Abstract. Let \( p \) be a prime, \( k \) a finite extension of \( \mathbb{F}_p \) of cardinal \( q \), \( l \) a finite extension of \( k \) of group \( \Sigma = \text{Gal}(l|k) \), and \( T \) a subgroup of \( l^\times \). Using the method of "little groups", we classify irreducible \( \mathbf{F}_p \)-representations of the group \( G = T \times_q \Sigma \), the twisted product of \( \Sigma \) with the \( \Sigma \)-module \( T \). We then use these results to classify irreducible continuous \( \mathbf{F}_p \)-representations of the profinite group \( \text{Gal}(\bar{K}|K) \) of \( K \)-automorphisms of the maximal galoisian extension \( \bar{K} \) of a \( p \)-field \( K \) with residue field \( k \).

1. Introduction

(1) Let \( p \) be a prime and let \( K \) be a \( p \)-field, namely a local field with finite residue field of characteristic \( p \). Let \( \bar{K} \) be a maximal galoisian extension of \( K \). Let \( V \) be the maximal tamely ramified extension of \( K \) in \( \bar{K} \). All representations of the profinite groups \( \text{Gal}(\bar{K}|K) \) and \( \text{Gal}(V|K) \) appearing below are assumed to be continuous. The ramification group \( \text{Gal}(\bar{K}|V) \), which is a pro-\( p \)-group, acts trivially on any irreducible \( \mathbf{F}_p \)-representation of \( \text{Gal}(\bar{K}|K) \). So classifying irreducible \( \mathbf{F}_p \)-representations of \( \text{Gal}(\bar{K}|K) \) comes down to classifying irreducible \( \mathbf{F}_p \)-representations of \( \text{Gal}(V|K) \), which comes down to classifying irreducible \( \mathbf{F}_p \)-representations of \( \text{Gal}(L|K) \) for every finite tamely ramified galoisian extensions \( L \) of \( K \).

(2) For such \( L \) with group of \( K \)-automorphisms \( G = \text{Gal}(L|K) \) and inertia subgroup \( G_0 \), the projection \( G \to G/G_0 \) need not have a section, but \( L \) has finite unramified extensions \( L' \) for which the corresponding projections \( G' \to G'/G_0' \) (where \( G' \) is \( \text{Gal}(L'|K) \) and \( G_0' \) is its inertia subgroup) do have sections; the smallest such \( L' \) is the one whose degree over \( L \) is equal to the order in \( H^2(\text{Gal}(L'/K), G_0') \) of the class of the extension \( G \) of \( G/G_0 \) by the \( (G/G_0) \)-module \( G_0 \); see for example [3, Lemma 2.3.4]. So it is enough to understand irreducible \( \mathbf{F}_p \)-representations of \( G \) in this

\textit{MSC2010} : Primary 11F80, 11S99, 20C20

\textit{Keywords} : Local fields, Galois representations, Little groups
split case; with a heavy heart, we choose a section of $G \to G/G_0$ in what follows.

(3) Our treatment, which is completely canonical and somewhat simpler than in the literature, is better adapted to this arithmetic application because the inertia group $G_0$ does not come with a generator, only a canonical character $\theta: G_0 \to l^\times$, where $l$ is the residue field of $L$. It is based upon §7 of [9, p. 205] and the method of “little groups” of Wigner and Mackey as exposed in §8.2 of [11, p. 62]; I thank my friend UK Anandavardhanan for pointing out the latter reference. The material is also worked out in §4.1 of [7, p. 329].

(4) Let $k$ be the residue field of $K$; the quotient $\Sigma = G/G_0$ can be identified with $\text{Gal}(l|k)$, which has the canonical generator $\sigma: x \mapsto x^q$ ($x \in l$), where $q = \text{Card} k$. The conjugation action of $\Sigma$ on $G_0$ is given by $\sigma.t = t^q$ for every $t \in G_0$; the character $\theta$ is $\Sigma$-equivariant. To determine the $F_p$-representations of $G$, we may forget the fields $K$ and $L$, and retain only $p$, $k$, $l$, and $e = \text{Card} G_0$. This is done in §2. In §3, we return to these local fields and make an observation which will be useful elsewhere [5].

2. Irreducible $F_p$-representations of little groups

(5) Notation. Let us restart and rename. Fix a prime number $p$, fix a finite extension $k$ of $F_p$, put $q = \text{Card} k$, fix a finite extension $l$ of $k$, put $f = [l : k]$, and denote by $\sigma: x \mapsto x^q$ ($x \in l$) the canonical generator of $\Sigma = \text{Gal}(l|k)$. Let $T \subset l^\times$ be a subgroup, let $e$ be the order of $T$ (so that $q^f \equiv 1 \pmod{e}$), and let $\theta: T \to l^\times$ be the inclusion (viewed as a character). Finally, let $G = T \times q \Sigma$ be the twisted product of $\Sigma$ with the $\Sigma$-module $T$ (for the galoisian action $\sigma.t = \sigma t \sigma^{-1} = t^q$ ($t \in T$)). Notice that the action is trivial, or equivalently $G$ is commutative, if and only if $q \equiv 1 \pmod{e}$.

(6) The problem. Classify irreducible $F_p$-representations of $G$.

(7) Notation. For every character $\chi: T \to l^\times$, we denote by $d_\chi$ the order of $\chi$ and by $r_\chi$ (resp. $s_\chi$) the order of the image $\bar{p}$ (resp. $\bar{q}$) in $(\mathbb{Z}/d_\chi\mathbb{Z})^\times$. Put $T_\chi = T/\text{Ker}(\chi)$ and let $\Sigma_\chi$ be the kernel of the action of $\Sigma$ on $T_\chi$; the group $\Sigma_\chi$ is generated by $\sigma^{s_\chi}$, and $s_\chi$ is also the size of the $\Sigma$-orbit $\bar{\chi}$ of $\chi$. We have the subgroup $G_\chi = T \times q \Sigma_\chi$ of $G$ and the quotient $\bar{G}_\chi = T_\chi \times \Sigma_\chi$ of $G_\chi$ which is commutative by construction. The numbers $d_\chi$, $r_\chi$, $s_\chi$, the groups $\Sigma_\chi$, $G_\chi$, $\bar{G}_\chi$, and some characters of these groups to be defined presently, depend only on the $\Sigma$-orbit $\bar{\chi}$ of $\chi$; we keep the notation light by writing $\chi$ in the subscript instead of $\bar{\chi}$. Let $\chi$ also stand for the faithful character $T_\chi \to l^\times$ coming from $\chi$. 

2
(8) We begin by determining the irreducible $\bar{l}$-representations of $G$, where $\bar{l} = l(\sqrt{t}), f' = fp^{-v_p(f)}$, and $v_p(f)$ is the exponent of $p$ in the prime decomposition of $f$; they will turn out to be absolutely irreducible. These representations will be parametrised by pairs $(\bar{\chi}, \lambda)$, where $\bar{\chi} \subset \text{Hom}(T, l^\times)$ is the $\Sigma$-orbit of a character $\chi: T \to l^\times$ (for the action $\sigma: \chi \mapsto \chi^q$) and $\lambda \in \bar{l}^\times$ is an element of order dividing $fs_\chi^{-1}$. This is achieved in several steps.

(9) The $\bar{l}$-representation $\rho_{\bar{\chi}, \lambda}$ of $G$ associated to a pair $(\bar{\chi}, \lambda)$. Choose $\chi \in \bar{\chi}$, and let $\psi_{\chi, \lambda}: \Sigma_\chi \to \bar{l}^\times$ be the unique character such that $\psi_{\chi, \lambda}(\sigma^{s_\chi}) = \lambda$. View the character $\chi \otimes \psi_{\chi, \lambda}$ of $G_\chi = T \times_{q} \Sigma_\chi$ as a character of $G_\chi = T \times_{q} \Sigma_\chi$, and take the induced representation $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$.

(10) To see that $\rho = \rho_{\bar{\chi}, \lambda}$ depends only on the pair $(\bar{\chi}, \lambda)$, and for later use, let us make all this explicit. The quotient $G/G_\chi$ is generated by the image of $\sigma$, so it can be identified with $Z/s_\chi Z$. By definition, the space $\text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$ has an $\bar{l}$-basis $(b_i)_{i \in Z/s_\chi Z}$ on which the action of $G_\chi$ is given by

$$\rho(t)(b_i) = \chi(\sigma^i, t)b_i = \chi^q(t)b_i \quad (t \in T, \ i \in Z/s_\chi Z),$$

and $\rho(\sigma^{s_\chi})(b_i) = \lambda b_i$. This action is extended to $G$ by $\rho(\sigma)(b_i) = b_{i+1}$ for $i \neq -1$ (mod. $s_\chi$) and $\rho(\sigma)(b_{-1}) = \lambda b_0$, which gives back, as it should, the action of $\sigma^{s_\chi}$. Now it is clear that $\rho_{\bar{\chi}, \lambda}$ depends only on $(\bar{\chi}, \lambda)$.

(11) The $\bar{l}$-representation $\rho_{\bar{\chi}, \lambda}$ is absolutely irreducible and determines the pair $(\bar{\chi}, \lambda)$. Write $\rho = \rho_{\bar{\chi}, \lambda}$. None of the $T$-stable lines in $\rho$ (the $s_\chi$ lines on which $T$ acts respectively via the characters $\chi^{q^i}$, which are distinct for distinct $i \in Z/s_\chi Z$) is stable under $\sigma$ unless $s_\chi = 1$, in which case $G_\chi = G$ and $\rho = \chi \otimes \psi_{\chi, \lambda}$, so $\rho$ is irreducible in every case, and in fact absolutely irreducible because the same argument works over any finite extension of $\bar{l}$. Note that the $\Sigma$-orbit $\bar{\chi}$ can be recovered from $\rho$ because $\rho|_T = \bigoplus_{\eta \in \bar{\chi}} \eta$, and then $\lambda \in \bar{l}^\times$ can be recovered because $\rho(\sigma^{s_\chi})$ is the homothety of ratio $\lambda$.

(12) Every irreducible $\bar{F}_p$-representations $\rho$ of $G$ come from a pair $(\bar{\chi}, \lambda)$ as in (8). Here $\bar{F}_p$ is a maximal galoisian extension of $\bar{l}$. Let $\bar{T} = T/\text{Ker}(\rho|_T)$, so that $\rho$ comes from an (irreducible) $\bar{F}_p$-representation $\bar{\rho}$ of $\bar{G} = \bar{T} \times_{\bar{q}} \Sigma$ whose restriction to $\bar{T}$ is faithful. Let $P$ be the intersection of the Sylow $p$-subgroups of $\bar{G}$. The image $\rho(P)$ is trivial because $P$ is a normal $p$-subgroup of $\bar{G}$, the characteristic of $\bar{l}$ is $p$, and $\bar{\rho}$ is irreducible [11, Chapitre 8, Proposition 26]. So $\bar{\rho}$ comes from a representation $\bar{\rho}$ of $G/P$. Let $\Sigma'$ denote the kernel of the action of $\Sigma$ on $\bar{T}$, so that the subgroup $\bar{G}' = \bar{T} \times \Sigma'$ of $\bar{G}$ is commutative. As $G' \cap P$ is the Sylow $p$-subgroup of $\Sigma'$,
the order of $\hat{\rho}(G')$ divides the order of $\tilde{l}^\times$, by our definition of $\tilde{l}$. It follows that $\hat{\rho}|_{G'}$ is a direct sum of characters $G' \to \tilde{l}^\times$ such that the restriction to $T$ of at least one of which — call it $\xi$ — is faithful.

(13) View $\chi = \xi|_T$ as a character of $T$. Since the order $e$ of $T$ divides the order $q^l - 1$ of $l^\times$, we have $\chi(T) \subset l^\times$. Also, $\text{Ker}(\chi) = \text{Ker}(\rho|_T)$, so that $G' = G_\chi = T_\chi \times \Sigma_\chi$, in the previous notation. Recall that $s_\chi$ is the size of the $\Sigma$-orbit $\bar{\chi}$, and that $\Sigma_\chi$ is generated by $\sigma^{s_\chi}$. Let $b_0 \neq 0$ be a vector (in the representation space of $\rho$) on which $G_\chi$ acts through $\xi$, and define $\lambda \in \tilde{l}^\times$ by $\xi(\sigma^{s_\chi})(b_0) = \lambda b_0$. We claim that $\rho = \rho_{\bar{\chi}, \lambda}$.

(14) Put $b_i = \rho(\sigma^i)(b_0)$ for $i \in [0, s_\chi[$. Note that $\rho(\sigma)(b_{s_\chi-1}) = \lambda b_0$ and

$$
\rho(t)(b_i) = \rho(t \sigma^i)(b_0) = \rho(\sigma^i t^{q^l i})(b_0) = \chi^{q^l}(t)b_i \quad (t \in T, i \in [0, s_\chi[).
$$

The characters $\chi^{q^l}$ are distinct for distinct $i \in [0, s_\chi[$, therefore the family $(b_i)_{i \in [0, s_\chi[}$ is linearly independent. Also, the subspace generated by the $b_i$ is $G$-stable, and in fact equal to $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$ as described earlier. Since $\rho$ is irreducible, we must have $\rho = \rho_{\bar{\chi}, \lambda}$, as claimed. Therefore:

(15) The set of irreducible $\tilde{l}$-representations of $G = T \times_q \Sigma$ is in natural bijection with the set of pairs $(\bar{\chi}, \lambda)$ consisting of the $\Sigma$-orbit $\bar{\chi}$ of a character $\chi : T \to l^\times$ and an element $\lambda \in \tilde{l}^\times$ of order dividing $f_{s_\chi-1}$, where $s_\chi = \text{Card} \bar{\chi}$. The pair $(\bar{\chi}, \lambda)$ gives rise to the induced representation $\rho_{\bar{\chi}, \lambda} = \text{Ind}_{G_\chi}^G(\chi \otimes \psi_{\chi, \lambda})$, where $G_\chi = T \times_q \Sigma_\chi$, $\Sigma_\chi$ is generated by $\sigma^{s_\chi}$, and $\psi_{\chi, \lambda} : \Sigma_\chi \to \tilde{l}^\times$ is the character such that $\psi_{\chi, \lambda}(\sigma^{s_\chi}) = \lambda$. All these representations are absolutely irreducible.

(16) Some natural characters. The group $T$ comes with the faithful character $\theta : T \to l^\times$, so $G$ has a natural absolutely irreducible $\tilde{l}$-representation $\rho_{\bar{\theta}, 1}$ of degree equal to the order of $\bar{q} \in (\mathbb{Z}/e\mathbb{Z})^\times$. We could also consider $\theta^d$ for various divisors $d$ of $e$. Notice that $\theta$ allows us to identify $\text{Hom}(T, l^\times)$ with $\mathbb{Z}/e\mathbb{Z}$, and the $\Sigma$-orbit of $\chi = \theta^i$ with the $\Sigma$-orbit of $i \in \mathbb{Z}/e\mathbb{Z}$ (for the action $\sigma \mapsto (j \mapsto jq)$).

(17) Let us now come to irreducible $\mathbb{F}_p$-representations $\pi$ of $G$, which are also treated in [7, Proposition 4.2]. The group $\Phi = \text{Gal}(\tilde{l}/\mathbb{F}_p)$ acts on the set of irreducible $\tilde{l}$-representations $\rho$ of $G$ by conjugation. Let $\varphi : x \mapsto x^p$ ($x \in \tilde{l}$) be the canonical generator of $\Phi$. If $\rho$ corresponds to the pair $(\bar{\chi}, \lambda)$ as above, then $\varphi \rho$ corresponds to the pair $(\bar{\chi}^p, \lambda^p)$. The set of irreducible $\mathbb{F}_p$-representations $\pi$ of $G$ is in natural bijection with the set of $\Phi$-orbits $R$ for this action ; $\pi$ and $R$ correspond to each other if $\pi \otimes_{\mathbb{F}_p} \tilde{l} = \bigoplus_{\rho \in R} \rho$. If so, then $\deg \pi = (\deg \rho)(\text{Card} R)$, for any $\rho \in R$. Regarding this kind of “galoisian descent”, see for example [1, V.60].
(18) Let us compute Card R, or the size of the \( \Phi \)-orbit \( \overline{(\chi, \lambda)} \) of any pair \((\chi, \lambda)\) such that \( \rho_{\chi, \lambda} \in R \). Recall that \( d_\chi \) is the common order of every \( \chi \in \bar{\chi} \), and that \( r_\chi \) (resp. \( s_\chi \)) is the order of \( \overline{\bar{\rho}} \) (resp. \( \bar{\bar{q}} \)) in \( (\mathbb{Z}/d_\chi \mathbb{Z})^\times \). (We already know that \( \deg \rho_{\chi, \lambda} = s_\chi \)). The size of the \( \Phi \)-orbit of the \( \Sigma \)-orbit \( \bar{\chi} \) is \( r_\chi s_\chi^{-1} \), so the number of \( \mathbb{F}_p \)-conjugates of the pair \((\bar{\chi}, \lambda)\) (or the size of the \( \Phi \)-orbit \( R = \overline{(\bar{\chi}, \lambda)} \)) is \( \text{lcm}(r_\chi s_\chi^{-1}, w_\lambda) \), where \( w_\lambda \) is the degree \( [\mathbb{F}_p(\lambda) : \mathbb{F}_p] \) (which obviously depends only on the \( \Phi \)-orbit of \( \lambda \)), and the degree of \( \pi \) is \( s_\chi \text{lcm}(r_\chi s_\chi^{-1}, w_\lambda) = \text{lcm}(r_\chi, s_\chi w_\lambda) \). Therefore:

(19) The set of irreducible \( \mathbb{F}_p \)-representations \( \pi \) of \( G = T \times_q \Sigma \) is in natural bijection with the set of \( \Phi \)-orbits \( R = \overline{(\bar{\chi}, \lambda)} \) of pairs \((\bar{\chi}, \lambda)\) consisting of the \( \Sigma \)-orbit \( \bar{\chi} \) of a character \( \chi : T \to \ell^\times \) and an element \( \lambda \in \bar{\ell}^\times \) of order dividing \( fs_\chi^{-1} \), where \( s_\chi \) is the order of \( \bar{\bar{q}} \) in \( (\mathbb{Z}/d_\chi \mathbb{Z})^\times \) and \( d_\chi \) is the order of \( \chi \), under the correspondence \( \pi \otimes_{\mathbb{F}_p} \bar{\ell} = \oplus_{(\bar{\chi}, \lambda) \in R} \rho_{\bar{\chi}, \lambda} \), where \( \rho_{\bar{\chi}, \lambda} \) is the absolutely irreducible \( \bar{\ell} \)-representation of \( G \) attached to \( (\bar{\chi}, \lambda) \). If \( t_\chi \) denotes the order of \( \bar{\rho} \in (\mathbb{Z}/d_\chi \mathbb{Z})^\times \) and \( w_\lambda = [\mathbb{F}_p(\lambda) : \mathbb{F}_p] \), then \( \deg \pi = \text{lcm}(r_\chi, s_\chi w_\lambda) \).

(20) The field of definition. Let \( k_{\bar{\chi}, \lambda} \subset \bar{\ell} \) be the extension of \( \mathbb{F}_p \) of degree \( \text{lcm}(r_\chi s_\chi^{-1}, w_\lambda) \). It follows for similar reasons that there is a unique (absolutely) irreducible \( k_{\bar{\chi}, \lambda} \)-representation \( \rho'_{\bar{\chi}, \lambda} \) which gives back \( \rho_{\bar{\chi}, \lambda} \) upon changing the base to \( \bar{\ell} \) in the sense that \( \rho'_{\bar{\chi}, \lambda} \otimes_{k_{\bar{\chi}, \lambda}} \bar{\ell} = \rho_{\bar{\chi}, \lambda} \); we call \( k_{\bar{\chi}, \lambda} \) the field of definition of \( \rho_{\bar{\chi}, \lambda} \) and henceforth think of \( \rho_{\bar{\chi}, \lambda} \) as a \( k_{\bar{\chi}, \lambda} \)-representation.

(21) We denote the irreducible \( \mathbb{F}_p \)-representation of \( G \) associated to the \( \Phi \)-orbit \( \overline{(\bar{\chi}, \lambda)} \) by \( \pi_{\bar{\chi}, \lambda} \). The degree of \( \pi_{\bar{\chi}, \lambda} \) is \( r_\theta \) (the order of \( \bar{\rho} \) in \( (\mathbb{Z}/e\mathbb{Z})^\times \)). The notation is somewhat ambiguous because it doesn’t refer to the group \( G \). Indeed, if \( l' \) is a finite extension of \( l \), then the same \( \Phi \)-orbit \( (\bar{\chi}, \lambda) \) also gives rise to an irreducible \( \mathbb{F}_p \)-representation \( \pi' = \pi_{\bar{\chi}, \lambda} \) of the group \( G' = T \times_q \Sigma' \), where \( \Sigma' = \text{Gal}(l'[k]) \). The saving grace is that if we use the galoisian projection \( \gamma : \Sigma' \to \Sigma \) to view \( G \) as a quotient of \( G' \), then \( \pi' = \pi \circ \gamma \).

(22) We give some examples which will be useful later [5] in classifying quartic extensions \( E \) of a dyadic field \( K \) which have no intermediate quadratic extensions. The set of such \( E \) was parametrised in [4, 14] by the set of pairs \((\rho, D)\), where \( \rho \) is an irreducible \( \mathbb{F}_2 \)-representation of \( \text{Gal}(\bar{K}/K) \) (and \( \bar{K} \) is the maximal galoisian extension of \( K \)) and \( D \) is an \( \mathbb{F}_2^\times \)-extension of the fixed field \( \mathbb{F}_\rho \) of the kernel of \( \rho \) such that \( D \) is galoisian over \( K \) and the resulting conjugation action of \( \text{Gal}(\mathbb{F}_\rho/K) \) on \( \text{Gal}(D|\mathbb{F}_\rho) \) is given by \( \rho \). If so, the group \( \text{Gal}(\hat{E}|K) \) (where \( \hat{E} \) is the galoisian closure of \( E \) over \( K \)) is given by \( \mathbb{F}_2^2 \times_{\rho} \text{Gal}(\mathbb{F}_\rho/K) \) [4]. Here we merely construct all
degree-2 irreducible $\mathbb{F}_2$-representations $\rho$ of certain groups $G$ and identify the twisted product $\mathbb{F}_2^2 \times_\rho G$. Why it suffices to consider only these $G$ was explained in [4, 15] and will also become clear at the very end.

(23) A $(\mathbb{Z}/3\mathbb{Z})^e$-example. Take $p = 2$, $f = 3$, $e = 1$, so that $T = \{1\}$, and $G = \Sigma = \mathbb{Z}/3\mathbb{Z}$. We have $\bar{l} = l(\sqrt[3]{1})$. The only $\chi : T \rightarrow l^\times$ is the trivial character $1$; for it, there are three possible $\lambda$, namely $1, \sqrt[3]{1}$ and $\sqrt[3]{1}^2$. So we get three $\bar{l}$-characters, namely $\rho_{1,1}$, $\rho_{1,\sqrt[3]{1}}$ and $\rho_{1,\sqrt[3]{1}^2}$ of which the latter two are in the same $\Phi$-orbit, and these are the only irreducible $\bar{l}$-representations of $G$. Thus we get two $\mathbb{F}_2$-representations, namely the trivial representation $\pi_{\bar{l},1}$ and the irreducible degree-2 representation $\pi = \pi_{\bar{l},\sqrt[3]{1}}$; the latter is not absolutely irreducible. The group $\mathbb{F}_2^2 \times_\pi G$ is isomorphic to $A_4$.

Or keep $p = 2$ and take $q \equiv 1 \pmod{3}$, $f = 1$, $e = 3$, so that $\bar{l} = l$. Then $G = T = A_3$ is cyclic of order 3, the three irreducible $l$-representations are $\rho_{1,1}$, $\rho_{3,1}$, $\rho_{2,1}$ (all three of degree 1) of which the latter two are in the same $\Phi$-orbit, so the two irreducible $\mathbb{F}_2$-representations are $\pi_{1,1}$ (trivial) and $\pi = \pi_{3,1}$ (degree 2). The group $\mathbb{F}_2^2 \times_\pi G$ is isomorphic to $A_4$, as before.

(24) An $S_3$-example. Keep $p = 2$ and take $q \equiv -1 \pmod{3}$, $f = 2$, $e = 3$, so that $\Sigma = \mathbb{Z}/3\mathbb{Z}$, $G$ is isomorphic to $S_3$, and $\bar{l} = l$. The only characters $T \rightarrow l^\times$ are 1 (of order $d = 1$) and $\theta$, $\theta^2$ (of order $d = 3$); they fall into two $\Sigma$-orbits, namely $1$ (of size $s = 1$) and $\theta$ (of size $s = 2$). The only possible $\lambda$ in either case is $\lambda = 1$. So $\rho_{1,1}$ (of degree 1) and $\rho_{3,1}$ (of degree 2) are the only two (absolutely) irreducible $l$-representations of $G$, each of which is its own $\Phi$-orbit. Therefore there are two irreducible $\mathbb{F}_2$-representations of $G$, namely $\pi_{1,1}$ (the trivial representation) and $\pi = \pi_{3,1}$ (of degree 2). In fact, $\pi : G \rightarrow \text{GL}_2(\mathbb{F}_2)$ is an isomorphism, and $\mathbb{F}_2^2 \times_\pi G$ is isomorphic to $S_4$.

(25) Another general algebraic observation we need is the following lemma culled from [7, 4.9]; see also [8, p. 154]. Let $G$ be any finite group, $F$ any field, $E$ a finite galoisian extension of $F$, $W$ an absolutely irreducible $E$-representation of $G$ such that the conjugates $\sigma W$ ($\sigma \in \text{Gal}(E|F)$) of $W$ are all inequivalent. By galoisian descent, there is a unique (irreducible) $F$-representation $V$ of $G$ such that $V \otimes_F E = \bigoplus_{\sigma \in \text{Gal}(E|F)} \sigma W$. By Schur’s lemma, we have $\text{End}_{E[G]}(W) = E$ and also $\text{End}_{F[G]}(V) = E$.

Let $m > 0$ be an integer. For every $a = (a_i)_{i \in [1,m]}$ in $E^m$, we have the $F[G]$-morphism $\varphi_a : V \rightarrow V^m$ sending $x$ to $(a_i x)_{i \in [1,m]}$; it is injective if and only if $a \neq 0$. For $a \neq 0$, the image $\varphi_a(V)$ depends only on the line $\tilde{a} \subset E^m$ generated by $a$. 

6
(26) The map \( \bar{a} \mapsto \varphi_a(V) \) is a bijection of the set \( \mathbb{P}_{m-1}(E) \) of lines in \( E^m \) with the set of submodules of \( V^m \) isomorphic to \( V \). In particular, if \( E \) is finite and \( q = \text{Card}(E) \), then the number of such submodules is \( (q^m - 1)(q-1)^{-1} \).

Proof. The map in question is injective: indeed, if \( a \neq 0 \) and \( b \neq 0 \) are in \( E^m \), and if \( \varphi_a(V) = \varphi_b(V) \), then (slightly abusing notation) \( \varphi_b^{-1} \circ \varphi_a \) is a \( G \)-automorphism of \( V \), so a homothety of some ratio \( \xi \in E^\times \), therefore \( a = \xi b \) and \( \bar{a} = \bar{b} \). Next, the map \( \bar{a} \mapsto \varphi_a(V) \) is surjective: if \( \psi : V \to V^m \) is an injective \( G \)-morphism, the maps \( \pi_i \circ \psi \), where the \( \pi_i : V^m \to V \) are the canonical projections, are homotheties of some ratio \( a_i \in E \) such that \( a = (a_i)_{i \in [1,m]} \) is \( \neq 0 \), and \( \psi = \varphi_a \).

3. Irreducible \( \mathbb{F}_p \)-representations over \( p \)-fields

(27) Let \( K \) be a \( p \)-field, \( k \) its residue field, \( q = \text{Card} k \), and let \( V_0 \) (resp. \( V \), resp. \( \bar{K} \)) be the maximal unramified (resp. tamely ramified, resp. galoisian) extension of \( K \). Put \( \Gamma_0 = \text{Gal}(V_0|K) \) and \( \Gamma = \text{Gal}(V|K) \). We have seen in the Introduction that every irreducible \( \mathbb{F}_p \)-representation of \( \text{Gal}(\bar{K}|K) \) factors through \( \Gamma \).

For every \( n > 0 \), put \( e_n = p^n - 1 \) and \( V_n = V_0(\sqrt[p^n]{\varpi}) \), where \( \varpi \) is a uniformiser of \( K \). It doesn’t matter which \( \varpi \) we choose because \( V_n \) is also obtained by adjoining the family \( \sqrt[p^n]{x} \) (indexed by \( x \in V_0^\times \)) to \( V_0 \). Every \( V_n \) is galoisian over \( K \); put \( \Gamma_n = \text{Gal}(V_n|K) \), so that \( V = \varprojlim V_n \) and \( \Gamma = \varprojlim \Gamma_n \). The salient quotients \( \Gamma_n \) of \( \Gamma \) have nothing to do with the ramification filtration on \( \Gamma \) which is quite simply \( \Gamma_0 \subset \Gamma \), where \( \Gamma_0 = \text{Gal}(V|V_0) \) is the inertia subgroup. If \( p = 2 \), then \( V_1 = V_0 \). Note that if \( K \) has characteristic 0, then the \( p \)-torsion subgroup \( pV_n^\times \) of \( V_n^\times \) has order \( p \) (because \( V_1 \) contains \( p^{1/2} \)).

(28) Note that \( V_n \) is the compositum of all finite extensions of \( K \) of ramification index dividing \( e_n \), so the indexing has something to do with ramification afterall. Note also that if \( a = v_p(q) \) is the exponent of \( p \) in \( q \), then \( V_a \) is the maximal tamely ramified abelian extension of \( K \).

(29) Let \( n > 0 \) be an integer. Every irreducible \( \mathbb{F}_p \)-representation of \( \Gamma \) of degree dividing \( n \) factors through the quotient \( \Gamma_n \) of \( \Gamma \).

Proof. Let \( \pi \) be such a representation, and let \( L \) be a finite unramified extension of the fixed field \( V^{\text{Ker}(\pi)} \) which is split over \( K \) in the sense the inertia subgroup \( G_0 \) of \( G = \text{Gal}(L|K) \) has a complement in \( G \); by hypothesis, \( \pi|_{G_0} \) is faithful. It suffices (27) to show that the ramification index \( e \) of \( L \) over \( K \) divides \( e_n \).
Let \( l \) be the residue field of \( L \). The filtration \( G_0 \subset G \) is split by hypothesis; the choice of a section \( G/G_0 \to G \) leads to an isomorphism of \( G \) with \( T \times_q \Sigma \), where \( \Sigma = \text{Gal}(l|k) \) and \( T \subset l^\times \) is the subgroup of order \( e \). Since \( \pi|_T \) is faithful, \( \chi|_T \) is faithful for any character \( \chi: T \to l^\times \) which occurs in \((\pi|_T) \otimes \tilde{l} \) as in (11). Therefore the order of \( \chi \) is \( e \). Let \( r \) be the order of \( \bar{p} \in (\mathbb{Z}/e\mathbb{Z})^\times \), so that \( p^r \equiv 1 \mod e \). Since \( n \) is a multiple of \( r \), we have \( p^n \equiv 1 \mod e \), and hence \( e \) divides \( e_n = p^n - 1 \).

(30) Since there are only finitely many irreducible \( \mathbb{F}_p \)-representations \( \pi \) of \( \Gamma \) of given degree \( n \) (because \( \Gamma \) is finitely generated and \( \text{GL}_n(\mathbb{F}_p) \) is finite), there are finite extensions \( M \) of \( K \) such that every irreducible \( \mathbb{F}_p \)-representation of \( \Gamma \) of degree \( n \) factors through \( \text{Gal}(M|K) \). For \( n = 1 \), the smallest possible \( M \) is clearly \( L_1 = K(\sqrt[p]{\overline{K}}) \), which was used in [2] (and in [6] in the characteristic-0 case); recently I’ve discovered that this observation was made already in [10, V.9].

(31) A partition. Notice that ramified irreducible \( \mathbb{F}_p \)-representations \( \pi \) of \( \Gamma \) of degree \( n > 0 \) can be partitioned into classes labelled by the divisors \( r \) of \( n \). The representation \( \pi \) belongs to the class labelled by \( r \) if \( r \) is the smallest (in the sense of divisibility) divisor of \( n \) such that \( \pi \) factors through \( \Gamma_r \); equivalently, \( r \) is the order of \( \bar{p} \in (\mathbb{Z}/e\mathbb{Z})^\times \), where \( e \) is the ramification index over \( K \) of the fixed field \( V^{\text{Ker}(\pi)} \). If \( p = 2 \), then the class of label 1 is \( \emptyset \) because \( \Gamma_1 = \Gamma_0 \) and \( \pi \) would be unramified.

(32) For every \( n > 0 \), \( K_n = K(\sqrt[s]{1}) \) is the unramified extension of \( K \) of degree equal to the order \( s_n \) of \( \bar{q} \in (\mathbb{Z}/e_n\mathbb{Z})^\times \); put \( L_n = K_n(\sqrt[s]{K_n^s}) \), so that \( L_n \subset V_n \) and indeed \( V_n = L_n V_0 \). Note that \( L_n \) is the maximal abelian extension of \( K_n \) of exponent dividing \( e_n \), so it is galoisian over \( K \); put \( G_n = \text{Gal}(L_n|K) \). We have

\[
V_0 = \lim_{\rightarrow} K_n, \quad V = \lim_{\rightarrow} L_n, \quad \Gamma = \lim_{\leftarrow} G_n.
\]

Note that if \( K \) has characteristic 0, then \( pL_n^\times \) has order \( p \) (because \( L_1 \) contains \( \sqrt[p-1]{-p} \)).

In the proof of the next proposition, we shall need to consider certain finite galoisian extensions \( M \) of \( K \). We denote the residue fields of \( K_n \) (resp. \( L_n \), resp. \( M \)) by \( k_n \) (resp. \( l_n \), resp. \( m \)). Note that \( L_n \) is split over \( K \) because \( L_n = L_{n,0}(\sqrt{\varpi}) \) for any uniformiser \( \varpi \) of \( K \), where \( L_{n,0} \) is the maximal unramified extension of \( K \) in \( L_n \). If \( M \) is unramified over \( L_n \), then \( M \) is also split over \( K \).

(33) Every irreducible \( \mathbb{F}_p \)-representation of \( \Gamma \) of degree dividing \( n \) factors through the finite quotient \( G_n = \text{Gal}(L_n|K) \) of \( \Gamma \).

Proof. Let \( \pi' \) be such a representation, and recall that it factors through \( \Gamma_n \) (28). Let \( M \) be a finite unramified extension of \( L_n \) such
that $H = \text{Gal}(M|K)$ has the property claimed for $G_n$; we have to show that $\text{Gal}(M|L_n) \subset \text{Ker}(\pi')$. Choose a uniformiser $\varpi$ of $K$ and identify $H$ with $T \times q \text{Gal}(m|k)$ and $G_n$ with $T \times q \text{Gal}(l_n|k)$ as above; these identifications are compatible with the galoisian projections $\gamma : H \to G_n$ and $\text{Gal}(m|k) \to \text{Gal}(l_n|k)$. The representation $\pi' = \pi_{\mu,\eta}$ of $H$ in question is associated to the $\Phi$-orbit of a pair $(\tilde{\eta},\mu)$ consisting of the $\text{Gal}(m|k)$-orbit of some character $\eta : T \to m^\times$ and some $\mu \in \tilde{m}^\times$ as in (19). We certainly have $\eta(T) \subset k^\times$, therefore $\tilde{\eta}$ can be viewed as the $\text{Gal}(l_n|k)$-orbit $\tilde{\chi}$ of a character $\chi : T \to l_n^\times$. Recall that the degree $w_\mu = [F_p(\mu) : F_p]$ divides $n$, therefore the order of $\mu$ divides $e_n$, and hence $\mu \in k_n^\times$; call it $\lambda$ in this avatar. The $\Phi$-orbit of this new pair $(\tilde{\chi},\lambda)$ gives a representation $\pi = \pi_{\chi,\lambda}$ of $G_n$, and $\pi'$ factors through it ($\pi' = \pi \circ \gamma$), as in (21).

(34) Remark. We define the optimal quotient of $\Gamma$ in degree $n$ to be the smallest quotient of $\Gamma$ through which every irreducible $F_p$-representation $\pi$ of $\Gamma$ of degree $n$ factors. We also say that the corresponding extension $M_n$ of $K$ is the optimal extension in degree $n$; it is the compositum, over all $\pi$, of the extensions $V^{\text{Ker}(\pi)}$ of $K$. For $n = 1$, the quotient $G_1$ of $\Gamma$ and the corresponding extension $L_1 = K(\sqrt[n]{K})$ of $K$ are clearly optimal.

For $n > 1$, the extension $M_n$ is introduced in [7] but we prefer working with $L_n$ (which contains $M_n$ by (33)) because $L_n$ is very explicit, contains $\sqrt[n]{K}$ in characteristic 0, and it is split over $K$ so that the general theory of little groups as explained above can be applied. Note that $M_n$ contains the unramified extension of $K$ of degree $e_n$ and every totally ramified extension of $K$ of degree dividing $e_n$. We haven’t checked whether $M_n = L_n$ in general.

(35) The $(\mathbb{Z}/3\mathbb{Z})$-, $A_3$- and $S_3$-examples. Consider the case $p = 2$ and $n = 2$, so that $e_2 = 3$. If $q \equiv 1$ (mod. 3), then we have $K_2 = K$ and $L_2 = K(\sqrt[3]{K})$, so that $L_2$ contains the unramified cubic extension and the three ramified cubic extensions (all three cyclic) of $K$. We thus get back the $(\mathbb{Z}/3\mathbb{Z})$- and $A_3$-examples of (23). If $q \equiv -1$ (mod. 3), then $[K_2 : K] = 2$, so that $L_2$ contains the unramified cubic extension and the unique $S_3$-extension (namely $K(\sqrt[3]{1}, \sqrt[3]{\varpi})$, where $\varpi$ is a uniformiser) of $K$. We thus get back the $(\mathbb{Z}/3\mathbb{Z})$-example of (23) and the $S_3$-example of (24).

Bibliography

[1] Bourbaki (N). — Algèbre, Chapitres 4 à 7, Masson, Paris, 1981, 422 p.

[2] Dalawat (C). — Serre’s “formule de masse” in prime degree, Monatshefte Math. 166 (2012) 1, 73–92. Cf. arXiv:1004.2016v6.
[3] Dalawat (C) & Lee (JJ). — Tame ramification and group cohomology, J. Ramanujan Math. Soc. 32 (2017) 1, 51–74. Cf. arXiv:1305.2580v4.

[4] Dalawat (C). — Solvable primitive extensions, arXiv:1608.04673.

[5] Dalawat (C). — Wildly primitive extensions, arXiv:1608.04183.

[6] Del Corso (I) & Dvornicich (R). — The compositum of wild extensions of local fields of prime degree, Monatsh. Math. 150 (2007) 4, 271–288.

[7] Del Corso (I), Dvornicich (R) & Monge (M). — On wild extensions of a p-adic field, J. Number Theory 174 (2017), 322–342. Cf. arXiv:1601.05939.

[8] Doerk (K) & Hawkes (T). — Finite soluble groups, Walter de Gruyter & Co., Berlin, 1992. xiv+891 pp.

[9] Koch (H). — Classification of the primitive representations of the Galois group of local fields, Invent. Math. 40 (1977) 2, 195–216.

[10] Koch (H). — On the local Langlands conjecture, Séminaire de théorie des nombres de Grenoble 8 (1979-1980), 1–14.

[11] Serre (J-P). — Représentations linéaires des groupes finis, Hermann, Paris, 1978, 182 p.