On the structure of a Galois Lie algebra

Romyar T. Sharifi

February 7, 2002

Let $X = \mathbf{P}^1_{\mathbf{Q}} - \{0, 1, \infty\}$. The long exact sequence of étale fundamental groups

$$1 \to \pi_1^{\mathrm{et}}(X_{\bar{\mathbf{Q}}}) \to \pi_1^{\mathrm{et}}(X) \to G_{\mathbf{Q}} \to 1,$$

with $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, yields a canonical representation $\phi\colon G_{\mathbf{Q}} \to \mathrm{Out}(\pi_1^{\mathrm{et}}(X_{\bar{\mathbf{Q}}}))$. Passing to the maximal pro-p quotient $\pi_1^{(p)}$ of $\pi_1^{\mathrm{et}}(X_{\bar{\mathbf{Q}}})$ for p odd, we may consider $\phi^{(p)}\colon G_{\mathbf{Q}} \to \mathrm{Out}(\pi_1^{(p)})$. Let Ω^* denote the fixed field of $\phi^{(p)}$. If $\pi_1^{(p)}(j)$ denotes the jth term in the lower central series of $\pi_1^{(p)}$, then we may also consider the representations

$$\phi_m^{(p)}\colon G_{\mathbf{Q}} \to \mathrm{Out}(\pi_1^{(p)}/\pi_1^{(p)}(m+1))$$

for $m \geq 1$. We remark that $K = \mathbf{Q}(\zeta_{p^\infty})$ is the fixed field of $\phi_1^{(p)}$. Set $G = \mathrm{Gal}(\Omega^*/K)$, define a filtration on G by $F^m G = \ker \phi_m^{(p)}$, and let $\mathfrak{g}$ be the associated graded object. We have the following [I1, I2].

Theorem 1 (Ihara).

a. The field Ω^* is a pro-p extension of K unramified outside p.

b. There is an isomorphism of $G_{\mathbf{Q}}$-modules, $\mathrm{gr}^m \mathfrak{g} \cong \mathbf{Z}_p(m)^{r_{m,p}}$, for some $r_{m,p} \geq 0$.

c. The commutator on G provides $\mathfrak{g}$ with the structure of a graded $\mathbf{Z}_p$-Lie algebra.

For each odd positive integer m, there exists a nontrivial $\mathrm{Gal}(K/\mathbf{Q})$-equivariant homomorphism $\kappa_m\colon G_K \to \mathbf{Z}_p(m)$ [So]. For each odd integer $m \geq 3$, the map κ_m induces a nontrivial homomorphism $\kappa_m\colon \mathrm{gr}^m \mathfrak{g} \to \mathbf{Z}_p$ [I2]. For such m, we let σ_m denote an element of $F^m G$ such that $\kappa_m(\sigma_m)$ generates $\kappa_m(F^m G)$. We also denote by σ_m the element of $\mathrm{gr}^m \mathfrak{g}$ given by the restriction of $\sigma_m \in F^m G$.

Let S be a free pro-p group on generators s_m with m odd ≥ 3, and let $\mathfrak{s}$ be a free graded $\mathbf{Z}_p$-Lie algebra on generators s_m in odd degrees $m \geq 3$. We define homomorphisms $\Psi\colon S \to G$ and $\psi\colon \mathfrak{s} \to \mathfrak{g}$ by $s_m \mapsto \sigma_m$.

Conjecture (Deligne). *The map $\psi \otimes \mathbf{Q}_p\colon \mathfrak{s} \otimes \mathbf{Q}_p \to \mathfrak{g} \otimes \mathbf{Q}_p$ is an isomorphism.*

Hain and Matsumoto have shown that $\psi \otimes \mathbf{Q}_p$ is surjective [HM]. The following diagram summarizes the relationships between this conjecture and its variants.

$$\begin{tikzcd}
\Psi\text{ injective} & \psi\text{ injective} \arrow[l, Rightarrow] \arrow[r, Leftrightarrow] & \psi \otimes \mathbf{Q}_p\text{ injective} \arrow[dd, Leftrightarrow, "{[I3]}"] \\
\Psi\text{ inj. and }\psi\text{ surj.} \arrow[u, Rightarrow] \arrow[dd, Leftrightarrow] \arrow[dr, Leftrightarrow, "{[Sh]}"'] & & \\
& \psi\text{ bijective} \arrow[uu, Rightarrow] \arrow[r, Rightarrow] \arrow[dd, Rightarrow] & \psi \otimes \mathbf{Q}_p\text{ bijective} \arrow[dd, Rightarrow] \\
\Psi\text{ surj. and }\psi\text{ inj.} \arrow[ur, Leftrightarrow, "{[I3]}"] \arrow[d, Rightarrow] & & \\
\Psi\text{ surjective} & \psi\text{ surjective} \arrow[l, Rightarrow] \arrow[r, Rightarrow] & \psi \otimes \mathbf{Q}_p\text{ surjective}
\end{tikzcd}$$

Let Ω denote the maximal pro-p extension of K unramified outside p.

Theorem 2. *Let p be an odd regular prime. Then Ψ is surjective. If Deligne's conjecture holds for p, then ψ and Ψ are isomorphisms and $\Omega = \Omega^*$.*

For any number field F, let F_∞ denote the compositum of all $\mathbf{Z}_p$-extensions of F. Greenberg has conjectured that the Galois group of the maximal pro-p unramified abelian extension of F_∞ is pseudo-null as an Iwasawa module [G]. For $F = \mathbf{Q}(\zeta_p)$, there is the following equivalent formulation [Mc], which we refer to as Greenberg's conjecture for p.

Conjecture (Greenberg). *Let M_∞ denote the maximal abelian pro-p extension of F_∞ unramified outside p. Then $\mathrm{Gal}(M_\infty/F_\infty)$ is torsion-free as a module over $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$.*

McCallum has proven Greenberg's conjecture for a large class of irregular primes [Mc].

Theorem 3. *Let p be an irregular prime for which Greenberg's conjecture holds. Then ψ and Ψ are not isomorphisms. If Deligne's conjecture holds for p, then ψ and Ψ are not surjective.*

The main ingredient in the proofs of Theorems 2 and 3 is the recursive construction of the $\sigma_m \in G$ for odd $m \geq 3$ beginning with those m with $m \leq p$. If γ denotes an element of $\mathrm{Gal}(\Omega^*/F)$ which restricts to a generator of $\mathrm{Gal}(K/F)$ and ω denotes the cyclotomic character, then this construction is given by

$$\sigma_{m+p-1} = (\gamma \sigma_m \gamma^{-1} \sigma_m^{-\omega(\gamma)^m})^{\epsilon_m},$$

where ϵ_m denotes the application of a sort of "idempotent" for the action of a subgroup of $\mathrm{Gal}(\Omega^*/\mathbf{Q})$ of order $p-1$.

This construction allows us to use known information on the sturcture of $\mathcal{G} = \mathrm{Gal}(\Omega/F)$ to gain knowledge of the structure of G. More precisely, the elements γ and σ_m with $m \leq p$ will (freely) generate the quotient $\mathrm{Gal}(\Omega^*/F)$ of $\mathcal{G}$ if and only the σ_m with $m \geq 3$ (freely) generate G. Theorem 2 and 3 follow from the latter observation and the following two statements regarding the structure of $\mathcal{G}$. If p is regular, then $\mathcal{G}$ is freely generated by lifts of the elements γ and σ_m with $m \leq p$. On the other hand, for any irregular prime p, Greenberg's conjecture implies that $\mathcal{G}$ has no free pro-p quotient on $(p+1)/2$ generators [Mc]. For more details, see [Sh].

References

[G] R. Greenberg, "Iwasawa theory - past and present," Class Field Theory - It's Centenary and Prospect (Tokyo, 1998), Adv. Stud. Pure Math. **30**, Math. Soc. Japan, 2001, 335–385.

[HM] R. Hain and M. Matsumoto, "Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$", arXiv:math.AG/0006158, Aug. 11, 2001.

[I1] Y. Ihara, "Profinite Braid Groups, Galois representations and complex multiplications," *Ann. of Math.* **123** (1986), 43–106.

[I2] Y. Ihara, "The Galois representation arising from $\mathbf{P}^1 - \{0, 1, \infty\}$ and Tate twists of even degree," Galois groups over $\mathbf{Q}$, Math. Sci. Res. Inst. Publ. **16** (1989), Springer, 299–313.

[I3] Y. Ihara, "Some arithmetic aspects of Galois actions of the pro-p fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$," Res. Inst. Math. Sci. Preprint Series, RIMS-1229, May 1999.

[Mc] W. McCallum, "Greenberg's Conjecture and units in multiple $\mathbf{Z}_p$-extensions," *Amer. J. Math.* **123** (2001), 909–930.

[Sh] R. Sharifi, "Relationships between conjectures on the structure of Galois groups unramified outside p," arXiv:math.NT/0104116, Oct. 3, 2001.

[So] C. Soulé, "On higher p-adic regulators," Lecture Notes in Math. **854** (1981), Springer, 372–401.