Self-dual Galois representations

CCR West, November 2008

Asher Auel University of Pennsylvania (joint with Ted Chinburg) $\rho: G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ $L(s, \rho)$ $W(\rho) = \epsilon(\frac{1}{2}, \rho)$ ρ^{\vee}

 K/\mathbb{Q}

- finite Galois extension with group $\operatorname{Gal}(K/\mathbb{Q})$
- $\rho: G \hookrightarrow \operatorname{GL}_n(\mathbb{C})$ faithful finite dimensional complex representation of $G = \operatorname{Gal}(K/\mathbb{Q})$

continuous finite dimensional complex Galois representation of the absolute Galois group $G_{\mathbb{Q}} = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Artin $L\text{-function of }\rho$

root number, sign of the functional equation of the completed Artin L- function of ρ

dual representation, $\rho^{\vee}(g)=\rho(g^{-1})^t$

1. Root numbers of *self-dual* Galois representations

$$\rho \cong \rho^{\vee}$$

1. Root numbers of *self-dual* Galois representations

 $\rho \cong \rho^{\vee}$

- (a) Symplectic representations
 - Quaternion representations
 - Galois module structure of algebraic integers

(b) Orthogonal representations

- Theorem of Fröhlich and Queyrut
- Deligne's interpretation in terms of Stiefel-Whitney classes

2. Consider of "essentially self-dual" Galois representations

$$\rho \cong \rho^{\vee} \otimes \lambda$$

for a fixed 1-dimensional Galois representation λ .

2. Consider of "essentially self-dual" Galois representations

 $\rho \cong \rho^{\vee} \otimes \lambda$

for a fixed 1-dimensional Galois representation λ .

(a) Symplectic essentially self-dual

• 2-dimensional representations

(b) Orthogonal essentially self-dual

• A new generalization of the 2nd Stiefel-Whitney class

Lemma. If ρ is irreducible and self-dual then either

- ρ is symplectic, i.e. ρ is isomorphic to $\rho' : G_{\mathbb{Q}} \to \operatorname{Sp}_{2n}(\mathbb{C})$, equivalently, to $\rho'' : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{H})$, or
- ρ is orthogonal, i.e. ρ is isomorphic to $\rho' : G_{\mathbb{Q}} \to O_n(\mathbb{C})$, equivalently, to $\rho'' : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{R})$.

Lemma. If ρ is irreducible and self-dual then either

- ρ is symplectic, i.e. ρ is isomorphic to $\rho' : G_{\mathbb{Q}} \to \operatorname{Sp}_{2n}(\mathbb{C})$, equivalently, to $\rho'' : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{H})$, or
- ρ is orthogonal, i.e. ρ is isomorphic to $\rho' : G_{\mathbb{Q}} \to O_n(\mathbb{C})$, equivalently, to $\rho'' : G_{\mathbb{Q}} \to GL_n(\mathbb{R})$.

Proof. Fixing an isomorphism $\varphi: \rho \xrightarrow{\sim} \rho^{\vee}$,

$$\operatorname{Hom}_{\mathbb{C}}(\rho,\rho) \cong \rho^{\vee} \otimes \rho \xrightarrow{\varphi} \rho^{\vee} \otimes \rho^{\vee} \cong \operatorname{Sym}^{2}(\rho^{\vee}) \oplus \bigwedge^{2}(\rho^{\vee}),$$

which, by Schur's lemma, has 1-dimensional $G_{\mathbb{Q}}$ -invariants.

Example. Generalized quaternion groups (or binary dihedral groups):

$$H_{4n} = \langle x, y \mid x^4 = 1, y^n = x^2, xyx^{-1} = y^{-1} \rangle$$

of order 4n, for $n \ge 2$. Then H_{4n} has an irreducible symplectic 2-dimensional complex representation

$$\rho: H_{4n} \to \operatorname{Sp}_2(\mathbb{C}) \subset \operatorname{GL}_2(\mathbb{C})$$
$$x \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$y \mapsto \begin{pmatrix} \zeta_{2n} & 0 \\ 0 & \zeta_{2n}^{-1} \end{pmatrix}$$

Example. Dihedral groups:

$$D_{2n} = \langle x, y \mid x^2 = y^n = 1, xyx^{-1} = y^{-1} \rangle$$

of order 2n, for $n \ge 3$. Then D_{2n} has an irreducible orthogonal 2-dimensional complex representation

$$\rho: D_{2n} \to \operatorname{GL}_2(\mathbb{C})$$
$$x \mapsto \begin{pmatrix} 0 & 1\\ 1 & 0 \end{pmatrix}$$
$$y \mapsto \begin{pmatrix} \zeta_n & 0\\ 0 & \zeta_n^{-1} \end{pmatrix}$$

Example. Dihedral groups:

$$D_{2n} = \langle x, y \mid x^2 = y^n = 1, xyx^{-1} = y^{-1} \rangle$$

of order 2n, for $n \ge 3$. Then D_{2n} has an irreducible orthogonal 2-dimensional complex representation

$$\rho: D_{2n} \to \operatorname{GL}_2(\mathbb{C}) \qquad \rho': D_{2n} \to \operatorname{O}_2(\mathbb{R})$$

$$x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$y \mapsto \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix} \qquad y \mapsto \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}$$

Functional equation for the completed Artin L-function

$$\Lambda(1-s,\rho) = W(\rho)\,\Lambda(s,\overline{\rho}),$$

where $W(\rho) \in \mathbb{C}$ is the root number:

•
$$|W(\rho)| = 1$$

•
$$W(\rho_1 \oplus \rho_2) = W(\rho_1)W(\rho_2)$$

• $W(\rho) = \prod_{v} W_v(\rho_v)$

Functional equation for the completed Artin L-function

$$\Lambda(1-s,\rho) = W(\rho)\,\Lambda(s,\overline{\rho}),$$

where $W(\rho) \in \mathbb{C}$ is the root number:

•
$$|W(\rho)| = 1$$

•
$$W(\rho_1 \oplus \rho_2) = W(\rho_1)W(\rho_2)$$

- $W(\rho) = \prod_{v} W_v(\rho_v)$
- $W(\rho) = \pm 1$ if ρ is self-dual

Question. How to determine the sign of $W(\rho)$ for self-dual representations?

Symplectic representations. Work of Serre, Armitage, Fröhlich, Cassou-Noguès, Taylor.

Let K/\mathbb{Q} be a finite extension with $G = \operatorname{Gal}(K/\mathbb{Q})$. Assume K/\mathbb{Q} is tamely ramified, i.e. $p \not| e_p$ for all primes p.

 $W(\rho)$ for symplectic $\longleftrightarrow \mathbb{Z}[G]$ -module structure of representations ρ of G the ring of integers \mathcal{O}_K **Symplectic representations.** Work of Serre, Armitage, Fröhlich, Cassou-Noguès, Taylor.

Let K/\mathbb{Q} be a finite extension with $G = \operatorname{Gal}(K/\mathbb{Q})$. Assume K/\mathbb{Q} is tamely ramified, i.e. $p \not| e_p$ for all primes p.

 $W(\rho)$ for symplectic $\longleftrightarrow \mathbb{Z}[G]$ -module structure of representations ρ of G the ring of integers \mathcal{O}_K

Normal basis theorem. $K \cong \mathbb{Q}[G]$ as $\mathbb{Q}[G]$ -modules.

Symplectic representations. Work of Serre, Armitage, Fröhlich, Cassou-Noguès, Taylor.

Let K/\mathbb{Q} be a finite extension with $G = \operatorname{Gal}(K/\mathbb{Q})$. Assume K/\mathbb{Q} is tamely ramified, i.e. $p \not| e_p$ for all primes p.

 $W(\rho)$ for symplectic $\longleftrightarrow \mathbb{Z}[G]$ -module structure of representations ρ of G the ring of integers \mathcal{O}_K

Normal basis theorem. $K \cong \mathbb{Q}[G]$ as $\mathbb{Q}[G]$ -modules.

Theorem. [Noether, 1932] The ring of integers \mathcal{O}_K is a locally free $\mathbb{Z}[G]$ -module iff K/\mathbb{Q} is at most tamely ramified.

Assume K/\mathbb{Q} is at most tamely ramified, $G = \operatorname{Gal}(K/\mathbb{Q})$. Classical results:

- (Hilbert) If G is abelian, then $\mathcal{O}_K \cong \mathbb{Z}[G]$.
- (Martinet, 1969) If $G \cong D_{2p}$, with p an odd prime, then $\mathcal{O}_K \cong \mathbb{Z}[G]$.
- (Martinet, 1971) If $G \cong Q = H_8$, then there exists K/\mathbb{Q} with $\mathcal{O}_K \not\cong \mathbb{Z}[G]$.

(Martinet, 1971) Then there is exactly one non-trivial isomorphism class M of locally free $\mathbb{Z}[Q]$ -modules of rank 1. If K/\mathbb{Q} is a tame Q-extension with discriminant $D_{K/\mathbb{Q}}$, then

$$\delta \prod_{p \mid D_{K/\mathbb{Q}}} p \equiv u \frac{1 + d_1 + d_2 + d_3}{4} \mod 4,$$

where $d_i = D_{L_i/\mathbb{Q}}$, and

$$\delta = \begin{cases} 1 & K \text{ is totally real} \\ -1 & K \text{ is totally complex} \end{cases}$$
$$u = \begin{cases} 1 & \mathcal{O}_K \cong \mathbb{Z}[Q] \\ -1 & \mathcal{O}_K \cong M \end{cases}$$

Example.



Example.



• (Fröhlich, 1972) For K/\mathbb{Q} a tame Q-extension, then

$$W(K/\mathbb{Q}) = u(K/\mathbb{Q}) = \begin{cases} 1 & \mathcal{O}_K \cong \mathbb{Z}[Q] \\ -1 & \mathcal{O}_K \cong M \end{cases},$$

where $W(K/\mathbb{Q}) = W(\rho)$, where $\rho : Q \to \operatorname{Sp}_2(\mathbb{C})$ is the unique irreducible symplectic representation of Q.

• (Fröhlich, 1972) For K/\mathbb{Q} a tame Q-extension, then

$$W(K/\mathbb{Q}) = u(K/\mathbb{Q}) = \begin{cases} 1 & \mathcal{O}_K \cong \mathbb{Z}[Q] \\ -1 & \mathcal{O}_K \cong M \end{cases},$$

where $W(K/\mathbb{Q}) = W(\rho)$, where $\rho : Q \to \operatorname{Sp}_2(\mathbb{C})$ is the unique irreducible symplectic representation of Q.

• (Taylor, 1981) Let K/\mathbb{Q} be a tame *G*-extension, then the $\mathbb{Z}[G]$ -module structure of \mathcal{O}_K is "completely determined" by the root numbers of symplectic representations of *G*. In particular, if $W(\rho) = 1$ for all symplectic representations ρ of *G*, then $\mathcal{O}_K \cong \mathbb{Z}[G]$.

Orthogonal representations. From the global point of view, there isn't much to say here:

Theorem. [Fröhlich and Queyrut, 1973] Let ρ be an orthogonal Galois representation, then

 $W(\rho) = 1.$

Orthogonal representations. From the global point of view, there isn't much to say here:

Theorem. [Fröhlich and Queyrut, 1973] Let ρ be an orthogonal Galois representation, then

$$W(\rho) = 1.$$

Use induction from the cases:

- quadratic characters $\chi_a: G_{\mathbb{Q}} \to \operatorname{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) \to \{\pm 1\},\$
- $\psi \oplus \overline{\psi}$ for cyclic characters $\psi : G_{\mathbb{Q}} \twoheadrightarrow C_n \hookrightarrow \mathbb{C}^{\times}$, and
- dihedral representations $\rho: G_{\mathbb{Q}} \twoheadrightarrow D_{2n} \hookrightarrow O_2(\mathbb{C}).$

Deligne's approach. There's a decomposition into local root numbers,

$$W(\rho) = \prod_{v} W_v(\rho_v),$$

where v ranges over the places of ${\mathbb Q}$ and

$$\rho_v: G_{\mathbb{Q}_v} \to \mathrm{GL}_n(\mathbb{C})$$

is the local v-adic component of ρ , i.e. restriction to the a decomposition group of v. Here $W_v(\rho_v)$ is defined using Deligne's theory of local ϵ -constants.

Lemma. For ρ_v a local self-dual Galois representation,

 $W_v(\rho_v) \in \{\pm 1, \pm i\}.$

Proof. For local Galois representations,

$$W_v(\rho_v)W_v(\rho_v^{\vee}) = \det(\rho)(-1),$$

where -1 is considered in $G_{\mathbb{Q}_v}$ via the norm-residue symbol of local class field theory.

Example. (Quadratic characters) Let χ_a be the quadratic character associated to $a \in \mathbb{Q}_v^{\times}/\mathbb{Q}_v^{\times 2}$,

$$\chi_a(g) = \frac{g\sqrt{a}}{\sqrt{a}}, \quad g \in G_{\mathbb{Q}_v}.$$

When v is real, we have:

a $ $	1	-1
$W_v(\chi_a)$	1	-i

When v = p is a finite place, local root numbers are evaluated by certain local Gauss sums. These calculation were first performed by Gauss.

	a	1	-1	2	-2	5	-5	10	-10
p=2	$W_2(\chi_a)$	1	-i	i	i	1	i	-1	-i

	a	1	u	p	up
$p \equiv 1(4)$	$W_p(\chi_a)$	1	1	1	-1
$p \equiv 3(4)$	$W_p(\chi_a)$	1	1	-i	i

With some work, one also proves, for ρ_v a local orthogonal Galois representation,

$$W(\rho_v)/W(\det(\rho_v)) \in \{\pm 1\}.$$

Deligne identifies this sign with a Stiefel-Whitney class $sw_2(\rho_v) \in H^2(G_{\mathbb{Q}_v}, \{\pm 1\}) \cong \{\pm 1\}.$

This class is the obstruction to lifting an orthogonal representation to a representation of the "pin" group:

$$1 \longrightarrow \{\pm 1\} \longrightarrow \operatorname{Pin}_{n}(\mathbb{C}) \longrightarrow \operatorname{O}_{n}(\mathbb{C}) \longrightarrow 1$$

Via the "long exact sequence" of pointed non-abelian Galois cohomology sets of trivial Galois modules,

$$H^{1}(G_{\mathbb{Q}_{v}}, \operatorname{Pin}_{n}(\mathbb{C})) \to H^{1}(G_{\mathbb{Q}_{v}}, \operatorname{O}_{n}(\mathbb{C})) \xrightarrow{d^{1}} H^{2}(G_{\mathbb{Q}_{v}}, \{\pm 1\})$$
$$[\rho_{v}] \mapsto sw_{2}(\rho_{v})$$

Via the "long exact sequence" of pointed non-abelian Galois cohomology sets of trivial Galois modules,

$$H^{1}(G_{\mathbb{Q}_{v}}, \operatorname{Pin}_{n}(\mathbb{C})) \to H^{1}(G_{\mathbb{Q}_{v}}, \operatorname{O}_{n}(\mathbb{C})) \xrightarrow{d^{1}} H^{2}(G_{\mathbb{Q}_{v}}, \{\pm 1\})$$
$$[\rho_{v}] \mapsto sw_{2}(\rho_{v})$$

Theorem. [Deligne, 1976] Let ρ_v be a local orthogonal Galois representation, then

$$sw_2(\rho_v) = W_v(\rho_v)/W_v(\det(\rho_v)),$$

under the identification $H^2(G_{\mathbb{Q}_v}, \{\pm 1\}) \cong \{\pm 1\}.$

Embedding problems in inverse Galois theory.

 ρ is the inflation from a finite Galois group $G = \operatorname{Gal}(K/\mathbb{Q})$



Then $sw_2(\rho) \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is precisely the obstruction to the embedding problem $(\tilde{G}, K/\mathbb{Q})$.

Klein four inside quaternion extensions.

V the Klein four group, $V \hookrightarrow O_2(\mathbb{C})$ diagonal embedding



 $K = \mathbb{Q}(\sqrt{a},\sqrt{b})/\mathbb{Q}$ can be embedded into a quaternion extension iff

$$W_v(\chi_a) W_v(\chi_b) / W_v(\chi_{ab}) = 1$$
 for every place v

Proof. (of the Fröhlich-Queyrut theorem) In the same way, the global orthogonal representation,

 $\rho: G_{\mathbb{Q}} \to \mathcal{O}_n(\mathbb{C}),$

has a Stiefel-Whitney class $sw_2(\rho) \in H^2(G_{\mathbb{Q}}, \{\pm 1\})$. Now,

$$W(\rho) = W(\rho)/W(\det(\rho)) = \prod_{v} W_v(\rho_v)/W_v(\det(\rho_v))$$
$$= \prod_{v} sw_2(\rho_v) = \prod_{v} sw_2(\rho)_v = 1$$

using finally the Hasse-Brauer-Noether exact sequence,

$$1 \to H^2(G_{\mathbb{Q}}, \{\pm 1\}) \to \bigoplus_v H^2(G_{\mathbb{Q}_v}, \{\pm 1\}) \xrightarrow{\Pi} \{\pm 1\} \to 1.$$

Essentially self-dual. Fix a Galois character $\lambda : G_{\mathbb{Q}} \to \mathbb{C}^{\times}$. Then a λ -self-dual Galois representation $\rho : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{C})$ satisfies

$$\rho \cong \rho^{\vee} \otimes \lambda.$$

Essentially self-dual. Fix a Galois character $\lambda : G_{\mathbb{Q}} \to \mathbb{C}^{\times}$. Then a λ -self-dual Galois representation $\rho : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{C})$ satisfies

$$\rho \cong \rho^{\vee} \otimes \lambda.$$

Example. For any character λ ,

$$\lambda = \lambda^{\vee} \otimes \lambda^2,$$

so λ is a λ^2 -self-dual representation.

Essentially self-dual. Fix a Galois character $\lambda : G_{\mathbb{Q}} \to \mathbb{C}^{\times}$. Then a λ -self-dual Galois representation $\rho : G_{\mathbb{Q}} \to \operatorname{GL}_n(\mathbb{C})$ satisfies

$$\rho \cong \rho^{\vee} \otimes \lambda.$$

Example. For any character λ ,

$$\lambda = \lambda^{\vee} \otimes \lambda^2,$$

so λ is a λ^2 -self-dual representation.

If ρ_1, ρ_2 are λ -self-dual, then so is $\rho_1 \oplus \rho_2$.

If ρ_i is λ_i -self-dual then $\rho_1 \otimes \rho_2$ is $\lambda_1 \otimes \lambda_2$ -self-dual.

Lemma. Let ρ be an irreducible λ -self-dual Galois representation, then either

- ρ is symplectic similitude, i.e. ρ is isomorphic to a representation $\rho': G_{\mathbb{Q}} \to \mathrm{GSp}_n(\mathbb{C})$, or
- ρ is orthogonal similitude, i.e. ρ is isomorphic to a representation $\rho' : G_{\mathbb{Q}} \to \mathrm{GO}_n(\mathbb{C})$.

 $GO_n(\mathbb{C}) = \{ M \in GL_n(\mathbb{C}) : M^t M = \mu(M) I_n \}$ $GSp_n(\mathbb{C}) = \{ M \in GL_{2n}(\mathbb{C}) : M^t J_n M = \mu(M) J_n \}$ **Symplectic similitude representations.** (The case n = 1) The matrix equation,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & ad - bc \\ -(ad - bc) & 0 \end{pmatrix},$$

proves that $\mathrm{GSp}_1(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})$. In terms of representations,

$$\rho \cong \rho^{\vee} \otimes \det(\rho),$$

for any $\rho: G_{\mathbb{Q}} \to \operatorname{GL}_2(\mathbb{C})$. Any 2-dimensional representation is "determinant-self-dual" of symplectic type!

There's not much hope studying root numbers of arbitrary 2-dimensional representations (though this may be feasible since the finite subgroups of $GL_2(C)$ are classified).

Orthogonal similitude representations.

Question. Does there exist a Deligne style approach to studying root numbers of orthogonal similitude representations using characteristic classes?

Orthogonal similitude representations.

Question. Does there exist a Deligne style approach to studying root numbers of orthogonal similitude representations using characteristic classes?

A new construction. A characteristic class gw_2 for λ -self-dual representations interpolating between the Stiefel-Whitney class and the 1st Chern class.



$$\begin{array}{c|c} H^{1}_{\text{\acute{e}t}}(X, \operatorname{Pin}_{n}) & \longrightarrow & H^{1}_{\text{\acute{e}t}}(X, \operatorname{O}_{n}) \xrightarrow{sw_{2}} H^{2}_{\text{\acute{e}t}}(X, \mu_{2}) \\ & & & & & \\ & & & & \\ H^{1}_{\text{\acute{e}t}}(X, \Gamma_{n}) & \longrightarrow & H^{1}_{\text{\acute{e}t}}(X, \operatorname{GO}_{n}) \xrightarrow{gw_{2}} H^{2}_{\text{\acute{e}t}}(X, \kappa) \\ & & & & \\ & & & & \\ & & & & \\ & & & & \\ H^{1}_{\text{\acute{e}t}}(X, \mathbb{G}_{m}) \xrightarrow{2} H^{1}_{\text{\acute{e}t}}(X, \mathbb{G}_{m}) \xrightarrow{c_{1}} H^{2}_{\text{\acute{e}t}}(X, \mu_{2}) \end{array}$$

Applications.

• Embedding problems of the form

$$1 \to \boldsymbol{\kappa} \to G' \to G \to 1$$

where $\kappa \cong \mathbb{Z}/4\mathbb{Z}$ or $\kappa \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $G \hookrightarrow \mathrm{GO}_n$.

Applications.

• Embedding problems of the form

$$1 \to \mathbf{\kappa} \to G' \to G \to 1$$

where $\kappa \cong \mathbb{Z}/4\mathbb{Z}$ or $\kappa \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $G \hookrightarrow \mathrm{GO}_n$.

• Normalized root number

 $W(\rho)/W(\lambda)$

where $\rho: G_{\mathbb{Q}} \to GO_n$ and $\mu: GO_n \to \mathbb{G}_m$ is the multiplier coefficient homomorphism.