Introduction

For $p \leq 37$, we classify all the mod p, finite dimensional representations of $G_{\mathbf{Q}}$ that are unramified outside p and tamely ramified at p, with tame inertia acting through level one characters. We show that any such representation is abelian and unramified when restricted to the p-th cyclotomic field $\mathbf{Q}(\mu_p)$. A preliminary step involves using Odlykzo's bounds to prove that the maximal unramified extension of $\mathbf{Q}(\mu_p)$ is its Hilbert Class Field. The results for $p = 29$, 31 and 37 are conditional to the *GRH*.

1. The maximal unramified extension of $\mathbf{Q}(\mu_p)$, for $p \leq 37$

Let $p \leq 37$ be an odd prime. We use Odlyzko bounds to determine the maximal extension of $\mathbf{Q}(\mu_p)$ which is *unramified at every finite prime*. The statements we give for $p \geq 29$ are conditional to the Generalized Riemann Hypothesis (*GRH*). We begin with a lemma.

Lemma 1. *Let p be an odd prime and K a finite unramified extension of $\mathbf{Q}(\mu_p)$ which is a Galois extension of $\mathbf{Q}$. Then*
i) $G(K/\mathbf{Q}(\mu_p))$ is the first derived subgroup of $G(K/\mathbf{Q})$;
ii) $G(K/\mathbf{Q}) \simeq G(K/\mathbf{Q}(\mu_p)) \times_{\varphi} (\mathbf{Z}/p\mathbf{Z})^*$.

Proof. Denote the Galois group $G(K/\mathbf{Q})$ by G and its first derived subgroup by G'. Clearly $\mathbf{Q}(\mu_p) \subset K^{G'}$ and $K^{G'}/\mathbf{Q}(\mu_p)$ is an unramified extension. By the Knonecker Weber theorem, $K^{G'} \subset \mathbf{Q}(\mu_{p^r})$, for a suitably large integer r. It follows that the field extension $K^{G'}/\mathbf{Q}$ is totally ramified at p and $K^{G'}$ must equal $\mathbf{Q}(\mu_p)$, the first part of the proposition follows.
To prove the second part we show that the following exact sequence splits:

$$1 \longrightarrow G' \longrightarrow G \longrightarrow (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow 1.$$

In fact, for any prime P of K above the rational prime p, the corresponding inertia subgroup I_P is a complement of G' in G: the intersection $I_P \cap G'$ is trivial since $K/K^{G'}$ is unramified and, on the other hand, I_P surjects onto $G(\mathbf{Q}(\mu_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^*$ under the restiction of the natural map $G \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*$, since $\mathbf{Q}(\mu_p)/\mathbf{Q}$ is totally ramified at p. □

Remark 1. The first part of the lemma can be alternatively proved using the fact that $\mathbf{Q}$ has no unramified extensions, without using the Kronecker Weber theorem, for more details cfr. [**?**].

Let F be a number field of degree n over $\mathbf{Q}$ and d_F the discriminant of $F/\mathbf{Q}$. For small values of the discriminant root $|d_F|^{1/n}$ (≤ 22 unconditionally and ≤ 41 under GRH) the Odlyzko bounds provide upper estimates on the degree n of the number field F. We shall investigate what they mean when F is a finite *unramified* extension of $\mathbf{Q}(\mu_p)$, for $p \leq 37$.

Let p be an odd prime and K a finite *unramified* extension of $\mathbf{Q}(\mu_p)$ of degree n over $\mathbf{Q}$. The discriminant roots of K and $\mathbf{Q}(\mu_p)$ coincide (cf [**?**],§4, prop. 4.8) and since $|d_{\mathbf{Q}(\mu_p)}| = p^{p-2}$ (cf [**?**],§2, th. 2.8) we have

$$|d_K|^{1/n} = p^{(p-2)/(p-1)}.$$

In the table below we list the estimates we get for $n = [K : \mathbf{Q}]$ for odd prime numbers less or equal than 37.
When K is Galois over $\mathbf{Q}$ with Galois group G, in the last column of the table we list the upper bound on the order of G', equal to $n/(p-1)$ by the lemma. For $p \geq 29$ we use conditional bounds and in the table they appear next to an asterisk.

p	$n \leq$	$\lvert G'\rvert \leq$
3	2	1
5	4	1
7	6	1
11	15	1
13	23	1
17	55	3
19	91	5
23	479	21
29	399(*)	14(*)
31	719(*)	23(*)
37	8861(*)	246(*)

We immediately prove the following:

Theorem 2. *Let* $p \leq 19$ *be an odd prime number. Then there are no non-trivial unramified extension of* $\mathbf{Q}(\mu_p)$.

Proof. Let K be the maximal *unramified* extension of $\mathbf{Q}(\mu_p)$. By its maximality property $K/\mathbf{Q}$ is Galois and we denote its Galois group by G.
Let now L be a finite extension of $\mathbf{Q}(\mu_p)$ inside K which is Galois over

$\mathbf{Q}$. For any prime p in the range, the table tells us that $[L : \mathbf{Q}(\mu_p)] \leq 5$. This implies that $K/\mathbf{Q}(\mu_p)$ is finite and $|G(K/\mathbf{Q}(\mu_p))| \leq 5$. The extension $K/\mathbf{Q}(\mu_p)$ is then abelian and K equals the Hilbert Class Field of $\mathbf{Q}(\mu_p)$. Now, if $p \leq 19$ than the class number $h(\mathbf{Q}(\mu_p))$ of $\mathbf{Q}(\mu_p)$ is 1 (cf. [**?**], §.11) and then $K = \mathbf{Q}(\mu_p)$. □

For $23 \leq p \leq 37$ the Class Group Cl_p of $\mathbf{Q}(\mu_p)$ is no longer trivial, its structure is (cf. [**?**], Appendix §.3):
$Cl_{23} \simeq \mathbf{Z}/3\mathbf{Z}$
$Cl_{29} \simeq (\mathbf{Z}/2\mathbf{Z})^3$
$Cl_{31} \simeq \mathbf{Z}/9\mathbf{Z}$
$Cl_{37} \simeq \mathbf{Z}/37\mathbf{Z}$.
The previous theorem obviously does not extend but what it is true is that the maximal unramified extension is abelian (for $p \geq 29$ we assume the GRH).
Denote the Hilbert Class Field of $\mathbf{Q}(\mu_p)$ by H_p, then by lemma 1

$$G(H_p/\mathbf{Q}) \simeq \mathrm{Cl}_p \times_\varphi (\mathbf{Z}/p\mathbf{Z})^*,$$

for a certain semidirect product structure given by φ. One can check that φ is described by the natural action of $(\mathbf{Z}/p\mathbf{Z})^*$ on Cl_p. For $23 \leq p \leq 37$ the semidirect product structure is (cf. Appendix A):

$$G(H_{23}/\mathbf{Q}) \simeq [Cl_{23} \times_\alpha \mathbf{Z}/2\mathbf{Z}] \times \mathbf{Z}/11\mathbf{Z},$$

where $\mathbf{Z}/2\mathbf{Z}$ acts non trivially on $Cl_{23} \simeq \mathbf{Z}/3\mathbf{Z}$ switching the two generators;

$$G(H_{29}/\mathbf{Q}) \simeq [Cl_{29} \times_\beta \mathbf{Z}/7\mathbf{Z}] \times \mathbf{Z}/4\mathbf{Z}$$

where $\mathbf{Z}/7\mathbf{Z}$ acts on $Cl_{29} \simeq (\mathbf{Z}/2\mathbf{Z})^3$ as the multiplicative group $\mathbf{F}_8^*$ acts on $\mathbf{F}_8$, for certain isomorphisms $\mathbf{Z}/7\mathbf{Z} \simeq \mathbf{F}_8^*$ and $Cl_{29} \simeq \mathbf{F}_8$;

$$G(H_{31}/\mathbf{Q}) \simeq [Cl_{31} \times_\gamma \mathbf{Z}/6\mathbf{Z}] \times \mathbf{Z}/5\mathbf{Z},$$

where $\mathbf{Z}/6\mathbf{Z}$ acts on $Cl_{31} \simeq \mathbf{Z}/9\mathbf{Z}$ as the multiplicative group $(\mathbf{Z}/9\mathbf{Z})^* \simeq \mathbf{Z}/6\mathbf{Z}$ acts on $\mathbf{Z}/9\mathbf{Z}$;

$$G(H_{37}/\mathbf{Q}) \simeq [Cl_{37} \times_\delta (\mathbf{Z}/37\mathbf{Z})],$$

where the action is given by Φ_{37}^{-3}.

Theorem 3. *The maximal unramified extension of $\mathbf{Q}(\mu_{23})$ is H_{23}, the Hilbert Class Field of $\mathbf{Q}(\mu_{23})$.*

Proof. Let K be the maximal unramified extension of $\mathbf{Q}(\mu_{23})$, denote its Galois group over $\mathbf{Q}$ by G. Using the previous table and arguing as in theorem 2, we see that $K/\mathbf{Q}(\mu_{23})$ is finite and $[K : \mathbf{Q}(\mu_{23})] \leq 21$. On the other hand, Cl_{23} is isomorphic to $\mathbf{Z}/3\mathbf{Z}$ and $[K : \mathbf{Q}(\mu_{23})] \geq 3$, we are going to show that the equality holds.

Fix a prime P of K above the rational prime 23; by lemma 1, G is isomorphic to a semidirect product

$$G' \times_{\varphi} I_P,$$

where $G' = G(K/\mathbf{Q}(\mu_{23}))$ is the first derived subgroup of G and $I_P \simeq (\mathbf{Z}/23\mathbf{Z})^*$ is the inertia subgroup at P, acting on the former by conjugation. The order $|G'|$ is smaller than 21 and in the lemma following the theorem we show that G' is too small to have an order 11 automorphism. This forces the action φ of $I_P \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z}$ to factor through its $\mathbf{Z}/2\mathbf{Z}$ quotient. Thus the index 2 subgroup $\mathbf{Z}/11\mathbf{Z} \subset I_P$ is normal in G and

$$G(\mathbf{Q}(\mu_{23})/\mathbf{Q}(\sqrt{-23})) \simeq G' \times \mathbf{Z}/11\mathbf{Z}.$$

Let now P' denote the prime of the quadratic field $\mathbf{Q}(\sqrt{-23})$ above the rational prime 23. We see that $\mathbf{Z}/11\mathbf{Z} \subset I_P$ is the inertia subgroup of $G(\mathbf{Q}(\mu_{23})/\mathbf{Q}(\sqrt{-23}))$ at the prime P above P'.

Setting $K^{\mathbf{Z}/11\mathbf{Z}} = K'$, the previous observations imply that K' is a Galois extension of $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt{-23})$ and *unramified* over $\mathbf{Q}(\sqrt{-23})$). Moreover

$$G(K'/\mathbf{Q}(\sqrt{-23})) \simeq G'.$$

We claim that K' is actually the maximal unramified extension of the quadratic subfield $\mathbf{Q}(\sqrt{-23})$.

To see this, first notice that, by its construction, K' is the maximal unramified extension of $\mathbf{Q}(\sqrt{-23})$ contained in K. Then, to conclude, observe that the maximal unramified extension of $\mathbf{Q}(\sqrt{-23})$ *has* to sit inside K since $\mathbf{Q}(\mu_{23})/\mathbf{Q}(\sqrt{-23})$ is totally ramified above P'.

To summarize, K is the compositum of $\mathbf{Q}(\mu_{23})$ and K', which are linearly disjoint over $\mathbf{Q}(\sqrt{-23})$. We have that

$$G' = G(K/\mathbf{Q}(\mu_{23})) \simeq G(K'/\mathbf{Q}(\sqrt{-23})).$$

Using the tables of Odlyzko we control the size of $G(K'/\mathbf{Q}(\sqrt{-23}))$. The discriminant root of K' equals $\sqrt{23} = 4.7985..$ and $[K' : \mathbf{Q}] \leq 6$ which implies $|G'| \leq 3$.
On the other hand $Cl_{23} \simeq \mathbf{Z}/3\mathbf{Z}$, so that

$$[K : \mathbf{Q}(\mu_{23})] = |G'| \geq 3.$$

Thus $G' \simeq \mathbf{Z}/3\mathbf{Z}$ and $K = H_{23}$, the Hilbert Class Field of $\mathbf{Q}(\mu_{23})$. □

To complete our argument in the previous theorem we still need the following

Lemma 4. *Let g be a finite group with $|g| \leq 21$. Then g has no order 11 automorphisms.*

Proof. Assume that g has an order 11 automorphism, call it σ. Then $|g| = k11 + m$, where k is the number of orbits of length 11 under the action of $< \sigma >= \mathbf{Z}/11\mathbf{Z}$ and $m \geq 1$ is the cardinality of the invariant subgroup.
By assumption $m < |g|$, thus $k \neq 0$ and this forces $k = 1$ so that $|g| = 11+m$. Since m divides $|g|$ it has also to divide 11 and we see that $m = 1$. Thus g is a group of order 12 with an action of $\mathbf{Z}/11\mathbf{Z}$ given by 2 orbits of respective lengths 1 and 11. In other words, any two non-identical elements of g are connected by an automophism. This is clearly a contradiction since g has order 12 and it has non-identical elements of relatively prime orders. □

Using the improved bounds under the *GRH* we prove in a similar way the corresponding statements of theorem 4 in the cases $p = 29, 31, 37$.

Theorem 5. *Assuming the GRH, for $p = 29, 31, 37$ the maximal unramified extension of $\mathbf{Q}(\mu_p)$ is H_p, the Hilbert Class Field of $\mathbf{Q}(\mu_p)$.*

Proof. **(p=29).** Let K be the *maximal unramified* extension of $\mathbf{Q}(\mu_{29})$, denote $G(K/\mathbf{Q})$ by G. Then $H_{29} \subset K$ and $[H_{29} : \mathbf{Q}(\mu_{29})] = 8$ divides $[K : \mathbf{Q}(\mu_{29})] = |G'|$. From the previous table we see that $|G'| \leq 14$, hence $|G'| = 8$ and $K = H_{29}$.
(p=31). Let K be the *maximal unramified* extension of $\mathbf{Q}(\mu_{31})$, denote $G(K/\mathbf{Q})$ by G. We see from the table that $|G'| \leq 23$ and then G' is solvable. Its abelianization G'/G'' is the Galois group $G(H_{31}/\mathbf{Q}(\mu_{31}))$, which is isomorphic to $\mathbf{Z}/9\mathbf{Z}$ the class group of $\mathbf{Q}(\mu_{31})$. We see from the bound

that if G'' were non trivial it would have to be isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and would make G' a group of order 18 whose abelianization is isomorphic to $\mathbf{Z}/9\mathbf{Z}$. To see that such a group doesn't exist we take a $3-$Sylow which has to be normal and hence gives a surjection onto $\mathbf{Z}/2\mathbf{Z}$, which contradicts the assumption on the abelianization of the group. This shows that G'' is trivial and $K = H_{31}$.

(p=37). Let K be the *maximal unramified* extension of $\mathbf{Q}(\mu_{37})$, denote $G(K/\mathbf{Q})$ by G. Then $G' = G(K/\mathbf{Q}(\mu_{37}))$, $H_{37} \subset K$ and the second derived subgroup G'' equals $G(K/H_{37})$. The bounds in the table tell us that $|G'| \leq 246$, this implies that $|G''| \leq 6$, taking in account $G(H_{37}/\mathbf{Q}(\mu_{37})) = G'/G'' \simeq \mathbf{Z}/37\mathbf{Z}$.

Consider now the exact sequence

$$1 \longrightarrow G'' \longrightarrow G' \longrightarrow \mathbf{Z}/37\mathbf{Z} \longrightarrow 0.$$

The order of G'' is relatively prime to 37 thus, by Schur-Zassenhaus lemma (cf. [**?**], theorem 7.13), the sequence splits and

$$G' \simeq G'' \times_{\varphi} \mathbf{Z}/37\mathbf{Z},$$

for a certain semidirect product structure φ. But G'' is too small to have an order 37 automorphism and the product is a *direct* product. This forces G'' to be trivial, otherwise there would be an abelian quotient of G' whose projection map would have a kernel strickly smaller than G'', a contradiction by the definition of G''. □

2. Classification of certain mod p Galois representations

We shall first define the type of Galois representations we are interested in. Fix an odd prime number p and embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. Denote by D and I, respectively, the *decomposition* and *inertia* subgroup of $G_{\mathbf{Q}}$ at p corresponding to the embedding. The *tame inertia* group is the quotient of I by its maximal *pro-p* subgroup, we denote it by I_t.

Consider an algebraic closure $\overline{\mathbf{F}}_p$ of the prime field with p elements and a finite dimensional vector space V over $\overline{\mathbf{F}}_p$ of dimension m. Let $\rho : G_{\mathbf{Q}} \to GL(V)$ be a continuous group homomorphism, $G_{\mathbf{Q}}$ being regarded with its natural pro-finite topology and $GL(V)$ being equipped with the discrete topology. The continuity condition is then equivalent to ρ factoring through

the Galois group of a number field. In the sequel we always assume that the representation ρ satisfies the following special conditions:
i) ρ is *unramified* outside p;
ii') ρ is *tamely* ramified at p;
ii") $\rho_{|I_t}$ is direct sum of *level* 1 characters.
The group I_t is isomorphic to the inverse limit $\lim_{\leftarrow} \mathbf{F}_{p^n}^*$ taken with respect to the norm maps. A level 1 character of I_t valued in $\overline{\mathbf{F}}_p^*$ is a non trivial character which factors through the quotient map $I_t \to \mathbf{F}_p^*$, i.e. it is a power of the mod p local cyclotomic character of $G(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, denoted by χ_p. One can show that condition $ii')$ is equivalent to asking to $\rho_{|D}$, the local representation at p, being semisimple (cf. [**?**], §1.6, prop. 4).
We have the following simple fact.

Proposition 6. *For an odd prime p, let K_ρ be the number field fixed by the kernel of ρ. Then $K_\rho\mathbf{Q}(\mu_p)/\mathbf{Q}(\mu_p)$ is an unramified extension. Equivalently, K_ρ is an unramified extension of $K_\rho \cap \mathbf{Q}(\mu_p)$.*

Proof. The Galois group $G_{\mathbf{Q}(\mu_p)}$ surjects onto $G(K_\rho\mathbf{Q}(\mu_p)/\mathbf{Q}(\mu_p))$. If $I' < G_{\mathbf{Q}}$ is *any* inertia subgroup at p we show that the image of $I' \cap G_{\mathbf{Q}(\mu_p)}$ under the quotient map

$$G_{\mathbf{Q}(\mu_p)} \longrightarrow G(K_\rho\mathbf{Q}(\mu_p)/\mathbf{Q}(\mu_p))$$

is trivial. Equivalently we show that

$$I' \cap G_{\mathbf{Q}(\mu_p)} < G_{K_\rho} \cdot G_{\mathbf{Q}(\mu_p)}.$$

This is easily done for $I' = I$: take $\sigma \in I \cap G_{\mathbf{Q}(\mu_p)}$, denote by

$$\Phi_p : G_{\mathbf{Q}} \longrightarrow \mathbf{F}_p^*$$

the *global* mod p cyclotomic character. Then

$$\chi_p(\sigma) = \Phi_p(\sigma) = 1,$$

which implies that $\rho(\sigma) = 1$. Equivalently, $\sigma \in G_{K_\rho}$ and therefore

$$I \cap G_{\mathbf{Q}(\mu_p)} < G_{K_\rho} \cdot G_{\mathbf{Q}(\mu_p)}.$$

If I' is now any inertia subgroup at p then we have $I' = \tau I \tau^{-1}$, for some $\tau \in G_{\mathbf{Q}}$. The groups $G_{\mathbf{Q}(\mu_p)}$ and $G_{K_\rho} \cdot G_{\mathbf{Q}(\mu_p)}$ are both normal in $G_{\mathbf{Q}}$ and conjugating the previous inclusion leads to

$$I' \cap G_{\mathbf{Q}(\mu_p)} < G_{K_\rho} \cdot G_{\mathbf{Q}(\mu_p)},$$

which completes the proof. □

Every representation ρ satisfying the above conditions has then to factor through the Galois group of the maximal unramified extension of $\mathbf{Q}(\mu_p)$. Thanks to the results of the previous section we are able to classify all such ρ for small primes p.
By assumption, the local shape at the inertia I at p of ρ is of the form

$$\rho_{|I} \simeq \begin{pmatrix} {\chi_p}^{a_1} & 0 & \cdots & 0 \\ 0 & {\chi_p}^{a_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & {\chi_p}^{a_m} \end{pmatrix},$$

for some integers a_i, where $1 \leq i \leq m$. There is an obvious representation ρ unramified outside p and with this behaviour at the inertia at p: it is obtained replacing χ_p with Φ_p, the global mod p cyclotomic character, in the previous matrix description. If $p \leq 19$, this is in fact the only possibility for ρ.

Theorem 7. *Let p be an odd prime, $p \leq 19$. Then $\rho \simeq \oplus_i \Phi_p^{a_i}$.*

Proof. For $p \leq 19$ there are no non-trivial unramified extension of $\mathbf{Q}(\mu_p)$. Thus, by the previous proposition, ρ factors through $G(\mathbf{Q}(\mu_p)/\mathbf{Q})$ and the theorem follows since I surjects onto $G(\mathbf{Q}(\mu_p)/\mathbf{Q})$. □

Consider next the cases $p = 23, 29$ and 31. From the facts of section §.1 we see that ρ factors through $G(H_p/\mathbf{Q})$, the Galois group of the Hilbert Class Field of $\mathbf{Q}(\mu_p)$ over $\mathbf{Q}$ (under *GRH* for $p = 29$ and 31). In each of these cases p is a *regular* prime and hence p does not divide $|G(H_p/\mathbf{Q})|$. In particular, the mod p representation ρ is *semisimple*. In Appendix B we describe all the absolutely irreducible representations of $G(H_p/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$, for a regular prime p. We also show that a positive integer $n \geq 1$ can occour as dimension of an irreducible representation if and only if the degree n subfield of $\mathbf{Q}(\mu_p)$ has class number *strictly bigger* that the one of any of its subfields. In particular, there exist an irreducible representation ρ satisfying *i*) and *ii*) of dimension 2 if and only if the class number of $\mathbf{Q}\sqrt{\pm p}$ is non trivial (+ holds if and only if $p \equiv 1 \bmod 4$).

In the case $p = 23$ we have the following:

Theorem 8. *If $p = 23$ then ρ is semisimple. Its irreducible subrepresentations are of the following type:*
i) Φ_{23}^{h}, for $h \in \{0; 1; \ldots; 21\}$;
ii) $\Phi_{23}^{2h} \otimes \delta$, for $h \in \{0; 1; \ldots; 10\}$, where δ is of dimension 2 and $\delta = Ind_H^G(\psi)$ for a non trivial character $\psi G(H_{23}/\mathbf{Q}\sqrt{-23})$ described below.

To obtain ψ take a non trivial character $\psi' : \mathrm{Cl}_{23} \simeq \mathbf{Z}/3\mathbf{Z} \rightarrow \mathbf{F}_{23^2}^*$ and extend it to the subgroup $\mathrm{Cl}_{23} I_P^2 = G() H_{23}/\mathbf{Q}\sqrt{-23}$ by the formula

$$\psi(a \cdot x) = \psi'(a).$$

One sees that $\mathrm{Ind}_H^G(\psi) \simeq \mathrm{Ind}_H^G(\psi^2)$, more details are avaiable in Appendix B. The representation δ induces an isomorphism

$$G(H_{\sqrt{-23}}/\mathbf{Q}) \simeq S_3 \longrightarrow GL_2(\overline{\mathbf{F}}_{23}),$$

where $H_{\sqrt{-23}}$ is the Hilbert Class Field of $\mathbf{Q}(\sqrt{-23})$ and S_3 is the permutation group in 3 letters. Among the 2-dimensional irreducible representations, δ has the "smallest image" and it is the only one with trivial center (cf. Appendix B).

The representation $\Phi_{23}^{2h} \otimes \delta$ induces an isomorphism

$$G(H_{\sqrt{-23}}\mathbf{Q}_{(}\mu_{23})^{\otimes 2h}/\mathbf{Q}) \simeq S_3 \times C_{2h} \subset GL_2(\overline{\mathbf{F}}_{23}),$$

where $\mathbf{Q}(\mu_{23})^{\otimes 2h}$ is the subfield of $\mathbf{Q}(\mu_{23})$ corresponding to the kernel of Φ_{23}^{2h} and C_{2h} is the cyclic group $G(\mathbf{Q}(\mu_{23})^{\otimes 2h}/\mathbf{Q})$.

The representation δ has Serre's weight 12 and it arises from the unique cusp form of weight 12 for the full modular group $PSL_2(\mathbf{Z})$. We now compute its trace at the Frobenius elements. Let G be the Galois group $G(H_{\sqrt{-23}}/\mathbf{Q})$. If $\mathbf{P} = \{P_1; P_2; P_3\}$ is the set of primes of $H_{\sqrt{-23}}$ above p then the action of G on $\mathbf{P}$ establishes an isomorphism $G \rightarrow S_3$ and gives rise to a 3 dimensional representation Π, viewing S_3 inside $GL_3(\mathbf{F}_{23})$. In the appendix we show that $\Pi \simeq 1 \oplus \delta$, where 1 is the trivial character of G^{ab}. This implies that the traces of δ on the conjugacy classes of S_3 are given from the table:

	$\{\mathrm{id}\}$	$\{(12);(23);(31)\}$	$\{(123);(132)\}$
$\mathrm{tr}(\delta)$	2	0	-1

If $f(X) \in \mathbf{Z}[X]$ is a monic polynomial of degree 3 whose splitting field is $H_{\sqrt{-23}}$ then one can show that for almost all primes $l \neq 23$ the equivalence modulo 23 holds:

$$tr(\Pi(\mathrm{Frob}_l)) \equiv \#\{\text{solutions of } f(X) \equiv 0(\bmod l)\}.$$

We can take for example $f(X) = X^3 - X - 1$.
If l is an unramified prime for δ, then it is easy to see, using a bit of Class Field Theory, that:
i) $\mathrm{Frob}_l = id \Leftrightarrow l = x^2 + 23y^2$, for some integers x, y;
ii) $\mathrm{Frob}_l \in \{(12);(23);(31)\} \Leftrightarrow (\frac{l}{23}) = 1$ but $l \neq x^2 + 23y^2$, for every x, y;
iii) $\mathrm{Frob}_l \in \{(123);(132)\} \Leftrightarrow (\frac{l}{23}) = -1$.
The previous translates into the well known congruences modulo 23 satisfied by the Ramanujan Δ function $\tau(n)$ evaluated at primes $l \neq 23$.

Let's now consider the situation for $p = 29$ and 31.

Theorem 9. *Assuming GRH, if $p = 29$ then ρ is semisimple. Its irreducible subrepresentations are of the following type:*
i) Φ_{29}^h, for $h \in \{0;1;\ldots;27\}$;
ii) $\Phi_{29}^{7h} \otimes \gamma$, for $h \in \{0;1;2;3\}$, where $\gamma = Ind_H^G(\psi)$, for a non trivial character $\psi : Cl_{29} \simeq (\mathbf{Z}/2\mathbf{Z})^3 \to \mathbf{F}_{29}^*$, the group G being $G(H_{29}/\mathbf{Q})$ and $H = G(H_{29}/\mathbf{Q}(\mu_{29})^{\otimes 4})$, where $\mathbf{Q}(\mu_{29})^{\otimes 4}$ is the degree 7 subfield of $\mathbf{Q}(\mu_{29})$, which corresponds to the kernel of Φ_{29}^4.

The representation $\Phi_{29}^{7h} \otimes \gamma$ has degree 7, its image has trivial center if and only if $h = 0$. Since the quadratic field $\mathbf{Q}(\sqrt{29})$ has class number 1, there are no irreducible 2 dimensional representations ρ.

Theorem 10. *Assuming GRH, if $p = 31$ then ρ is semisimple. Its irreducible subrepresentations are of the following type:*
i) Φ_{31}^h, for $h \in \{0;1;\ldots;29\}$;
ii) $\Phi_{31}^{2h} \otimes \theta$, for $h \in \{0;1;\ldots;14\}$, where $\theta = Ind_H^G(\psi)$, for an order 3 character $\psi : Cl_{31} \simeq \mathbf{Z}/9\mathbf{Z} \to \mathbf{F}_{31}^*$, the group G being $G(H_{31}/\mathbf{Q})$ and $H = G(H_{31}/\mathbf{Q}(\sqrt{-31})$;
iii) $\Phi_{31}^{6h} \otimes \lambda$, for $h \in \{0;1;2;3;4\}$, where $\lambda = Ind_H^G(\psi)$, for an order 9

character $\psi : Cl_{31} \simeq \mathbf{Z}/9\mathbf{Z} \to \mathbf{F}^*_{31^3}$, the group G being $G(H_{31}/\mathbf{Q})$ and $H = G(H_{31}/\mathbf{Q}(\mu_{31})^{\otimes 5}))$; where $\mathbf{Q}(\mu_{31})^{\otimes 5}$ is the degree 6 subfield of $\mathbf{Q}(\mu_{31})$, which corresponds to the kernel of Φ^5_{31}.

The representation $\Phi^{2h}_{31} \otimes \theta$ has degree 2 and observations analogous to the case $p = 23$ can be carried out. The existence of 2 dimensional irreducible ρ reflets the fact that $\mathbf{Q}(\sqrt{-31})$ has non trivial class number. The Serre's weight of θ equals 16 and the representation arises from the unique modular form of the same weight which is $E_2\Delta$, the product of the weight 4 Eisenstein serie and the Ramanujan Delta function. Reasoning as before we can write down congruences that the coefficients of $E_2\Delta$ satisfy at primes $l \neq 31$ modulo 31.

The representation $\Phi^{6h}_{31} \otimes \lambda$ has degree 6 and *even* determinant. Its existence is related to the fact that the degree 6 subfield of $\mathbf{Q}(\mu_{31})$ has class number stricly bigger than the one of any of its subfields.

Appendix A: Computation of $G(H_p/\mathbf{Q})$, for $p = 23, 29$ and 31

Proposition 11. *Let p be a prime number. Denote with G_p the Galois group of H_p over $\mathbf{Q}$. Then*

- $G_{23} \simeq S_3 \times \mathbf{Z}/11\mathbf{Z}$

S_3 being the permutation group in three letters;

- $G_{29} \simeq \{(\mathbf{Z}/2\mathbf{Z})^3 \times_\alpha \mathbf{Z}/7\mathbf{Z}\} \times \mathbf{Z}/4\mathbf{Z}$,

where α maps a generator to an order 7 element of $GL_3(\mathbf{F}_2)$;

- $G_{31} \simeq \{\mathbf{Z}/9\mathbf{Z} \times_\beta \mathbf{Z}/6\mathbf{Z}\} \times \mathbf{Z}/5\mathbf{Z}$,

where β gives an isomorphism $\mathbf{Z}/6\mathbf{Z} \simeq (\mathbf{Z}/9\mathbf{Z})^*$.

The extension $H_p/\mathbf{Q}(\mu_p)$ is unramified with Galois group Cl_p. We already remarked that (cf. §.1, lemma 1):

- $G'_p = Gal(H_p/\mathbf{Q}) \simeq \mathrm{Cl}_p$;
- $G_p \simeq G'_p \times_\varphi I_p = \mathrm{Cl}_p \times_\varphi (\mathbf{Z}/p\mathbf{Z})^*$;

where I_p is an inertia subgroup of G_p at a prime above p. Since $G'_p = \mathrm{Cl}_p$ is abelian, we observe that the semidirect product structure described by φ is not trivial unless $\mathrm{Cl}_p = 1$.

The three class groups are (cfr Washington)

- $\mathrm{Cl}_{23} \simeq \mathbf{Z}/3\mathbf{Z}$;
- $\mathrm{Cl}_{29} \simeq (\mathbf{Z}/2\mathbf{Z})^3$;

- $\mathrm{Cl}_{31} \simeq \mathbf{Z}/9\mathbf{Z}$.

We need to determine the corresponding actions. They are described by a non trivial group homomorphism $\varphi_p : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathrm{Aut}(\mathrm{Cl}_p)$.

(p=23) The automorphisms group of $\mathrm{Cl}_{23} \simeq \mathbf{Z}/3\mathbf{Z}$ is cyclic of order 2, $(\mathbf{Z}/23\mathbf{Z})^*$ is cyclic of order 22. Hence there's only one non trivial map

$$\varphi_{23} : (\mathbf{Z}/23\mathbf{Z})^* \longrightarrow \mathrm{Aut}(\mathbf{Z}/3\mathbf{Z});$$

$(\mathbf{Z}/23\mathbf{Z})^*$ acts on $\mathbf{Z}/3\mathbf{Z}$ permuting the 2 non trivial elements. The index 2 subgroup of $(\mathbf{Z}/23\mathbf{Z})^*$ acts trivially. $(\mathbf{Z}/23\mathbf{Z})^*$ is isomorphic to $\mathbf{Z}/22\mathbf{Z} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z}$, this implies that

$$G_{23} \simeq \mathbf{Z}/3\mathbf{Z} \times_{\varphi_{23}} \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z},$$

and we proved the statement for $p = 23$.

Remark 2. The order 11 subgroup of $(\mathbf{Z}/23\mathbf{Z})^*$ is the kernel of φ_{23}. This means that the class group of $\mathbf{Q}(\mu_{23})$ is isomorphic to the class group of its quadratic subfield $\mathbf{Q}(\sqrt{-23})$ (for the details cf. [**?**]). Moreover if we denote the Hilbert Class Field of $\mathbf{Q}(\sqrt{-23})$ by $H_{\sqrt{-23}}$ we have that H_{23} is the compositum of $\mathbf{Q}(\mu_{23})$ and $H_{\sqrt{-23}}$, which are linearly disjoint extension of $\mathbf{Q}(\sqrt{-23})$. With the aid of maple, one then shows that the splitting field of $f(X) = X^3 - X - 1$ is an unramified extension of $\mathbf{Q}(\sqrt{-23})$ and it is therefore equal to $H_{\sqrt{-23}}$.

(p=29) Before we prove the proposition for $p = 29$ we need a lemma:

Lemma 12. *There are no unramified $\mathbf{Z}/2\mathbf{Z}$-extensions of $\mathbf{Q}(\mu_p)$ which are Galois over $\mathbf{Q}$.*

Proof. Let K be such a number field. Then (cf. §.1, lemma 1)

$$G(K/\mathbf{Q}) \simeq G(K/\mathbf{Q}(\mu_p)) \times_{varphi} (\mathbf{Z}/p\mathbf{Z})^*.$$

But $G(K/\mathbf{Q}(\mu_p)) = \mathbf{Z}/2\mathbf{Z}$ has no non-trivial automorphisms and we already remarked above that the semidirect product structure φ cannot be trivial. Hence K does not exist. □

We know that $G_{29} \simeq (\mathbf{Z}/2\mathbf{Z})^3 \times_{\varphi_{29}} (\mathbf{Z}/29\mathbf{Z})^*$ for some φ_{29}, and the invariant subgroup $(\mathbf{Z}/2\mathbf{Z})^3$ is $G_{29}{}'$.

$(\mathbf{Z}/29\mathbf{Z})^*$ is cyclic of order 28, take a generator $\sigma \in (\mathbf{Z}/29\mathbf{Z})^*$; $\varphi(\sigma)$ is then an automorphism of $(\mathbf{Z}/2\mathbf{Z})^3$ and can be thought as a matrix $A_\sigma \in GL_3(\mathbf{F}_2)$. Replacing A_σ by a conjugate would give rise to an isomorphic semidirect product structure. Then we just have to determine the conjugacy class of A_σ. Notice also that we made a choice by picking a generator σ of $(\mathbf{Z}/29\mathbf{Z})^*$. The linear action of A_σ corresponds to conjugation by σ on $(\mathbf{Z}/2\mathbf{Z})^3$. Invariant lines in $(\mathbf{Z}/2\mathbf{Z})^3$ under A_σ correspond exatly to $\mathbf{Z}/2\mathbf{Z}$ extension of $\mathbf{Q}(\mu_{29})$ inside H_{29} which are normal over $\mathbf{Q}$. We notice in the lemma that such extensions don't exist, hence A_σ doesn't fix any line or, equivalently, $A_\sigma - 1$ is invertible.

Clearly ${A_\sigma}^{28} = 1$ and A_σ satisfies the polynomial $X^{28} - 1 \in \mathbf{F}_2[X]$ whoose factorization into irreducible factors is

$$X^{28} - 1 = (X^7 - 1)^4 = (X-1)^4 (X^3 + X^2 + 1)^4 (X^3 + X + 1)^4.$$

Since $A_\sigma - 1$ is invertible, A_σ satisfies

$$Q(X) = (X^3 + X^2 + 1)^4 (X^3 + X + 1)^4,$$

and if $M(X)$ is the monic minimal polynomial of A_σ, $M(X)|Q(X)$.

But $deg(M(X)) \leq 3$ and the irreducible factors of $Q(X)$ have both degree 3. This implies $M(X) \in \{(X^3 + X^2 + 1); (X^3 + X + 1)\}$, $M(X)$ is irreducible, $M(X)|X^7 - 1$ and A_σ has order 7. Looking at the factorization

$$(X^7 - 1) = (X-1)(X^3 + X^2 + 1)(X^3 + X + 1)$$

we see that the 6 powers of A_σ different than the identity divide into 2 subsets according to their minimal polynomial. This means that up to replacing σ with σ^k for some $k \in (\mathbf{Z}/7\mathbf{Z})^*$ we can assume that A_σ satisfies, let's say, $X^3 + X + 1$. Since the polynomial is irreducible, the conjugacy class of A_σ is determined and we are done.

(p=31) $G_{31} \simeq (\mathbf{Z}/9\mathbf{Z}) \times_{\varphi_{31}} (\mathbf{Z}/31\mathbf{Z})^*$ and its derived subgroup is $\mathbf{Z}/9\mathbf{Z}$. The automorphism group of $(\mathbf{Z}/9\mathbf{Z})$ is cyclic of order 6, generated by multiplication by $2 \in (\mathbf{Z}/9\mathbf{Z})^*$. $(\mathbf{Z}/31\mathbf{Z})^*$ is isomorphic to $(\mathbf{Z}/6\mathbf{Z}) \times (\mathbf{Z}/5\mathbf{Z})$ and then it has to act on $\mathbf{Z}/9\mathbf{Z}$ via its $\mathbf{Z}/6\mathbf{Z}$ quotient. Hence

$$G_{31} \simeq \{\mathbf{Z}/9\mathbf{Z} \times_\varphi \mathbf{Z}/6\mathbf{Z}\} \times \mathbf{Z}/5\mathbf{Z}$$

and we need to determine the morphism φ.

Take a generator σ of $\mathbf{Z}/6\mathbf{Z}$, then $\varphi(\sigma)$ is a non-trivial automorphism of $(\mathbf{Z}/9\mathbf{Z})$ and it corresponds to a certain $a_\sigma \in (\mathbf{Z}/9\mathbf{Z})^*$, $a_\sigma \neq 1$. Up to replacing σ with σ^5 (the other generator of $\mathbf{Z}/6\mathbf{Z}$) we can assume $a_\sigma \in \{2,4,8\} \subset (\mathbf{Z}/9\mathbf{Z})^*$. And, in fact, these 3 possibilities give rise to pairwise non-isomorphic groups. We show that $a_\sigma = 2$ obtaining contradictions in the other two cases.

If $a_\sigma = 4$ then the action of $\mathbf{Z}/6\mathbf{Z}$ on $\mathbf{Z}/9\mathbf{Z}$ would be trivial modulo the order 3 subgroup of $\mathbf{Z}/9\mathbf{Z}$, which would make such subgroup invariant and equal to the derived subgroup; and this can't be the case.

If $a_\sigma = 8$ then the action of $\mathbf{Z}/6\mathbf{Z}$ on $\mathbf{Z}/9\mathbf{Z}$ would factor through the $\mathbf{Z}/2\mathbf{Z}$ quotient of $\mathbf{Z}/6\mathbf{Z}$. This mean that the index 2 subgroup of I acts trivially. Which, in particular, implies that $\mathbf{Q}(\sqrt{-31})$, the quadratic subfield of $\mathbf{Q}(\mu_{31})$, has class number 9. This is a contradiction since the class number of $\mathbf{Q}(\sqrt{-31})$ is 3. To see this one can refere to the correspondece between ideal class group of a quadratic field of negative discriminant and proper equivalence classes of quadratic forms of a fixed discriminant to conclude that there are only 3 such classes (representative of these classes may be taken to be: $(X^2 + XY + 8Y^2); (2X^2 + XY + 4Y^2); (2X^2 - XY + 4Y^2)$). For a beautiful account of these correspondence the reader is referred to [**?**].

Appendix B: representations of $G(H_p/\mathbf{Q})$ in char p, for a regular prime

Fix a regular prime $p \geq 23$ and for simplicity denote $G(H_p/\mathbf{Q})$ by G. We know that $G \simeq Cl_p \times_\varphi (\mathbf{Z}/p\mathbf{Z})^*$ and $G' = Cl_p$ (cf. §.1). By assumption the order of G is not divisible by p and every finite dimensional representation of G on a vector space over $\overline{\mathbf{F}}_p$ is semisimple, i.e. it is isomorphic to the direct sum of its irreducible subrepresentations. Following the criterion of Mackey and Wigner for small groups we recall the construction of all the absolutely irreducible finite dimensional representations of G over $\overline{\mathbf{F}}_p$.

Denote by $\widehat{Cl}_p$ the group of characters

$$\psi : Cl_p \longrightarrow \overline{\mathbf{F}}_p^*$$

valued in $\overline{\mathbf{F}}_p^*$. Since p is regular, $Cl_p \simeq \widehat{Cl}_p$ and any irreducible characteristic p representation of Cl_p is given by one of these characters.

The cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$ acts on $\widehat{Cl}_p$ in a natural way by the formula

$$\psi^\sigma(x) = \psi(\sigma^{-1}.x),$$

where $\psi \in \widehat{Cl}_p$, $\sigma \in (\mathbf{Z}/p\mathbf{Z})^*$ and $x \in Cl_p$.
For a character $\psi \in \widehat{Cl}_p$, define S_ψ to be the subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$ which stabilizes ψ and denote by $Cl_p \cdot S_\psi$ the subgroup generated by Cl_p and S_ψ in G. This is readily seen to be isomorphic to

$$Cl_p \times_\varphi S_\psi,$$

where, by abuse of notation, we keep using φ to indicate the semidirect product structure.
If $[(\mathbf{Z}/p\mathbf{Z})^* : S_\psi] = f$ then every character of S_ψ valued in $\overline{\mathbf{F}}_p^*$ is of the restiction to S_ψ of Φ_p^{fk}, for a unique $k \in \{1; 2; \ldots; (p-1)/f\}$, and in fact ϕ takes values in $\mathbf{F}_p^*$. We will think of such a ϕ as a character on $Cl_p \cdot S_\psi$.
Extend $\psi \in \widehat{Cl}_p$ to a character ψ' of $Cl_p \cdot S_\psi$ by the formula

$$\psi'(x\sigma) = \psi(x),$$

where $\sigma \in S_\psi$ and $x \in Cl_p$.
Then consider the tensor product $\psi' \otimes \phi$, where $\phi = \Phi_p^{fk}$. Define

$$\theta_{\psi,\phi} = \mathrm{Ind}(\psi' \otimes \phi)$$

to be the corresponding induced representation to the whole group $Cl_p \times_\varphi (\mathbf{Z}/p\mathbf{Z})^*$.
Then
i) $\theta_{\psi,\phi}$ is *irreducible*;
ii) $\theta_{\psi_1,\phi_1} \sim \theta_{\psi_2,\phi_2}$ if and only if ψ_1 and ψ_2 are in the same $(\mathbf{Z}/p\mathbf{Z})^*$-orbit and $\phi_1 = \phi_2$;
iii) any irreducible representation of G is isomorphic to one of the $\theta_{\psi,\phi}$.

Remark 3. If F is a subfield of $\mathbf{Q}(\mu_p)$ and Cl_F is its class group, then Cl_p surjects onto Cl_F under the natural Norm map N_F of (classes of) ideals. More generally, if $F \subset F' \subset \mathbf{Q}(\mu_p)$ then the norm map $N_{F'/F}$ between class group is surjective. This is to say that the dual group $\widehat{\mathrm{Cl}}_p$ is equipped with the subgroups $\widehat{\mathrm{Cl}}_F$, where $\widehat{\mathrm{Cl}}_F < \widehat{\mathrm{Cl}}_{F'}$ if $F \subset F'$.
If $\psi : \mathrm{Cl}_p \to \overline{\mathbf{F}}_p^*$ is a character of Cl_p, then the smallest subfield F of $\mathbf{Q}(\mu_p)$ so that $\psi \in \widehat{\mathrm{Cl}}_F$, is the unique subfield whose degree over $\mathbf{Q}$ equals the index $f = [(\mathbf{Z}/p\mathbf{Z})^* : S_\psi]$. In particular such an F has class number stricly bigger than the one of any of its proper subfields. Now notice that as ψ runs in $\widehat{\mathrm{Cl}}_p$ the integers $f = [(\mathbf{Z}/p\mathbf{Z})^* : S_\psi]$ describe all the possible dimension of the

irreducible mod p representations of $G(H_p/\mathbf{Q})$. We then conclude that in order for an integer $n \geq 1$ to be equal to the dimension of one of the $\theta_{\psi,\lambda}$ it is necessary and sufficient that there is a degree n subfield of $\mathbf{Q}(\mu_p)$ whose class number is strictly bigger than the one of any of its proper subfields.

Denoting by 1 the trivial character of S_ψ, it is immediate to verify that

$$\theta_{\psi,\phi} \sim \theta_{\psi,1} \otimes \Phi_p^{fh},$$

for a unique integer $h \in \{1; 2 \dots (p-1)/f\}$. Thus, as ψ runs into the orbit space $(\mathbf{Z}/p\mathbf{Z})^* \backslash \widehat{Cl}_p$ the representations $\theta_{\psi,1} = \theta_\psi$ give a set of pairwise non-isomorphic irreducible representations of $G(H_p/\mathbf{Q})$ so that any other irreducible representation can be obtained by tensoring one of the previous by a suitable power of Φ_p. We can caracterize them in the following way:

Proposition 13. *Let p a regular prime and π a characteristic p irreducible representation of $G(H_p/\mathbf{Q})$. Then $Im(\pi)$ has trivial center if and only if $\pi \sim \theta_\psi$, for some $\psi \in \widehat{Cl}_p$.*

Proof. We begin by showing that $\mathrm{Im}(\theta_\psi)$ has trivial center. This can be done by using the following model for θ_ψ.
Consider $O_\psi = \{\psi; \psi^\sigma; \dots \psi^{\sigma^{f-1}}\}$, the $(\mathbf{Z}/p\mathbf{Z})^*$-orbit of ψ, where σ generates $(\mathbf{Z}/p\mathbf{Z})^*$ and $f = [(\mathbf{Z}/p\mathbf{Z})^* : S_\psi]$. Construct the representation of Cl_p given by the direct sum

$$\pi_\psi = \oplus_i \psi^{\sigma^i},$$

where $i = 0, 1, \dots f-1$. For $i \in \mathbf{Z}/f\mathbf{Z}$, take a vector v_i in the underlying vector space of π_ψ generating the ψ^{σ^i} isotypical component. Then π_ψ becomes a $Cl_p \times_\varphi (\mathbf{Z}/p\mathbf{Z})^*$-module by the formula

$$\pi_\psi(x\sigma^k)v_i = \psi^{\sigma^{k+i}}(x)v_{i+k},$$

where $x \in Cl_p$. We have $\pi_\psi \sim \theta_\psi$.
If $y \in G(H_p/\mathbf{Q})$ is so that $\pi_\psi(y)$ is central in $\mathrm{Im}(\pi_\psi)$, then, by Schur's lemma, $\pi_\psi(y)$ has to be the multiplication by a scalar. From the explicit description of π_ψ, we see that $\pi_\psi(y) = 1$ and the center of $\mathrm{Im}(\pi_\psi) = \mathrm{Im}(\theta_\psi)$ is trivial.
In order to prove the other direction, let π be a characteristic p irreducible representation of $G(H_p/\mathbf{Q})$, so that the center of $\mathrm{Im}(\pi)$ is trivial. We have

$$\pi \sim \theta_{\psi,1} \otimes \Phi_p^{fh},$$

for a unique integer h, with $1 \leq h \leq (p-1/f)$, where $f = [(\mathbf{Z}/p\mathbf{Z})^* : S_\psi]$. The kernel of the representation is the subgroup defined by $y \in G(H_p/\mathbf{Q})$ so that

$$\theta_{\psi,1}(y) = \Phi_p^{-fh}(y).$$

But since $\theta_{\psi,1}(y)$ is never a scalar unless $y = 1$ we have that the kernel of π is given by the $y \in G(H_p/\mathbf{Q})$ so that

$$\theta_{\psi,1}(y) = 1 \text{ and } \Phi_p^{fh}(y) = 1.$$

The center of π consists of the elements y so that $\pi(y)$ is scalar and it is therefore isomorphic to

$$\{y|\theta_{\psi,1}(y) = 1\}/\{y|\theta_{\psi,1}(y) = 1 \text{ and } \Phi_p^{fh}(y) = 1\}.$$

But since Φ_p^f generates the character group of S_ψ, the only way the center can be trivial is for $h = (p-1/f)$. So that $\pi \sim \theta_\psi$ and the proposition follows. □

Define Π to be the direct sum

$$\Pi = \oplus_\psi \theta_\psi,$$

as ψ runs into a complete set of $(\mathbf{Z}/p\mathbf{Z})^*$ inequivalent characters of Cl_p. Then Π is meaninful from an arithmetical point of view:

Proposition 14. *Let $\mathbf{P} = \{P_1; \ldots; P_h\}$ be the set of primes of H_p above the rational prime p. Consider the representation*

$$\pi : G(H_p/\mathbf{Q}) \longrightarrow S_h \subset GL_h(\mathbf{Z}),$$

given by the natural permutation action on P.
Then the kernel of π equals the center $Z(G(H_p/\mathbf{Q}))$ and $\pi \otimes \overline{\mathbf{F}}_p \sim \Pi$.

Proof. For simplicity denote $G(H_p/\mathbf{Q})$ by G. Let $I_P \simeq (\mathbf{Z}/p\mathbf{Z})^*$ be any inertia subgroup of G above p, then $G \simeq Cl_p \times_\varphi I_P$, for a certain $\varphi : I_P \to \mathrm{Aut}(Cl_p)$.
The group G acts transitively on $\mathbf{P}$ and there is a bijection

$$\mathbf{P} \leftrightarrow G/I_P,$$

moreover such coset space can be described as

$$G/I_P = \{x \cdot I_P,\ x \in Cl_p\}.$$

We have that

$$\sigma(x \cdot I_P) = \varphi_\sigma(x) \cdot I_P,$$

where $\sigma \in I_P$, $x \in Cl_p$ and φ_σ is the automorphism of Cl_p induced by conjugation by σ.

This is to say that φ describes the action of I_P on the set of primes of H_P above p.

It is known that the only fixed point of the action φ of I_P on Cl_P is the identical element. A simple computation then shows that the center is given by the elements of I_P acting trivially on Cl_p. By the previous observation this is precisely the kernel of π.

To prove the second part of the proposition notice that $\pi \otimes \overline{\mathbf{F}}_p$ is isomorphic to $\mathrm{Ind}_I^G(1)$, where 1 is the trivial character of I_P valued in $\mathbf{F}_p$, and the dimensions of $\pi \otimes \overline{\mathbf{F}}_p$ and of Π both equal $|Cl_p|$, the class number of $\mathbf{Q}(\mu_p)$. It will then suffice to show that θ_ψ occours as a subrepresentation of $\pi \otimes \overline{\mathbf{F}}_p$, for any $\psi \in \widehat{Cl}_p$ or, equivalently, that the $\overline{\mathbf{F}}_p$ vector space

$$\mathrm{Hom}_G(\theta_\psi, \pi \otimes \overline{\mathbf{F}}_p)$$

has dimension 1. By the Frobenius reciprocity

$$\mathrm{Hom}_G(\theta_\psi, \pi \otimes \overline{\mathbf{F}}_p) \simeq \mathrm{Hom}_{I_P}(\mathrm{Res}_{I_P}^G \theta_\psi, 1).$$

Recall that $\theta_\psi = \mathrm{Ind}_{Cl_p \cdot S_\psi}^G(\psi')$, where ψ' denotes the extension of ψ to the group $Cl_p \cdot S_\psi$ that we discussed above. Furthemore $\mathrm{Res}_{I_P}^G \theta_\psi$ is isomorphic to the direct sum of all the characters of I_P whose conductor contains S_ψ. In particular

$$\mathrm{Hom}_{I_P}(\mathrm{Res}_{I_P}^G \theta_\psi, 1)$$

is one dimensional and the proposition follows. □

Remark 4. Using the same notation as before, let A be any subgroup of $\widehat{\mathrm{Cl}}_p$ and S_A the subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$ which stabilizes any element of A. It can be shown that A *is isomorphic to the character group valued in* $\overline{\mathbf{F}}_p^*$ *of the class group of* $\mathbf{Q}(\mu_p)^{S_A}$, call this field F (for the details, cf. [**?**]). Moreover, let B the intersection of the kernels of all the elements of A. Then $B \cdot S_A$ is a normal subgroup of $G(H_p/\mathbf{Q})$ and the corresponding subfield $H_p^{B \cdot S_A}$ is the Hilbert Class Field H_F of F. Arguing as in the proposition we can show that

$$\Pi_F \simeq \oplus_{\psi \in A} \theta_\psi,$$

where Π_F is the representation of $G(H_q/\mathbf{Q})$ arising from the permutation action on primes of H_F above p.