MOD p GALOIS REPRESENTATIONS AND THE MOD p LOCAL LANGLANDS CORRESPONDENCE FOR $\mathrm{GL}_2(\mathbb{Q}_p)$

ZACHARY FENG

1. Galois groups

Let F be a finite extension of $\mathbb{Q}_p$, with uniformizer ϖ, and residue field $k_F \cong \mathbb{F}_q$. Let $\overline{F}$ be the algebraic closure of F. Let $\Gamma_F := \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group of F.

1.1. Maximal unramified extension F^{ur} of F.

For each $n \geq 1$, let $\mathbb{F}_{q^n}$ denote the unique degree n extension of $\mathbb{F}_q$. We can lift the minimal polynomial of a primitive element of $\mathbb{F}_{q^n}/\mathbb{F}_q$ from $k_F[X]$ to $\mathcal{O}_F[X]$, and let F_n be the splitting field of this polynomial over F. We then have that F_n/F is an unramified extension of degree n, ϖ is still a uniformizer for F_n, and $k_{F_n} \cong \mathbb{F}_{q^n}$. Set

$$F^{\mathrm{ur}} := \bigcup_{n\geq 1} F_n.$$

Some facts about F^{ur}:

(1) $F^{\mathrm{ur}} = \bigcup_{(s,p)=1} F(\zeta_s)$ (since $F_n = F(\zeta_{q^n-1})$).
(2) $k_{F^{\mathrm{ur}}} \cong \overline{k}_F \cong \overline{\mathbb{F}}_q$.
(3) F^{ur}/F is Galois (as each F_n/F is) and

$$\mathrm{Gal}(F^{\mathrm{ur}}/F) = \varprojlim \mathrm{Gal}(F_n/F) \cong \varprojlim \mathrm{Gal}(k_{F_n}/k_F) \cong \varprojlim(\mathbb{Z}/n\mathbb{Z}) = \widehat{\mathbb{Z}}.$$

(4) $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ is topologically generated by φ (arithmetic Frobenius) whose action on $k_{F^{\mathrm{ur}}} \cong \overline{k}_F$ is given by $x \mapsto x^q$.

1.2. Maximal tamely ramified extension F^{tr} of F.

Let K be a complete DVF, with Dedekind ring A and maximal ideal $\mathfrak{p}$, and we assume that $A/\mathfrak{p}$ is perfect. Let E/K be an extension of degree n. Then the integral closure B of A in E is the Dedekind ring of E, and we let $\mathfrak{P}$ be its maximal ideal.

We write $n = ef$ where $\mathfrak{p}B = \mathfrak{P}^e$ and $[B/\mathfrak{P} : A/\mathfrak{p}] = f$. We say that E is *totally ramified* over K if $n = e$, and that E is *tamely ramified* over K if the characteristic p of the residue field $A/\mathfrak{p}$ does not divide e. We describe totally and tamely ramified extensions of K.

Proposition 1.1 (II, Proposition 11 [Lan94] or Theorem 11.5 [Sut21])**.**
Assume that E is totally ramified over K, so that $n = e$. Let $\Pi \in B$ be an element of order 1 at $\mathfrak{P}$, that is, Π is a uniformizer for B. Then $E = K(\Pi)$ and in fact the minimal polynomial of Π over K is an Eisenstein equation

$$X^e + a_{e-1}X^{e-1} + \cdots + a_0 = 0,$$

where $a_i \in \mathfrak{p}$ for all i and $a_0 \not\equiv 0 \pmod{\mathfrak{p}^2}$. Conversely, every such equation is irreducible, and a root of it generates a totally ramified extension of K of degree e.

Proposition 1.2 (II, Proposition 12 [Lan94] or Theorem 11.10 [Sut21]).
Assume that E is totally and tamely ramified over K. Then there exists an element Π of order 1 at $\mathfrak{P}$ in E with irreducible polynomial

$$X^e - \pi = 0$$

with π of order 1 at $\mathfrak{p}$ in K. Conversely, if a is an element of A, and e is a positive integer coprime to p. Then any root of an equation

$$X^e - a = 0$$

generates a tamely ramified extension of K, and this extension is totally ramified if the order of a at $\mathfrak{p}$ is relatively prime to e.

Lemma 1.3 (p. 53 [Lan94]).
Let e be a positive integer coprime to p. Let E be a finite extension of K, π_0 a prime element in $\mathfrak{p}$, and β an element of E such that $|\beta|^e = |\pi_0|$. Then there exists an element π of order 1 in $\mathfrak{p}$ such that one of the roots of the equation $X^e - \pi = 0$ is contained in $K(\beta)$.

Theorem 1.4. *Let E/K be a totally and tamely ramified extension of degree e. Then E is generated by the root of an equation*

$$X^e - \pi = 0$$

for some prime element π of $\mathfrak{p}$. Note that difference choices for the uniformizing element π can lead to different extensions, which "differ by an unramified extension".

Proof. Let $\beta = \Pi$ in the previous lemma. $\square$

Theorem 1.5 (Theorem 2.62 [Cla]).
Suppose that K is a complete DVF with algebraically closed residue field k of characteristic exponent p. Then there exists, for each positive integer e coprime to p, a unique degree e tamely ramified extension L_e/K, obtained by taking the e^{th} root of any uniformizing element of K. Moreover, we have $K^{\text{tr}} = \bigcup_e L_e$ and $\text{Gal}(K^{\text{tr}}/K) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

Proof. Since $k = \overline{k}$, one has that K contains all the roots of unity of order coprime to p, and hence $K = K^{\text{ur}}$. Therefore, all extensions of K are totally ramified, and hence any tamely ramified extension is totally and tamely ramified. The previous theorems show that every degree e tamely ramified extension L of K is of the form $K(\pi^{1/e})$ for some choice of uniformizer π of K. Conversely, for any uniformizer π of K, we have that $K(\pi^{1/e})$ is a tamely ramified extension of degree e. The uniqueness statement will follow if we can show that for any two uniformizers π and π' of K, we have that $K(\pi^{1/e}) = K(\pi'^{1/e})$.

By Kummer theory, this is the case if and only if $\langle \pi \rangle = \langle \pi' \rangle$ as subgroups of $K^\times/(K^\times)^e$. So there exists d such that $\pi^d \equiv \pi' \mod (K^\times)^e$. So $dv_{\mathfrak{p}}(\pi) \equiv v_{\mathfrak{p}}(\pi') \pmod{e}$. However, $v_{\mathfrak{p}}(\pi) = v_{\mathfrak{p}}(\pi') = 1$. So $d \equiv 1 \pmod{e}$. So $\pi \equiv \pi' \mod (K^\times)^e$. In other words, we want to show that π/π' is an e^{th} power in $K^\times$.

Since k is algebraically closed, every element of $k^\times$ is an e^{th} power. Then by Hensel's lemma, every unit in the valuation ring of K is an e^{th} power, so in particular π/π' is an e^{th} power. So we have shown that $K(\pi^{1/e}) = K(\pi'^{1/e})$.

Let $L_e := K(\pi^{1/e})$ be the unique degree e extension of K. By the basic structure of Kummer extensions, $\text{Gal}(L_e/K) \cong \langle \pi \rangle \cong \mathbb{Z}/e\mathbb{Z}$. However, this isomorphism is <u>not</u> canonical. For $e \mid e'$, one easily checks that the following diagram commutes:

$$\begin{tikzcd} \mathrm{Gal}(L_{e'}/K) \arrow[r, "\sim"] \arrow[d, two heads] & \mathbb{Z}/e'\mathbb{Z} \arrow[d, two heads] \\ \mathrm{Gal}(L_e/K) \arrow[r, "\sim"] & \mathbb{Z}/e\mathbb{Z}. \end{tikzcd}$$

Therefore, $\mathrm{Gal}(K^{\mathrm{tr}}/K) \cong \varprojlim \mathbb{Z}/e\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. $\square$

Let $F/\mathbb{Q}_p$ be a finite extension, with uniformizer ϖ. By our above discussion, for each $n \geq 1$ with $(n,p) = 1$, there is a unique extension E_n/F^{ur} of degree n, of the form

$$E_n := F^{\mathrm{ur}}(\varpi^{1/n}).$$

By Kummer theory, there is a canonical isomorphism:

$$\begin{aligned} \mathrm{Gal}(E_n/F^{\mathrm{ur}}) &\xrightarrow{\sim} \mu_n(\overline{F}) \\ \sigma &\mapsto \frac{\sigma(\varpi^{1/n})}{\varpi^{1/n}}. \end{aligned}$$

This isomorphism is independent of the choices of ϖ and $\varpi^{1/n}$. Set

$$F^{\mathrm{tr}} := \bigcup_{(n,p)=1} E_n.$$

There is the following isomorphism:

$$\mathrm{Gal}(F^{\mathrm{tr}}/F^{\mathrm{ur}}) = \varprojlim_{(n,p)=1} \mathrm{Gal}(E_n/F^{\mathrm{ur}}) = \varprojlim_{(n,p)=1} \mu_n(\overline{F}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell.$$

This last isomorphism is <u>not</u> canonical, as it relies on the choice of a compatible system of roots of unity $(\zeta_n)_{(n,p)=1}$. By compatible, we mean that if $n = md$, then $\zeta_n^d = \zeta_m$. For any integer $m \geq 1$, we can also define a projection map:

$$\mathrm{Gal}(F^{\mathrm{tr}}/F^{\mathrm{ur}}) \twoheadrightarrow \mathrm{Gal}(E_{q^m-1}/F^{\mathrm{ur}}) = \mu_{q^m-1}(\overline{F}) = [k_{F_m}^\times] \cong k_{F_m}^\times \hookrightarrow \overline{\mathbb{F}}_q^\times.$$

Here, $[-]$ denotes the Teichmüller lift. This induces another isomorphism:

$$\mathrm{Gal}(F^{\mathrm{tr}}/F^{\mathrm{ur}}) \cong \varprojlim_m k_{F_m}^\times.$$

The following diagram summarizes our discussion. Let $\Gamma_F := \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group of F, $I_F := \mathrm{Gal}(\overline{F}/F^{\mathrm{ur}})$ be the inertia subgroup of F, and $P_F := \mathrm{Gal}(\overline{F}/F^{\mathrm{tr}})$ be the wild inertia subgroup of F. Note that P_F is pro-p and quite big.

$$\begin{tikzcd} \overline{F} \arrow[d, dash, "P_F"'] \arrow[dd, bend left, dash, "I_F"] \arrow[ddd, bend right=60, dash, "\Gamma_F"'] \\ F^{\mathrm{tr}} \arrow[d, dash, "\prod_{\ell \neq p} \mathbb{Z}_\ell"'] \\ F^{\mathrm{ur}} \arrow[d, dash, "\widehat{\mathbb{Z}}"] \\ F \end{tikzcd}$$

2. Galois representations over $\overline{\mathbb{F}}_p$

2.1. 1-dimensional $\mathrm{Gal}(\overline{F}/F)$-representations.

Fix an isomorphism $\overline{k}_F \cong \overline{\mathbb{F}}_p$ and identify their subfields:

$$\mathbb{F}_{p^m} \cong \{x \in \overline{k}_F : x^{p^m} = x\}.$$

Lemma 2.1. *Any continuous character $\theta : I_F \to \overline{\mathbb{F}}_p^\times$ factors as:*

$$I_F \twoheadrightarrow I_F/P_F = \varprojlim_m k_{F_m}^\times \cong \varprojlim_m \mathbb{F}_{q^m}^\times \twoheadrightarrow \mathbb{F}_{q^{m'}}^\times \hookrightarrow \overline{\mathbb{F}}_p^\times.$$

Proof. The codomain has the discrete topology, so that $\ker\theta$ is open. We want to start by showing that $\theta(P_F)$ is finite. But this follows because P_F is a pro-p group, and $\ker\theta \cap P_F$ is open and normal in P_F, and hence $P_F/(\ker\theta \cap P_F)$ is a p-group (which is finite).

So $\theta(P_F)$ is a finite p-group in $\overline{\mathbb{F}}_p^\times$, and hence it must be trivial. Therefore, $P_F \leq \ker\theta$. This means that θ factors through the profinite group I_F/P_F. We are reduced to considering continuous maps from the profinite group I_F/P_F to the discrete group $\overline{\mathbb{F}}_p^\times$. This still has open kernel, which is then both closed and of finite index. Therefore, θ factors through a finite quotient of I_F/P_F, as claimed. □

Definition 2.2 (Serre's fundamental characters)**.** *For $n \geq 1$, define*

$$\omega_n : I_F \twoheadrightarrow I_F/P_F = \varprojlim_m k_{F_m}^\times \cong \varprojlim_m \mathbb{F}_{q^m}^\times \twoheadrightarrow \mathbb{F}_{q^n}^\times \hookrightarrow \overline{\mathbb{F}}_p^\times.$$

Proposition 2.3.
(a) If $m \mid n$, then $\omega_n^{1+q^m+q^{2m}+\cdots+q^{(n/m-1)m}} = \omega_m$.
(b) $\omega_n^{q^n-1} = \mathbb{1}$, where $\mathbb{1}$ is the trivial character.
(c) Every mod p character of I_F can be written uniquely as ω_n^r for some n and primitive r. By primitive, we mean that $0 \leq r < q^n - 1$ and r is not divisible by $(q^n-1)/(q^d-1)$ where d is a proper divisor of n.

Proof.

(a) Recall the isomorphisms:

$$\varprojlim_s \mu_{q^s-1}(\overline{F}) \cong \varprojlim_s k_{F_s}^\times \cong \varprojlim_s \overline{\mathbb{F}}_{q^s}^\times.$$

If $m \mid n$, then $q^m - 1 \mid q^n - 1$. If we let $d := \frac{q^n-1}{q^m-1} = 1 + q^m + q^{2m} + \cdots + q^{(n/m-1)m}$, then the left hand side has a natural transition map:

$$\sigma : \mu_{q^m-1}(\overline{F}) \to \mu_{q^n-1}(\overline{F})$$
$$\zeta \mapsto \zeta^d.$$

These are isomorphisms of multiplicative groups, so it follows at once that:

$$\omega_n^d = \omega_m.$$

(b) This is because ω_n has image in $\mathbb{F}_{q^n}^\times$.

(c) Let $\theta : I_F \to \overline{\mathbb{F}}_p^\times$ be a continuous character. We just saw that it factors through a finite quotient of I_F/P_F, and we can identify this quotient with the subgroup $\mathbb{F}_{q^n}^\times$ of $\overline{\mathbb{F}}_p^\times$ for some $n \geq 1$. We are then reduced to thinking about group homomorphisms $\mathbb{F}_{q^n}^\times \to \overline{\mathbb{F}}_p^\times$. Note that the inclusion $\mathbb{F}_{q^n}^\times \subset \overline{\mathbb{F}}_p^\times$ corresponds to the map ω_n.

Note that a group homomorphism $\mathbb{F}_{q^n}^\times \to \overline{\mathbb{F}}_p^\times$ must have image inside the copy of $\mathbb{F}_{q^n}^\times$. So we are reduced again to thinking about group endomorphisms $\mathbb{F}_{q^n}^\times \to \mathbb{F}_{q^n}^\times$. As $\mathbb{F}_{q^n}^\times$ is cyclic, we can let $g \in \mathbb{F}_{q^n}^\times$ be a generator. Then a map $\mathbb{F}_{q^n}^\times \to \overline{\mathbb{F}}_p^\times$ is determined by the image of g. The map sending g to g^r corresponds to ω_n^r. These are all the possible maps since the codomain $\mathbb{F}_{q^n}^\times$ is generated by g as well.

We have just shown that $\theta = \omega_n^r$ for some n, r. By part (b), we can choose r to be in the range $0 \leq r < q^n - 1$ without changing the character. If r is divisible by a quotient of the form $(q^n - 1)/(q^d - 1)$, then by part (a), $\omega_n^r = \omega_{n'}^{r'}$ for some $n' \mid n$. □

Lemma 2.4. *Let φ be a lift of the Frobenius in $\mathrm{Gal}(\overline{k}_F/k_F)$ to $\mathrm{Gal}(F^{\mathrm{tr}}/F)$ and τ be an element of the subgroup $\mathrm{Gal}(F^{\mathrm{tr}}/F^{\mathrm{ur}})$, then $\varphi\tau\varphi^{-1} = \tau^q$.*

Proof. Since $F^{\mathrm{tr}} = \bigcup_{m \geq 1} F^{\mathrm{ur}}(\varpi^{1/(q^m-1)})$ and we know that $\varphi\tau\varphi^{-1}$ fixes F^{ur}, it suffices to calculate $\varphi\tau\varphi^{-1}(\varpi^{1/(q^m-1)})$ for all $m \geq 1$.

Fix $m \geq 1$. Let $\omega := \varpi^{1/(q^m-1)}$ and $\zeta := \zeta_{q^m-1}$ be a primitive $(q^m-1)^{\mathrm{st}}$ root of unity.

$$\begin{aligned} \varphi(\zeta) &= \zeta^q & \tau(\zeta) &= \zeta \\ \varphi(\omega) &= \zeta^s\omega & \tau(\omega) &= \zeta^t\omega \end{aligned}$$

Note that the action on ω has this form because the automorphisms of $\mathrm{Gal}(F^{\mathrm{tr}}/F)$ act on the roots of the irreducible polynomial $X^{q^m-1} - \varpi$ in $F[X]$. Compute

$$\varphi\tau\varphi^{-1}(\omega) = \varphi\tau(\zeta^{-s/q}\omega) = \varphi(\zeta^{-s/q}\zeta^t\omega) = \zeta^{-s}\zeta^{tq}\zeta^s\omega = \zeta^{tq}\omega.$$

On the other hand, $\tau^q(\omega) = \zeta^{tq}\omega$. This completes the proof. □

Lemma 2.5. *The inertial character $\omega_n : I_F \to \overline{\mathbb{F}}_p^\times$ can be extended (non-uniquely) to a character of Γ_F if and only if $n = 1$.*

Proof. Suppose ω_n extends to Γ_F. Let $\varphi \in \Gamma_F$ be a lift of Frobenius, and $\tau \in I_F$. Then

$$\begin{aligned} \omega_n(\tau) &= \omega_n(\varphi)\omega_n(\tau)\omega_n(\varphi^{-1}) \\ &= \omega_n(\varphi\tau\varphi^{-1}) \\ &= \omega_n(\tau)^q && (\omega_n \text{ factors through } P_F) \end{aligned}$$

Therefore, ω_n has image inside $\mathbb{F}_q^\times$. This implies $\mathbb{F}_{q^n}^\times \subset \mathbb{F}_q^\times$. Therefore, $n = 1$.

On the other hand, suppose $n = 1$. Set $\omega_1(\varphi) := 1$. Every $\gamma \in \Gamma_F$ can be written as a product $\gamma = \tau\varphi^d$ for some $\tau \in I_F$ and $d \in \mathbb{Z}$. We set $\omega_1(\gamma) := \omega_1(\tau)\omega_1(\varphi)^d = \omega_1(\tau)$.

To show ω_1 is well-defined, suppose $\tau\varphi^d = \tau'\varphi^e$. Then $1 = \tau^{-1}\tau'\varphi^{e-d}$. This cannot happen unless $d = e$, in which case also $\tau = \tau'$.

To show ω_1 is a homomorphism, we compute:

$$\begin{aligned}
\omega_1(\tau\varphi^d\tau'\varphi^e) &= \omega_1(\tau\varphi^d\tau'\varphi^{-d}\varphi^{d+e}) \\
&= \omega_1(\tau\varphi^d\tau'\varphi^{-d}) && (\text{since } \varphi^d\tau'\varphi^{-d} \in I_F) \\
&= \omega_1(\tau(\tau')^{q^d}) && (\text{since } \omega_1(P_F) = 1) \\
&= \omega_1(\tau)\omega_1(\tau')^{q^d} \\
&= \omega_1(\tau)\omega_1(\tau') && (\text{since } \omega_1(I_F) \subset \mathbb{F}_q^\times) \\
&= \omega_1(\tau\varphi^d)\omega_1(\tau'\varphi^e).
\end{aligned}$$

□

Corollary 2.6. *Fix a lift of Frobenius $\varphi \in \Gamma_F$. Extend ω_1 to Γ_F by the condition that $\omega_1(\varphi) = 1$. Then any continuous character $\chi : \Gamma_F \to \overline{\mathbb{F}}_p^\times$ is of the form:*

$$\chi = \omega_1^r \cdot \mu_\lambda$$

for $0 \leq r < q-1$ and where $\mu_\lambda : \Gamma_F \twoheadrightarrow \Gamma_F/I_F \to \overline{\mathbb{F}}_p^\times$ sends φ to some $\lambda \in \overline{\mathbb{F}}_p^\times$.

Remark 2.7. *The condition "continuous" is the same as "smooth" mod p.*

2.2. n-dimensional $\mathrm{Gal}(\overline{F}/F)$-representations.

Lemma 2.8 (p-groups lemma)**.**
Let C be a field of characteristic $p > 0$, and $|G| = p^k$ for some $k \geq 1$. Let V be a C-vector space, equipped with a representation of G. Then $V^G \neq 0$.

Proof. We forget the C-vector space structure on V, and view it as a $\mathbb{F}_p$-vector space. We may also replace V by the $\mathbb{F}_p$-span of $\{gv\}_{g\in G}$ for any $v \in V$, $v \neq 0$. Then V is finite-dimensional over $\mathbb{F}_p$, as G is finite.

Now we have $\pi : G \to \mathrm{GL}_d(\mathbb{F}_p)$ for some d, and the image of π is contained in a Sylow p-subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$, all of which are conjugate to:

$$\begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

So after conjugating, $\operatorname{im}\pi$ fixes the first basis vector. □

Lemma 2.9 (pro-p-groups lemma)**.**
Let C be a field of characteristic $p > 0$, and G be a pro-p group. Let (π, V) be a smooth non-zero G-representation on a C-vector space. Then $V^G \neq 0$.

Proof. Replacing V by the C-span of $\{gv\}_{g\in G}$ for any $v \in V$, $v \neq 0$, we can assume that there is some v that generates V. Since $\mathrm{Stab}_G(v)$ is an open subgroup of G, there is an open normal subgroup $H \trianglelefteq G$ such that $H \leq \mathrm{Stab}_G(v)$. Then

$$V = \mathrm{span}_C\{gv : g \in G\} = \mathrm{span}_C\{gv : [g] \in G/H\}.$$

So the (finite) p-group G/H acts on V. The result follows from the p-groups lemma. □

Proposition 2.10. *Let $\rho : \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ be a continuous irreducible representation. Then*

$$\rho|_{I_F} = \bigoplus_{i=1}^{n} \omega_{m_i}^{r_i}$$

for some integers $m_i \geq 1$ and some $0 \leq r_i < q^{m_i} - 1$.

Proof. Let $V := V_\rho$. Since P_F is pro-p, and ρ is smooth, the pro-p-groups lemma tells us that $V^{P_F} \neq 0$. Since $P_F \trianglelefteq \Gamma_F$, V^{P_F} is Γ_F-stable. Since V is irreducible, $V^{P_F} = V$ as representations of Γ_F. Therefore, ρ factors through Γ_F/P_F.

Now consider the restriction $\rho|_{I_F} : I_F \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Since ρ is trivial on P_F, we have:

$$\rho|_{I_F} : I_F \twoheadrightarrow I_F/P_F \to \mathrm{GL}_n(\overline{\mathbb{F}}_p).$$

The group I_F/P_F is profinite, as it is a product of profinite groups. Since $\rho|_{I_F}$ is continuous, $\ker\rho$ is an open normal subgroup of I_F/P_F, which furthermore implies that $\ker\rho$ is closed and finite index in I_F/P_F. Thus $\rho|_{I_F}$ factors through a finite quotient H of I_F/P_F, and by the explicit description of I_F/P_F, we know that the order of H is coprime to p.

So Maschke's theorem for finite groups tells us that $\rho|_{I_F}$ is semisimple, and since I_F/P_F is abelian, Schur's lemma tells us that the irreducible constituents of $\rho|_{I_F}$ are one-dimensional. We conclude that $\rho|_{I_F}$ is a sum of characters. We classified all such characters earlier. $\square$

Proposition 2.11. *Let $\Gamma_{F_n} := \langle I_F, \varphi^n \rangle$.*

(i) The element φ^{-1} acts transitively (by an n-cycle) on the eigenspaces of $\rho|_{I_F}$. So φ^{-n} preserves the eigenspace decomposition of $\rho|_{I_F}$. This forces all of the $m_i \mid n$ (and so in particular we can choose $m_i = n$) from the previous proposition. This also tells us that φ^n acts by a scalar on each of the eigenspaces.

(ii) In general, if $m \mid n$, then the inertial character $\omega_m : I_F \to \overline{\mathbb{F}}_p^\times$ can be extended to a character on Γ_{F_n} by imposing that $\omega_m(\varphi^n) = 1$.

(iii) There exists a single $\lambda \in \overline{\mathbb{F}}_p^\times$ and a character $\kappa_\lambda : \Gamma_{F_n} \to \overline{\mathbb{F}}_p^\times$ which is trivial on I_F and for which $\kappa_\lambda(\varphi^n) = \lambda$ such that

$$\rho|_{\Gamma_{F_n}} = \bigoplus_{i=1}^{n} \omega_n^{rq^{i-1}} \kappa_\lambda.$$

Proof.

(i) Let v be in the $\omega_{m_i}^{r_i}$-isotypic component of V, and $\tau \in I_F$. Since $\varphi\tau\varphi^{-1} = \tau^q$ in I_F/P_F:

$$\tau\varphi^{-1}v = \varphi^{-1}\tau^q v = \omega_{m_i}^{r_i}(\tau)^q \varphi^{-1}v.$$

So $\varphi^{-1}v$ is in the $\omega_{m_i}^{qr_i}$-isotypic component of V, and it is in particular an eigenvector for the representation $\rho|_{I_F}$. To make things easy, let us assume for simplicity that all of the characters $\omega_{m_i}^{r_i}$ are distinct. The irreducibility of ρ implies that for all j there exists k such that $\varphi^{-k}v$ is $\omega_{m_j}^{r_j}$-isotypic. So the action of $\varphi^{\mathbb{Z}}$ on v is transitive, in the sense that the action sends v to every possible eigenspace of $\rho|_{I_F}$. So φ must act on the eigenspaces via an n-cycle, and $\varphi^{-n}v$ lands back into the $\omega_{m_i}^{r_i}$-isotypic component. Since this is true for all i, φ^{-n} respects the eigenspace decomposition of $\rho|_{I_F}$. Since $\varphi^{-n}v$ is $\omega_{m_i}^{r_i}$-isotypic, one has $\tau\varphi^{-n}v = \omega_{m_i}^{r_i}(\tau)\varphi^{-n}v$ for $\tau \in I_F$. But also:

$$\tau\varphi^{-n}v = \varphi^{-n}\tau^{q^n}v = \omega_{m_i}^{r_i}(\tau)^{q^n}\varphi^{-1}v.$$

So $\omega_{m_i}^{r_i} = \omega_{m_i}^{r_i q^n}$. This implies $m_i \mid n$, so we can in particular choose $m_i = n$. So far everything we did works for an arbitrary i. Now let $m := m_1$ and $r := r_1$, and note that we can let $m_1 = n$ as just discussed. To reach any isotypic component, we just have to push the ω_n^r-isotypic component around by φ^{-1}. So this leads us to conclude:

$$\rho|_{I_F} = \bigoplus_{i=1}^{n} \omega_n^{rq^{i-1}}.$$

(ii) We just need to extend ω_n. If we can do that, then the extension of ω_m is an easy consequence of the formula generating ω_m from ω_n as characters of I_F.

One needs to check that the extension of ω_n is well-defined and that it satisfies the homomorphism property. The latter crucially depends on the fact that ω_n and φ^n have the same n. We give a partial calculation. Let $\tau, \tau' \in I_F$. Then

$$\omega_n(\tau\varphi^n\tau'\varphi^{-n}) = \omega_n(\tau\tau'^{q^n}) = \omega_n(\tau)\omega_n(\tau')^{q^n} = \omega_n(\tau)\omega_n(\tau').$$

(iii) We know that φ^n preserves the eigenspaces of $\rho|_{I_F}$. It suffices to check that φ^n acts by the same scalar in each eigenspace. Suppose φ^n acts on the ω_m^r-isotypic component by the scalar λ, and acts on the $\omega_{m'}^{r'}$-isotypic component by the scalar μ. Let v be ω_m^r-isotypic. There exists j such that φ^{-j} is $\omega_{m'}^{r'}$-isotypic. Then

$$\mu\varphi^{-j}v = \varphi^n\varphi^{-j}v = \varphi^{-j}\varphi^n v = \lambda\varphi^{-j}v.$$

So $\mu = \lambda$. The semisimple decomposition of $\rho|_{\Gamma_{F_n}}$ follows easily.

□

Corollary 2.12. *Let $\rho : \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ be a continuous irreducible representation. Then ρ is isomorphic, for some $0 \le r < q^n - 1$ and $\lambda \in \overline{\mathbb{F}}_p^\times$, to the induction*

$$\mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F} \omega_n^r \kappa_\lambda.$$

Moreover, the only non-trivial isomorphisms are, for some $j \in \mathbb{Z}$, of the form

$$\mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F} \omega_n^r \kappa_\lambda \cong \mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F} \omega_n^{rq^j} \kappa_\lambda.$$

Remark 2.13. *The converse is not true. Not all of these inductions are irreducible!*

3. MOD p LOCAL LANGLANDS CORRESPONDENCE FOR $\mathrm{GL}_2(\mathbb{Q}_p)$

Let us recall some facts from the complex representation theory of finite groups, which continue to be true in our setting, even though our groups are not finite.

Proposition 3.1 (Irreducibility of induction from normal subgroup)**.**
Let G be a finite group, and $H \trianglelefteq G$ be a normal subgroup. Let ρ be an irreducible complex representation of H. Then $\mathrm{Ind}_H^G \rho$ is irreducible if and only if $\rho \ncong \rho^b$ for all $b \notin H$. Here,

$$\rho^b(g) := \rho(bgb^{-1}).$$

Proof. Let χ be the character of ρ. Then check the right hand side is equivalent to:

$$\langle \chi, \mathrm{Res}_H^G \mathrm{Ind}_H^G \chi \rangle_H = \langle \mathrm{Ind}_H^G \chi, \mathrm{Ind}_H^G \chi \rangle_G = 1.$$

□

Proposition 3.2 (Push-pull formula)**.**
Let G be a finite group, and $H \leq G$ be a subgroup. Let ρ and σ be finite-dimensional complex representations of H and G, respectively. Then,

$$\mathrm{Ind}_H^G(\rho \otimes \sigma|_H) \cong \mathrm{Ind}_H^G(\rho) \otimes \sigma.$$

The first thing we can do is pull out the κ_λ from the induction formula. Let $\lambda_0 \in \overline{\mathbb{F}}_p^\times$ be any root of $X^n - \lambda$, and define a character $\mu_{\lambda_0} : \Gamma_F \to \overline{\mathbb{F}}_p^\times$ which is trivial on I_F and for which $\mu_{\lambda_0}(\varphi) = \lambda_0$. Then $\mu_{\lambda_0}|_{\Gamma_{F_n}} = \kappa_\lambda$, so that

$$\mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F}(\omega_n^r \kappa_\lambda) \cong \mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F}(\omega_n^r) \otimes \mu_{\lambda_0}.$$

So moving forward, we will set $\lambda = 1$ so that κ_λ is trivial. But we will compensate for this by allowing twists by smooth characters. In other words, we want to try and understand irreducible representations of the form

$$\mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F}(\omega_n^r) \otimes \chi$$

for an arbitrary smooth character $\chi : \Gamma_F \to \overline{\mathbb{F}}_p^\times$. Clearly, the irreducibility of this induction does not depend on twisting by characters, so we are reduced to understanding

$$\mathrm{Ind}_{\Gamma_{F_n}}^{\Gamma_F}(\omega_n^r).$$

From this point onward, let us fix $n = 2$ and $F = \mathbb{Q}_p$, so that we restrict our attention to just the 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, with the goal of stating the mod p local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$.

Proposition 3.3. *Let $\mathbb{Q}_{p^2}/\mathbb{Q}_p$ denote the unique unramified extension of degree 2. Then for every $0 \leq r < p^2 - 1$, we defined an induced representation*

$$\mathrm{Ind}_{\Gamma_{\mathbb{Q}_{p^2}}}^{\Gamma_{\mathbb{Q}_p}}(\omega_2^r).$$

This is reducible if and only if $(p+1) \mid r$.

Proof. We want to find the values of r for which:

$$\omega_2^r(\tau)^p = \omega_2^r(\varphi\tau\varphi^{-1}) =: (\omega_2^r)^\varphi(\tau) = \omega_2^r(\tau).$$

This is true if and only if $\omega_2^{r(p-1)} = \mathbb{1}$. So $r(p-1) \equiv 0 \pmod{p^2-1}$, and hence

$$r \equiv 0 \pmod{p+1}.$$ ☐

Proposition 3.4. *Let $r \geq p+1$. Recall the formula $\omega := \omega_1 = \omega_2^{p+1}$ and the fact that ω can be extended to a character of $\Gamma_{\mathbb{Q}_p}$. This implies*

$$\mathrm{Ind}_{\Gamma_{\mathbb{Q}_{p^2}}}^{\Gamma_{\mathbb{Q}_p}}(\omega_2^r) = \mathrm{Ind}_{\Gamma_{\mathbb{Q}_{p^2}}}^{\Gamma_{\mathbb{Q}_p}}(\omega_2^{r-p-1}\omega) = \mathrm{Ind}_{\Gamma_{\mathbb{Q}_{p^2}}}^{\Gamma_{\mathbb{Q}_p}}(\omega_2^{r-p-1}) \otimes \omega.$$

Proof. Use the push-pull formula. ☐

Corollary 3.5. *Let $\rho : \Gamma_{\mathbb{Q}_p} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be a continuous irreducible representation. Then there exists a smooth character $\chi : \Gamma_{\mathbb{Q}_p} \to \overline{\mathbb{F}}_p^\times$ and $r \in \{0, \ldots, p-1\}$ such that*

$$\rho \cong \rho(r, \chi) := \mathrm{Ind}_{\Gamma_{\mathbb{Q}_{p^2}}}^{\Gamma_{\mathbb{Q}_p}}(\omega_2^{r+1}) \otimes \chi.$$

The only non-trivial intertwiners between these representations are

$$\rho(r, \chi) \cong \rho(r, \chi\mu_{-1}) \cong \rho(p-1-r, \chi\omega^r) \cong \rho(p-1-r, \chi\omega^r\mu_{-1}).$$

Let $G := \mathrm{GL}_2(\mathbb{Q}_p)$, $K := \mathrm{GL}_2(\mathbb{Z}_p)$, $B := \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ be the standard upper triangular Borel subgroup of G, and $Z \cong \mathbb{Q}_p^\times$ be the centre of G. Recall the classification of irreducible smooth admissible mod p representations of $G := \mathrm{GL}_2(\mathbb{Q}_p)$.

Definition 3.6. *Given $0 \le r < p-1$, $\lambda \in \overline{\mathbb{F}}_p$, and a smooth character $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$, let*

$$\pi(r, \lambda, \chi) := \frac{\text{c-Ind}_{KZ}^G(\mathrm{Sym}^r\, \overline{\mathbb{F}}_p^2)}{(T_p - \lambda)} \otimes (\chi \circ \det).$$

Theorem 3.7. *Let $\lambda \in \overline{\mathbb{F}}_p$, $r \in \{0, \dots, p-1\}$, and $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ be a smooth character.*

(i) $\pi(r, \lambda, \chi)$ is smooth and admissible, with central character $\omega^r \chi^2$.
(ii) $\pi(r, \lambda, \chi)$ is irreducible, unless $(r, \lambda) \in \{(0, \pm 1), (p-1, \pm 1)\}$.
(iii) For $(r, \lambda) \in \{(0, \pm 1), (p-1, \pm 1)\}$, there are composition series

$$0 \longrightarrow \mathrm{St} \otimes (\chi\mu_\lambda \circ \det) \longrightarrow \pi(0, \lambda, \chi) \longrightarrow \chi\mu_\lambda \circ \det \longrightarrow 0$$

$$0 \longrightarrow \chi\mu_\lambda \circ \det \longrightarrow \pi(p-1, \lambda, \chi) \longrightarrow \mathrm{St} \otimes (\chi\mu_\lambda \circ \det) \longrightarrow 0$$

(iv) These are all of the irreducible smooth admissible representations of $\mathrm{GL}_2(\mathbb{Q}_p)$ over $\overline{\mathbb{F}}_p$.

Definition 3.8. *Let $\lambda = 0$, $r \in \{0, \dots p-1\}$, and $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ a smooth character. Then representations of the form $\pi(r, 0, \chi)$ are called supersingular.*

Proposition 3.9.

(i) For $\lambda \neq 0$, $r \in \{0, \dots, p-1\}$, and $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$,

$$\pi(r, \lambda, \chi)^{\mathrm{ss}} \cong \mathrm{Ind}_B^G(\chi\mu_{1/\lambda}, \chi\mu_\lambda\omega^r)^{\mathrm{ss}}.$$

(ii) For $\lambda = 0$, $r \in \{0, \dots, p-1\}$, and $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$,

$$\pi(r, 0, \chi) \cong \pi(r, 0, \chi\mu_{-1}) \cong \pi(p-1-r, 0, \chi\omega^r) \cong \pi(p-1-r, 0, \chi\omega^r\mu_{-1}).$$

Theorem 3.10 (The semi-simple mod p local Langlands correspondence)**.**

Let χ and $\omega := \omega_1$ be smooth characters $\Gamma_{\mathbb{Q}_p} \to \overline{\mathbb{F}}_p^\times$, which can also be viewed as smooth characters $\mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ via local class field theory. Then

(i) For $r \in \{0, \dots, p-1\}$:

$$\rho(r, \chi) \longleftrightarrow \pi(r, 0, \chi).$$

(ii) For $r \in \{0, \dots, p-2\}$ and $\lambda \in \overline{\mathbb{F}}_p^\times$:

$$(\omega^{r+1}\mu_\lambda \oplus \mu_{1/\lambda}) \otimes \chi \longleftrightarrow \pi(r, \lambda, \chi)^{\mathrm{ss}} \oplus \pi(p-3-r, 1/\lambda, \omega^{r+1}\chi)^{\mathrm{ss}}.$$

Remark 3.11. *The objects on the Galois side have determinant $\omega^{r+1}\chi^2$, and the objects on the automorphic side have central character $\omega^r\chi^2$.*

References

[Cla] Pete L. Clark. Algebraic number theory II: valuations, local fields and adeles. URL: `http://alpha.math.uga.edu/~pete/8410FULL.pdf`. Last visited on 2024/01/24.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Sut21] Andrew V. Sutherland. Lecture 11: Totally ramified extensions and Krasner's lemma, 2021. URL: `https://math.mit.edu/classes/18.785/2021fa/LectureNotes11.pdf`. Last edited on 2021/10/18. Last visited on 2024/01/24.