Stronger arithmetic equivalence

Andrew V. Sutherland*

Abstract: Motivated by a recent result of Prasad, we consider three stronger notions of arithmetic equivalence: *local integral equivalence*, *integral equivalence*, and *solvable equivalence*. In addition to having the same Dedekind zeta function (the usual notion of arithmetic equivalence), number fields that are equivalent in any of these stronger senses must have the same class number, and solvable equivalence forces an isomorphism of adele rings. Until recently the only nontrivial example of integral and solvable equivalence arose from a group-theoretic construction of Scott that was exploited by Prasad. Here we provide infinitely many distinct examples of solvable equivalence, including a family that contains Scott's construction as well as an explicit example of degree 96. We also construct examples that address questions of Scott, and of Guralnick and Weiss, and shed some light on a question of Prasad.

1 Introduction

Number fields that have the same Dedekind zeta function are said to be *arithmetically equivalent*. Arithmetically equivalent number fields need not be isomorphic, but they necessarily have the same normal closure and share many arithmetic invariants. The first nontrivial example of arithmetically equivalent number fields was given by Gassmann [15], who showed that all such examples arise from a simple group-theoretic construction, a *Gassmann triple* (G, H_1, H_2) of finite groups in which H_1 and H_2 are subgroups of G that intersect every G-conjugacy class with the same cardinality; see Proposition 2.6 for several equivalent definitions. Gassmann proved that number fields K_1, K_2 with Galois closure L are arithmetically equivalent if and only if $(\mathrm{Gal}(L/\mathbf{Q}), \mathrm{Gal}(L/K_1), \mathrm{Gal}(L/K_2))$ is a Gassmann triple. The number fields K_1 and K_2 are isomorphic if and only if $\mathrm{Gal}(L/K_1)$ and $\mathrm{Gal}(L/K_2)$ are conjugate in

ANDREW V. SUTHERLAND

$\mathrm{Gal}(L/\mathbf{Q})$; we are thus interested in *nontrivial Gassmann triples* (G, H_1, H_2), those in which H_1 and H_2 are nonconjugate subgroups of G.

Gassmann triples (G, H_1, H_2) naturally arise in many other settings, most notably in the construction of isospectral manifolds. As shown by Sunada [47], if $\pi \colon M \to M_0$ is a normal finite Riemannian covering with transformation group G, the quotient manifolds M/H_1 and M/H_2 are *isospectral*: they have the same sequence of Laplacian eigenvalues. Unlike the number field case, M_1 and M_2 may be isometric even when H_1 and H_2 are nonconjugate, but if H_1 and H_2 are nonisomorphic and M is the universal covering of M_0, then M/H_1 and M/H_2 have nonisomorphic fundamental groups H_1 and H_2 and cannot be isometric; see [44, §4.2] and [47, Corollary 1]. A consequence of this result is that there are infinitely many distinct ways in which one cannot "hear the shape of a drum" [16, 23, 33]. A similar result holds in algebraic geometry: if X is a projective curve over a number field K and (G, H_1, H_2) is a Gassmann triple with $G \subseteq \mathrm{Aut}(X)$, then the Jacobians of the quotient curves X/H_1 and X/H_2 are isogenous over K, as proved by Prasad and Rajan in [39]. As shown in [1], this result can be generalized to étale Galois covers of K-varieties. There is also a discrete analog to Sunada's theorem in which one considers a finite graph Γ with automorphism group G: Gassmann triples (G, H_1, H_2) can be used to construct nonisomorphic isospectral graphs Γ/H_1 and Γ/H_2, subject to conditions on H_1 and H_2; see [19]. An introduction to the topics of arithmetic equivalence and isospectrality can be found in [49].

Subgroups H_1, H_2 of G form a Gassmann triple (G, H_1, H_2) if and only if the permutation modules $\mathbf{Q}[H_1 \backslash G]$ and $\mathbf{Q}[H_2 \backslash G]$ given by the G-action on right cosets are isomorphic as $\mathbf{Q}[G]$-modules. We then say that H_1 and H_2 are *rationally equivalent*, and if $\mathbf{Z}[H_1 \backslash G]$ and $\mathbf{Z}[H_2 \backslash G]$ are isomorphic as $\mathbf{Z}[G]$-modules, we say that H_1 and H_2 are *integrally equivalent*. Prasad calls (G, H_1, H_2) a *refined Gassmann triple* when $H_1, H_2 \leq G$ are integrally equivalent, and shows that if G is the Galois group of a Galois number field $L/\mathbf{Q}$ then the fixed fields $K_1 := L^{H_1}$ and $L_2 := K_2^{H_2}$ not only have the same Dedekind zeta function, they must also have isomorphic idele groups (and in particular, isomorphic class groups); see [38, Theorem 2]. The first (and so far only) nontrivial example of a refined Gassmann triple was constructed by Scott [42] more than thirty years ago. Prasad notes that this example can be realized by number fields, and that such number fields not only have the same Dedekind zeta function and isomorphic idele groups, they have isomorphic rings of adeles [38, Theorem 3], and are thus *locally isomorphic*, meaning their local algebras are isomorphic at every place (see Theorem 2.16). Thus even when taken in aggregate these invariants are not enough to guarantee an isomorphism of number fields.[1]

As noted by Prasad, Scott's example is essentially the only nontrivial example of integral equivalence currently known [38, Remark 1]. It is not clear whether the particular feature of Scott's refined Gassmann triple that allowed Prasad to prove an isomorphism of adele rings is necessarily enjoyed by others (assuming there are any). Whether Scott's example is a singular special case or just the most accessible example of a general phenomenon remains an open question.

In this article we consider two alternative strengthenings of the notion of arithmetic equivalence: *local integral equivalence* and *solvable equivalence*. The latter implies the former and is sufficient to prove equality of the number field invariants considered by Prasad, notably including local isomorphism, which is not obviously implied by integral equivalence (indeed, we show that it is not implied by the similar but weaker notion of local integral equivalence).

---

[1]One can attach auxiliary L-functions to a number field that in combination with the Dedekind zeta function ensure an isomorphism of number fields whenever all of these L-functions coincide [9, 46]; for function fields see [4, 8, 45].

An attractive feature of both local integral equivalence and solvable equivalence is that they are much easier conditions to check than integral equivalence; see Propositions 2.2 and 3.1, and Definition 3.5. In this article we provide infinitely many nontrivial examples of solvably equivalent triples (G, H_1, H_2) that can be realized as Galois groups of number fields (see Theorem 3.9), and we prove that

- locally integrally equivalent subgroups need not be isomorphic (see §4.1);
- locally integrally equivalent number fields need not be locally isomorphic (see §4.2);
- locally integrally equivalent subgroups need not be integrally equivalent (see §4.3);
- solvably equivalent subgroups need not be integrally equivalent (see §4.4).

We construct an explicit example of locally integrally equivalent number fields of degree 32 arising from a triple (G, H_1, H_2) with $H_1 \not\simeq H_2$, and an explicit example of solvably equivalent number fields of degree 96 that are not integrally equivalent. Thus solvable equivalence does not imply integral equivalence; we leave open the question of whether integral equivalence implies solvable equivalence.

The example in §4.1 negatively answers a question of Guralnick and Weiss [18, Question 2.11] and is relevant to the question of Prasad [38, Question 1] as to whether integrally equivalent subgroups must be isomorphic, since it shows that locally integrally equivalent subgroups need not be. The solvably equivalent subgroups we construct are all isomorphic, which leads to the question of whether solvably equivalent subgroups are necessarily isomorphic. This question is perhaps more accessible than Prasad's question, since the only example of integral equivalence currently known arises in a setting where rational equivalence is already enough to force isomorphism (rationally equivalent subgroups of $\mathbf{GL}_2(\mathbf{F}_p)$, $\mathbf{SL}_2(\mathbf{F}_p)$, $\mathbf{PSL}_2(\mathbf{F}_p)$ must be isomorphic, see [38, Question 1] and [48, Remark 3.7]). The example of solvable equivalence given in §4.4 does not arise in this setting, and one can find many others.

The example in §4.2 refines an answer to a question of Stuart and Perlis [37, §4] given by Mantilla-Soler [30, Theorem 3.7] by showing that the sum of the ramification indices above a given prime in arithmetically equivalent number fields need not coincide even when their products do (as they must for number fields that are locally integrally equivalent; see Proposition 3.1).

The examples in §4.3, §4.4 negatively answer a question of Guralnick and Weiss [18, Question 2.10] as to whether local integral equivalence implies integral equivalence (this question appears to have also been addressed in the thesis of D. Hahn in the case of solvable groups [40]). The example in §4.4 also addresses a question of Scott [42, Remark 4.3] regarding low rank permutation modules.

2   Background and preparation

In this section we recall background material, set notation, and summarize some of the results we will use. The material in this section is well known to experts, but we provide short proofs in cases where we were unable to find a suitable reference (a few of these results seem to be folklore).

Let G be a finite group. For each subgroup $H \leq G$ we use $[H \backslash G]$ to denote the transitive G-set given by the (right) action of G on (right) cosets of H; this action is faithful if and only if the intersection of all the G-conjugates of H (its *normal core* in G) is the trivial group. We use $\chi_H \colon G \to \mathbf{Z}$ to denote the permutation character $g \mapsto \#[H \backslash G]^g$ that sends g to the number of H-cosets it fixes (the induced character 1_H^G), and note that $\chi_H(g) \neq 0$ if and only if g is conjugate to an element of H.

We extend χ_H to subgroups K of G by defining $\chi_H(K) := \#[H\backslash G]^K$ (the *mark* of K on $[H\backslash G]$), so that $\chi_H(\langle g\rangle) = \chi_H(g)$; equivalently, $\chi_H(K)$ is the number of singleton fibers in the map $[H\backslash G] \to [H\backslash G/K]$ defined by $Hg \mapsto HgK$. For $g \in G$ we have $HgK = Hg$ if and only if $gKg^{-1} \subseteq H$, and it follows that

$$\chi_H(K) = \frac{\#\{g \in G : gKg^{-1} \leq H\}}{\#H} = \frac{\#N_G(K)}{\#H}\#\{gKg^{-1} \leq H : g \in G\}, \tag{2.1}$$

where $N_G(K)$ denotes the normalizer of K in G.

Lemma 2.1. *Let H and K be subgroups of a finite group G. The integer $\chi_H(K)$ depends only on the G-conjugacy classes of H and K and the function χ_H depends only on the G-conjugacy class of H.*

Proof. Replacing either H or K with a G-conjugate does not change the RHS of (2.1). ☐

If $\mathcal{P}$ is a class of groups (e.g. cyclic groups or solvable groups), we call its elements $\mathcal{P}$-*groups*, and refer to the subgroups of a group G that lie in $\mathcal{P}$ as its $\mathcal{P}$-*subgroups*. We say that $\mathcal{P}$ is *subgroup-closed* if it contains all subgroups of its elements. A function that maps subgroups of G to subgroups of G is *G-class preserving* if it maps subgroups to G-conjugates.

Proposition 2.2. *Let G be a finite group and let $\mathcal{P}$ be a subgroup-closed class of groups. For any two subgroups $H_1, H_2 \leq G$ the following are equivalent:*

(i) *There is G-class preserving bijection between the sets of $\mathcal{P}$-subgroups of H_1 and H_2;*

(ii) $\#\{gKg^{-1} \leq H_1 : g \in G\} = \#\{gKg^{-1} \leq H_2 : g \in G\}$ *for every $\mathcal{P}$-subgroup K of G;*

(iii) $\chi_{H_1}(K) = \chi_{H_2}(K)$ *for every $\mathcal{P}$-subgroup K of G;*

(iv) $\chi_{H_1}(K) = \chi_{H_2}(K)$ *for every $\mathcal{P}$-subgroup K of H_1 or H_2;*

(v) *the G-sets $[H_1\backslash G]$ and $[H_2\backslash G]$ are isomorphic as K-sets for every $\mathcal{P}$-subgroup K of G.*

(vi) *the G-sets $[H_1\backslash G]$ and $[H_2\backslash G]$ are isomorphic as K-sets for every $\mathcal{P}$-subgroup K of H_1 or H_1.*

Proof. (i) $\Leftrightarrow$ (ii) is immediate, (ii) $\Leftrightarrow$ (iii) follows from (2.1), (iii) $\Leftrightarrow$ (iv) follows from the fact that $\chi_{H_i}(K) = 0$ if K is not conjugate to a subgroup of H_i, and the implications (v) $\Rightarrow$ (vi) $\Rightarrow$ (iv) are clear; it thus suffices to show (iii) $\Rightarrow$ (v).

Let K be a $\mathcal{P}$-group and consider the K-sets $X_1 := [H_1\backslash G]$ and $X_2 = [H_2\backslash G]$. We have $\chi_{H_1}(k) = \chi_{H_2}(k)$ for all $k \in K$, thus $\#X_1 = \chi_{H_i}(1) = \#X_2$, and X_1 and X_2 both have $\frac{1}{\#K}\sum_k \chi_{H_i}(k)$ orbits. The stabilizer $H \leq K$ of any element x in a K-orbit X of X_1 or X_2 is a $\mathcal{P}$-group, and $\chi_{H_1}(H) = \chi_{H_2}(H)$ implies that the K-orbits of X_1 and X_2 can be put in a bijection that preserves conjugacy classes of stabilizers (and thus preserves cardinalities). If H is the stabilizer of an element of a K-orbit X in X_1 or X_2, then X is isomorphic to the K-set $[H\backslash K]$. It follows that X_1 and X_2 are isomorphic K-sets. ☐

We call subgroups $H_1, H_2 \leq G$ that satisfy the equivalent properties of Proposition 2.2 $\mathcal{P}$-*equivalent*, and this defines an equivalence relation on the subgroups of G. A necessary condition for $\mathcal{P}$-equivalence is that H_1 and H_2 must have the same $\mathcal{P}$-*statistics*, meaning that they contain the same number of $\mathcal{P}$-subgroups in every isomorphism class of groups. When $\mathcal{P}$ is the class of cyclic groups this amounts to having the same *order statistics* (numbers of elements of each order).

Remark 2.3. Condition (iv) of Proposition 2.2 provides an efficient method for testing whether two subgroups of G are $\mathcal{P}$-equivalent. Conditions (ii) and (iii) can both be used to efficiently partition the set of subgroups of G into $\mathcal{P}$-equivalence classes without the need for pairwise testing; conjugate subgroups lie in the same equivalence class, so it suffices to work with a set of conjugacy class representatives.

Lemma 2.4. *Let K, H_1, H_2 be finite groups with $|H_1| = |H_2| = n$, let $\phi_1 \colon K \to H_1$ and $\phi_2 \colon K \to H_2$ be injective group homomorphisms, and let $\rho_1 \colon H_1 \to S_n$ and $\rho_2 \colon H_2 \to S_n$ be left regular representations of H_1 and H_2. Then $K_1 := \rho_1(\phi_1(H_0))$ and $K_2 := \rho_2(\phi_2(H_0))$ are conjugate subgroups of S_n.*

Proof. The K-sets $X_1 = X_2 = \{1, \ldots, n\}$ given by the actions of $K_1 := \rho_1(\phi_1(H_0))$ and $K_2 := \rho_2(\phi_2(H_0))$ are free K-sets with the same number of orbits, hence isomorphic. There is thus a K-equivariant map $\sigma \colon X_1 \to X_2$ with $\sigma \in S_n$ satisfying $\rho_1(\phi_1(k))\sigma = \sigma \rho_2(\phi_2(k))$ for $k \in K$, and $\sigma^{-1} K_1 \sigma = K_2$. □

Corollary 2.5. *Let $\mathcal{P}$ be a subgroup-closed class of groups. Finite groups H_1 and H_2 of the same order can be embedded as $\mathcal{P}$-equivalent subgroups of some group G if and only if they have the same $\mathcal{P}$-statistics.*

Proof. The necessity of having the same $\mathcal{P}$-statistics is obvious, and Lemma 2.4 proves sufficiency. □

For any integral domain R, we use $R[H \backslash G]$ to denote the corresponding permutation module; this is the free R-module with basis $[H \backslash G]$ equipped with the R-linear extension of the G-action on $[H \backslash G]$; we thus view $R[H \backslash G]$ as a (right) $R[G]$-module.

If $H_1, H_2 \le G$ have the same index n, after ordering the G-sets $[H_1 \backslash G]$ and $[H_2 \backslash G]$, we may uniquely identify each $R[G]$-module homomorphism $R[H_1 \backslash G] \to R[H_2 \backslash G]$ with a matrix $M \in R^{n \times n}$ whose determinant $\det M$ does not depend on our choices. If $\rho_1, \rho_2 \colon G \to S_n$ are the permutation representations of G acting on $\{1, \ldots, n\}$ via our chosen orderings of $[H_1 \backslash G]$ and $[H_2 \backslash G]$, respectively, then the matrices $M \in R^{n \times n}$ that correspond to elements of $\operatorname{Hom}_{R[G]}(R[H_1 \backslash G], R[H_2 \backslash G])$ are precisely those that are fixed by the diagonal action of $\rho_1 \times \rho_2$ on matrix entries; in other words, the entries of M must satisfy

$$M_{ij} = M_{\rho_1(g)(i), \rho_2(g)(j)} \qquad \text{(for all } g \in G).$$

We define

$$d(H_1, H_2) := \gcd\left\{ \det M : M \in \operatorname{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G]) \right\},$$

and extend this definition to all subgroups of G by defining $d(H_1, H_2) = 0$ whenever $\#H_1 \ne \#H_2$.

We now give several equivalent conditions for subgroups to be $\mathcal{P}$-equivalent when $\mathcal{P}$ is the class of cyclic groups.

Proposition 2.6. *Let G be a finite group. For all subgroups H_1 and H_2 of G the following are equivalent:*

(i) *There is a bijection of sets $H_1 \leftrightarrow H_2$ that preserves G-conjugacy;*

(ii) *$\#(H_1 \cap C) = \#(H_2 \cap C)$ for every conjugacy class C of G;*

(iii) *$\chi_{H_1}(K) = \chi_{H_2}(K)$ for every cyclic $K \le G$;*

(iv) *The G-sets $[H_1 \backslash G]$ and $[H_2 \backslash G]$ are isomorphic as K-sets for every cyclic $K \le G$;*

(v) *$\mathbf{Q}[H_1 \backslash G] \simeq \mathbf{Q}[H_2 \backslash G]$;*

(vi) *$d(H_1, H_2) \ne 0$.*

Proof. The equivalence of (i) and (ii) is immediate. The equivalence of (ii) and (iii) follows from the formula $\chi_{H_i}(g)\#H_i = \#(H_i \cap C(g))\#Z(g)$, where $C(g)$ is the conjugacy class of g and $Z(g)$ is its centralizer (in G); see [36, Eq. 8]. The equivalence of (iii) and (iv) follows from applying Proposition 2.2 to the class of cyclic groups. For the equivalence of (iii) and (v), note that $\dim_{\mathbf{Q}}(\mathbf{Q}[H_i \backslash G]^K) = \chi_{H_i}(K)$ for cyclic $K \leq G$ and then apply the corollary to [43, Theorem 30]. Clearing the denominators in $M \in \mathrm{Hom}_{\mathbf{Q}[G]}(\mathbf{Q}[H_1 \backslash G], \mathbf{Q}[H_2 \backslash G])$ shows the equivalence of (v) and (vi). $\qquad\square$

Remark 2.7. The condition $K \leq G$ in (iii), (iv) can be replaced by "$K \leq H_1$ or $K \leq H_2$" via Lemma 2.2.

Definition 2.8. Subgroups H_1 and H_2 of a finite group G that satisfy the equivalent conditions of Proposition 2.6 are said to be *rationally equivalent* (or *Gassmann equivalent*).

A triple of groups (G, H_1, H_2) with $H_1, H_2 \leq G$ rationally equivalent is called a *Gassmann triple* [15]. By Proposition 2.6, rational equivalence defines an equivalence relation on the subgroups of G. Conjugate subgroups of G are necessarily rational equivalent, so we may view this as an equivalence relation on conjugacy classes of subgroups. Rational equivalence classes may be arbitrarily large [27].

We are interested in the nontrivial rational equivalence classes, those which contain nonconjugate but rationally equivalent subgroups $H_1, H_2 \leq G$. Equivalently, we are interested in the cases where $[H_1 \backslash G] \not\simeq [H_2 \backslash G]$ as G-sets, but $\mathbf{Q}[H_1 \backslash G] \simeq \mathbf{Q}[H_2 \backslash G]$ as $G[\mathbf{Q}]$-modules. Standard examples include the subgroups $H_1 := \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \in \mathbf{GL}_2(\mathbf{F}_p) \right\}$ and $H_2 := \left\{ \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix} \in \mathbf{GL}_2(\mathbf{F}_p) \right\}$ of $G := \mathbf{GL}_2(\mathbf{F}_p)$, where p is an odd prime [11], and similar examples in $\mathbf{GL}_n(\mathbf{F}_p)$ for $n > 2$ and any prime p. In these examples the subgroups H_1 and H_2 are not G-conjugate, but transposition gives a bijection $H_1 \leftrightarrow H_2$ that preserves G-conjugacy. The smallest example occurs for the group G with GAP identifier $\langle 32, 43 \rangle$, which contains two nonconjugate rationally equivalent subgroups H_1 and H_2 isomorphic to the Klein 4-group.[2]

Remark 2.9. Rationally equivalent subgroups necessarily have the same order but need not be isomorphic. The smallest example of a Gassmann triple (G, H_1, H_2) with $H_1 \not\simeq H_2$ arises for $G \simeq \langle 384, 5755 \rangle$ with subgroups $H_1 \simeq \langle 16, 3 \rangle$ and $H_2 \simeq \langle 16, 10 \rangle$. The groups H_1 and H_2 are the first of infinitely many pairs of nonisomorphic groups with the same order statistics (one can take $(\mathbf{Z}/p\mathbf{Z})^3$ and the Heisenberg group $H_3(\mathbf{F}_p)$ for any prime p, for example). Corollary 2.5 implies that all such pairs H_1 and H_2 can be realized as part of a Gassmann triple (G, H_1, H_2).

The original motivation for studying rational equivalence stems from its relationship to zeta functions of number fields. Recall that the *Dedekind zeta function* of a number field K is defined by

$$\zeta_K(z) := \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-z})^{-1},$$

where $\mathfrak{p}$ varies over primes of K (nonzero prime ideals of its ring of integers $\mathcal{O}_K$) and $N(\mathfrak{p}) := [\mathcal{O}_K : \mathfrak{p}]$ is the cardinality of the residue field at $\mathfrak{p}$ (its absolute norm). The Euler product for $\zeta_K(z)$ defines a

---

[2]A GAP identifier $\langle m, n \rangle$ denotes the isomorphism class of an abstract group of order m; the positive integer n is an ordinal that distinguishes distinct isomorphism classes of groups of order m. For $m \leq 2000$ not equal to 1024 explicit presentations of these groups can be found in the small groups database [3], which is available in both GAP [14] and Magma [5].

holomorphic function on $\mathrm{Re}(z) > 1$ that extends to a meromorphic function on $\mathbf{C}$ with a simple pole at $z = 1$ whose residue is given by the *analytic class number formula*:

$$\lim_{z \to 1^+} (z-1)\zeta_K(z) = \frac{2^r(2\pi)^s h_K R_K}{\#\mu(K)|D_K|^{1/2}}. \tag{2.2}$$

Here r and s are the number of real and complex places of K (its *signature*), h_K is the class number, R_K is the regulator, $\mu(K)$ is the group of roots of unity in $K^\times$, and D_K is the discriminant of K.

Theorem 2.10. *For number fields K_1 and K_2 the following are equivalent:*

(i) $\zeta_{K_1}(s) = \zeta_{K_2}(s)$;

(ii) K_1 *and* K_2 *have Galois closure* L *with* $\mathrm{Gal}(L/K_1), \mathrm{Gal}(L/K_2) \leq \mathrm{Gal}(L/\mathbf{Q})$ *rationally equivalent;*

(iii) *There is a bijection between the primes of* K_1 *and* K_2 *that preserves residue fields.*

Proof. These equivalences all follow from [35, Theorem 1]. □

Definition 2.11. Number fields K_1 and K_2 that satisfy the equivalent conditions of Theorem 2.10 are said to be *arithmetically equivalent*.

If K_1 and K_2 are arithmetically equivalent number fields with common Galois closure L and we put $G := \mathrm{Gal}(L/\mathbf{Q})$, $H_1 := \mathrm{Gal}(L/K_1)$, $H_2 := \mathrm{Gal}(L/K_2)$, then (G, H_1, H_2) is a *faithful* Gassmann triple, meaning that $\mathbf{Q}[H_1 \backslash G] \simeq \mathbf{Q}[H_2 \backslash G]$ is a faithful representation of G. Equivalently, H_1 and H_2 have trivial normal core in G. There is no loss of generality in restricting our attention to faithful Gassmann triples: if $H_1, H_2 \leq G$ are rationally equivalent then they necessarily have the same normal core N, the quotients $H_1/N, H_2/N \leq G/N$ are rationally equivalent, and H_1/N and H_2/N are conjugate in G/N if and only if H_1 and H_2 are conjugate in G.

Arithmetically equivalent number fields share many (but not all) arithmetic invariants.

Theorem 2.12. *Arithmetically equivalent number fields have the same degree, discriminant, signature, and roots of unity.*

Proof. See [35, Theorem 1]. □

The analytic class number formula (2.2) implies that if K_1 and K_2 are arithmetically equivalent number fields then we must have

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

but it may happen that $h_{K_1} \neq h_{K_2}$ (in which case $R_{K_1} \neq R_{K_2}$), and even when $h_{K_1} = h_{K_2}$ the class groups need not be isomorphic.[3] It follows from Theorem 2.12 that if K_1 and K_2 are arithmetically equivalent then a prime p of $\mathbf{Q}$ ramifies in K_1 if and only if it ramifies in K_2.

---

[3]The fields $\mathbf{Q}[x]/(x^7 - 3x^6 + 10x^5 - 21x^4 - 6x^3 + 58x^2 - 41x - 6)$ and $\mathbf{Q}[x]/(x^7 - x^6 + x^5 + 5x^4 + 9x^3 + 5x^2 - 7x - 4)$ with LMFDB [29] labels `7.3.1427382162361.1` and `7.3.1427382162361.2` are an example; see [2] for analogous exceptions in the context of isospectral Riemannian manifolds.

Remark 2.13. The ramified rational primes in arithmetically equivalent number fields necessarily coincide, but they may have different factorization patterns. This was shown by Perlis in [35, page 351] for the arithmetically equivalent number fields $K_1 := \mathbf{Q}(\sqrt[8]{97})$ and $K_2 := \mathbf{Q}(\sqrt[8]{1552})$ where we have

$$2\mathcal{O}_{K_1} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4^4 \qquad \text{versus} \qquad 2\mathcal{O}_{K_2} = \mathfrak{q}_1^2\mathfrak{q}_2^2\mathfrak{q}_3^2\mathfrak{q}_4^2.$$

In this example the products of the ramification indices differ, but the sums are the same. As shown by Mantilla-Soler [30, Thm. 3.7], there are cases where the sums also differ. Indeed, the number fields $K_1 := \mathbf{Q}[x]/(x^7 - 3x^6 + 4x^5 - 5x^4 + 3x^3 - x^2 - 2x + 1)$ and $K_2 := \mathbf{Q}[x]/(x^7 - x^5 - 2x^4 - 2x^3 + 2x^2 - x + 4)$ with LMFDB labels `7.3.30558784.1` and `7.3.30558784.2` are arithmetically equivalent with

$$2\mathcal{O}_{K_1} = \mathfrak{p}_1\mathfrak{p}_2^4 \qquad \text{versus} \qquad 2\mathcal{O}_{K_2} = \mathfrak{q}_1\mathfrak{q}_2^2.$$

This example settled a question of Stuart and Perlis [37, §4].

For a number field K with Galois closure L that is the fixed field of $H \leq G = \text{Gal}(L/\mathbf{Q})$, the decomposition of rational primes in K, can be computed using the G-set $[H \backslash G]$. The lemma below can be used to explain the examples in Remark 2.13 and to prove part (iii) of Theorem 2.10.

Lemma 2.14. *Let L be a Galois extension of $\mathbf{Q}$ with Galois group G, let $\mathfrak{p}$ be a prime of L above $p := \mathfrak{p} \cap \mathbf{Q}$ with decomposition group $D_\mathfrak{p}$ and inertia group $I_\mathfrak{p}$, and let K be the fixed field of $H \leq G$.*

  (i) *There is a bijection $[H\backslash G/D_\mathfrak{p}] \to \{\text{primes of } K \text{ above } p\}$ defined by $H\sigma D_\mathfrak{p} \mapsto \sigma(\mathfrak{p}) \cap K$.*

  (ii) *The prime $\sigma(\mathfrak{p}) \cap K$ has ramification index $[H\sigma I_\mathfrak{p} : H\sigma]$ and residue field degree $[H\sigma D_\mathfrak{p} : H\sigma I_\mathfrak{p}]$.*

Proof. This is well known; see [34, §9] and [51], for example. $\square$

Theorem 2.10 implies that if K_1 and K_2 are arithmetically equivalent number fields then for every unramified rational prime p there is a bijection between the primes of K_1 above p and the primes of K_2 above p such that the completions of K_1 and K_2 at corresponding primes above p are isomorphic extensions of $\mathbf{Q}_p$, since (up to isomorphism) there is a unique unramified extension of $\mathbf{Q}_p$ of each degree. By Theorem 2.12, this also holds for the archimedean place ∞ of $\mathbf{Q}$, since the signatures of K_1 and K_2 coincide, but as shown by the examples of Remark 2.13, this need not hold at ramified primes.

Definition 2.15. Two number fields K_1 and K_2 are said to be *locally isomorphic* if there is a bijection between the places of K_1 and the places of K_2 such that the completions at corresponding places are isomorphic (both as topological rings and as $\mathbf{Q}_p$-algebras); equivalently, $K_1 \otimes_\mathbf{Q} \mathbf{Q}_p \simeq K_2 \otimes_\mathbf{Q} \mathbf{Q}_p$ for all $p \leq \infty$. If this holds for all but finitely many places then K_1 and K_2 are said to be *locally isomorphic almost everywhere*.

For a number field K we use $\mathbf{A}_K$ to denote its ring of adeles, which we may regard both as a topological ring and as an $\mathbf{A}_\mathbf{Q}$-algebra.

Theorem 2.16. *Let K_1 and K_2 be number fields. The following hold:*

  (i) *K_1 and K_2 are locally isomorphic almost everywhere if and only if they are arithmetically equivalent, and if and only if almost every prime of $\mathbf{Q}$ has the same number of primes above it in K_1 and K_2;*

(ii) K_1 and K_2 are locally isomorphic if and only if $\mathbf{A}_{K_1} \simeq \mathbf{A}_{K_2}$ (as topological rings and $\mathbf{A}_{\mathbf{Q}}$-algebras);

(iii) if K_1 and K_2 are locally isomorphic then there is a natural isomorphism of their Brauer groups that commutes with all restriction maps induced by common inclusions of number fields.

Proof. The first equivalence in (i) follows from [35, Theorem 1] and the second was proved in [37], the forward implication in (ii) is immediate and the reverse implication is due to Iwasawa [22, Lemma 7] (also see [26, Lemma 3]), and the implication in (iii) is proved in [28]. $\square$

Remark 2.17. The converse of part (iii) of Theorem 2.16 is false. Arithmetically equivalent number fields with naturally isomorphic Brauer groups need not be locally isomorphic, as shown in [31].

Theorem 2.16 implies that locally isomorphic number fields are necessarily arithmetically equivalent, but the converse need not hold. As observed in Remark 2.13, arithmetically equivalent number fields may have incompatible ramification indices, which precludes local isomorphism.

Remark 2.18. Locally isomorphic number fields need not have the same class number; the fields $\mathbf{Q}(\sqrt[8]{-33})$ and $\mathbf{Q}(\sqrt[8]{-528})$ with class numbers 256 and 128 are an example [12, p. 214].

The following proposition provides an effective way to test for local isomorphism.

Proposition 2.19. *Let L, K_1, K_2 be number fields corresponding to a Gassmann triple (G, H_1, H_2), and let $D_{\mathfrak{p}} \subseteq G$ be the decomposition group of a place $\mathfrak{p}$ of L above a place p of $\mathbf{Q}$. Then $K_1 \otimes_{\mathbf{Q}} \mathbf{Q}_p \simeq K_2 \otimes_{\mathbf{Q}} \mathbf{Q}_p$ if and only if $[H_1\backslash G]$ and $[H_2\backslash G]$ are isomorphic as $D_{\mathfrak{p}}$-sets. These equivalent conditions necessarily hold for every unramified place p of $\mathbf{Q}$.*

Proof. Recall that for any field F with separable closure Ω there is a functorial equivalence between the category of étale F-algebras A and the category of finite $\mathrm{Gal}(\Omega/F)$-sets S; see [32, Theorem 8.20]. The $\mathrm{Gal}(\Omega/F)$-action on S is continuous, hence factors through a finite quotient Q, and by a Q-set S we mean the $\mathrm{Gal}(\Omega/F)$-set S with the action of each $\sigma \in \mathrm{Gal}(\Omega/F)$ given by the action of its projection to Q.

For $i = 1, 2$, the G-set $[H_i\backslash G]$ corresponds to the étale $\mathbf{Q}$-algebra K_i. If we view $D_{\mathfrak{p}}$ as the Galois group of the étale $\mathbf{Q}_p$-algebra $L \otimes \mathbf{Q}_p$, the $D_{\mathfrak{p}}$-set $[H_i\backslash G]$ corresponds to the étale $\mathbf{Q}_p$-algebra $K_i \otimes \mathbf{Q}_p$.

The last statement follows from (iv) of Proposition 2.6, since if $\mathfrak{p}$ is unramified then $D_{\mathfrak{p}}$ is cyclic. $\square$

Finally we recall the following result on arithmetical isomorphisms which can be found in [24, IV].

Proposition 2.20. *Let G be a finite group with subgroups $H_1, H_2 \leq G$, let R be an integral domain, let A be an $R[G]$-module, and let $A_1 := A^{H_1}$ and $A_2 := A^{H_2}$ be the R-submodules of A fixed by H_1 and H_2, respectively. Every $M \in \mathrm{Hom}_{R[G]}(R[H_1\backslash G], R[H_2\backslash G])$ with $\det M \in R^{\times}$ induces an $R[G]$-module isomorphism $\delta_M : A_1 \to A_2$.*

Proof. See [24, Theorem IV.1.6a]. $\square$

3 Stronger forms of arithmetic equivalence

Recall that a finite group K is said to be *cyclic modulo p* (or *p-hypo-elementary*) if the quotient of K by the intersection of its p-Sylow subgroups (its p-core) is cyclic. For the sake of brevity we shall simply call such a group *p-cyclic*. The class of p-cyclic groups includes all p-groups and all cyclic groups.

Proposition 3.1. *Let G be a finite group and p a prime. For $H_1, H_2 \leq G$ the following are equivalent:*

 (i) *There is a G-class preserving bijection between the sets of p-cyclic subgroups of H_1 and H_2;*
 (ii) $\chi_{H_1}(K) = \chi_{H_2}(K)$ *for every p-cyclic $K \leq G$;*
 (iii) *the G-sets $[H_1 \backslash G]$ and $[H_2 \backslash G]$ are isomorphic as K-sets for every p-cyclic $K \leq G$;*
 (iv) $\mathbf{Z}_p[H_1 \backslash G] \simeq \mathbf{Z}_p[H_2 \backslash G]$;
 (v) $\mathbf{F}_p[H_1 \backslash G] \simeq \mathbf{F}_p[H_2 \backslash G]$;
 (vi) $p \nmid d(H_1, H_2)$.

Moreover, in (ii) and (iii) one can replace "$K \leq G$" with "$K \leq H_1$ or $K \leq H_2$".

Proof. The equivalence of (i), (ii), (iii) is given by Proposition 2.2. The equivalence of (ii) and (iv) follows from [42, Proposition 3.1] (attributed to Conlon [10]). The equivalence of (iv) and (v) is given by [17, Theorem 2.9(i)]. The equivalence of (v) and (vi) is immediate, since $\mathbf{F}_p[H_1 \backslash G] \simeq \mathbf{F}_p[H_2 \backslash G]$ if and only if there exists $M \in \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_1 \backslash G])$ whose reduction modulo p is invertible, equivalently, $p \nmid \det M$). That the weakened forms of (ii) and (iii) suffice follows form Proposition 2.2 $\quad\square$

Definition 3.2. Let $H_1, H_2 \leq G$ be finite groups. If $\mathbf{Z}_p[H_1 \backslash G] \simeq \mathbf{Z}_p[H_2 \backslash G]$ for every prime p then H_1 and H_2 are *locally integrally equivalent*, and if $\mathbf{Z}[H_1 \backslash G] \simeq \mathbf{Z}[H_2 \backslash G]$ then they are *integrally equivalent*.

Remark 3.3. Two $\mathbf{Z}[G]$-modules that are isomorphic as $\mathbf{Z}_p[G]$-modules for every prime p are said to *lie in the same genus* [18, 42]; subgroups $H_1, H_2 \leq G$ are locally integrally equivalent if and only of the permutation modules $\mathbf{Z}[H_1 \backslash G]$ and $\mathbf{Z}[H_2 \backslash G]$ lie in the same genus.

Proposition 3.1 implies that subgroups $H_1, H_2 \leq G$ are locally integrally equivalent if and only if

$$d(H_1, H_2) = \gcd\{\det M : M \in \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G])\} = 1,$$

in which case there is a finite set of matrices $M \in \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G]$ whose determinants have trivial GCD. Integral equivalence holds if and only if a singleton set with this property exists, that is, $\det M = \pm 1$ for some $M \in \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G])$. Rational equivalence only requires $d(H_1, H_1) \neq 0$ and is obviously implied by local integral equivalence.

Essentially only one nontrivial example of integral equivalence is known, due to Scott [42], in which $G \simeq \mathbf{PSL}_2(29)$ and H_1 and H_2 are nonconjugate subgroups of G isomorphic to the alternating group A_5 that are conjugate in $\mathbf{PGL}_2(29)$; one can use this example to construct others, but these all have a subgroup with a quotient isomorphic to $\mathbf{PSL}_2(29)$. As noted by Scott and proved in Theorem 3.9 below, for every prime $p \equiv \pm 29 \mod 120$ the group $\mathbf{PSL}_2(p)$ contains nonconjugate subgroups isomorphic to A_5 that are locally integrally equivalent. But with the exception of $p = 29$ it is not known whether these subgroups are also integrally equivalent.

Proposition 3.4. *Let K_1 and K_2 be number fields with common Galois closure L, and let $H_1 := \mathrm{Gal}(L/K_1)$, $H_2 := \mathrm{Gal}(L/K_2)$ be locally integrally equivalent subgroups of $G := \mathrm{Gal}(L/\mathbf{Q})$. Then the following hold:*

(i) *K_1 and K_2 are arithmetically equivalent;*

(ii) *the class groups of K_1 and K_2 are isomorphic;*

(iii) *the regulators of K_1 and K_2 are equal;*

(iv) *for every prime p the products of the ramification indices of the primes of K_1 and K_2 above p coincide.*

Proof. As noted above, local integral equivalence implies rational equivalence, so (i) follows from Proposition 2.6 and Theorem 2.10. Proposition 3.1 and [36, Theorem 3] together imply that the class groups of K_1 and K_2 have isomorphic p-Sylow subgroups for every prime p and are therefore isomorphic (since they are abelian), so (ii) holds. Properties (i) and (ii) together imply (iii), by Theorem 2.12 and the analytic class number formula. Local integral equivalence implies $d(H_1, H_2) = 1$, which when combined with [24, Theorem IV.2.3] implies (iv). □

For number fields satisfying the hypothesis of Proposition 3.4, all the quantities that appear in the analytic class number formula (2.2) must coincide. However, such fields need not be locally isomorphic, as shown by the example in §4.2, and locally isomorphic number fields may have different class numbers and regulators, as shown by the example in Remark 2.18.

We now introduce a strictly stronger notion of equivalence that implies both local integral equivalence and local isomorphism of corresponding number fields.

Definition 3.5. Subgroups H_1 and H_2 of a finite group G are *solvably equivalent* if they satisfy the following equivalent properties (as guaranteed by Proposition 2.2):

(i) There is a G-class preserving bijection between the sets of solvable subgroups of H_1 and H_2;

(ii) $\chi_{H_1}(K) = \chi_{H_2}(K)$ for every solvable $K \leq G$;

(iii) the G-sets $[H_1 \backslash G]$ and $[H_2 \backslash G]$ are isomorphic as K-sets for every solvable $K \leq G$.

Solvably equivalent subgroups are always locally integrally equivalent, since p-cyclic groups are solvable, but as demonstrated by the example in §4.3, locally integrally equivalent subgroups need not be solvably equivalent. As shown by the example in §4.4, solvably equivalent subgroups need not be integrally equivalent, but it is not clear whether the converse holds; the integrally equivalent subgroups of $\mathbf{PSL}_2(29)$ in Scott's example are solvably equivalent, but as noted in the introduction, it is not clear whether this is always true, nor is it clear that integral equivalence guarantees local isomorphism of corresponding number fields (this is not true of local integral equivalence, and if it were true for integral equivalence then property (2) in Theorem 3 in [38] could have been included in Theorem 2 in [38]).

Question 3.6. Is there a Gassmann triple (G, H_1, H_2) in which H_1 and H_2 are integrally equivalent but not solvably equivalent? More precisely, is there a group G containing subgroups H_1, H_2 and a solvable subgroup K such that $\mathbf{Z}[H_1 \backslash G]$ and $\mathbf{Z}[H_2 \backslash G]$ are isomorphic as $\mathbf{Z}[G]$-modules but not as K-sets?

Proposition 3.7. *Let K_1 and K_2 be number fields with the same Galois closure L, and put $H_1 := \mathrm{Gal}(L/K_1)$ and $H_2 := \mathrm{Gal}(L/K_2)$. If H_1 and H_2 are solvably equivalent subgroups of $G := \mathrm{Gal}(L/\mathbf{Q})$ then*

(i) K_1 and K_2 are arithmetically equivalent;

(ii) K_1 and K_2 have isomorphic class groups and equal regulators;

(iii) K_1 and K_2 are locally isomorphic, and in particular there is a bijection between the primes of K_1 and K_2 that preserves both inertia degrees and ramification indices;

(iv) the adele rings $\mathbf{A}_{K_1}$ and $\mathbf{A}_{K_2}$ are isomorphic (as topological groups and $\mathbf{A}_{\mathbf{Q}}$-algebras);

Proof. Solvable equivalence implies local integral equivalence, so (i) and (ii) both follow from Proposition 3.4. For each prime $\mathfrak{p}$ of L the decomposition subgroup $D_\mathfrak{p} \subseteq \mathrm{Gal}(L/\mathbf{Q})$ is solvable, so we have an isomorphism of $D_\mathfrak{p}$-sets $[H_1 \backslash G] \simeq [H_2 \backslash G]$, which implies (iii), by Proposition 2.19, and (iv) is then implied by Theorem 2.16. $\qquad\square$

Remark 3.8. In Proposition 3.7, the hypothesis that H_1 and H_2 are solvably equivalent is stronger than necessary. It could be replaced, for example, by the condition that $\chi_{H_1}(K) = \chi_{H_2}(K)$ for every $K \leq G$ with normal subgroups $W \leq I$ such that W is a p-group, I/W is cyclic of order prime to p, and K/I is cyclic. Even this is stronger than necessary, since, for example, it is satisfied by both C_2^4 and $\mathbf{SL}_2(3)$, neither of which occurs as the Galois group of an extension of $\mathbf{Q}_p$ for any prime p (the former contains too many normal subgroups of index 2 and the latter was ruled out by Weil in [50, §15]).

The following theorem gives an infinite family of groups each of which contain a pair of nonconjugate solvably equivalent subgroups.

Theorem 3.9. *Let $p \equiv \pm 29 \bmod 120$ be prime. The group $\mathbf{SL}_2(\mathbf{F}_p)$ contains a pair of nonconjugate solvably equivalent subgroups H_1, H_2 whose projective images are nonconjugate solvably equivalent subgroups of $\mathbf{PSL}_2(\mathbf{F}_p)$ isomorphic to the alternating group A_5.*

Proof. It follows from [48, Lemma 3.21.3c] that for $p \equiv \pm 1 \bmod 5$, up to conjugacy in $\mathbf{GL}_2(\mathbf{F}_p)$ there is a unique subgroup H_1 of $\mathbf{SL}_2(\mathbf{F}_p)$ with projective image isomorphic to A_5; it is isomorphic to $\mathbf{SL}_2(\mathbf{F}_5)$. The outer automorphism of $\mathbf{SL}_2(\mathbf{F}_p)$ corresponds to conjugation by an element with nonsquare determinant; let $\sigma := \left[\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right]$ be such an element, with $r \in \mathbf{F}_p^\times - \mathbf{F}_p^{\times 2}$. Conjugation by σ fixes all but four of the conjugacy classes in $\mathbf{SL}_2(\mathbf{F}_p)$: it interchanges the conjugacy classes of $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right]$, and also those of $\left[\begin{smallmatrix} -1 & -1 \\ 0 & -1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -1 & -r \\ 0 & -1 \end{smallmatrix}\right]$ (these are the conjugacy classes of elements of order divisible by p).

Let $H_2 := \sigma H_1 \sigma^{-1}$; the groups H_1 and H_2 are not conjugate in $\mathbf{SL}_2(\mathbf{F}_p)$, by [13, Theorem 4.1]. These groups do not contain any elements of order divisible by p, since $p \geq 29$ and $\#\mathbf{SL}_2(\mathbf{F}_5) = 2^2 \cdot 3 \cdot 5$. Conjugation by σ thus defines an $\mathbf{SL}_2(\mathbf{F}_p)$-conjugacy preserving bijection between H_1 and H_2, implying that H_1 and H_2 are rationally equivalent subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$.

To show that H_1 and H_2 are solvably equivalent, it suffices to show that σ defines an $\mathbf{SL}_2(\mathbf{F}_p)$-conjugacy class preserving bijection of solvable subgroups of H_1 and H_2, and having proved rational equivalence we only need to consider the noncyclic solvable subgroups of H_1 and H_2. Up to isomorphism, there are four possibilities for the image of such a subgroup in in $\mathbf{PSL}_2(\mathbf{F}_p)$: D_2, D_3, D_5, and A_4, where $D_2 := C_2 \times C_2$ is the Klein group. It follows from Proposition 3.13 below that there is exactly one $\mathbf{SL}_2(\mathbf{F}_p)$-conjugacy class of subgroups isomorphic to D_2, D_3, D_5, A_4 when $p \equiv \pm 3 \bmod 8$, $p \equiv \pm 5 \bmod 12$, $p \equiv \pm 9 \bmod 20$, and $p \equiv \pm 3 \bmod 8$, respectively. These constraints are simultaneously met precisely when $p \equiv \pm 29 \bmod 120$, and in this situation it is clear that σ must define an $\mathbf{SL}_2(\mathbf{F}_p)$-conjugacy class preserving bijection of solvable subgroups of H_1 and H_2, since it preserves isomorphism classes.

Finally, note that the conjugacy class preserving bijection between solvable subgroups of H_1 and H_2 descends to $\mathbf{PSL}_2(\mathbf{F}_p)$, while H_1 and H_2 both contain -1 and remain nonconjugate in $\mathbf{PSL}_2(\mathbf{F}_p)$. $\square$

Remark 3.10. Theorem 3.9 accounts for all nontrivial pairs of solvably equivalent subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$, in fact all nontrivial pairs of locally integrally equivalent subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$, as noted by Scott [42]. Up to a central extension the same applies to subgroups of $\mathbf{GL}_2(\mathbf{F}_p)$, since every nonsolvable subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$ that does not contain $\mathbf{SL}_2(\mathbf{F}_p)$ has projective image A_5 [43, §2].

Remark 3.11. As proved by Zywina [52], the group $\mathbf{PSL}_2(\mathbf{F}_p)$ can be realized as the Galois group of a number field for every prime p. This implies that there are infinitely many distinct examples of pairs of nonisomorphic solvably equivalent number fields whose Galois groups do not admit a common quotient.

Remark 3.12. As shown in §4.4, subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$ are not the only source of nontrivial solvably equivalent pairs of subgroups, and one can do better than the minimal degree 203 admitted by Theorem 3.9: degree 96 is possible.

Recall that each subgroup of $\mathbf{GL}_2(\mathbf{F}_p)$ of order prime to p can be classified according to the isomorphism class of its image in $\mathbf{PGL}_2(\mathbf{F}_p)$, which must be cyclic, dihedral, or one of A_4, S_4, A_5; see [43, §2], for example. Note that we consider $D_2 := C_2 \times C_2$ to be a dihedral group. The proposition below characterizes the isomorphism classes of order prime to p that arise in $\mathbf{SL}_2(\mathbf{F}_p)$, up to conjugacy in $\mathbf{SL}_2(\mathbf{F}_p)$; see [48, §3] for an analogous classification for conjugacy classes of subgroups of $\mathbf{GL}_2(\mathbf{F}_p)$ (including those of order divisible by p), which we will use in the proof of the proposition.

We use the notation $2D_n$ to denote the binary dihedral group of order $4n$, these arise as subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$ containing -1 with projective image D_n, and similar define $2A_4$, $2S_4$, $2A_5$. We say that a conjugacy class of subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$ is C_n (resp. $2D_n$, $2A_4$, $2S_4$, $2A_5$) if it is the conjugacy class of a subgroup isomorphic to C_n (resp. $2D_n$, $2A_4$, $2S_4$, $2A_5$).

Proposition 3.13. *Let $p > 3$ be prime, and let S be the set of integers that divide either $p-1$ or $p+1$. Up to conjugacy in $\mathbf{SL}_2(\mathbf{F}_p)$ the subgroups of $\mathbf{SL}_2(\mathbf{F}_p)$ of order prime to p are as follows:*

- *For each integer $n \geq 1$ with $p \equiv \pm 1 \bmod n$, a single conjugacy class C_n.*
- *For each integer $2n > 2$ with $p \equiv \pm 1 \bmod 4n$, two conjugacy classes $2D_n$.*
- *For each integer $2n > 2$ with $p \equiv \pm 1 \bmod 2n$ and $p \not\equiv \pm 1 \bmod 4n$, a single conjugacy class $2D_n$.*
- *Two conjugacy classes $2A_4$ if $p \equiv \pm 1 \bmod 8$ and one otherwise.*
- *Two conjugacy classes $2S_4$ if $p \equiv \pm 1 \bmod 8$ and none otherwise.*
- *Two conjugacy classes $2A_5 \simeq \mathbf{SL}(2,5)$ if $p \equiv \pm 1 \bmod 5$ and none otherwise.*

Proof. Every cyclic subgroup of $\mathbf{SL}_2(\mathbf{F}_p)$ order prime to p must be conjugate in $\mathbf{GL}_2(\mathbf{F}_p)$ to a subgroup of one of the two Cartan subgroups C: the *split Cartan* isomorphic to $\mathbf{F}_p^\times \times \mathbf{F}_p^\times$, or the *nonsplit Cartan* isomorphic to $\mathbf{F}_{p^2}^\times$. The intersection of C with $\mathbf{SL}_2(\mathbf{F}_p)$ is cyclic of order $p-1$ or $p+1$, and the intersection of these groups is the cyclic group $\{\pm 1\}$ of order $2 = \gcd(p-1, p+1)$. It follows that up to $\mathbf{GL}_2(\mathbf{F}_p)$-conjugacy there is a unique cyclic subgroup C_n of $\mathbf{SL}_2(\mathbf{F}_p)$ of order n for each n dividing $p-1$ or $p+1$, and [13, Theorem 4.1] implies that it is also unique up to $\mathbf{SL}_2(\mathbf{F}_p)$-conjugacy.

For a Cartan subgroup C of $\mathbf{GL}_2(\mathbf{F}_p)$, let C^+ denote its normalizer. It follows from [48, Lemma 3.13] that for each subgroup H of $C \cap \mathbf{SL}_2(\mathbf{F}_p)$ there is at most one subgroup G of $C^+ \cap \mathbf{SL}_2(\mathbf{F}_p)$ with dihedral

image in $\mathbf{PSL}(2,p)$, and that subgroup must contain -1. It follows from [48, Lemmas 3.16 and 3.18] that there is exactly one G for each $H \neq \{\pm 1\}$ that contains -1, up to conjugacy in $\mathbf{GL}_2(\mathbf{F}_p)$. It follows that for each integer $2n > 2$ dividing $p-1$ or $p+1$ that up to $\mathbf{GL}_2(\mathbf{F}_p)$-conjugacy there is a unique conjugacy class $2D_n$ of $\mathbf{SL}_2(\mathbf{F}_p)$, and it follows from [13, Theorem 4.1] and Remark 3.14 below that this $\mathbf{GL}_2(\mathbf{F}_p)$-conjugacy class splits into two $\mathbf{GL}_2(\mathbf{F}_p)$-conjugacy classes if and only if $p \equiv \pm 1 \bmod 4n$.

The statements for $2A_4$, $2S_4$, $2A_5$ are immediate from [48, Lemma 3.21] and [13, Theorem 4.1]. $\qquad\square$

Remark 3.14. There is a minor error in the statement [13, Theorem 4.1] regarding the group $2D_2$, which is denoted $BD_{4\cdot2}$ in [13]. There are two conjugacy classes $2D_2$ in $\mathbf{SL}_2(\mathbf{F}_p)$ when $\sqrt{2} \in \mathbf{F}_p$, equivalently, when $p \equiv \pm 1 \bmod 8$, but only one otherwise; this follows from the fact that the normalizer of $BD_{4\cdot2}$ in $\mathbf{SL}_2(\overline{\mathbf{F}}_p)$ is $2S_4$ (not $2A_4$ as claimed in [13]), which is present in $\mathbf{SL}_2(\mathbf{F}_p)$ only when $\sqrt{2} \in \mathbf{F}_p$. The author is grateful to Yuval Flicker for clarifying this point.

4 Computational results

In this section we present examples that realize the claims made in the introduction, including that local integral equivalence does not imply group isomorphism (§4.1), local isomorphism of number fields (§4.2), or integral equivalence (§4.3), and that solvable equivalence does not imply integral equivalence (§4.4). We also give a degree 32 example of locally integrally equivalent number fields in §4.3 (best possible), and a degree 96 example of solvably equivalent number fields in §4.4 (best known).

4.1 Locally integrally equivalent subgroups need not be isomorphic

In [38, Question 1], Prasad asks if integrally equivalent subgroups are necessarily isomorphic. This is true in Scott's example with two subgroups of $\mathbf{PSL}_2(\mathbf{F}_{29})$ isomorphic to the alternating group A_5. The following example shows that locally integrally equivalent subgroups need not be isomorphic. Let G by the symmetric group S_{21} and consider the subgroups

$$
\begin{aligned}
H_1 &:= \big\langle\, (4\,5)(6\,15\,7\,14)(8\,17\,9,16)(10\,19\,11\,18)(12\,21\,13\,20), \\
&\qquad (1\,2)(3\,5)(6\,20\,8\,18)(7\,21\,9\,19)(10\,14\,12\,16)(11\,15\,13\,17)\,\big\rangle, \\
H_2 &:= \big\langle\, (4\,5)(6\,16\,8\,14)(7\,17\,9\,15)(10\,20\,12\,18)(11\,21\,13\,19), \\
&\qquad (1\,2)(3\,5)(6\,20\,8\,18)(7\,21\,9\,19)(10\,17\,12\,15)(11\,16\,13\,14)\,\big\rangle,
\end{aligned}
$$

with GAP identifiers $\langle 48,12\rangle$ and $\langle 48,13\rangle$, respectively. Each contains 41 subgroups that are p-cyclic for some prime p. These fall into 15 distinct G-conjugacy classes and 11 distinct isomorphism classes, which makes it easy to find a G-conjugacy class preserving bijection between them (if one takes into account the isomorphism class and the number of subgroups in each conjugacy classes, there are only 2 choices to consider). The subgroups $H_1, H_2 \le G$ are thus locally integrally equivalent, but not isomorphic. This negatively answers Question 2.11 posed by Guralnick and Weiss in [18].

This example is realized by infinitely many number fields: over $\mathbf{Q}$ the Galois group of a generic polynomial of degree 21 is $G = S_{21}$ and the fixed fields of H_1 and H_2 are locally integrally equivalent number fields of degree $21!/48$. It is one of many that were found by applying Corollary 2.5 to the

clas $\mathcal{P}$ of groups that are p-cyclic for some prime p: computing $\mathcal{P}$-statistics for the isomorphism classes of groups of order up to 255 already finds 107 pairs of isomorphism classes with the same $\mathcal{P}$-statistics, including four isomorphism classes of groups of order 192 with the same $\mathcal{P}$-statistics. One can often find permutation representations of degree less than $|H_1| = |H_2|$ that also work, as happens above.

Question 4.1. Are solvably equivalent subgroups of a finite group G necessarily isomorphic?

Question 4.1 is equivalent to asking whether the isomorphism class of a nonsolvable group determine its $\mathcal{P}$-statistics, where $\mathcal{P}$ is the class of solvable groups (by Corollary 2.5). For the 1022 isomorphism classes of nonsolvable groups of order less than 2000, these $\mathcal{P}$-statistics are all distinct, so any pair of nonisomorphic solvably equivalent subgroups must have order greater than 2000.

4.2 Local integral equivalence does not imply local isomorphism of number fields

Let G be the group $A_4 \times S_5$ with GAP identifier $\langle 1440, 5846 \rangle$. There is a unique pair of nonconjugate locally integrally equivalent subgroups $H_1, H_2 \leq G$, both of which are isomorphic to the dihedral group D_6 of order 12. The groups G, H_1, H_2 can be explicitly represented as subgroups of S_9 via

$$G := \langle (1\ 2\ 3)(5\ 6\ 7\ 8\ 9),\ (1\ 2)(3\ 4)(5\ 6) \rangle,$$
$$H_1 := \langle (1\ 2)(3\ 4)(5\ 6\ 7)(8\ 9),\ (1\ 3)(2\ 4)(5\ 6) \rangle,$$
$$H_2 := \langle (1\ 2)(3\ 4)(5\ 6\ 7)(8\ 9),\ (1\ 4)(2\ 3)(5\ 6) \rangle,$$

and $H_1 \cap H_2$ is cyclic of order 6. The four maximal subgroups of H_1, isomorphic to C_2^2, S_3, S_3, C_6, correspond to distinct conjugacy classes of subgroups of G, and these are precisely the G-conjugacy classes of the four maximal subgroups of H_2. There is thus a G-conjugacy preserving bijection between the proper subgroups of H_1 and H_2 (all of which are p-cyclic for some prime p), and the group $D_6 \simeq H_1, H_2$ is not p-cyclic for any prime p. It follows that H_1 and H_2 are locally integrally equivalent subgroups of G.

The subgroups H_1 and H_2 are not G-conjugate, even though they are S_9-conjugate, as can be verified by comparing their permutation characters: $\chi_{H_1}(H_1) = 4$ differs from $\chi_{H_2}(H_1) = 0$, and $\chi_{H_1}(H_2) = 0$ differs from $\chi_{H_2}(H_2) = 4$. The group D_6 arises as a Galois group of extensions of $\mathbf{Q}_p$ for $p \not\equiv 1 \mod 6$, and it follows from Proposition 2.19 that if H_1 is the decomposition group of a prime above p in a Galois extension $L/\mathbf{Q}$ with Galois group G, then the fixed fields $K_1 := L^{H_1}$ and $K_2 := L^{H_2}$ are locally integrally equivalent fields that cannot be locally isomorphic because four primes of K_1 above 2 must have residue field degree 1 and ramification index 1 (corresponding to the four cosets in $[H_1 \backslash G]$ fixed by H_1), but no primes of K_2 above 2 can have residue field degree 1 and ramification index 1.

To realize such an example it suffices to find a pair of linearly disjoint A_4 and S_5 fields such that that there is a prime of the compositum with decomposition group conjugate to H_1 or H_2. A search of A_4 and S_5 fields in the L-functions and modular forms database (LMFDB) unramified away from 2,3,5,7 finds a suitable pair: we may take the Galois closures for the fields $F_1 := \mathbf{Q}[x]/(x^4 - 6x^2 - 8x + 60)$ and $F_2 := \mathbf{Q}[x]/(x^5 + 5x^3 + 10x - 2)$ with LMFDB labels 4.0.254016.2 and 5.1.500000.1, respectively. The compositum of their Galois closures is a degree 1440 number field L with Galois group G. The 120 primes of L above 2 all have residue degree 2, ramification index 6, decomposition group conjugate to H_1, and inertia group conjugate to $H_1 \cap H_2$; the local algebra $L \otimes_{\mathbf{Q}} \mathbf{Q}_2$ is isomorphic to k^{120}, where k is the unique D_6-extension of $\mathbf{Q}_2$ of degree 12 containing $\mathbf{Q}_2(\sqrt{2})$, with LMFDB label 2.12.22.60.

Using the `GaloisSubgroup` function in Magma [5] one can compute defining polynomials of degree 120 for the number fields $K_1 := L^{H_1}$ and $K_2 := L^{H_2}$, and using the p-adic valuation `extensions` method in Sage [41] one can determine the residue field degrees and ramification indices of the primes above 2 in K_2 and K_2 by computing all extensions of the 2-adic valuation of $\mathbf{Q}$ to K_1 and K_2. We have

$$2\mathcal{O}_{K_1} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5^6\mathfrak{p}_6^6\mathfrak{p}_7^6\mathfrak{p}_8^6\mathfrak{p}_9^6\mathfrak{p}_{10}^6\mathfrak{p}_{11}^6\mathfrak{p}_{12}^6\mathfrak{p}_{13}^2\mathfrak{p}_{14}^2\mathfrak{p}_{15}^3\mathfrak{p}_{16}^3\mathfrak{p}_{17}^6\mathfrak{p}_{18}^6\mathfrak{p}_{19}^6\mathfrak{p}_{20}^6,$$
$$2\mathcal{O}_{K_2} = \mathfrak{q}_1^2\mathfrak{q}_2^2\mathfrak{q}_3^2\mathfrak{q}_4^2\mathfrak{q}_5^3\mathfrak{q}_6^3\mathfrak{q}_7^3\mathfrak{q}_8^3\mathfrak{q}_9^6\mathfrak{q}_{10}^6\mathfrak{q}_{11}^6\mathfrak{q}_{12}^6\mathfrak{q}_{13}\mathfrak{q}_{14}\mathfrak{q}_{15}^6\mathfrak{q}_{16}^6\mathfrak{q}_{17}^6\mathfrak{q}_{18}^6\mathfrak{q}_{19}^6\mathfrak{q}_{20}^6,$$

where the primes $\mathfrak{p}_i$ of K_1 and $\mathfrak{q}_i$ of K_2 have residue degree 1 for $i \le 12$ and residue degree 2 for $i > 12$.

Remark 4.2. This example can be viewed as a refinement of the example of Mantilla-Soler [30] noted in Remark 2.13: the sums 82 and 86 of the ramification indices differ. But in the Mantilla-Soler example the products of the ramification indices also differ, which is possible because the subgroups are rationally equivalent but not locally integrally equivalent. Proposition 3.4 shows that this is not possible when the subgroups are locally integrally equivalent. To our knowledge, this is the first example of a pair of arithmetically equivalent number fields and a prime p for which the sums of the ramification indices of the primes above p differ but the products do not.

Finally, we note that the groups H_1 and H_2 are isomorphic to D_6, hence solvable, but the values of the permutation characters χ_{H_1} and χ_{H_2} differ on these groups, as noted above, so they are not solvably equivalent, which shows that solvable equivalence is a strictly stronger condition (as one would expect).

4.3 A minimal degree example of local integral equivalence

An exhaustive search of isomorphisms classes of groups of order less than 1024 in the small groups database [3] finds 74 groups G that contain nonconjugate $H_1, H_2 \le G$ that are locally integrally equivalent and have trivial normal core in G (meaning that (G, H_1, H_2) is a faithful Gassmann triple). The order of G is necessarily not a prime power, since p-groups can be locally integrally equivalent only if they are conjugate, so only 1,206,112 of the 11,759,892 groups of order less than 1024 need to be checked. Of these, two have order 384, seventeen have order 576, fifty have order 768, and five have order 864, with the index of H_1, H_2 in G taking values in $\{32, 48, 64, 72\}$.

The two groups G of order 384 have GAP identifiers $\langle 384, 18046 \rangle$ and $\langle 384, 18050 \rangle$, and are isomorphic to transitive permutation groups of degree 32 with LMFDB labels 32T9403 and 32T9408, following the labeling convention in [7]. Both are (nonsplit) 2-extensions of $D_4 \times S_4$, making it feasible to explicitly construct examples of nonconjugate number fields K_1 and K_2 of degree 32 with common Galois closure L with $G = \text{Gal}(L/\mathbf{Q})$, and $H_1 = \text{Gal}(L/K_1)$ and $H_2 = \text{Gal}(L/K_2)$ locally integrally equivalent, by taking a quadratic extension of the compositum of the Galois closure of two suitably chosen D_4 and S_4 quartic number fields. Below we describe one such example in detail.

The Magma computer algebra system [5] includes a database of transitive permutation groups of degree up to 48 whose construction is described in [7, 20, 21]. An exhaustive analysis of the 40,238 transitive groups of degree less than 32 finds none that contain a pair of locally integrally equivalent subgroups of index equal to the degree. The following example thus achieves the minimal possible degree 32; for comparison, the minimal degree of arithmetically equivalent number fields is 7; see [6].

We begin with the D_4 field $\mathbf{Q}[x]/(x^4 - 6x^2 - 9)$ and the S_4 field $\mathbf{Q}[x]/(x^4 - 2x^3 - 6x + 3)$, with LMFDB labels `4.2.9216.1` and `4.2.3888.1`, which are linearly disjoint over $\mathbf{Q}$. The compositum of their Galois closures coincides with the splitting field of the polynomial

$$x^{16} + 12x^{14} + 72x^{12} + 120x^{10} - 234x^8 + 108x^6 + 396x^4 - 432x^2 + 81,$$

which has Galois group $D_4 \times S_4$. The number fields $K_1 := \mathbf{Q}[x]/(f_1(x))$, $K_2 := \mathbf{Q}[x]/(f_2(x))$ defined by

$$f_1 := x^{32} + 12x^{28} + 72x^{24} + 120x^{20} - 234x^{16} + 108x^{12} + 396x^8 - 432x^4 + 81,$$
$$f_2 := x^{32} - 12x^{28} + 72x^{24} - 120x^{20} - 234x^{16} - 108x^{12} + 396x^8 + 432x^4 + 81,$$

have the same Galois closure L of degree 384. The group $G := \mathrm{Gal}(L/\mathbf{Q})$ is the transitive permutation group `32T9403`, generated by

$\sigma_0 := (3,4,5,6,7,8)(9,10,11,12,13,14)(15,16,17,18,19,20)(21,22,23)(24,25,26)(27,28)(29,30)(31,32),$

$\sigma_1 := (3,5)(6,8)(9,10)(11,14)(12,13)(15,17)(18,20)(21,24)(22,26)(23,25)(27,31)(28,32),$

$\sigma_2 := (1,2)(3,17)(4,16)(5,15)(6,20)(7,19)(8,18)(9,13)(10,12)(22,23)(25,26)(29,30),$

$\sigma_3 := (1,3,2,15)(4,9,16,12)(5,24,17,21)(6,30,18,29)(7,22,19,25)(8,14,20,11)(10,32,13,28)(23,27,26,31).$

The group G contains exactly two conjugacy classes of subgroups of index 32 with trivial normal core, represented by $H_1 := \langle \sigma_1, \sigma_2 \rangle$ and $H_2 := \langle \sigma_0, \sigma_2 \rangle$, both isomorphic to D_6. If we view G as acting on the roots of $f_1(x)$, then under a suitable ordering of roots we have $H_1 = \mathrm{Gal}(L/K_1)$ and $H_2 = \mathrm{Gal}(L/K_2)$. The subgroups H_1 and H_2 are locally integrally equivalent but not integrally equivalent. Indeed, for a suitable choice of bases for $[H_1 \backslash G]$ and $[H_2 \backslash G]$, every $M \in \mathrm{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G])$ has the form

$$M := \begin{bmatrix}
x_8 & x_8 & x_5 & x_8 & x_8 & x_7 & x_8 & x_5 & x_8 & x_2 & x_1 & x_8 & x_6 & x_8 & x_8 & x_7 & x_7 & x_8 & x_7 & x_4 & x_3 & x_3 & x_1 & x_7 & x_8 & x_6 & x_2 & x_4 & x_5 & x_6 & x_7 & x_8 \\
x_8 & x_8 & x_7 & x_8 & x_8 & x_5 & x_8 & x_7 & x_8 & x_3 & x_4 & x_8 & x_7 & x_8 & x_8 & x_5 & x_6 & x_8 & x_5 & x_4 & x_2 & x_2 & x_1 & x_6 & x_8 & x_7 & x_3 & x_1 & x_7 & x_7 & x_6 & x_8 \\
x_7 & x_6 & x_8 & x_3 & x_7 & x_8 & x_5 & x_1 & x_2 & x_8 & x_7 & x_5 & x_8 & x_3 & x_7 & x_8 & x_8 & x_2 & x_1 & x_5 & x_8 & x_8 & x_6 & x_8 & x_6 & x_4 & x_8 & x_7 & x_8 & x_8 & x_4 & x_7 \\
x_8 & x_1 & x_6 & x_8 & x_8 & x_2 & x_8 & x_5 & x_8 & x_7 & x_8 & x_4 & x_5 & x_8 & x_1 & x_7 & x_7 & x_8 & x_7 & x_8 & x_5 & x_6 & x_8 & x_2 & x_8 & x_6 & x_7 & x_8 & x_3 & x_3 & x_7 & x_4 \\
x_8 & x_8 & x_6 & x_8 & x_8 & x_7 & x_8 & x_6 & x_8 & x_2 & x_4 & x_8 & x_5 & x_8 & x_8 & x_7 & x_7 & x_8 & x_7 & x_1 & x_3 & x_3 & x_4 & x_7 & x_8 & x_5 & x_2 & x_1 & x_6 & x_5 & x_7 & x_8 \\
x_5 & x_7 & x_8 & x_2 & x_6 & x_8 & x_7 & x_4 & x_3 & x_8 & x_5 & x_7 & x_8 & x_2 & x_5 & x_8 & x_8 & x_3 & x_1 & x_7 & x_8 & x_8 & x_7 & x_8 & x_7 & x_1 & x_8 & x_6 & x_8 & x_8 & x_4 & x_6 \\
x_8 & x_4 & x_7 & x_8 & x_8 & x_3 & x_8 & x_7 & x_8 & x_5 & x_8 & x_1 & x_7 & x_8 & x_1 & x_5 & x_6 & x_8 & x_6 & x_8 & x_7 & x_7 & x_8 & x_3 & x_8 & x_7 & x_6 & x_8 & x_2 & x_2 & x_5 & x_4 \\
x_8 & x_8 & x_7 & x_8 & x_8 & x_6 & x_8 & x_7 & x_8 & x_3 & x_1 & x_8 & x_7 & x_8 & x_8 & x_3 & x_6 & x_5 & x_8 & x_6 & x_1 & x_2 & x_2 & x_4 & x_5 & x_8 & x_7 & x_3 & x_4 & x_7 & x_5 & x_8 \\
x_5 & x_7 & x_8 & x_7 & x_6 & x_8 & x_7 & x_8 & x_6 & x_1 & x_3 & x_7 & x_8 & x_7 & x_6 & x_8 & x_8 & x_5 & x_8 & x_2 & x_1 & x_4 & x_2 & x_8 & x_7 & x_8 & x_4 & x_3 & x_8 & x_8 & x_8 & x_5 \\
x_4 & x_8 & x_2 & x_8 & x_1 & x_6 & x_4 & x_7 & x_8 & x_5 & x_8 & x_8 & x_2 & x_8 & x_8 & x_3 & x_3 & x_8 & x_5 & x_8 & x_7 & x_7 & x_8 & x_5 & x_1 & x_7 & x_6 & x_8 & x_7 & x_7 & x_6 & x_8 \\
x_7 & x_3 & x_8 & x_5 & x_7 & x_1 & x_6 & x_8 & x_7 & x_8 & x_7 & x_3 & x_8 & x_6 & x_2 & x_8 & x_8 & x_7 & x_8 & x_5 & x_8 & x_8 & x_6 & x_4 & x_5 & x_8 & x_8 & x_7 & x_1 & x_4 & x_8 & x_2 \\
x_4 & x_8 & x_3 & x_8 & x_1 & x_7 & x_1 & x_6 & x_8 & x_7 & x_8 & x_8 & x_3 & x_8 & x_2 & x_2 & x_8 & x_7 & x_8 & x_8 & x_3 & x_6 & x_8 & x_7 & x_4 & x_5 & x_7 & x_8 & x_5 & x_6 & x_7 & x_8 \\
x_7 & x_5 & x_8 & x_3 & x_7 & x_8 & x_6 & x_4 & x_2 & x_8 & x_7 & x_6 & x_8 & x_3 & x_7 & x_8 & x_8 & x_2 & x_4 & x_6 & x_8 & x_8 & x_5 & x_8 & x_5 & x_1 & x_8 & x_7 & x_8 & x_8 & x_1 & x_7 \\
x_8 & x_4 & x_5 & x_8 & x_8 & x_2 & x_8 & x_6 & x_8 & x_7 & x_8 & x_1 & x_6 & x_8 & x_4 & x_7 & x_7 & x_8 & x_7 & x_8 & x_6 & x_5 & x_8 & x_2 & x_8 & x_5 & x_7 & x_8 & x_3 & x_3 & x_7 & x_1 \\
x_7 & x_5 & x_8 & x_5 & x_7 & x_8 & x_5 & x_8 & x_7 & x_1 & x_2 & x_6 & x_8 & x_6 & x_7 & x_8 & x_8 & x_7 & x_8 & x_3 & x_4 & x_1 & x_3 & x_8 & x_6 & x_8 & x_4 & x_2 & x_8 & x_8 & x_8 & x_7 \\
x_1 & x_8 & x_3 & x_8 & x_4 & x_7 & x_4 & x_5 & x_8 & x_7 & x_8 & x_8 & x_3 & x_8 & x_3 & x_8 & x_2 & x_2 & x_8 & x_7 & x_8 & x_6 & x_5 & x_8 & x_7 & x_1 & x_7 & x_8 & x_6 & x_5 & x_7 & x_8 \\
x_5 & x_2 & x_8 & x_7 & x_6 & x_4 & x_7 & x_8 & x_5 & x_8 & x_6 & x_2 & x_8 & x_7 & x_3 & x_8 & x_8 & x_6 & x_8 & x_7 & x_3 & x_8 & x_8 & x_7 & x_1 & x_7 & x_8 & x_8 & x_5 & x_1 & x_4 & x_8 & x_3 \\
x_1 & x_8 & x_2 & x_8 & x_4 & x_5 & x_1 & x_7 & x_8 & x_6 & x_8 & x_8 & x_2 & x_8 & x_8 & x_3 & x_3 & x_8 & x_6 & x_8 & x_7 & x_7 & x_8 & x_6 & x_4 & x_7 & x_5 & x_8 & x_7 & x_7 & x_5 & x_8 \\
x_6 & x_7 & x_8 & x_2 & x_5 & x_8 & x_7 & x_1 & x_3 & x_8 & x_6 & x_7 & x_8 & x_2 & x_6 & x_8 & x_8 & x_3 & x_4 & x_7 & x_8 & x_8 & x_7 & x_8 & x_7 & x_4 & x_8 & x_5 & x_8 & x_8 & x_1 & x_5 \\
x_8 & x_1 & x_7 & x_8 & x_8 & x_3 & x_8 & x_7 & x_8 & x_6 & x_8 & x_4 & x_7 & x_8 & x_4 & x_6 & x_5 & x_8 & x_5 & x_8 & x_7 & x_7 & x_8 & x_3 & x_8 & x_7 & x_5 & x_8 & x_2 & x_2 & x_6 & x_1 \\
x_8 & x_8 & x_5 & x_1 & x_8 & x_7 & x_8 & x_3 & x_1 & x_7 & x_8 & x_6 & x_8 & x_4 & x_6 & x_5 & x_8 & x_5 & x_4 & x_3 & x_8 & x_7 & x_7 & x_8 & x_6 & x_8 & x_8 & x_7 & x_3 & x_7 & x_5 & x_8 \\
x_3 & x_7 & x_4 & x_7 & x_3 & x_8 & x_2 & x_8 & x_5 & x_8 & x_5 & x_7 & x_1 & x_7 & x_6 & x_1 & x_4 & x_6 & x_8 & x_7 & x_8 & x_8 & x_7 & x_8 & x_2 & x_8 & x_8 & x_6 & x_8 & x_8 & x_8 & x_5 \\
x_8 & x_8 & x_7 & x_4 & x_8 & x_5 & x_8 & x_2 & x_1 & x_5 & x_8 & x_8 & x_7 & x_1 & x_8 & x_6 & x_5 & x_4 & x_3 & x_8 & x_7 & x_7 & x_8 & x_6 & x_8 & x_2 & x_6 & x_8 & x_7 & x_7 & x_3 & x_8 \\
x_2 & x_6 & x_4 & x_5 & x_2 & x_8 & x_3 & x_8 & x_7 & x_8 & x_7 & x_5 & x_1 & x_6 & x_7 & x_4 & x_1 & x_7 & x_8 & x_6 & x_8 & x_8 & x_5 & x_8 & x_3 & x_8 & x_8 & x_7 & x_8 & x_8 & x_8 & x_7 \\
x_8 & x_8 & x_6 & x_4 & x_8 & x_7 & x_8 & x_3 & x_4 & x_7 & x_8 & x_8 & x_5 & x_1 & x_8 & x_7 & x_7 & x_1 & x_2 & x_8 & x_6 & x_5 & x_8 & x_7 & x_8 & x_3 & x_7 & x_8 & x_5 & x_6 & x_2 & x_8 \\
x_6 & x_7 & x_8 & x_7 & x_5 & x_8 & x_5 & x_4 & x_3 & x_7 & x_8 & x_8 & x_6 & x_2 & x_4 & x_1 & x_2 & x_8 & x_7 & x_8 & x_8 & x_6 & x_7 & x_8 & x_1 & x_3 & x_8 & x_8 & x_8 & x_8 & x_6 & x_6 \\
x_7 & x_3 & x_8 & x_6 & x_7 & x_4 & x_5 & x_8 & x_7 & x_8 & x_7 & x_3 & x_8 & x_5 & x_2 & x_8 & x_8 & x_7 & x_8 & x_6 & x_8 & x_8 & x_5 & x_1 & x_6 & x_8 & x_8 & x_7 & x_4 & x_1 & x_8 & x_2 \\
x_6 & x_2 & x_8 & x_7 & x_5 & x_1 & x_7 & x_8 & x_6 & x_8 & x_5 & x_2 & x_8 & x_7 & x_3 & x_8 & x_8 & x_5 & x_8 & x_7 & x_8 & x_8 & x_7 & x_4 & x_7 & x_8 & x_8 & x_6 & x_4 & x_1 & x_8 & x_3 \\
x_2 & x_5 & x_1 & x_6 & x_2 & x_8 & x_3 & x_8 & x_7 & x_8 & x_7 & x_6 & x_4 & x_5 & x_7 & x_1 & x_4 & x_7 & x_8 & x_5 & x_8 & x_8 & x_6 & x_8 & x_3 & x_8 & x_8 & x_7 & x_8 & x_8 & x_8 & x_7 \\
x_3 & x_7 & x_1 & x_7 & x_3 & x_8 & x_2 & x_8 & x_6 & x_8 & x_6 & x_7 & x_4 & x_7 & x_5 & x_4 & x_1 & x_5 & x_8 & x_7 & x_8 & x_8 & x_7 & x_8 & x_2 & x_8 & x_8 & x_5 & x_8 & x_8 & x_8 & x_6 \\
x_8 & x_8 & x_7 & x_1 & x_8 & x_6 & x_8 & x_2 & x_4 & x_6 & x_8 & x_8 & x_7 & x_4 & x_8 & x_5 & x_6 & x_1 & x_3 & x_8 & x_7 & x_7 & x_8 & x_5 & x_8 & x_2 & x_5 & x_8 & x_7 & x_7 & x_3 & x_8 \\
x_7 & x_6 & x_8 & x_6 & x_7 & x_8 & x_6 & x_8 & x_7 & x_4 & x_2 & x_5 & x_8 & x_5 & x_7 & x_8 & x_8 & x_7 & x_8 & x_3 & x_1 & x_4 & x_3 & x_8 & x_5 & x_8 & x_1 & x_2 & x_8 & x_8 & x_8 & x_7
\end{bmatrix}$$

for some $x_1,\ldots,x_8 \in \mathbf{Z}$ corresponding to the decomposition of G into eight double cosets $H_1 g H_2$, consisting of $2,2,2,2,3,3,6,12$ right cosets of H_1, respectively. A (nontrivial) calculation finds that

$$\begin{aligned}
\det M = &-(2(x_2-x_3)^2+3(x_5-x_6)^2)^8 \\
&\cdot (2(x_1-x_4)+(x_5+x_6-2x_7))^6 \\
&\cdot (2(x_1+x_2+x_3+x_4)-(x_5+x_6+2x_7+4x_8))^3 \\
&\cdot (2(x_1-x_2-x_3+x_4)-(x_5+x_6+2x_7-4x_8))^3 \\
&\cdot (2(x_1-x_4)-3(x_5+x_6-2x_7))^2 \\
&\cdot (2(x_1+x_2+x_3+x_4)+3(x_5+x_6+2x_7+4x_8)) \\
&\cdot (2(x_1-x_2-x_3+x_4)+3(x_5+x_6+2x_7-4x_8)).
\end{aligned}$$

The assignment

$$x_1=x_2=1, \quad x_3=-1, \quad x_4=x_5=x_6=x_7=x_8=0$$

gives $\det M = 2^{32}$, while the assignment

$$x_5=1, \quad x_1=x_2=x_3=x_4=x_6=x_7=x_8=0$$

gives $\det M = 3^{12}$; thus $d(H_1,H_2)=1$. It follows that H_1 and H_2 are locally integrally equivalent, by Proposition 3.1. But no assignment of $x_1,\ldots,x_8 \in \mathbf{Z}$ makes $\det M = \pm 1$; indeed, any such assignment would require all 7 factors of $\det M$ listed above to have values in $\{\pm 1\}$, which is not possible. Thus H_1 and H_2 are not integrally equivalent; as noted in the introduction, this negatively answers Question 2.10 of Guralnick and Weiss in [18].

There are infinitely many nonisomorphic variations of this example; replacing $f_1(x)$ and $f_2(x)$ with $f_1(x\sqrt{T})$ and $f_2(x\sqrt{T})$ yields polynomials with Galois group G over $\mathbf{Q}(T)$; for almost all squarefree $a \in \mathbf{Z}$ the substitution $T=a$ yields nonisomorphic K_1, K_2 ramified at primes dividing a.

4.4 A degree 96 example of solvable equivalence

The results of §4.3 imply that any group G that contains nonconjugate solvably equivalent subgroups must have order at least $32 \cdot 60 = 1920$, since nonconjugate locally integrally equivalent subgroups must have index at least 32, and nonsolvable groups must have order at least 60. A search of the small groups database shows that there are no such G of order 1920 or 1980, and a search of transitive groups of degree up to 48 and order at most $48 \cdot 60 = 2880$ finds no such G, which implies a lower bound of 2940.

An exhaustive search of transitive groups of degree up to 48 and order at most 48,000 finds transitive groups of degrees 12, 16, 20, 24, 30, 32, 36, and 40 that contain nonconjugate solvably equivalent subgroups, including examples of index 96, 192, 384, 576, 672, and 768. The first example of index 96 occurs for the transitive group 16T1654 of order 5760, which is the smallest order we found. This group G contains five conjugacy classes of subgroups isomorphic to A_5, of which exactly two have representatives H_1 and H_2 with the property that every proper subgroup of H_1 is also a proper subgroup of H_2. The groups H_1 are thus solvably equivalent subgroups of index 96. There are 5 double cosets $H_1 g H_2$,

comprised of $5, 6, 10, 15, 60$ right cosets of H_1, respectively; each $M \in \text{Hom}_{\mathbf{Z}[G]}(\mathbf{Z}[H_1 \backslash G], \mathbf{Z}[H_2 \backslash G])$ can thus be viewed as a matrix in indeterminates $x_1, x_2, x_3, x_4, x_5 \in \mathbf{Z}$, and we have

$$\begin{aligned}
\det M = &- (5x_1 + 6x_2 + 10x_3 + 15x_4 + 60x_5) \\
&\cdot (x_1 - 6x_2 - 10x_3 + 3x_4 + 12x_5)^5 \\
&\cdot (3x_1 + 2x_2 - 2x_3 - 7x_4 + 4x_5)^{15} \\
&\cdot (3x_1 - 2x_2 + 2x_3 + x_4 - 4x_5)^{30} \\
&\cdot (x_1 + 2x_2 - 2x_3 + 3x_4 - 4x_5)^{45}
\end{aligned}$$

By solving 32 systems of linear equations, one finds that no assignment of $x_1, x_2, x_3, x_4, x_5 \in \mathbf{Z}$ makes every factor in $\det M$ equal to ± 1. Thus H_1 and H_2 are not integrally equivalent.

The regular inverse Galois problem for `16T1654` is known (it is a quotient of `12T277`), thus there are infinitely many pairs of solvably equivalent number fields K_1 and K_2 with Galois closure L that satisfy $\text{Gal}(L/\mathbf{Q}) = G$, $\text{Gal}(L/K_1) = H_1$, $\text{Gal}(L/K_2) = H_2$. For example, we may take L as the splitting field of

$$x^{16} - 2x^{15} + 3x^{14} - 16x^{13} + 18x^{12} - 10x^{10} + 40x^9 - 39x^8 + 54x^7 + 23x^6 + 16x^5 - 140x^4 - 188x^3 - 28x^2 + 104x - 4,$$

corresponding to the number field with LMFDB label `16.4.711702043399998895292416.2`. The field L contains solvable equivalent subfields K_1 and K_2 of degree 96 that are necessarily arithmetically equivalent, locally isomorphic, and have isomorphic class groups, by Proposition 3.7. One can find 190 examples of `16T1654` number fields in the Klüners and Malle Database of Number Fields [25].

Remark 4.3. In [42, Remark 4.3] Scott raises several questions related to integral permutation modules that lie in the same genus, which in our setting corresponds to local integral equivalence. The *rank* of a group G acting on a finite set Ω is the number of orbits of the diagonal action on $\Omega \times \Omega$. Scott shows that if the rank of G acting on Ω is 2 or 3 then local integral equivalence of $\mathbf{Z}[G]$-modules Ω and Ω' implies an isomorphism of G-sets [42, Proposition 4.1]. His example with $G = \mathbf{PSL}_2(29)$ proves that this does not hold when the rank is 8. The example in §4.4 shows that this also fails to hold when the rank is 5.

Acknowledgments

References

[1] Donu Arapura, Justin Katz, D.B. McReynolds, and P. Solapurkar, *Integral Gassmann equivalence of algebraic and hyperbolic manifolds*, Math. Z. **291** (2019), 179–214. (MR3936064) 2

[2] Alex Bartel and Aurel Page, *Torsion homology and regulators of isospectral manifolds*, J. Topology **9** (2016), 1237–1256. (MR3620456) 7

[3] Hans Ulrich Besche, Bettina Eick, and E.A. O'Brien, *The groups of order at most* 2000, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 1–4. (MR1826989) 6, 16

[4] Jeremy Booher and José-Felipe Voloch, *Recovering algebraic curves from L-function of Hilbert class fields*, Res. Number Theory **6** (2020), article no. 43. (MR4167327) 2

[5] Wieb Bosma, John J. Cannon, Claus Fieker, and Allan Steel (Eds.), *Handbook of Magma functions*, v2.25, 2020. 6, 16

[6] 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. (MR204107)) 16

[7] John J. Cannon and Derek Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008) 307–314. (MR2355702) 16

[8] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm, *Arithmetic equivalence for function fields, the Goss zeta function and a generalisation*, J. Number Theory **130** (2010), 1000–1012. (MR2600417) 2

[9] Gunther Cornelissen, Bart de Smit, Xin Li, Matilde Marcolli, and Harry Smit, *Characterization of global fields by Dirichlet L-series*, Res. Number Theory **5** (2019), article no. 7. (MR3887225) 2

[10] S.B. Conlon, *Monomial representations under integral similarity*, J. Algebra **13** (1969), 496–508. (MR0252527) 10

[11] 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. (MR1726087) 6

[12] Bart de Smit and Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. **31** (1994), 213–215. (MR1260520) 9

[13] Yuval Flicker, *Conjugacy classes of finite subgroups of* $\mathbf{SL}(2,F), \mathbf{SL}(3,F)$, J. Théor. Nombres Bordeaux **31** (2019), 555–571. (MR4102614) 12, 13, 14

[14] The GAP group, *GAP — Groups, Algorithms, and Programming*, Version 4.8.3, 2016. 6

[15] 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. 1, 6

[16] 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. (MR1136137) 2

[17] Robert M. Guralnick and David B. Wales, *Subgroups inducing the same permutation representation, II*, J. Algebra **96** (1985), 94–113. (MR0808843) 10

[18] Robert M. Guralnick and Al Weiss, *Transitive permutation lattices in the same genus and embedding groups*, Contemp. Math. **153** (1993), 21–33. (MR1247496) 3, 10, 14, 18

[19] Lorenz Halbeisen and Norbert Hungerbühler, *Generation of isospectral graphs*, J. Graph Theory **31** (1999), 255–265. (MR1688950) 2

[20] Derek Holt, Gordon Royle, Gareth Tracey, *The transitive groups of degree 48 and some applications*, Journal of Algebra, published online 29 June 2021. 16

[21] Alexander Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), 1–30. (MR2168238) 16

[22] Kenkichi Iwasawa, *On the rings of valuation vectors*, Ann. of Math. **57** (1953), 331–356. (MR0053970) 9

[23] Mark Kac, *Can one hear the shape of a drum?*, Amer. Math. Monthly **73** (1966) no. 4, 1–23. (MR0201237) 2

[24] Norbert Klingen, *Arithmetical similarities*, Oxford Science Publications, 1998. (MR1638821) 9, 11

[25] Jürgen Klüners and Gunter Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196. (MR1901356) 19

[26] Keiichi Komatsu, *On the adele rings of algebraic number fields*, Kodai Math. Sem. Rep. **28** (1976), 78–84. (MR0424760) 9

[27] Keiichi Komatsu, *On adele rings of arithmetically equivalent fields*, Acta Arith. **43** (1984), 93–95. (MR0736723) 6

[28] Benjamin Linowitz, D.B. McReynolds, and Nicholas Miller, *Locally equivalent correspondences*, Ann. Inst. Fourier (Grenoble) **67** (2017), 451–482. (MR3669503) 9

[29] The LMFDB Collaboration, *The L-functions and modular forms database*, 2021, available at www.lmfdb.org. 7

[30] Guillermo Mantilla-Soler, *On a question of Perlis and Stuart regarding arithmetic equivalence*, New York J. Math. **25** (2019), 558–573. (MR3982253). 3, 8, 16

[31] D.B. McReynolds, *Geometric spectra and commensurability*, Canad. J. Math. **67** (2015), 184–197. (MR3292699) 9

[32] J.S. Milne, *Fields and Galois theory*, v4.61, 2020, available at www.jmilne.org/math. 9

[33] John Milnor, *Eigenvalues of the Laplace operator on certain manifolds*, Proc. Natl. Acad. Sci. **51** (1964), 542. (MR162204) 2

[34] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999. (MR1697859) 8

[35] Robert Perlis, *On the equation $\zeta_k(s) = \zeta_{k'}(s)$*, J. Number Theory **9** (1977), 342–360. (MR0447188) 7, 8, 9

[36] Robert Perlis, *On the class numbers of arithmetically equivalent fields*, J. Number Theory **10** (1978), 489–509. (MR0515057) 6, 11

[37] Donna Joy Stuart and Rober Perlis, *A new characterization of arithmetic equivalence*, J. Number Theory **53** (1995), 300-308. (MR1348765) 3, 8, 9

[38] Dipendra Prasad, *A refined notion of arithmetically equivalent number fields and curves with isomorphic Jacobians*, Advances Math. **312** (2017), 198–208. (MR3635810) 2, 3, 11, 14

[39] Dipendra Prasad and Conjeeveram S. Rajan, *On an Archimedean analogue of Tate's conjecture*, J. Number Theory **99** (2003), 180–184. (MR1957251) 2

[40] Klaus W. Roggenkamp, *Permutation modules in the same genus, results from D. Hahn's Ph.D. thesis* (English summary), in *Darstellungstheorietage Jena 1996*, B. Kühlshammer and K. Rosenbaum, eds., Sitzungsber. Math.-Naturwiss. Kl., Akad. Gemein. Wiss. Erfurt, Erfurt, Germany, 1996, 211-223. (MR1441096) 3

[41] The Sage Development Team, *Sage Mathematics Software (Version 9.2)*, 2020, http://www.sagemath.org. 16

[42] Leonard L. Scott, *Integral equivalence of permutation representations*, in *Group theory (Granville, OH, 1992)*, 262–274, World Sci. Publ., 1993. (MR1348907) 2, 3, 10, 13, 19

[43] Jean-Pierre Serre, *Linear representations of finite groups*, Springer, 1977. (MR0450380) 6, 13

[44] Igor R. Shafarevich, *Basic algebraic geometry 2*, English third edition, Springer, 2013; translated from 2007 Russian third edition by Miles Reid. (MR3100288) 2

[45] Pavel Solomatin, *Global fields and their L-functions*, PhD Thesis, Universiteit Leiden, 2021. 2

[46] Harry Smit, *L-series and homomorphisms of number fields*, arXiv:1910.12321. 2

[47] Toshikazu Sunada, *Riemannian coverings and isospectral manifolds*, Ann. of Math. **121** (1985), 169–186. (MR0782558) 2

[48] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), 79 pages. (MR3482279) 3, 12, 13, 14

[49] Andrew V. Sutherland, *Arithmetic equivalence and isospectrality*, preprint, 2018. 2

[50] André Weil, *Exercices dyadiques*, Invent. Math. **27** (1974), 1–22. (MR0379445) 12

[51] Melanie Matchett Wood, *How to determine the splitting type of a prime*, 2011. 8

[52] David Zywina, *The inverse Galois problem for $\mathbf{PSL}_2(\mathbf{F}_p)$*, Duke Math. J. **164** (2015), 2253–2292. (MR3397386) 13

AUTHOR

Andrew V. Sutherland
Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, Massachusetts 02139
USA
drew@math.mit.edu
https://math.mit.edu/~drew