Galois representations with open image

Ralph Greenberg

University of Washington
Seattle, Washington, USA

May 7th, 2011

Introduction

This talk will be about representations of the absolute Galois group of $\mathbf{Q}$:

$$G_{\mathbf{Q}} \;=\; \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \quad .$$

We will consider continuous representations

$$\rho : \; G_{\mathbf{Q}} \;\longrightarrow\; GL_n(\mathbf{Z}_p)$$

where $n \geq 3$ and $\mathbf{Z}_p$ denotes the ring of p-adic integers. We will be interested in constructing such representations so that the index

$$[GL_n(\mathbf{Z}_p) : Im(\rho)]$$

is finite. Equivalently, this means that $Im(\rho)$ is an open subgroup of $GL_n(\mathbf{Z}_p)$.

The case $n = 1$

For $n = 1$, for any prime p, and for any $t \geq 0$, the group of p^t-th roots of unity in $\overline{\mathbf{Q}}^\times$ is isomorphic to $\mathbf{Z}/p^t\mathbf{Z}$. We denote this group by μ_{p^t}. The group $G_{\mathbf{Q}}$ acts on μ_{p^t}. One can consider the inverse limit of the μ_{p^t}'s as $t \to \infty$. This is isomorphic to $\mathbf{Z}_p$ and has a continuous action of $G_{\mathbf{Q}}$. This gives a continuous representation

$$\chi_p : \; G_{\mathbf{Q}} \longrightarrow GL_1(\mathbf{Z}_p) \quad .$$

The map χ_p is surjective.

The case $n = 2$

For $n = 2$, One obtains examples from the theory of elliptic curves. Suppose that E is an elliptic curve defined over $\mathbf{Q}$. Suppose that p is any prime. For any $t \geq 0$, the p^t-torsion in the abelian group $E(\overline{\mathbf{Q}})$ is isomorphic to $\mathbf{Z}/p^t\mathbf{Z} \times \mathbf{Z}/p^t\mathbf{Z}$. It is denoted by $E[p^t]$.

The Galois group $G_{\mathbf{Q}}$ acts on $E[p^t]$. The p-adic Tate module for E is defined to be the inverse limit of the groups $E[p^t]$ as $t \to \infty$. It is a free $\mathbf{Z}_p$-module of rank 2. Thus, we get a continuous representation

$$\rho_{E,p} : \; G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{Z}_p) \quad .$$

Serre's Theorem

There is a famous theorem of Serre which states that if $End_{\mathbf{C}}(E) \cong \mathbf{Z}$, then $Im(\rho_{E,p})$ has finite index in $GL_2(\mathbf{Z}_p)$.

Furthermore, under the same assumption, $\rho_{E,p}$ is surjective for all but finitely many primes p (depending on E).

The assumption that $End_{\mathbf{C}}(E) \cong \mathbf{Z}$ means that E does not have complex multiplications. The entire first page of Cremona's table of elliptic curves are such non-CM elliptic curves.

Some known results when $n = 3$

Representations $\rho : G_{\mathbf{Q}} \to GL_3(\mathbf{Z}_p)$ with open image have been constructed by Spencer Hamblen when $p \equiv 8 \pmod{21}$. The approach uses deformation theory.

Surjective representations $\rho : G_F \to GL_3(\mathbf{Z}_p)$, where $F = \mathbf{Q}(\sqrt{-3})$, and for all but finitely many primes $p \equiv 1 \pmod{3}$, have been constructed by Margaret Upton. The construction is based on the action of G_F on the p-adic Tate module of certain abelian varieties whose endomorphism ring contains the integers of F.

More results for $n \geq 3$.

I have managed to construct such representations ρ in the following cases:

1. p is an odd, regular prime and $\left[\frac{n}{2}\right] \leq \frac{p-1}{4}$

In particular, the construction works if $n = 3$ and p is a regular prime ≥ 5.

Definition: Recall that p is a regular prime if p doesn't divide the class number of $\mathbf{Q}(\mu_p)$. Here μ_p denotes the p-th roots of unity.

All primes $p < 100$ are regular, except for $p = 37,\ 59$, and 67.

More results.

2. $n = 3$, $p \equiv 1 \pmod 4$ and $p < 10,000$
(and even $p < 3 \times 10^9$ if $p \equiv 1$ or $4 \pmod 5$).

3. $p = 3$, $4 \leq n \leq 29$; $p = 5$, $4 \leq n \leq 13$.

In principle, the construction should work for every pair (p, n) where p is odd and $n \geq 3$, except for $(p, n) = (3, 3)$. It depends on finding an abelian extension K of $\mathbf{Q}$ with certain properties.

Our approach

The approach that we will describe here is an algebraic number theory approach and involves the structure of the Galois groups of certain infinite extensions. The approach also involves some observations about the structure of a Sylow pro-p subgroup of $SL_n(\mathbf{Z}_p)$.

A Sylow p-subgroup of $SL_n(\mathbf{F}_p)$ is the subgroup U_n of upper triangular, unipotent matrices. A Sylow pro-p subgroup of $SL_n(\mathbf{Z}_p)$ is the subgroup of matrices whose image under reduction modulo p is in U_n. We denote this subgroup by P_n.

Let D_n denote the subgroup of the diagonal matrices in $GL_n(\mathbf{Z}_p)$ whose entries are $(p-1)$-st root of unity (in $\mathbf{Z}_p^\times$.) Thus, D_n is a finite subgroup of $GL_n(\mathbf{Z}_p)$ of order $(p-1)^n$.

The group D_n acts (as a group of automorphisms) on P_n by conjugation.

More about the structure of P_n

The Sylow pro-p subgroup P_n of $SL_n(\mathbf{Z}_p)$ can be topologically generated by the following set of n elements:

$$T_n \;=\; \{\; I_n + E_{12},\; \ldots,\; I_n + E_{(n-1)n} \;\} \bigcup \{\; I_n + pE_{n1} \;\} \;\;.$$

In contrast, the congruence subgroup $I_n + pM_n(\mathbf{Z}_p)$ requires n^2 topological generators. Its intersection with $SL_n(\mathbf{Z}_p)$ requires $n^2 - 1$ generators.

Why does T_n generate P_n?

A key lemma in proving that P_n is generated topologically by T_n is the following. We let $M_n(\mathbf{F}_p)^{(0)}$ denote the matrices of trace 0.

Lemma: *Let U_n act on $M_n(\mathbf{F}_p)^{(0)}$ by conjugation. Then $M_n(\mathbf{F}_p)^{(0)}$ is a cyclic $\mathbf{F}_p[U_n]$-module generated by E_{n1}.*

One applies this lemma to the successive quotients

$$\big(I_n + p^t M_n(\mathbf{Z}_p)\big)\big/\big(I_n + p^{t+1} M_n(\mathbf{Z}_p)\big)$$

for $t \geq 1$, all of which can be identified with $M_n(\mathbf{F}_p)$ by the maps

$$I_n + p^t A \longrightarrow A \pmod{pM_n(\mathbf{Z}_p)} \ .$$

The action of D_n on the elements of T_n

The above topological generating set T_n for P_n has an additional property. Each element generates a subgroup (topologically) which is fixed by the action of D_n.

If one conjugates by an element d of D_n, with entries $d_1, \ldots, d_n$ along the diagonal, then

$$d\big(I_n + E_{ij}\big)d^{-1} \;=\; \big(I_n + E_{ij}\big)^{d_i d_j^{-1}} \quad .$$

In particular, since $(I_n + pE_{n1}) = (I_n + E_{n1})^p$, one has

$$d\big(I_n + pE_{n1}\big)d^{-1} \;=\; \big(I_n + pE_{n1}\big)^{d_n d_1^{-1}} \quad .$$

These facts about P_n and the action of D_n on that group is a

A refinement of the Burnside Basis Theorem

Suppose that Π is a pro-p group and that Δ is a finite abelian group such that every element of Δ has order dividing $p-1$. Suppose that Δ acts on Π. Let $\widetilde{\Pi}$ denote the Frattini quotient of Π, the maximal abelian quotient of Π which has exponent p. Then $\widetilde{\Pi}$ is an $\mathbf{F}_p$-vector space with a linear action of Δ. Assume it is finite dimensional.

Lemma: *If $v \in \widetilde{\Pi}$ and Δ acts on v by a character $\chi : \Delta \to \mathbf{F}_p^\times$, then there exists an element $\pi \in \Pi$ which is mapped to v by the map $\Pi \to \widetilde{\Pi}$ and such that*

$$\delta(\pi) \;=\; \pi^{\chi(\delta)} \quad .$$

p-rational number fields

Shafarevich proved the following theorem in the 1960s.

Theorem *Let $K = \mathbf{Q}(\mu_p)$. Assume that p is an odd, regular prime. Let M be the compositum of all finite p-extensions of K which are unramified except at the prime above p. Let $\Pi = Gal(M/K)$. Then Π is a free pro-p group on $\frac{p+1}{2}$ generators.*

The field M is very big in general. It contains $K(\mu_{p^t})$ for all $t \geq 1$. It contains the field generated by the p^t-th roots of all units in that field. It contains the field generated by all the p^t-th roots of all units in all of those new fields. Etc.

In general, a number field K is said to be p-rational if $\Pi = Gal(M/K)$ is a free pro-p group.

The basic idea of the construction

Consider $K = \mathbf{Q}(\mu_p)$ and assume that $p \geq 3$ and is a regular prime. Let $\Delta = Gal(K/\mathbf{Q})$.

1. If $\frac{p+1}{2} \geq n$, then one can construct a surjective homomorphism $\sigma_0 : \Pi \to P_n$.

2. If σ_0 is chosen carefully, then one can extend σ_0 to a homomorphism

$$\sigma : Gal(M/\mathbf{Q}) \to D_n P_n \quad .$$

3. Define $\rho = \sigma \otimes \chi_p$.

Then the image of ρ is an open subgroup of $GL_n(\mathbf{Z}_p)$.

The structure of $Gal(M/\mathbf{Q})$

Let $K = \mathbf{Q}(\mu_p)$.

Recall the notation $\Delta = Gal(K/\mathbf{Q})$ and $\Pi = \mathrm{Gal}(M/K)$. Let $G = Gal(M/\mathbf{Q})$.

We have an exact sequence

$$1 \longrightarrow \Pi \longrightarrow G \longrightarrow \Delta \longrightarrow 1$$

This sequence turns out to split and so we can identify Δ with a subgroup of G. Then G is a semidirect product and Δ acts on Π by conjugation.

The structure of $Gal(M/\mathbf{Q})$

If p is regular, then the Frattini quotient $\widetilde{\Pi}$ can be identified with $Gal(L/K)$, where $L = K(\ \{p - th\ roots\ of\ units\ in\ K\}\ )$.

The action of Δ on $\widetilde{\Pi}$ is determined by the action of Δ on the units of K. The characters of Δ which occur in its action on $\widetilde{\Pi}$ are

$$\widehat{\Delta}^{odd} \cup \{\chi_0\} \quad ,$$

all with multiplicity 1.

Thus, one can choose a topological generating set for Π so that Δ acts on the generators by the above characters.

The construction of σ

Δ acts on Π. Under the assumption that p is a regular prime, the Δ-type for this action is $\widehat{\Delta}^{odd} \cup \{\chi_0\}$.

If we choose a homomorphism $\varepsilon : \Delta \to D_n$, then we have an action of Δ on P_n. The Δ-type of P_n is a set of n elements of $\widehat{\Delta}$, depending on ε. If one can arrange to have

$$\Delta - \mathit{type\ of}\ P_n \quad \leq \quad \Delta - \mathit{type\ of}\ \Pi \ ,$$

then we can define a surjective, Δ-equivariant homomorphism $\sigma_0 : \Pi \to P_n$.

We can then extend σ_0 to the semidirect product $G = \Delta\Pi$:

$$\sigma : G \longrightarrow D_n P_n \quad .$$

The choice of ε

If $\left[\frac{n}{2}\right] \leq \frac{p-1}{4}$, then one can choose

$$\chi_1, ..., \chi_n \ \in \ \widehat{\Delta}^{odd} \cup \{\chi_o\}$$

so that they are distinct and $\chi_1 ... \chi_n = \chi_0$.

One can then define $\varepsilon : \Delta \to D_n$ by using characters $\varepsilon_1, ..., \varepsilon_n$ chosen so that

$$\varepsilon_1/\varepsilon_2 = \chi_1, \ldots, \ \varepsilon_n/\varepsilon_1 = \chi_n \quad .$$

The other cases

2. $n = 3$, $p \equiv 1 \pmod 4$ and $p < 10,000$
(and even $p < 3 \times 10^9$ if $p \equiv 1$ or $4 \pmod 5$).

One applies the idea to $K = \mathbf{Q}(\mu_5)$. For $p \neq 5$, it turns out that $\Pi = Gal(M/K)$ is a free pro-p group (on 3 generators) if and only if $\frac{1+\sqrt{5}}{2}$ is not a p-th power in the completion of K at the prime(s) above p. This is true for all the primes that we've check (myself and Rob Pollack).

3. $p = 3,\ \ 4 \leq n \leq 29;$

One applies the idea to

$$K \;=\; \mathbf{Q}(\sqrt{-1}, \sqrt{13}, \sqrt{145}, \sqrt{209}, \sqrt{269}, \sqrt{373})$$

which turns out to be p-rational for $p = 3$.

This example was found by Robert Bradshaw.

Thank you!