Odd Galois representations

Benedict H. Gross

Elie Cartan studied involutions i of complex, semi-simple Lie algebras $\mathfrak{g}$ in order to determine their real forms. He proved the inequality

$$-\mathrm{rank}(\mathfrak{g}) \leq \mathrm{Tr}(i|\mathfrak{g}) \leq \dim(\mathfrak{g})$$

and constructed an involution τ with

$$\mathrm{Tr}(\tau|\mathfrak{g}) = -\mathrm{rank}(\mathfrak{g}).$$

The conjugacy class of τ in $\mathrm{Aut}(\mathfrak{g})$ is determined uniquely by this identity.

In fact, there is a Cartan sub-algebra $\mathfrak{h}$ in the -1 eigenspace for τ, and τ interchanges the root spaces $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ in the Cartan decomposition of $\mathfrak{g} = \mathfrak{h} + \bigoplus_{\alpha \neq 0} \mathfrak{g}_\alpha$. Cartan and Weyl used the involution τ to study the compact real form of $\mathfrak{g}$; for an explicit construction of τ see [S1, Ch. VI, §4].

We call a Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathfrak{g})$$

odd if the image $\rho(c)$ of any complex conjugation c in the Galois group lies in the conjugacy class of τ in $\mathrm{Aut}(\mathfrak{g})$.

For example, if $\mathfrak{g} = \mathfrak{s}\ell_2$ the group $\mathrm{Aut}(\mathfrak{g}) = PGL_2(\mathbb{C})$ has exactly two conjugacy classes of involutions—represented by the identity e and the involution τ. A representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to PGL_2(\mathbb{C})$$

is odd provided that $\rho(c) \neq e$. In this case, ρ lifts to a two-dimensional Galois representation (cf. [S2, pgs. 226-227])

$$\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$$

with $\tilde{\rho}(c)$ conjugate to the involution $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $GL_2(\mathbb{C})$ of trace zero. This is the condition which Serre uses to define an "odd two-dimensional Galois representation."

More generally, Serre defines an odd modular two-dimensional Galois representation

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F),$$

where F is a finite field, by insisting that $\mathrm{Tr}\ \overline{\rho}(c) = 0$ in F. His conjectures (proved by Khare and Wintenberger) state that all odd, irreducible, modular two-dimensional representations arise from a construction of Deligne, starting from a cuspidal modular form (mod p), where $p = \mathrm{char}(F)$.

The involution τ studied by Cartan also appears in the Langlands parameters of discrete series for real, simply-connected Lie groups. We begin with a discussion of these parameters, which are homomorphisms from the Weil group of $\mathbb{R}$ to the L-group. We then review the theory of algebraic modular forms on a simply connected algebraic group G over $\mathbb{Q}$ whose real points $G(\mathbb{R})$ are compact.

Associated to a Hecke eigenspace in the space of algebraic modular forms, with eigenvalues in the number field E, we conjectured the existence of a compatible system of p-adic representations

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to {}^{L}G(E \otimes \mathbb{Q}_p).$$

Composing this with the action of ${}^LG$ on the Lie algebra $\hat{\mathfrak{g}}$ of the (adjoint) dual group $\hat{G}$, we obtain homomorphisms

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\hat{\mathfrak{g}}(E_p)),$$

which should be odd in the sense defined above. The reduction of these Galois representations (mod p) should provide a large supply of odd modular Galois representations to ${}^LG(F)$, generalizing those studied by Serre.

1. The Weil group of $\mathbb{R}$

We review some facts about the Weil group $W(\mathbb{R})$ of $\mathbb{R}$. A basic reference is [T, (1.4.3)].

The group $W(\mathbb{R})$ is isomorphic to the normalizer of the subgroup $\mathbb{C}^*$ in $\mathbb{H}^*$, where $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ denotes Hamilton's quaternions. It is the union of two components

$$W(\mathbb{R}) = \mathbb{C}^* \cup \mathbb{C}^* j$$

where $j^2 = -1$ and $jzj^{-1} = \overline{z}$ for all $z \in \mathbb{C}^*$. The canonical map $W(\mathbb{R}) \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ has kernel $\mathbb{C}^*$, and the exact sequence

$$1 \to \mathbb{C}^* \to W(\mathbb{R}) \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to 1$$

is *not* split (the only involutions in $\mathbb{H}^*$ are ± 1). Finally the commutator subgroup of $W(\mathbb{R})$ is equal to the elements S^1 in $\mathbb{C}^*$ with norm 1, and $W(\mathbb{C})^{ab} \simeq \mathbb{R}^*$.

The quotient group $W(\mathbb{R})/\langle \pm 1 \rangle$ has a simpler structure. The map sending z in $\mathbb{C}^*$ to the pair $(z/\overline{z}, z\overline{z})$ identifies $\mathbb{C}^*/\langle \pm 1 \rangle$ with the product $S^1 \times \mathbb{R}_+^*$. Let σ be an involution acting on S^1 by inversion and acting trivially on $\mathbb{R}_+^*$. Then the map sending j to σ identifies

$$\begin{aligned} W(\mathbb{R})/\langle \pm 1 \rangle &\simeq (S^1 \times \mathbb{R}_+^*) \rtimes \langle 1, \sigma \rangle \\ &= S^1 \rtimes \langle 1, \sigma \rangle \times \mathbb{R}_+^* \end{aligned}$$

The maximal compact subgroup $S^1 \rtimes \langle 1, \sigma \rangle$ of $W(\mathbb{R})/\langle \pm 1 \rangle$ is of dihedral type. In particular, every self-dual irreducible representation of $W(\mathbb{R})/\langle \pm 1 \rangle$ is orthogonal.

2. The parameters of discrete series

In this section, we give the Langlands parameters for irreducible complex representations V of a compact, simply-connected real Lie group G. A reference is [B, 10.5], although this contains some incorrect statements about the Weil group $W(\mathbb{R})$.

Let $T \subset G$ be a maximal torus, and let $B_{\mathbb{C}} \subset G_{\mathbb{C}}$ be a Borel subgroup containing $T_{\mathbb{C}}$. Let λ be the highest weight of T on V, with respect to the system of positive roots determined by the choice of $B_{\mathbb{C}}$. Let ρ be half the sum of the positive roots. Since G is simply-connected, ρ is a character of T, and we define

$$\mu = \lambda + \rho \quad \text{in} \quad X^*(T) = \mathrm{Hom}(T, S^1)$$

Then μ gives the (regular) infinitesimal character of the center of $U(\mathfrak{g}_{\mathbb{C}})$ acting on V.

The Langlands parameter φ of V is a group homomorphism

$$\varphi : W(\mathbb{R}) \to {}^LG = \hat{G}_{\mathbb{C}} \rtimes \mathrm{Gal}(\mathbb{C}/\mathbb{R}).$$

Here $\hat{G}_{\mathbb{C}}$ is the complex dual group, of adjoint type, and $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\hat{G}_{\mathbb{C}}$ through an outer involution (possibly trivial). Let $\hat{T}_{\mathbb{C}}$ be a maximal torus in $\hat{G}_{\mathbb{C}}$. By the definition of the dual group, we have a canonical isomorphism

$$\mathrm{Hom}_{\mathrm{alg.}}(\mathbb{C}^*, \hat{T}_{\mathbb{C}}) = \mathrm{Hom}_{\mathrm{cont.}}(T, S^1).$$

On the subgroup $\mathbb{C}^*$ of $W(\mathbb{R})$, we have

$$\varphi(z) = \mu(z/\overline{z}) \quad \text{in} \quad \hat{T}_{\mathbb{C}}.$$

Moreover,

$$\varphi(j) = n$$

is an element in the normalizer of $\hat{T}_{\mathbb{C}}$ in ${}^LG$ which acts by inversion on $\hat{T}_{\mathbb{C}}$. Thus

$$n \equiv -1 \quad \text{in} \quad {}^LW = N_{{}^LG}(\hat{T}_{\mathbb{C}})/\hat{T}_{\mathbb{C}}.$$

The co-character μ is regular, so the centralizer of φ in $\hat{G}_{\mathbb{C}}$ is the finite group $\hat{T}_{\mathbb{C}}[2]$ of elements of order 2 in $\hat{T}_{\mathbb{C}}$.

Since ρ is a character of T, $\varphi(-1) = 1$ and the Langlands parameter of V factors through the quotient group $W(\mathbb{R})\langle \pm 1\rangle \simeq S^1 \rtimes \langle 1, \tau\rangle \times \mathbb{R}_+^*$. It is trivial on $\mathbb{R}_+^*$, and satisfies

$$\begin{cases} \varphi(\alpha) = \mu(\alpha) & \text{for} \quad \alpha \quad \text{in} \quad S^1 \\ \varphi(\tau) = n \end{cases}$$

In particular, $n^2 = 1$ in ${}^LG$ and n acts as -1 on $\mathrm{Lie}(\hat{T}_{\mathbb{C}})$. This implies that

$$\mathrm{Tr}(n|\mathrm{Lie}(\hat{G}_{\mathbb{C}})) = -\dim(T)$$

as n must interchange the positive and negative root spaces on $\mathrm{Lie}(\hat{G}_{\mathbb{C}})$.

We recall that E. Cartan proved the inequality

$$\text{-rank}(\mathfrak{g}) \leq \mathrm{Tr}(i|\mathfrak{g}) \leq \dim(\mathfrak{g})$$

for any involution i of a complex semi-simple Lie algebra, and that the involutions with $\mathrm{Tr}(\tau) = -\mathrm{rank}(\mathfrak{g})$ form a single conjugacy class in $\mathrm{Aut}(\mathfrak{g})$. By the above remarks, the involution $n = \varphi(j)$ lies in the conjugacy class of τ in $\mathrm{Aut}(\hat{\mathfrak{g}}_{\mathbb{C}})$.

The parameters φ also occur for discrete series representations of inner forms G' of G. See [G-R] for more details. They are the only

Langlands parameters of $W(\mathbb{R})$ where the centralizer of φ in $\hat{G}_{\mathbb{C}}$ is finite. There are slightly more general parameters involving the involution τ, where μ is replaced by an arbitrary (not necessarily regular) co-character of $\hat{T}$. These correspond to irreducible representations which are "limits of discrete series".

Serre has shown that the inequality

$$\text{-rank}(\mathfrak{g}) \leq \mathrm{Tr}(s|\mathfrak{g}) \leq \dim(\mathfrak{g})$$

holds more generally for any automorphism s of finite order. Equality holds on the left only when s is conjugate to τ and on the right only when $s = e$.

3. Algebraic modular forms

We now assume G is a simply-connected algebraic group over $\mathbb{Q}$, whose real points $G(\mathbb{R})$ are compact. A theory of algebraic modular forms for G was developed in [G2]; we review parts of it here.

Let G_0 be the quasi-split inner form of G and let k be the splitting field of G_0. The L-group of G is a semi-direct product.

$$^LG = \hat{G} \rtimes \mathrm{Gal}(k/\mathbb{Q}),$$

where $\hat{G}$ is the split group, of adjoint type, which is dual to G over $\mathbb{Q}$.

Let V be an absolutely irreducible algebraic representation of G, and let $K = \Pi K_\ell \subset G(\hat{\mathbb{Q}})$ be an open compact subgroup. The space $M(V, K)$ of modular forms of weight V and level K is defined as the $\mathbb{Q}$-vector space:

$$M(V, K) = \{f : G(\hat{\mathbb{Q}})/K \to V : f(\gamma g) = \gamma f(g) \quad \text{for all} \quad \gamma \quad \text{in } G(\mathbb{Q})\}.$$

This is finite-dimensional, and has an action of the Hecke algebra $\mathcal{H}$ of K [G2, Ch. II, §7].

Associated to a simple $\mathcal{H}$-submodule $N \subset M(V, K)$ we conjecture the existence of a compatible system of p-adic Galois representations

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to {}^LG(E \otimes \mathbb{Q}_p).$$

Here E is the center of $\mathrm{End}_{\mathcal{H}}(N)$, which is either totally real or a CM-field. The representation ρ should be unramified at all primes $\ell \neq p$ where K_ℓ is hyperspecial, and the semi-simple part of $\rho(\mathrm{Frob}_\ell)$ should be an E-rational class, independent of p, determined by the $\mathcal{H}_\ell$-module structure of N. Finally, the representation ρ should be *odd*:

$\rho(c)$ should be conjugate to the involution n in the previous section (or to τ in $\mathrm{Aut}(\hat{\mathfrak{g}})$). Indeed, the local representation associated to N at the real place is $V \otimes \mathbb{C}$, which is in the discrete series of $G(\mathbb{R})$.

Since algebraic modular forms are easy to calculate, this predicts the existence of a large supply of odd Galois representations. Some explicit calculations are given in [G1] and [G-P]. .

4. Bibliography

[B] A. Borel, Automorphic L-functions. *Proc. Symp. Pure Math. AMS* 33 (1979), 27–61.

[G1] B. Gross,Modular forms (mod p) and Galois representations. *IMRN* 16 (1998), 865–875.

[G2] B. Gross, Algebraic modular forms. *Israel J. of Math.* 113 (1999), 61–93.

[G-P] B. Gross and D. Pollack, On the Euler characteristic of the discrete spectrum. *J. Number Theory* 110 (2005), 136–163.

[G-R] B. Gross and M. Reeder, From Laplace to Langlands via representations of orthogonal groups. *Bull. AMS* 43 (2006), 163–205.

[S1] J.-P. Serre, *Complex semi-simple Lie algebras*, Springer, 1987.

[S2] J.-P. Serre, Modular forms of weight one and Galois representations. *Algebraic Number Fields* (1977), 193–268.

[T] J. Tate, Number theoretic background. *Proc. Symp.Pure Math. AMS* 33 (1979), 3–26.