Reconstructing global fields and elliptic curves

using Dirichlet L-series

Harry Smit
h.j.smit@uu.nl

Utrecht University

joint with: Gunther Cornelissen
Bart de Smit
Xin Li
Matilde Marcolli

ArXiv: 1706.04515
1706.04517

Introduction

Games

Large difference between poker and chess: chess has perfect information for both players, while poker does not.

Professional poker players try to reconstruct their opponent's hand by assigning probabilities to each option.

Playing poker in number theory: reconstruction problems

A very general and vague question.

To what extent does an invariant determine its underlying object?

Number of primes is a very interesting invariant

The zeta function of a number field K is an invariant counts the number of primes of K of a certain norm:

$$\zeta_K(s) = \sum_{I \in \mathcal{I}_K} \frac{1}{\mathbb{N}I^s}.$$

Number of primes is a very interesting invariant

The zeta function of a number field K is an invariant counts the number of primes of K of a certain norm:

$$\zeta_K(s) = \sum_{I \in \mathcal{I}_K} \frac{1}{\mathbb{N}I^s}.$$

Question.

Is a number field K completely determined by the number of primes in K? More precisely, does $\zeta_K = \zeta_L$ imply $K \simeq L$?

Number of primes is a very interesting invariant

The zeta function of a number field K is an invariant counts the number of primes of K of a certain norm:

$$\zeta_K(s) = \sum_{I \in \mathcal{I}_K} \frac{1}{\mathbb{N}I^s}.$$

Question.

Is a number field K completely determined by the number of primes in K? More precisely, does $\zeta_K = \zeta_L$ imply $K \simeq L$?

Theorem. (Bauer)

Let K, L be number fields such that $L/\mathbb{Q}$ is Galois. If $\mathsf{Spl}_1(M/\mathbb{Q}) \subseteq \mathsf{Spl}(L/\mathbb{Q})$, then $L \subseteq M$.

Corollary of Chebotarev.

Let K, L be number fields. If $\mathsf{Spl}(K/\mathbb{Q}) = \mathsf{Spl}(L/\mathbb{Q})$, then the Galois closures of K and L are the same.

Gaßmann shatters the dream

Theorem. (Gaßmann, 1926)

There exist non-isomorphic number fields with equal zeta functions.

Example: $\mathbb{Q}(\sqrt[8]{3})$ and $\mathbb{Q}(\sqrt[8]{3} \cdot \sqrt{2})$.

Moreover, Gaßmann gave a group theoretic equivalent condition for two number fields being arithmetically equivalent (i.e. $\zeta_K = \zeta_L$).

Adding information on the ramified localisations does not help

Theorem. (Komatsu, 1976)

There exist non-isomorphic number fields the same zeta function and isomorphic localisations (i.e. isomorphic adele rings).

Example: $\mathbb{Q}(\sqrt[8]{2 \cdot 9})$ and $\mathbb{Q}(\sqrt[8]{2^5 \cdot 9})$.

Another approach: extensions of a global field

Neukirch-Uchida theorem. (Neukirch 1969, Uchida 1972)

Let K, L be global fields such that $G_K \simeq G_L$. Then $K \simeq L$. Moreover, $\mathsf{Aut}(K) \simeq \mathsf{Out}(G_K, G_K)$.

One of the proof ideas: find the decomposition groups in G_K and create a prime bijection from this.

Remark.

One cannot replace G_K by its abelianisation.

A one-sentence summary of this talk so far

Summary.

Prime bijections do not suffice for field isomorphisms,
but *meaningful* ones do.

Another meaningful prime bijection

Dirichlet characters: a generalisation to number fields

Definition. (Dirichlet character)

Let K be a number field. The group of Dirichlet characters $X(K)$ is the set of continuous homomorphisms $G_K \to \mathbb{C}^\times$ (with respect to the discrete topology on $\mathbb{C}^\times$).

Every character factors through a finite cyclic extension K_χ (i.e. a Galois extension with cyclic Galois group).

Definition of $\chi(\mathfrak{p})$.

Let $\mathfrak{p}$ be a prime of K.

- If $\mathfrak{p}$ is unramified in K_χ/K, set $\chi(\mathfrak{p}) = \chi(\mathrm{Frob}_{\mathfrak{p}})$. If $\mathfrak{p}$ has inertia degree l in K_χ/K, then $\chi(\mathfrak{p})$ is a primitive l^{th} root of unity.
- If $\mathfrak{p}$ ramifies in K_χ/K, set $\chi(\mathfrak{p}) = 0$.

A more intuitive "definition" of characters and the Grünwald-Wang theorem

For this talk it suffices to view a Dirichlet character of order l as a map $\mathcal{P}_K \to \mu_l \cup \{0\}$.

However, one can prescribe the values of Dirichlet characters for *finitely* many primes:

Grünwald-Wang theorem (simplified).

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be primes of K not lying over 2 and let $a_1, \ldots a_n \in \mu_l$. Then there exists a Dirichlet character χ of order l such that $\chi(\mathfrak{p}_i) = a_i$ for all $1 \leqslant i \leqslant n$.

A prime bijection that preserves Dirichlet characters is meaningful

Theorem. (Uchida, CdSLMS)

Let K, L be global fields. Suppose there is a prime bijection $\phi : \mathcal{P}_K \to \mathcal{P}_L$ and an isomorphism $\psi : X(K) \to X(L)$ such that

$$\chi(\mathfrak{p}) = \psi(\chi)(\phi(\mathfrak{p}))$$

for all $\chi \in X(K)$ and $\mathfrak{p} \in \mathcal{P}_K$. Then K and L are isomorphic.

The L-series of a Dirichlet character

Definition.

Let $\chi \in X(K)$. The Dirichlet L-series of χ is defined as

$$L_K(\chi, s) = \sum_{I \in \mathcal{I}_K} \chi(I) \mathbb{N} I^{-s} = \prod_{\mathfrak{p} \in \mathcal{P}_K} \frac{1}{1 - \chi(\mathfrak{p}) \mathbb{N} \mathfrak{p}^{-s}}.$$

If χ is the trivial character, then $L_K(\chi, s) = \zeta_K(s)$.

Main theorem (1/2)

Theorem. (CdSLMS, Dalla Torre)

Let K and L be global fields. Suppose there exists an isomorphism $\psi : X(K) \to X(L)$ such that

$$L_K(\chi, s) = L_L(\psi(\chi), s)$$

for every Dirichlet character χ. Then K and L are isomorphic as fields. Moreover, there is a bijection between the set of isomorphisms ψ with this property and isomorphisms $\sigma : K \to L$.

Remark.

For number fields, it suffices to restrict to characters of order 2, i.e. $\psi : X(K)[2] \to X(L)[2]$.

Main theorem (2/2)

Theorem.

Let K and L be number fields. For any $k \geqslant 3$ there exists a character χ of order k such that if

$$L_K(\chi) = L_L(\chi')$$

for any character $\chi' \in X(L)$, then K and L are isomorphic as fields.

Proof sketches

L-series bunch up information about primes of the same characteristic

What information does $L_K(\chi, s) = L_L(\psi(\chi), s)$ give?

L-series bunch up information about primes of the same characteristic

What information does $L_K(\chi, s) = L_L(\psi(\chi), s)$ give?

Multiplicative notation:

$$\prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{\mathbb{N}\mathfrak{p}^s}\right) = \prod_{\mathfrak{q}|p} \left(1 - \frac{\psi(\chi)(\mathfrak{q})}{\mathbb{N}\mathfrak{q}^s}\right).$$

Set $T = p^{-s}$:

$$\prod_{\mathfrak{p}|p} (1 - \chi(\mathfrak{p}) T^{f_\mathfrak{p}}) = \prod_{\mathfrak{q}|p} (1 - \psi(\chi)(\mathfrak{q}) T^{f_\mathfrak{q}}).$$

L-series bunch up information about primes of the same characteristic

What information does $L_K(\chi, s) = L_L(\psi(\chi), s)$ give?

Multiplicative notation:

$$\prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{\mathbb{N}\mathfrak{p}^s}\right) = \prod_{\mathfrak{q}|p} \left(1 - \frac{\psi(\chi)(\mathfrak{q})}{\mathbb{N}\mathfrak{q}^s}\right).$$

Set $T = p^{-s}$:

$$\prod_{\mathfrak{p}|p} (1 - \chi(\mathfrak{p}) T^{f_\mathfrak{p}}) = \prod_{\mathfrak{q}|p} (1 - \psi(\chi)(\mathfrak{q}) T^{f_\mathfrak{q}}).$$

Additive notation:

$$\sum_{N(\mathfrak{p})=p} \chi(\mathfrak{p}) = \sum_{N(\mathfrak{q})=p} \psi(\chi)(\mathfrak{q}).$$

A priori this need not be true for primes of norm p^k, $k \geqslant 2$.

In number fields, one can use the multiplicative notation

The order of the zero at $T = 1$ is exactly the number of primes $\mathfrak{p} \mid p$ for which $\chi(\mathfrak{p}) = 1$.

In number fields, one can use the multiplicative notation

The order of the zero at $T = 1$ is exactly the number of primes $\mathfrak{p} \mid p$ for which $\chi(\mathfrak{p}) = 1$.

	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
χ	1	-1	ζ_3	-1	ζ_3^2	-1

	$\mathfrak{q}_1$	$\mathfrak{q}_2$	$\mathfrak{q}_3$	$\mathfrak{q}_4$	$\mathfrak{q}_5$	$\mathfrak{q}_6$
$\psi(\chi)$		1				

In number fields, one can use the multiplicative notation

The order of the zero at $T = 1$ is exactly the number of primes $\mathfrak{p} \mid p$ for which $\chi(\mathfrak{p}) = 1$.

	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
χ	1	-1	ζ_3	-1	ζ_3^2	-1
χ^2	1	1	ζ_3^2	1	ζ_3	1

	$\mathfrak{q}_1$	$\mathfrak{q}_2$	$\mathfrak{q}_3$	$\mathfrak{q}_4$	$\mathfrak{q}_5$	$\mathfrak{q}_6$
$\psi(\chi)$		1		-1	-1	-1

In number fields, one can use the multiplicative notation

The order of the zero at $T = 1$ is exactly the number of primes $\mathfrak{p} \mid p$ for which $\chi(\mathfrak{p}) = 1$.

	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
χ	1	-1	ζ_3	-1	ζ_3^2	-1
χ^2	1	1	ζ_3^2	1	ζ_3	1
χ^3	1	-1	1	-1	1	-1

	$\mathfrak{q}_1$	$\mathfrak{q}_2$	$\mathfrak{q}_3$	$\mathfrak{q}_4$	$\mathfrak{q}_5$	$\mathfrak{q}_6$
$\psi(\chi)$	ζ_3	1	ζ_3^2	-1	-1	-1

The prime bijection comes from well-chosen characters

	$\mathfrak{p}_1$	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{p}_4$	$\mathfrak{p}_5$	$\mathfrak{p}_6$
χ	ζ_l	1	1	1	1	1

	$\mathfrak{q}_1$	$\mathfrak{q}_2$	$\mathfrak{q}_3$	$\mathfrak{q}_4$	$\mathfrak{q}_5$	$\mathfrak{q}_6$
$\psi(\chi)$	1	1	ζ_l	1	1	1

One prime at a time, one constructs a prime bijection.

Remark.

The multiplicativity of ψ ensures that the prime bijection is consistent over all characters.

The function field case

This approach does not work for function fields: there are infinitely many primes lying over p!

The function field case

This approach does not work for function fields: there are infinitely many primes lying over p!

Solution.

There are only finitely many primes of every norm. By closely inspecting the additive notation and using an inductive argument, one obtains the same result.

Twists of elliptic curves

An elliptic curve is determined by the L-functions of its twists

Theorem.

Let K, L be number fields and E_1/K, and E_2/L elliptic curves such that either

- E_1 has no complex multiplication.
- E_1 has complex multiplication and its complex multiplication field is contained in K.

Suppose there is an isomorphism $\psi : X(K) \to X(L)$ such that

$$L(E_1/K, \chi, s) = L(E_2/L, \psi(\chi), s)$$

for all $\chi \in X(K)$. Then there is an isomorphism $\sigma : K \to L$ such that E_1^σ is isogenous to E_2 over L.

Remark.

Once again it suffices to restrict to characters of order 2, the quadratic twists of the elliptic curve.

A small exercise

The additive notation of the L-function gives an equality:

$$\sum_{\mathbb{N}\mathfrak{p}=p} \chi(\mathfrak{p}) a_{\mathfrak{p}} = \sum_{\mathbb{N}\mathfrak{q}=p} \psi(\chi)(\mathfrak{q}) a_{\mathfrak{q}}.$$

A small exercise

The additive notation of the L-function gives an equality:

$$\sum_{\mathbb{N}\mathfrak{p}=p} \chi(\mathfrak{p}) a_{\mathfrak{p}} = \sum_{\mathbb{N}\mathfrak{q}=p} \psi(\chi)(\mathfrak{q}) a_{\mathfrak{q}}.$$

If we ignore the fact that ψ is an homomorphism, then after some reductions and simplifications one obtains the following combinatorial reconstruction problem:

Question.

Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be integers. Suppose for every subset $S \subseteq [1..n]$ there is a subset $T \subseteq [1..n]$ such that

$$\sum_{i \in S} a_i = \sum_{j \in T} b_j.$$

Does it hold that $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are the same numbers? What if $S \mapsto T$ is a bijection? What if all integers are positive?

Summary

Insight.
Prime bijections do not suffice for field isomorphisms,
but *meaningful* ones do.

One example of such a meaningful prime bijection is one that respects characters, which we have seen to be equivalent to respecting L-functions.

Summary

Insight.
Prime bijections do not suffice for field isomorphisms, but *meaningful* ones do.

One example of such a meaningful prime bijection is one that respects characters, which we have seen to be equivalent to respecting L-functions.

Thanks for listening! Any questions?

E-mail: h.j.smit@uu.nl

ArXiv: 1706.04515

The number field case

Theorem.

Let K and L be number fields. For any $k \geqslant 3$ there exists a character χ of order k such that if

$$L_K(\chi) = L_L(\chi')$$

for any character $\chi' \in X(L)$, then K and L are isomorphic as fields.

Induced representations

Because of $\mathbb{Q}$, we can use induced representations.

Two facts on L-series:

- $L_K(\chi) = L_{\mathbb{Q}}(\mathrm{Ind}(\chi))$;
- $L_{\mathbb{Q}}(\rho) = L_{\mathbb{Q}}(\rho') \Longrightarrow \rho \cong \rho'$.

Hence we want to create a special character χ such that

$$\mathrm{Ind}(\chi) \cong \mathrm{Ind}(\chi') \Longrightarrow K \cong L.$$

This happens when $\mathrm{Ind}(\chi)$ has a unique monomial structure.

Monomial structure is not always unique

The symmetry group D_4 of a square has two non-isomorphic monomial structures: one consisting of the axes and one consisting of the diagonals.

This results in the following: let χ be the character of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and χ' be the character of $\mathbb{Q}(i\sqrt{2}, (1+i)\sqrt[4]{2})/\mathbb{Q}(i\sqrt{2})$. The L-series of χ and χ' are equal, but $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$ are not isomorphic.