Pair Arithmetical Equivalence for Quadratic Fields

Joint work with Zeev Rudnick

Upstate New York Online Number Theory Colloquium

October 11, 2021

Winnie Li

Pennsylvania State University

Arithmetical equivalence of fields

The Riemann zeta function is

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}, \quad \Re(s) > 1.$$

Let K be a finite extension of $\mathbb{Q}$. Each nonzero prime ideal $\mathfrak{P}$ in the ring of integers $\mathbb{Z}_K$ divides a unique prime p, and it has finite index $N(\mathfrak{P})$ in $\mathbb{Z}_K$. The Dedekind zeta function of K is

$$\zeta_K(s) = \prod_{p \text{ prime}} \prod_{\mathfrak{P}|(p)} \frac{1}{1 - N(\mathfrak{P})^{-s}}, \quad \Re(s) > 1.$$

Two number fields K_1 and K_2 are *arithmetically equivalent*
$\Leftrightarrow \zeta_{K_1}(s) = \zeta_{K_2}(s)$
$\Leftrightarrow$ For each p, there is a norm preserving bijection from prime ideals of K_1 dividing p to those of K_2.

Gassmann criterion for arithmetical equivalence

Theorem. Let K be a finite Galois extension of $\mathbb{Q}$ containing K_1, K_2. Let H_i, $i = 1, 2$, be two subgroups of $G = Gal(K/\mathbb{Q})$ with fixed field K_i (so that $H_i = Gal(K/K_i)$). TFAE:

(1) $\zeta_{K_1}(s) = \zeta_{K_2}(s)$, i.e., K_1 and K_2 are arithmetically equiv;

(2) H_1 and H_2 are *locally conjugate* in G, i.e., for each conjugacy class $\mathcal{C}$ of G,

$$\#(\mathcal{C} \cap H_1) = \#(\mathcal{C} \cap H_2);$$

(3) The representation induced from 1_{H_1} to G is isomorphic to that from 1_{H_2} to G, i.e., $\mathrm{Ind}_{H_1}^G 1_{H_1} \simeq \mathrm{Ind}_{H_2}^G 1_{H_2}$.

Moreover, K_1 and K_2 are isomorphic if and only if H_1 and H_2 are conjugate in G.

An example of arith. equiv. but non-isomorphic pair of fields

Example [F. Gassmann 1926].

$$G = \text{the permutation group } S_6 \text{ on 6 letters},$$

$$H_1 = \{id, (12)(34), (13)(24), (14)(23)\},$$

$$H_2 = \{id, (12)(34), (12)(56), (34)(56)\}.$$

Arithmetically solitary

K is called *arithmetically solitary* if $\zeta_K = \zeta_F \Rightarrow K \simeq F$.

Ex. Finite Galois extensions of $\mathbb{Q}$ are arithmetically solitary.

The above example, discovered by Gassmann in 1926, gives the first pair of non-solitary fields of degree 180 which are arithmetically equivalent.

Perlis showed that all number fields K with $[K : \mathbb{Q}] \leq 6$ are arithmetically solitary, and constructed a non-solitary field of degree 7.

Artin L-functions

- K: a number field
- $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$: the absolute Galois group of K
- χ: a finite order character of G_K
- The Artin L-function attached to χ is

$$L(s,\chi,K) = \prod_{\text{prime ideal } \mathfrak{P}\subset\mathbb{Z}_K,\ \mathfrak{P}\nmid \mathrm{cond}(\chi)} \frac{1}{1-\chi(Frob_{\mathfrak{P}})N(\mathfrak{P})^{-s}} ,$$

which converges absolutely for $\Re s > 1$.

A variant of arith. equiv.

Klüners and Nicolae considered the Artin L-functions of two finite order characters χ_1 and χ_2 of $G_{\mathbb{Q}}$, and showed

$$L(s, \chi_1, \mathbb{Q}) = L(s, \chi_2, \mathbb{Q}) \Rightarrow \chi_1 = \chi_2.$$

They also showed that if the base field is not $\mathbb{Q}$, this need not be true.

One such example is the base field $K = \mathbb{Q}(\sqrt[4]{3})$, χ_i being the quadratic character of $\mathrm{Gal}(K_i/K)$, where $K_1 = \mathbb{Q}(\sqrt[8]{3})$ and $K_2 = \mathbb{Q}(\sqrt[8]{16 \cdot 3})$ over K.

Pair arithmetical equivalence

Given two non-isomorphic number fields K and M, let χ and η be two finite order characters of G_K and G_M respectively.

Definition. Two distinct pairs (χ, K) and (η, M) are called *arithmetically equivalent*, denoted $(\chi, K) \sim (\eta, M)$, if the associated Artin L-functions coincide:

$$L(s, \chi, K) = L(s, \eta, M).$$

Observations. (1) $(\chi, K) \sim (\eta, M) \Rightarrow [K : \mathbb{Q}] = [M : \mathbb{Q}]$.

(2) If χ and η are trivial, then $(\chi, K) \sim (\eta, M)$ is the same as K and M arith. equiv.

Connection with dihedral modular forms

- Identify a finite order char. χ of G_K with a finite order idele class char. (or Hecke Grossenchar.) of K by class field theory.
- For K quadratic over $\mathbb{Q}$, there is a unique normalized automorphic Hecke-eigenform g_χ of $GL(2)$ over $\mathbb{Q}$, which is cuspidal iff χ is not self-conjugate, with

$$L(s, g_\chi) = L(s, \chi, K).$$

- g_χ corresponds to the 2-dim'l dihedral rep'n $\rho_\chi := \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \chi$ of $G_{\mathbb{Q}}$.
- If ρ_χ is odd, i.e., $\det \rho_\chi(c) = -1$ at the complex conjugation c, then g_χ is a holomorphic weight one modular form on the

upper half-plane, with Fourier expansion (if cuspidal)

$$g_\chi(z) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z},$$

summing over ideals $0 \neq \mathfrak{a} \subset \mathbb{Z}_K$ coprime to $\mathrm{cond}(\chi)$.

- If ρ_χ even, i.e., $\det \rho_\chi(c) = 1$, then $\rho_\chi(c) = \pm I_2$, in which case g_χ is a Maass form with Laplacian eigenvalue $1/4$, and has Fourier expansion (if cuspidal)

$$\begin{aligned} &g_\chi(z) \\ &= \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \sqrt{y} K_0(2\pi N(\mathfrak{a}) y) 2 \begin{cases} \cos(2\pi N(\mathfrak{a}) x), & \text{if } \rho_\chi(c) = I_2; \\ \sin(2\pi N(\mathfrak{a}) x), & \text{if } \rho_\chi(c) = -I_2. \end{cases} \end{aligned}$$

Here K_0 is the K-Bessel function.

- If $(\chi, K) \sim (\eta, M)$ for distinct quadratic extensions K and M, then the modular form $g_\chi = g_\eta$ arises from Hecke characters of two different fields.

  An example was first found by Hecke with $K = \mathbb{Q}(\sqrt{-1})$, $M = \mathbb{Q}(\sqrt{-3})$, χ and η quadratic characters.

- Rohrlich (2015) encountered such pairs when he studied the number $\vartheta^{im}(x)$ of isom. classes of irreducible ρ_χ with conductor bounded by x:

$$\vartheta^{im}(x) \sim \kappa x^2,$$

  where

$$\kappa = \frac{\pi}{2} \sum_{K \text{ imag. quad}} |d_K|^{-5/2} \zeta_K(0)^2 / \zeta_K(2)^2.$$

Pair arith. equiv. for quadratic extensions of $\mathbb{Q}$

Let K be a quadratic extension of $\mathbb{Q}$. Shall consider

Question 1.[existence] Characterize finite order characters χ of G_K such that $(\chi, K) \sim (\eta, M)$ for another pair (η, M).

If so, there is a third pair (ξ, N), where N is the third quad. extension contained in the biquadratic extension KM.

Question 2.[construction] Explicitly construct finite order characters of G_K (or idele class characters of K).

Question 3. [classification] Classify quadratic χ in Q1.

Re-interpretation of pair arith. equiv.

Interpret the equality

$$L(s,\chi,K) = L(s,\eta,M)$$

on L-functions of characters as the equality

$$L(s,\mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}\chi) = L(s,\mathrm{Ind}_{G_M}^{G_{\mathbb{Q}}}\eta)$$

on L-functions of induced degree-two representations $\rho_\chi = \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}\chi$ and $\rho_\eta = \mathrm{Ind}_{G_M}^{G_{\mathbb{Q}}}\eta$ of the Galois group $G_{\mathbb{Q}}$.

This converts the problem on pair arithmetical equivalence to a problem on isomorphism of induced representations, similar to Gassmann's criterion.

Self-conjugacy

Suppose $\mathrm{Gal}(K/\mathbb{Q}) = \langle c \rangle$. The conjugate of a char. χ of G_K is $\chi^c(g) = \chi(c^{-1}gc)$ for $g \in G_K$.

By class field theory,
$\chi = \chi^c$ is self-conjugate if and only if it comes from base change
$\Leftrightarrow$ there is a char. μ of $G_{\mathbb{Q}}$ such that

$$L(s, \chi, K) = L(s, \mu, \mathbb{Q}) L(s, \mu\delta_{K/\mathbb{Q}}, \mathbb{Q}),$$

where $\delta_{K/\mathbb{Q}}$ is the quadratic char. associated to $K/\mathbb{Q}$.

In this case the induced representation $\rho_\chi = \mu \oplus \mu\delta_{K/\mathbb{Q}}$ is reducible and g_χ is an Eisenstein series. Such (χ, K) is solitary since K is determined by the ratio of the two chars, and $\chi = \mu|_{G_K} = \mu\delta_{K/\mathbb{Q}}|_{G_K}$.

Shall assume χ not self-conjugate.

A criterion for pair arith. equiv.

Thm. *Let K be a quadratic extension of $\mathbb{Q}$ with $Gal(K/\mathbb{Q}) = \langle c \rangle$. Suppose a finite order character χ of G_K is not equal to its conjugate χ^c. Then*

(a) (χ, K) *is arithmetically equivalent to another pair*

$\Leftrightarrow$

(b) $\chi^c = \chi \cdot \delta$ *for a quadratic character δ of G_K.*

Two reductions:

- Suffices to consider χ up to base change;
- May assume the order of χ is a power of 2.

Study the conductor of such χ.

Explicit construction of χ

We construct such χ for

(i) $K = \mathbb{Q}(\sqrt{-p})$ where p is prime, $p \equiv 3 \bmod 4$ or $p = 2$, and $K = \mathbb{Q}(\sqrt{-1})$. (These are the imaginary quadratic fields with odd class number.)

(r) $K = \mathbb{Q}(\sqrt{q})$ where $q \equiv 1 \bmod 4$ is prime or $q = 2$. (These are the real quadratic fields with odd class number and containing a unit with norm -1.)

Prop. *For K as above, let $\mathfrak{A}$ be a nonzero ideal of $\mathbb{Z}_K$ and ξ a primitive character of $(\mathbb{Z}_K/\mathfrak{A})^\times$ of order 2^e for an integer $e \geq 1$ such that $\xi((\mathbb{Z}_K)^\times) = 1$ for K imaginary and $\xi((\mathbb{Z}_K)^\times) \subset \{\pm 1\}$ for K real. Then there is a unique idele class char. χ of K with cond$(\chi) = \mathfrak{A}$ and order 2^e extending ξ.*

Classification of quadratic χ up to base change

We classify quadratic characters χ up to base change for K satisfying (i) or (r), and determine possible conductors.

Note that for χ quadratic, $\chi \neq \chi^c$ if and only if χ and χ^c differ by a quadratic character; therefore we have classified, for such K, all pairs (χ, K) with quadratic χ arithmetically equivalent to another pair.

To give a flavor, we state one case. Other cases are similar.

Thm. *Let $K = \mathbb{Q}(\sqrt{-1})$. For each prime $p \equiv 1 \bmod 4$, choose one prime v of K above p and let S_K be the collection of these chosen primes. Then*

(I) *Up to multiplication by characters from base change, a quadratic idele class character* χ *of* K *with conductor* $\mathfrak{f} = \prod_{v \text{ prime}} v^{m(v)}$ *satisfies the conditions*

(A) *None of primes above* $p \equiv 3 \bmod 4$ *divide* $\mathfrak{f}$*;*

(B) *If a prime* v *above* $p \equiv 1 \bmod 4$ *divides* $\mathfrak{f}$*, then* $v \in S_K$ *and* $m(v) = 1$*;*

(C) *If a prime* v *above* 2 *divides* $\mathfrak{f}$*, then* $m(v) = 2$ *or* 5*. Further* $\chi_v(\sqrt{-1}) = -1$ *if* $m(v) = 2$*, and* $\chi_v(1 + \pi_v^3) = 1$ *if* $m(v) = 5$*. Here* $\pi_v = \sqrt{-1} - 1$*.*

(II) *Any quadratic idele class character* χ *of* K *with non-trivial conductor* $\mathfrak{f}$ *satisfying (A)-(C) does not arise from base change.*

(III) *No two distinct quadratic idele class characters of K satisfying (A)-(C) differ by a character from base change.*

(IV) *Let* $\mathfrak{f} = \prod_{v \text{ prime}} v^{m(v)}$ *be an integral ideal of K satisfying (A)-(C). Let*

$$r(\mathfrak{f}) = \#\{v|\mathfrak{f} \ : \ v \textit{ is above a prime } p \equiv 5 \mod 8\}.$$

Then there is a quadratic idele class character χ of K with conductor $\mathfrak{f}$ satisfying the conditions (A)-(C) if and only if

- $r(\mathfrak{f})$ *is even if no $v|\mathfrak{f}$ is above 2,*
- $r(\mathfrak{f})$ *is odd if there is a prime $v|\mathfrak{f}$ above 2 with $m(v) = 2$,*
- *no condition on $r(\mathfrak{f})$ if there is a prime $v|\mathfrak{f}$ above 2 with $m(v) = 5$.*

Examples of holo. wt 1 cusp form arising from two different fields

Let $K = \mathbb{Q}(\sqrt{-1})$. Let q be a prime $\equiv 1 \mod 8$, and $\mathfrak{Q}$ a prime of K above q.

Let ξ be the quadratic char. of $(\mathbb{Z}_K/\mathfrak{Q})^\times \simeq (\mathbb{F}_q)^\times$. Then $\xi(\sqrt{-1}) = 1$. By Prop., there is a unique quadratic idele class character χ of K with $\mathrm{cond}(\chi) = \mathfrak{Q}$ lifting ξ. Have $\chi \neq \chi^c$. So $(\chi, K) \sim (\eta, M)$ for some pair (η, M).

The induced rep'n ρ_χ has conductor $4q$. Take $M = \mathbb{Q}(\sqrt{q})$ in which 2 splits. In order that ρ_η has conductor $4q$, and η not self-conjugate with $\mathrm{cond}(\eta) = \mathfrak{T}^2$ for a prime $\mathfrak{T}$ of M above 2.

Let η be the lifting of the quadratic character of $(\mathbb{Z}_M/\mathfrak{T}^2)^\times$. Check that $\rho_\chi = \rho_\eta$ is odd so that $g_\chi = g_\eta$ is holomorphic of weight 1, and cuspidal.

Examples of Maass cusp forms arising from two different fields

Let $K = \mathbb{Q}(\sqrt{t})$ and $M = \mathbb{Q}(\sqrt{q})$, where $t \neq q$ are primes $\equiv 1 \bmod 4$ such that the Legendre symbol $(\frac{q}{t}) = (\frac{t}{q}) = 1$. Suppose $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$ and $\mathrm{Gal}(M/\mathbb{Q}) = \langle \tau \rangle$.

By choice $(q) = \mathfrak{Q} \cdot \sigma(\mathfrak{Q})$ splits in K and $(t) = \mathfrak{T} \cdot \tau(\mathfrak{T})$ splits in M. Let χ be the unique quadratic idele class char. of K with conductor $\mathfrak{Q}$. One checks that

$$\chi^\sigma = \chi \cdot \delta_{KM/M}.$$

So $L(s, \chi, K) = L(s, \eta, M)$ for some char. η of G_M. By checking the conductor of ρ_χ, we may choose η to be the unique quadratic char. of G_M with conductor $\mathfrak{T}$. It is not self-conjugate and ρ_η is even.

Then $g = g_\chi = g_\eta$ is a Maass cusp form. There are two possibilities for its Fourier expansion, depending on $\rho_\chi(c) = \pm I_2$. The sign for $\rho_\chi(c)$ is given by the sign of

$$\chi_{\mathfrak{Q}}(\epsilon_K) \equiv \epsilon_K^{(N(\mathfrak{Q})-1)/2} \mod \mathfrak{Q},$$

where ϵ_K is a fundamental unit of K with norm -1. As shown from the examples below, both signs can occur.

Ex 1. $t = 5$ and $q = 29$. Then $(\frac{5}{29}) = 1$. The field $K = \mathbb{Q}(\sqrt{5})$ has class number 1 with a fundamental unit

$$\epsilon_K = \frac{1+\sqrt{5}}{2}$$

of norm -1. Have $(29) = \mathfrak{Q} \cdot \sigma(\mathfrak{Q})$ where

$$\mathfrak{Q} = (7 + 2\sqrt{5}).$$

One computes $\chi_{\mathfrak{Q}}(\epsilon_K) = +1$ so that $\rho_\chi(c) = I_2$.

Ex 2. $t = 5$ and $q = 41$, and $K = \mathbb{Q}(\sqrt{5})$. Have $(41) = \mathfrak{Q} \cdot \sigma(\mathfrak{Q})$ with

$$\mathfrak{Q} = (6 + \frac{1 + \sqrt{5}}{2}).$$

One finds $\chi_{\mathfrak{Q}}(\epsilon_K) = -1$ in this case so that $\rho_\chi(c) = -I_2$.

Other variants of arith. equiv.

- Two compact Riemannian manifolds are called isospectral if they have the same Laplacian eigenvalues. People constructed isospectral but non-isometric pairs. Eg., Milnor (1964), Vignéras (1982), Sunada (1985), Gordon-Webb-Wolpert (1991)
- Similarly, in graph theory, people considered pairs of finite non-isomorphic graphs with the same spectrum.
- Using Gassmann method, Prasad-Rajan (2003) constructed curves with isogenous Jacobians, Prasad (2017) constructed curves with isomorphic Jacobians, and Arapura et al (2017) constructed varieties with the same Chow motives.

Thank you!