Cubo Matemática Educacional
Vol. 3., N°1, ENERO 2001

Galois Representations in Mordell-Weil Groups of Elliptic Curves

David E. Rohrlich
Department of Mathematics & Statistics
Boston University,
Boston, MA 02215
USA

Consider the following two problems:

Problem 1. *Let G be a finite group. Does there exist a Galois extension K of $\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong G$?*

Problem 2. *Let K be a finite Galois extension of $\mathbb{Q}$ and τ an irreducible complex representation of $Gal(K/\mathbb{Q})$. Does there exist an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of $Gal(K/\mathbb{Q})$ on $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$?*

Of course Problem 1 is the famous "inverse Galois problem". It has a distinguished pedigree going back to Hilbert and E. Noether, and it remains an active topic of research to this day. Problem 2 by contrast has received little attention, but it arises naturally when one investigates the possible vanishing of certain Rankin-Selberg convolutions [9], and in the present expository article it will be treated simply as a natural companion to Problem 1. The remarks and examples which comprise the article are intended to show that this point of view is reasonable. We begin by mentioning a special case in which Problem 2 has an affirmative answer.

1 A Result in low degree

Problem 2 has an affirmative answer whenever τ occurs in the representation of $\mathrm{Gal}(K/\mathbb{Q})$ induced by the trivial representation of a subgroup of index $\leqslant 9$

([11], p. 123). Note that τ is then of dimension $\leqslant 8$. Using Frobenius reciprocity, we may state the result as follows:

Proposition 1 *Let K be a finite Galois extension of $\mathbb{Q}$ and τ an irreducible complex representation of Gal $(K/\mathbb{Q})$. Suppose there is a subfield L of K satisfying the following conditions:*
(a) $[L:\mathbb{Q}] \leqslant 9$.
(b) Gal(K/L) fixes a nonzero vector in the space of τ.

Then there is an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of Gal$(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$.

By way of illustration, consider the case where τ is a character $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ (we use "character" as an abbreviation for "one-dimensional character" when the meaning is clear from context). Take L to be the fixed field of the kernel of χ, so that (ii) holds. If χ has order $\leqslant 9$ then (i) is also satisfied and we deduce that χ occurs in $\mathbb{C} \otimes E(K)$ for some E. Thus Problem 2 has an affirmative answer for characters of order $\leqslant 9$. Actually we can do a little better than this by using the following lemma:

Lemma *If ϵ is a quadratic character of Gal$(K/\mathbb{Q})$ and E^ϵ the corresponding quadratic twist of E then $E^\epsilon(K)$ and $E(K) \otimes \epsilon$ are isomorphic as $\mathbb{Z}[$ Gal$(K/\mathbb{Q})]$-modules.*

Proof. Let $y^2 = x^3 + ax + b$ be an equation for E over $\mathbb{Q}$ and write the fixed field of the kernel of ϵ as $\mathbb{Q}(\sqrt{d})$, where $\sqrt{d}$ denotes a fixed square root of some $d \in \mathbb{Q}$. Then E^ϵ has equation $dy^2 = x^3 + ax + b$ and $(x, y) \mapsto (x, \sqrt{d}y)$ is an isomorphism of $E^\epsilon(K)$ onto $E(K) \otimes \epsilon$.

Suppose now that χ is a character of Gal$(K/\mathbb{Q})$ of order 10, 14, or 18. Then we can write $\chi = \epsilon\xi$ with ϵ as in the lemma and ξ :Gal$(K/\mathbb{Q}) \to \mathbb{C}^\times$ a character of order 5, 7, or 9 respectively. As we have just noted, ξ occurs in some $\mathbb{C} \otimes E(K)$ by Proposition 1, whence χ occurs in $\mathbb{C} \otimes E^\epsilon(K)$ by the lemma.

Remark. More generally, the lemma gives:

Proposition 2 *Problem 2 has an affirmative answer for a given τ if and only if it has an affirmative answer for every quadratic twist of τ.*

Thus Problem 2 is "invariant under quadratic twists".

To summarize, Problem 2 has an affirmative answer for characters of order $\leqslant 10$ and also for characters of order 14 or 18. However the case of an arbitrary character remains open. Note by contrast that when G is abelian Problem 1 is an easy exercise.

The proof of Proposition 1 is elementary. Since $[L:\mathbb{Q}] \leqslant 9$, any 10 elements of L are linearly dependent over $\mathbb{Q}$. On the other hand, there are 10 monomials in

x and y of degree $\leqslant 3$. Thus for each $\xi \in L$ there is a nonzero polynomial $F(x, y)$ over $\mathbb{Q}$ of degree $\leqslant 3$ such that $F(\xi^{-2}, \xi^{-3}) = 0$. If ξ and F are chosen properly then the equation $F(x, y) = 0$ defines a smooth plane cubic with a rational point – in other words an elliptic curve E over $\mathbb{Q}$ – and τ occurs in $\mathbb{C} \otimes E(K)$.

2 Irreducible Trinomials

The same approach sometimes works even when $[L : \mathbb{Q}] > 9$. Here is an example where $[L : \mathbb{Q}]$ is an arbitrary integer $n \geqslant 2$:

Proposition 3 *Let K be a splitting field over $\mathbb{Q}$ of the polynomial $f(u) = u^n - u - 1$.*

(i) Gal($K/\mathbb{Q}$) is isomorphic to S_n, the symmetric group on n letters.

(ii) Let $\xi \in K$ be a root of $f(u) = 0$, and put $L = \mathbb{Q}(\xi)$. Up to isomorphism there is a unique nontrivial irreducible complex representation τ of Gal($K/\mathbb{Q}$) such that Gal(K/L) fixes a nonzero vector in the space of τ. Furthermore, the dimension of τ is $n - 1$.

(iii) Assume that $n \not\equiv 0, 1$ modulo 12. Then there exists an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of Gal($K/\mathbb{Q}$) on $\mathbb{C} \otimes E(K)$.

For a proof of (i) see Selmer [12] and Serre [13], p.42. The key point is the irreducibility of f, which is proved in [12]. Conversely, (i) implies that f is irreducible.

Assertion (ii) amounts by Frobenius reciprocity to a standard fact about representations of S_n (cf.[7], p.50, Ex. 4.14): if H is a subgroup of index n in S_n (necessarily isomorphic to S_{n-1}) then the representation of S_n induced by the trivial representation of H is a direct sum of the trivial representation of S_n and an irreducible representation of dimension $n - 1$. Incidentally, the latter representation is sometimes called the "standard" representation of S_n, but this terminology is dangerous when $n = 6$: there are two conjugacy classes of embeddings of S_5 in S_6 and consequently two inequivalent candidates for the "standard" representation of S_6.

It remains to prove (iii). If $n \leqslant 9$ then the assertion follows from Proposition 1, so we may assume that $n \geqslant 10$. Let d denote the discriminant of K and put $M = \mathbb{Q}(\sqrt{d})$. Then Gal(K/M) is isomorphic to the alternating group A_n and is therefore a nonabelian simple group since $n > 4$. The following result is a slight variant of the proposition on p.129 of [11]:

Proposition 4 *Let K be a finite Galois extension of $\mathbb{Q}$ and τ an irreducible complex representation of $Gal(K/\mathbb{Q})$. Suppose that there are subfields L and M of K satisfying the following conditions:*

(i) $[L:\mathbb{Q}] = 1 + \dim \tau$.

(ii) *$Gal(K/L)$ fixes a nonzero vector in the space of τ.*

(iii) *$Gal(K/M)$ is a nonabelian simple group, M is Galois over $\mathbb{Q}$, and $L \cap M = \mathbb{Q}$.*

If E is any elliptic curve over $\mathbb{Q}$ such that $E(L) \neq E(\mathbb{Q})$ then τ occurs in the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$.

We see that to complete the proof of part (iii) of Proposition 3 it suffices to exhibit an elliptic curve E over $\mathbb{Q}$ together with a point $P \in E(L)$ such that $P \notin E(\mathbb{Q})$. For every congruence class of integers $n \not\equiv 0, 1$ modulo 12 a possible choice of E and P is shown in the following table.

n	E	P
2 mod 3	$y^2 - y = x^3$	$(-\xi^{(1-2n)/3}, \xi^{-n+1})$
2 mod 4	$y^2 = x^3 - x$	$(\xi^{n/2}, \xi^{(n+2)/4})$
3 mod 4	$xy^2 + y = x^3$	$(\xi^{(n+1)/4}, \xi^{(3-n)/4})$
3 mod 6	$y^2 = x^3 + 1$	$(-\xi^{-n/3}, \xi^{(1-n)/2})$
4 mod 6	$y^2 = x^3 + 1$	$(-\xi^{(1-n)/3}, \xi^{-n/2})$

Strictly speaking, since the equation in the third row of the table is not in generalized Weierstrass form, the nonsingular cubic curve E it defines does not deserve to be called an elliptic curve until we designate some point $O \in E(\mathbb{Q})$ as origin. However all that matters is that $E(\mathbb{Q})$ is nonempty, so that some choice of O (e. g. $O = [0:1:0]$ or $O = (0,0)$) is possible.

When $n \equiv 0$ or 1 modulo 12 this elementary approach fails. Furthermore, while it succeeds for many other irreducible trinomials, its applicability is ultimately rather limited: the requirement that a finite Galois extension K of $\mathbb{Q}$ be a splitting field of an irreducible trinomial appears to be a rather severe restriction on K. For example, suppose that p is a prime $\geqslant 13$ which is not a Fermat prime. If K is a splitting field of an irreducible trinomial of degree p then $\mathrm{Gal}(K/\mathbb{Q})$ is either solvable or isomorphic to S_p or A_p (Feit [6], p. 179, Cor. 4.4).

Nonetheless, let us briefly indicate how the argument on pp. 129 – 130 of [11] can be modified to yield a proof of Proposition 4. Put $G = \mathrm{Gal}(K/\mathbb{Q})$, $H = \mathrm{Gal}(K/L)$, and $J = \mathrm{Gal}(K/M)$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be representatives for the distinct left cosets of $J \cap H$ in J, with $\sigma_1 \in H \cap J$. Also choose a point $P \in E(L)$ not belonging to $E(\mathbb{Q})$, and put $v_i = 1 \otimes (P - \sigma_i(P)) \in \mathbb{C} \otimes E(K)$ for $2 \leqslant i \leqslant n$. Let V be the subspace of $\mathbb{C} \otimes E(K)$ spanned by the vectors v_i. Since $L \cap M = \mathbb{Q}$ and M is Galois over $\mathbb{Q}$ we have $G = JH$ by Galois theory, and consequently the elements σ_i are also a set of representatives for the distinct left cosets of H in G. Therefore V is stable under G. In fact let us write "ind" for induction and 1_X for the trivial representation of a group X, so that conditions (i) and (ii) of Proposition 4 take the form $\mathrm{ind}_H^G 1_H = 1_G \oplus \tau$. Then the universal property of the induction functor shows that the representation of G on V is a quotient of τ. Consequently, since τ is irreducible it suffices to show that $V \neq \{0\}$. This is proved just as in [11], except that the symbols G, H, and L of [11] correspond to the present J, $J \cap H$, and LM. Thus the key hypothesis in [11] becomes the requirement that P belong to $E(LM)$ but not to $E(M)$. This condition is in fact satisfied, because P belongs to $E(L)$ but not to $E(\mathbb{Q})$, and $L \cap M = \mathbb{Q}$.

3 L-functions

Although Problem 1 is widely expected to have an affirmative answer, this expectation does not seem to be founded on any broader conjectural framework. By contrast, if one grants the standard conjectures about L-functions then an affirmative answer to a special case of Problem 2 follows as a corollary. To explain this point, let K and τ be as in Problem 2, let E be any elliptic curve over $\mathbb{Q}$, and consider the "Rankin-Selberg convolution" $L(E, \tau, s)$ associated to the tensor product of τ with the ℓ-adic representations determined by E. (More precisely, replace τ by an equivalent representation defined over a number field $\mathbb{E} \subset \mathbb{C}$, and for each place λ of $\mathbb{E}$ over ℓ form the tensor product of the representations at issue by taking their common field of definition to be $\mathbb{E}_\lambda$, the completion of $\mathbb{E}$ at λ). The order of vanishing of $L(E, \tau, s)$ at $s = 1$ is conjectured to satisfy

$$\mathrm{ord}_{s=1} L(E, \tau, s) = \langle \tau, E \rangle, \tag{1}$$

where $\langle \tau, E \rangle$ denotes the multiplicity of τ in $\mathbb{C} \otimes E(K)$. This is also the multiplicity of the dual representation $\check{\tau}$, because the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$ is obtained by extension of scalars from the representation on $\mathbb{Q} \otimes E(K)$ and is therefore defined over $\mathbb{Q}$, hence in particular over $\mathbb{R}$. In any case, we are certainly justified in viewing (1) as one of the "standard conjectures about L-functions", for it is a routine extension of the Birch-Swinnerton-Dyer conjecture and even a formal consequence of the Birch-Swinnerton-Dyer conjecture when the latter is supplemented the Deligne-Gross conjecture (cf. [4], p. 323, Conj. 2.7 (ii) and [9], p. 127, and note that the phrase "complex embedding of the motive" in [9] should be "complex embedding of the coefficient field of the motive"). On the other hand, another standard conjecture – the Hasse-Weil conjecture for motivic L-functions – gives

$$\Lambda(E,\tau,s) = W(E,\tau)\Lambda(E,\bar{\tau},2-s), \tag{2}$$

where $W(E,\tau)$ is a constant of absolute value 1 and

$$\Lambda(E,\tau,s) = ((2\pi)^{-s}\Gamma(s))^{[K:\mathbb{Q}]}D^{s/2}L(E,\tau,s), \tag{3}$$

the quantity $D = D(E,\tau)$ being a certain positive integer. Both $W(E,\tau)$ and $D(E,\tau)$ have a definition independent of [1] and [?] and are in principle computable (cf. [4] and [18]).

Now suppose that τ is self-dual, or equivalently that $\mathrm{tr}\,\tau$ is real-valued. Then [2] becomes $\Lambda(E,\tau,s) = W(E,\tau)\Lambda(E,\tau,2-s)$, whence $W(E,\tau) = \pm 1$ and $\mathrm{ord}_{s=1}L(E,\tau,s)$ is even or odd according as $W(E,\tau)$ is 1 or -1. Therefore [1] leads to a statement which no longer makes any explicit reference to L-functions:

The Parity Conjecture. *Suppose that $\tau \cong \bar{\tau}$. Then*

$$W(E,\tau) = (-1)^{\langle\tau,E\rangle}.$$

In particular, if $W(E,\tau) = -1$ then the multiplicity of τ in $\mathbb{C}\otimes E(K)$ is odd and hence positive.

The connection with Problem 2 is that for certain self-dual representations τ it is easy to produce an E such that $W(E,\tau) = -1$. The simplest general statement along these lines is the following (cf. [10], p. 311, Prop. A):

Proposition 5 *Suppose that τ has real-valued character and either odd dimension or nontrivial determinant. Then there exists an elliptic curve E over $\mathbb{Q}$ such that $W(E,\tau) = -1$.*

For example, take K to be a Galois extension of $\mathbb{Q}$ with Galois group S_n, and suppose that τ is "standard": in other words, suppose that τ is the nontrivial constituent of the representation of $\mathrm{Gal}(K/\mathbb{Q})$ induced by the trivial representation of some subgroup $\mathrm{Gal}(K/L)$ of index n. Then $\dim\tau = n-1$. Hence for even n we conclude under the Parity Conjecture that τ occurs in some $\mathbb{C}\otimes E(K)$. In fact the same conclusion holds when n is odd, because for any n the determinant of a standard representation of S_n is the sign character.

These remarks apply in particular to the example considered earlier, where K was the splitting field of the polynomial $f(u) = u^n - u - 1$ and L the extension of $\mathbb{Q}$ generated by a root of $f(u) = 0$. When $n \equiv 0$ or 1 modulo 12 we were unable to prove that τ occurred in some $\mathbb{C} \otimes E(K)$. Under the Parity Conjecture this conclusion now follows from Proposition 5.

4 Specialization

The basic strategy for attacking Problem 1 has not changed since Hilbert: one first realizes G as a Galois group over a field of rational functions over $\mathbb{Q}$, and one then quotes the Hilbert irreducibility theorem to deduce that G is a Galois group over $\mathbb{Q}$. In principle there is an analogous approach to Problem 2 in which the role of the Hilbert irreducibility theorem is played by a different sort of specialization theorem, namely that of Néron [8], Silverman [17], and Tate [19]. Given K and τ as in Problem 2, one first finds an elliptic curve $\mathcal{C}$ over $\mathbb{Q}(t)$ with nonconstant j-invariant such that τ occurs in the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes \mathcal{E}(K(t))$, and one then quotes the theorem of Néron-Silverman-Tate to deduce that τ occurs in $\mathbb{C} \otimes \mathcal{E}_{t_0}(K)$ for all but finitely many specializations $\mathcal{E}_{t_0}$ of $\mathcal{E}$ over $\mathbb{Q}$. Here $\mathcal{E}_{t_0}$ denotes the fiber over $t_0 \in \mathbf{P}^1(\mathbb{Q})$ of a relatively minimal elliptic fibration $\mathcal{S} \to \mathbf{P}^1$ with generic fiber $\mathcal{E}$, and the finite set of excluded values of t_0 is understood to contain all $t_0 \in \mathbf{P}^1(\mathbb{Q})$ such that $\mathcal{E}_{t_0}$ is not an elliptic curve.

To see this approach implemented in practice we must turn to the work of Shioda [15], [16]. Shioda focuses on the case where the elliptic surface $\mathcal{S}$ is rational. In this case the Mordell-Weil rank of $\mathcal{E}(\bar{\mathbb{Q}}(t))$ is $\leqslant 8$ and can be computed from a knowledge of the reducible fibers of $\mathcal{S} \to \mathbf{P}^1$. For example, if there are no reducible fibers at all then the rank of $\mathcal{E}(\bar{\mathbb{Q}}(t))$ is exactly 8, and in fact $\mathcal{E}(\bar{\mathbb{Q}}(t))$ is a free $\mathbb{Z}$-module of this rank. The negative of the height pairing then makes $\mathcal{E}(\bar{\mathbb{Q}}(t))$ into a positive-definite, even, integral, unimodular lattice of rank 8, so that as a lattice $\mathcal{E}(\bar{\mathbb{Q}}(t))$ is isomorphic to the $\mathbf{E}_8$ root lattice. Quite generally, for any root system $\mathbf{X}$ let $W(\mathbf{X})$ denote the associated Weyl group.

Proposition 6 (Shioda) *Let K be a Galois extension of $\mathbb{Q}$ with $Gal(K/\mathbb{Q}) \cong W(\mathbf{E}_n)$, where $n = 6$, 7, or 8, and let τ be an n-dimensional irreducible complex representation of $Gal(K/\mathbb{Q})$. Then there exists an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of $Gal(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$.*

This is an immediate consequence of Theorem 7.2 of [15] and the following remark:

Every irreducible n-dimensional complex representation of $W(\mathbf{E}_n)$ is equivalent either to the standard representation of $W(\mathbf{E}_n)$ on the complex span of $\mathbf{E}_n$ or *to the twist of the standard representation by the unique quadratic character of $W(\mathbf{E}_n)$. Hence by the "invariance of Problem 2 under quadratic twists" (Proposition 2), the proof of Proposition 6 is reduced to the case where τ corresponds to the standard representation of $W(\mathbf{E}_n)$ under some identification of Gal$(K/\mathbb{Q})$ with $W(\mathbf{E}_n)$.*

The remark can be verified using the character tables for $U_4(2)$, $S_6(2)$, and $O_8^+(2)$ in [3]. Note that $W(\mathbf{E}_6)$ contains $U_4(2)$ as a subgroup of index 2, that $W(\mathbf{E}_7) \cong S_6(2) \times \{\pm 1\}$, and that $W(\mathbf{E}_8)/\{\pm 1\}$ contains $O_8^+(2) \times \{\pm 1\}$ as a subgroup of index 2.

Proposition 6 is nonvacuous in the strong sense that the groups $W(\mathbf{E}_n)$ do occur as Galois groups over $\mathbb{Q}$. This follows from Chevalley's theorem on finite reflection groups [2], but Shioda's construction gives an independent proof. Indeed the underlying construction pertains not to K but to the fraction field $\mathcal{K}$ of the symmetric algebra of the rational span of $\mathbf{E}_n$, and Shioda shows directly that the fixed field $\mathcal{K}^{W(\mathbf{E}_n)}$ is a rational function field over $\mathbb{Q}$.

The fact that Shioda's construction is "generic" rather than specific to $\mathbb{Q}$ gives it much broader scope than is indicated in Proposition 6. In particular, let $\mathbf{X}$ be one of the root systems $\mathbf{A}_n$ $(1 \leqslant n \leqslant 7)$ or $\mathbf{D}_n$ $(4 \leqslant n \leqslant 7)$, and view $W(\mathbf{X})$ as a subgroup of $W(\mathbf{E}_8)$ via an embedding of Dynkin diagrams. By combining Shioda's construction with Chevalley's theorem (applied to the field $\mathcal{K}^{W(\mathbf{X})}$, where $\mathcal{K}$ is attached to $\mathbf{E}_8$ as above) it should be possible to deduce a statement similar to Proposition 6 for $W(\mathbf{X})$. Alternatively, we can obtain a statement along these lines for a slightly different collection of root systems by using Proposition 1 (note that at least the cases of $\mathbf{A}_2$ and $\mathbf{D}_4$ were already examined by Shioda in [16]):

Proposition 7 *Let $\mathbf{X}$ be one of the following root systems:* $\mathbf{A}_n$ $(1 \leqslant n \leqslant 8)$, $\mathbf{B}_2$, $\mathbf{B}_3$, $\mathbf{B}_4$, $\mathbf{D}_4$, $\mathbf{G}_2$. *Let K be a Galois extension of $\mathbb{Q}$ with Gal$(K/\mathbb{Q}) \cong W(\mathbf{X})$, and let τ be an irreducible complex representation of Gal$(K/\mathbb{Q})$ of dimension equal to the rank of $\mathbf{X}$. Then there exists an elliptic curve E over $\mathbb{Q}$ such that τ occurs in the natural representation of Gal$(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$.*

A proof of Proposition 7 is briefly summarized in the following table.

$\mathbf{X}$	$G = W(\mathbf{X})$	H	$[G:H]$
$\mathbf{A}_n (1 \leq n \leq 8)$	S_{n+1}	S_n	$n+1$
$\mathbf{B}_n (2 \leq n \leq 4)$	$(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$	$(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes S_{n-1}$	$2n$
$\mathbf{D}_4$	$(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_4$	$(\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_3$	8
$\mathbf{G}_2$	D_6	$\mathbb{Z}/2\mathbb{Z}$	6

In the first column of the table we list each of the root systems $\mathbf{X}$ in the proposition, and in the second column we indicate the structure of the corresponding Weyl group $G = W(\mathbf{X})$. Let n denote the rank of $\mathbf{X}$. A case-by-case verification using the standard facts about irreducible representations of semidirect products with abelian kernel shows that if π is an n-dimensional irreducible representation of G then there is a subgroup H of G such that either π or a quadratic twist of π occurs in $\mathrm{ind}_H^G 1_H$. The structure of H is independent of π and is indicated in the third column of the table, but what really matters is the index $[G : H]$ displayed in the fourth column: in every case, $[G : H] \leqslant 9$, so that the data fall within the purview of Proposition 1. Although the isomorphism class of H can be specified independently of π, the reader is cautioned that the abstract isomorphism class of H need not determine a unique conjugacy class of embeddings of H in G. Indeed in the case $G = W(\mathbf{A}_5) \cong S_6$, $H \cong S_5$ we have already noted that there are two such conjugacy classes, corresponding to two inequivalent choices of π, and in the case $G = W(\mathbf{G}_2) \cong D_6$ (the dihedral group of order 12), $H \cong \mathbb{Z}/2\mathbb{Z}$ there are three such conjugacy classes, of which only the two noncentral classes give rise to the irreducible two-dimensional representation of D_6. Finally, we remark that the root systems $\mathbf{C}_3$ and $\mathbf{C}_4$ could also have been listed in Proposition 7 but would have added nothing new, because $W(\mathbf{C}_n) \cong W(\mathbf{B}_n)$.

5 Multiplicities

Formulated positively, Problem 2 asserts that for every finite Galois extension K of $\mathbb{Q}$ and every irreducible complex representation τ of $\mathrm{Gal}(K/\mathbb{Q})$ there is an elliptic curve E over $\mathbb{Q}$ such that $\langle \tau, E \rangle > 0$. Our final remark is that if this conjecture is correct then the set of all multiplicities is unbounded:

(*) $$\sup_{K,\tau,E} \langle \tau, E \rangle = \infty.$$

The reason is simple. First of all, since the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{C} \otimes E(K)$ is defined over $\mathbb{Q}$, the multiplicity $\langle \rho, E \rangle$ is divisible by the Schur index of τ. Now it was observed long ago by Brauer ([1], pp. 742 – 745) that for every integer $n \geqslant 1$ there is a finite group G_n and an irreducible representation π_n of G_n with Schur index n. Furthermore, Brauer's example is one for which Problem 1 has an affirmative answer: in other words, we can write $G_n \cong \mathrm{Gal}(K_n/\mathbb{Q})$ for some Galois extension K_n of $\mathbb{Q}$. Thus π_n becomes a representation τ_n of $\mathrm{Gal}(K_n/\mathbb{Q})$, and $\langle \tau_n, E \rangle \geqslant n$ whenever $\langle \tau_n, E \rangle > 0$. Hence if Problem 2 has an affirmative solution then (*) follows. Note however that (*) is much weaker than the conjecture that ranks of elliptic curves over $\mathbb{Q}$ can be arbitrarily large, because the latter conjecture amounts to saying that τ in (*) can be chosen to be the trivial representation.

Let us briefly indicate how to construct G_n, π_n, and K_n. We may assume that $n > 1$. Choose a prime $p \equiv 1$ modulo n such that $(p-1)/n$ and n are relatively prime, and fix an embedding of $\mathbb{Z}/n\mathbb{Z}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $\mathbb{Z}/n\mathbb{Z}$ acts on $\mathbb{Z}/p\mathbb{Z}$ via the natural action of $(\mathbb{Z}/p\mathbb{Z})^\times$, and $\mathbb{Z}/n^2\mathbb{Z}$ acts on $\mathbb{Z}/p\mathbb{Z}$ via the natural map $\mathbb{Z}/n^2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. It suffices to put

$$G_n = (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/n^2\mathbb{Z})$$

and to take for π_n any representation of G_n induced by a faithful character of the subgroup $(\mathbb{Z}/p\mathbb{Z}) \times (n\mathbb{Z}/n^2\mathbb{Z})$. As for K_n, one can appeal to general theorems on the realizability of solvable groups as Galois groups (cf. Shafarevich [14]) or perhaps more appropriately to weaker statements which suffice for the application at hand (cf. Serre [13] pp. 17 - 18). However it is also easy to give a direct construction. Let L be a totally real cyclic extension of $\mathbb{Q}$ of degree n^2, and let F be the subfield of L with $[F:\mathbb{Q}] = n$; fix an identification of $\mathrm{Gal}(L/\mathbb{Q})$ with $\mathbb{Z}/n^2\mathbb{Z}$ and hence of $\mathrm{Gal}(F/\mathbb{Q})$ with $\mathbb{Z}/n\mathbb{Z}$. By composing the latter identification with our fixed embedding of $\mathbb{Z}/n\mathbb{Z}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, we obtain a character $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{F}_p^\times$. We note that any representation of $\mathrm{Gal}(F/\mathbb{Q})$ over $\mathbb{F}_p$ is semisimple, because $p \nmid n$.

Proposition 8 *Let q and r be distinct primes congruent to 1 modulo p which split completely in F, and write C for the wide ray class group of F modulo $qr\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of F. View C/C^p as a representation space for $\mathrm{Gal}(F/\mathbb{Q})$ over $\mathbb{F}_p$. Then χ occurs in C/C^p.*

Granting the proposition, let D be a subgroup of index p in C, stable under $\mathrm{Gal}(F/\mathbb{Q})$, such that $\mathrm{Gal}(F/\mathbb{Q})$ acts on C/D via χ. Let M be the class field over F corresponding to D. Then $\mathrm{Gal}(LM/\mathbb{Q}) \cong G_n$, so we may take $K_n = LM$. It remains to prove the proposition. Put $U = \mathcal{O}^\times$, $A = (\mathcal{O}/qr\mathcal{O})^\times$, and $B = A/\iota(U)$, where $\iota : U \to A$ is the natural map.

Lemma *Every irreducible representation of $\mathrm{Gal}(F/\mathbb{Q})$ over $\mathbb{F}_p$ occurs in B/B^p.*

Proof. . Consider the exact sequence

$$U/U^p \longrightarrow A/A^p \longrightarrow B/B^p \longrightarrow \{1\}.$$

The Dirichlet unit theorem shows that as a representation for $\mathrm{Gal}(F/\mathbb{Q})$ over $\mathbb{F}_p$, the space U/U^p is isomorphic to the augmentation representation (the subrepresentation of the regular representation afforded by the augmentation ideal). On the other hand, our choice of q and r ensures that A/A^p is the direct sum of two copies of the regular representation of $\mathrm{Gal}(F/\mathbb{Q})$. Therefore at least one copy of the regular representation survives in B/B^p.

For any abelian group X and any positive integer m let $X[m]$ denote the subgroup of X annihilated by m. According to the lemma, χ occurs in B/B^p, so by the Jordan-Hölder theorem there is an integer $j \geqslant 0$ such that χ occurs in $B[p^{j+1}]/B[p^j]$. On the other hand, B is naturally a subgroup of C, whence $B[p^{j+1}]/B[p^j]$ is naturally a subspace of $C[p^{j+1}]/C[p^j]$. Therefore χ occurs in the latter space, and a second appeal to the Jordan-Hölder theorem shows that χ occurs in some $C^{p^k}/C^{p^{k+1}}$ $(k \geqslant 0)$. Finally, since $C^{p^k}/C^{p^{k+1}}$ is naturally a quotient of C/C^p we conclude that χ occurs in C/C^p, proving Proposition 8.

Referencias

[1] **R. Brauer**, *Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen II*, Math. Z. Vol. 31, 733 – 747, 1930.

[2] **C. Chevalley**, *Invariants of finite groups generated by reflexions*, Amer. J. of Math. Vol. 77, 778 – 782, 1955.

[3] **J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson**, *Atlas of Finite Groups*, Clarendon Press, 1985.

[4] **P. Deligne**, *Les constantes des équations fonctionelles des fonctions L*, Modular Functions of One Variable, II, Lect. Notes in Math. Vol. 349, Springer-Verlag 501–595, 1973.

[5] **P. Deligne**, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math., Vol. 33 – Part 2, Amer. Math. Soc., Providence 313 – 346, 1979.

[6] **W. Feit**, *Some consequences of the classification of finite simple groups*, The Santa Cruz Conference on Finite Groups, Proc. Symp. Pure Math. Vol. 37, 175 – 181, AMS, Providence, 1980.

[7] **W. Fulton and J. Harris**, *Representation Theory: A First Course*, GTM Readings in Math. Vol. 129, Springer-Verlag, 1991.

[8] **A. Néron**, *Propriétés arithmétiques de certaines familles de courbes algébriques*, Proc. Int. Cong. Math., Vol. III, 481 - 488, 1954.

[9] **D. E. Rohrlich**, *The vanishing of certain Rankin-Selberg convolutions*, Automorphic Forms and Analytic Number Theory, Les publications CRM, Montreal, 123 – 133, 1990.

[10] **D. E. Rohrlich**. *Galois theory, elliptic curves, and root numbers*, Compositio Math., Vol. 100, 311 – 349, 1996.

[11] **D. E. Rohrlich**, *Realization of some Galois representations of low degree in Mordell-Weil groups*, Math. Research Letters, Vol. 4, 123-130, 1997.

[12] **E. S. Selmer**, *On the irreducibility of certain trinomials*, Math. Scand., Vol. 4, 287 – 302, 1956.

[13] **J-P. Serre**, *Topics in Galois Theory (Notes by Henri Darmon)*, Research Notes in Math., Vol. 1, Jones and Bartlett, Boston, London, 1992.

[14] **I. R. Shafarevich**, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Vol. 18, 525 – 578, 1954.

[15] **T. Shioda**, *Theory of Mordell-Weil lattices*, Proc. Int. Cong. Math., Vol. I, Springer-Verlag, 473 – 489, 1991.

[16] **T. Shioda**, *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan, Vol. 43, 673 – 719, 1991.

[17] **J. H. Silverman**, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math., Vol. 342, 197 – 211, 1983.

[18] **J. Tate**, *Number theoretic background*, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math., Vol. 33 – Part 2, Amer. Math. Soc., 3 – 26, Providence, 1979.

[19] **J. Tate**, *Variation of the canonical height of a point depending on a parameter map for families of abelian varieties*, Amer. J. Math., Vol. 105, 287 – 294, 1983.