Hanoi, Chicago, Boston and Western
A panoramic view of absolute Galois groups

JOINT TALK
MINI-WORKSHOP: ALGEBRA AND HOMOGENEOUS SPACES
ONLINE SEMINAR ON QUADRATIC FORMS, LINEAR ALGEBRAIC GROUPS AND BEYOND

Jan Mináč, Tung T. Nguyen

June 2nd, 2021

The University of Western Ontario
London, Ontario, Canada

Thank you!


THANK YOU: KIRILL, NICOLE, NIKITA,
PHILIPPE AND ZINOVY
ĎAKUJEM
VEĽA KRÁT
Cảm ơn
rất nhiều

Hanoi Institute of Mathematics

The University of Chicago

Wellesley College

The University of Western Ontario

The beginning of the story

Approximate excerpts from Tung T. Nguyen's email:

"Dear Professor Mináč,
My name is Tung and I am interested in your work with Nguyen Duy Tan on Massey products in Galois cohomology. Can we please speak via Skype?"

The continuing story

WE DID!

In my talk today, I would like to cover some of the subsequent developments which fill my life and the lives of our students, collaborators and friends with joy, excitement, endless enthusiasm, and hopes.

Consider

- F is a field.
- $F^\times = F \setminus \{0\}$.
- p is a prime number and $p \neq \mathrm{char}(F)$.
- $\zeta_p \in F^\times$.
- $G_F = \mathrm{Gal}(F^{\mathrm{sep}}/F)$.
- $a_1, a_2, \ldots, a_n \in F^\times$.
- $(a_1), (a_2), \ldots, (a_n) \in H^1(G_F, \mathbb{F}_p)$ be the image of $a_1, a_2, \ldots, a_n$ under the Kummer map
$$F^\times/(F^\times)^p \to H^1(G_F, \mathbb{F}_p).$$
Concretely $(a_i) \in \mathrm{Hom}(G_F, \mathbb{F}_p)$ defined via the equation
$$\frac{\sigma(\sqrt[p]{a_i})}{\sqrt[p]{a_i}} = \zeta_p^{a_i(\sigma)}, \forall \sigma \in G_F.$$

We shall now connect a condition when a Massey product $\langle (a_1), (a_2), \ldots, (a_n) \rangle$ is defined and when it vanishes with a beautiful embedding problem.

Recall first unipotent upper triangular matrices

$$U_{n+1}(\mathbb{F}_p) = \begin{pmatrix} 1 & * & * & * & \ldots & * \\ 0 & 1 & * & * & \ldots & * \\ 0 & 0 & 1 & * & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & & \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Thus they are p-Sylow subgroups of $GL_{n+1}(\mathbb{F}_p)$.

The center of $U_{n+1}(\mathbb{F}_p)$ is

$$U_{n+1}(\mathbb{F}_p) = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & \boxed{*} \\ 0 & 1 & 0 & 0\dots & 0 & \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & & \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix} \cong \mathbb{F}_p \, .$$

In fact it was Evariste Galois himself who already observed the order of $GL_n(\mathbb{F}_p)$ is :

$$(p^n - 1)(p^n - p)(p^n - p^2)\dots(p^n - p^{n-1}),$$

in studying the Galois group of the general equation of degree p^n.

Thus indeed we see that $p^{\frac{n(n-1)}{2}}$ is the highest power of p dividing the order of $GL_n(\mathbb{F}_p)$ confirming that the $U_n(\mathbb{F}_p)$ is a p- Sylow subgroup of $Gl_n(\mathbb{F}_p)$.

Now the critical Galois embedding problems associated with the definition of n-Massey products
$\langle (a_1), (a_2), \ldots, (a_n)\rangle \subset H^2(G_F, \mathbb{F}_p)$ and its vanishing

$$0 \in \langle (a_1), (a_2), \ldots, (a_n)\rangle,$$

are related to the following diagram

$$\begin{tikzcd}
& & & G_F \arrow[dl, dashed, "\omega"'] \arrow[d, "\gamma"] & \\
1 \arrow[r] & \mathbb{F}_p \arrow[r] & U_{n+1}(\mathbb{F}_p) \arrow[r] & \overline{U_{n+1}(\mathbb{F}_p)} \arrow[r] & 1
\end{tikzcd}$$

where

$$\overline{U_{n+1}(\mathbb{F}_p)} = \frac{U_{n+1}(\mathbb{F}_p}{\mathcal{Z}(U_{n+1}(\mathbb{F}_p))} = \frac{U_{n+1}(\mathbb{F}_p)}{\mathbb{F}_p}.$$

The product $\langle (a_1), (a_2), \ldots, (a_n) \rangle$ is defined if there exists a continuous homomorphism

$$\gamma : G_F \to \overline{U_{n+1}(\mathbb{F}_p)},$$

such that for each $\sigma \in G$

$$[\gamma(\sigma)]_{i,i+1} = a_i(\sigma),$$

where $a_i \in H^1(G_F, \mathbb{F}_p) = \mathrm{Hom}(G_F, \mathbb{F}_p)$ is viewed as a homomorphism from G_F to $\mathbb{F}_p$.

If $\langle (a_1), (a_2), \ldots, (a_n) \rangle$ is defined then one can associate certain elements in $H^2(G_F, \mathbb{F}_p)$ as one runs through different suitable γ as above.

For us, the only important fact is to know when $\langle (a_1), (a_2), \ldots, (a_n)\rangle \subset H^2(G_F, \mathbb{F}_p)$ is defined and when

$$0 \in \langle (a_1), (a_2), \ldots, (a_n)\rangle.$$

If $0 \in \langle (a_1), (a_2), \ldots, (a_n)\rangle$, we say that $\langle (a_1), (a_2), \ldots, (a_n)\rangle$ the n-th Massey product of $(a_1), (a_2), \ldots, (a_n)$ vanishes. This happens if and only if there exists $\gamma : G_F \to \overline{U_{n+1}(\mathbb{F}_p)}$ with the property described earlier and $\omega : G_F \to U_{n+1}(\mathbb{F}_p)$ such that the following diagram commutes

$$\begin{tikzcd}
 & & & G_F \arrow[dl, dashed, "\omega"'] \arrow[d, "\gamma"] & \\
1 \arrow[r] & \mathbb{F}_p \arrow[r] & U_{n+1}(\mathbb{F}_p) \arrow[r] & \overline{U_{n+1}(\mathbb{F}_p)} \arrow[r] & 1.
\end{tikzcd}$$

In J. Eur. Math. Soc 2017 and also J. London Math Soc 2016, with Tan we proposed a conjecture known as the Mináč-Tan conjecture or simply the n-th Massey vanishing conjecture for $n \geq 3$.

Conjecture

For every field F, prime p and cohomology class $a_1, a_2, \ldots, a_n \in H^1(G_F, \mathbb{F}_p)$ with $n \geq 3$, if the n-the Massey product $\langle a_1, a_2, \ldots, a_n \rangle$ is defined then it contains $0 \in H^2(G_F, \mathbb{F}_p)$.

In J. Eur. Math. Soc 2017 and also J. London Math Soc 2016, with Tan we proposed a conjecture known as the Mináč-Tan conjecture or simply the n-th Massey vanishing conjecture for $n \geq 3$.

Conjecture

For every field F, prime p and cohomology class $a_1, a_2, \ldots, a_n \in H^1(G_F, \mathbb{F}_p)$ with $n \geq 3$, if the n-the Massey product $\langle a_1, a_2, \ldots, a_n \rangle$ is defined then it contains $0 \in H^2(G_F, \mathbb{F}_p)$.

Some highlights related to history and developments and results related to this conjecture are contained in 1975 paper of W. Dwyer in JPPA, Hopkins-Wickelgren 2015 JPAA paper, Efrat 2014 Advances paper. In particular, Hopkins and Wickelgren established the n-Massey vanishing conjecture when F is a global field and $n = 3, p = 2$. In joint work with Tan in JEMS in 2017, we extend these results to all fields and we formulate the above conjecture.

Further known results of the n-Massey vanishing conjecture

- When $n = 3$, F and p are arbitrary. This is due to the work of Matzri, Efrat-Matzri, and Mináč-Tan. Matzri first posted these results in 2014 in Arxiv and subsequently all our teams published various proofs of this result. In Advances 2017 with Tan, we provided a constructive Galois theoretic solution of the corresponding Galois embedding problem.
- When F is a local field and $n \geq 3$ and all primes by Mináč-Tan in JEMS 2017.
- When F is a number field, $n = 4$, $p = 2$ by the work of Guillot, Mináč, Topaz, Wittenberg in Compositio Math in 2019.
- When F is an algebraic number field and $n \geq 3$, arbitrary p are established by Harpaz and Wittenberg.

Euler's discovery

Let us start our story with the beautiful Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

In 1734, Leonhard Euler found the following remarkable formula

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots = \frac{\pi^2}{6}.$$

Indeed, Euler did much more. In particular, he showed that

$$\zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k},$$

where $\{B_n\}$ are the Bernoulli numbers defined by following Taylor's expansion

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n.$$

Special value of motivic zeta functions

- ◇ Ever since Euler made the stunning discoveries connecting some values of zeta functions with powers of π, there has been a tremendous effort of mathematicians to comprehend well the "true reasons behind these connections" and extend further these results to other values and other zeta functions.
- ◇ Beilinson and Deligne made a breakthrough by putting this study in the framework of mixed motives and motivic cohomology. However, their work only predicts L-values up to an undetermined rational factor. Beilinson's approach is inspired by the work of Bloch on K_2 of CM elliptic curves.
- ◇ Bloch and Kato formulated a more precise conjecture using tools from p-adic Hodge theory discovered by Fontaine.

The Bloch-Kato conjecture

Let M be a motive (i.e a compatible system of Galois representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. A folklore definition: $H^n(X)(r)$ where X is a smooth variety over $\mathbb{Q}$. It has different realizations depending on different cohomology theories (de Rham, Betti, etale, crystalline.) The Bloch-Kato conjecture says that

$$\mathrm{Tam}(M) = \frac{\# H^0(\mathbb{Q}, M^* \otimes \mathbb{Q}/\mathbb{Z}(1))}{\# Ш(M)},$$

where

- $\mathrm{Tam}(M)$ is the Tamagawa number of M which is closely related to the zeta value $L(M, 0)$.
- $Ш(M)$ is the Tate-Shafarevich group associated with M. It is conjectured to be a finite group.

Height of motives and the Bloch-Kato conjecture

In my thesis, I study the relations between heights of motives and their zeta values. More precisely, we have the following theorem.

Theorem (Nguyen)

Let M be a pure motives with integer coefficients of weight $-d$ such that $d \geq 3$. We assume further that M has semistable reduction at all places. Then

$$\lim_{B \to \infty} \frac{\#\{x \in B(\mathbb{Q}) | H_{\diamond,d}(x) \leq B\}}{\mu\left(x \in \prod'_{p \leq \infty} B(\mathbb{Q}_p) | H_{\diamond,d}(x) \leq B\right)} = \frac{1}{Tam(M)}.$$

Here $B(\mathbb{Q})$ (respectively $B(\mathbb{Q}_p)$) is the relevant motivic cohomology associated with M (respectively the local Selmer group at p), μ is the Tamagawa measure associated with M and, $H_{\diamond,d}(x)$ is the height function defined by K. Kato.

Massey products and the Bloch-Kato conjecture

We hope to generalize the above theorem to a more general situation as follow.

- ◇ Let us fix motives $M_0, .., M_n$.
- ◇ We consider the set of all mixed motives M with a decreasing filtration M^i such that $M^0 = M, M^{n+1} = 0$, and $M^i/M^{i+1} = M_i$.
- ◇ Massey products are related to the obstructions for such M and therefore to zeta values.

An interesting observation

- $\zeta(0) = 1 + 1 + 1 + \ldots = -\frac{1}{2}$.
- $\zeta(-1) = 1 + 2 + 3 + = -\frac{1}{12}$.

Furthermore

$$\zeta(0) = \int_0^1 (x-1)dx = -\frac{1}{2}.$$

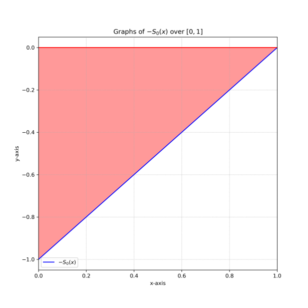

Figure 1: Graph of $x - 1$ over $[0, 1]$

Similarly $\zeta(-1)$ is the minus are of the red region in figure 2.

$$\zeta(-1) = \int_0^1 \frac{x(x-1)}{2} = -\frac{1}{12}.$$

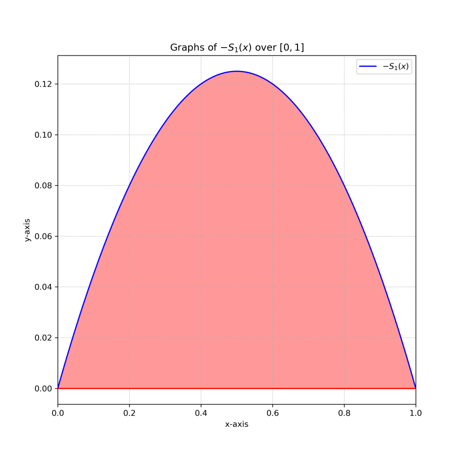

Figure 2: Graph of $\frac{x(x-1)}{2}$ over $[0, 1]$

Hurwitz zeta functions

In 1882, Hurwitz defined the following infinite series

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s},$$

where $0 < a \leq 1$.

- ◇ When $a = 1$, we have $\zeta(s, 1) = \zeta(s)$ is the classical Riemann zeta function.
- ◇ Like the Riemann zeta function, the Hurwitz zeta function has an analytic continuation to $\mathbb{C}$ with a simple pole at $s = 1$.
- ◇ While Hurwitz zeta functions are not motivic, they play an important role in understanding Dirichlet L-functions.

Power sums and special values of Hurwitz zeta functions

Let $S_{n,a}$ is the generalized power sum defined by

$$S_{n,a}(M) = a^n + (1+a)^n + (2+a)^n + \ldots + (M+a-2)^n.$$

It is known that $S_{n,a}$ is a polynomial of degree $n+1$.

Theorem (Mináč, Tan, Nguyen)

$$\zeta(-n, a) = \int_{1-a}^{2-a} S_{n,a}(x)dx,$$

We have three different proofs for this theorem.

Fekete polynomials

Let p be a prime number such that $p \equiv 3 \pmod 4$. Let $\chi_p : \mathbb{Z} \to \mathbb{C}^\times$ be the quadratic character $\chi_p(a) = \left(\frac{a}{p}\right)$ where $\left(\frac{a}{p}\right)$ is the Legendre symbol. The L-function associated with χ_p is given by

$$L(\chi_p, s) = \sum_{n=1}^{\infty} \frac{\chi_p(n)}{n^s}.$$

The special value at $s = 1$ has a nice formula

$$L(\chi_p, 1) = \int_0^1 \frac{F_p(x)}{x(1 - x^p)} dx.$$

where

$$F_p(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a.$$

This polynomial is called the Fekete polynomial associated with p.

Fekete polynomials

Fekete polynomials have some two trivial zeros, namely 0 and 1. Let

$$f_p(x) = \frac{F_p(x)}{x(1-x)}.$$

It can be shown that $f_p(x)$ is a reciprocal polynomial of degree $p-3$. Hence there exists a polynomial $g_p(x)$ such that

$$f_p(x) = x^{\frac{p-3}{2}} g_p\left(x + \frac{1}{x}\right).$$

We call $g_p(x)$ the reduced Fekete polynomial.

It turns out that $g_p(x)$ has remarkable properties. Furthermore, it contains lot of important arithemtic information.

Special values of reduced Fekete polynomials

Theorem (Mináč, Tan, Nguyen)

- $g_p(2) = f_p(1) = ph(-p)$.
- $g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(-1) = -\frac{1}{2}\left(\left(\frac{p}{3}\right) + 3\right) h(-p)$.
- $g_p(0) = g_p(-2) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(1) = -\left(\frac{6}{p}\right)\left[6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right]\frac{h(-p)}{2}$.
  Here $h(-p)$ is the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

From this theorem, we can also say something quite interesting about the splitting field of f_p.

Some conjectures

Numerical computations for $p \leq 43$ lead us to the following conjecture.

Conjecture

f_p and g_p are irreducible over $\mathbb{Q}$. Furthermore, there is a split short exact sequence

$$1 \to (\mathbb{Z}/2)^{h_p} \to Gal(\mathbb{Q}(f_p)/\mathbb{Q}) \to Gal(\mathbb{Q}(g_p)/\mathbb{Q}) \cong S_{h_p} \to 1.$$

Here $h_p = \deg(g_p)$. Consequently, $Gal(\mathbb{Q}(f_p)/\mathbb{Q})$ is a semi-direct product of $(\mathbb{Z}/2)^{h_p}$ and S_{h_p}.

Today it is June second. It is the day when Evariste Galois was buried in a common grave of the Montparnasse Cemetery. Galois died on May 30 . Leslie my wife will read his last words to his younger brother Alfred which were:

“Ne pleure pas, Alfred! J’ai besoin de tout mon courage pour mourir à vingt ans!”

(Don’t cry, Alfred! I need all my courage to die at twenty!)

Thank you