Advances in Mathematics 312 (2017) 198–208

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

A refined notion of arithmetically equivalent number fields, and curves with isomorphic Jacobians

Dipendra Prasad

School of Mathematics, Tata Institute of Fundamental Research, Colaba, Mumbai-400005, India

A R T I C L E I N F O

Article history:
Received 3 May 2016
Received in revised form 8 March 2017
Accepted 16 March 2017
Available online xxxx
Communicated by Roman Bezrukavnikov

Keywords:
Zeta function of a number field
Arithmetically equivalent number fields
Gassmann triple
Permutation representations
Integral representations
Adele, Idele, and idele class groups
Algebraic curves
Jacobians
Correspondences
Hecke algebras

A B S T R A C T

We construct examples of number fields which are not isomorphic but for which their adele groups, the idele groups, and the idele class groups are isomorphic. We also construct examples of projective algebraic curves which are not isomorphic but for which their Jacobian varieties are isomorphic. Both are constructed using an example in group theory provided by Leonard Scott of a finite group G and subgroups H_1 and H_2 which are not conjugate in G but for which the G-module $\mathbb{Z}[G/H_1]$ is isomorphic to $\mathbb{Z}[G/H_2]$.

For a number field K with ring of integers $\mathcal{O}_K$, define its zeta function to be

E-mail address: dprasad@math.tifr.res.in.

http://dx.doi.org/10.1016/j.aim.2017.03.017

$$\begin{aligned}\zeta_K(s) &= \textstyle\sum_{0\neq\mathfrak{A}\subset\mathcal{O}_K} \dfrac{1}{(N\mathfrak{A})^s},\\ &= \textstyle\prod_{0\neq\wp} \dfrac{1}{1-\frac{1}{(N\wp)^s}}.\end{aligned}$$

Two number fields K_1 and K_2 are said to be arithmetically equivalent if their zeta functions are the same. It is known that arithmetically equivalent number fields have the same degree over $\mathbb{Q}$, same infinity type, same discriminant, same roots of unity, but possibly different finite types, i.e., $K \otimes \mathbb{Q}_p$ may not be the same for certain (ramified) primes, and also class numbers and regulators might be different (this was first noticed in [4]). Arithmetically equivalent number fields all arise from a simple group theoretic point of view which we now recall; for all this, we refer to [7] as well as the survey book [6].

Definition 1. (Gassmann triple) Call a triple of finite groups (G, H_1, H_2) with H_1 and H_2 subgroups of G, a Gassmann triple, if any one of the following equivalent conditions is satisfied.

(1) $\mathbb{C}[G/H_1]$ and $\mathbb{C}[G/H_2]$ are isomorphic as G-modules.
(2) $\mathbb{Q}[G/H_1]$ and $\mathbb{Q}[G/H_2]$ are isomorphic as G-modules.
(3) The subgroups H_1 and H_2 of G intersect each conjugacy class in G in equal number of elements, i.e., $|C \cap H_1| = |C \cap H_2|$ for any conjugacy class C in G.

It is known by [7] that two number fields K_1 and K_2 have the same zeta functions if and only if they have the same Galois closure over $\mathbb{Q}$, with Galois group G, and are obtained as fixed fields of subgroups H_1 and H_2 of G such that (G, H_1, H_2) forms a Gassmann triple.

Clearly if H_1 and H_2 are conjugate in G, then $\mathbb{C}[G/H_1]$ and $\mathbb{C}[G/H_2]$ are isomorphic as G-modules. Therefore the interest in a Gassmann triple (G, H_1, H_2) arises only when H_1 and H_2 are not conjugate in G. Such examples exist in abundance, and one good source of them is $(G(\mathbb{F}_q), P_1(\mathbb{F}_q), P_2(\mathbb{F}_q))$ where G is a reductive group over a finite field $\mathbb{F}_q$, with P_1 and P_2 non-conjugate parabolic subgroups in G but for which their Levi subgroups are conjugate; the smallest such example is therefore for $G = SL_3(\mathbb{F}_2)$, a simple group of order 168 containing $P_1(\mathbb{F}_2)$ and $P_2(\mathbb{F}_2)$, the two conjugacy classes of maximal parabolics, as subgroups of index 7. (It is a theorem of Perlis in [7] that number fields K with $[K : \mathbb{Q}] \leq 6$ are determined up to isomorphism by their zeta functions.) It is useful to note that if (G, H_1, H_2) is a Gassmann triple, and if N is a normal subgroup of G, then $(G/N, H_1', H_2')$ is a Gassmann triple in G/N where H_i' is the image of H_i in G/N; in particular, $H_1 \cap N$ and $H_2 \cap N$ have the same order in G for any normal subgroup N in G.

The refined notion of arithmetic equivalence that we discuss in this paper replaces the isomorphism between $\mathbb{Q}[G/H_1]$ and $\mathbb{Q}[G/H_2]$ to one between $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$. This implies closer relationship between the number fields involved than has been considered before, in particular, as we will see, their class groups and idele class groups are isomorphic. Let's make this crucial definition.

Definition 2. (Refined Gassmann triple) Call a triple of finite groups (G, H_1, H_2) with H_1 and H_2 subgroups of G, a refined Gassmann triple, if $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$ are isomorphic as G-modules.

Given the analogy between class groups and the Jacobian of projective algebraic curves, it is natural that the same ideas also give a general construction of curves with isomorphic Jacobians. Indeed this is the case, and we are able to construct a general class of curves which are not isomorphic but whose Jacobians are. Apparently, the known examples so far were only for small genus by explicit constructions, such as by E. Howe [5] for genus 2 and 3, and by C. Ciliberto and G. van de Geer [2] for genus 4. It may be recalled that the Jacobian $J(C)$ of an algebraic curve C of genus g comes equipped with a principal polarization which can be taken to be the Θ-divisor in $J(C)$ which is the image of C^{g-1} in $J(C)$. By a well-known theorem due to Torelli, two algebraic curves C_1 and C_2 are isomorphic if and only if their Jacobians $J(C_1)$ and $J(C_2)$ are isomorphic by an isomorphism $\phi : J(C_1) \to J(C_2)$ (which is not required to take the zero element of $J(C_1)$ to the zero of $J(C_2)$) which takes the Θ-divisor on $J(C_1)$ to the Θ-divisor on $J(C_2)$.

A somewhat surprising example due to Leonard Scott [10] in finite group theory lies at the heart of this work. We state it as a theorem.

Theorem 1. *(Leonard Scott) There is a triple of finite groups (G, H_1, H_2) with H_1 and H_2 subgroups of G such that $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$ are isomorphic as G-modules, but H_1 and H_2 are not conjugate in G. In fact, there is such an example for the group $G = \mathrm{PSL}_2(\mathbb{F}_{29})$, with both H_1 and H_2 isomorphic to A_5 (and are conjugate in $\mathrm{PGL}_2(\mathbb{F}_{29})$).*

Question 1. It may be noted that for a Gassmann triple of finite groups (G, H_1, H_2), the subgroups H_1 and H_2 need not be isomorphic, whereas the triple of finite groups (G, H_1, H_2) occurring in the previous theorem due to L. Scott have not only H_1 and H_2 isomorphic as groups, but with the much stronger property that one can embed G in a *finite* group G' where H_1 and H_2 become conjugate. Whether an isomorphism of $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$ forces these conclusions is an interesting question to investigate. For Gassmann triples constructed using $G = \mathrm{GL}_2(\mathbb{F}_p)$ (even without the stronger property of being refined Gassmann triple), isomorphism of H_1 and H_2 is a consequence of Lemma 3.6 and Remark 3.7 of [14] as has been pointed out by the referee of this paper. Since a Gassmann triple in $\mathrm{SL}_2(\mathbb{F}_p)$ is naturally a Gassmann triple in $\mathrm{GL}_2(\mathbb{F}_p)$, the conclusion (on isomorphism of H_1 and H_2) follows for Gassmann triples in $\mathrm{SL}_2(\mathbb{F}_p)$ also, and can be seen for $\mathrm{PSL}_2(\mathbb{F}_p)$ too.

Remark 1. Triples of finite groups (G, H_1, H_2) with nonconjugate subgroups H_1 and H_2 in G such that $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$ are isomorphic as G-modules seem quite rare, and the above example of Scott in Theorem 1 is the 'only' known example at this moment. (One can of course generate more examples by embedding $\mathrm{PSL}_2(\mathbb{F}_{29})$ in any bigger group, or by doing a product construction etc., but these should not really be counted as new examples.) It may be added that among the large class of examples (G, P_1, P_2) with P_1 and P_2 associate but nonconjugate parabolics inside a finite group of Lie type $G = \underline{G}(\mathbb{F}_q)$ mentioned earlier, we have $\mathbb{Q}[G/P_1] \cong \mathbb{Q}[G/P_2]$, but for these $\mathbb{Z}[G/P_1] \ncong \mathbb{Z}[G/P_2]$, since in fact $\mathbb{F}_q[G/P_1] \ncong \mathbb{F}_q[G/P_2]$. We give a proof of this due to F. Herzig. Note that if there was an isomorphism between $\mathbb{F}_q[G/P_1]$ and $\mathbb{F}_q[G/P_2]$, then their maximal semi-simple quotient will be isomorphic too. By Frobenius reciprocity,

$$\mathrm{Hom}_P[\mathbb{F}_q, \pi] \cong \mathrm{Hom}_G[\mathbb{F}_q[G/P], \pi],$$

and therefore the irreducible representations π of G over $\mathbb{F}_q$ which appear as a quotient of $\mathbb{F}_q[G/P]$ are exactly those which contain the trivial representation of P. By a result of Curtis in [3], Corollary 6.14, for each parabolic P of G, there exists an irreducible representation π of G over $\mathbb{F}_q$, and a line $\langle v_0 \rangle$ whose stabilizer is exactly P. Further, given a Borel subgroup B in G, by Theorem 4.3(c) of [3], an irreducible representation of G has a unique line fixed by B. This proves that for P_1 and P_2 distinct parabolics containing B, co-socles of $\mathbb{F}_q[G/P_1]$ and $\mathbb{F}_q[G/P_2]$ are distinct.

Lemma 1. *The two G-sets G/H_1 and G/H_2 of $G = \mathrm{PSL}_2(\mathbb{F}_{29})$ appearing in Theorem 1 are isomorphic as H-sets when restricted to any solvable subgroup H of G.*

Proof. (Due to L. Scott) It is well-known and easy to see that the action of a group H on two sets X_1 and X_2 are isomorphic (i.e., there exists an isomorphism of X_1 with X_2 commuting with the action of H) if and only if for any subgroup K of H, the number of fixed points of K on X_1 is the same as on X_2. We prove the lemma using this criterion.

Assume without loss of generality that K has some fixed point in either G/H_1 or G/H_2. Thus K is a subgroup of A_5, and cannot be equal to A_5, since K is a subgroup of H which is solvable. So K is a proper subgroup of A_5.

By an easy inspection, all subgroups K of A_5 are cyclic extensions of p-groups for some prime p, so have the same number of fixed points by Prop. 3.1 of the paper [10] since we know the isomorphism of $\mathbb{Z}_p[G/H_1]$ with $\mathbb{Z}_p[G/H_2]$ as G-modules, and a fortiori as K-modules. Since this is true for all subgroups K of H, the lemma is proved. □

Recall the (contravariant) duality between tori T of dimension n over a field k, and free abelian groups $X(T)$ of rank n together with a representation of $\mathrm{Gal}(\bar{k}/k)$ on $X(T)$. Theorem 1 then allows us to construct tori T_1 and T_2 over k (we are assuming existence of a Galois extension of k with Galois group G; for the particular example of Scott in Theorem 1 above, there is a recent theorem due to D. Zywina [15] constructing a Galois extension K of $k = \mathbb{Q}$ with Galois group $G = \mathrm{PSL}_2(\mathbb{F}_p)$ for any prime p, in particular for $G = \mathrm{PSL}_2(\mathbb{F}_{29})$). Taking the fixed fields under the two non-conjugate copies of A_5 inside $G = \mathrm{PSL}_2(\mathbb{F}_{29})$, we get field extensions K_1, K_2 of $\mathbb{Q}$. Define the two tori T_1, T_2

over $\mathbb{Q}$ such that, $T_1(\mathbb{Q}) = K_1^\times$, and $T_2(\mathbb{Q}) = K_2^\times$. The tori T_1 and T_2 have the property that although $T_1 \cong T_2$ as tori over $\mathbb{Q}$, in particular $K_1^\times \cong K_2^\times$ through an algebraic isomorphism, there is no isomorphism of fields $K_1 \to K_2$.

Given an (algebraic) isomorphism of tori T_1 and T_2 over $\mathbb{Q}$, we get a (topological) isomorphism of adelic groups $T_1(\mathbb{A}_\mathbb{Q})$ and $T_2(\mathbb{A}_\mathbb{Q})$ (which come equipped with natural locally compact Hausdorff topological group structure), taking $T_1(\mathbb{Q})$ to $T_2(\mathbb{Q})$, and hence an isomorphism of the idele class groups:

$$C_{K_1} = \mathbb{A}_{K_1}^\times / K_1^\times \xrightarrow{\cong} \mathbb{A}_{K_2}^\times / K_2^\times = C_{K_2},$$

which does not arise from an isomorphism of fields $K_1 \to K_2$. Further, since we have an algebraic isomorphism of tori T_1 and T_2 over $\mathbb{Q}$, for every number field L, we get an isomorphism of adelic groups $T_1(\mathbb{A}_L)$ and $T_2(\mathbb{A}_L)$, taking $T_1(L)$ to $T_2(L)$, and hence we have a (compatible family of) isomorphisms of the idele class groups:

$$C_{K_1 \otimes L} = \mathbb{A}_{K_1 \otimes L}^\times / (K_1 \otimes L)^\times \xrightarrow{\cong} \mathbb{A}_{K_2 \otimes L}^\times / (K_2 \otimes L)^\times = C_{K_2 \otimes L}.$$

Since an isomorphism of C_{K_1} with C_{K_2} induces an isomorphism of $\pi_0(C_{K_1}) = C_{K_1}/C_{K_1}^0$ with $\pi_0(C_{K_2}) = C_{K_2}/C_{K_2}^0$ where $C_{K_i}^0$ is the connected component of identity of C_{K_i}, we conclude that the Neukirch-Uchida-Pop theorem according to which an isomorphism of $\mathrm{Gal}(\bar{\mathbb{Q}}/K_1)$ with $\mathrm{Gal}(\bar{\mathbb{Q}}/K_2)$ forces an isomorphism of the fields K_1 and K_2 does not hold good for their maximal abelian quotients $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_1)$ and $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_2)$. (In fact much simpler examples are known where $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_1)$ and $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_2)$ are isomorphic to $\widehat{\mathbb{Z}}^2 \times \prod_{n>1} \mathbb{Z}/n$ as profinite groups without K_1 being isomorphic to K_2, such as for imaginary quadratic extensions of $\mathbb{Q}$ which have class number one but are not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, cf. [1].)

We now come to the main result of this paper about number fields.

Theorem 2. *Let (G, H_1, H_2) be a refined Gassmann triple. Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, with subfields K_1 and K_2 defined as the fixed fields of H_1 and H_2. Then we have:*

(1) $\zeta_{K_1} = \zeta_{K_2}$.
(2) $\mathbb{A}_{K_1}^\times \cong \mathbb{A}_{K_2}^\times$ *as topological groups with an isomorphism taking $K_1^\times$ to $K_2^\times$, and therefore, inducing an isomorphism of the idele class groups:*

$$C_{K_1} = \mathbb{A}_{K_1}^\times / K_1^\times \xrightarrow{\cong} \mathbb{A}_{K_2}^\times / K_2^\times = C_{K_2},$$

as well as for all number fields L, a (compatible family of) isomorphisms of the idele class groups:

$$C_{K_1 \otimes L} = \mathbb{A}_{K_1 \otimes L}^\times / (K_1 \otimes L)^\times \xrightarrow{\cong} \mathbb{A}_{K_2 \otimes L}^\times / (K_2 \otimes L)^\times = C_{K_2 \otimes L}.$$

(3) *If $C\ell(K)$ is the class group of a number field K, then $C\ell(K_1) \cong C\ell(K_2)$, as well as compatible isomorphisms $C\ell(K_1 \otimes L) \cong C\ell(K_2 \otimes L)$ for all number fields L.*
(4) $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_1) \cong \mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_2)$ *as profinite groups; further,* $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/LK_1) \cong \mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/LK_2)$ *as profinite groups for all number fields L which are disjoint from K so that $LK_1 = L \otimes K_1$ and $LK_2 = L \otimes K_2$ are number fields contained in $\bar{\mathbb{Q}}$.*

Proof. Most parts of the theorem are already discussed before. We only discuss proof for part (3).

For proving the isomorphism of class groups, note that the class group $C\ell(K)$ of a number field K is in the adelic notation, $K^\times \backslash \mathbb{A}_K^\times / [K_\infty^\times \cdot \prod_v \mathcal{O}_v^\times]$. Since the topological isomorphism between $\mathbb{A}_{K_1}^\times$ and $\mathbb{A}_{K_2}^\times$ constructed in this paper takes $K_{1,\infty}^\times$ isomorphically to $K_{2,\infty}^\times$, and must take the maximal compact subgroup of $\mathbb{A}_{K_1}^\times$ to the maximal compact subgroup of $\mathbb{A}_{K_2}^\times$, therefore takes $K_{1,\infty}^\times \cdot \prod_v \mathcal{O}_{1,v}^\times$ isomorphically to $K_{1,\infty}^\times \cdot \prod_v \mathcal{O}_{2,v}^\times$. It follows that the class group of K_1 is isomorphic to the class group of K_2; the assertion on the class group of $K_1 \otimes L$ follows similarly. (The result on isomorphism of class groups also follows from Perlis [8].) □

The refined Gassmann triple $(\mathrm{PSL}_2(\mathbb{F}_{29}), A_5, A_5)$ provided by Scott in Theorem 1 when combined with construction of number fields due to Shih [11] and Zywina [15] with Galois group $\mathrm{PSL}_2(\mathbb{F}_{29})$ allows one to construct examples of number fields which have remarkably similar properties without being isomorphic.

Theorem 3. *There are number fields K_1 and K_2 of degree $\frac{|\mathrm{PSL}_2(\mathbb{F}_{29})|}{|A_5|} = 203$ over $\mathbb{Q}$ which lie in the same Galois extension K of $\mathbb{Q}$ with Galois group $G = \mathrm{PSL}_2(\mathbb{F}_{29})$ which are not isomorphic as fields, but have:*

(1) $\zeta_{K_1} = \zeta_{K_2}$.
(2) $\mathbb{A}_{K_1} \cong \mathbb{A}_{K_2}$ *as topological rings, as well as $\mathbb{A}_{\mathbb{Q}}$-algebras.*
(3) $\mathbb{A}_{K_1}^\times \cong \mathbb{A}_{K_2}^\times$ *as topological groups with an isomorphism taking $K_1^\times$ to $K_2^\times$, and therefore, inducing an isomorphism of the idele class groups:*

$$C_{K_1} = \mathbb{A}_{K_1}^\times / K_1^\times \xrightarrow{\cong} \mathbb{A}_{K_2}^\times / K_2^\times = C_{K_2},$$

as well as for all number fields L, a (compatible family of) isomorphisms of the idele class groups:

$$C_{K_1 \otimes L} = \mathbb{A}_{K_1 \otimes L}^\times / (K_1 \otimes L)^\times \xrightarrow{\cong} \mathbb{A}_{K_2 \otimes L}^\times / (K_2 \otimes L)^\times = C_{K_2 \otimes L}.$$

(4) *If $C\ell(K)$ is the class group of a number field K, then $C\ell(K_1) \cong C\ell(K_2)$, as well as compatible isomorphisms $C\ell(K_1 \otimes L) \cong C\ell(K_2 \otimes L)$ for all number fields L.*
(5) $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_1) \cong \mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/K_2)$ *as profinite groups; further,* $\mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/LK_1) \cong \mathrm{Gal}^{ab}(\bar{\mathbb{Q}}/LK_2)$ *as profinite groups for all number fields L which are disjoint from K so that $LK_1 = L \otimes K_1$ and $LK_2 = L \otimes K_2$ are number fields contained in $\bar{\mathbb{Q}}$.*

Proof. The existence of a number field K with Galois group $G = \mathrm{PSL}_2(\mathbb{F}_p)$ for any prime p is due to Zywina, cf. [15]; for us, the earlier work of Shih [11] suffices for $\mathrm{PSL}_2(\mathbb{F}_{29})$, and in fact gives the stronger conclusion of constructing infinitely many linearly disjoint number fields with this as the Galois group. We take K_1 and K_2 to be fixed fields of two copies of A_5 inside $G = \mathrm{PSL}_2(\mathbb{F}_{29})$ which are non-conjugate, but are conjugate by $G = \mathrm{PGL}_2(\mathbb{F}_{29})$. By Theorem 1 due to Scott $(\mathrm{PSL}_2(\mathbb{F}_{29}), A_5, A_5)$ is a refined Gassmann triple, so Theorem 2 applies, and as a result, we need to discuss proof for only part (2) of this theorem which is the only extra conclusion in this theorem compared to the last one.

It is well-known that the structure of the algebra $K_1 \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is dictated by the structure of the coset space G/H_1 as a $D_\wp$-set, where $D_\wp$ is the decomposition subgroup of G at a prime $\wp$ of K. Since $D_\wp$ is a solvable group, by Lemma 1, G/H_1 and G/H_2 are isomorphic as $D_\wp$-sets, therefore the algebras $K_1 \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $K_1 \otimes_{\mathbb{Q}} \mathbb{Q}_p$ are isomorphic (for all places p of $\mathbb{Q}$ including infinity), proving part (2) of the theorem. $\square$

Remark 2. We do not know if arithmetically equivalent number fields K_1 and K_2 arising out of refined Gassmann triples have isomorphic adelic spaces $\mathbb{A}_{K_1} \cong \mathbb{A}_{K_2}$ as topological rings, generalizing the previous theorem for the triple $(\mathrm{PSL}_2(\mathbb{F}_{29}), A_5, A_5)$. It may be remarked here that we do not need to check Lemma 1 for *all* solvable subgroups of G, but only for those subgroups which arise as the Galois group of a local field, and as in the proof of Lemma 1, if we know that all decomposition groups of local fields (as subgroups of G) are extensions of p-groups by cyclic groups (for some prime p) — a condition which is vacuously satisfied if G itself is of this form — then $\mathbb{A}_{K_1} \cong \mathbb{A}_{K_2}$ as topological rings.

Remark 3. The isomorphism between the idele class groups $\mathbb{A}^\times_{K_1}/K_1^\times$ and $\mathbb{A}^\times_{K_2}/K_2^\times$ allows us to define a natural identification of the Grössencharacters on K_1 with that on K_2 (depending on an isomorphism of integral representations $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$). However, the resulting identification $\chi_1 \longleftrightarrow \chi_2$ between Grössencharacters on K_1 with that on K_2 does *not* have the property that

$$L(\chi_1, s) = L(\chi_2, s),$$

which is the case if the isomorphism of $\mathbb{A}^\times_{K_1}/K_1^\times$ with $\mathbb{A}^\times_{K_2}/K_2^\times$ came from a field isomorphism $K_1 \to K_2$. This motivates one to ask: if for two number fields K_1 and K_2, if the set of abelian L-functions $L(\chi_1, s)$ for Grössencharacters χ_1 on K_1 (as holomorphic functions of s) is the same as the set of abelian L-functions $L(\chi_2, s)$ for Grössencharacters χ_2 on K_2, are K_1 and K_2 isomorphic? (The case of $\chi_1 = \chi_2 = 1$, gives $\zeta_{K_1}(s) = \zeta_{K_2}(s)$, so at least some Grössencharacters can give rise to the same L-function!)

1. Isomorphism of Jacobians

Theorem 4. *Let $p : X \to Y$ be a Galois cover (not necessarily unramified) of geometrically irreducible, smooth and projective algebraic curves over a field k with Galois group G.*

Let H_1 and H_2 be two subgroups of G such that the integral representations $\mathbb{Z}[G/H_1]$ and $\mathbb{Z}[G/H_2]$ of G are isomorphic. Define curves X_1 and X_2 over k such that their function fields are the H_1 and H_2 invariants of the function field of X. Then the Jacobian of X_1 is isomorphic to the Jacobian of X_2 as abelian varieties over k.

Proof. Note the commutative diagram of algebraic curves:

$$\begin{tikzcd} & X \arrow[dl, "p_1"'] \arrow[dr, "p_2"] & \\ X_1 \arrow[dr, "q_1"'] & & X_2 \arrow[dl, "q_2"] \\ & Y. & \end{tikzcd}$$

For any geometrically irreducible, smooth and projective algebraic curve C over k, let $\mathrm{Div}(C)$ denote the group of divisors on C, $\mathrm{Div}^0(C)$ group of divisors of degree zero, and $J(C)$ the Jacobian variety of C over k. The proof of the theorem depends on constructing a natural homomorphism $[H_2gH_1] : J(X_1) \longrightarrow J(X_2)$ for each element of the double coset $H_2\backslash G/H_1$. This is a very classical topic, and is related to the action of Hecke algebras on various cohomology theories. We refer to the book of Shimura [12] for a general treatment. For the convenience of the reader, we give two ways of looking at these in the present context.

Let $H_2gH_1 = \amalg_{k=1}^m g_kH_1$, a disjoint union. Define a map,

$$[H_2gH_1] : \mathrm{Div}(X_1) \longrightarrow \mathrm{Div}(X_2),$$

as follows. For $x \in X_1$, let $[H_2gH_1](x)$ be the divisor on X_2 for which,

$$p_2^\star[H_2gH_1](x) = \sum_{k=1}^m g_k p_1^\star(x).$$

Note that the right hand side is well-defined, i.e., independent of the representatives g_k chosen, and $\sum_{k=1}^m g_k p_1^\star(x)$ belongs to $p_2^\star\mathrm{Div}(X_2) \subset \mathrm{Div}(X)$. Extend the definition of $[H_2gH_1]$ linearly to all divisors on X_1. Clearly, $[H_2gH_1]$ maps divisors on X_1 of degree zero to divisors on X_2 of degree zero. If f is a function on X_1, then $\prod_{k=1}^m g_k(f)$ is a function on X_2, and

$$[H_2gH_1](\mathrm{div}_{X_1}(f)) = \mathrm{div}_{X_2}(\prod_{k=1}^m g_k(f)),$$

so, $[H_2gH_1]$ induces a homomorphism from $J(X_1)$ to $J(X_2)$, which is known to be algebraic.

The homomorphism $[H_2gH_1] : J(X_1) \longrightarrow J(X_2)$ can also be interpreted by using covariant and contravariant nature of the Jacobian. For this, define $H' = H_2 \cap g^{-1}H_1g$, X' the quotient of X by H', and construct the correspondence,

$$\begin{tikzcd} & X' \arrow[dl, "p_1'"'] \arrow[dr, "p_2'"] & \\ X_1 & & X_2, \end{tikzcd}$$

where p_2' is the natural map from X' to X_2 (since $H' \subset H_2$), and p_1' is the map $x \mapsto gx$ on X which descends to give a map from X' to X_1. The homomorphism $[H_2gH_1]$ from $J(X_1)$ to $J(X_2)$ is in this notation nothing but $p'_{2\star} \circ p_1'^{\star}$. (Here for a morphism $\phi : C_1 \to C_2$ of curves, $\phi_\star : J(C_1) \to J(C_2)$ and $\phi^\star : J(C_2) \to J(C_1)$ are the standard maps on the Jacobians.)

The following Lemma is standard, see for example, Proposition 7.1 of [12].

Lemma 2. *The natural homomorphism from* $\mathrm{Hom}_G(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$ *to* $\mathrm{Hom}(J(X_2), J(X_1))$, *which sends a homomorphism* $\phi : \mathrm{Hom}_G(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$ *represented by* $\phi(1) = \sum_i n_iH_1g_iH_2 \in \mathbb{Z}[H_1\backslash G/H_2]$ *to the homomorphism* $\sum_i n_i[H_1g_iH_2]$ *from* $J(X_2)$ *to* $J(X_1)$ *(constructed above) has the property that for any subgroup* H_3 *of* G *with corresponding algebraic curve* X_3*, the natural composition of* G*-homomorphisms:*

$$\mathbb{Z}[G/H_1] \longrightarrow \mathbb{Z}[G/H_2] \longrightarrow \mathbb{Z}[G/H_3],$$

corresponds to composition of the corresponding maps on the Jacobian:

$$J(X_1) \longleftarrow J(X_2) \longleftarrow J(X_3).$$

It follows from the lemma that if a G-homomorphism $\mathbb{Z}[G/H_1] \longrightarrow \mathbb{Z}[G/H_2]$ is an isomorphism, the corresponding mapping from $J(X_2)$ to $J(X_1)$ is an isomorphism, completing the proof of the theorem. $\square$

Remark 4. It requires some care to prove that the curves X_1 and X_2 in the previous theorem (arising from subgroups H_1 and H_2 of G which are not conjugate in G), are non-isomorphic over k in some situations. By their construction, there is no isomorphism from X_1 to X_2 making the following diagram commute

$$\begin{tikzcd} X_1 \arrow[rr] \arrow[dr, "q_1"'] & & X_2 \arrow[dl, "q_2"] \\ & Y, & \end{tikzcd}$$

but how do we ensure that there is no isomorphism at all between X_1 and X_2 over k?

For $k = \mathbb{C}$, Sunada in [13] ensures that there is no isomorphism at all between X_1 and X_2 over $\mathbb{C}$ using transcendental methods by appealing to the existence of a curve Y which is uniformized by a discrete subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ whose commensurator in $\mathrm{PSL}_2(\mathbb{R})$ is Γ. This uses a theorem of Margulis, according to which for non-arithmetic discrete groups Γ, the commensurator of Γ contains Γ as a subgroup of finite index, and a theorem of L. Greenberg according to which most discrete subgroups giving rise to a compact Riemann surface of genus $g > 2$ are maximal. This then gives examples of non-isomorphic curves X_1 and X_2 of genus $g(X_1) = g(X_2)$ with isomorphic Jacobians for example for $2g(X_i) - 2 = 203(2g(Y) - 2)$ with $g(Y) > 2$ any integer (using the example of Scott earlier in the paper for any unramified Galois cover of Y with Galois group $G = \mathrm{PSL}_2(\mathbb{F}_{29})$, which is possible for $g(Y) \geq 2$).

It is not clear if these transcendental methods can be replaced by more algebraic ones so that they work for $k = \bar{\mathbb{F}}_p$, or $k = \bar{\mathbb{Q}}$.

Remark 5. Theorem 3 for refined Gassmann triple improves upon corollary 4 of [9] where it was proved that $J(X_1)$ and $J(X_2)$ are isogenous for Gassmann triples.

Question 2. We end the paper by remarking that many constructions of isospectral varieties are related to the Gassmann triples (G, H_1, H_2), e.g., see the pioneering work of Sunada [13]. What extra information does being refined Gassmann triple give in such a context? Gassmann triples give rise to varieties which have isomorphic cohomology with rational coefficients, and an obvious extra information supplied by being a refined Gassmann triple is to have isomorphic cohomology with integral coefficients.

Acknowledgments

The author thanks Maneesh Thakur for asking a question which started it all: if an isomorphism of tori $K_1^\times$ with $K_2^\times$ (where K_1, K_2 are finite extensions of a field k) comes from an isomorphism of fields K_1 and K_2. The corresponding question on integral representations was answered in successive approximation by Bart de Smit, Wolfgang Kimmerle, and finally by Leonard Scott who had the counter-example. I am thankful to them all. I thank the referee of this paper for a careful reading and many nice suggestions. This paper is based upon work supported by the National Science Foundation under grant No. 0932078000 while the author was in residence at the MSRI, Berkeley during the Fall semester of 2014.

References

[1] A. Angelakis, P. Stevenhagen, Imaginary quadratic fields with isomorphic abelian Galois groups, in: ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium, in: Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 21–39.

[2] C. Ciliberto, G. van der Geer, Non-isomorphic curves of genus four with isomorphic (non-polarized) Jacobians, in: Classification of Algebraic Varieties, in: Contemp. Math. AMS, vol. 162, 1994, pp. 129–133.

[3] C.W. Curtis, Modular representations of finite groups with split (B, N)-pairs, in: Seminar on Algebraic Groups and Related Finite Groups, The Institute for Advanced Study, Princeton, NJ, 1968/69, in: Lecture Notes in Math., vol. 131, Springer, 1970, pp. 57–95.
[4] B. de Smit, R. Perlis, Zeta functions do not determine class numbers, Bull. Amer. Math. Soc. (N.S.) 31 (2) (1994) 213–215.
[5] E. Howe, Infinite families of pairs of curves over $\mathbb{Q}$ with isomorphic Jacobians, J. Lond. Math. Soc. 72 (2005) 327–350.
[6] N. Klingen, Arithmetical Similarities, Oxford Science Publications, 1998.
[7] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory 9 (3) (1977) 342–360.
[8] R. Perlis, On the class numbers of arithmetically equivalent fields, J. Number Theory 10 (4) (1978) 489–509.
[9] D. Prasad, C.S. Rajan, On an Archimedean analogue of Tate's conjecture, J. Number Theory 99 (2003) 180–184.
[10] L.L. Scott, Integral equivalence of permutation representations, in: Group Theory, Granville, OH, 1992, World Sci. Publ., River Edge, NJ, 1993, pp. 262–274.
[11] K.-Y. Shih, On the construction of Galois extensions of function fields and number fields, Math. Ann. 207 (1974) 99–120.
[12] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, 1971.
[13] T. Sunada, Riemannian coverings and isospectral manifolds, Ann. of Math. 121 (1985) 169–186.
[14] A.V. Sutherland, Computing images of Galois representations attached to elliptic curves, Forum Math. Sigma 4 (2016).
[15] D. Zywina, The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$, Duke Math. J. 164 (12) (2015) 2253–2292.