Strong arithmetic equivalence

Andrew V. Sutherland

Massachusetts Institute of Technology

June 23, 2017

Arithmetic Geometry, Cryptography, and Coding Theory

Centre International de Recontres Mathématiques

Arithmetic equivalence

Definition

Number fields K_1 and K_2 are arithmetically equivalent if $\zeta_{K_1}(s) = \zeta_{K_2}(s)$. The fields $K_1 \sim K_2$ must have the same degree and Galois closure L.

Let $G := \mathrm{Gal}(L/\mathbb{Q})$, $H_1 := \mathrm{Gal}(L/K_1)$, and $H_2 := \mathrm{Gal}(L/K_2)$.

Definition

A Gassmann triple (G, H_1, H_2) consists of finite groups $H_1, H_2 \leq G$ that satisfy $\#(H_1 \cap C) = \#(H_2 \cap C)$ for every G-conjugacy class C.

Theorem (Gassmann 1926)

$K_1 \sim K_2$ if and only if (G, H_1, H_2) is a Gassmann triple.

$K_1 \simeq K_2$ if and only if H_1 and H_2 are conjugate in G.

Examples

Let $G = \mathrm{GL}_2(\mathbb{F}_3)$, let $H_1 = \{\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right) \in G\}$, and let $H_2 = \{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \in G\}$. Then (G, H_1, H_2) is a non-trivial Gassmann triple (de Smit, ANTS III).

Let $E/\mathbb{Q}$ be an elliptic curve with surjective mod-3 Galois image and let $L = \mathbb{Q}(E[3])$. then $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$ and the fields $K_1 := L^{H_1}$ and $K_2 = L^{H_2}$ are non-conjugate arithmetically equivalent number fields of degree 8.

This example generalizes: one can replace p with any odd degree, and the matrix entry 1 can be replaced squares in $\mathbb{F}_p$; the degree is $2p + 2$.

One can achieve degree 7 using similar subgroups of $\mathrm{SL}_3(\mathbb{F}_2)$, which is best possible (Bosma–de Smit, ANTS V, de Smit–Lenstra 2000).

The subgroups H_1 and H_2 need not be isomorphic; for example, take $G \simeq [384, 3755]$, $H_1 \simeq [16, 3]$, $H_2 \simeq [16, 10]$ (in GAP notation).

Gassmann triples in other contexts

Gassmann triples (G, H_1, H_2) arise in many other contexts involving potentially non-isomorphic objects with the same "zeta function":

- If $\pi : M \to M_0$ is a normal finite Riemannian covering with deck group G then M/H_1, and M/H_2 are isospectral (Sunada 1985).
- If Γ is a finite graph with $G = \mathrm{Aut}(\Gamma)$ then Γ/H_1 and Γ/H_2 are isospectral (Halbeisen–Hungerbühler 1995).
- If X/k is a projective curve with $G = \mathrm{Aut}(X)$, then X/H_1 and X/H_2 have isogenous Jacobians (Prasad–Rajan 2003).
- If $\pi : X \to Y$ is a Galois étale cover of k-varieties then X/H_1 and X/H_2 have isomorphic Chow motives (Arapura et al. 2017).

Unlike the number field case, non-trivial Gassmann triples may give rise to isomorphic objects (imposing further conditions prevents this).

Characterizations of Gassmann triples

Let $[G/H]$ be the transitive G-set consisting of cosets of H.
Let $\chi_H\colon G \to \mathbb{Z}$ be the permutation character $g \mapsto \#[G/H]^g$, and for $K \le G$ define $\chi_H(K) := \#[G/H]^K$. We then have

$$\chi_H(K) \neq 0 \iff K \le_G H$$

(indeed, $HgK = Hg \iff gKg^{-1} \subseteq H$).

Proposition

For $H_1, H_2 \le G$ the following are equivalent:

1. $\#(H_1 \cap C) = \#(H_2 \cap C)$ *for all* $C \in \mathrm{conj}(G)$.
2. *There is a G-conjugacy preserving bijection* $H_1 \leftrightarrow H_2$.
3. $\chi_{H_1}(K) = \chi_{H_2}(K)$ *for all cyclic subgroups* $K \le G$ *(or all* $K \le H_1, H_2$*).*
4. $\mathbb{Q}[G/H_1] \simeq \mathbb{Q}[G/H_2]$ *(as* $\mathbb{Q}[G]$ *modules).*

How strong is arithmetic equivalence?

Let K_1 and K_2 be arithmetically equivalent number fields.

Theorem (Perlis 1977)

The number fields K_1 and K_2 have the same degree, discriminant, signature, and roots of unity.

The analytic class number formula

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

implies $R_{K_1}h_{K_1} = R_{K_2}h_{K_2}$ but the class numbers and regulars may differ.

There is a bijection of the places of K_1 and K_2 that preserves residue field degrees, but not necessarily ramification indices.

The adèle rings and idèle groups of K_1 and K_2 need not be isomorphic.

Stronger notions of arithmetic equivalence

Definition

Two number fields are locally isomorphic if there is a bijection of there places such that corresponding completions are isomorphic.

Locally isomorphic fields are arithmetically equivalent (Klingen 1998).

Proposition (Iwasawa 1953)

Two number fields K_1, K_2 are locally isomorphic if and only if they have isomorphic rings of adèles $\mathbb{A}_{K_1} \simeq \mathbb{A}_{K_2}$.

Proposition (Linowitz–McReynolds–Miller 2017)

Locally isomorphic number fields have isomorphic Brauer groups.

But locally isomorphic fields may have distinct class numbers, as happens with $\mathbb{Q}(\sqrt[8]{-33})$ and $\mathbb{Q}(\sqrt[8]{-33 \cdot 16})$ (de Smit–Perlis, 1994).

Local integral equivalence

A finite group K is p-cyclic (or p-hypoelementary) if the quotient of K by the intersection of its p-Sylow subgroups (its p-core) is cyclic.

Proposition

Let p be a prime. For $H_1, H_2 \leq G$ the following are equivalent:

- $\chi_{H_1}(K) = \chi_{H_2}(K)$ *for all p-cyclic $K \leq G$ (or all $K \leq H_1, H_2$);*
- $\mathbb{Z}_p[G/H_1] \simeq \mathbb{Z}_p[G/H_2]$;
- $\mathbb{F}_p[G/H_1] \simeq \mathbb{F}_p[G/H_2]$;
- $\det(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])) \not\subseteq p\mathbb{Z}$.

If $\mathbb{Z}_p[G/H_1] \simeq \mathbb{Z}_p[G/H_2]$ for all p we have local integral equivalence.

Theorem (Perlis 1978)

Number fields K_1, K_2 corresponding to a locally integrally equivalent $H_1, H_2 \leq G$ have isomorphic class groups.

Integral equivalence

Definition

Subgroups $H_1, H_2 \leq G$ are integrally equivalent if $\mathbb{Z}[G/H_1] \simeq \mathbb{Z}[G/H_2]$.

Let $H_1, H_2 \leq G$ have index n, let $\rho_1, \rho_2 \colon G \to S_n$ be the representations corresponding to the permutation modules $\mathbb{Z}[G/H_1]$, $\mathbb{Z}[G/H_2]$.

Fix an ordering of $[G/H_1]$ and $[G/H_2]$. We may represent elements of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])) \not\subseteq p\mathbb{Z}$ by matrices $M \in \mathbb{Z}^{n\times n}$ that satisfy

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

Our two notions of integral equivalence are distinguished by:

- local integral equivalence: $\gcd(\det(M_1), \ldots, \det(M_r)) = 1$ for some $M_1 \ldots, M_r \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$.
- global integral equivalence: $\det(M) = \pm 1$ for some $M \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$.

What we know about integral equivalence

Theorem (Prasad 2017)

Let $\pi : X \to Y$ be a Galois cover of nice curves over k with Galois group G. If $H_1.H_2 \leq G$ are integrally equivalent then $\mathrm{Jac}(X/H_1) \simeq \mathrm{Jac}(X/H_2)$.

Remark: Infinite families of non-isomorphic curves of low genus with isomorphic Jacobians were previously known (Howe 2005).

Essentially only one non-trivial example of integral equivalence is known: $G = \mathrm{PSL}_2(\mathbb{F}_{29})$ with $H_1, H_2 \simeq A_5$ non-conjugate of index 203.

This example is due to Leonard Scott, who proved it by explicitly exhibiting $M \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2]) \subseteq \mathbb{Z}^{203\times 203}$ with $\det M = 1$.

Similar triples exist for $p \equiv \pm 29 \bmod 120 \ldots$
$\ldots$ but for $p = 149$ we already have to work with $M \in \mathbb{Z}^{27565\times 27565}$.

What we don't know about integral equivalence

Question 1: Must integrally equivalent $H_1, H_2 \leq G$ be isomorphic? How about locally integrally equivalent $H_1, H_2 \leq G$?

Both necessarily hold if $G = \mathrm{PSL}_2(\mathbb{F}_p)$. In fact, Gassmann equivalent subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$, $\mathrm{SL}_2(\mathbb{F}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$ are isomorphic (S 2016).

Scott's triple gives rise to infinitely many arithmetically equivalent number non-isomorphic number fields of degree 203 that are also locally isomorphic, hence have isomorphic adèle rings.

But (as noted by Prasad), is is not clear that integral equivalence alone guarantees that we will get locally isomorphic number fields.

Question 2: Do locally integrally equivalent $H_1, H_2 \leq G$ give rise to locally isomorphic number fields? If not, does integral equivalence?

Solvable integral equivalence

Definition

Subgroups $H_1, H_2 \leq G$ are solvably equivalent if $\chi_{H_1}(K) = \chi_{H_2}(K)$ for all solvable subgroups $K \leq G$.

Like integral equivalence, solvable equivalence obviously implies local integral equivalence (hence isomorphic class groups).

Proposition

Number fields K_1, K_2 corresponding to solvably equivalent $H_1, H_2 \leq G$ are arithmetically equivalent, locally isomorphic, and have the same class number. Moreover, there is a bijection of the places of K_1 and K_2 that preserves residue degrees and ramification indices.

Remark: Solvable equivalence is stronger than necessary

Results

Proposition

There are infinitely many non-isomorphic pairs of degree 32 number fields arising from locally (not globally) integrally equivalent $H_1, H_2 \leq G$.

Proposition

There are infinitely many non-isomorphic pairs of degree 96 number fields arising from solvably (not integrally) equivalent $H_1, H_2 \leq G$.

These results are effective; we can construct explicit examples.

The fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ contains non-conjugate solvably equivalent subgroups H_1, H_2 for all primes $p \equiv \pm 29 \bmod 120$ implies that there are infinitely many non-isomorphic pairs of number fields arising from infinitely many solvably equivalent $H_1, H_2 \leq G$, but the degrees of these fields is at least 203 and they hard to construct explicitly.

First example

An exhaustive search of the 11,759,892 groups of order less than 1024 finds exactly 74 groups G that contain non-conjugate locally integrally equivalent subgroups H_1, H_2.

The smallest two have GAP ids $[384, 18050]$ and $[384, 18046]$, isomorphic to transitive permutation groups `32T9403` and `32T9408`. Both are 2-extensions of $D_4 \times S_4$, which makes it easy to construct explicit examples.

For instance, the polynomials

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

both have Galois group $G =$`32T9403`. They define non-isomorphic fields K_1, K_2 corresponding to locally integrally equivalent $H_1, H_2 \leq G$.

First example (continued)

We can view each $M \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$ as 32×32 matrix with entries $x_1, \ldots, x_8 \in \mathbb{Z}$. corresponding to the decomposition of G into eight double cosets $H_1 g H_2$. A (non-trivial) calculation finds that

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

One can choose the x_i so that $\det M = 2^{32}$, and so that $\det M = 3^{12}$. Thus H_1 and H_2 are locally integrally equivalent, but they not integrally equivalent because there is no choice of the x_i for which $\det M = \pm 1$.

This negatively answers a question of Guralnick–Weiss from 1993.

Second example

Let $G = \texttt{16T1654}$ of order 5760. It contains non-conjugate $H_1, H_2 \simeq A_5$ of index 96 such that every proper subgroup of H_1 is a proper subgroup of H_2.

The group G is the Galois group of an extension of $\mathbb{Q}[T]$; Hilbert irreducibility gives infinitely many examples of corresponding number fields, including:

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

Each $M \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H_1], \mathbb{Z}[G/H_2])$ has entries $x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}$, and

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

No assignment of $x_1, x_2, x_3, x_4, x_5 \in \mathbb{Z}$ makes every factor in $\det M$ equal to ± 1, so H_1 and H_2 are not integrally equivalent.