J. Indian Inst. Sci.
A Multidisciplinary Reviews Journal
ISSN: 0970-4140 Coden-JIISAD
© Indian Institute of Science 2022.

Check for updates

STARTER

Galois Groups, Galois Representations and Iwasawa Theory

R. Sujatha*

In Memory of John Henry Coates.

1 Introduction

Let F be an algebraic number field, i.e. a finite extension of $\mathbb{Q}$, the field of rational numbers. For a field L, we shall denote a fixed algebraic closure of the field L by $\bar{L}$ and the Galois group Gal $(\bar{L}/L)$ by G_L. A fundamental problem in algebraic number theory is to understand the Galois group of F which we denote by G_F. Local and Global Class field theory provide important insights and there are several conjectures that add more via the theory of Motives and the Motivic Galois group[1]. Let v be a place of F such that v lies above a rational prime l. Then, the completion F_v is a finite algebraic extension of $\mathbb{Q}_l$, the l-adic local field. The Galois groups G_{F_v} are subgroups of G_F and Local Class field theory provides information on these subgroups. For every rational prime l, let μ_{l^∞} denote the group of l-primary roots of unity considered as a Galois module. The extension $F(\mu_{l^\infty})/F$ is a Galois extension whose Galois group Gal $(F(\mu_{l^\infty})/F)$ is isomorphic to $\mathbb{Z}_l^*$, the group of units in the ring $\mathbb{Z}_l$ of l-adic integers. This also gives the corresponding l-adic cyclotomic character

$$\chi_l : G_F \to \mathbb{Z}_l^*$$

such that the fixed field of the image of χ_l is the Galois extension $F(\mu_{l^\infty})$ of F (see[2].) Since $\mathbb{Z}_l^* \simeq \mathbb{Z}_l \times \mathbb{Z}/(l-1)$, considering the quotient of $F(\mu_{l^\infty})$ corresponding to the subfield fixed by $\mathbb{Z}/(l-1)$, one obtains the cyclotomic $\mathbb{Z}_l$ extension $F_{l,\mathrm{cyc}}$ of F with Gal $(F_{l,\mathrm{cyc}}/F) \simeq \mathbb{Z}_l$ and $F \subset F_{l,\mathrm{cyc}} \subset F(\mu_{l^\infty}) \subset \bar{F}$. In particular, for every prime l, there are natural abelian quotients of G_F isomorphic to $\mathbb{Z}_l$. Further, the classical Kronecker–Weber theorem asserts that every abelian Galois extension of F is contained in a cyclotomic extension. This note outlines some intertwinings between Galois groups of number fields, representation theory and Iwasawa theory. The interested reader is invited to consult the references for more details.

It is natural to ask how many linearly disjoint Galois extensions $\mathcal{L}$ of F exist such that Gal $(\mathcal{L}/H) \simeq \mathbb{Z}_l$ for a fixed prime number l. This is related to Leopoldt's conjecture whose validity would imply that there are $r_2 + 1$ such extensions, where r_2 is the number of pairs of complex embeddings of F. In particular, for totally real number fields, the cyclotomic $\mathbb{Z}_l$ extension is the unique Galois extension of F with Galois group $\mathbb{Z}_l$. It is known, thanks to a result of Brumer, that Leopoldt's conjecture is true for number fields F that are abelian over $\mathbb{Q}$. In particular, if F is a totally imaginary quadratic extension of $\mathbb{Q}$, then F admits of two linearly independent $\mathbb{Z}_l$-extensions. These are the cyclotomic $\mathbb{Z}_l$-extension $F_{l,\mathrm{cyc}}$ and the anticyclotomic extension $F_{l,\mathrm{ac}}$. The extension $F_{l,\mathrm{ac}}$ is the unique $\mathbb{Z}_l$-extension of F which is Galois over $\mathbb{Q}$ but not abelian over $\mathbb{Q}$. Leopoldt's conjecture has an equivalent formulation in terms of 'p-adic regulators', defined originally by Leopoldt for number fields and prime numbers p. Note that for every prime number p, Leopoldt's conjecture, in particular, asserts the existence of abelian Galois extensions $\mathcal{L}$ of a number field F with Gal $(\mathcal{L}/F)$ isomorphic to $\mathbb{Z}_p^{r_2+1}$.

2 Galois Representations

Local Class field theory provides information on important subgroups of G_F, namely the decomposition groups G_v for every place v of F. Another important class of quotient groups of G_F arises from the study of Galois representations. Suppose G is a topological group and V is a vector space over a field k equipped with a topology. A finite-dimensional k-representation of G is a continuous homomorphism

$$\rho : G \to \mathrm{Aut}\,(V) \simeq \mathrm{GL}_n(k).$$

Here, V is a k-vector space of dimension n and Aut (V) is the group of k-linear automorphisms of V, identified naturally with the group $\mathrm{GL}_n(k)$ of invertible $(n \times n)$ matrices over k. This latter group comes equipped with a topology that is induced by the topology on k. When $G = G_F$, the

[1] Department of Mathematics, University of British Columbia, Vancouver V6T1Z2, Canada.
*sujatha@math.ubc.ca

Springer IISc PRESS

corresponding representations are called Galois representations. Such representations arise naturally and plentifully in Arithmetic and in Geometry, over a variety of fields k. The image of any such representation would then yield a quotient of G_F. Typically, such Galois representations arise as a package, in the sense that there are finite-dimensional vector spaces V_l over the local fields $\mathbb{Q}_l$, for every prime l, with some additional compatibility properties. Such classes of representations are called l-adic representations[1]. It is fruitful to study the entire class of such representations collectively rather than for a single fixed prime l.

The simplest case of a Galois representation is the one-dimensional $\mathbb{Q}_l$-vector space $\mathbb{Q}_l$ with the trivial action of the Galois group. For every integer n, consider the one-dimensional vector space $\mathbb{Q}_l(n)$ whose underlying vector space is $\mathbb{Q}_l$, but the action of the Galois group is via the l-adic cyclotomic character. Thus, for $g \in G_F$ and $v \in \mathbb{Q}_l(n)$, the element $g.v \in \mathbb{Q}_l(n)$ is defined by $\chi(g).v$, where χ is the cyclotomic character. Here are some other examples of l-adic representations of the Galois group. Suppose E is an elliptic curve over F. Let $E(\bar{F})$ be the points of the elliptic curve over $\bar{F}$. Then, $E(\bar{F})$ is an abelian group and comes equipped with the natural action of the Galois group G_F. For a prime number l, and integer $n \geq 1$, let $E_{l^n} = E_{l^n}(\bar{F})$ denote the kernel of the "multiplication by l^n-map" on $E(\bar{F})$. It is clear that E_{l^n} inherits the structure of a G_F-module. The l-adic Tate module of E, denoted $T_l(E)$ is the inverse limit $\varprojlim E_{l^n}$ where the inverse limit is taken with respect to multiplication by l. The Tate module T_lE is a free $\mathbb{Z}_l$-module of rank 2 with a G_F-action. There is the associated $\mathbb{Q}_l$-vector space $V_lE := T_lE \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, of dimension two which affords a two dimensional Galois representation over $\mathbb{Q}_l$ for every prime l.

More generally, let X be a smooth projective variety over F and set $\bar{X} = X \times_F \bar{F}$ to denote the variety base changed to the algebraic closure. For every prime number l, and $i \geq 0$, the étale cohomology groups $V_l := H^i_{\text{ét}}(\bar{X}, \mathbb{Q}_l)$ are finite-dimensional $\mathbb{Q}_l$-vector spaces equipped with the natural action of G_F arising from base change. This yields an important class of l-adic representations arising from algebraic geometry with deep connections to the theory of Motives[1]. The 'Tate twists' are the Galois representations $V_l(n) := V_l \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(n)$, with the Galois group action given by the diagonal action. Another important class of l-adic Galois representations arises from modular forms[3], and this follows from deep results of Eichler, Shimura, Deligne and Serre. The class of l-adic representations arising from elliptic curves lies in the intersection of those arising from étale cohomology and arithmetic, since $V_l(E) \simeq H^1_{\text{ét}}(\bar{E}, \mathbb{Q}_l(1))$. For $F = \mathbb{Q}$, it follows from the deep results on modularity that the Galois representation associated to an elliptic curve is modular, in the sense that it is equivalent to a Galois representation arising from a normalised, cuspidal eigenform of weight 2.

3 Iwasawa Theory

Galois representations naturally provide modules over certain algebras that encode interesting arithmetic associated intrinsically to the representations. Iwasawa theory provides a powerful framework to study these modules and in extracting important arithmetic information. An exemplar of this is the study of class groups of number fields. It was pioneered by Iwasawa in the 1960s to study the growth of the l-part of the class groups of the number fields F_n $(n \geq 0)$, which are the finite layers of the cyclotomic $\mathbb{Z}_l$-extension $F_{l,\text{cyc}}$ of F such that $\text{Gal}\,(F_n/F) \simeq \mathbb{Z}/l^n$. Let $\text{Cl}\,(F_n)$ denote the class group of F_n and e_n be the cardinality of the l-primary part of $\text{Cl}\,(F_n)$. A fundamental result of Iwasawa demonstrates the systematic growth of e_n, more generally for a $\mathbb{Z}_l$-extension of F (see[4,5]).

Theorem 3.1 (Iwasawa) *Let F be a number field and let F_∞/F be a Galois extension with $\text{Gal}\,(F_\infty/F) \simeq \mathbb{Z}_l$. Then, there exist integers $\lambda = \lambda(F_\infty/F) \geq 0$, $\mu = \mu(F_\infty/F) \geq 0$ and $\nu = \nu(F_\infty/F)$, a such that*

$$e_n = \lambda n + \mu l^n + \nu, \tag{3.1}$$

for all sufficiently large n.

Iwasawa's study leads naturally to the study of certain subquotients of the Galois group G_F for a number field F. Let F_∞/F be a $\mathbb{Z}_l$-extension. For $n \geq 0$, let M'_n be the maximal unramified l-extension of F_n which is completely decomposed at all primes of F that lie above l. Set M_n to be the maximal unramified l-extension of F_n. For a group M, we denote the abelianisation of M by M^{ab}; it is the quotient of M by the commutator subgroup of M. If L/F is an extension with Galois group $\mathcal{G}$, the subfield of L which is fixed by $\mathcal{G}^{\text{ab}}$ is denoted L^{ab}. Then, $\text{Gal}\,(L^{\text{ab}}/F) \simeq \mathcal{G}^{\text{ab}}$. Set

$$H_n = M_n^{\text{ab}}, \quad H'_n = {M'_n}^{\text{ab}}$$
$$\mathcal{H} = \varprojlim M_n \quad \mathcal{H}' = \varprojlim H'_n. \tag{3.2}$$

The field extension M_n^{ab} is the l-Hilbert class field of F_n. Let $\mathcal{L}$ (resp. $\mathcal{L}'$) denote the maximal abelian, pro-p extension of F_∞ that is everywhere unramified (resp. where the primes above p split completely). Taking direct limits over n, define

$$\mathcal{L} = \varinjlim M_n, \quad \mathcal{L}' = \varinjlim M'_n. \tag{3.3}$$

There is an inclusion of fields

$$F \subset F_n \subset F_\infty \subset \mathcal{L}, \quad F \subset F_n \subset M_n^{\text{ab}} \subset M_n.$$

The fields $\mathcal{L}$ and $\mathcal{L}'$ are extensions over F_∞ and the corresponding Galois groups over F (respectively, over F_∞) are quotients (respectively, subquotients) of G_F. Consider the Galois groups

$$\begin{aligned} X_{\text{nr}} &= \text{Gal}\,(\mathcal{L}/F_\infty) &= \text{Gal}\,(\mathcal{H}/F_\infty)^{\text{ab}} \\ X_{\text{cs}} &= \text{Gal}\,(\mathcal{L}'/F_\infty) &= \text{Gal}\,(\mathcal{H}'/F_\infty)^{\text{ab}}, \end{aligned} \tag{3.4}$$

where $\mathcal{H}$ and $\mathcal{H}'$ are as in (3.2).

The Galois groups X_{nr} and X_{cs} are $\mathbb{Z}_l$-modules with a continuous action of the Galois group $\text{Gal}\,(F_\infty/F) \simeq \mathbb{Z}_l$. The Galois group X_{nr} is the pro-l Hilbert class field of F_∞ and is an extension of the Hilbert class feld of number fields, to infinite Galois extensions of number fields.

Let G be a profinite group. The Iwasawa algebra $\mathbb{Z}_l[[G]]$ of G over $\mathbb{Z}_l$ is defined to be the inverse limit

$$\mathbb{Z}_l[[G]] = \varprojlim \mathbb{Z}_l[G/G'],$$

where G' varies over open normal subgroups of G, and the inverse limit is taken with respect to the natural surjective maps on the quotient groups. When $G \simeq \mathbb{Z}_l$, the Iwasawa algebra of G is a compact $\mathbb{Z}_l$-algebra and is isomorphic to the power series ring in one variable over $\mathbb{Z}_l$,

$$\mathbb{Z}_l[[G]] = \mathbb{Z}_l[[T]].$$

The isomorphism is given by $(\gamma - 1) \mapsto T$, for a topological generator γ of $\mathbb{Z}_l$. In particular, $\mathbb{Z}_l[[G]]$ is a regular local ring and hence a unique factorial domain. The structure theorem for finitely generated modules over such rings provides algebraic invariants.

Theorem 3.2 *Let M be a finitely generated compact module over $\mathbb{Z}_l[[G]] = \mathbb{Z}_l[[T]]$. Then, there is a homomorphism of $\mathbb{Z}_l[[G]]$-modules*

$$M \to (\mathbb{Z}_l[[G]])^r \left(\bigoplus_{i=1}^{n} \mathbb{Z}_l[[G]]/l^{k_i} \right) \bigoplus_{j=1}^{m} \left(\frac{\mathbb{Z}_l[[G]]}{(f_j(T)^{r_j})} \right)$$

with finite kernel and cokernel, and such that the integers r, n, m, k_i, r_j are positive integers. Here, $f_j(T)$ are distinguished polynomials in $\mathbb{Z}_l[[T]]$. Moreover, the decomposition is unique up to reordering.

The integer r is called the rank of M. Let t_j be the degree of the polynomial $f_j(T)$. The two other invariants obtained from the structure theorem are the λ-invariant and μ-invariant, defined by

$$\begin{aligned} \lambda(M) &= \sum\nolimits_{j=1}^{m} t_j \cdot r_j \\ \mu(M) &= \sum\nolimits_{i=1}^{n} k_i. \end{aligned} \tag{3.5}$$

This leads to the natural question of what these invariants are for the $\mathbb{Z}_l[[G]]$-modules X_{nr} and X_{cs} over a $\mathbb{Z}_l$-extension F_∞/F. For the cyclotomic $\mathbb{Z}_l$-extension $F_\infty = F_{\text{cyc}}$, these modules are finitely generated. A fundamental result of Iwasawa proves that these modules are even torsion. In particular, the rank is zero and the invariants of interest are the λ and μ-invariants. In this regard, there is the following conjecture.

Conjecture 1 (Iwasawa's $\mu = 0$ conjecture:) *Let F be a number field and let F_{cyc} be the cyclotomic $\mathbb{Z}_l$-extension of F. Let $X_{nr,\text{cyc}}$ be the maximal abelian, unramified l-extension of F_{cyc}. Then, the μ-invariant of $X_{nr,cyc}$ is zero.*

This conjecture postulates that the pro-l Hilbert class field of the cyclotomic $\mathbb{Z}_l$-extension of a number field is a finitely generated $\mathbb{Z}_l$-module. The μ-invariant captures the l-primary torsion part while the λ-invariant is the $\mathbb{Z}_l$-rank of the module. A celebrated result of Ferrero–Washington proves this conjecture when F is an abelian extension. For $F = \mathbb{Q}$, the λ-invariant and the μ-invariant are both trivial.

A prime number p is regular if p does not divide the class number of $\mathbb{Q}(\mu_p)$. The prime $p = 37$ is the smallest irregular prime. Let $\mathbb{Q}(\mu_p)^+$ denote the totally real subfield of $\mathbb{Q}(\mu_p)$. A deep conjecture, called the Kummer–Vandiver conjecture, states that p does not divide the class number of $\mathbb{Q}(\mu_p)^+$. There is substantial numerical evidence for this conjecture. Using Iwasawa theory, one may prove that if Kummer–Vandiver's conjecture holds, then for $F = \mathbb{Q}(\mu_p)$, the p-Hilbert class field of F, i.e. the maximal abelian, unramified, p-extension of F is contained in the composite of all $\mathbb{Z}_p$-extensions of F.

4 Greenberg's Pseudonullity Conjecture

The discussion above gives an indication that Iwasawa theory provides insights into understanding certain subquotients of the absolute Galois groups of number fields. Indeed, there are analogous statements for global fields as well[6]. Greenberg postulated a far-reaching generalisation of Vandiver's conjecture, and particular cases of this conjecture are known to be true[7]. While Iwasawa's $\mu = 0$ conjecture is a statement about the l-torsion part of the pro-l Hilbert class field of the cyclotomic $\mathbb{Z}_l$-extension of a number field F, Greenberg's Pseudonullity Conjecture[8] is a statement about the $\mathbb{Z}_l$-rank for totally real number fields. Let F be a totally real number field and let $F_{l,\mathrm{cyc}}$ be the cyclotomic $\mathbb{Z}_l$-extension of F. Consider the pro-l-Hilbert class field $X_{\mathrm{nr},\mathrm{cyc}}$ of $F_{l,\mathrm{cyc}}$, which is a torsion module over $\mathbb{Z}_l[[G]]$ with $G = \mathrm{Gal}(F_{l,\mathrm{cyc}}/F)$. Greenberg's conjecture is the statement that the Iwasawa invariants λ and μ are zero for $X_{\mathrm{nr},\mathrm{cyc}}$. In particular, the Galois group $X_{\mathrm{nr},\mathrm{cyc}}$ is finite and has Krull dimension zero as a module over $\mathbb{Z}_l[[T]]$.

More generally, suppose that R is a commutative Noetherian ring with Krull dimension t and let M be a finitely generated R-module. Then, M is said to be pseudonull if the Krull dimension of M is at most $t-2$. In other words, M is pseudonull if it is of codimension at least 2 as an R-module. Let F be a number field and let $\tilde{F}$ be the composite of all $\mathbb{Z}_l$-extensions of F. Then, the Galois group $G = \mathrm{Gal}(\tilde{F}/F) \simeq \mathbb{Z}_l^d$ and let R be the Iwasawa algebra $\mathbb{Z}_l[[G]]$. Further, R is isomorphic to the power series ring $\mathbb{Z}_l[[T_1, \ldots, T_d]]$ in d variables, and has Krull dimension $d+1$. There is another conjecture of Greenberg that generalises the above conjecture to the field $\tilde{F}$. Let $\tilde{\mathcal{L}}$ be the pro-l Hilbert class field of $\tilde{F}$, which again is a finitely generated torsion module over R. Set

$$\tilde{X} = \mathrm{Gal}(\tilde{\mathcal{L}}/\mathcal{L}).$$

For a finite Galois extension L such that $F \subset L \subset \tilde{F}$, let $\mathrm{Cl}_l(L)$ denote the l-Sylow subgroup of the class group of L. The Galois group $\mathrm{Gal}(L/F)$ acts on $\mathrm{Cl}_l(L)$. Consider the inverse limit

$$\mathcal{A} := \varprojlim \mathrm{Cl}_l(L)$$

where the inverse limit is taken with respect to the norm maps. The $\mathbb{Z}_l$-module $\mathcal{A}$ naturally acquires a structure of an R-module and it is finitely generated as an R-module, with R as above. Further, by Class field theory, $\mathcal{A}$ can be identified with $\tilde{X}$, the Galois group of the pro-l-Hilbert class field $\tilde{\mathcal{L}}$, of $\tilde{F}$. Greenberg's Pseudonullity Conjecture is the statement that $\tilde{X}$ is pseudonull as an R-module. We remark that analogous conjectures can be formulated for Iwasawa modules arising from the Iwasawa theory of elliptic curves. These statements postulate the sizes of subquotients of the absolute Galois group G_F and also have interesting consequences in studying the arithmetic of Galois representations over infinite extensions of algebraic number fields.

Coates[9] observed that the techniques in Iwasawa's study of class numbers could be fruitfully applied to the study of the growth of Mordell–Weil ranks of elliptic curves over number fields along the finite layers of cyclotomic extensions. In particular, this led to proving the following particular case of the celebrated Birch and Swinnerton-Dyer conjecture. Suppose E is an elliptic curve defined over an imaginary quadratic field K with complex multiplication by K. If the complex L-function of E satisfies $L(E,1) = 0$, then $E(K)$ is finite. The Iwasawa modules that one studies in the Iwasawa theory of Galois representations associated to elliptic curves are the Selmer groups of elliptic curves. It is germane to mention that there are conjectural analogues of Iwasawa's $\mu = 0$ conjecture, as well as Greenberg's Pseudonullity Conjecture[10] for modules arising from the study of Iwasawa theory for Galois representations associated to elliptic curves.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Received: 14 September 2022 Accepted: 14 September 2022
Published online: 6 December 2022

References

1. Serre J-P (1994) Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques. In: Motives (Seattle, WA 1991), Proc. symp. pure math., vol 55, pp 377–400
2. Washington L (1997) Introduction to cyclotomic fields, second ed., graduate texts in mathematics. Springer, New York
3. Ribet K (1995) Galois representations and modular forms. Bull Am Math Soc 32:375–402
4. Iwasawa K (1959) On Γ-extensions of algebraic number fields. Bull Am Math Soc 65:183–226
5. Iwasawa K (1973) On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann Math 98:246–326
6. Greenberg R (1978) On the structure of certain Galois groups. Invent Math 47:85–99
7. McCallum WG (2001) Greenberg's conjecture and units in multiple $\mathbb{Z}_p$ -extensions. Am J Math 123:909–930
8. Greenberg R (2001) Iwasawa theory-past and present. Adv Stud Pure Math 30:335–385
9. Coates J (1991) Elliptic curves with complex multiplication and Iwasawa theory. Bull Lond Math Soc 23:321–350
10. Coates J, Sujatha R (2005) Fine Selmer groups of elliptic curves over p-adic Lie extensions. Math Annalen 331:809–839

Sujatha Ramdorai is a Tier 1 Canada Research Chair in Mathematics biography at the Department of Mathematics, University of British Columbia. Her research focus is on Galois representations and their intertwinings with algebra, arithmetic and geometry.