Galois groups with restricted ramification

Romyar Sharifi

Harvard University

Unique factorization:

Let K be a *number field*, a finite extension of the rational numbers $\mathbf{Q}$.
The *ring of integers* $\mathcal{O}_K$ of K consists of all roots in K of monic polynomials in one variable with coefficients in the integers $\mathbf{Z}$.

In general, $\mathcal{O}_K$ is not a unique factorization domain (UFD).
I.e., nonzero elements need not factor uniquely as products of prime elements up to units.

Example. *The ring of integers of* $\mathbf{Q}(\sqrt{-5})$ *is* $\mathbf{Z}[\sqrt{-5}]$, *which is not a* (*UFD*)*: e.g.,*

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 3 \cdot 2.$$

(*Note that the only units in* $\mathbf{Z}[\sqrt{-5}]$ *are* ± 1.)

The class group:

Let us define a measure of how far $\mathcal{O}_K$ is from having unique factorization.

The set of nonzero ideals I_K of K is closed under multiplication.
Let P_K denote the subset of nonzero principal ideals.
The quotient I_K/P_K is a finite group.

Definition. We define the *class group* Cl_K of K to be I_K/P_K.

The order h_K of Cl_K is called the *class number* of K.
$\mathcal{O}_K$ is a UFD $\Leftrightarrow \mathcal{O}_K$ is a PID $\Leftrightarrow h_K = 1$.

Example. *$h_{\mathbf{Q}(\sqrt{-5})} = 2$, and $\mathrm{Cl}_{\mathbf{Q}(\sqrt{-5})}$ is generated by the image of $(2, 1+\sqrt{-5})$.*

Ramification of prime ideals:

Definition. We say that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is *ramified* in a finite extension L/K if

$$\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{q}^2$$

for some prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$. Otherwise, $\mathfrak{p}$ is *unramified*.

Only finitely many primes are ramified in L/K.

If S is the set of ramified primes of $\mathcal{O}_K$ in L/K, we say that L/K is *unramified outside* S, or the primes in S.

Example. $\mathbf{Q}(\sqrt{-5})$ *is unramified outside* 2 *and* 5*:* $2\mathbf{Z}[\sqrt{-5}] = (2, 1 + \sqrt{-5})^2$ *and* $5\mathbf{Z}[\sqrt{-5}] = (\sqrt{-5})^2$*.*

Cyclotomic fields:

For a positive integer n, we let μ_n denote the group of nth roots of unity in a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$.

$\mathbf{Q}(\mu_n)$ is called the *cyclotomic field* of nth roots of unity.

$\mathbf{Q}(\mu_n)/\mathbf{Q}$ is Galois with Galois group

$$\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^{\times}.$$

The extension $\mathbf{Q}(\mu_n)/\mathbf{Q}$ is ramified exactly at the primes dividing (the numerator of) $n/2$.

Regular and irregular primes:

Definition. A prime p is called *regular* if p does not divide $h_{\mathbf{Q}(\mu_p)}$. Otherwise, p is *irregular*.

Some interesting facts:

1. Let B_k denote the kth Bernoulli number, which is defined by the power series

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k.$$

p is regular if and only if p does not divide the numerator of the Bernoulli number B_k for any even k with $2 \leq k \leq p - 3$.

2. 37 is the smallest irregular prime, and it divides the numerator of B_{32}.

3. Kummer proved Fermat's Last Theorem for regular primes in 1850.

Galois groups:

$G_K = \text{Gal}(\overline{K}/K)$ is the Galois group of the extension of K given by its algebraic closure $\overline{K} \cong \overline{\mathbf{Q}}$.
We call G_K the *absolute Galois group* of K.

G_K is a huge, uncountable group. However, as with any Galois group of an algebraic extension, it is *profinite*, an inverse limit of finite groups.
$G_K = \varprojlim G_{L/K}$ with L/K finite Galois.

A profinite group G is a topological group, with its topology arising from the discrete topology on the inverse system chosen to define it.

We say that a profinite group G is (topologically) *finitely generated* if there is a finite set of elements of G such that the closure of the subgroup they generate is G.
G_K is not topologically finitely generated.

Quotients of G_K:

G_K^{ab} = maximal abelian quotient of G_K.
Equivalently, this is the Galois group of the maximal abelian extension of K.

Example. *The maximal abelian extension* $\mathbf{Q}^{\text{ab}}$ *of* $\mathbf{Q}$ *is* $\cup_{n \geq 1} \mathbf{Q}(\mu_n)$ *and* $G_{\mathbf{Q}}^{\text{ab}} \cong \varprojlim (\mathbf{Z}/n\mathbf{Z})^{\times}$.

$G_K^{(p)}$ = the maximal pro-p quotient of G_K.
A p-group is a finite group of p-power order.
A pro-p group is an inverse limit of p-groups.

Let S be a set of prime ideals of K.
$G_{K,S}$ = the Galois group of the maximal algebraic extension of K unramified outside S.
(An algebraic extension is unramified outside S if this is true in every finite subextension.)

Example. $G_{\mathbf{Q},\varnothing} = 1$.

In general, the structure of $G_{K,S}$ is very far from known.
Class field theory: $G_{K,\varnothing}^{\text{ab}} \cong \text{Cl}_K$.

Galois group of the maximal pro-p unramified outside p extension of $\mathrm{Q}(\mu_p)$:

Take $K = \mathbf{Q}(\mu_p)$ and S the set consisting of the unique prime above p, for an odd prime p.

Let $\mathcal{G} = G^{(p)}_{\mathbf{Q}(\mu_p),S}$.

Theorem (Koch). *Let s denote the p-rank of Cl_K (i.e., p^s is the order of $\mathrm{Cl}_K/p\mathrm{Cl}_K$). The group $\mathcal{G}$ has a minimal presentation*

$$1 \to \mathcal{R} \to \mathcal{F} \to \mathcal{G} \to 1$$

with $\mathcal{F}$ a free pro-p group on $s+\frac{p+1}{2}$ generators and $\mathcal{R}$ a free pro-p group which is the normal closure of a subgroup generated by s elements.

In particular, $\mathcal{G}^{\mathrm{ab}} \cong \mathbf{Z}_p^{\oplus(p+1)/2} \oplus$ torsion, where $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^n\mathbf{Z}$.

The torsion in $\mathcal{G}^{\mathrm{ab}}$ does not lift to torsion in $\mathcal{G}$. However, we can ask how close it is to being torsion.

$\Delta = \mathrm{Gal}(K/\mathbf{Q})$ is a cyclic group of order $p-1$.
Teichmüller character: $\omega\colon \Delta \to \mathbf{Z}_p^\times$.
ω takes values in the $(p-1)$st roots of 1 in $\mathbf{Z}_p^\times$ and

$$\delta(\zeta) = \zeta^{\omega(\delta)}$$

for any $\delta \in \Delta$ and $\zeta \in \mu_p$.

$\Omega =$ maximal pro-p extension of K unramified outside p.
Denote also by Δ a fixed choice of lifting of $\mathrm{Gal}(K/\mathbf{Q})$ to a subgroup of $\mathrm{Gal}(\Omega/\mathbf{Q})$.

Proposition (S.). *We may choose a set of generators X of $\mathcal{G}$ such that for any $\delta \in \Delta$, we have $\delta x \delta^{-1} = x^{\omega(\delta)^i}$ for some i for each $x \in X$.*

In particular, we note that we may decompose $\mathcal{G}^{\text{ab}}$ into "eigenspaces" for the action of Δ.

The ω^i-eigenspaces corresponding to the non-torsion part of $\mathcal{G}^{\text{ab}}$ are of rank 1 when $i = 0$ or i is odd and zero otherwise.

Vandiver's conjecture: the nonzero eigenspaces of the torsion all have i even.

We will choose our generating set X as in the proposition, and let x_i for i odd ($1 \leq i \leq p - 2$) or $i = 0$ as above be an element which reduces to a generator of the ω^i-eigenspace of the nontorsion part of $\mathcal{G}^{\text{ab}}$.

An example: $p = 37$

$37 \mid B_{32}$ and $h_{\mathbf{Q}(\mu_{37})} = 37$.
The torsion part of $\mathcal{G}^{\text{ab}}$ is $\mathbf{Z}/37\mathbf{Z}$ and lies in the ω^{32}-eigenspace.

Let $y \in X$ be a lift of a generator of this torsion group, so that $X = \{y, x_0, x_1, x_3, \ldots, x_{35}\}$.

We get a relation in $\mathcal{R}$ from the following identity:

$$y^{37}[x_0, y]^{a_0}[x_1, x_{31}]^{a_1}[x_3, x_{29}]^{a_3} \ldots \\ [x_{15}, x_{17}]^{a_{15}}[x_{33}, x_{35}]^{a_{33}} \in [\mathcal{G}, [\mathcal{G}, \mathcal{G}]].$$

$a_0 \not\equiv 0 \bmod 37$ (classical Iwasawa theory).
The triviality, or not, of the numbers $a_1, a_3, \ldots, a_{15}, a_{33}$ is much deeper.

A pairing on cyclotomic p-units:

Definition. The *cyclotomic p-unit* group $\mathcal{C}$ is the subgroup of $K^\times$ generated by elements of the form $1-\zeta$ with $\zeta \in \mu_p$, $\zeta \neq 1$.

As a group, $\mathcal{C}$ has the following structure:

$$\mathcal{C} \cong \mathbf{Z}^{\oplus(p-1)/2} \oplus \mathbf{Z}/p\mathbf{Z}.$$

Let k be even with $k \leq p-2$ such that $p \mid B_k$.
$A = \mathrm{Cl}_K/p\mathrm{Cl}_K$.
$A^{(1-k)} =$ the ω^{1-k}-eigenspace of A.

McCallum and I defined a pairing (via a cup product in Galois cohomology)

$$\langle\ ,\ \rangle_{p,k} \colon \mathcal{C} \times \mathcal{C} \to A^{(1-k)}.$$

If p satisfies Vandiver's conjecture (e.g., $p < 16{,}000{,}000$), then $A^{(1-k)}$ is a 1-dimensional $\mathbf{F}_p$-vector space.

Conjecture (McCallum, S.). $\langle\ ,\ \rangle_{p,k}$ *is surjective.*

We have special cyclotomic p-units for odd i:

$$\eta_i \equiv \prod_{\delta \in \Delta} (1 - \zeta^\delta)^{\omega(\delta)^{i-1}} \bmod \mathcal{C}^p.$$

Fact: $\langle \eta_i, \eta_j \rangle_{p,k} = 0$ if $i + j \not\equiv k \bmod (p-1)$.
Set $e_{i,k} = \langle \eta_i, \eta_{k-i} \rangle_{p,k}$.

Remark. I have given interpretations of the $e_{i,k}$ as products in K-theory and, conjecturally, algebraic periods of modular forms.

We further require that the $x_i \in X$ satisfy

$$x_i(\eta_i^{1/p}) = \zeta \cdot \eta_i^{1/p}$$

for a fixed choice of $\zeta \in \mu_p$, $\zeta \neq 1$.

Our example: $p = 37, k = 32$

There exists a choice of isomorphism

$$\phi\colon A^{(1-k)} \to \mathbf{F}_p$$

such that $\phi(e_{i,k}) = a_i$ for $i = 1, 3, \ldots, 15, 33$. (I.e., for odd i with $1 \leq i \leq [k-i]$, where $[j]$ denotes the least positive residue of j modulo $p-1$.)

Theorem 1 (McCallum, S.). *We have* $a_i \equiv 0 \bmod 37$ *if and only if* $i = 5$.

The $a_i \bmod 37$ in the order $i = 1, 3, ..., 15, 33$ up to a common nonzero scalar multiple: $1, 26, 0, 36, 1, 35, 31, 34, 11$.

A representation of $G_{\mathbf{Q}}$:

The fundamental group of the complex projective line minus three points is free on two generators:

$$\pi_1(\mathbf{P}^1_{\mathbf{C}} - \{0, 1, \infty\}) \cong \mathbf{Z} * \mathbf{Z}.$$

One can consider its *profinite completion*:

$$\widehat{\pi_1} = \varprojlim \pi_1(\mathbf{P}^1_{\mathbf{C}} - \{0, 1, \infty\})/N,$$

where the limit is taken over subgroups N of finite index.

There is a canonical outer action of $G_{\mathbf{Q}}$ on $\widehat{\pi_1}$. In fact, Belyi showed that the homomorphism

$$\rho\colon G_{\mathbf{Q}} \to \operatorname{Out} \widehat{\pi_1}$$

is injective.

We focus on the induced action on the maximal pro-p quotient $\pi_1^{(p)}$ of $\widehat{\pi_1}$:

$$\rho_p \colon G_{\mathbf{Q}} \to \operatorname{Out} \pi_1^{(p)}.$$

As shown by Ihara, the kernel of ρ_p contains G_Ω, where Ω is the maximal pro-p extension of $\mathbf{Q}(\mu_p)$ unramified outside p.
In other words, restriction to $G_{\mathbf{Q}(\mu_p)}$ induces a map

$$\psi_p \colon \mathcal{G} \to \operatorname{Out} \pi_1^{(p)}.$$

Open question: Is ψ_p an injective map?

A p-adic Lie algebra:

ψ_p gives rise to a torsion-free graded $\mathbf{Z}_p$-Lie algebra $\mathfrak{g}_p$.

Specifically, one filters $\pi_1^{(p)}$ by its lower central series $\pi_1^{(p)}(k)$ to obtain a filtration on $\mathcal{G}$ given by the kernels $F^k\mathcal{G}$ of the induced maps

$$\mathcal{G} \to \mathrm{Out}(\pi_1^{(p)}/\pi_1^{(p)}(k+1)).$$

One defines

$$\mathfrak{g}_p = \oplus_{k=1}^{\infty} F^k\mathcal{G}/F^{k+1}\mathcal{G}.$$

Conjecture (Deligne). *The Lie algebra $\mathfrak{g}_p \otimes \mathbf{Q}_p$ is free on one generator in each odd degree $i \geq 3$.*

$\mathfrak{g}_p \otimes \mathbf{Q}_p$ is the p-adic realization of a motivic Lie algebra (Deligne) which encodes multiple zeta values and spaces of modular forms (Goncharov).

The Lie algebra $\mathfrak{g}_p$ itself contains a rich arithmetic structure not found in $\mathfrak{g}_p \otimes \mathbf{Q}_p$.

Theorem 2 (S.). *a. If p is regular and Deligne's conjecture holds at p, then $\mathfrak{g}_p$ is free on one generator in each odd degree $i \geq 3$.*
b. If p is irregular and Greenberg's pseudo-null conjecture holds for $\mathbf{Q}(\mu_p)$, then $\mathfrak{g}_p$ is not free.

Remark. The two cases in the theorem correspond to exactly the cases in which $\mathcal{G}$ is free/not free, and this fact is key to the proof.

Greenberg's pseudo-null conjecture is outside the scope of this talk. It has been proven by McCallum for a large class of irregular primes.

Ihara showed that there exist special nonzero (noncanonical) elements $\sigma_i \in \mathrm{gr}^i\mathfrak{g}_p$ for $i \geq 3$ odd ($\mathrm{gr}^1\mathfrak{g}_p = \mathrm{gr}^2\mathfrak{g}_p = 0$) with nontrivial image in $\mathrm{gr}^i\mathfrak{g}_p^{\mathrm{ab}}$.
It is these elements upon which Deligne conjectures that $\mathfrak{g}_p \otimes \mathbf{Q}_p$ is free.

Ihara conjectures the existence of a relation in $\mathrm{gr}^{12}\mathfrak{g}_{691}$ of the form:

$$691h = [\sigma_3, \sigma_9] - 50[\sigma_5, \sigma_7]$$

with h having nontrivial image in $\mathrm{gr}^{12}\mathfrak{g}_{691}^{\mathrm{ab}}$.
In particular, he expects that $\mathrm{gr}^{12}\mathfrak{g}_{691}$ is not generated by the σ_i.

Note that $691 \mid B_{12}$.

Theorem 3 (S.). $\langle\ ,\ \rangle_{691,12} \neq 0$ *if and only if Ihara's conjecture is true.*

More generally (and imprecisely), I expect that whenever $p \mid B_k$ with $k < p$, there is a relation in $\mathrm{gr}^k \mathfrak{g}_p$ such that the coefficients of $[\sigma_i, \sigma_{k-i}]$ are given by the pairing values $e_{i,k}$.

Philosophy: relations in the Lie algebra $\mathfrak{g}_p$ arise from relations in $\mathcal{G}$.

In particular, there is a relation in $\mathcal{G}$ for $p = 691$ of the form

$$y^{691}[x_0, y]^{a_0}[x_1, x_{11}]^{a_1}[x_3, x_9]^{a_3}[x_5, x_7]^{a_5} \\ [x_{13}, x_{689}]^{a_{13}} \dots [x_{349}, x_{353}]^{a_{349}} \in [\mathcal{G}, [\mathcal{G}, \mathcal{G}]]$$

and Ihara's relation is the "image" of this relation in $\mathrm{gr}^{12} \mathfrak{g}_{691}$.

Relationship with Modular Forms:

Let k be a positive even integer.
Let G_k denote the normalized Eisenstein series of weight k:

$$G_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_{k-1}(n) = \sum_{1 \le d | n} d^{k-1}$, $q = e^{2\pi i z}$.

Let p exactly divide the numerator of B_k/k. Then there exists weight k cusp form

$$f = \sum_{n=1}^{\infty} a_n q^n$$

for $SL_2(\mathbf{Z})$ which is a Hecke eigenform and satisfies a certain mod p congruence with G_k.

Specifically, there is a prime $\mathfrak{p}$ lying over p in the field F generated by the coefficients a_n of f such that

$$\sigma_{k-1}(n) \equiv a_n \bmod \mathfrak{p}$$

for all $n \ge 1$.

Consider the L-function

$$L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

The ratios

$$c_i(f) = \frac{(i-1)!}{(-2\pi\sqrt{-1})^{i-1}} \frac{L(f,i)}{L(f,1)}$$

are elements of F for odd i with $3 \leq i \leq k-3$ (Shimura, Manin).
In fact, they have positive valuation at $\mathfrak{p}$.

Let R denote the localization of $\mathcal{O}_F$ at $\mathfrak{p}$.
The images $\bar{c}_i(f)$ of the $c_i(f)$ in $\mathfrak{p}R/\mathfrak{p}^2R$ lie in a one-dimensional $\mathbf{F}_p$-vector subspace.

Conjecture (S.). *Assume that p satisfies Vandiver's conjecture. The $e_{i,k} = \langle \eta_i, \eta_{k-i} \rangle_{p,k}$ and $\bar{c}_i(f)$, for i odd with $3 \leq i \leq k-3$, define the same one-dimensional subspace of $\mathbf{F}_p^{(k-4)/2}$.*

Remark. The assumption of Vandiver's conjecture can be removed.