Matemática Contemporânea, Vol. 6, 13–18
http://doi.org/10.21711/231766361994/rmc63

SERRE'S CONJECTURE: THE JUGENTRAUM OF THE 20TH CENTURY

Robert F. Coleman

1. The Galois group of Q.

Let $\bar{\mathbf{Q}}$ be an algebraic closure of the rational numbers $\mathbf{Q}$ and $\mathcal{G}$ denote $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$. This may be considered the central object of study in modern arithmetic but there are many things one doesn't know about it. For example, it is not known if every finite group is a quotient of this group. However, it is a consequence of the first version of the theorem of Kronecker and Weber stated below that this is true about Abelian finite groups. A source of motivation is the analogy between the Galois group $\mathcal{G}_S$ of the maximal extension of $\mathbf{Q}$ in $\bar{\mathbf{Q}}$ unramified outside a finite set of primes S and the fundamental group of the affine line minus a finite set of points. Since this fundamental group is finitely generated one is tempted to ask (as did Shafarevich):

Question. *Is the group $\mathcal{G}_S$ topologically finitely generated?*

This would mean that there is a finite subset T of $\mathcal{G}_S$ such that every finite quotient of $\mathcal{G}_S$ is generated by the image of T. At present, this is only known when S is empty for then $\mathcal{G}_S$ is trivial. It is an immediate consequence of the second version of the theorem of Kronecker and Weber stated below that this is true about finite Abelian quotients.

Question. *(Harbater) When $S = \{2\}$ (and does not contain ∞) is $\mathcal{G}_S$ Abelian?*

This would imply $\mathcal{G}_{\{2\}}$ is topologically cyclic.

2. Kronecker's Jugentraum.

Kronecker began and Weber finished the proof of:

Theorem 1. *Suppose K is a finite extension of $\mathbf{Q}$. Then $Gal(K/\mathbf{Q})$ is Abelian if and only if there exists an integer N such that $K \subseteq \mathbf{Q}(\exp(\frac{2\pi i}{N}))$.*

In particular, this implies that every Abelian extension of $\mathbf{Q}$ lies inside an extension obtained by adjoining some root of unity. Kronecker went on to conjecture that every Abelian extension of an imaginary quadratic field could be found inside a extension obtained by adjoining the coordinates of points of finite order on an elliptic curve with complex multiplication in that field. This was Kronecker's jugentraum. In fact, Kronecker described the precise N needed in both the theorem and the conjecture. We will do this for the theorem below.

3. Conductors.

Let F be a finite field. Suppose ρ is homomorphism of $\mathcal{G}$ into $GL_n(F)$. Let H denote the image of $\mathcal{G}$. Then H is finite. We define the conductor (see Serre's Corps Locaux) of ρ as follows:

First we can think of ρ as giving an action of $\mathcal{G}$ on the n-dimensional vector space $V = F^n$ by

$$\sigma v = \rho(\sigma)v,$$

for $\sigma \in \mathcal{G}$, $v \in V$.

Now for each prime p of $\mathbf{Q}$ and any prime $\wp$ of $\bar{\mathbf{Q}}$ above there is a natural sequence of subgroups

$$H_{-1} \supseteq H_0 \supseteq H_1 \supseteq \ldots \supseteq H_i \supseteq \ldots$$

of H called the ramification groups at $\wp$. The group H_{-1} is the decomposition group and corresponds to the subgroup of a fundamental group generated by the cycle around a point.

Let V_i denote the subspace of V fixed by H_i. Set

$$n(\rho,p) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} dim_F V/V_i.$$

Then $n(\rho,p)$ is an integer, is zero if the fixed field of the kernel of ρ is unramified above p and we set

$$N(\rho) = \prod_p p^{n(\rho,p)}$$

4. Characters.

Let χ_N denote the homomorphism from $\mathcal{G}$ into $(\mathbf{Z}/N\mathbf{Z})^*$ determined by

$$\exp(\frac{2\pi i}{N})^\sigma = \exp(\chi(\sigma)\frac{2\pi i}{N}).$$

Note that,

$$\chi_N(Frob_p) = p \bmod N$$

for p a prime not dividing N.

Now suppose $n = 1$, i.e. ρ is a character. Then, a refined version of the theorem Kronecker and Weber stated above is:

Theorem 2. *There exists a unique homomorphism ϕ: $(\mathbf{Z}/N(\rho)\mathbf{Z})^* \to GL_1(F)$ such that*

$$\rho = \phi \circ \chi_{N(\rho)}.$$

Moreover, if $\rho = \psi \circ \chi_M$ for some ψ and M, then $N(\rho)|M$.

Since, $|(\mathbf{Z}/p^m\mathbf{Z})^*| = p^{m-1}(p-1)$ and if F has characterstic p, the order of F^* is prime to p one has

Corollary 3. *The number of characters whose conductor is a power of p with values in $GL_1(\bar{\mathbf{F}}_p)$ is finite.*

To stress the analogy with what follows we remark that if one sets $a_l = \phi(l)$ for l not dividing $N(\rho)$ it follows from the Tchebotarev density theorem that ρ is characterized by the identities:

$$\rho(Frob_l) = a_l.$$

5. Modular forms.

(See Ribet, Report on Modular $\bmod l$ representations of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$,to appear in the Proceedings of Symposia on Pure Math.)

"Let $N \geq 1$ and $k \geq 2$ be integers. Let $\Gamma_1(N)$ be the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0, a \equiv d \equiv 1 \bmod N \right\}$$

and let $S = S_k(\Gamma_1(N))$ be the complex vector space of cusp forms on $\Gamma_1(N)$. There is a standard action of $(\mathbf{Z}/N\mathbf{Z})^*$ on S $d \mapsto \langle d \rangle$. There is also a family of Hecke operators T_n, $(n \geq 1)$ which act on S."

If $f \in S_k(\Gamma_1(N))$, N is called the level of f and k is called the weight. It is called an eigenform if it is an eigenvalue for all the Hecke and diamond operators.

If f is an eigenform and

$$f(q) = \sum_{n \geq 0} a_n q^n$$

is the q-expansion of f with $a_1 = 1$ then

$$f|T_n = a_n f.$$

There also exists a character ϵ on $(\mathbf{Z}/N\mathbf{Z})^*$ such that

$$f|\langle d \rangle = \epsilon(d) f.$$

The coefficients a_n lie in a finite extension of $\mathbf{Q}$ and $\epsilon(-1) = (-1)^k$.

Examples. *First,*

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_n \tau(n) q^n$$

is the q-expansion of an eigenform of level 1 *and weight* 12. *Next,*

$$q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2$$

is the q expansion of an eigenform of level 11 *and weight* 2.

Let f be an eigenform in S and E be the field generated by its coefficients. For each prime λ of E let F_λ be the residue field at λ. Using results of Deligne there exists a representation

$$\rho_\lambda =: \rho_{f,\lambda}: \mathcal{G} \to GL_2(F_\lambda).$$

It has the properties: It is unramified at primes not dividing Nl,

$$Trace(\rho_\lambda(Frob_p)) \equiv a_p$$
$$Det(\rho_\lambda(Frob_p)) \equiv \epsilon(p) p^{k-1} \bmod \lambda$$

for primes p such that $(p, Nl) = 1$ where $l = char(F_\lambda)$. The last congruence can be restated,

$$Det(\rho_\lambda) = \epsilon\chi_l^{k-1}$$

Also one can show $Det(\rho_\lambda(c)) = -1$ where c is complex conjugation, i.e. the representation is odd.

When $k = 2$ these representations may be found in the l-torsion of the Jacobian of the modular curve $X_1(N)$. In fact, let H be the ring generated by the Hecke operators and the diamond operators. It acts on this Jacobian. Let I be the kernel of the homomorphism

$$T_n \mapsto a_n \quad \text{and} \quad \langle d \rangle \mapsto \epsilon(d)$$

from H to F_λ. Then, when $l > 2$ the representation ρ_λ can be identified with the representation on the kernel of I in the torsion on the Jacobian.

Then one has:

Weak Serre Conjecture. *Let*

$$\rho: \mathcal{G} \to GL_2(F)$$

be an irreducible, odd representation where F is a finite field. Then ρ is isomorphic to $\rho_{f,\lambda}$ for some f and λ as above.

In fact, in addition to the conclusion of the above conjecture Serre also conjectured,

Stronger Serre Conjecture. *The form f must be of level $N(\rho)l^{-n(\rho,l)}$ of character ϵ and weight k where $k \leq l^2$ and*

$$det(\rho) = \epsilon\chi_l^{k-1}.$$

This, of course, does not completely determine k. The complete conjecture may be found in Serre's article, Sur les représentations modulaires de degré 2 de $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$, Duke Math Jour. Vol. 54, 1987. Since there are only finitely many eigenforms on $X_1(N)$ of a given weight, this implies,

Corollary of conjecture. *There exist only a finite number of irreducible odd representations of conductor a power of p with values in $GL_2(\bar{\mathbf{F}}_p)$, up to conjugation.*

Further Questions and Remarks: It is known that $\rho_{f,\lambda}$ is reducible if and only if f is congruent to an Eisenstein series modulo λ. One only has a necessary condition for a prime p of $\mathbf{Q}$ to split completely in the fixed field of the kernel of $\rho_{f,\lambda}$; a_p must equal 2 and $\epsilon(p)$ must equal p^{1-k}. But this is not sufficient. Can one find a simple criterion in terms of f? Similarly, because $Det(\rho_\lambda(c) = -1$ it follows that this field is not totally real when λ does not lie over 2 but is there a simple criterion when it does? Finally, it follows from class field theory that the conclusion of the last corollary is true with the hypotheses irreducible and odd replaced by reducible. Is it true without any hypotheses on the representation?

Department of Mathematics
University of California
Berkeley, California 94720
U.S.A.