a Lie group G equipped with a G-invariant Riemannian metric. If Γ_1 and Γ_2 are representation equivalent then the compact Riemannian manifolds $\Gamma_1\backslash G$ and $\Gamma_2\backslash G$ are isospectral, equivalently, $\zeta_{\Gamma_1\backslash G}(s) = \zeta_{\Gamma_2\backslash G}(s)$.*

Proof. Let $X_1, \ldots, X_n \in \mathfrak{T}(M)$ be an orthonormal global frame of left-invariant vector fields. We can express the Laplace-Beltrami operator $\Delta_G\colon C^\infty(G) \to C^\infty(G)$ as

$$\Delta_G(f) = \sum_{1\le i,j\le n} c_{ij} X_i X_j f,$$

for some $c_{ij} \in \mathbf{C}$, where each $X_i\colon C^\infty(G) \to C^\infty(G)$ acts via derivations that can be expressed as

$$X_i(f)(x) := \frac{d}{dt}\Big|_{t=0} f(x\exp(tX_i)),$$

where $\exp(tX_i)$ is the image of X_i under the exponential map $\exp\colon \mathfrak{g} \to G$. Observe that the action of X_i on f is defined via composition with right translation by $\exp(tX_i)$. It follows that for $k = 1, 2$ the induced action of the Laplace-Beltrami operator on the Hilbert space $L^2(\Gamma\backslash G)$ is given by

$$X_i(f)(x) := \frac{d}{dt}\Big|_{t=0} (\rho_{\Gamma_k}(\exp(tX_i))(f))(x),$$

since $\rho_{\Gamma_k}(\exp(tX_i))$ acts on f via composition with the right translation operator $R_{\Gamma_k,\exp(tX_i)}$. If Γ_1 and Γ_2 are representation equivalent then the intertwining operator that relates them intertwines the Laplace-Beltrami operators of $\Gamma_1\backslash G$ and $\Gamma_2\backslash G$ which thus have the same eigenvalue spectrum and therefore the same zeta function. $\square$

3.3. **Arithmetic Fuchsian groups.** In [51] Vignéras constructs non-isomorphism isospectral Riemann surfaces using the Lie group $G = \mathbf{SL}_2(\mathbf{R})$ equipped with the G-invariant metric corresponding to its Haar measure. If we let $K := \mathbf{SO}_2(\mathbf{R})$, the quotient G/K is a (non-compact) Riemannian manifold isomorphic to the hyperbolic plane $\mathfrak{h} := \{z \in \mathbf{C} : \operatorname{Im} z > 0\}$ equipped with the hyperbolic metric

$$ds^2 = \frac{dx^2 + dy^2}{y^2},$$

where $z = x + iy$ and has constant negative curvature -1; the real manifold $\mathfrak{h}$ has a natural complex structure (given by its embedding in the complex plane) and is thus also a *Riemann surface* (a complex manifold of dimension one). The Riemann surface $\mathfrak{h}$ is not compact, but if we extend $\mathfrak{h}$ to $\mathfrak{h}^* := \mathfrak{h} \cup \mathbf{P}^1(\mathbf{R})$ by including the real line and a point ∞ at infinity, we obtain a compact Riemann surface isomorphic to the closed unit disk in $\mathbf{C}$. The automorphism group of $\mathfrak{h}^*$ as a Riemann surface (biholomorphic maps of complex manifolds) and the group of orientation-preserving isometries of $\mathfrak{h}^*$ as a Riemannian manifold are both isomorphic to $\mathbf{PSL}_2(\mathbf{R})$, which acts on $\mathfrak{h}$ via linear fractional transformations: for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{R})$ the map $z \mapsto \frac{ax+b}{cz+d}$ is biholomorphic orientation-preserving isometry (note that $1/0 := \infty$). The kernel of the $\mathbf{SL}_2(\mathbf{R})$-action is ± 1 and the $\mathbf{PSL}_2(\mathbf{R})$-action is faithful and transitive. The stabilizer of $\sqrt{-1} \in \mathfrak{h}$ is $\mathbf{SO}_2(\mathbf{R})$, and we can thus identify the left coset space $\mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R})$ with $\mathfrak{h}$ via the bijection $\gamma\mathbf{SO}_2(\mathbf{R}) \mapsto \gamma\sqrt{-1}$, which is an isomorphism of left $\mathbf{SL}_2(\mathbf{R})$-sets, and of real manifolds, which we can extend to an isomorphism of Riemannian manifolds equipped with the hyperbolic metric.

As noted above, the Lie group $\mathbf{SL}_2(\mathbf{R})$ is unimodular (and second countable), so for any discrete subgroup $\Gamma \leq \mathbf{SL}_2(\mathbf{R})$, the coset space G/Γ admits a left Haar measure, by Lemma 3.10, and Γ is a lattice if and only if this Haar measure is finite, in which case we say that Γ is *cofinite*. As noted above, the same applies to the right coset space $\Gamma\backslash\mathbf{SL}_2(R)$, since $\mathbf{SL}_2(\mathbf{R})$ is unimodular. Discrete subgroups $\Gamma \leq \mathbf{SL}_2(\mathbf{R})$ (or $\mathbf{PSL}_2(\mathbf{R})$) are known as *Fuchsian groups*, which act on $\mathfrak{h}$ properly discontinuously via orientation preserving isometries. The *limit set* $\Lambda(\Gamma)$ of a Fuchsian group Γ is the set of points $x \in \mathfrak{h}^*$ such that $x = \lim_{n\to\infty} \gamma_n x_0$ for some $x_0 \in \mathfrak{h}$ and infinite sequence of distinct $\gamma_n \in \Gamma$; because Γ is discrete, its limit set $\Lambda(\Gamma)$ lies in $\mathfrak{h}^* - \mathfrak{h} = \mathbf{P}^1(\mathbf{R})$. Fuchsian groups Γ for which $\Lambda(\Gamma) = \mathbf{P}^1(\mathbf{R})$ are said to be *of the first kind* (or *of the first type*).

Lattices $\Gamma \leq \mathbf{SL}_2(\mathbf{R})$ are discrete subgroups, hence Fuchsian groups. The fact that lattices are cofinite (meaning that $\mathbf{SL}_2(\mathbf{R})/\Gamma$ has finite measure) implies that lattices are Fuchsian groups of the first kind; in fact, they are precisely the Fuchsian groups of the first kind that are finitely generated (we won't need this so we won't prove it). Note that $\mathbf{SO}_2(\mathbf{R})$ is compact, so if Γ is a uniform lattice in $\mathbf{SL}_2(\mathbf{R})$ then $\Gamma\backslash\mathfrak{h} \simeq \Gamma\backslash\mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R})$ is a compact Riemann surface and also a compact Riemannian manifold with constant negative curvature -1.

To explicitly construct uniform lattices in $\mathbf{SL}_2(\mathbf{R})$ we shall use *arithmetic* subgroups of $\mathbf{SL}_2(\mathbf{R})$. Recall that an (affine) *K-algebraic group* is a group object in the category of affine varieties over the field K. The set of $\mathbf{R}$-points on a $\mathbf{Q}$-algebraic group form a Lie group (the group operations are given by $\mathbf{Q}$-morphisms that induce smooth maps on $\mathbf{R}$-points). The matrix groups $\mathbf{SL}_n$ and $\mathbf{GL}_n$ are $\mathbf{Q}$-algebraic groups.

Definition 3.19. Let G be a Lie group. A subgroup $\Gamma \leq G$ is *arithmetic* if there is a $\mathbf{Q}$-algebraic group H and a morphism of Lie groups $\phi : H(\mathbf{R}) \to G$ with compact kernel and finite cokernel such that $\phi(H(\mathbf{Z}))$ is *commensurable* with Γ, meaning that $\phi(H(\mathbf{Z})) \cap \Gamma$ has finite index in both $\phi(H(\mathbf{Z}))$ and Γ.

Arithmetic groups are discrete (since $\mathbf{Z}$ is discrete in $\mathbf{R}$), and they are also cofinite, which implies that they are lattices (this follows from Lemma 3.12 in the cocompact case, which is all we shall use). Not every discrete cofinite subgroup of a Lie group is an arithmetic group; in particular, $\mathbf{SL}_2(\mathbf{R})$ contains lattices that are nonarithmetic.[4] The simplest examples of nonarithmetic lattices arise as *triangle groups*; see [49] for details. Nevertheless, there are many arithmetic lattices in $\mathbf{SL}_2(\mathbf{R})$, including infinitely many nonconjugate uniform and nonuniform lattices.

For $G = \mathbf{SL}_2(\mathbf{R})$, if we take H to be the $\mathbf{Q}$-algebraic group $\mathbf{SL}_2$ and let $\phi : \mathbf{SL}_2(\mathbf{R}) \to \mathbf{SL}_2(\mathbf{R})$ be the identity map, then any subgroup of $\mathbf{SL}_2(\mathbf{R})$ that is commensurable with $\mathbf{SL}_2(\mathbf{Z})$ is an arithmetic group, and also a lattice (since $\mathbf{SL}_2(\mathbf{Z})$ is). But these arithmetic groups are not uniform lattices, because $\mathbf{SL}_2(\mathbf{Z})$ is not a cocompact subgroup of $\mathbf{SL}_2(\mathbf{R})$, as noted in Example 3.13. For finite index $\Gamma \in \mathbf{SL}_2(\mathbf{Z})$ the quotient $\Gamma\backslash\mathfrak{h}$ is not compact (the quotient $\mathbf{SL}_2(\mathbf{Z})\backslash\mathfrak{h}^*$ is, but we want to be able to use the isomorphism $\Gamma\backslash\mathfrak{h} \simeq \Gamma\backslash\mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R})$). To obtain uniform lattices $\Gamma \leq \mathbf{SL}_2(\mathbf{R})$ that give rise to compact Riemann surfaces $\Gamma\backslash\mathfrak{h}$ we want H to be an order in a division algebra over a number field.

[4] For semisimple Lie groups of higher rank every irreducible lattice is an arithmetic subgroup, as shown by Margulis [33].

3.4. **Quaternion algebras and arithmetic lattices.**

Definition 3.20. Let K be a field whose characteristic is not 2. A *quaternion algebra B over K* is a K-algebra with a basis $1, i, j, k$ satisfying

$$i^2 = a, \qquad j^2 = b, \qquad k = ij = -ji,$$

with $a, b \in K^\times$. We use $\left(\frac{a,b}{K}\right)$ to denote this quaternion algebra, which depends only on the square classes of a and b in $k^\times$ (their images in $k/k^{\times 2}$, where $k^{\times 2} := \{x^2 : x \in k^\times\}$), and we note that

$$\left(\tfrac{a,b}{K}\right) = \left(\tfrac{b,a}{K}\right) = \left(\tfrac{a,-ab}{K}\right) = \left(\tfrac{b,-ab}{K}\right),$$

via a suitable change of basis. The *standard involution* $\alpha \mapsto \bar{\alpha}$ of a quaternion algebra is defined by

$$w + xi + yj + zk \mapsto w - xi - yj - zk.$$

The (reduced) *norm* and *trace* of $\alpha \in B$ are $n(\alpha) := \alpha\bar{\alpha}$ and $t(\alpha) := \alpha + \bar{\alpha}$, respectively, both of which are elements of K, and we have $\alpha^2 - t(\alpha)\alpha + n(\alpha) = 0$ for all α. A quaternion algebra can always be viewed as a subalgebra of the matrix algebra $\mathbf{M}_2(K(\sqrt{a}))$ via the injective K-algebra homomorphism $\phi : B \to \mathbf{M}_2(K(\sqrt{a})$ defined by

$$w + xi + yj + zk \mapsto \begin{pmatrix} w + x\sqrt{a} & b(y + z\sqrt{a}) \\ y - z\sqrt{a} & w - x\sqrt{a} \end{pmatrix}. \tag{2}$$

A quaternion algebra is either a division algebra (every nonzero element is invertible), or isomorphic to the matrix algebra $\mathbf{M}_2(K)$. The latter case occurs if and only if $ax^2 + by^2 = 1$ has a solution $x, y \in K^2$, in which case we say that B is a *split* quaternion algebra. This necessarily holds if either a or b is a square (and by swapping i and j we can assume it is a), in which case the injective K-algebra homomorphism above is an isomorphism to $\mathbf{M}_2(K) = \mathbf{M}_2(K(\sqrt{a}))$. The *Hilbert symbol* $(a, b)_K$ is defined to be 1 if the corresponding quaternion algebra is split and -1 otherwise.

The unit group $B^\times$ is a noncommutative multiplicative group that we may embed in $\mathbf{GL}_2(K(\sqrt{a})$ by restricting the map ϕ defined in (2). This allows us to view $B^\times$ a K-algebraic group as follows. The determinant of $\phi(w+xi+y_zk)$ is the quadratic form $f(w,x,y,z) := w^2 - ax^2 - by^2 + abz^2 \in K[w,x,y,z]$. If we take the affine variety with coordinate ring $K[u,w,x,y,z]/(uf(w,x,y,z) - 1)$ and equip it with morphisms corresponding to the group operations for the algebraic group $\mathbf{GL}_2$ over K, we obtain an algebraic group $G_{B^\times}/K$ with the property that $G_{B^\times}(L) \simeq (B \otimes_K L)^\times$ for any étale K-algebra L.[5] The group of norm one elements $B^1 := \{\alpha \in B : n(\alpha) = 1\}$ is a subgroup of $B^\times$, and we can similarly construct a K-algebraic group G_{B^1} such that $G_{B^1}(L) \simeq (B \otimes_K L)^1$ for any étale K-algebra L.

Recall that a *place* v of a number field K is the equivalence class of a nontrivial absolute value $|\;|_v$ on K; we use K_v to denote the completion of K with respect to the absolute value $|\;|_v$. As a topological field, the completion K_v is locally compact, hence a *local field*. The place v and the local field K_v are *nonarchimedean* if v satisfies the nonarchimedean triangle inequality $|x+y|_v \le \max(x,y)$ for all $x, y \in K$, and v and K_v are *archimedean* otherwise. There is a one-to-one correspondence between prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and nonarchimedean places v in which the corresponding local fields K_v are finite extensions of the p-adic field $\mathbf{Q}_p$, where $(p) = \mathfrak{p} \cap \mathbf{Z}$. Each archimedean place corresponds to an embedding of K into $\mathbf{R}$ (in which case $K_v \simeq \mathbf{R}$ and v is a *real place*), or a conjugate pair of distinct embeddings into $\mathbf{C}$ (in which case $K_v \simeq \mathbf{C}$ and v is a *complex place*).

[5]This holds for any K-algebra, but we shall only be interested in *étale K-algebras*, K-algebras that are isomorphic to a finite product of separable field extensions of K; these naturally arise as base changes of separable extensions of K.

A quaternion algebra $B := \left(\frac{a,b}{K}\right)$ over a number field K *splits* at a place v if the quaternion algebra $B_v := B \otimes_K K_v = \left(\frac{a,b}{K_v}\right)$ is split, meaning that $B_v \simeq \mathbf{M}_2(K_v)$, and otherwise it is *ramified* at v, meaning that B_v is a division algebra. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ then we say that B splits or is ramified at $\mathfrak{p}$ according to whether it splits or is ramified at the corresponding nonarchimedean place of K. The product formula for Hilbert symbols implies that B is ramified at only finitely many places, and that the number of ramified places is even; see [52, Cor 14.6.2]. Note that B cannot be ramified at any complex places (every quaternion algebra over $\mathbf{C}$ splits because every element of $\mathbf{C}^\times$ is a square), thus the set $\Sigma(B)$ of ramified places is a finite subset of the noncomplex places of K that has even cardinality. The set $\Sigma(B)$ determines B up to isomorphism [52, Thm. 14.6.1]. We record this fact in the following theorem.

Theorem 3.21. *Let K be a number field. The map $B \mapsto \Sigma(B)$ defines a bijection between isomorphism classes of quaternion algebras over K and finite subsets of noncomplex places of K with even cardinality.*

We say that B is *indefinite* if it splits at some archimedean place of K (this is automatic if K has any complex places). There are two square classes in $\mathbf{R}^\times$, represented by 1 and -1, and it follows that there are two quaternion algebras over $\mathbf{R}$: the split quaternion algebra $\mathbf{M}_2(\mathbf{R}) = \left(\frac{1,1}{\mathbf{R}}\right) = \left(\frac{1,-1}{\mathbf{R}}\right) = \left(\frac{-1,1}{\mathbf{R}}\right)$ and the Hamiltonian division algebra $\mathbf{H} := \left(\frac{-1,-1}{\mathbf{R}}\right)$. There is one square class in $\mathbf{C}^\times$ and thus only one quaternion algebra $\mathbf{M}_2(\mathbf{C}) = \left(\frac{1,1}{\mathbf{C}}\right)$ over $\mathbf{C}$ It follows that if K has r real places c complex places and B splits at exactly t of the real places then

$$B_{\mathbf{R}} := B \otimes_{\mathbf{Q}} \mathbf{R} \simeq \prod_{v|\infty} B_v \simeq \mathbf{M}_2(\mathbf{R})^t \times \mathbf{H}^{r-t} \times \mathbf{M}_2(\mathbf{C})^c, \tag{3}$$

where we write $v|\infty$ to indicate that v ranges over the archimedean places of K. For $t = 1, r = 1, c = 0$ (which occurs when B is an indefinite quaternion algebra over a real quadratic field), composing the natural inclusion $B \hookrightarrow B_{\mathbf{R}}$ with the isomorphism in (3) yields an injective ring homomorphism that we may restrict to embed the unit group $B^\times$ in the matrix group $\mathbf{GL}_2(\mathbf{R})$. If we further restrict to the group of norm one elements of $B^\times$ we obtain a subgroup of $\mathbf{SL}_2(\mathbf{R})$. To obtain lattices $\Gamma \leq \mathbf{SL}_2(\mathbf{R})$ we will further restrict to *orders* in B.

Definition 3.22. Let R be a Dedekind domain with fraction field K. An *R-lattice* in a K-vector space V is a finitely generated R-submodule of V that contains a K-basis for V (equivalently, $A \otimes_R K \simeq V$). An *order* $\mathcal{O}$ in a quaternion algebra B over K is an R-lattice that is a subring of B (in particular, $1 \in \mathcal{O}$).

For any nonzero $a, b \in R$ the ring $R\langle i,j\rangle := R \oplus Ri \oplus Rj \oplus Rk$ is an order in the quaternion algebra $B = \left(\frac{a,b}{K}\right)$ (where $i^2 = a$, $j^2 = b$, $k = ij$). Moreover, every order $\mathcal{O}$ in B contains a suborder of this form: if we write i and j in terms of K-basis for B contained in $\mathcal{O}$ and multiply by a suitable $c \in R$ to clear denominators then ci and cj are elements of $\mathcal{O}$, as are $(ci)^2 = c^2a$ and $(cj)^2 = c^2b$, and $B = \left(\frac{c^2a,c^2b}{K}\right)$, so if we replace a with c^2a and b with c^2b and then $R\langle i,j\rangle$ is a suborder of $\mathcal{O}$.

An order is *maximal* if it is not properly contained in another order; the order $R\langle i,j\rangle$ need not be maximal, in general. Zorn's lemma implies that every order lies in a maximal order, in which it necessarily has finite index (and the same finite index in every maximal order that contains it). In general a quaternion algebras may have infinitely many distinct maximal orders; indeed, if $\mathcal{O}$ is an order then so is $\alpha\mathcal{O}\alpha^{-1}$, which may be distinct from $\mathcal{O}$ if $\alpha \notin K$.

We say that an element of a quaternion algebra over the fraction field of a Dedekind domain is *integral* if its norm and trace lie in R. Every integral element of B is contained in an order, and orders in B can contain only integral elements; see [52, Cor. 10.3.3]. One might suppose that the set of integral elements of B forms a unique maximal order, but this is not true because the set of integral elements is not a ring. Indeed, consider

$$\alpha := \left(\begin{smallmatrix} 1/2 & -3 \\ 1/4 & 1/2 \end{smallmatrix}\right), \qquad \beta := \left(\begin{smallmatrix} 0 & 1/5 \\ 5 & 0 \end{smallmatrix}\right)$$

in the split quaternion algebra $\left(\frac{1,1}{\mathbf{Q}}\right) \simeq \mathbf{M}_2(\mathbf{Q})$; both α and β are integral but neither $\alpha+\beta$ nor $\alpha\beta$ are (this example is taken from [10]).

If $\mathcal{O}$ is an order in a quaternion algebra B then its set of norm one elements

$$\mathcal{O}^1 := \mathcal{O} \cap B^1 = \{\alpha \in \mathcal{O} : n(\alpha) = 1\}$$

forms a multiplicative subgroup of B^1. Now suppose that B is a quaternion algebra over a totally real number field K of degree n that is split at exactly one real place, and let $\iota\colon B \to \mathbf{M}_2(\mathbf{R})$ be the map

$$B \hookrightarrow B_{\mathbf{R}} \simeq \mathbf{M}_2(\mathbf{R}) \times \mathbf{H}^{n-1} \to \mathbf{M}_2(\mathbf{R}),$$

where the first map is the natural injection $B \hookrightarrow B_{\mathbf{R}} = B \otimes_K \mathbf{R}$ and the last map is the natural projection. Restricting to the group of norm one elements $B^1 := \{\alpha \in B : n(\alpha) = 1\}$ yields a map $\iota\colon B^1 \to \mathbf{SL}_2(\mathbf{R})$. We now want to consider

$$\Gamma^1(\mathcal{O}) := \iota(\mathcal{O}^1) \subseteq \mathbf{SL}_2(\mathbf{R}),$$

which we claim is an arithmetic Fuchsian subgroup. The number field K is a $\mathbf{Q}$-algebra, and its multiplicative group $K^\times$ is a $\mathbf{Q}$-algebraic group. This allows us to view the K-algebraic group G_{B^1} as a $\mathbf{Q}$-algebraic group H with the property that $H(\mathbf{R}) \simeq \mathbf{SL}_2(\mathbf{R}) \times (\mathbf{H}^1)^{n-1}$. The Lie group $\mathbf{H}^1 = \{(w,x,y,z) \in \mathbf{R}^4 : w^2 + x^2 + y^2 + z^2 = 1\}$ is compact, as is $(\mathbf{H}^1)^{n-1}$, so the projection map $\phi\colon H(\mathbf{R}) \to \mathbf{SL}_2(\mathbf{R})$ has compact kernel, and it is obviously surjective. Integral elements of B^1 correspond to points in $H(\mathbf{Z})$; this applies in particular to elements of $\mathcal{O}^1 \subseteq B^1$, and we note that $\Gamma^1(\mathcal{O})$ is commensurable with $\phi(H(\mathbf{Z}))$ (this follows from the fact that the order $\mathcal{O}$ has finite index in any maximal order that contains it). Therefore $\Gamma^1(\mathcal{O})$ is an arithmetic subgroup of $\mathbf{SL}_2(\mathbf{R})$, hence a Fuchsian group of the first kind, since arithmetic subgroups are discrete and cofinite, and it follows that $\Gamma^1(\mathcal{O})$ is a lattice in $\mathbf{SL}_2(\mathbf{R})$. Moreover, if B is a division algebra then $\Gamma^1(\mathcal{O})$ is cocompact and therefore a uniform lattice [52, Thm. 38.4,3].[6]

Thus given any order $\mathcal{O}$ in a non-split quaternion algebra over a totally real number field that is split at exactly one real place we can construct a uniform arithmetic lattice $\Gamma^1(\mathcal{O}) \le SL_2(\mathbf{R})$. It turns out that every uniform arithmetic lattice in $\mathbf{SL}_2(\mathbf{R})$ arises in this way, as shown by Weil [54].

3.5. **Vignéras' construction.** To construct non-isomorphic isospectral Riemann surfaces Vignéras uses a quaternion algebra B over a totally real number field K with the following properties:

(1) B is split at exactly one real place of K;
(2) B contains no roots of unity other than ± 1;
(3) B is not split over K;
(4) B contains maximal orders $\mathcal{O}_1$, $\mathcal{O}_2$ that are non-conjugate by any $\mathbf{Q}$-automorphism of B;
(5) B is ramified at a prime ideal (a) of $\mathcal{O}_K$ with $v(a) > 0$ for all real places v of K ramified in B (if K is quadratic this is equivalent to requiring B to be ramified at some principal prime ideal).

Properties (1) and (3) ensure that for any order $\mathcal{O}$ of B we have an associated uniform arithmetic lattice $\Gamma^1(\mathcal{O}) \le \mathbf{SL}_2(\mathbf{R})$, as described in the previous section. Properties (2) and (5) ensure that for any two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ the subgroups $\Gamma_1 := \Gamma^1(\mathcal{O}_1)$ and $\Gamma_2 := \Gamma^1(\mathcal{O}_2)$ of $\mathbf{SL}_2(\mathbf{R})$ are representation equivalent (see [51, Thm. 7] and the remarks following). Property (4) ensures that we can construct non-isometric compact Riemannian manifolds as compact Riemann surfaces $X_1 := \Gamma^1(\mathcal{O}_1)\backslash\mathfrak{h}$

[6] This is sometimes known as Hey's Theorem, after Käte Hey who proved this for $K = \mathbf{Q}$ in her 1929 PhD thesis [26].

and $X_2 := \Gamma^1(\mathcal{O}_2)\backslash\mathfrak{h}$, where $\mathcal{O}_1$ and $\mathcal{O}_2$ are non-conjugate maximal orders of B; see [51, Thm. 3]. As explained in §3.3, the hyperbolic metric on $\mathfrak{h}$ induces a Riemannian metric on X_1 and X_2.

To ensure (2) we can apply the following proposition.

Proposition 3.23. *Let B be a quaternion algebra over a number field K and let ζ_n be a primitive nth root of unity with $n > 2$. The group $B^\times/K^\times$ contains a cyclic subgroup of order n if and only $\zeta_n + \zeta_n^{-1} \in K$ and the quaternion algebra $B \otimes_K K(\zeta_n)$ splits.*

Proof. See [52, Prop. 32.5.1]. □

The simplest way to achieve (4) is to first ensure that any $\mathbf{Q}$-automorphism of B is an inner automorphism (conjugation by an element of B); this will necessarily be the case if there are $\mathrm{Gal}(K/\mathbf{Q})$-conjugate prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_K$ such that B is ramified at $\mathfrak{p}_1$ but not at $\mathfrak{p}_2$. The *type number* T_B of a quaternion algebra B is the number of conjugacy classes of maximal orders; in order to achieve 4 we must have $t_B > 1$. When B is a quaternion algebra over a totally real field split that is split at exactly on real place we can compute its type number using the formula

$$t_B = [I_K : I_K^2 D_B P_B],$$

where I_K is the ideal group of $\mathcal{O}_K$ (the group of nonzero fractional ideals), D_B is the subgroup of I_K generated by prime ideals that are ramified in B, and P_B is the subgroup of the group P_K of principal fractional ideals (a) of $\mathcal{O}_K$ for which $v(a)$ is positive for all ramified real places of K; see [51, §5]. In order to achieve $t_H > 1$ the class number $[I_K : P_K]$ of K must be even. When the class number of K is even, we will have $t_B = 2$ if and only if $D_B, P_B \leq P_K$, since in this case $I_K^2 = P_K$. This means that we want B to be ramified only at principal prime ideals, so that $D_H \leq P_K$

Thus to obtain non-isometric isospectral compact Riemannian surfaces via Vignéras' method it suffices to pick a real quadratic field K of class number 2 and a quaternion algebra B over K containing no roots of unity other than ± 1 that is ramified at exactly one infinite place and at an odd number of principal prime ideals, one of which has a distinct Galois conjugate that is not ramified in B.

The field $K = \mathbf{Q}(\sqrt{10})$ with class number 2 and the quaternion algebra B ramified at one real place K and at the principal prime ideals (3), (7), $(11 + 3\sqrt{10})$ satisfies these criteria. To verify that B has no roots of unity other than ± 1 we apply Proposition 3.23. The only integers $n > 2$ for which $\zeta_n + \zeta_n^{-1} \in K$ are $n = 3, 4, 6$, and it is enough to check $n = 3, 4$. The prime ideal (7) of $\mathcal{O}_K$ which is ramified in B splits in $K(\zeta_n)$ for $n = 3, 4$, and this implies that $B \times_K K(\zeta_n)$ does *not* split for $n = 3, 4$ (see [52, Prop. 14.6.7]), and therefore B does contains no roots of unity other than ± 1. We have $t_B = 2$, so if let $\mathcal{O}_1$ and $\mathcal{O}_2$ be maximal orders in B representing the two distinct conjugacy classes of maximal orders then the groups $\Gamma^1(\mathcal{O}_1), \Gamma^1(\mathcal{O}_2) \leq \mathbf{SL}_2(\mathbf{R})$ are representation equivalent and the Riemann surfaces $X_1 := \Gamma^1(\mathcal{O}_1)\backslash\mathfrak{h}$ and $X_2 := \Gamma^1(\mathcal{O}_2)\backslash\mathfrak{h}$ are isospectral Riemannian manifolds that are not isometric.

3.6. **A common generalization.** In [14] DeTurck and Gordon prove a generalization of Theorems 3.1 and 3.18 that provides a common framework for the results of both Sunada and Vignéras.

Theorem 3.24. *Let M be a connected Riemannian manifold on which a Lie group G acts via isometries. Let Γ_1 and Γ_2 be representation equivalent uniform lattices in G that act freely and properly discontinuously on M such that $M_1 := \Gamma_1\backslash M$ and $M_2 := \Gamma_2\backslash M$ are compact Riemannian manifolds. Then $\zeta_{M_1}(s) = \zeta_{M_2}(s)$.*

Proof. As noted in Remark 4.3B (iii) of [19], this follows from Theorem 1.16 in [14]. □

Corollary 3.25 (Sunada's theorem)**.** *Let G be a finite group that acting on a compact Riemannian manifold M freely and properly discontinuously via isometries. If Γ_1 and Γ_2 are Gassmann equivalent subgroups of G then the compact Riemannian manifolds $M_1 := \Gamma_1\backslash M$ and $M_2 := \Gamma_2\backslash M$ are isospectral.*

Corollary 3.26 (Vignéras theorem for Riemann surfaces)**.** *If Γ_1 and Γ_2 are representation equivalent uniform arithmetic lattices in $\mathbf{SL}_2(\mathbf{R})$ then the compact Riemann surfaces $M_1 := \Gamma_1\backslash\mathfrak{h}$ and $M_2 := \Gamma_2\backslash\mathfrak{h}$ are isospectral Riemannian manifolds (with the induced hyperbolic metric).*

4. Jacobians of isospectral surfaces

In [41] Prasad and Rajan prove an analog of Sunada's theorem in the setting of algebraic geometry. An *abelian variety* is a connected projective variety that is also an algebraic group (being projective forces the group operation to be commutative, whence the term abelian variety). An *isogeny* $\varphi\colon A \to B$ of abelian varieties over k is a surjective morphism (defined over k) whose kernel is finite (over $\bar{k}$). Two abelian varieties are said to be *isogenous* if they are related by an isogeny, in which case they necessarily have the same dimension. Associated to any smooth projective curve X/k of genus g there is g-dimensional abelian variety $\mathrm{Jac}(X)/k$ known as the *Jacobian* of X; see [35, §III] for a precise definition of $\mathrm{Jac}(X)$ over arbitrary fields k (we give a concrete description for $k = \mathbf{C}$ in terms of tori below). The map $X \to \mathrm{Jac}(X)$ is canonical and defines a functor from the category of smooth projective curves to the category of abelian varieties.[7]

Recall that if G is a finite group of automorphisms of a smooth projective curve X, then there is a smooth projective curve X/G whose points correspond to G-orbits of points of X, equipped with a canonical projection map $\pi_G\colon X \to X/G$ that is a surjective morphism. We use $\mathrm{Aut}(X)$ to denote the automorphism group of X; these are invertible morphisms $X \to X$ that are defined over k.

Theorem 4.1 (Prasad-Rajan)**.** *Let X be a smooth projective curve over a field k and let G be a finite subgroup of* $\mathrm{Aut}(X)$*. If $H_1, H_2 \le G$ are Gassmann equivalent then X/H_1 and X/H_2 have isogenous Jacobians.*

Before proving the theorem, let us explain how it implies an equivalence of zeta functions when k is a finite field or a number field.

Definition 4.2. Let X be a smooth projective curve over a finite field $\mathbf{F}_q$ of cardinality q. The *zeta function* of X is defined as the formal power series

$$Z_X(T) := \exp\left(\sum_{r\ge1} \#X(\mathbf{F}_{q^r})\frac{T^r}{r}\right) = \frac{L_q(T)}{(1-T)(1-qT)};$$

as shown by Artin [1], it is a rational function with numerator $L_q \in \mathbf{Z}[T]$ of degree $2g$. One also defines the *local zeta function* $\zeta_X(s) = Z_X(q^{-s})$. As proved by Tate [50], smooth projective curves over finite fields have the same zeta function if and only if their Jacobians are isogenous; this result is known as *Tate's isogeny theorem*.

Now Let X be a smooth projective geometrically irreducible curve of genus g over a number field K given by an $\mathcal{O}_K$-integral model. The *Hasse-Weil zeta function* of X is defined as a product of local zeta functions

$$\zeta_X(s) := \prod_{\mathfrak{p}} \zeta_{X_{\mathfrak{p}}}(S) = \zeta(s)\zeta(s-1)\prod_{\mathfrak{p}} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s}),$$

[7] The Jacobian can be defined as the unique abelian variety (up to isomorphism) that is birationally equivalent to the gth symmetric power of genus g smooth projective curve X (when X has a k-rational point one can take $\mathrm{Jac}(X) = \mathrm{Pic}^0(X)$).

where $\zeta(s) = \sum_{n\ge1} n^{-s}$ is the Riemann zeta function, $\mathfrak{p}$ varies over prime ideals of $\mathcal{O}_K$, and $X_\mathfrak{p}$ is the reduction of $X_\mathfrak{p}$ to the residue field $\mathcal{O}_K/\mathfrak{p}$. Each $L_\mathfrak{p}(T)$ is an integer polynomial of degree at most $2g$. For all but finitely many primes $\mathfrak{p}$ the curve $X_\mathfrak{p}$ is a smooth projective curve of genus g (in which case we say that X has *good reduction* at $\mathfrak{p}$), and then $L_\mathfrak{p}(T)$ is the numerator of the zeta function $Z_X(T)$ defined above. The definition of $L_\mathfrak{p}(T)$ at bad primes is slightly more complicated and will not concern us here. The key point is that, as proved by Faltings [15], Tate's isogeny theorem also applies to number fields: two smooth projective curves over a number field have the same zeta function if and only if their Jacobians are isogenous.[8]

Thus when k is a finite field or a number field, Theorem 4.24 can be viewed as a direct analog of Sunada's theorem: we have a geometric object X (now an algebraic curve rather than a Riemannian manifold) that is equipped with an action by a finite group G, and Gassmann equivalent subgroups $H_1, H_2 \le G$ give rise to quotients X/H_1 and X/H_2 with the same zeta function.

4.1. **Permutation modules.** In order to prove the theorem of Prasad and Rajan we need to recall a few facts about permutation representations. For a commutative ring R and a group G we use $R[G]$ to denote the *group ring* formed by the free R-module with basis G with multiplication of basis elements defined by the group operation of G. Elements of $R[G]$ are formal sums $\alpha \coloneqq \sum_{g\in G} n_g g$ with only finitely many $n_g \in R$ nonzero, and we define $\operatorname{ord}_g(\alpha) \coloneqq n_g$ so that $\alpha = \sum_{g\in G} \operatorname{ord}_g(\alpha) g$ always holds.

Definition 4.3. Let R be a commutative ring and let X be a left G-set. The *permutation module* $R[X]$ is the left $R[G]$-module given by the free R-module with basis X with multiplication defined by the group action; in other words, we have

$$\Big(\sum_{g\in G} r_g g\Big)\Big(\sum_{x\in X} r_x x\Big) \coloneqq \sum_{g\in G}\sum_{x\in X} r_g r_x g x,$$

where all the sums are finite (only finitely many r_g and r_x can be nonzero). When X is a right G-set the permutation module $R[X]$ is similarly defined as a right $R[G]$-module.

For any subgroup $H \le G$, multiplication on the left by G makes left coset space G/H a left G-set and we have a corresponding permutation module $R[G/H]$, and we similarly have a permutation module $R[H\backslash G]$ given by the right coset space $H\backslash G$ equipped with the natural right action by G. We have natural projections $\pi_{G/H}\colon R[G] \to R[G/H]$ and $\pi_{H\backslash G}\colon R[G] \to R[H\backslash G]$ defined by $g \mapsto gH$ and $g \mapsto Hg$, respectively. The map $\pi_{G/H}$ (resp. $\pi_{H\backslash G}$) is a surjective left (resp. right) $R[G]$-module homomorphism whose kernel is the left (resp. right) $R[G]$-ideal $I_H \coloneqq \langle h-1 : h\in H\rangle$.

Recall that for subgroups H_1, H_2 of a finite group G we use $H_1 \sim H_2$ to denote Gassmann equivalence, and $\chi_{H_i}\colon G \to \mathbf{Z}$ is the character of the permutation representation given by the right G-set $H\backslash G$.

Lemma 4.4. *For subgroups H_1, H_2 of a finite group G the following are equivalent:*

(a) $H_1 \sim H_2$; (b) $\chi_{H_1} = \chi_{H_2}$; (c) $\mathbf{Q}[H_1\backslash G] \simeq \mathbf{Q}[H_2\backslash G]$; (d) $\mathbf{Q}[G/H_1] \simeq \mathbf{Q}[G/H_2]$.

Moreover, the equivalence of (b), (c), (d) *holds for finite index subgroups H_1, H_2 of an infinite group G.*

Proof. The equivalence of (a) and (b) was proved in Lemma 2.7. The equivalence of (b) and (c) follows from the equalities

$$\dim_\mathbf{Q}(\mathbf{Q}[H_i\backslash G]^g) = \chi_{H_i}(\sigma) = \dim_\mathbf{C}(\mathbf{C}[H_i\backslash G]^g),$$

[8] In number theory the *L-function* $L(X,s) \coloneqq \zeta(s)\zeta(s-1)/\zeta_X(S)$ is often used instead of the Hasse-Weil zeta function (as in the conjecture of Birch and Swinnerton-Dyer, for example); the two functions obviously determine each other.

valid hold for all $g \in G$ and $i = 1, 2$. The equivalence of (c) and (d) is given by applying the same equalities with χ_{H_i} replaced by the character $\tilde{\chi}_{H_i}(g)$ of the permutation representation given by the left G-set G/H and noting that $\tilde{\chi}_{H_i}(g) = \chi_{H_i}(g^{-1})$ for all $g \in G$. The last statement in the lemma is clear, since G-sets that arise in (b), (c), (d) are still finite, even if G is not. $\square$

For subgroups H_1, H_2 of a group G and commutative ring R we use $R^{H_1 \backslash G / H_2}$ to denote the R-module of R-valued functions on the set of double cosets $H_1 \backslash G / H_2$.

Lemma 4.5. *Let H_1, H_2 be finite index subgroups of a group G and let R be a commutative ring. We have an R-module isomorphism $\Phi(H_1, H_2)\colon R^{H_1 \backslash G/H_2} \to \mathrm{Hom}_{R[G]}(R[H_1 \backslash G], R[H_2 \backslash G])$ defined by*

$$f \mapsto \Big(H_1 g_1 \mapsto \sum_{H_2 g_2 \in H_2 \backslash G} f(H_1 g_1 g_2^{-1} H_2) H_2 g_2\Big)$$

and an R-module isomorphism $\Psi(H_1, H_2)\colon R^{H_2 \backslash G/H_1} \to \mathrm{Hom}_{R[G]}(R[G/H_1], R[G/H_2])$ defined by

$$f \mapsto \Big(g_1 H_1 \mapsto \sum_{g_2 H_2 \in G/H_2} f(H_2 g_2^{-1} g_1 H_1) g_2 H_2\Big).$$

Proof. We first show $\Phi := \Phi(H_1, H_2)$ is well defined. Clearly $\Phi(f)$ is an R-module homomorphism, but we need to verify that it is a right $R[G]$-module homomorphism. For $g, g_1 \in G$ and $f \in R^{H_1 \backslash G/H_2}$ we have

$$\Phi(f)(H_1 g_1 g) = \sum_{H_2 g_2 \in H_2 \backslash G} f(H_1 g_1 g g_2^{-1} H_2) H_2 g_2 = \sum_{H_2 g_2 \in H_2 \backslash G} f(H_1 g_1 g_2^{-1} H_1) H_2 g_2 g = \Phi(f)(H_1 g_1) g,$$

so $\Phi(f)$ is compatible with the right G-action as required. It is clear that Φ is an R-module homomorphism, we just need to show that it is bijective. If $\Phi(f) = 0$ then $f(H_1 \sigma H_2) = 0$ for all $\sigma \in G$ (take $\tau \in H_2$), and therefore $f = 0$, so Φ is injective.

To show that Φ is surjective, let $\sigma_1, \ldots, \sigma_m \in G$ be a complete set of H_1 right coset representatives, let $\tau_1, \ldots, \tau_n \in G$ be a complete set of H_2 right coset representatives, and let $\pi_1\colon G \to S_m$ and $\pi_2\colon G \to S_n$ be the corresponding permutation representations on the index sets $1 \le i \le m$ and $1 \le j \le n$. Given a right $R[G]$-module homomorphism $\phi : R[H_1 \backslash G] \to R[H_2 \backslash G]$ there is a unique matrix $[r_{ij}] \in R^{m \times n}$ for which $\phi(H_1 \sigma_i) = \sum_j r_{ij} H_2 \tau_j$, and for all $\gamma \in G$ and $1 \le i \le m$ we have

$$\phi(H_1 \sigma_{\pi_1(\gamma)(i)}) = \phi(H_1 \sigma_i \gamma) = \phi(H_1 \sigma_i)\gamma = \sum_{1 \le j \le n} r_{ij} H_2 \tau_j \gamma = \sum_{1 \le j \le n} r_{ij} H_2 \tau_{\pi_2(\gamma)(j)},$$

thus $r_{\pi_1(\gamma)(i)\pi_2(\gamma)(j)} = r_{ij}$ for all i and j. Now suppose that $H_1 \sigma_i \tau_j^{-1} H_2 = H_1 \sigma_k \tau_l^{-1} H_2$ for some i, j, k, l. If we put $\gamma := \sigma_k^{-1} \sigma_i$, so that $H_1 \sigma_k \gamma = H_1 \sigma_i$, then

$$H_1 \sigma_i \tau_j^{-1} H_2 = H_1 \sigma_k \tau_l^{-1} H_2 = H_1 \sigma_k \gamma \gamma^{-1} \tau_l^{-1} H_2 = H_1 \sigma_i (\tau_l \gamma)^{-1} H_2,$$

which implies that $\tau_j^{-1} H_2 = (\tau_l \gamma)^{-1} H_2$ and $H_2 \tau_j = H_2 \tau_l \gamma$. We then have $r_{kl} = r_{\pi_1(\gamma)(k)\pi_2(\gamma)(l)} = r_{ij}$. It follows that the map $H_1 \sigma_i \tau_j^{-1} H_2 \mapsto r_{ij}$ is a well-defined function $f : H_1 \backslash G/H_2 \to R$ for which $\Phi(f) = \phi$, thus Φ is surjective as claimed.

The proof for $\Psi(H_1, H_2)$ is essentially the same (replace right actions with left actions). $\square$

Remark 4.6. There is a canonical bijection of double coset spaces $H_1 \backslash G/H_2 \leftrightarrow H_2 \backslash G/H_1$ given by the map $H_1 g H_2 \mapsto H_2 g^{-1} H_1$. We can pre-compose the corresponding bijection $R^{H_1 \backslash G/H_2} \leftrightarrow R^{H_2 \backslash G/H_1}$ with the isomorphisms $\Phi(H_1, H_2)$ and $\Psi(H_1, H_2)$ in Lemma 4.5 whenever it is convenient to do so.

Let $H_1, H_2 \leq G$ be finite and let $\varphi\colon R[G] \to R[G]$ be a right $R[G]$-module homomorphism such that

$$\varphi(h_1 g) = \varphi(g), \qquad h_2\varphi(g) = \varphi(g) \qquad (h_1 \in H_1,\ h_2 \in H_2,\ g \in G). \tag{4}$$

Then φ is constant on right H_1-cosets, and for every $\alpha \in \operatorname{im}\varphi$ the function $g \mapsto \operatorname{ord}_g(\alpha)$ is constant on right H_2-cosets. The homomorphism φ thus corresponds to a right $R[G]$-module homomorphism $\bar\varphi\colon R[H_1\backslash G] \to R[H_2\backslash G]$ that is uniquely determined by the identity

$$\operatorname{ord}_{H_2 g_2}(\bar\varphi(H_1 g_1)) = \operatorname{ord}_{g_2}(\varphi(g_1)) \qquad (g_1, g_2 \in G). \tag{5}$$

Conversely, for every right $R[G]$-module homomorphism $\bar\varphi\colon R[H_1\backslash G] \to R[H_2\backslash G]$ there is a unique right $R[G]$-module homomorphism φ for which (5) holds, and this φ also satisfies (4). The map $\varphi \mapsto \bar\varphi$ defines an R-module isomorphism $M(H_1,H_2) \to \operatorname{Hom}_{R[G]}(R[H_1\backslash G], R[H_2\backslash G])$, where $M(H_1,H_2)$ is the R-subalgebra of $\operatorname{End}_{R[G]}(R[G])$ whose elements satisfy (4). For any $g_1 \in G$ and $\varphi \in M(H_1,H_2)$ we have

$$\bar\varphi(H_1 g_1) = \sum_{H_2 g_2 \in H_2\backslash G} \operatorname{ord}_{g_2}(\varphi(g_1)) H_2 g_2, \qquad \text{and} \qquad \varphi(g_1) = \sum_{g_2 \in G} \operatorname{ord}_{H_2 g_2}(\bar\varphi(H_1 g_1)) g_2 \tag{6}$$

This also applies to left $R[G]$-module homomorphisms $\varphi\colon R[G] \to R[G]$ and $\bar\varphi\colon R[G/H_1] \to R[G/H_2]$ with appropriate modifications to (4) and (5) (multiply on the right in (4) and use left cosets in (5)).

Corollary 4.7. *Let (G,H_1,H_2) be a Gassmann triple, R a commutative ring, and $\bar\varphi\colon R[H_1\backslash G] \xrightarrow{\sim} R[H_2\backslash G]$ a right $R[G]$-module isomorphism with inverse $\bar\psi\colon R[H_2\backslash G] \xrightarrow{\sim} R[H_1\backslash G]$. Let $f_1 := \Phi(H_1,H_2)(\bar\varphi)$ and $f_2 := \Phi(H_2,H_1)(\bar\psi)$ be the corresponding functions on double cosets given by Lemma 4.5. The following identity holds in the ring $R[G]$:*

$$\Big(\sum_{g\in G} f_1(H_1 g H_2) g\Big)\Big(\sum_{g\in G} f_2(H_2 g H_1) g\Big) = \#H_2 \sum_{h\in H_1} h. \tag{7}$$

Similarly, if $\bar\varphi$ and $\bar\psi$ are inverse left $R[G]$-module isomorphisms between $R[G/H_1]$ and $R[G/H_2]$ with $f_1 := \Psi(H_1,H_2)(\bar\varphi)$ and $f_2 := \Psi(H_2,H_1)(\bar\psi)$ then

$$\Big(\sum_{g\in G} f_1(H_2 g H_1) g\Big)\Big(\sum_{g\in G} f_2(H_1 g H_2) g\Big) = \#H_1 \sum_{h\in H_2} h. \tag{8}$$

Proof. Let $\varphi,\psi\colon R[G] \to R[G]$ be the unique right $R[G]$-module homomorphisms corresponding to $\bar\varphi, \bar\psi$ as determined by (5). We have $\bar\psi(\bar\varphi(H_1)) = H_1$, since $\bar\psi$ is the inverse of $\bar\phi$, thus

$$H_1 = \sum_{H_2 g_2 \in H_2\backslash G} \operatorname{ord}_{H_2 g_2}(\bar\varphi(H_1))\bar\psi(H_2 g_2) = \sum_{H_1 g_1 \in H_1\backslash G}\ \sum_{H_2 g_2 \in H_2\backslash G} \operatorname{ord}_{H_2 g_2}(\bar\varphi(H_1)) \operatorname{ord}_{H_1 g_1}(\bar\psi(H_2 g_2)) H_1 g_1$$

and therefore

$$\sum_{H_2 g_2 \in H_2\backslash G} \operatorname{ord}_{H_2 g_2}(\bar\varphi(H_1)) \operatorname{ord}_{H_1 g_1} \bar\psi(H_2 g_2)) = \begin{cases} 1 & \text{if } H_1 g_1 = H_1, \\ 0 & \text{otherwise.} \end{cases}$$

Combining this with (5) yields

$$\begin{aligned}
\psi(\varphi(1)) &= \sum_{g_2\in G} \mathrm{ord}_{g_2}(\varphi(1))\psi(g_2)\\
&= \sum_{g_1\in G}\sum_{g_2\in G} \mathrm{ord}_{g_2}(\varphi(1))\,\mathrm{ord}_{g_1}(\psi(g_2))g_1\\
&= \sum_{g_1\in G}\sum_{g_2\in G} \mathrm{ord}_{H_2g_2}(\bar\varphi(H_1))\,\mathrm{ord}_{H_1g_1}(\bar\psi(H_2g_2))g_1\\
&= \#H_2\sum_{h\in H_1} h
\end{aligned}$$

which is the RHS of (7). Notice that this implies $\mathrm{ord}_g(\psi\varphi(1))) = \mathrm{ord}_{g^{-1}}(\psi\varphi(1))$ for all $g\in G$.

To establish the LHS of (7), Lemma 4.5 implies that for any $g_1, g_2\in G$ we have

$$\mathrm{ord}_{H_2g_2}(\bar\varphi(H_1)) = f_1(H_1g_2^{-1}H_2) \qquad\text{and}\qquad \mathrm{ord}_{H_1g_1}(\bar\psi(H_2g_2)) = f_2(H_2g_2g_1^{-1}H_1),$$

and therefore

$$\begin{aligned}
\psi(\varphi(1)) &= \sum_{g_1\in G}\sum_{g_2\in G} f_1(H_1g_2^{-1}H_2)f_2(H_2g_2g_1^{-1}H_1)g_1\\
&= \sum_{g_1\in G}\sum_{g_2\in G} f_1(H_1g_2^{-1}H_2)f_2(H_2g_1^{-1}H_1)g_1g_2\\
&= \sum_{g_1\in G}\sum_{g_2\in G} f_1(H_1g_2^{-1}H_2)f_2(H_2g_1^{-1}H_1)(g_1g_2)^{-1}\\
&= \Big(\sum_{g\in G} f_1(H_1gH_2)g\Big)\Big(\sum_{g\in G} f_2(H_2gH_1)g\Big),
\end{aligned}$$

where the third equality is justified by the identity $\mathrm{ord}_g(\psi\varphi(1))) = \mathrm{ord}_{g^{-1}}(\psi\varphi(1))$ noted above. If $\bar\varphi$ and $\bar\psi$ are inverse left $R[G]$-module isomorphisms the identity (8) is proved similarly. $\square$

We note that Corollary 4.7 is not very useful when $\#H_2$ is divisible by the characteristic of R; we will apply it in characteristic zero, so this will not be a concern for us.

4.2. **Endomorphism rings.** An endomorphism of an abelian variety A over k is a morphism $\varphi\colon A\to A$ of k-algebraic groups; this means that if $m\colon A\times A\to A$ is the morphism defining the group operation then $\varphi\circ m = m\circ(\varphi\times\varphi)$ (as morphisms). The endomorphisms of A form a ring $\mathrm{End}(A)$ under composition and point-wise addition. There is a natural embedding of $\mathbf{Z}$ into $\mathrm{End}(A)$ that identifies $n\in\mathbf{Z}$ with the multiplication-by-n map $[n]\colon A\to A$ defined by $P\mapsto nP := P+\cdots+P$ (notice that this a morphism of k-algebraic groups; it can be expressed as a rational map of projective varieties by composing the diagonal morphism $A\to A\times A$ with the morphism defining the group operation appropriately).

Every isogeny $A\to A$ is an endomorphism, but only endomorphisms with finite kernel are isogenies; this includes the multiplication-by-n maps $[n]$ for all $n\neq 0$, since the n-torsion subgroup $A[n]$ is finite (it is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{2g}$ when n is prime to the characteristic of k and is never larger than this).

If G is a group of automorphisms (invertible endomorphisms) of an abelian variety A, then we can naturally embed the group ring $\mathbf{Z}[G]$ in $\mathrm{End}(A)$ via $\sum n_g g\mapsto \sum[n_g]g$ and view A as a $\mathbf{Z}[G]$-module. When A is the Jacobian of a smooth projective curve X, automorphisms of X induce corresponding automorphism of A, so if G is a subgroup of $\mathrm{Aut}(X)$ we can also view it as a subgroup of $\mathrm{Aut}(\mathrm{Jac}(X))$.

4.3. **Proof of the Prasad-Rajan isogeny theorem.** We are now ready to prove Theorem 4.24, which states that for a smooth projective curve X/k and a finite group $G \leq \mathrm{Aut}(X)$, if (G, H_1, H_2) is a Gassmann triple then the Jacobians of the quotient curves X/H_1 and X/H_2 are isogenous.

Proof of Theorem 4.24. We have $\mathbf{Q}[G/H_1] \simeq \mathbf{Q}[G/H_2]$, by Lemma 4.4, so let $\bar{\varphi} \colon \mathbf{Q}[G/H_1] \xrightarrow{\sim} \mathbf{Q}[G/H_2]$ and $\bar{\psi} \colon : \mathbf{Q}[G/H_1] \xrightarrow{\sim} \mathbf{Q}[G/H_2]$ be inverse left $\mathbf{Q}[G]$-module isomorphisms, and let $f_1 \colon \Psi(H_1, H_2)(\bar{\varphi})$ and $f_2 :- \Psi(H_2, H_1)(\bar{\psi})$ as in Corollary 4.7, so that

$$\Big(\sum_{g\in G} f_1(H_2 g H_1) g\Big)\Big(\sum_{g\in G} f_2(H_1 g H_2) g\Big) = \#H_2 \sum_{h\in H_1} h.$$

The images of f_1 and f_2 in $\mathbf{Q}$ are finite, so there exist positive integers $n_1, n_2 \in \mathbf{Z}$ such that the functions $n_1 f_1$ and $n_2 f_2$ have images in $\mathbf{Z}$. Now define $\phi_1 \in \mathbf{Z}[G]$ by $\phi_1 := n_1 \sum_{g\in G} f_1(H_2 g H_1) g$ and $\phi_2 \in Z[G]$ by $\phi_2 := n_2 \sum_{g\in G} f_2(H_1 g H_2) g$ so that

$$\phi_1 \phi_2 = n_1 n_2 \#H_2 \sum_{h\in H_1} h.$$

As noted above, we may embed $\mathbf{Z}[G]$ in $\mathrm{End}(\mathrm{Jac}(X))$ and view ϕ_1, ϕ_2 as endomorphisms of $\mathrm{Jac}(X)$, and we view each $g \in G \subseteq \mathrm{Aut}(X)$ as an element of $\mathrm{Aut}(\mathrm{Jac}(X))$. The endomorphism $\phi_1 \mathrm{End}(\mathrm{Jac}(X))$ is constant on H_1-orbits and its image is H_2-invariant. Indeed for $P \in \mathrm{Jac}(X)$ and $h_1 \in H_1$,

$$\phi(h_1 P) = n_1 \sum_{g\in G} f_1(H_2 g H_1) g h_1 P = n_1 \sum_{g\in G} f_1(H_2 g h_1 H_1) g h_1 P = n_1 \sum_{g\in G} f_1(H_2 g H_1) g P = \phi(P),$$

and for $h_2 \in H_2$,

$$h_2 \phi(P) = n_1 \sum_{g\in G} f_1(H_2 g H_1) h_2 g P = n_1 \sum_{g\in G} f_1(H_2 h_2 g H_1) g h_1 P = n_1 \sum_{g\in G} f_1(H_2 g H_1) g P = \phi(P),$$

Similarly, the endomorphism $\phi_2 \in \mathrm{End}(\mathrm{Jac}(X))$ is constant on H_2-orbits and its image is H_1-invariant. For $i = 1, 2$ let J_i denote the abelian subvariety of $\mathrm{Jac}(X)$ given by taking the connected component of the identity in the subvariety of $\mathrm{Jac}(X)$ fixed by every element of H_i; the abelian variety J_i is isogenous to the Jacobian $\mathrm{Jac}(X/H_i)$, as shown in [41, Lemma 2], and the endomorphisms $\phi_1, \phi_2 \in \mathrm{End}(\mathrm{Jac}(X))$ induce morphisms of abelian varieties $\bar{\phi}_1 \colon J_1 \to J_2$ and $\bar{\phi}_2 \colon J_2 \to J_1$. The endomorphism of J_1 induced by $\sum_{h\in H_1} h \in \mathbf{Z}[G] \subseteq \mathrm{End}(\mathrm{Jac}(X))$ is the multiplication-by-$\#H_1$ map $[\#H_1]$, since each $h \in H_1$ acts as the identity on J_1. It follows that

$$\bar{\phi}_1 \circ \bar{\phi}_2 = [n_1 n_2 \#H_2 \#H_1],$$

and therefore the kernel of $\bar{\phi}_1$ is finite. Thus $\bar{\phi}_1$ is an isogeny (as is $\bar{\phi}_2$), so the abelian varieties J_1 and J_2 are isogenous, as are the Jacobians $\mathrm{Jac}(X/H_1)$ and $\mathrm{Jac}(X/H_2)$. □

4.4. **Isospectral Riemann surfaces with isogenous Jacobians.** Let X be a compact Riemann surface. The field $\mathbf{C}(X)$ of meromorphic functions on X is a finitely generated extension of $\mathbf{C}$ of transcendence degree 1 (a *function field* over $\mathbf{C}$); conversely, every such field arises from a compact Riemann surface and we have a contravariant equivalence (or *anti-equivalence*) of categories between the category of compact Riemann surfaces (whose morphisms are nonconstant holomorphic maps) and the category of function fields over $\mathbf{C}$ (whose morphisms are field embeddings). We also have a contravariant equivalence of categories between function fields over a field k and smooth projective curves over k (whose morphisms are non-constant morphisms of curves), and in the case $k = \mathbf{C}$ this yields an equivalence between the category of Riemann surfaces and the category of smooth projective curves over $\mathbf{C}$; see [23] or [37] for proofs of these equivalences. Note that if we start with a smooth projective curve over a number field k, we can always extend the field of definition to $\mathbf{C}$ and thereby obtain a corresponding Riemann surface.

Any compact Riemann surface X is a smooth manifold which can be naturally be endowed with a Riemannian metric of constant negative curvature -1, making it a compact Riemannian manifold that we can also view as a smooth projective curve over $\mathbf{C}$. This naturally leads to the following question. Suppose G is a finite group of automorphisms of X acting via isometries and (G, H_1, H_2) is a Gassmann triple such that X/H_1 and X/H_2 are compact Riemann surfaces (and compact Riemannian manifolds with the induced metric). Sunada's theorem implies that X/H_1 and X/H_2 are isospectral, and we can also ask whether the corresponding Jacobians are isogenous. The answer is yes. This follows from the work of Prasad and Rajan in [41]. Gordon, Makover, and Webb [20] give an elegant proof of this result using a general technique they call *algebraic transplantation* which is interesting in its own right and presented in the sections that follow.

Remark 4.8. More generally one can ask whether isospectral compact Riemann surfaces necessarily have isogenous Jacobians, independent of whether their isospectrality arises from a Gassmann triple. Prasad and Rajan make a precise conjecture to this effect at the end of [41] that remains open.

4.5. **Jacobians or Riemann surfaces.** Let X be a compact Riemann surface of positive genus g. As with smooth manifolds, we have tangent and cotangent spaces that are $\mathbf{C}$-vector spaces of dimension 1, and tangent and cotangent bundles that are complex manifolds of dimension 2 equipped with projection maps to X. The $\mathbf{C}$-vector space of holomorphic sections of the cotangent bundle is denoted $\Omega(X)$ (or $\Omega^1(X)$); its elements are *holomorphic differentials* (or *regular differentials* or *holomorphic* 1-*forms*). The dimension of $\Omega(X)$ as a $\mathbf{C}$-vector space is equal to the genus g of X (in fact this is often used to define the genus).

If ω is holomorphic differential, and $\phi_i\colon U_i \to V_i \subseteq \mathbf{C}$ is a chart, there is a holomorphic function $f_i\colon V_i \to \mathbf{C}$ such that for any derivation $D \in \mathcal{T}(X)$ and point $x \in U$ we have $\omega(D)(x) = f_i(\phi_i(x))D_x(\phi_i)$; the shorthand $\omega_i = f_i(z_i)dz_i$ is used to denote this, where $z_i := \phi_i(x)$ is the *local coordinate* for ϕ_i. If $\phi_j\colon U_j \to V_j \subseteq \mathbf{C}$ is an overlapping chart with local coordinate $z_j := \phi_j(x)$ and $T := \phi_i \circ \phi_j^{-1}$ is the transition map then for $x \in U_i \cap U_j$ then $f_j(z_j) = f_i(T(z_j))T'(z_j)$, where T' denotes the complex derivative of the holomorphic function $T\colon V_j \to V_i$. Alternatively, one can simply define a holomorphic differential as a family $\{\omega_i\} = \{f_i(z_i)dz_i\}$ that satisfies these compatibility constraints; this uniquely determines a holomorphic differential ω that does not depend on the choice of atlas.

A *path* on a Riemann surface X is a continuous piecewise C^∞ function $\gamma\colon [a,b] \to X$, where $[a,b] \subseteq \mathbf{R}$ is a closed interval. The path γ is *closed* if $\gamma(a) = \gamma(b)$. If $\gamma([a,b]) \subseteq U$ lies in the domain of a chart $\phi\colon U \to V$ with local coordinate $z := \phi(x)$ and $\omega = f(z)dz$ on ϕ, we put $z(t) := \phi \circ \gamma$ and define

$$\int_\gamma \omega := \int_\gamma f(z)dz = \int_a^b f(z(t))z'(t)dt \in \mathbf{C}.$$

If the image of γ does not lie in the domain of a single chart we subdivide γ into a finite sequence of paths γ_i whose images each lie in the domain of a single chart (this is always possible) and define $\int_\gamma \omega := \sum_i \int_{\gamma_i} \omega$. This integral has standard properties of contour integrals: it is $\mathbf{C}$-linear in ω, obeys the fundamental theorem of calculus, changes sign when the direction of a path is reversed, and depends only on the homotopy class of the path γ; in particular, if γ corresponds to the boundary of the homeomorphic image in X of a circle or polygon in $\mathbf{C}$ then $\int_\gamma \omega = 0$ for all $\omega \in \Omega(X)$.

The group of *chains* $C(X)$ is the free abelian group generated by paths on X; its elements are finite formal sums of paths with integer coefficients. There is a natural map from $C(X)$ to the divisor group of X (the free abelian group generated by the points of X) that sends each chain to the sum of the difference of its end points. Chains that lie in the kernel of this map are called *closed chains* (or 1-*cycles*); we use $Z(X)$ to denote this free abelian group. The subgroup of $Z(X)$ generated by boundaries of triangles (homeomorphic images of oriented triangles in $\mathbf{C}$) is denoted $B(X)$; these are the *boundary chains* of X. The quotient $H_1(X) := Z(X)/B(X)$ is the *first homology group* of X.

We now define the $\mathbf{Z}$-linear map

$$Z(X) \to \Omega(X)^*$$
$$\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$$

which induces a homomorphism of abelian groups $H_1(X) \to \Omega(X)^*$ called the *period map*, since (as noted above) the integral $\int_\gamma \omega$ vanishes whenever γ is a boundary. The image of the period map Λ_X is the *period lattice* of X; it is a free $\mathbf{Z}$-module of rank $2g$ that we may view as a lattice in $\Omega(X)^* \simeq \mathbf{C}^g \simeq \mathbf{R}^{2g}$.

Definition 4.9. Let X be a compact Riemann surface of genus $g > 0$. The *Jacobian* of X is the torus $J(X) := \Omega(X)^*/\Lambda_X$; it is a complex Lie group of dimension g (and a real Lie group of dimension $2g$).

If X is a smooth projective curve defined over a field $k \subseteq \mathbf{C}$ and $X_\mathbf{C}$ denotes the Riemann surface corresponding to the base change of X to $\mathbf{C}$, then $\mathrm{Jac}(X)(\mathbf{C}) \simeq J(X_\mathbf{C})$ (as complex Lie groups). Recall that we have an equivalence of categories between smooth projective curves $X/\mathbf{C}$ and compact Riemann surfaces X; this equivalence identifies the abelian variety $\mathrm{Jac}(X)$ with the complex Lie group $J(X)$ via the isomorphism $\mathrm{Jac}(X)(\mathbf{C}) \simeq J(X)$.

If $\varphi\colon X \to Y$ is a morphism of Riemann surfaces (a nonconstant holomorphic map), then it induces a contravariant *pullback* map $\varphi^*\colon \Omega(Y) \to \Omega(X)$ on differentials which is locally defined by

$$\varphi^*(f_j(z_j)dz_j) := f(\varphi(z_i))\varphi_i'(z_i))dz_i,$$

where $\varphi_i\colon U_i \to U_j$ is the holomorphic map induced by φ from the chart $U_i \to V_i$ of X to the chart $U_j \to V_j$ of Y. We then have obtain a forward map $\varphi_*\colon \Omega(X)^* \to \Omega(Y)^*$ defined by $\varphi_*(f) = (\omega \mapsto f(\varphi^*(\omega)))$ which is compatible with the period maps (φ sends path on X to paths on Y via composition and this induces a morphism of homology groups $\varphi_*\colon H_1(X) \to H_1(Y)$), and we thus obtain a *pushforward* map $J(X) \to J(Y)$ on Jacobians (a morphism of complex Lie groups). In particular, automorphisms of X induce automorphisms of $J(X)$.

4.6. **More on permutation modules.** In order to present the algebraic transplantation result of Gordon-Makover-Webb we need to recall a bit more background on permutation modules, following [20, §3]. Throughout this section G is an arbitrary group and R is a commutative ring. For any right $R[G]$-module W we define the $R[G]$-submodule of *G-invariants*

$$W^G := \{w \in W : wg = w \text{ for all } g \in G\};$$

it is the largest submodule of W on which G acts trivially. For any left $R[G]$-module V we define the quotient $R[G]$-module of *G-coinvariants* by

$$V_G := V/I_G V,$$

where $I_G := \langle g - 1 : g \in G \rangle$ is the *augmentation ideal*, the kernel of the map $R[G] \to R$ defined by $\sum r_g g \mapsto \sum r_g$; it is the largest quotient module of V on which G acts trivially.

For any subgroup $\Gamma \leq G$ we may naturally view W and V as $R[\Gamma]$-modules; these are typically denoted $\mathrm{Res}^G_\Gamma W$ and $\mathrm{Res}^G_\Gamma V$, but we will not use this notation when it is clear from context that we are viewing W and/or V as $R[\Gamma[$-modules. We may then consider the corresponding modules of Γ-invariants and

Γ-coinvariants. The Γ-invariant module W^Γ is a right $R[G]$-module on which Γ acts trivially and thus has a natural structure as a right $R[\Gamma\backslash G]$-module via

$$w\Gamma g := wg \qquad (w \in W^\Gamma, g \in G).$$

Similarly the Γ-coinvariant module V_Γ is a left $R[G]$-module on which Γ acts trivially and thus has a natural structure as a left $R[G/\Gamma]$-module via

$$\Gamma g v := g v \qquad (v \in V_\Gamma, g \in G).$$

4.6.1. *Transplantation of invariants.* In this subsection we treat right $R[G]$-modules W and their submodules of invariants W^Γ, for $\Gamma \le G$.

Definition 4.10. Let G be a group, $\Gamma \le G$ a subgroup, R a commutative ring, and W a right $R[\Gamma]$-module. We define the *coinduced* right $R[G]$-module

$$\operatorname{CoInd}_\Gamma^G W := \operatorname{Hom}_{R[\Gamma]}(R[G], W),$$

with the right G-action given by $f g := (h \mapsto f(gh))$, for $f \in \operatorname{Hom}_{R[\Gamma]}(R[G], W)$ and $g \in G$.

Lemma 4.11. *Let G be a group, $\Gamma \le G$ a subgroup, R a commutative ring, and W a right $R[\Gamma]$-module. We have an isomorphism of (trivial) right $R[\Gamma]$-modules*

$$\begin{aligned} W^\Gamma &\xrightarrow{\sim} (\operatorname{CoInd}_\Gamma^G W)^G \\ w &\mapsto (g \mapsto w) \\ f(1) &\leftarrow\!\shortmid f \end{aligned}$$

Proof. The isomorphism of abelian groups is a special case of Shapiro's Lemma [6, Prop. III.6.2], and it is clearly R-linear and therefore $R[\Gamma]$-linear, since Γ acts trivially on both sides. $\square$

Let Γ be a subgroup of G, and let W be a right $R[G]$-module. The R-module $\operatorname{Hom}_R(R[\Gamma\backslash G], W)$ becomes a right $R[G]$-module when equipped with the diagonal right G-action

$$f g := (\Gamma h \mapsto f(\Gamma h g^{-1}) g) \qquad (f \in \operatorname{Hom}_R(R[\Gamma\backslash G], W), g \in G).$$

Proposition 4.12. *Let G be a group, $\Gamma \le G$ a subgroup, R a commutative ring, and W a right $R[G]$-module. We have a right $R[G]$-module isomorphism*

$$\begin{aligned} \operatorname{Hom}_{R[\Gamma]}(R[G], W) &\xrightarrow{\sim} \operatorname{Hom}_R(R[\Gamma\backslash G], W) \\ f &\mapsto (\Gamma g \mapsto f(g^{-1}) g) \\ (g \mapsto f(\Gamma g^{-1}) g) &\leftarrow\!\shortmid f \end{aligned}$$

and a corresponding right $R[G]$-module isomorphism

$$\begin{aligned} \phi^\Gamma \colon W^\Gamma &\xrightarrow{\sim} \operatorname{Hom}_R(R[\Gamma\backslash G], W)^G \\ w &\mapsto (\Gamma g \mapsto wg) \\ f(\Gamma) &\leftarrow\!\shortmid f \end{aligned}$$

Proof. This is straight-forward verification; the second isomorphism (which is all we shall use) is the composition of the first with the isomorphism in Lemma 4.11 and very easy to check it directly. $\square$

Theorem 4.13 (Transplantation of invariants). *Let Γ_1, Γ_2 be subgroups of a group G, let R be a commutative ring, and let $\varphi\colon R[\Gamma_1\backslash G] \to R[\Gamma_2\backslash G]$ a right $R[G]$-module homomorphism. For any right $R[G]$-module W we have a right $R[G]$-module homomorphism*

$$\varphi_W^{\#}\colon W^{\Gamma_2} \xrightarrow{\sim} W^{\Gamma_1}$$
$$w \mapsto w\varphi(\Gamma_1).$$

The map $\varphi \mapsto \varphi_W^{\#}$ is contravariantly functorial in the sense that for any right $R[G]$-module homomorphism $\psi\colon R[\Gamma_2\backslash G] \to R[\Gamma_3\backslash G]$ we have $(\psi\circ\varphi)_W^{\#} = \varphi_W^{\#}\circ\psi_W^{\#}$.

Proof. We have an induced homomorphism of right $R[G]$-modules

$$\varphi^*\colon \operatorname{Hom}_R(R[\Gamma_2\backslash G], W) \to \operatorname{Hom}_R(R[\Gamma_1\backslash G], W)$$
$$f \mapsto f\circ\varphi,$$

which restricts to a homomorphism on G-invariants. Composing with the isomorphisms $\phi^{\Gamma_1}, \phi^{\Gamma_2}$ given by Proposition 4.12, the map $\varphi_W^{\#} := (\phi^{\Gamma_1})^{-1}\circ\varphi^*\circ\phi^{\Gamma_2}\colon W^{\Gamma_2} \to W^{\Gamma_1}$ is defined by

$$w \mapsto (\Gamma_2 g \mapsto wg) \mapsto (\Gamma_1 g \mapsto w\varphi(\Gamma_1 g)) \mapsto w\varphi(\Gamma_1),$$

as claimed ($w\varphi(\Gamma_1 g)$) is well defined because $w \in W_2^{\Gamma}$ and $\varphi(\Gamma_1 g)$ is an R-sum of right Γ_2-cosets). The map $\varphi \mapsto \varphi_W^{\#}$ is contravariantly functorial because the map $R[\Gamma\backslash G] \mapsto \operatorname{Hom}_R(R[\Gamma\backslash G], W)$ is. ☐

Corollary 4.14. *Let Γ_1, Γ_2 be subgroups of a group G, R be a commutative ring, and $\varphi\colon R[\Gamma_1\backslash G] \to R[\Gamma_2\backslash G]$ a right $R[G]$-module homomorphism. For any right $R[G]$-module homomorphism $\psi\colon X \to Y$ we have a commutative diagram of right $R[G]$-modules:*

$$\begin{tikzcd} X^{\Gamma_2} \arrow[r, "\varphi_X^{\#}"] \arrow[d, "\psi"] & X^{\Gamma_1} \arrow[d, "\psi"] \\ Y^{\Gamma_2} \arrow[r, "\varphi_Y^{\#}"] & Y^{\Gamma_1}. \end{tikzcd}$$

Proof. For any $x \in X_2^{\Gamma}$ we have $\psi(\varphi_X^{\#}(x)) = \psi(x\varphi(\Gamma_1)) = \psi(x)\varphi(\Gamma_1) = \varphi_Y^{\#}(\psi(x))$; the middle equality follows from the fact that ψ is a right $R[G]$-module homomorphism and $\psi(x) \in Y_2^{\Gamma}$. ☐

Example 4.15. Corollary 4.14 provides another proof of Sunada's theorem. If M is a compact Riemannian manifold equipped with an isometric G-action and (G, Γ_1, Γ_2) is a Gassmann triple, then Γ_1 and Γ_2 are representation equivalent, by Lemma 4.4, and if we endow the $\mathbf{C}$-vector spaces $\mathbf{C}[\Gamma_i/\backslash G]$ with a Hermitian inner product by declaring the natural basis of right cosets to be orthonormal, Lemma 3.17 implies that we have a unitary isomorphism of right $\mathbf{C}[G]$-modules $\varphi\colon \mathbf{C}[\Gamma_1\backslash G] \to \mathbf{C}[\Gamma_2\backslash G]$. For $i = 1, 2$ let $M_i := \Gamma_i\backslash M$, and note that $C^\infty(M_i) = C^\infty(\Gamma_i\backslash M) \simeq C^\infty(M)^{\Gamma_i}$ (a smooth function on Γ_i-orbits of M is the same thing as a Γ_i-invariant smooth function on M). If we now put $X = Y = C^\infty(M)$ and let $\psi\colon C^\infty(M) \to C^\infty(M)$ be the Laplace-Beltrami operator Δ_M, which commutes with the G-action (since G acts via isometries) and therefore induces the Laplace-Beltrami operator Δ_{M_i} via its action on $C^\infty(M)^{\Gamma_i}$, for $i = 1, 2$. Corollary 4.14 then yields the commutative diagram

$$\begin{tikzcd} C^\infty(M_2) \arrow[r, "\varphi_X^{\#}"] \arrow[d, "\Delta_{M_2}"] & C^\infty(M_1) \arrow[d, "\Delta_{M_1}"] \\ C^\infty(M_2) \arrow[r, "\varphi_Y^{\#}"] & C^\infty(M_1) \end{tikzcd}$$

whose rows are unitary isomorphisms; this implies that M_1 and M_2 are isospectral.

4.6.2. *Transplantation of coinvariants.* We now consider left $\mathbf{R}[G]$-modules V and their quotient modules of coinvariants V_Γ, for $\Gamma \leq G$.

Definition 4.16. Let G be a group, $\Gamma \leq G$ a subgroup, R a commutative ring, and V a left $R[\Gamma]$-module. We define the *induced* left $R[G]$-module

$$\operatorname{Ind}_\Gamma^G V := R[G] \otimes_{R[\Gamma]} V$$

with the left G-action given by $g(h \otimes v) := (gh) \otimes v$, for $h \in G$, $v \in V$, and $g \in G$.

Lemma 4.17. *Let G be a group, $\Gamma \leq G$ a subgroup, R a commutative ring, and V a left $R[\Gamma]$-module. We have an isomorphism of (trivial) left $R[\Gamma]$-modules*

$$\begin{aligned} V_\Gamma &\xrightarrow{\sim} (\operatorname{Ind}_\Gamma^G W)_G \\ \bar{v} &\mapsto \overline{1 \otimes v} \\ \bar{v} &\leftarrow\!\shortmid \overline{g \otimes v} \end{aligned}$$

Proof. The isomorphism of abelian groups is a special case of Shapiro's Lemma [6, Prop. III.6.2], and it is clearly R-linear and therefore $R[\Gamma]$-linear, since Γ acts trivially on both sides. □

Let Γ be a subgroup of G, and let V be a left $R[G]$-module. The R-module $R[\Gamma\backslash G] \otimes_R V$ becomes a left $R[G]$-module when equipped with the diagonal left G-action

$$g(\Gamma h \otimes v) := (\Gamma h g^{-1} \otimes gv) \qquad (g, h \in G, v \in V).$$

Proposition 4.18. *Let G be a group, $\Gamma \leq G$ a subgroup, R a commutative ring, and V a left $R[G]$-module. We have a left $R[G]$-module isomorphism*

$$\begin{aligned} R[G] \otimes_{R[\Gamma]} V &\xrightarrow{\sim} R[\Gamma\backslash G] \otimes_R V \\ g \otimes v &\mapsto \Gamma g^{-1} \otimes gv \\ g^{-1} \otimes gv &\leftarrow\!\shortmid \Gamma g \otimes v \end{aligned}$$

and a corresponding left $R[G]$-module isomorphism

$$\begin{aligned} \phi_\Gamma \colon V_\Gamma &\xrightarrow{\sim} (R[\Gamma\backslash G] \otimes_R V)_G \\ \bar{v} &\mapsto \overline{\Gamma \otimes v} \\ \overline{gv} &\leftarrow\!\shortmid \overline{\Gamma g \otimes v} \end{aligned}$$

Proof. This is straight-forward verification; the second isomorphism (which is all we shall use) is the composition of the first with the isomorphism in Lemma 4.17 and very easy to check it directly. □

Theorem 4.19 (Transplantation of invariants)**.** *Let Γ_1, Γ_2 be subgroups of a group G, let R be a commutative ring, and let $\varphi \colon R[\Gamma_1\backslash G] \to R[\Gamma_2\backslash G]$ a right $R[G]$-module homomorphism. For any left $R[G]$-module V we have a left $R[G]$-module homomorphism*

$$\begin{aligned} \varphi_\#^V \colon V_{\Gamma_1} &\xrightarrow{\sim} V_{\Gamma_2} \\ \bar{v} &\mapsto \overline{\varphi(\Gamma_1) v} \end{aligned}$$

The map $\varphi \mapsto \varphi_\#^V$ is covariantly functorial in the sense that for any left $R[G]$-module homomorphism $\psi \colon R[\Gamma_2\backslash G] \to R[\Gamma_3\backslash G]$ we have $(\psi \circ \varphi)_\#^V = \psi_\#^V \circ \varphi_\#^V$.

Proof. We have an induced homomorphism of left $R[G]$-modules

$$\begin{aligned}\varphi_*\colon R[\Gamma_1\backslash G]\otimes_R V &\to R[\Gamma_2\backslash G]\otimes_R V\\ \Gamma_1 g\otimes v &\mapsto \varphi(\Gamma_1 g)\otimes v.\end{aligned}$$

which induces a homomorphism on G-coinvariants. Composing with the isomorphisms $\phi_{\Gamma_1}, \phi_{\Gamma_2}$ given by Proposition 4.18, the map $\varphi_\#^V := \phi_{\Gamma_2}^{-1}\circ\varphi_*\circ\phi_{\Gamma_1}\colon V_{\Gamma_1}\to V_{\Gamma_2}$ is defined by

$$\bar v\mapsto \overline{\Gamma_1\otimes v}\mapsto\overline{\varphi(\Gamma_1)\otimes v}\mapsto\overline{\varphi(\Gamma_1)v}$$

The map $\varphi\mapsto\varphi_\#^V$ is covariantly functorial because the map $R[\Gamma\backslash G]\mapsto R[\Gamma\backslash G]\otimes_R V$ is. $\square$

Corollary 4.20. *Let Γ_1,Γ_2 be subgroups of a group G, R be a commutative ring, and $\varphi: R[\Gamma_1\backslash G]\to R[\Gamma_2\backslash G]$ a right $R[G]$-module homomorphism. For any left $R[G]$-module homomorphism $\psi\colon X\to Y$ we have a commutative diagram of left $R[G]$-modules:*

$$\begin{array}{ccc} X_{\Gamma_1} & \xrightarrow{\varphi_\#^X} & X_{\Gamma_2}\\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi}\\ Y_{\Gamma_1} & \xrightarrow{\varphi_\#^Y} & Y_{\Gamma_2}.\end{array}$$

Proof. For any $\bar x\in X_{\Gamma_1}$ we have $\psi(\varphi_\#^X(\bar x)) = \psi(\overline{\varphi(\Gamma_1)x}) = \overline{\varphi(\Gamma_1)\psi(x)} = \varphi_\#^Y(\psi(x))$; the middle equality follows from the fact that ψ is a right $R[G]$-module homomorphism and $\psi(\bar x)\in Y_{\Gamma_1}$. $\square$

4.7. **The pairing lemma.**

Definition 4.21. Let G be a group, let W be a right $\mathbf{C}[G]$-module, and let V be a left $\mathbf{Z}[G]$-module. A $\mathbf{Z}$-bilinear pairing $\langle\cdot,\cdot\rangle\colon W\times V\to\mathbf{C}$ is *G-balanced* if for all $w\in W$, $v\in V$, $g\in G$ we have $\langle w, gv\rangle = \langle wg, v\rangle$.

Example 4.22. Let X be a compact Riemann surface on which G acts on the left via automorphisms; this means that for each $g\in G$ the map $x\mapsto gx$ is a holomorphic map $X\to X$ (with a holomorphic inverse). Let $W=\Omega(X)$ be the right $\mathbf{C}[G]$-module of holomorphic differentials on X, equipped with the pullback action $\omega\mapsto g^*\omega$, and let $V=C(X)$ be the left $\mathbf{Z}[G]$-module of chains on X, equipped with the pushforward action $\gamma\mapsto\varphi\circ\gamma$, and let $\langle\cdot,\cdot\rangle\colon W\times V\to\mathbf{C}$ be the *integration pairing* $\langle\omega,\gamma\rangle\mapsto\int_\gamma\omega$. The integration pairing is G-balanced: $\int_{g\gamma}\omega=\int_\gamma g^*\omega$ for all $\gamma\in C(X)$ and $\omega\in\Omega(X)$.

Given a G-balanced pairing $W\times V\to\mathbf{C}$, for any subgroup $\Gamma\le G$ we have an induced G-balanced pairing

$$\begin{aligned}\langle\cdot,\cdot\rangle_\Gamma\colon W^\Gamma\times V_\Gamma &\to\mathbf{C}\\ (w,\bar v)&\mapsto\langle w,v\rangle.\end{aligned}$$

It is well defined because for any $\gamma\in\Gamma$ we have $\langle w,\gamma v\rangle=\langle w\gamma, v\rangle=\langle w,v\rangle$, since $w\in W^\Gamma$ is Γ-invariant, and this implies that $\langle w,\bar v\rangle_\Gamma$ depends only on the image $\bar v\in V_\Gamma = V/I_\Gamma V$ of $v\in V$.

The pairing $\langle\cdot,\cdot\rangle_\Gamma$ induces a homomorphism of left $\mathbf{Z}[G]$-modules

$$\begin{aligned}\pi_\Gamma\colon V_\Gamma &\to (W^\Gamma)^*\\ \bar v&\mapsto(w\mapsto\langle w,\bar v\rangle_\Gamma),\end{aligned}$$

where the left G-action on $(W^\Gamma)^*$ is given by $gf:=(w\mapsto f(wg))$; note that π_Γ depends on the pairing.

Lemma 4.23 (Pairing lemma)**.** *Let G be a group with subgroups $\Gamma_1, \Gamma_2 \le G$, and let $\varphi\colon \mathbf{Z}[\Gamma_1\backslash G] \to \mathbf{Z}[\Gamma_2\backslash G]$ be a right $\mathbf{Z}[G]$-module homomorphism. For any G-balanced pairing $\langle\cdot,\cdot\rangle\colon W \times V \to \mathbf{C}$ the following diagram commutes*

$$\begin{array}{ccc} V_{\Gamma_1} & \xrightarrow{\pi_{\Gamma_1}} & (W^{\Gamma_1})^* \\ \Big\downarrow{\scriptstyle \varphi^V_\#} & & \Big\downarrow{\scriptstyle (\varphi^\#_W)^*} \\ V_{\Gamma_2} & \xrightarrow{\pi_{\Gamma_2}} & (W^{\Gamma_2})^*. \end{array}$$

where $(\varphi^\#_W)^*\colon (W^{\Gamma_1})^* \to (W^{\Gamma_2})^*$ is defined by $f \mapsto f \circ \varphi^\#_W$.

Proof. For any $\bar{v} \in V_{\Gamma_1}$ we have

$$\begin{aligned} (\varphi^\#_W)^*(\pi_{\Gamma_1}(\bar{v})) &= (\varphi^\#_W)^*(w_1 \mapsto \langle w_1, \bar{v}\rangle_{\Gamma_1}) = (w_2 \mapsto \langle \varphi^\#_W(w_2), \bar{v}\rangle_{\Gamma_1}) \\ &= (w_2 \mapsto \langle w_2\varphi(\Gamma_1), \bar{v}\rangle_{\Gamma_1}) = (w_2 \mapsto \langle w_2\varphi(\Gamma_1), v\rangle) \\ &= (w_2 \mapsto \langle w_2, \varphi(\Gamma_1)v\rangle) = (w_2 \mapsto \langle w_2, \overline{\varphi(\Gamma_1)v}\rangle_{\Gamma_2}) \\ &= \pi_{\Gamma_2}(\overline{\varphi(\Gamma_1)v}) = \pi_{\Gamma_2}(\varphi^V_\#(\bar{v})), \end{aligned}$$

where we used the fact that $\langle\cdot,\cdot\rangle$ is G-balanced to go from the second line to the third. □

4.8. **Isospectral Riemann surfaces with isogenous Jacobians.** As an application of the pairing lemma, let us prove that Riemann surfaces constructed from Gassmann triples (which are necessarily isospectral) have isogenous Jacobians. This result appears as Theorem 4.2 in [20]; as noted therein, it was originally proved in [41].

Theorem 4.24. *Let X be a compact Riemann surface, let $G \le \mathrm{Aut}(X)$ be a finite group, let (G, Γ_1, Γ_2) be a Gassmann triple, and let $X_1 := \Gamma_1\backslash X$ and $X_2 := \Gamma_2\backslash X$. Then $J(X_1)$ and $J(X_2)$ are isogenous.*

Proof. We have $\mathbf{Q}[\Gamma_1\backslash G \simeq \mathbf{Q}[\Gamma_2\backslash G]$, by Lemma 4.4, and after clearing denominators we obtain $\mathbf{Z}[G]$-module homomorphisms $\varphi\colon \mathbf{Z}[\Gamma_1\backslash G] \to \mathbf{Z}[\Gamma_2\backslash G]$ and $\psi\colon \mathbf{Z}[\Gamma_1\backslash G] \to \mathbf{Z}[\Gamma_1\backslash G]$ for which $\varphi\circ\psi$ and $\psi\circ\varphi$ both correspond to multiplication by an integer. The right $\mathbf{Z}[G]$-module homomorphism

$$\varphi^*\colon \operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}[\Gamma_2\backslash G], \Omega(X)) \to \operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}[\Gamma_1\backslash G], \Omega(X))$$

is an isomorphism of $\mathbf{C}[G]$-modules, and this implies that $\varphi^\#_{\Omega(X)} = (\phi^{\Gamma_1})^{-1} \circ \varphi^*\phi^{\Gamma_2}\colon \Omega(X)^{\Gamma_2} \to \Omega(X)^{\Gamma_1}$ is an isomorphism of $\mathbf{C}[G]$-modules (see the proof of Theorem 4.13). Similarly, the left $\mathbf{Z}[G]$-module homomorphism

$$\varphi_*\colon \mathbf{Z}[\Gamma_1\backslash G] \otimes_{\mathbf{Z}} C(X) \to \mathbf{Z}[\Gamma_2\backslash G] \otimes_{\mathbf{Z}} C(X)$$

corresponds to an isomorphism of $\mathbf{Q}[G]$-modules, and therefore $\varphi^{C(X)}_\# = \phi^{-1}_{\Gamma_2}\circ\varphi_*\circ\phi_{\Gamma_1}\colon C(X)_{\Gamma_1} \to C(X)_{\Gamma_2}$ can be viewed as an isomorphism of $\mathbf{Q}[G]$-modules after tensoring with $\mathbf{Q}$.

We have $\Omega(X)^{\Gamma_i} \simeq \Omega(X_i)$ and $C(X)_{\Gamma_i} \simeq C(X_i)$, and applying the pairing lemma to the G-balanced integration pairing $\langle\cdot,\cdot\rangle\colon \Omega(X) \times C(X) \to \mathbf{C}$ yields the commutative diagram

$$\begin{array}{ccc} C(X_1) & \xrightarrow{\pi_{\Gamma_1}} & \Omega(X_1)^* \\ \Big\downarrow{\scriptstyle \varphi^{C(X)}_\#} & & \Big\downarrow{\scriptstyle (\varphi^\#_{\Omega(X)})^*} \\ C(X_2) & \xrightarrow{\pi_{\Gamma_2}} & \Omega(X_2)^*, \end{array}$$

where the left vertical map is a rational isomorphism of $\mathbf{Z}$-module and the right vertical map is an isomorphism of $\mathbf{C}$-vector spaces. We can replace $C(M_i)$ by $H_1(M_i)$, because the transplantation map $\varphi_{\#}^{C(M)}$ carries cycles to cycles and boundaries to boundaries; this induces maps $\pi_{\Gamma_i}\colon H_1(X_i) \to \Omega(X_i)^*$ that are precisely the period maps for X_i (the maps π_{Γ_i} are defined by the integration pairing). Recalling that the Jacobian is the cokernel of the period map, we obtain a commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & H_1(X_1) \arrow[r, "\pi_{\Gamma_1}"] \arrow[d, "\varphi_{\#}^{C(X)}"] & \Omega(X_1) \arrow[r] \arrow[d, "\varphi^{\#}_{\Omega(X)}"] & J(X_1) \arrow[r] \arrow[d, dotted, "\exists\phi"] & 0 \\
0 \arrow[r] & H_1(X_2) \arrow[r, "\pi_{\Gamma_2}"] & \Omega(X_2) \arrow[r] & J(X_2) \arrow[r] & 0
\end{tikzcd}$$

where the left vertical map $\varphi_{\#}^{C(X)}$ is a rational isomorphism, hence has finite kernel and cokernel as $\mathbf{Z}$-linear map. The homology groups $H_1(X_1)$ and $H_1(X_2)$ are torsion free $\mathbf{Z}$-modules and therefore must have the same rank (so X_1 and X_2 have the same genus), and this implies that $\varphi_{\#}^{C(X)}$ is injective. The snake lemma then implies that ϕ must be a surjective map with finite kernel, hence an isogeny. □

References

[1] Emil Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. I, II*, Math. Z. **19**, 153–246.

[2] Pierre H. Bérard, *Spectral geometry: Direct and inverse problems*, Lecture Notes in Mathematics **1207**, Springer, 1986.

[3] Wieb Bosma and Bart de Smit, *On arithmetically equivalent number fields of small degree*, in *Algorithmic Number Theory, Fifth International Symposium, ANTS-V*, C. Fieker and D.R. Kohel (Eds.), Lec. Notes Comp. Sci. **2369** (2002), 67–79.

[4] Alexander von Brill, *Ueber die Discriminante*, Math. Ann. **12** (1877), 87–89.

[5] Robert Brooks, *Non-Sunada graphs*, Ann. Inst. Fourier (Grenoble) **49** (1999), 707–725.

[6] Kenneth S. Brown, *Cohomology of groups*, Springer-Verlag, 1982.

[7] Peter Buser, *Geometry and spectra of compact Riemann surfaces*, Springer, 2010.

[8] Henri Cartan, *Sur la measure do Haar*, C.R. Acad. Sci. Paris **211** (1940), 759–762.

[9] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, first edition, London Mathematical Society, 1967.

[10] Pete Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*, PhD thesis, Harvard University, 2003.

[11] Dragoš Cvetković, Michael Doob, Ivan Gutman, A. Torgašev, *Recent results in the theory of graph spectra*, Annals of Discrete Mathematics **36**, North-Holland Publishing Co., Amsterdam, 1988.

[12] Bart de Smit, *Generating arithmetically equivalent number fields with elliptic curves*, in *Algorithmic Number Theory, Third International Symposium (ANTS-III)*, J.P. Buhler (Ed.), Lec. Notes Comp. Sci. **1423** (1998), 392–399.

[13] Anton Deitmar and Siegfried Echterhoff, *Principles of harmonic analysis*, 2nd edition, Springer, 2014

[14] Dennis DeTurck and Carolyn S. Gordon, *Isospectral deformations II: Trace formulas, metrics, and potentials*, Comm. Pure Appl. Math. **42** (1989), 1067–1095.

[15] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[16] The GAP group, *GAP — Groups, Algorithms, and Programming*, Version 4.8.3, 2016.

[17] Fritz Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz* (comments on the article *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe* by Hurwitz) Math. Z. **25** (1926), 655-665.

[18] Norberto Gavioli, *Subgroups of finite soluble groups inducing the same permutation character*, Trans. Amer. Math. Soc. **349** (1997), 2969–2980.

[19] Carolyn Gordon, *Survey of isospectral manifolds*, in *Handbook of differential geometry, Vol. I* (eds. F.J.E. Dillen and L.C.A. Verstraelen), Elsevier, 2000.

[20] Carolyn Gordon, Eran Makover, and David Webb *Transplantation and Jacobians of Sunada isospectral Riemann surfaces*, Adv. Math. **197** (2005), 86–119.

[21] Carolyn Gordon, David L. Webb, and Scott Wolpert, *One cannot hear the shape of a drum*, Bull. Amer. Math. Soc. (N.S.) **27** (1992), 134–138.

[22] Lorenz Halbeisen and Norbert Hungerbühler, *Generation of isospectral graphs*, J. Graph Theory **31** (1999), 255–265.

[23] Robin Hartshorne, *Algebraic geometry*, Springer, 1977.

[24] Erich Hecke, *Über die beliebiger algebraischer Zahlkörper*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch–Physikalische Klasse (1917) 77–89.

[25] Erich Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch–Physikalische Klasse (1917) 299–318.

[26] Käte Hey, *Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen*, PhD. thesis, Universitẗ Hamburg, 1929.

[27] Kenkichi Iwasawa, *On the rings of valuation vectors*, Ann. of Math. **57** (1953), 331–356.

[28] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), 1547–1570.

[29] Mark Kac, *Can one hear the shape of a drum?*, Amer. Math. Monthly **73** (1966), 1–23.

[30] Jerzy Kaczorowski and Alberto Perelli, *Strong multiplicity one for the Selberg class*, C.R. Acad. Sci. Paris Sér I Math. **332** (2001), 963–968.

[31] Anthony W. Knapp, *Compact and Locally Compact Groups*, Birkhäuser, 2005.

[32] Keiichi Komatsu, *On the adele rings and zeta-functions of algebraic number fields*, Kodai Math. J. **1** (1978), 394–400.

[33] Grigory Margulis, *Arithmeticity of the irreducible lattices in the semi-simple groups of rank greater than* 1, Invent. Math. **76** (1984), 93–120.

[34] S. Minakshisundaram and A. Pleijel, *Some properties of the eigenfunctions of the Laplace-Operator on Riemannian manifolds*, Canad. J. Math. **1** (1949), 242–256.

[35] J.S. Milne, *Abelian varieties*, version 2.0, online course notes, 2008.

[36] John Milnor, *Eigenvalues of the Laplace operator on certain manifolds*, Proc. Natl. Acad. Sci. **51** (1964), 542.

[37] Rick Miranda, *Algebraic curves and Riemann surfaces*, American Mathematical Society, 1995.

[38] Calvin Moore, *Cocompact subgroups of semisimple Lie groups*, J. Reine Angew Math. **350** (1984), 173–177.

[39] Jürgen Neukirch, *Algebraic number thoery*, Springer, 1999.

[40] Robert Perlis, *On the equation* $\zeta_k(s) = \zeta_{k'}(s)$, J. Number Theory **9** (1977), 342–360.

[41] Dipendra Prasad and Conjeeveram S. Rajan, *On an Archimedean analogue of Tate's conjecture*, J. Number Theory **99** (2003), 180–184.

[42] Conjeeveram S. Rajan, *On isospectral arithmetical spaces*, Amer. J. Math. **129** (2007), 791–806.

[43] Walter Rudin, *Functional analysis*, second edition, McGraw–Hill, 1991.

[44] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[45] Jean-Pierre Serre, *Linear representations of finite groups*, Springer, 1977.

[46] Igor R. Shafarevich, *Basic Algebraic Geometry 2*, third edition, Springer, 1994.

[47] Toshikazu Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. **121** (1985), 169–186.

[48] Toshikazu Sunada, *Discrete geometric analysis*, in *Analysis on graphs and its applications*, 51–83, Proc. Sympos. Pure Math. **77**, Amer. Math. Soc., 2008.

[49] Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), 91–106.

[50] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134-144.

[51] Marie-France Vignéras, *Variétés riemanniennes isospectrales et non isométriques*, Ann. of Math. 112 (1980), 21-32.

[52] John Voight, *Quaternion algebras*, preprint, 2018.

[53] André Weil, *L'integration dans les Groupes topologiques et ses applications*, Hermann et Cie., Paris, 1940.

[54] André Weil, *Algebras with involutions and the classical groups*, J. Indian Math. Soc. (NS) **24** (1960), 589–623

[55] Ernst Witt, *Eine Identität zwischen Modulformen zweiten Grades*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 323–337.

[56] Scott Wolpert, *The length spectra as moduli for compact Riemann surfaces*, Ann. of Math. **109** (1979), 323–351.