Relations in the maximal pro-p quotients of absolute Galois groups

Nguyễn Duy Tân

Hanoi University of Science and Technology

Conference PANT-Kyoto 2021
December 6-10, 2021, RIMS, Kyoto University

Contents

- Introduction
- Main results

This talk is based on joint work with Jan Mináč and Michael Rogelstad "Relations in the maximal pro-p quotients of absolute Galois groups" TAMS 2020.

Absolute Galois groups

- F a field, and F_s its separable closure; $G_F = \mathrm{Gal}(F_s/F)$ the absolute Galois group of F.
- Fix a prime number p, $G_F(p)$= the maximal pro-p quotient of G_F.
- G_F is a profinite group and $G_F(p)$ is pro-p group.

We want to

- Describe the absolute Galois groups of fields among profinite groups.
- Describe the maximal pro-p quotients of absolute Galois groups of general fields for a given prime number p.

One can show that any profinite group occurs as a Galois group of *some* Galois extension L/F. However not every profinite group occurs as an absolute Galois group.

A guiding problem ["Absolute" inverse Galois problem]

What groups can occur as G_F or $G_F(p)$?
What groups cannot occur as G_F or $G_F(p)$?

- (Artin-Schreier, 1927) If G_F is nontrivial and finite then $G_F \simeq \mathbb{Z}/2\mathbb{Z}$.
- (Becker, 1974) If $G_F(p)$ is nontrivial and finite then $p = 2$ and $G_F(2) \simeq \mathbb{Z}/2\mathbb{Z}$.

$G_F(p)$: F is a p-adic field

For each $n \geq 1$, let $\mu_n = \{z \in F_s \mid z^n = 1\} = \langle \zeta_n \rangle$.

- (Shafarevich 1947) If $\mu_p \not\subseteq F$ then $G_F(p)$ is a free pro-p group of rank $[F : \mathbb{Q}_p] + 1$.
- (Kawada 1954) If $\mu_p \subseteq F$ then $G_F(p)$ admits a presentation

$$1 \to R \to S \to G_F(p) \to 1,$$

  where S is a free pro-p-group and R is a normal subgroup of S generated (as a normal subgroup) by a single relation r.
- In the case $\mu_p \subseteq F$, the works of Demushkin, Serre, Labute determine the relation r explicitly.

$G_F(p)$: F is a p-adic field

For example, suppose $p > 2$ then

$$r = x_1^{p^s}[x_1, x_2] \cdots [x_{n-1}, x_n], \tag{1}$$

where $n = [F : \mathbb{Q}_p] + 2$ is even and p^s is the highest power q of p such that F cotains a primitive q-th root of unity. (Here $[x, y] = x^{-1}y^{-1}xy$.)

Vague questions

If we modify r slightly, can $S/\langle r \rangle$ still be $G_F(p)$ for some field F?
Must the relations in $G_F(p)$ for general field F take on only certain forms?

From now on, field F is assumed to contains μ_p, and p odd prime.

A more precise question

Let p be an odd prime and n is odd. Let $G = S/\langle r \rangle$, where S is a free pro-p group on generators $x_1, x_2, \ldots, x_n$, and

$$r = x_1^{p^s}[x_2, x_3] \cdots [x_{n-1}, x_n], \tag{2}$$

with $s \in \mathbb{N}$, and $\langle r \rangle$ is the smallest closed normal subgroup of S which contains r.

Question

Can $G \simeq G_F(p)$ for some F containing μ_p?

Note that using technique involving triple Massey products in Galois cohomology, one can show that some relations which include triple commutator $[[x_1, x_2], x_3]$ as a factor *cannot* be in $G_F(p)$ (Mináč-T. 2017).

Brief discussion on Massey products in Galois cohomology

- Triple Massey product: partially defined and multi-valued which "generalizes" cup product.
- Let p be a prime, G a profinite group. Consider $\mathbb{F}_p$ as a trivial G-module.
- Triple Massey product $\langle \alpha, \beta, \gamma \rangle$ of α, β and γ in $H^1(G, \mathbb{F}_p)$ is *defined* precisely when $\alpha \cup \beta = \beta \cup \gamma = 0$ in $H^2(G, \mathbb{F}_p)$. And if it is defined, it is a certain nonempty subset of $H^2(G, \mathbb{F}_p)$.
- For any $n \geq 3$ can define n-Massey products $\langle \alpha_1, \ldots, \alpha_n \rangle$ for (suitable) $\alpha_i \in H^1(G, \mathbb{F}_p)$.

Motivated by work of Hopkins-Wickelgren 2015 some other works.

Conjecture (Mináč-T. 2017)

Let p be prime number, $n \geq 3$ an integer and, F field (containing a primitive p-th root of unity), $\alpha_i \in H^1(G_F, \mathbb{F}_p)$.
If n-fold Massey product $\langle \alpha_1, \ldots, \alpha_n \rangle$ is defined then it vanishes (i.e., it contains 0).

- In the case $n = 3$, the conjecture was proved. (Hopkins-Wickelgren 2015 for $p = 2$ and F local or global field, Mináč-T. 2017 for $p = 2$ and any F, Efrat-Matzri 2017 and Mináč-T. 2016 for any p and F, Matzri 2018, Lam-Liu-Sharifi-Wang-Wake 2020,...)
- The case $n \geq 4$ is still open.
- Wittenberg-Harpaz arXiv 2019 prove the conjecture for the case of any n, any p and F a number field (via the study of rational points on some homeogenous spaces, see also Wittenberg's ICM 2022 talk).

The conjecture has some applications.

- Providing new large family of groups which cannot be $G_F(p)$. For example, the pro-p group

$$G = \langle x_1, x_2, x_3, x_4, x_5 \mid [x_4, x_5][[x_2, x_3], x_1] = 1 \rangle$$

  cannot be $G_F(p)$ because G does not have the vanishing property for triple Massey products. This group could not be treated by previous known methods. (Mináč-T. 2017)
- Artin-Schreier's theorem and Becker's theorem can be recovered from the vanishing of certain Massey products.

- However, for the case we are considering, $G = S/\langle r\rangle$, S is a free pro-p group on generators $x_1, x_2, \dots, x_n$, and

$$r = x_1^{p^s}[x_2, x_3]\cdots[x_{n-1}, x_n],$$

  the relation involves only p-th powers and commutators and one cannot use triple Massey products to deal with.
- In fact, one can show that G has the vanishing triple Massey product property (Efrat-Quadrelli 2019). That means for $\alpha, \beta, \gamma \in H^1(G, \mathbb{F}_p)$, if $\langle\alpha, \beta, \gamma\rangle$ is defined then this subset of $H^2(G, \mathbb{F}_p)$ contains 0.

Result

Theorem (Mináč-Rogelstad-T. 2020)

F a field containing μ_p, p odd prime. Suppose $G_F(p)$ admits presentation

$$1 \to R \to S \xrightarrow{\pi} G_F(p) \to 1,$$

where S is a free pro-p-group on a set of generators $\{x\} \sqcup \{y_i\}_{i\in I}$.
Let T be the (closed) subgroup of S generated by $\{y_i\}_{i\in I}$.
Then there is no relation of the form $r = x^{p^\ell} s \in R$, where $\ell \geq 1$ and $s \in T$.

For example, if $G = S/\langle r\rangle$, where S is a free pro-p group on generators $x_1, x_2, \dots, x_n$, and

$$r = x_1^{p^s}[x_2, x_3]\cdots[x_{n-1}, x_n],$$

then $G \not\simeq G_F(p)$ for every F containing μ_p.

Idea of proof

- Suppose that we have a Galois p-extension L/F with $G = \mathrm{Gal}(L/F)$ a p-group. Then we have a surjective homomorphism

$$\mathrm{res}\colon G_F(p) \twoheadrightarrow G.$$

- Clearly, $\mathrm{res} \circ \pi(r) = 1$ in G. In particular, $\mathrm{res} \circ \pi(r)(a) = a$ for every $a \in L$.
- For $r = x^{p^\ell} s$ as in Theorem, we construct the extension L/F in a way that $\mathrm{res} \circ \pi(r) \neq 1$.

Galois extensions "detect" relations.

For example, for simplicity, suppose F contains μ_{p^2}, and suppose $r = x^p s \in R$, where $s \in T$. Choose $a \in F^\times$ and a p^2-th root $\sqrt[p^2]{a}$ of a such that

$$\pi(x)(\sqrt[p^2]{a}) = \zeta_{p^2} \sqrt[p^2]{a}$$
$$\pi(y_i)(\sqrt[p^2]{a}) = \sqrt[p^2]{a}, \ \forall i \in I.$$

Let $L = F(\sqrt[p^2]{a})$. Then $G = \mathrm{Gal}(L/F) \simeq \mathbb{Z}/p^2\mathbb{Z}$ and

$$S \xrightarrow{\pi} G_F(p) \overset{\mathrm{res}}{\twoheadrightarrow} G = \mathbb{Z}/p^2\mathbb{Z}.$$

Note that $\mathrm{res}(\pi(x)) = \bar{1}$ in $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathrm{res}(\pi(y_i)) = \bar{0}$. One has

$$\mathrm{res}(\pi(r)) = (\mathrm{res}(x))^p \, \mathrm{res}(\pi(s)) = \bar{p} \neq \bar{0} \in \mathbb{Z}/p^2\mathbb{Z},$$

a contradiction.

Proof of Theorem

(Proof by contradiction) Suppose $r = x^{p^\ell} s$, with $s \in T$.
Pick $m > \ell$. Choose $a \in F^\times$ and a p^m-th root $\sqrt[p^m]{a}$ of a such that

$$\pi(x)(\sqrt[p^m]{a}) = \zeta_{p^m} \sqrt[p^m]{a}$$
$$\pi(y_i)(\sqrt[p^m]{a}) = \sqrt[p^m]{a}, \ \forall i \in I.$$

Let $L = F(\sqrt[p^m]{a}, \zeta_{p^m})$. Then L/F is Galois with

$$G := \mathrm{Gal}(L/F) = \mathrm{Gal}(L/F(\zeta_{p^m})) \rtimes \mathrm{Gal}(L/F(\sqrt[p^m]{a})) \simeq C_{p^m} \rtimes C_{p^{m-k}}.$$

(Here k is the integer such that $\zeta_{p^k} \in F$ but $\zeta_{p^{k+1}} \notin F$.) Consider

$$S \xrightarrow{\pi} G_F(p) \overset{\mathrm{res}}{\twoheadrightarrow} G = C_{p^m} \rtimes C_{p^{m-k}}.$$

Note that $\mathrm{res}(\pi(s))(\sqrt[p^m]{a}) = \sqrt[p^m]{a}$. Hence

$$(\sqrt[p^m]{a}) = \pi(r)(\sqrt[p^m]{a}) = \pi(x)^{p^\ell}(\sqrt[p^m]{a}).$$

Case 1: $\pi(x)$ acts trivially on ζ_{p^m}

One has

$$\sqrt[p^m]{a} = \pi(x)^{p^\ell}(\sqrt[p^m]{a}) = \zeta_{p^m}^{p^\ell}\sqrt[p^m]{a}.$$

This implies $\zeta_{p^m}^{p^\ell} = 1$, hence $p^m \mid p^\ell$, a contradiction.

Case 2: $\pi(x)$ acts non-trivially on ζ_{p^m}

Since

$$\pi(x)(\zeta_{p^m})^{p^{m-k}} = \pi(x)(\zeta_{p^k}) = \zeta_{p^k} = \zeta_{p^m}^{p^{m-k}},$$

one has

$$\pi(x)(\zeta_{p^m}) = \zeta_{p^m}\zeta_{p^{m-k}}^{\nu}, \text{ for some } \nu \in \mathbb{Z}.$$

This implies that

$$\sqrt[p^m]{a} = \pi(x)^{p^\ell}(\sqrt[p^m]{a}) = \zeta_{p^m}^{N}\sqrt[p^m]{a},$$

where $N = \dfrac{(1+p^k\nu)^{p^\ell}-1}{p^k\nu}$. Hence $p^m \mid N$ and $m \leq v_p(N)$.
Check that for p odd prime, and $\alpha \in p\mathbb{Z}$ then

$$v_p((1+\alpha)^n - 1) = v_p(\alpha) + v_p(n).$$

Hence $v_p(N) = v_p(p^k\nu) + v_p(p^\ell) - v_p(p^k\nu) = \ell$, a contradiction

A summary result

Let F be a field such that F contains μ_p and it contains μ_4 if $p=2$. Let S be a free pro-p-group on a set of generators $\{x\}\cup\{y_i \mid i\in I\}$ such that

$$1\longrightarrow R\longrightarrow S\xrightarrow{\pi} G_F(p)\longrightarrow 1$$

is a minimal presentation of $G_F(p)$. Let T be the (closed) subgroup of S generated by $\{y_i\}_{i\in I}$. Then there is no relation of the form $r=x^{p^l u}s\in R$, where l and u are nonzero integers with $l\geq 1$, $\gcd(p,u)=1$, and

1. $s\in [S,S]T$ and $l<m$ if F contains ζ_{p^m} for some $m\geq 2$;
2. $s\in [S,S]$ such that any commutator of the form $[u,v]$ $(u,v\in X\sqcup X^{-1})$ appearing is a fixed commutator expression for s has $u\neq x^{\pm 1}$ and $v\neq x^{\pm 1}$;
3. $s\in T$;

Some references

- I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. 19 (2017), 3629–3640.
- I. Efrat and C. Quadrelli, *The Kummerian property and maximal pro-p Galois groups*, J. Algebra 525 (2019), 284–310.
- Y. Harpaz and O. Wittenberg, *The Massey Vanishing Conjecture for number fields*, preprint 2019, on Wittenberg's homepage.
- M. J. Hopkins and K. G. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra 219 (2015), 1304–1319.
- Y.H.J. Lam, Y. Liu, R. Sharifi, P. Wang, J. Wake, *Generalized Bockstein maps and Massey products*, preprint 2020, on Sharifi's homepage.
- J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. 19 (2017), 255-284.
- J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, J. London Math. Soc. 94 (2016), 909-932.
- J. Mináč, M. Rogelstad and N. D. Tân, *Relations in the maximal pro-p quotients of absolute Galois groups*, Trans. Amer. Math. Soc. 373 (2020), 2499–2524.
- O. Wittenberg, *Some aspects of rational points and rational curves*, ICM talk 2022, arXiv:2111.00504.

Thank you very much for your attention!

- G a pro-p-group, $\mathbb{U}_p = \mathbb{Z}_p^\times$ the group of p-adic units with the p-adic topology, and $\chi\colon G \to \mathbb{U}_p$ a continuous homomorphism.
- We define an action of G on $\mathbb{Z}_p$ by $\sigma \cdot x = \chi(\sigma)x$ for $\sigma \in G$, $x \in \mathbb{Z}_p$. Then $\mathbb{Z}_p$, with the p-adic topology, becomes a topological G-module which we denote by $\mathcal{I} = \mathcal{I}(\chi)$.

Lemma

Consider the following two statements:

1. For all $m \geq 1$ the canonical homomorphism $H^1(G, \mathcal{I}/p^m\mathcal{I}) \to H^1(G, \mathcal{I}/p\mathcal{I})$ is surjective.
2. For all $m \geq 1$ we may arbitrarily prescribe the values of crossed homomorphisms of G to $\mathcal{I}/p^i\mathcal{I}$ on a minimal system of generators of G provided we require that for all but a finite number of generators, these values are 0.

Then (1) implies (2).

Now F any field containing a primitive p-th root of unity. The action of $G_F(p)$ on μ_{p^∞} is given by a character

$$\chi_{p,cycl}\colon G_F(p) \to \mathbb{U}_p.$$

The character $\chi_{p,cycl}$ is called the p-cyclotomic character. For any $\sigma \in G_F(p)$, $\chi_{p,cycl}(\sigma)$ is determined by the condition that

$$\sigma(\xi) = \xi^{\chi_{p,cycl}(\sigma)}, \quad \forall \xi \in \mu_{p^\infty}.$$

Proposition

Let $\mathcal{I} = \mathcal{I}(\chi_{p,cycl})$. Then for each $i \geq 1$, the canonical homomorphism

$$H^1(G_F(p), \mathcal{I}/p^m\mathcal{I}) \to H^1(G_F(p), \mathcal{I}/p\mathcal{I})$$

is surjective.

Corollary

Let F be a field containing ζ_p. Assume that $\{x\} \sqcup \{y_i\}_{i\in I}$ is a minimal system of generators for $G_F(p)$. Then for every $m \geq 1$, there exists $a \in F^\times$ and a p^m-th root $\sqrt[p^m]{a}$ of a such that

$$x(\sqrt[p^m]{a}) = \zeta_{p^m} \sqrt[p^m]{a} \quad \text{and } y_i(\sqrt[p^m]{a}) = \sqrt[p^m]{a} \quad \forall i \in I.$$

Proof.

There exists a crossed homomorphism $D\colon G_F(p) \to \mu_{p^m}$ such that

$$D(x) = \zeta_{p^m} \quad \text{and } D(y_i) = 1 \quad \forall i \in I.$$

Consider D as a cocycle with values in $F(p)^\times$, then D is a 1-coboundary by Hilbert's Theorem 90. Thus there exists $\alpha \in F(p)^\times$ such that $D(\sigma) = \sigma(\alpha)/\alpha$ for all $\sigma \in G_F(p)$. Since $\sigma(\alpha)/\alpha \in \mu_{p^m}$ for all $\sigma \in G_F(p)$, we see that $\alpha^{p^m} =: a$ is in $F^\times$. □

Some further related works

- Works of C. De Clercq and M. Florence on smooth profinite groups which are motivated by the search for an ”explicit” proof of the Bloch-Kato conjecture in Galois cohomology. In particular, the paper "Lifting theorems and smooth profinite groups", arxiv:1710.10631, 2017.
- Some works of C.Quadrelli and his collaborators, in particular, C. Quadrelli and T. Weigel, *Profinite groups with a cyclotomic p-orientation*, Doc. Math. 25 (2020), 1881–1916.

F p-adic field, with residue field F_q, $\ell \neq p$, l prime.
If $\ell \nmid q-1$ then $G_F(\ell) \simeq \mathbb{Z}_l$.
If $\ell \mid q-1$ then $G_F(\ell) = \langle x, y \mid yxy^{-1} = x^{1+\ell^m} \rangle$ ($\ell \neq 2$ or (if $\ell = 2$ and $m \neq 1$)).
Here m is the largest integer such that F contains the ℓ^m-th roots of unity.
If $\ell = 2$, $m = 1$, let $n = v_2(q+1)$ then $G_F(2) = \langle x, y \mid yxy^{-1} = x^{-(1+2^n)} \rangle$