Takahiro Tsushima

Local Galois representations associated to additive polynomials

Received: 30 November 2022 / Accepted: 8 March 2024

Abstract. For an additive polynomial and a positive integer, we define an irreducible smooth representation of a Weil group of a non-archimedean local field. We study several invariants of this representation. We obtain a necessary and sufficient condition for it to be primitive.

1. Introduction

Let p be a prime number and q a power of it. An additive polynomial $R(x)$ over $\mathbb{F}_q$ is a one-variable polynomial with coefficients in $\mathbb{F}_q$ such that $R(x+y) = R(x)+R(y)$. It is known that $R(x)$ has the form $\sum_{i=0}^{e} a_i x^{p^i}$ ($a_e \neq 0$) with an integer $e \geq 0$. Let F be a non-archimedean local field with residue field $\mathbb{F}_q$. We take a separable closure $\overline{F}$ of F. Let W_F be the Weil group of $\overline{F}/F$. Let $v_F(\cdot)$ denote the normalized valuation on F. We take a prime number $\ell \neq p$. For a non-trivial character $\psi \colon \mathbb{F}_p \to \overline{\mathbb{Q}}_\ell^\times$, a non-zero additive polynomial $R(x)$ over $\mathbb{F}_q$ and a positive integer m which is prime to p, we define an irreducible smooth W_F-representation $\tau_{\psi,R,m}$ over $\overline{\mathbb{Q}}_\ell$ of degree p^e if $v_F(p)$ is sufficiently large. This is unconditional if F has positive characteristic. The integer m is related to the Swan conductor exponent of $\tau_{\psi,R,m}$. As m varies, the isomorphism class of $\tau_{\psi,R,m}$ varies.

Let C_R denote the algebraic affine curve defined by $a^p - a = xR(x)$ in $\mathbb{A}^2_{\mathbb{F}_q} = \operatorname{Spec} \mathbb{F}_q[a,x]$. This curve is studied in [6] and [1] in detail. For example, the smooth compactification of C_R is proved to be supersingular if $(p,e) \neq (2,0)$. The automorphism group of C_R contains a semidirect product Q_R of a cyclic group and an extra-special p-group (Definition 2.7). Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Then a semidirect group $Q_R \rtimes \mathbb{Z}$ acts on the base change $C_{R,\mathbb{F}} := C_R \times_{\mathbb{F}_q} \mathbb{F}$ as endomorphisms, where $1 \in \mathbb{Z}$ acts on $C_{R,\mathbb{F}}$ as the Frobenius endomorphism over $\mathbb{F}_q$. The center $Z(Q_R)$ of Q_R is identified with $\mathbb{F}_p$, which acts on C_R as $a \mapsto a+\zeta$ for $\zeta \in \mathbb{F}_p$. Let $H^1_c(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ be the first étale cohomology group of $C_{R,\mathbb{F}}$ with compact support. Each element of $Z(Q_R)$ is fixed by the action of $\mathbb{Z}$ on Q_R. Thus its ψ-isotypic part $H^1_c(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is regarded as a $Q_R \rtimes \mathbb{Z}$-representation.

T. Tsushima (✉): Department of Mathematics and Informatics, Faculty of Science, Chiba University 1-33 Yayoi-cho, Inage, Chiba 263-8522, Japan.
e-mail: tsushima@math.s.chiba-u.ac.jp

Mathematics Subject Classification: Primary 11F80; Secondary 14H37

https://doi.org/10.1007/s00229-024-01550-6
Published online: 30 March 2024

We construct a concrete Galois extension over F whose Weil group is isomorphic to a subgroup of $Q_R \rtimes \mathbb{Z}$ associated to the integer m (Definition 3.1 and Lemma 3.9(1)). Namely we will define a homomorphism $\Theta_{R,m,\varpi} : W_F \to Q_R \rtimes \mathbb{Z}$ in (3.17). As a result, we define $\tau_{\psi,R,m}$ to be the composite

$$W_F \xrightarrow{\Theta_{R,m,\varpi}} Q_R \rtimes \mathbb{Z} \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(H_{\mathrm{c}}^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]).$$

This is a smooth irreducible representation of W_F of degree p^e.

We state our motivation and reason why we introduce and study $\tau_{\psi,R,m}$. It is known that the reductions of concentric affinoids in the Lubin–Tate curve fit into this type of curves C_R with special R. For example, see [18] and [19]. When R is a monomial and $m = 1$, the representation $\tau_{\psi,R,m}$ is studied in [9] and [10] in detail. In these papers, the reduction of a certain affinoid in the Lubin–Tate space is related to C_R in some sense and the supercuspidal representation π of $\mathrm{GL}_{p^e}(F)$ which corresponds to $\tau_{\psi,R,m}$ under the local Langlands correspondence explicitly. The homomorphism $\Theta_{R,1}$ with $R(x) = x^{p^e}$ ($e \in \mathbb{Z}_{\geq 1}$) does appear in the work [9]. An irreducible representation of a group is said to be primitive if it is not isomorphic to an induction of any representation of a proper subgroup. The representation $\tau_{\psi,R,m}$ in [9] and [10] is primitive and this property makes it complicated to describe π in a view point of type theory. For example, see [2]. It is an interesting problem to do the same thing for general $\tau_{\psi,R,m}$. In this direction, it would be valuable to know when $\tau_{\psi,R,m}$ is primitive. We expect that another C_R will be related to concentric affinoids in the Lubin–Tate spaces as in [9].

We briefly explain the content of each section. In 2, we state several things on the curves C_R and the extra-special p-subgroups contained in the automorphism groups of the curves.

In 3.1 and 3.2, we construct the Galois extension mentioned above and define $\tau_{\psi,R,m}$. Let $d_R := \gcd\{p^i + 1 \mid a_i \neq 0\}$. We show that the Swan conductor exponent of $\tau_{\psi,R,m}$ equals $m(p^e + 1)/d_R$ (Corollary 3.15). In 3.3, we study primitivity of $\tau_{\psi,R,m}$. In particular, we write down a necessary and sufficient condition for $\tau_{\psi,R,m}$ to be primitive. Using this criterion, we give examples that $\tau_{\psi,R,m}$ is primitive (Example 3.29). The necessary and sufficient condition is that a symplectic module (V_R, ω_R) associated to $\tau_{\psi,R,m}$ is completely anisotropic (Corollary 3.28). If R is a monomial, (V_R, ω_R) is studied in 3.4 in more detail. In Proposition 3.44, a primary module in the sense of [9, 11] is constructed geometrically via the Künneth formula.

Our aim in 4 is to show the following theorem.

Theorem 1.1. *Assume $p \neq 2$. The following two conditions are equivalent.*

(1) *There exists a non-trivial finite étale morphism*

$$C_R \to C_{R_1};\ (a, x) \mapsto (a - \Delta(x), r(x)),$$

where $\Delta(x) \in \mathbb{F}_q[x]$ and $r(x)$, $R_1(x)$ are additive polynomials over $\mathbb{F}_q$ such that $d_{R,m} \mid d_{R_1}$ and $r(\alpha x) = \alpha r(x)$ for any $\alpha \in \mu_{d_{R,m}}$.

(2) *The W_F-representation $\tau_{\psi,R,m}$ is imprimitive.*

If $\tau_{\psi,R,m}$ is imprimitive, it is written as a form of an induced representation of a certain explicit $W_{F'}$-representation $\tau'_{\psi,R_1,m}$ associated to a finite extension F'/F. The proof of the above theorem depends on several geometric properties of C_R developed in [6] and [1]. See the beginning of 4 for more details.

Notation

Let k be a field. Let $\mu(k)$ denote the set of all roots of unity in k. For a positive integer r, let $\mu_r(k) := \{x \in k \mid x^r = 1\}$.

For a positive integer i, let $\mathbb{A}^i_k$ and $\mathbb{P}^i_k$ be an i-dimensional affine space and a projective space over k, respectively. For a scheme X over k and a field extension l/k, let X_l denote the base change of X to l. For a closed subset Z of a variety X, we regard Z as a closed subscheme with the reduced scheme structure.

Throughout this paper, we set $q := p^f$ with a positive integer f. For a positive integer i, we simply write $\mathrm{Nr}_{q^i/q}$ and $\mathrm{Tr}_{q^i/q}$ for the norm map and the trace map from $\mathbb{F}_{q^i}$ to $\mathbb{F}_q$, respectively.

Let X be a scheme over $\mathbb{F}_q$ and let $F_q \colon X \to X$ be the q-th power Frobenius endomorphism. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Let $\mathrm{Fr}_q \colon X_{\mathbb{F}} \to X_{\mathbb{F}}$ be the base change of F_q to $X_{\mathbb{F}}$. This endomorphism Fr_q is called the Frobenius endomorphism of X over $\mathbb{F}_q$.

For a Galois extension l/k, let $\mathrm{Gal}(l/k)$ denote the Galois group of the extension.

2. Extra-special p-groups and affine curves

Definition 2.1. Let k be a field. A polynomial $f(x) \in k[x]$ is called *additive* if $f(x+y) = f(x) + f(y)$. Let $\mathscr{A}_k$ be the set of all additive polynomials with coefficients in k.

Let p be a prime number. We simply write $\mathscr{A}_q$ for $\mathscr{A}_{\mathbb{F}_q}$. Let $R(x) := \sum_{i=0}^{e} a_i x^{p^i} \in \mathscr{A}_q$ with $e \in \mathbb{Z}_{\geq 0}$ and $a_e \neq 0$. Let

$$E_R(x) := R(x)^{p^e} + \sum_{i=0}^{e} (a_i x)^{p^{e-i}} \in \mathscr{A}_q. \tag{2.1}$$

We always assume

$$(p, e) \neq (2, 0). \tag{2.2}$$

This condition and $a_e \neq 0$ guarantee that $E_R(x)$ is a separable polynomial of degree p^{2e}. We simply write μ_r for $\mu_r(\mathbb{F})$ for a positive integer r. Let

$$d_R := \gcd\{p^i + 1 \mid a_i \neq 0\}.$$

If $a_i \neq 0$, we have $\alpha^{p^i} = \alpha^{-1}$ and $\alpha^{p^{e-i}} = \alpha$ for $\alpha \in \mu_{d_R}$. Hence

$$\alpha R(\alpha x) = R(x), \quad E_R(\alpha x) = \alpha E_R(x) \quad \text{for } \alpha \in \mu_{d_R}. \tag{2.3}$$

We consider the polynomial

$$f_R(x, y) := -\sum_{i=0}^{e-1}\left(\sum_{j=0}^{e-i-1}(a_i x^{p^i} y)^{p^j} + (xR(y))^{p^i}\right) \in \mathbb{F}_q[x, y].$$

This is linear with respect to x and y. By (2.3), we have an equality

$$f_R(\alpha x, \alpha y) = f_R(x, y) \quad \text{for } \alpha \in \mu_{d_R}. \tag{2.4}$$

Lemma 2.2. *We have $f_R(x, y)^p - f_R(x, y) = -x^{p^e}E_R(y) + xR(y) + yR(x)$. In particular, if $E_R(y) = 0$, we have $f_R(x, y)^p - f_R(x, y) = xR(y) + yR(x)$.*

Proof. The former equality follows from

$$\begin{aligned} f_R(x, y)^p - f_R(x, y) &= xR(y) - (xR(y))^{p^e} + \sum_{i=0}^{e-1}(a_i x^{p^i} y - (a_i x^{p^i} y)^{p^{e-i}}) \\ &= -x^{p^e}E_R(y) + xR(y) + yR(x). \end{aligned}$$

□

Definition 2.3. (1) Let $V_R := \{\beta \in \mathbb{F} \mid E_R(\beta) = 0\}$, which is a $(2e)$-dimensional $\mathbb{F}_p$-vector space.

(2) Let

$$Q_R := \left\{(\alpha, \beta, \gamma) \in \mathbb{F}^3 \mid \alpha \in \mu_{d_R},\ \beta \in V_R,\ \gamma^p - \gamma = \beta R(\beta)\right\}$$

be the group whose group law is given by

$$(\alpha_1, \beta_1, \gamma_1) \cdot (\alpha_2, \beta_2, \gamma_2) := (\alpha_1\alpha_2, \beta_1 + \alpha_1\beta_2, \gamma_1 + \gamma_2 + f_R(\beta_1, \alpha_1\beta_2)). \tag{2.5}$$

We check that this is well-defined and Q_R is a group. From (2.3), it follows that $E_R(\alpha_1\beta_2) = \alpha_1 E_R(\beta_2) = 0$. Furthermore, letting $\gamma := \gamma_1+\gamma_2+f_R(\beta_1, \alpha_1\beta_2)$, we compute

$$\begin{aligned} \gamma^p - \gamma &= \beta_1 R(\beta_1) + \beta_2 R(\beta_2) + \beta_1 R(\alpha_1\beta_2) + \alpha_1\beta_2 R(\beta_1) \\ &= (\beta_1 + \alpha_1\beta_2)R(\beta_1 + \alpha_1\beta_2), \end{aligned}$$

where we use Lemma 2.2 for the first equality and use (2.3) for the last one. Hence the right hand side of (2.5) is in Q_R. Via (2.4), both of $((\alpha_1, \beta_1, \gamma_1) \cdot (\alpha_2, \beta_2, \gamma_2)) \cdot (\alpha_3, \beta_3, \gamma_3)$ and $(\alpha_1, \beta_1, \gamma_1) \cdot ((\alpha_2, \beta_2, \gamma_2) \cdot (\alpha_3, \beta_3, \gamma_3))$ equal

$$\begin{aligned} &(\alpha_1\alpha_2\alpha_3, \beta_1 + \alpha_1(\beta_2 + \alpha_2\beta_3), \gamma_1 + \gamma_2 + \gamma_3 + f_R(\beta_1, \alpha_1(\beta_2 + \alpha_2\beta_3)) \\ &\quad + f_R(\beta_2, \alpha_2\beta_3)). \end{aligned}$$

Finally, $(1, 0, 0)$ is the identity element of Q_R and the inverse element of $(\alpha, \beta, \gamma) \in Q_R$ is given by

$$(\alpha, \beta, \gamma)^{-1} = (\alpha^{-1}, -\alpha^{-1}\beta, -\gamma + f_R(\beta, \beta)), \tag{2.6}$$

where the right hand side is in Q_R due to Lemma 2.2 and (2.3).

(3) Let $H_R := \{(\alpha, \beta, \gamma) \in Q_R \mid \alpha = 1\}$, which is a normal subgroup of Q_R.

If $e = 0$, we have $p \neq 2$ by (2.2). We have $H_R = \mathbb{F}_p \subset Q_R = \mu_2 \times \mathbb{F}_p$ if $e = 0$.

For a group G and elements $g, g' \in G$, let $[g, g'] := gg'g^{-1}g'^{-1}$.

Lemma 2.4. *For $g = (1, \beta, \gamma)$, $g' = (1, \beta', \gamma') \in H_R$, we have $[g, g'] = (1, 0, f_R(\beta, \beta') - f_R(\beta', \beta))$. In particular, we have $f_R(\beta, \beta') - f_R(\beta', \beta) \in \mathbb{F}_p$.*

Proof. Using (2.6) and letting $\gamma_1 := -\gamma - \gamma' + f_R(\beta, \beta) + f_R(\beta', \beta') + f_R(\beta, \beta')$, we compute

$$\begin{aligned}
[g, g'] &= (1, \beta, \gamma)(1, \beta', \gamma')(1, -\beta, -\gamma + f_R(\beta, \beta))(1, -\beta', -\gamma' + f_R(\beta', \beta')) \\
&= (1, \beta + \beta', \gamma + \gamma' + f_R(\beta, \beta'))(1, -\beta - \beta', \gamma_1) \\
&= (1, 0, f_R(\beta, \beta) + f_R(\beta', \beta') + 2f_R(\beta, \beta') - f_R(\beta + \beta', \beta + \beta')) \\
&= (1, 0, f_R(\beta, \beta') - f_R(\beta', \beta)).
\end{aligned}$$ □

For a group G, let $Z(G)$ denote its center and $[G, G]$ the commutator subgroup of G.

Definition 2.5. A non-abelian p-group G is called an *extra-special p-group* if $[G, G] = Z(G)$ and $|Z(G)| = p$.

Lemma 2.6. *Assume $e \geq 1$.*

(1) *The group H_R is non-abelian. We have $Z(H_R) = Z(Q_R) = \{(1, 0, \gamma) \mid \gamma \in \mathbb{F}_p\}$. The quotient $H_R/Z(H_R)$ is isomorphic to V_R.*
(2) *The group H_R is an extra-special p-group. The $\mathbb{F}_p$-bilinear form $\omega_R \colon V_R \times V_R \to \mathbb{F}_p;\ (\beta, \beta') \mapsto f_R(\beta, \beta') - f_R(\beta', \beta)$ is a non-degenerate symplectic form.*

Proof. We show (1). Let $X_\beta := \{x \in \mathbb{F} \mid f_R(\beta, x) = f_R(x, \beta)\}$ for $\beta \in V_R$. Then X_β is an $\mathbb{F}_p$-vector space of dimension $2e - 1$ if $\beta \neq 0$. Since V_R has dimension $2e$, we have $V_R \not\subset X_\beta$ for $\beta \in V_R \backslash \{0\}$. We take $\beta' \in V_R \backslash X_\beta$ and $g = (1, \beta, \gamma)$, $g' = (1, \beta', \gamma') \in H_R$. Then $[g, g'] = (1, 0, f_R(\beta, \beta') - f_R(\beta', \beta)) \neq 1$ in H_R according to Lemma 2.4. Hence H_R is non-abelian.

Clearly we have $Z := \{(1, 0, \gamma) \mid \gamma \in \mathbb{F}_p\} \subset Z(Q_R) \subset Z(H_R)$. It suffices to show $Z(H_R) \subset Z$. Let $(1, \beta, \gamma) \in Z(H_R)$. We have $V_R \subset X_\beta$ by Lemma 2.4. This implies $\beta = 0$. Thus we obtain $Z(H_R) \subset Z$. The last claim is easily verified.

We show (2). By Lemma 2.4, we have $[H_R, H_R] \subset Z(H_R)$. Since H_R is non-abelian, $[H_R, H_R]$ is non-trivial. Hence we have $[H_R, H_R] = Z(H_R)$ by $|Z(H_R)| = p$. Thus H_R is extra-special. Assume $\omega_R(\beta, \beta') = 0$ for any $\beta' \in V_R$. We take an element $(1, \beta, \gamma) \in H_R$. By Lemma 2.4, we have $(1, \beta, \gamma) \in Z(H_R)$. Thus $\beta = 0$ by (1). □

Definition 2.7. (1) Let C_R be the affine curve over $\mathbb{F}_q$ defined by $a^p - a = xR(x)$.
(2) Let Q_R act on $C_{R,\mathbb{F}}$ by

$$(a, x) \cdot (\alpha, \beta, \gamma) = \Big(a + f_R(x, \beta) + \gamma, \alpha^{-1}(x + \beta)\Big), \tag{2.7}$$

for $(a, x) \in C_{R,\mathbb{F}}$ and $(\alpha, \beta, \gamma) \in Q_R$. This is well-defined by (2.3) and Lemma 2.2.

The curve C_R is studied in [6] and [1].

We take a prime number $\ell \neq p$. For a finite abelian group A, let $A^\vee$ denote the character group $\mathrm{Hom}_{\mathbb{Z}}(A, \overline{\mathbb{Q}}_\ell^\times)$. For a representation M of A over $\overline{\mathbb{Q}}_\ell$ and $\chi \in A^\vee$, let $M[\chi]$ denote the χ-isotypic part of M.

According to Lemma 2.6(1), we identify a character $\psi \in \mathbb{F}_p^\vee$ with a character of $Z(H_R)$.

Lemma 2.8. *Let $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$.*

(1) *Let $W \subset V_R$ be an $\mathbb{F}_p$-subspace of dimension e, which is totally isotropic with respect to ω_R. Let $W' \subset H_R$ be the inverse image of W by the natural map $H_R \to V_R$; $(1, \beta, \gamma) \mapsto \beta$. Let $\xi \in W'^\vee$ be an extension of $\psi \in Z(H_R)^\vee$. Let $\rho_\psi := \mathrm{Ind}_{W'}^{H_R} \xi$. Then ρ_ψ is a unique (up to isomorphism) irreducible representation of H_R containing ψ. In particular, $\rho_\psi|_{Z(H_R)}$ is a multiple of ψ.*

(2) *The ψ-isotypic part $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is isomorphic to ρ_ψ as H_R-representations.*

Proof. From Lemma 2.4, it follows that the subgroup $W' \subset H_R$ is abelian, since W is totally isotropic via ω_R. Hence an extension $\xi \in W'^\vee$ of ψ always exists. From Lemma 2.6(2) and [8, 16.14(2) Satz], the claim (1) follows. By [18, Remark 3.29], we have $\dim H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi] = p^e$. Hence the claim (2) follows from (1). □

The representation ρ_ψ induces a projective representation

$$\bar{\rho}_\psi : H_R/Z(H_R) \to \mathrm{PGL}_{p^e}(\overline{\mathbb{Q}}_\ell).$$

Lemma 2.9. *The map $\bar{\rho}_\psi$ is injective.*

Proof. As in the proof of [15, Theorem 6], we have $\mathrm{Tr}\,\rho_\psi(x) = 0$ for $x \in H_R \backslash Z(H_R)$. Assume $\bar{\rho}_\psi(xZ(H_R)) = 1$ for $x \in H_R$. Then $\rho_\psi(x)$ is a non-zero scalar matrix. Hence $\mathrm{Tr}\,\rho_\psi(x) \neq 0$. This implies $x \in Z(H_R)$. □

Let $\mathbb{Z} \ni 1$ act on $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ by the pull-back Fr_q^*. Let $\mathbb{Z} \ni 1$ act on Q_R by $(\alpha, \beta, \gamma) \mapsto (\alpha^{q^{-1}}, \beta^{q^{-1}}, \gamma^{q^{-1}})$. The semidirect product $Q_R \rtimes \mathbb{Z}$ acts on $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$.

A smooth projective geometrically connected curve X over $\mathbb{F}_q$ is said to be supersingular when the Jacobian of $X_{\mathbb{F}}$ is isogenous to a power of a supersingular elliptic curve.

Proposition 2.10. *Let $\overline{C}_R$ denote the smooth compactification of C_R. The projective curve $\overline{C}_R$ is supersingular. In particular, this curve has positive genus. The natural map $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^1(\overline{C}_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ is an isomorphism.*

Proof. The former claim is shown in [6, Theorems (9.4) and (13.7)] ([1, Proposition 8.5], [17, Theorem 1.1]). The last claim follows from [18, Lemmas 3.27 and 3.28(3)]. □

3. Local Galois representation

In this section, we define an irreducible smooth W_F-representation $\tau_{\psi,R,m}$ and determine several invariants associated to it. In 3.2.2, we determine the Swan conductor exponent of $\tau_{\psi,R,m}$. In 3.3, we determine the symplectic module associated to $\tau_{\psi,R,m}$, and give a necessary and sufficient condition for $\tau_{\psi,R,m}$ to be primitive. As a result, we obtain several examples such that $\tau_{\psi,R,m}$ is primitive. In Lemma 3.36, if R is a monomial, we calculate invariants of the root system corresponding to (V_R, ω_R) defined in [11].

3.1. Galois extension

For a valued field K, let $\mathcal{O}_K$ denote the valuation ring of K.

Let F be a non-archimedean local field. We denote the characteristic of F by char F. Let $\overline{F}$ be a separable closure of F. Let $\widehat{\overline{F}}$ denote the completion of $\overline{F}$. Let $v(\cdot)$ denote the unique valuation on $\widehat{\overline{F}}$ such that $v(\varpi) = 1$ for a uniformizer ϖ of F, which we now fix. We simply write $\mathcal{O}$ for $\mathcal{O}_{\widehat{\overline{F}}}$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$.

For an element $x \in \mathcal{O}$, let $\bar{x}$ denote the image of x by the reduction map $\mathcal{O} \to \mathcal{O}/\mathfrak{p}$. For a positive integer r prime to p, we have the bijection

$$\mu_r(\overline{F}) \cup \{0\} \xrightarrow{\sim} \mu_r(\mathbb{F}) \cup \{0\};\ x \mapsto \bar{x}. \tag{3.1}$$

The inverse of this map is given by Teichmüller lift. Let q be the cardinality of the residue field of $\mathcal{O}_F$. For an element $a \in \mathbb{F}_q$, let $\widetilde{a} \in \mu_{q-1}(F) \cup \{0\}$ denote its lift via (3.1).

We take $R(x) = \sum_{i=0}^{e} a_i x^{p^i} \in \mathscr{A}_q$. Let

$$\widetilde{R}(x) := \sum_{i=0}^{e} \widetilde{a}_i x^{p^i}, \quad \widetilde{E}_R(x) := \widetilde{R}(x)^{p^e} + \sum_{i=0}^{e} (\widetilde{a}_i x)^{p^{e-i}} \in \mathcal{O}_F[x].$$

Similarly as in (2.3),

$$\alpha \widetilde{R}(\alpha x) = \widetilde{R}(x), \quad \widetilde{E}_R(\alpha x) = \alpha \widetilde{E}_R(x) \quad \text{for } \alpha \in \mu_{d_R}(\overline{F}). \tag{3.2}$$

Definition 3.1. Let m be a positive integer prime to p. Let $\alpha_{R,\varpi}, \beta_{R,m,\varpi}, \gamma_{R,m,\varpi} \in \overline{F}$ be elements such that

$$\alpha_{R,\varpi}^{d_R} = \varpi, \quad \widetilde{E}_R(\beta_{R,m,\varpi}) = \alpha_{R,\varpi}^{-m}, \quad \gamma_{R,m,\varpi}^{p} - \gamma_{R,m,\varpi} = \beta_{R,m,\varpi} \widetilde{R}(\beta_{R,m,\varpi}).$$

For simplicity, we write $\alpha_R, \beta_{R,m}, \gamma_{R,m}$ for $\alpha_{R,\varpi}, \beta_{R,m,\varpi}, \gamma_{R,m,\varpi}$, respectively.

Remark 3.2. By $\deg \widetilde{E}_R(x) = p^{2e}$ and $\deg \widetilde{R}(x) = p^e$, we have

$$v(\alpha_R) = \frac{1}{d_R}, \quad v(\beta_{R,m}) = -\frac{m}{p^{2e} d_R}, \quad v(\gamma_{R,m}) = -\frac{m(p^e + 1)}{p^{2e+1} d_R}.$$

The integer m controls the depth of ramification of the resulting field extension $F(\alpha_R, \beta_{R,m}, \gamma_{R,m})/F$. We will understand this later in 3.2.2.

Let

$$\widetilde{f}(x, y) := -\sum_{i=0}^{e-1} \left(\sum_{j=0}^{e-i-1} (\widetilde{a}_j x^{p^i} y)^{p^j} + (x\widetilde{R}(y))^{p^i} \right).$$

Let $\mathfrak{p}[x] := \mathfrak{p}\mathcal{O}[x]$ and $\mathfrak{p}[x, y] := \mathfrak{p}\mathcal{O}[x, y]$. We assume that

$$\begin{aligned} &\beta_{R,m}^{p^e}(\widetilde{E}_R(\beta_{R,m} + x) - \widetilde{E}_R(\beta_{R,m}) - \widetilde{E}_R(x)),\\ &\beta_{R,m}(\widetilde{R}(\beta_{R,m} + x) - \widetilde{R}(\beta_{R,m}) - \widetilde{R}(x)),\\ &\widetilde{f}(\beta_{R,m}, x)^p - \widetilde{f}(\beta_{R,m}, x) + \beta_{R,m}^{p^e} \widetilde{E}_R(x) - x\widetilde{R}(\beta_{R,m}) - \beta_{R,m}\\ &\widetilde{R}(x) \text{ are contained in } \mathfrak{p}[x] \text{ and}\\ &(\gamma_{R,m} + \widetilde{f}(\beta_{R,m}, y) + x)^p - \gamma_{R,m}^p - \widetilde{f}(\beta_{R,m}, y)^p - x^p \in \mathfrak{p}[x, y]. \end{aligned} \tag{3.3}$$

If char $F = p$, these differences are zero by $(x + y)^p = x^p + y^p$ and Lemma 2.2. Thus (3.3) is always satisfied in this case.

For $r \in \mathbb{Q}_{\geq 0}$ and $f, g \in \overline{F}$, we write $f \equiv g \mod r+$ if $v(f - g) > r$. For a local field K contained in $\overline{F}$, let W_K be the Weil group of $\overline{F}/K$. Let

$$n \colon W_K \twoheadrightarrow \mathbb{Z};\ \sigma \mapsto n_\sigma \tag{3.4}$$

denote the homomorphism defined by $\sigma(x) \equiv x^{q^{-n_\sigma}} \mod 0+$ for $x \in \mathcal{O}_{\overline{F}}$. Let $v_K(\cdot)$ denote the normalized valuation on K.

Definition 3.3. For $\sigma \in W_F$, we set

$$\begin{aligned} a_{R,\sigma} &:= \sigma(\alpha_R)/\alpha_R \in \mu_{d_R}(\overline{F}), \quad b_{R,\sigma} := a_{R,\sigma}^m \sigma(\beta_{R,m}) - \beta_{R,m},\\ c_{R,\sigma} &:= \sigma(\gamma_{R,m}) - \gamma_{R,m} - \widetilde{f}(\beta_{R,m}, b_{R,\sigma}). \end{aligned} \tag{3.5}$$

In the following, we simply write $a_\sigma, b_\sigma, c_\sigma$ for $a_{R,\sigma}, b_{R,\sigma}, c_{R,\sigma}$, respectively.

In the following proofs, for simplicity, we often write α, β and γ for α_R, $\beta_{R,m}$ and $\gamma_{R,m}$, respectively.

Lemma 3.4. *We have $b_\sigma, c_\sigma \in \mathcal{O}$, $E_R(\bar{b}_\sigma) = 0$ and $\bar{c}_\sigma^p - \bar{c}_\sigma = \bar{b}_\sigma R(\bar{b}_\sigma)$.*

Proof. Using (3.2), the equality $\widetilde{E}_R(\beta) = \alpha^{-m}$ in Definition 3.1 and (3.5),

$$\widetilde{E}_R(\beta + b_\sigma) = \widetilde{E}_R(a_\sigma^m \sigma(\beta)) = a_\sigma^m \widetilde{E}_R(\sigma(\beta)) = a_\sigma^m \sigma(\alpha)^{-m} = \alpha^{-m} = \widetilde{E}_R(\beta).$$

Using $v(\beta) < 0$ in Remark 3.2 and (3.3), we have $\Delta(x) := \widetilde{E}_R(\beta + x) - \widetilde{E}_R(\beta) - \widetilde{E}_R(x) \in \mathfrak{p}[x]$. By letting $x = b_\sigma$ and applying the previous relationship, we obtain that $\widetilde{E}_R(b_\sigma) + \Delta(b_\sigma) = 0$. Hence $b_\sigma \in \mathcal{O}$ and $E_R(\bar{b}_\sigma) = 0$.

By (3.3), we have

$$\begin{aligned} \beta\widetilde{R}(\beta + b_\sigma) &\equiv \beta\widetilde{R}(\beta) + \beta\widetilde{R}(b_\sigma),\\ \widetilde{f}(\beta, b_\sigma)^p - \widetilde{f}(\beta, b_\sigma) &\equiv b_\sigma \widetilde{R}(\beta) + \beta\widetilde{R}(b_\sigma) \mod 0+. \end{aligned} \tag{3.6}$$

Substituting $y = b_\sigma \in \mathcal{O}$ to (3.3), we obtain

$$\Delta_1(x) := (\gamma + \widetilde{f}(\beta, b_\sigma) + x)^p - \gamma^p - \widetilde{f}(\beta, b_\sigma)^p - x^p \in \mathfrak{p}[x].$$

We have $\sigma(\beta)\widetilde{R}(\sigma(\beta)) = (\beta + b_\sigma)\widetilde{R}(\beta + b_\sigma)$ by substituting (3.5) and using (3.2). By multiplying the first congruence in (3.6) by $b_\sigma \beta^{-1}$, we obtain $b_\sigma \widetilde{R}(\beta + b_\sigma) \equiv b_\sigma \widetilde{R}(\beta) + b_\sigma \widetilde{R}(b_\sigma) \mod 0+$. Hence, we compute

$$\begin{aligned}
\sigma(\gamma)^p - \sigma(\gamma) = \sigma(\beta)\widetilde{R}(\sigma(\beta)) &= (\beta + b_\sigma)\widetilde{R}(\beta + b_\sigma) \\
&\equiv \beta\widetilde{R}(\beta) + b_\sigma\widetilde{R}(\beta) + \beta\widetilde{R}(b_\sigma) + b_\sigma\widetilde{R}(b_\sigma) \\
&\equiv \gamma^p - \gamma + \widetilde{f}(\beta, b_\sigma)^p - \widetilde{f}(\beta, b_\sigma) + b_\sigma\widetilde{R}(b_\sigma) \\
&\equiv \sigma(\gamma)^p - \sigma(\gamma) - (c_\sigma^p - c_\sigma + \Delta_1(c_\sigma)) + b_\sigma\widetilde{R}(b_\sigma) \mod 0+,
\end{aligned}$$

where we have used (3.5) for the last congruence. Therefore, we obtain $c_\sigma^p - c_\sigma + \Delta_1(c_\sigma) \equiv b_\sigma \widetilde{R}(b_\sigma) \mod 0+$. By $b_\sigma \in \mathcal{O}$, we have $c_\sigma \in \mathcal{O}$ and $\bar{c}_\sigma^p - \bar{c}_\sigma = \bar{b}_\sigma R(\bar{b}_\sigma)$. □

Assume that

$$\begin{aligned}
&(x + \beta_{R,m})^{p^i} - x^{p^i} - \beta_{R,m}^{p^i} \in \mathfrak{p}[x] \quad \text{for } 1 \leq i \leq e-1, \\
&\widetilde{f}(\beta_{R,m}, x + y) - \widetilde{f}(\beta_{R,m}, x) - \widetilde{f}(\beta_{R,m}, y) \in \mathfrak{p}[x, y],
\end{aligned} \tag{3.7}$$

which are satisfied if char $F = p$, because these differences are zero. Let

$$\Theta_{R,m,\varpi} \colon W_F \to Q_R \rtimes \mathbb{Z};\ \sigma \mapsto ((\bar{a}_\sigma^m, \bar{b}_\sigma, \bar{c}_\sigma), n_\sigma). \tag{3.8}$$

Lemma 3.5. *The map $\Theta_{R,m,\varpi}$ is a homomorphism.*

Proof. Let $\sigma, \sigma' \in W_F$. Recall that $\sigma(x) \equiv x^{q^{-n_\sigma}} \mod 0+$ for $x \in \mathcal{O}_{\overline{F}}$. Using Definition 2.3(2), we reduce the claim to checking that

$$\begin{aligned}
\bar{a}_{\sigma\sigma'} &= \bar{a}_\sigma \bar{a}_{\sigma'}^{q^{-n_\sigma}}, \\
\bar{b}_{\sigma\sigma'} &= \bar{a}_\sigma^m \bar{b}_{\sigma'}^{q^{-n_\sigma}} + \bar{b}_\sigma, \\
\bar{c}_{\sigma\sigma'} &= \bar{c}_\sigma + \bar{c}_{\sigma'}^{q^{-n_\sigma}} + f_R(\bar{b}_\sigma, \bar{a}_\sigma^m \bar{b}_{\sigma'}^{-n_\sigma}).
\end{aligned} \tag{3.9}$$

We easily check that $a_{\sigma\sigma'} = \sigma(a_{\sigma'})a_\sigma$ and $b_{\sigma\sigma'} = a_\sigma^m \sigma(b_{\sigma'}) + b_\sigma$. Hence the first two equalities in (3.9) follow. We compute

$$\begin{aligned}
c_{\sigma\sigma'} &= c_\sigma + \sigma(c_{\sigma'}) + \sigma(\widetilde{f}(\beta, b_{\sigma'})) + \widetilde{f}(\beta, b_\sigma) - \widetilde{f}(\beta, b_{\sigma\sigma'}) \\
&\equiv c_\sigma + \sigma(c_{\sigma'}) + \sigma(\widetilde{f}(\beta, b_{\sigma'})) - \widetilde{f}(\beta, a_\sigma^m \sigma(b_{\sigma'})) \mod 0+,
\end{aligned}$$

where we use the second condition in (3.7) for the second congruence. We have

$$\begin{aligned}
\sigma(\widetilde{f}(\beta, b_{\sigma'})) &= -\sum_{i=0}^{e-1} \sum_{j=0}^{e-i-1} (\widetilde{a}_j \sigma(b_{\sigma'}) \sigma(\beta)^{p^i})^{p^j} - \sum_{i=0}^{e-1} (\sigma(\beta)\widetilde{R}(\sigma(b_{\sigma'})))^{p^i} \\
&\equiv \widetilde{f}(b_\sigma, a_\sigma^m \sigma(b_{\sigma'})) + \widetilde{f}(\beta, a_\sigma^m \sigma(b_{\sigma'})) \mod 0+,
\end{aligned}$$

where we substitute $\sigma(\beta) = a_\sigma^{-m}(\beta + b_\sigma)$, (3.7) and (3.2) for the second congruence. The last equality in (3.9) follows from $\overline{\widetilde{f}(b_\sigma, a_\sigma^m \sigma(b_{\sigma'}))} = f_R(\bar{b}_\sigma, \bar{a}_\sigma^m \bar{b}_{\sigma'}^{q^{-n_\sigma}})$, since $\widetilde{f}(x, y)$ is a lift of $f_R(x, y)$ to $\mathcal{O}_F[x, y]$. □

Lemma 3.6. *If $v(p)$ is large enough, the conditions* (3.3) *and* (3.7) *are satisfied.*

Proof. There exists $s \in \mathbb{Z}_{\geq 1}$ such that the coefficients of all polynomials in (3.3) and (3.7) have the form: $p \cdot \beta_{R,m}^s \cdot a$ with $a \in \mathcal{O}_{\overline{F}}$ by Remark 3.2. Since the valuation of $v(\beta_{R,m})$ is independent of F, the claim follows. □

In the sequel, we assume that the conditions (3.3) and (3.7) are satisfied. Let F^{ur} denote the maximal unramified extension of F in $\overline{F}$.

Lemma 3.7. *The extension $F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m})/F$ is Galois.*

Proof. Let $L_0 := F^{\mathrm{ur}}(\alpha^m, \beta, \gamma)$ and $L := \widehat{L_0}$ be the completion of L_0. Let $\sigma \in G_F$. We note that $a_\sigma \in \mu_{d_R}(\overline{F}) \subset F^{\mathrm{ur}}$ by $p \nmid d_R$. Hence $\sigma(\alpha^m) = a_\sigma^m \alpha^m \in L_0$. We show $\sigma(\beta), \sigma(\gamma) \in L_0$. It suffices to prove

$$b_\sigma, c_\sigma \in L_0,$$

since

$$\sigma(\beta) = \frac{b_\sigma + \beta}{a_\sigma^m}, \quad \sigma(\gamma) = \gamma + c_\sigma + \widetilde{f}(\beta, b_\sigma)$$

by (3.5). As in the proof of Lemma 3.4, we have $(\widetilde{E}_R + \Delta)(b_\sigma) = 0$, $E(x) := (\widetilde{E}_R + \Delta)(x) \in \mathcal{O}_{L_0}[x]$ and $\deg E(x) = p^{2e}$. The equation $E(x) \equiv 0 \mod 0+$ has p^{2e} different roots. Thus by Hensel's lemma, $E(x) = 0$ has p^{2e} different roots in $\mathcal{O}_L$. Hence $b_\sigma \in L \cap \overline{F} = L_0$. As in the proof of Lemma 3.4, we have

$$f(c_\sigma) := c_\sigma^p - c_\sigma + \Delta_1(c_\sigma) - y = 0 \text{ with } y \in \mathcal{O}_{L_0},$$

where $f(x) \in \mathcal{O}_{L_0}[x]$ with $\deg f(x) = p$. We have $y \equiv b_\sigma \widetilde{R}(b_\sigma) \mod 0+$. The equation $f(x) \equiv x^p - x - y \equiv x^p - x - b_\sigma \widetilde{R}(b_\sigma) \equiv 0 \mod 0+$ has p different roots. By Hensel's lemma, $f(x) = 0$ has p different roots in $\mathcal{O}_L$. Hence $c_\sigma \in L \cap \overline{F} = L_0$. □

Definition 3.8. Let

$$d_{R,m} := \frac{d_R}{\gcd(d_R, m)}, \quad Q_{R,m} := \{(\alpha, \beta, \gamma) \in Q_R \mid \alpha \in \mu_{d_{R,m}}\}.$$

We have

$$F^{\mathrm{ur}} \subset F^{\mathrm{ur}}(\alpha_R^m) \subset F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}) \subset F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m}). \tag{3.10}$$

Using Definition 3.1 and $p \nmid d_{R,m}$, the first extension is a tamely ramified extension of degree $d_{R,m}$. According to Remark 3.2, the second and last extensions are totally ramified extensions of degree p^{2e} and p, respectively. Thus

$$[F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m}) : F^{\mathrm{ur}}] = d_{R,m} p^{2e+1}. \tag{3.11}$$

Lemma 3.9. (1) *The homomorphism $\Theta_{R,m,\varpi}$ in* (3.8) *induces the isomorphism*

$$W(F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m})/F) \xrightarrow{\sim} Q_{R,m} \rtimes \mathbb{Z}; \ \sigma \mapsto ((\bar{a}_\sigma^m, \bar{b}_\sigma, \bar{c}_\sigma), n_\sigma). \tag{3.12}$$

(2) *The homomorphism* $\Theta_{R,m,\varpi}$ *induces*

$$\mathrm{Gal}(F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m})/F^{\mathrm{ur}}) \xrightarrow{\sim} Q_{R,m},$$
$$\mathrm{Gal}(F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m})/F^{\mathrm{ur}}(\alpha_R^m)) \xrightarrow{\sim} H_R.$$

Proof. We use the same notation as in the proof of Lemma 3.4. Let

$$I := \mathrm{Gal}(F^{\mathrm{ur}}(\alpha^m, \beta, \gamma)/F^{\mathrm{ur}}) \supset P := \mathrm{Gal}(F^{\mathrm{ur}}(\alpha^m, \beta, \gamma)/F^{\mathrm{ur}}(\alpha^m))$$

and $\Theta\colon I \to Q_{R,m}$ be the restriction of (3.12). By the snake lemma, the assertion (1) is reduced to showing that Θ is an isomorphism. In order to show that Θ is an isomorphism, it suffices to show that Θ is injective according to (3.11) and $|Q_{R,m}| = d_{R,m}p^{2e+1}$. If Θ is injective, it follows that $\Theta|_P\colon P \to H_R$ is an isomorphism from $|P| = |H_R| = p^{2e+1}$.

We will now show that Θ is injective. Assume $\Theta(\sigma) = 1$ for $\sigma \in I$. We will show $\sigma = 1$. By the assumption, $\bar{a}_\sigma^m = 1$, $\bar{b}_\sigma = 0$ and $\bar{c}_\sigma = 0$. Recall (3.1). By $\bar{a}_\sigma^m = 1$ and $a_\sigma \in \mu_{d_R}(\overline{F})$ in (3.5), we have $a_\sigma^m = 1$ and $\sigma(\alpha^m) = \alpha^m$.

We recall the equality $\widetilde{E}_R(b_\sigma) + \Delta(b_\sigma) = 0$ in the proof of Lemma 3.4, where $\Delta(x) \in \mathfrak{p}[x]$ has no constant coefficient. We write $\widetilde{E}_R(x) + \Delta(x) = \sum_{i=1}^r c_i x^i \in \mathcal{O}[x]$. From $E'_R(0) \neq 0$ and $\Delta(x) \in \mathfrak{p}[x]$, it follows that $v(c_1) = 0$. We have $v(b_\sigma) > 0$ by $\bar{b}_\sigma = 0$. Thus, for an integer $2 \leq i \leq r$, we obtain $v(c_1 b_\sigma) = v(b_\sigma) < v(b_\sigma^i) \leq v(c_i b_\sigma^i)$. Hence $v(b_\sigma) = v(c_1 b_\sigma) = v(\widetilde{E}_R(b_\sigma) + \Delta(b_\sigma)) = \infty$. Hence $b_\sigma = 0$ and $\sigma(\beta) = \beta$.

By the last condition in (3.3) with $y = 0$,

$$\Lambda(x) := (\gamma + x)^p - \gamma^p - x^p \in \mathfrak{p}[x].$$

Definition 3.1 induces $\sigma(\gamma)^p - \sigma(\gamma) = \gamma^p - \gamma$. Thus $(\gamma + c_\sigma)^p - \gamma^p = c_\sigma$ and $c_\sigma^p + \Lambda(c_\sigma) = c_\sigma$. Since $\Lambda(x) \in \mathfrak{p}[x]$ has no constant coefficient, if $0 < v(c_\sigma) < \infty$, we have $v(c_\sigma^p + \Lambda(c_\sigma)) > v(c_\sigma)$, which can not occur. Hence $c_\sigma = 0$ and $\sigma(\gamma) = \gamma$. As a result, we obtain $\sigma = 1$. Thus Θ is injective. □

3.2. Galois representations associated to additive polynomials

3.2.1. Construction of Galois representation We assume that (3.3) and (3.7) are satisfied. If char F is positive, these are unconditional. If char F is zero, these conditions are satisfied if the absolute ramification index of F is large enough as in Lemma 3.6.

Definition 3.10. Let $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$. We define $\tau_{\psi,R,m,\varpi}$ to be the W_F-representation which is the inflation of the $Q_R \rtimes \mathbb{Z}$-representation $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ by $\Theta_{R,m,\varpi}$ in (3.8). For simplicity, we write $\tau_{\psi,R,m}$ for $\tau_{\psi,R,m,\varpi}$.

For a non-archimedean local field K, let I_K denote the inertia subgroup of K. Then Ker $\tau_{\psi,R,m}$ contains the open compact subgroup $I_{F(\alpha_R^m,\beta_{R,m},\gamma_{R,m})}$ by Lemma 3.9(1). According to Lemma 3.9(2) and Lemma 2.8(1), $\tau_{\psi,R,m}|_{I_{F(\alpha_R^m)}}$ is irreducible. Hence the representation $\tau_{\psi,R,m}$ is a smooth irreducible representation of W_F.

Let $G_F := \mathrm{Gal}(\overline{F}/F)$. We consider a general setting in the following lemma.

Lemma 3.11. *Let $\widetilde{\tau}$ be a continuous representation of G_F over $\overline{\mathbb{Q}}_\ell$ such that there exists an unramified continuous character ϕ of G_F such that $(\widetilde{\tau} \otimes \phi)(G_F)$ is finite. Assume that $\tau := \widetilde{\tau}|_{W_F}$ is irreducible. Then $\widetilde{\tau} \otimes \phi$ is primitive if and only if τ is primitive.*

Proof. Let $\widetilde{\tau}' := \widetilde{\tau} \otimes \phi$ and $\tau' := \tau \otimes \phi|_{W_F}$. The subgroup $\operatorname{Ker} \widetilde{\tau}'$ is open by $|G_F / \operatorname{Ker} \widetilde{\tau}'| < \infty$. Hence $\operatorname{Ker} \tau' \subset W_F$ is open. Therefore τ' is smooth. Hence so is τ. Since τ is irreducible and smooth, we have $\dim \tau < \infty$. We will show that $\widetilde{\tau}'$ is imprimitive if and only if τ is imprimitive.

First, assume an isomorphism $\widetilde{\tau}' \simeq \operatorname{Ind}_H^{G_F} \eta'$ with a proper subgroup H. We can check $\operatorname{Ker} \widetilde{\tau}' \subset H$. Hence H is open. Hence we can write $H = G_{F'}$ with a finite extension F'/F. Thus we obtain an isomorphism $\tau \simeq \operatorname{Ind}_{W_{F'}}^{W_F} (\eta'|_{W_{F'}} \otimes \phi^{-1}|_{W_{F'}})$.

To the contrary, assume $\tau \simeq \operatorname{Ind}_H^{W_F} \sigma$. In the same manner as above with replacing G_F by W_F, the subgroup H is an open subgroup of W_F of finite index by $\dim \tau < \infty$. Hence we can write $H = W_{F'}$ with a finite extension F'/F. Let $\sigma' := \sigma \otimes \phi|_{W_{F'}}$. We have $\tau' \simeq \operatorname{Ind}_{W_{F'}}^{W_F} \sigma'$. From Frobenius reciprocity, we have that $\sigma'(W_{F'}) \subset \tau'(W_F)$. By the assumption, the image $\sigma'(W_{F'})$ is finite. Hence the smooth $W_{F'}$-representation σ' extends to a smooth representation of $G_{F'}$, for which we write $\widetilde{\sigma}$ ([2, Proposition 28.6]). The restriction of $\operatorname{Ind}_{G_{F'}}^{G_F} \widetilde{\sigma}$ to W_F is isomorphic to $\operatorname{Ind}_{W_{F'}}^{W_F} \sigma' \simeq \tau'$. Both of $\operatorname{Ind}_{G_{F'}}^{G_F} \widetilde{\sigma}$ and $\widetilde{\tau}'$ are smooth irreducible G_F-representations whose restrictions to W_F are isomorphic to τ'. Hence we obtain an isomorphism $\widetilde{\tau}' \simeq \operatorname{Ind}_{G_{F'}}^{G_F} \widetilde{\sigma}$ as G_F-representations by [2, Lemma 28.6.2(2)]. □

We identify as $\operatorname{Gal}(\mathbb{F}/\mathbb{F}_q) \xrightarrow{\sim} \widehat{\mathbb{Z}}$, which sends the geometric Frobenius to 1. The group $\operatorname{Gal}(\mathbb{F}/\mathbb{F}_q)$ acts on $Q_{R,m}$ naturally. Then $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is regarded as a representation of $Q_{R,m} \rtimes \widehat{\mathbb{Z}}$. We identify as $\operatorname{Gal}(F^{\mathrm{ur}}/F) \xrightarrow{\sim} \operatorname{Gal}(\mathbb{F}/\mathbb{F}_q) \xrightarrow{\sim} \widehat{\mathbb{Z}}$, where the first isomorphism is the natural map. Let $\widehat{n} \colon G_F \xrightarrow{\text{rest.}} \operatorname{Gal}(F^{\mathrm{ur}}/F) \xrightarrow{\sim} \widehat{\mathbb{Z}}$ be the composite, which is an extension of $n \colon W_F \to \mathbb{Z};\ \sigma \mapsto n_\sigma$ in (3.4). Then we have

$$\widehat{\Theta}_{R,m,\varpi} \colon G_F \to Q_{R,m} \rtimes \widehat{\mathbb{Z}};\ \sigma \mapsto ((\bar{a}_\sigma^m, \bar{b}_\sigma, \bar{c}_\sigma), \widehat{n}_\sigma),$$

which is defined by the same formulas as in (3.5). Then $\widehat{\Theta}_{R,m,\varpi}$ extends $\Theta_{R,m,\varpi}$. By inflating $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ via $\widehat{\Theta}_{R,m,\varpi}$, we obtain a continuous representation of G_F, which we denote by $\widetilde{\tau}_{\psi,R,m}$.

We fix an isomorphism $\iota \colon \mathbb{C} \xrightarrow{\sim} \overline{\mathbb{Q}}_\ell$, and work with the choice of square root q in $\overline{\mathbb{Q}}_\ell$ given by $\iota(\sqrt{q})$.

Lemma 3.12. *The eigenvalues of Fr_q^* on $H_c^1(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ have the forms $\zeta\sqrt{q}$ with roots of unity ζ in $\overline{\mathbb{Q}}_\ell$. The automorphism Fr_q^* is semi-simple.*

Proof. As in [14, 2.3], it is well-known that a smooth projective geometrically connected curve X over $\mathbb{F}_q$ is supersingular if and only if all the eigenvalues of Fr_q^* on $H^1(X_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ have the form $\zeta\sqrt{q}$ with $\zeta \in \mu(\overline{\mathbb{Q}}_\ell)$. Hence the claim follows from Proposition 2.10. □

Let $\phi\colon G_F \to \overline{\mathbb{Q}}_\ell^\times$ be the unramified character sending a geometric Frobenius to $\sqrt{q}^{-1}$. The image of G_F by the twist $\widetilde{\tau}' := \widetilde{\tau}_{\psi,R,m} \otimes \phi$ is finite by Lemma 3.12.

By the isomorphism $\iota\colon \overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$, we obtain a continuous representation $\widetilde{\tau}'_{\mathbb{C}}$ of G_F over $\mathbb{C}$ by $\widetilde{\tau}'$. Then $\widetilde{\tau}'_{\mathbb{C}}$ is primitive if and only if $\widetilde{\tau}_{\psi,R,m}$ is primitive.

Corollary 3.13. *The W_F-representation $\tau_{\psi,R,m}$ is primitive if and only if the continuous G_F-representation $\widetilde{\tau}'_{\mathbb{C}}$ is primitive.*

Proof. Clearly $\widetilde{\tau}'_{\mathbb{C}}$ is primitive if and only if $\widetilde{\tau}'$ is primitive. We obtain the claim by applying Lemma 3.11 with $\widetilde{\tau} = \widetilde{\tau}_{\psi,R,m}$ and $\tau = \tau_{\psi,R,m}$. □

3.2.2. Swan conductor exponent In the sequel, we compute the Swan conductor exponent $\mathrm{Sw}(\tau_{\psi,R,m})$.

We simply write α, β, γ for $\alpha_R, \beta_{R,m}, \gamma_{R,m}$ in Definition 3.1, respectively. We consider the unramified field extension F_r/F of degree r such that $N := F_r(\alpha, \beta, \gamma)$ is Galois over F. Let $T := F_r(\alpha)$ and $M := T(\beta)$. Then we have

$$F \subset F_r \subset T \subset M \subset N.$$

Let L/K be a Galois extension of non-archimedean local fields with Galois group G. Let $\{G^i\}_{i \geq -1}$ denote the upper numbering ramification groups of G in [16, IV 3]. Let $\psi_{L/K}$ denote the Herbrand function of L/K.

Lemma 3.14. *Let $G := \mathrm{Gal}(N/F)$. Then we have*

$$\psi_{N/F}(t) = \begin{cases} t & \text{if } t \leq 0, \\ d_R t & \text{if } 0 < t \leq \frac{m}{d_R}, \\ p^{2e} d_R t - (p^{2e}-1)m & \text{if } \frac{m}{d_R} < t \leq \frac{p^e+1}{p^e}\frac{m}{d_R}, \\ p^{2e+1} d_R t - (p^e+1)(p^{e+1}-1)m & \text{otherwise} \end{cases}$$

and

$$G^i = \begin{cases} G & \text{if } i = -1, \\ \mathrm{Gal}(N/F_r) & \text{if } -1 < i \leq 0, \\ \mathrm{Gal}(N/T) & \text{if } 0 < i \leq \frac{m}{d_R}, \\ \mathrm{Gal}(N/M) & \text{if } \frac{m}{d_R} < i \leq \frac{p^e+1}{p^e}\frac{m}{d_R}, \\ \{1\} & \text{otherwise}. \end{cases}$$

Proof. Similarly as in (3.10), T/F is a totally ramified extension of degree d_R. We easily have

$$\psi_{T/F}(t) = \begin{cases} t & \text{if } t \leq 0, \\ d_R t & \text{otherwise}. \end{cases}$$

For a finite Galois extension L/K, let $\{\mathrm{Gal}(L/K)_u\}_{u \geq -1}$ be the lower numbering ramification subgroups. Let $1 \neq \sigma \in \mathrm{Gal}(M/T)$. Let $b_\sigma = \sigma(\beta) - \beta$ as before. We have $\widetilde{E}_R(\beta + b_\sigma) = \widetilde{E}_R(\beta)$ by the proof of Lemma 3.4. If $v(b_\sigma) > 0$, we obtain $b_\sigma = 0$ by the same arguments as in the proof of Lemma 3.9. This induces $\sigma = 1$.

Hence $v(b_\sigma) = 0$. From $v_M(\beta) = -m$, we obtain $v_M(\sigma(\varpi_M) - \varpi_M) = m + 1$. Thus

$$\mathrm{Gal}(M/T)_u = \begin{cases} \mathrm{Gal}(M/T) & \text{if } u \le m, \\ \{1\} & \text{otherwise,} \end{cases}$$
$$\psi_{M/T}(t) = \begin{cases} t & \text{if } t \le m, \\ p^{2e}t - (p^{2e} - 1)m & \text{otherwise.} \end{cases}$$

Let $1 \neq \sigma \in \mathrm{Gal}(N/M)$. If $v_N(\sigma(\gamma) - \gamma) > 0$, we obtain $\sigma(\gamma) = \gamma$ in the same way as the proof of Lemma 3.9. This implies that $\sigma = 1$. Hence $v_N(\sigma(\gamma) - \gamma) = 0$. Let ϖ_N be a uniformizer of N. From $v_N(\gamma^{-1}) = (p^e + 1)m$, it follows that $v_N(\sigma(\varpi_N) - \varpi_N) = (p^e + 1)m + 1$. Thus

$$\mathrm{Gal}(N/M)_u = \begin{cases} \mathrm{Gal}(N/M) & \text{if } u \le (p^e + 1)m, \\ \{1\} & \text{otherwise,} \end{cases}$$
$$\psi_{N/M}(t) = \begin{cases} t & \text{if } t \le (p^e + 1)m, \\ pt - (p - 1)(p^e + 1)m & \text{otherwise.} \end{cases}$$

Hence the former claim follows from $\psi_{N/F} = \psi_{N/M} \circ \psi_{M/T} \circ \psi_{T/F}$.

We can check

$$G_u = \begin{cases} G & \text{if } u = -1, \\ \mathrm{Gal}(N/F_r) & \text{if } -1 < u \le 0, \\ \mathrm{Gal}(N/T) & \text{if } 0 < u \le m, \\ \mathrm{Gal}(N/M) & \text{if } m < u \le (p^e + 1)m, \\ \{1\} & \text{otherwise} \end{cases}$$

by using the former claim and [16, Propositions 12(c), 13(c) and 15 in IV3]. Hence the latter claim follows from $G^i = G_{\psi_{N/F}(i)}$. □

Corollary 3.15. *We have $Sw(\tau_{\psi,R,m}) = m(p^e + 1)/d_R$.*

Proof. Before Corollary 3.13, it is stated that the twist $\tau_{\psi,R,m} \otimes \phi$ factors through a finite group $Q_R \rtimes (\mathbb{Z}/r\mathbb{Z}) \simeq \mathrm{Gal}(F_r(\alpha, \beta, \gamma)/F)$ with a certain integer r. Since ϕ is unramified, $\mathrm{Sw}(\tau_{\psi,R,m}) = \mathrm{Sw}(\tau_{\psi,R,m} \otimes \phi)$. It follows that $\mathrm{Sw}(\tau_{\psi,R,m} \otimes \phi) = m(p^e + 1)/d_R$ from Lemma 3.14 and [7, Théorème 7.7] ([16, Exercise 2 in 2VI]). □

3.3. Symplectic module associated to Galois representation

We simply write $\mathrm{PGL}(\overline{\mathbb{Q}}_\ell)$ for $\mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi])/\overline{\mathbb{Q}}_\ell^\times$. Let ρ denote the composite

$$W_F \xrightarrow{\tau_{\psi,R,m}} \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]) \xrightarrow{\text{can.}} \mathrm{PGL}(\overline{\mathbb{Q}}_\ell).$$

Namely, ρ is the projective representation associated to $\tau_{\psi,R,m}$. Similarly, let ρ' be the projective representation associated to $\widetilde{\tau}' = \widetilde{\tau}_{\psi,R,m} \otimes \phi$.

Lemma 3.16. *We have $\rho(W_F) = \rho'(G_F)$, which is finite.*

Proof. Since $\widetilde{\tau}'$ is a smooth irreducible G_F-representation, we have that $\widetilde{\tau}'(G_F) = (\tau_{\psi,R,m} \otimes \phi)(W_F)$ ([2, the proof of Lemma 2 in 28.6]). Thus the claim follows. □

Let F_ρ denote the kernel field of ρ and T_ρ the maximal tamely ramified extension of F in F_ρ. Let

$$H := \mathrm{Gal}(F_\rho/T_\rho) \subset G := \mathrm{Gal}(F_\rho/F).$$

The homomorphism ρ induces an injection $\bar{\rho} \colon G \to \mathrm{PGL}(\overline{\mathbb{Q}}_\ell)$.

Recall that $H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is regarded as a $Q_R \rtimes \mathbb{Z}$-representation as in 2. We have the subgroup $Q_{R,m} \rtimes \mathbb{Z} \subset Q_R \rtimes \mathbb{Z}$. Now we regard $H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ as a $Q_{R,m} \rtimes \mathbb{Z}$-representation. Let τ denote the composite

$$Q_{R,m} \rtimes \mathbb{Z} \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]) \to \mathrm{PGL}(\overline{\mathbb{Q}}_\ell).$$

From Definition 3.10 and Lemma 3.9(1), it follows that $\tau \circ \Theta_{R,m,\varpi} = \rho$. Let $i \colon H_R \hookrightarrow Q_{R,m} \rtimes \mathbb{Z}$ be the natural inclusion. Since $\tau \circ i$ equals $\bar{\rho}_\psi$ in Lemma 2.9, we obtain $\mathrm{Ker}(\tau \circ i) = Z(H_R)$ according to the lemma. Let V_R be as in Lemma 2.6. Then we have $\mathrm{pr} \colon H_R/Z(H_R) \xrightarrow{\sim} V_R;\ (1, \beta, \gamma)Z(H_R) \mapsto \beta$. Thus we have a commutative diagram

$$\begin{tikzcd}
W_F \arrow[rr, two heads] \arrow[d, two heads, "\Theta_{R,m,\varpi}"'] \arrow[rrrd, "\rho"] & & G \arrow[rd, hook, "\bar{\rho}"] & \\
Q_{R,m} \rtimes \mathbb{Z} \arrow[rrr, "\tau"] & & & \mathrm{PGL}(\overline{\mathbb{Q}}_\ell) \\
H_R \arrow[u, hook, "i"] \arrow[rrru, "\tau \circ i"] \arrow[r, "\text{can.}"'] & H_R/Z(H_R) \arrow[rru, hook] \arrow[rr, "\mathrm{pr}", "\simeq"'] & & V_R.
\end{tikzcd} \tag{3.13}$$

Lemma 3.17. *We have an isomorphism $\bar{\rho}(H) \simeq V_R$.*

Proof. Let $L := F^{\mathrm{ur}}(\alpha_R^m, \beta_{R,m}, \gamma_{R,m})$ and $K := F^{\mathrm{ur}}(\alpha_R^m)$. From Lemma 3.9, we recall

$$W(L/F) \simeq Q_{R,m} \rtimes \mathbb{Z}, \quad W(L/K) \simeq H_R.$$

The subfield K is the maximal tamely ramified extension of F in L. In the sequel, we freely use (3.13). From Lemma 3.9(1), it follows that $F_\rho \subset L$ and $T_\rho = F_\rho \cap K$. The homomorphism $\Theta_{R,m,\varpi}$ induces $G = W(F_\rho/F) \simeq W_F/\operatorname{Ker}\rho \xrightarrow{\sim} (Q_{R,m} \rtimes \mathbb{Z})/\operatorname{Ker}\tau$. Thus we have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \ker(\tau \circ i) \simeq W(L/F_\rho K) \arrow[r] \arrow[d, hook] & H_R \simeq W(L/K) \arrow[r, "\text{rest.}"] \arrow[d, hook] & H = W(F_\rho/T_\rho) \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & \ker\tau \simeq W(L/F_\rho) \arrow[r] & Q_{R,m} \rtimes \mathbb{Z} \simeq W(L/F) \arrow[r, "\text{rest.}"] & G = W(F_\rho/F) \arrow[r] & 1,
\end{tikzcd}$$

where the two horizontal sequences are exact. This induces that

$$H = \mathrm{Gal}(F_\rho/T_\rho) \simeq H_R/\operatorname{Ker}(\tau \circ i) = H_R/Z(H_R) \xrightarrow{\sim} V_R.$$

Since $\overline{\rho}$ is injective, the claim follows. □

Let

$$\mathscr{H}_0 := G/H = \mathrm{Gal}(T_\rho/F).$$

Let $\sigma \in \mathscr{H}_0$. We take a lifting $\widetilde{\sigma} \in G \twoheadrightarrow \mathscr{H}_0$ of σ. Let $\mathscr{H}_0$ act on H by $\sigma \cdot \sigma' := \widetilde{\sigma}\sigma'\widetilde{\sigma}^{-1}$ for $\sigma' \in H$. This is well-defined because H is abelian according to Lemma 3.17. We regard $H \simeq V_R$ as an $\mathbb{F}_p[\mathscr{H}_0]$-module.

By Lemma 3.12, we can take a positive integer r such that $r\mathbb{Z} \subset \mathrm{Ker}\,\tau$ and $x^{q^r} = x$ for $x \in \mu_{d_{R,m}}$. Let $\mathbb{Z}/r\mathbb{Z}$ act on $\mu_{d_{R,m}}$ by $1 \cdot x = x^{q^{-1}}$. We take a generator $\alpha \in \mu_{d_{R,m}}$. Let

$$\mathscr{H} := \mu_{d_{R,m}} \rtimes (\mathbb{Z}/r\mathbb{Z}) \xrightarrow{\sim} \left\langle \sigma, \tau \mid \sigma^r = 1,\ \tau^{d_{R,m}} = 1,\ \sigma\tau\sigma^{-1} = \tau^q \right\rangle, \tag{3.14}$$

where the isomorphism is given by $(\alpha, 0) \mapsto \tau$ and $(1, -1) \mapsto \sigma$. The groups $\mathscr{H}_0$ and $\mathscr{H}$ are supersolvable. We consider the commutative diagram

$$\begin{tikzcd}
Q_{R,m} \rtimes \mathbb{Z} \arrow[r] \arrow[d] & (Q_{R,m} \rtimes \mathbb{Z})/\,\mathrm{Ker}\,\tau \simeq G \arrow[d] \\
\mathscr{H} \simeq (Q_{R,m} \rtimes \mathbb{Z})/(H_R \rtimes r\mathbb{Z}) \arrow[r, "\varphi"] & (Q_{R,m} \rtimes \mathbb{Z})/(\mathrm{Ker}\,\tau \cdot H_R) \simeq \mathscr{H}_0,
\end{tikzcd}$$

where every map is canonical and surjective.

Lemma 3.18. *The elements $\varphi(\alpha, 0)$ and $\varphi(1, -1)$ in $\mathscr{H}_0$ act on $H \simeq V_R$ by $x \mapsto \alpha x$ and $x \mapsto x^q$ for $x \in V_R$, respectively.*

Proof. These are directly checked. □

We can regard V_R as an $\mathbb{F}_p[\mathscr{H}]$-module via φ. Let ω_R be as in Lemma 2.6(2).

Lemma 3.19. *We have $\omega_R(hx, hx') = \omega_R(x, x')$ for $h \in \mathscr{H}$.*

Proof. The claim for $h = \alpha$ follows from (2.4). For $h = (1, -1)$, the claim follows from $\omega_R(x^q, x'^q) = (f_R(x, x') - f_R(x', x))^q = f_R(x, x') - f_R(x', x) = \omega_R(x, x')$. □

Definition 3.20. Let G be a finite group. Let V be an $\mathbb{F}_p[G]$-module with $\dim_{\mathbb{F}_p} V < \infty$. Let $\omega \colon V \times V \to \mathbb{F}_p$ be a symplectic form. We say that the pair (V, ω) is *symplectic* if ω is non-degenerate and satisfies $\omega(gv, gv') = \omega(v, v')$ for $g \in G$ and $v, v' \in V$.

Lemma 3.21. *The $\mathbb{F}_p[\mathscr{H}]$-module (V_R, ω_R) is symplectic.*

Proof. The claim follows from Lemma 2.6(2) and Lemma 3.19. □

Definition 3.22. The $\mathbb{F}_p[\mathscr{H}_0]$-module (V_R, ω_R) is called a symplectic module associated to $\tau_{\psi,R,m}$.

Definition 3.23. Let $\sigma : \mathbb{F} \to \mathbb{F};\ x \mapsto x^q$. For $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$, we set $f^{\sigma}(x) := \sum_{i=0}^{n} \sigma(a_i)x^i$.

Let k be a field. We say that a polynomial $f(x) \in k[x]$ is reduced if the ring $k[x]/(f(x))$ is reduced. An additive polynomial $f(x) \in \mathscr{A}_{\mathbb{F}} \setminus \{0\}$ is reduced if and only if $f'(0) \neq 0$.

Lemma 3.24. *Let $E(x) \in \mathscr{A}_{\mathbb{F}}$ be a reduced polynomial. Let $V := \{\beta \in \mathbb{F} \mid E(\beta) = 0\}$.*

(1) *Assume that $E(x)$ is monic and V is stable under σ. Then we have $E(x) \in \mathbb{F}_q[x]$.*
(2) *Let r be a positive integer. Assume that V is stable under μ_r-multiplication. Then we have $E(\alpha x) = \alpha E(x)$ for $\alpha \in \mu_r$.*

Proof. We show (1). The assumption implies that $E^{\sigma}(\beta) = (E(\beta^{q^{-1}}))^q = 0$ for any $\beta \in V$. Since $E(x)$ is separable, there exists $\alpha \in \mathbb{F}^{\times}$ such that $E^{\sigma}(x) = \alpha E(x)$. Then $\alpha = 1$, because $E(x)$ is monic. Hence we have the claim.

We show (2). Let $\alpha \in \mu_r$. By the assumption, $E(\alpha\beta) = 0$ for any $\beta \in V$. Since $E(x)$ is separable, there exists a constant $c \in \mathbb{F}^{\times}$ such that $E(\alpha x) = cE(x)$. By considering the derivatives of $E(\alpha x)$, $cE(x)$ and substituting $x = 0$, we obtain $\alpha = c$ by $E'(0) \neq 0$. Hence the claim follows. □

Definition 3.25. Let $f(x) \in \mathscr{A}_q$.

(1) A decomposition $f(x) = f_1(f_2(x))$ with $f_i(x) \in \mathscr{A}_q$ is said to be *non-trivial* if $\deg f_i > 1$ for $i \in \{1, 2\}$.
(2) We say that $f(x) \in \mathscr{A}_q$ is *prime* if it does not admit a non-trivial decomposition $f(x) = f_1(f_2(x))$ with $f_i(x) \in \mathscr{A}_q$.

Definition 3.26. Let (V, ω) be a symplectic $\mathbb{F}_p[\mathscr{H}]$-module. Then (V, ω) is said to be *completely anisotropic* if V does not admit a non-zero totally isotropic proper $\mathbb{F}_p[\mathscr{H}]$-submodule.

For an $\mathbb{F}_p$-subspace $W \subset V$, let $W^{\perp} := \{v \in V \mid \omega(v, w) = 0 \text{ for all } w \in W\}$.

Proposition 3.27. *The symplectic $\mathbb{F}_p[\mathscr{H}]$-module (V_R, ω_R) is completely anisotropic if and only if there does not exist a non-trivial decomposition $E_R(x) = f_1(f_2(x))$ with $f_i(x) \in \mathscr{A}_q$ such that $f_2(\alpha x) = \alpha f_2(x)$ for $\alpha \in \mu_{d_{R,m}}$ and $V_{f_2} := \{\beta \in \mathbb{F} \mid f_2(\beta) = 0\}$ satisfies $V_{f_2} \subset V_{f_2}^{\perp}$.*

Proof. Assume that there exists such a decomposition $E_R(x) = f_1(f_2(x))$. Since the decomposition is non-trivial, we have $V_{f_2} \neq \{0\}$. Hence V_{f_2} is a non-zero totally isotropic proper $\mathbb{F}_p[\mathscr{H}]$-submodule of V_R. Thus V_R is not completely anisotropic.

Assume that V_R is not completely anisotropic. We take a non-zero totally isotropic $\mathbb{F}_p[\mathscr{H}]$-submodule $V' \subset V_R$. According to [13, 4 in Chap. 1], there exists a monic reduced polynomial $f(x) \in \mathscr{A}_{\mathbb{F}}$ such that $V' = \{\beta \in \mathbb{F} \mid f(\beta) = 0\}$. Since V' is stable by σ, we have $f(x) \in \mathbb{F}_q[x]$ by Lemma 3.24(1). Since V' is stable by τ, we have $f(\alpha x) = \alpha f(x)$ for $\alpha \in \mu_{d_{R,m}}$ from Lemma 3.18 and Lemma 3.24(2). There exist $f_1(x), r(x) \in \mathscr{A}_q$ such that $E_R(x) = f_1(f(x)) + r(x)$ and

$\deg r(x) < \deg f(x)$ according to [13, Theorem 1]. For any root $\beta \in V'$ of $f(x)$, we have $r(\beta) = 0$ from $E_R(\beta) = 0$. Since $f(x)$ is separable, $r(x)$ is divisible by $f(x)$. Hence $\deg r(x) < \deg f(x)$ induces $r(x) \equiv 0$. From definition, we obtain $V' \subset V'^{\perp}$. Thus the converse is shown. □

Corollary 3.28. (1) *The W_F-representation $\tau_{\psi,R,m}$ is primitive if and only if the symplectic $\mathbb{F}_p[\mathscr{H}]$-module (V_R, ω_R) is completely anisotropic.*

(2) *The W_F-representation $\tau_{\psi,R,m}$ is primitive if and only if there does not exist a non-trivial decomposition $E_R(x) = f_1(f_2(x))$ with $f_i(x) \in \mathscr{A}_q$ such that $f_2(\alpha x) = \alpha f_2(x)$ for $\alpha \in \mu_{d_{R,m}}$ and $V_{f_2} := \{\beta \in \mathbb{F} \mid f_2(\beta) = 0\}$ satisfies $V_{f_2} \subset V_{f_2}^{\perp}$.*

(3) *If $E_R(x) \in \mathscr{A}_q$ is prime, the W_F-representation $\tau_{\psi,R,m}$ is primitive.*

(4) *If $R(x) = a_e x^{p^e}$ and $\mathbb{F}_p(\mu_{d_{R,m}}) = \mathbb{F}_{p^{2e}}$, the $\mathbb{F}_p[\mathscr{H}]$-module V_R is irreducible. The W_F-representation $\tau_{\psi,R,m}$ is primitive. If $\gcd(p^e+1, m) = 1$, the condition $\mathbb{F}_p(\mu_{d_{R,m}}) = \mathbb{F}_{p^{2e}}$ is satisfied.*

Proof. The claim (1) follows from Corollary 3.13, Lemma 3.17, and [11, Theorem 4.1].

The claim (2) follows from (1) and Proposition 3.27. The claim (3) follows from (2) immediately.

We show (4). We assume that there exists a non-zero $\mathbb{F}_p[\mathscr{H}]$-submodule $W \subset V_R = \{\beta \in \mathbb{F} \mid (a_e x^{p^e})^{p^e} + a_e x = 0\}$. We take a non-zero element $\beta \in W$. Then $\mathbb{F}_p(\mu_{d_{R,m}}) = \mathbb{F}_{p^{2e}}$ implies $\mathbb{F}_{p^{2e}}\beta = \mathbb{F}_p(\mu_{d_{R,m}})\beta \subset W$. Since V_R is the set of the roots of a separable polynomial $E_R(x)$ of degree p^{2e}, we have $|V_R| = p^{2e}$. Hence $W = V_R = \mathbb{F}_{p^{2e}}\beta$. Thus the first claim follows. The second claim follows from the first one and [11, Theorem 4.1]. If $\gcd(p^e + 1, m) = 1$, we have $d_{R,m} = d_R = p^e + 1$. Hence the third claim follows from $\mathbb{F}_p(\mu_{p^e+1}) = \mathbb{F}_{p^{2e}}$. □

Example 3.29. For a positive integer s, we consider the set

$$\mathcal{A}_{q,s} := \left\{ \varphi(x) \in \mathbb{F}_q[x] \,\middle|\, \varphi(x) = \sum_{i=0}^{n} c_i x^{p^{si}} \right\},$$

which is regarded as a ring with multiplication $\varphi_1 \circ \varphi_2 := \varphi_1(\varphi_2(x))$ for $\varphi_1, \varphi_2 \in \mathcal{A}_{q,s}$. The number of prime elements in $\mathcal{A}_{q,s}$ in the sense of Definition 3.25(2) is calculated in [4] and [12]. We will review this now.

In the following, we give examples such that $E_R(x)$ is prime. We write $d_R = p^t + 1$ with $t \geq 0$. Then $E_R \in \mathcal{A}_{q,t}$. We write $q = p^f$. Assume $f \mid t$. We have

$$E_R(x) = \sum_{i=0}^{e} a_i x^{p^{e+i}} + \sum_{i=0}^{e} a_i x^{p^{e-i}}. \tag{3.15}$$

Because of $f \mid t$, we have the ring isomorphism $\Phi \colon \mathcal{A}_{q,t} \xrightarrow{\sim} \mathbb{F}_q[y];\ \sum_{i=0}^{r} c_i x^{p^{ti}} \mapsto \sum_{i=0}^{r} c_i y^i$, where $\mathbb{F}_q[y]$ is a usual polynomial ring. The polynomial $E_R(x) \in \mathscr{A}_q$ is prime if and only if $\Phi(E_R(x))$ is irreducible in $\mathbb{F}_q[y]$ in a usual sense. Recall that a polynomial $\sum_{i=0}^{r} c_i y^i \in \mathbb{F}_q[y]$ is said to be reciprocal if $c_i = c_{r-i}$ for $0 \leq i \leq r$.

Via (3.15), we know that $\Phi(E_R(x))$ is a reciprocal polynomial. The number of the monic irreducible reciprocal polynomials is calculated in [3, Theorems 2 and 3].

In general, we do not know a necessary and sufficient condition on $R(x)$ for $E_R(x)$ to be prime.

Proposition 3.30. *Assume $d_{R,m} \in \{1, 2\}$. There exists an unramified finite extension F'/F such that $\tau_{\psi,R,m}|_{W_{F'}}$ is imprimitive.*

Proof. We take a non-zero element $\beta \in V_R$. Let t be the positive integer such that $\mathbb{F}_{q^t} = \mathbb{F}_q(\beta)$. Let $\mathscr{H}_t \subset \mathscr{H}$ be the subgroup generated by σ^t, τ. Since $d_{R,m} \leq 2$, according to Lemma 3.18, τ acts on V_R as multiplication by sign. Thus the subspace $W_R := \mathbb{F}_p\beta \subset V_R$ is an $\mathbb{F}_p[\mathscr{H}_t]$-submodule, since σ^t acts on W_R trivially. From Lemma 2.6(2), it follows that $\omega_R(\zeta\beta, \zeta'\beta) = \zeta\zeta'\omega_R(\beta, \beta) = 0$ for any $\zeta, \zeta' \in \mathbb{F}_p$. Thus W_R is a totally isotropic proper $\mathbb{F}_p[\mathscr{H}_t]$-submodule of V_R. Hence V_R is not a completely anisotropic $\mathbb{F}_p[\mathscr{H}_t]$-module. Let F_t/F be the unramified extension of degree t in $\overline{F}$. Then $\tau_{\psi,R,m}|_{W_{F_t}}$ is imprimitive by [11, Theorem 4.1]. □

Lemma 3.31. *The W_{T_ρ}-representation $\tau_{\psi,R,m}|_{W_{T_\rho}}$ is imprimitive.*

Proof. We take a non-zero element $\beta \in V_R$. Then $\mathbb{F}_p\beta$ is a totally isotropic symplectic submodule of the symplectic module V_R associated to $\tau_{\psi,R,m}|_{W_{T_\rho}}$. Hence $\tau_{\psi,R,m}|_{W_{T_\rho}}$ is imprimitive by Corollary 3.28(1). □

3.4. Root system associated to irreducible $\mathbb{F}_p[\mathscr{H}]$-module

A root system associated to an irreducible $\mathbb{F}_p[\mathscr{H}]$-module is defined in [11]. We determine the root system associated to V_R in the situation of Corollary 3.28(4).

We recall the definition of a root system.

Definition 3.32. ([11, 7])

(1) Let Φ be the group of the automorphisms of the torus $(\mathbb{F}^\times)^2$ generated by the automorphisms $\theta \colon (\alpha, \beta) \mapsto (\alpha^p, \beta^p)$ and $\sigma \colon (\alpha, \beta) \mapsto (\alpha^{q^{-1}}, \beta)$. A Φ-orbit of $(\mathbb{F}^\times)^2$ is called a *root system*.

(2) Let $W = \Phi(\alpha, \beta)$ be a root system. Let

$$a = a(W) \text{ be the minimal positive integer with } \alpha^{q^a} = \alpha,$$
$$b = b(W) \text{ the minimal positive integer with} \alpha^{p^b} = \alpha^{q^x}, \beta^{p^b} = \beta \text{ with } x \in \mathbb{Z}, \text{ and}$$
$$c = c(W) \text{ the minimal non-negative integer with } \alpha^{p^b} = \alpha^{q^c}.$$

Let $e' = e'(W)$ and $f' = f'(W)$ be the orders of α and β, respectively. These integers are independent of (α, β) in W.

(3) Let $\mathscr{H}_{d,r} := \langle \sigma, \tau \mid \tau^d = 1,\ \sigma^r = 1,\ \sigma\tau\sigma^{-1} = \tau^q \rangle$ with $q^r \equiv 1 \pmod{d}$.

(4) We say that a root system W *belongs to* $\mathscr{H}_{d,r}$ if $e' \mid d$ and $af' \mid r$.

(5) Let $W = \Phi(\alpha, \beta)$ be a root system which belongs to $\mathscr{H}_{d,r}$. Let $\overline{M(W)}$ be the $\mathbb{F}$-module with the basis

$$\{\theta^i \sigma^j m \mid 0 \leq i \leq b-1,\ 0 \leq j \leq a-1\}$$

and with the action of $\mathscr{H}$ by

$$\tau m = \alpha m, \quad \sigma^a m = \beta m, \quad \theta^b m = \sigma^{-c} m.$$

Theorem 3.33. *([11, Theorems 7.1 and 7.2])*

(1) *There exists an irreducible $\mathbb{F}_p[\mathscr{H}_{d,r}]$-module $M(W)$ such that $M(W) \otimes_{\mathbb{F}_p} \mathbb{F}$ is isomorphic to $\overline{M(W)}$ as $\mathbb{F}[\mathscr{H}_{d,r}]$-modules.*

(2) *The map $W \mapsto M(W)$ defines a one-to-one correspondence between the set of root systems belonging to $\mathscr{H}_{d,r}$ and the set of isomorphism classes of irreducible $\mathbb{F}_p[\mathscr{H}_{d,r}]$-modules.*

We go back to the original situation. Assume that $R(x) = a_e x^{p^e}$ and $\mathbb{F}_p(\mu_{d_{R,m}}) = \mathbb{F}_{p^{2e}}$. Let $\mathscr{H}$ be as in (3.14). In the above notation, we have $\mathscr{H} = \mathscr{H}_{d_{R,m},r}$. As in Corollary 3.28(4), the $\mathbb{F}_p[\mathscr{H}]$-module V_R is irreducible.

Proposition 3.34. *We write $q = p^f$. Let $e_1 := \gcd(f, 2e)$ and $\beta := \mathrm{Nr}_{q/p^{e_1}}(-a_e^{-(p^e-1)})$. Let $\alpha \in \mu_{d_{R,m}}$ be a primitive $d_{R,m}$-th root of unity. We consider the root system $W := \Phi(\alpha, \beta)$.*

(1) *We have $a(W) = 2e/e_1$ and $b(W) = e_1$. Further, $c(W)$ is the minimal non-negative integer such that $fc(W) \equiv e_1 \pmod{2e}$.*

(2) *The root system W belongs to $\mathscr{H}$.*

(3) *We have an isomorphism $V_R \simeq M(W)$ as $\mathbb{F}_p[\mathscr{H}]$-modules.*

Proof. We show (1). We simply write a, b, c for $a(W), b(W), c(W)$, respectively. By definition, a is the minimal natural integer such that $\alpha^{q^a} = \alpha$. Because of $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{2e}}$, a is the minimal positive integer satisfying $fa \equiv 0 \pmod{2e}$. Thus we obtain $a = 2e/e_1$.

From definition, b is the minimal natural integer such that $\alpha^{p^b} = \alpha^{q^x}$ with some integer x and $\beta^{p^b} = \beta$. The first condition implies that $fx \equiv b \pmod{2e}$. Hence b is divisible by e_1. The congruence $fx \equiv e_1 \pmod{2e}$ has a solution x and $\beta \in \mathbb{F}_{p^{e_1}}$ means $\beta^{p^{e_1}} = \beta$. Thus $b = e_1$.

By definition, c is the minimal non-negative integer such that $\alpha^{p^b} = \alpha^{q^c}$. This is equivalent to $e_1 = b \equiv fc \pmod{2e}$. We have shown (1).

We show (2). The order e' of α equals $d_{R,m}$. Let f' be the order of β. It suffices to show $af' \mid r$. By the choice of r, we have $\alpha^{q^r} = \alpha$. Hence $2e \mid fr$, since $\mathbb{F}_{p^{2e}} = \mathbb{F}_p(\alpha)$ and $a \mid r$. These imply that $\mathbb{F}_{p^{2e}} \subset \mathbb{F}_{q^a} \subset \mathbb{F}_{q^r}$.

Let $\eta \in V_R \setminus \{0\}$. Using $\eta^{p^{2e}} = -a_e^{-(p^e-1)}\eta$, $a_e \in \mathbb{F}_q^\times$ and $2e \mid fr$, we compute

$$\eta^{q^r} = (\eta^{p^{2e}-1})^{\frac{q^r-1}{p^{2e}-1}}\eta = \mathrm{Nr}_{q^r/p^{2e}}(-a_e^{-(p^e-1)})\eta = \mathrm{Nr}_{q^a/p^{2e}}(-a_e^{-(p^e-1)})^{r/a}\eta. \tag{3.16}$$

The restriction map $\mathrm{Gal}(\mathbb{F}_{q^a}/\mathbb{F}_{p^{2e}}) \to \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{p^{e_1}})$ is an isomorphism because of $a = 2e/e_1$. Since $a_e \in \mathbb{F}_q^\times$, we have $\mathrm{Nr}_{q^a/p^{2e}}(-a_e^{-(p^e-1)}) = \beta$. Hence $\eta^{q^r} = \beta^{r/a}\eta$ by (3.16). Since $\eta^{q^r} = \eta$ by Lemma 3.18 and Definition 3.32(3), we obtain $\beta^{r/a} = 1$. Thus $f' \mid (r/a)$.

We show (3). Let $\eta \in V_R \setminus \{0\}$. Similarly to (3.16), we have $\sigma^a\eta = \eta^{q^a} = \beta\eta$. From Lemma 3.18, we have $\tau\eta = \alpha\eta$. The $\mathbb{F}_p[\mathscr{H}]$-module V_R satisfies the assumption in [11, Lemma 7.3] by (2). Hence [11, Lemma 7.3] induces $\{0\} \neq M(W) \subset V_R$. Since V_R is irreducible as in Corollary 3.28(4), we obtain $M(W) = V_R$. □

A necessary and sufficient condition for an irreducible $\mathbb{F}_p[\mathscr{H}]$-module to have a symplectic form is determined in [11, Theorem 8.1]. We recall the result.

Theorem 3.35. *([11, Theorem 8.1]) Let $W = \Phi(\alpha, \beta)$ be a root system. The irreducible $\mathbb{F}_p[\mathscr{H}]$-module $M(W)$ has a symplectic form if and only if*

(A) $a(W) \equiv 0 \pmod 2$, $\alpha \in \mu_{q^{a(W)/2}+1}$ *and* $\beta = -1$,
(B) $b(W), c(W) \equiv 0 \pmod 2$, $\alpha \in \mu_{p^{b(W)/2}+q^{c(W)/2}}$ *and* $\beta \in \mu_{p^{b(W)/2}+1}$, *or*
(C) $b(W) \equiv 0 \pmod 2$, $c(W) \equiv a(W) \pmod 2$, $\alpha \in \mu_{p^{b(W)/2}+q^{(a(W)+c(W))/2}}$ *and* $\beta \in \mu_{p^{b(W)/2}+1}$.

There are two isomorphism classes of symplectic structures on $M(W)$ in the case A, $p \neq 2$ and one in all other cases.

Lemma 3.36. *Let W be as in Proposition 3.34. Let $v_2(\cdot)$ denote the 2-adic valuation on $\mathbb{Q}$.*

(1) *Assume $v_2(e) \geq v_2(f)$. Then the module $M(W)$ is of type A in Theorem 3.35.*
(2) *Assume $v_2(e) < v_2(f)$. Then we have $a(W) \equiv 1 \pmod 2$, $b(W) \equiv 0 \pmod 2$ and $(b(W)/2) \mid e$. Hence we have $\beta \in \mu_{p^{b(W)/2}+1}$.*
 (i) *If $c(W) \equiv 0 \pmod 2$, the module $M(W)$ is of type B in Theorem 3.35.*
 (ii) *If $c(W) \equiv 1 \pmod 2$, the module $M(W)$ is of type C in Theorem 3.35.*

Proof. We show (1). Recall that $e_1 = \gcd(f, 2e)$ and $\beta = \mathrm{Nr}_{q/p_1}(-a_e^{-(p^e-1)})$. We have $e_1 \mid e$, $a(W) = 2e/e_1 \equiv 0 \pmod 2$ and $f/e_1 \equiv 1 \pmod 2$. From $(p^{e_1}-1) \mid (p^e-1)$, it follows that

$$\beta = (-1)^{\frac{f}{e_1}} \left(a_e^{-\frac{p^e-1}{p^{e_1}-1}}\right)^{q-1} = -1,$$

where we use $a_e \in \mathbb{F}_q^\times$ for the last equality. By $fa(W)/2 = fe/e_1$ and $q = p^f$, we have $q^{a(W)/2} = p^{fe/e_1}$. Since fe/e_1 is divisible by e and f/e_1 is odd, $d_{R,m} \mid (p^e+1) \mid p^{fe/e_1}+1 = q^{a(W)}+1$. Hence we obtain $\alpha \in \mu_{q^{a(W)/2}+1}$. Thus the claim follows.

We show (2). Recall $b(W) = e_1$. The former claims are clear. Since $(e_1/2) \mid e$, we have $(p^{e_1/2}-1) \mid (p^e-1)$. From the definition of β and $a_e \in \mathbb{F}_q^\times$, it follows that

$$\beta^{p^{\frac{e_1}{2}}+1} = \left(a_e^{-\frac{p^e-1}{p^{e_1/2}-1}}\right)^{q-1} = 1.$$

Hence $\beta \in \mu_{p^{b(W)/2}+1}$. Assume that $c(W)$ is even. We write $(c(W)/2)f = (e_1/2) + le$ with $l \in \mathbb{Z}$ by Proposition 3.34(1). Then l is odd by $e_1 = \gcd(f, 2e)$. Thus $(p^e + 1) \mid (p^{le} + 1)$. This induces that $\alpha \in \mu_{p^{b(W)/2}+q^{c(W)/2}}$. Hence (2)(i) follows. The remaining claim is shown similarly. □

3.4.1. Künneth formula and primary module **Classification results in** [11] We recall classification results on completely anisotropic symplectic modules given in [11] restricted to the case $p \neq 2$.

Theorem 3.37. *([11, Theorem 9.1]) Let $(V, \omega) = \bigoplus_{i=1}^{n}(V_i, \omega_i)$ be a direct sum of irreducible symplectic $\mathbb{F}_p[\mathscr{H}]$-modules. Assume that $p \neq 2$. Then (V, ω) is completely anisotropic if and only if, for each isomorphism class, the modules of type B or C occur at most once and of type A at most twice among $V_1, \ldots, V_n$.*

Assume that $p \neq 2$. Let $(M(W), 0)$ denote the unique symplectic module on $M(W)$ which is of type B or C by Theorem 3.35. Let $(M(W), 0)$, $(M(W), 1)$ denote the two symplectic modules on $M(W)$ in the case where $p \neq 2$ and $M(W)$ is of type A. We denote by $(M(W), 2)$ the completely anisotropic symplectic module on $M(W) \oplus M(W)$, where $M(W)$ is of type A.

Theorem 3.38. *([11, Theorem 8.2]) Each completely anisotropic symplectic $\mathbb{F}_p[\mathscr{H}]$-module is isomorphic to one and only one symplectic module of the form*

$$\bigoplus_{i=1}^{n}(M(W_i), \nu_i),$$

where $W_1, \ldots, W_n$ are mutually different root systems belonging to $\mathscr{H}$.

Let k be a positive integer. Let $R := \{R_i\}_{1 \le i \le k}$ with $R_i \in \mathscr{A}_q$. We consider the k-dimensional affine smooth variety X_R defined by

$$a^p - a = \sum_{i=1}^{k} x_i R_i(x_i)$$

in $\mathbb{A}^{k+1}_{\mathbb{F}_q}$. The product group $Q_R := Q_{R_1} \times \cdots \times Q_{R_k}$ acts on X_R naturally similarly as (2.7). Let $\mathbb{Z}$ act on Q_R naturally. Let $\psi \in \mathbb{F}_p^{\vee} \setminus \{1\}$. We regard $H_c^k(X_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ as a $Q_R \rtimes \mathbb{Z}$-representation. Let the notation be as in (3.5). Let $m = \{m_i\}_{1 \le i \le k}$, where m_i is a positive integer. We have the homomorphism

$$\Theta_{R,m,\varpi} : W_F \to Q_R \rtimes \mathbb{Z};\ \sigma \mapsto ((a_{R_i,\sigma}^{m_i}, b_{R_i,\sigma}, c_{R_i,\sigma})_{1 \le i \le k}, n_\sigma). \quad (3.17)$$

Definition 3.39. We define a smooth W_F-representation $\tau_{\psi,R,m}$ to be the inflation of the $Q_R \rtimes \mathbb{Z}$-representation $H_c^k(X_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ by $\Theta_{R,m,\varpi}$.

Lemma 3.40. *We have an isomorphism $\tau_{\psi,R,m} \simeq \bigotimes_{i=1}^{k} \tau_{\psi,R_i,m_i}$ as W_F-representations.*

Proof. Let $Q_{R_i,\mathbb{Z}} := Q_{R_i} \rtimes \mathbb{Z}$ and $\Theta_{R_i,m_i,\varpi}\colon W_F \to Q_{R_i,\mathbb{Z}}$ be as in (3.8). Let

$$\delta'\colon Q_R \rtimes \mathbb{Z} \to Q_{R_1,\mathbb{Z}} \times \cdots \times Q_{R_k,\mathbb{Z}};\ ((g_i)_{1\leq i\leq k}, n) \mapsto (g_i, n)_{1\leq i\leq k}.$$

Each $H_{\mathrm{c}}^1(C_{R_i,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is regarded as a $Q_{R_i,\mathbb{Z}}$-representation. Via the Künneth formula, we have an isomorphism $H_{\mathrm{c}}^k(X_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi] \simeq \bigotimes_{i=1}^k (H_{\mathrm{c}}^1(C_{R_i,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi])$ as $Q_R \rtimes \mathbb{Z}$-representations, where the right hand side is regarded as a $Q_R \rtimes \mathbb{Z}$-representation via δ'. We consider the commutative diagram

$$\begin{tikzcd}
W_F \arrow[r, "\delta"] \arrow[d, "\Theta_{R,m,\varpi}"'] & W_F^k \arrow[d, "\Theta_{R_1,m_1,\varpi}\times\cdots\times\Theta_{R_k,m_k,\varpi}"] \\
Q_R \rtimes \mathbb{Z} \arrow[r, "\delta'"] & Q_{R_1,\mathbb{Z}} \times \cdots \times Q_{R_k,\mathbb{Z}},
\end{tikzcd}$$

where δ is the diagonal map. Hence the claim follows. □

Remark 3.41. Let $+\colon \prod_{i=1}^k Z(Q_{R_i}) \to \mathbb{F}_p;\ (1, 0, \gamma_i)_{1\leq i\leq k} \mapsto \sum_{i=1}^k \gamma_i$ and $\overline{Q}_R := Q_R/\operatorname{Ker}+$. The action of $Q_R \rtimes \mathbb{Z}$ on $H_{\mathrm{c}}^k(X_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ factors through $\overline{Q}_R \rtimes \mathbb{Z}$. Let $\overline{H}_R$ denote the image of $H_{R_1} \times \cdots \times H_{R_k}$ under $Q_R \to \overline{Q}_R$. The group $\overline{H}_R$ is an extra-special p-group. The quotient $\overline{H}_R/Z(\overline{H}_R)$ is isomorphic to $\bigoplus_{i=1}^k V_{R_i}$. Moreover, $\overline{Q}_R/\overline{H}_R$ is supersolvable.

Lemma 3.42. *The W_F-representation $\tau_{\psi,R,m}$ is irreducible.*

Proof. The $\overline{H}_R$-representation $H_{\mathrm{c}}^k(X_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ is irreducible by [8, 16.14(2) Satz]. The claim follows from this. □

Let ρ_{ψ,R_i,m_i} denote the projective representation associated to τ_{ψ,R_i,m_i}. Let F_i denote the kernel field of ρ_{ψ,R_i,m_i} and T_i the maximal tamely ramified extension of F in F_i. The field T_i is called the tame kernel field of ρ_{ψ,R_i,m_i}. Let $F_R := F_1 \cdots F_k$.

Lemma 3.43. *Let $\rho_{\psi,R,m}$ be the projective representation associated to $\tau_{\psi,R,m}$. The kernel field of $\rho_{\psi,R,m}$ is F_R.*

Proof. By Lemma 3.40, we can check $\operatorname{Ker}\rho_{\psi,R,m} = \bigcap_{i=1}^k \operatorname{Ker}\rho_{\psi,R_i,m_i}$. The claim follows from this. □

Let T_R be the maximal tamely ramified extension of F in F_R. We have the restriction map $V_R \hookrightarrow \prod_{i=1}^k \operatorname{Gal}(F_i/T_i) \simeq \bigoplus_{i=1}^k V_{R_i}$. Then $V_R := \operatorname{Gal}(F_R/T_R)$ has a bilinear form stable under the action of $\mathbb{F}_p[\operatorname{Gal}(T_R/F)]$ ([11, 4]). The form on V_R is given by $\omega_R := \sum_{i=1}^k \omega_{R_i}$.

Let ω_{R_i} be the form on V_{R_i} in Lemma 2.6(2). We give a recipe to make an example of $(M(W), 2)$ below.

Proposition 3.44. *Assume $k = 2$. Let $R_i(x) = a_{e,i}x^{p^e} \neq 0$ for $i \in \{1, 2\}$. Assume*

$$m_1 \neq m_2, \quad d := d_{R_1,m_1} = d_{R_2,m_2}.$$

(1) *We have an isomorphism* $V_R \simeq V_{R_1} \oplus V_{R_2}$.
(2) *We have* $T_R = T_1 \cdot T_2$.
(3) *Assume that* $p \neq 2$, $v_2(e) \geq v_2(f)$ *and* $\mathbb{F}_p(\mu_d) = \mathbb{F}_{p^{2e}}$. *If* (V_R, ω_R) *is completely anisotropic as a symplectic* $\mathbb{F}_p[\mathrm{Gal}(T_R/F)]$*-module,* V_R *is isomorphic to a primary module* $(M(W), 2)$ *with a root system* W.

Proof. Via Lemma 2.9 and Lemma 3.12, there exists an unramified finite extension E of F such that $F_i \subset E(\alpha_{R_i}^{m_i}, \beta_{R_i,m_i})$ for $i = 1, 2$ and $E(\alpha_{R_i}^{m_i}, \beta_{R_i,m_i})/E$ is Galois. We put $T := E(\alpha_{R_i}^{m_i}) = E(\varpi^{1/d})$ and $E_i := T(\beta_{R_i,m_i})$ for $i = 1, 2$. Let $n_i := m_i d/d_R = m_i/\gcd(d_R, m_i)$. Let $\{\mathrm{Gal}(E_i/T)^v\}_{v \geq -1}$ be the upper numbering ramification subgroups of $\mathrm{Gal}(E_i/T)$. Similarly as the proof of Lemma 3.14, we have

$$\mathrm{Gal}(E_i/T)^v = \begin{cases} \mathrm{Gal}(E_i/T) & \text{if } v \leq n_i, \\ \{1\} & \text{if } v > n_i. \end{cases}$$

Let $H := E_1 \cap E_2$. Since E_i/T is Galois, so is H/T. By [16, Proposition 14 in IV3], the subgroup $\mathrm{Gal}(H/T)^v$ equals $\mathrm{Gal}(H/T)$ if $v \leq n_i$ and $\{1\}$ if $v > n_i$. Hence we conclude $\mathrm{Gal}(H/T) = \{1\}$ by $n_1 \neq n_2$. We obtain $H = T$. Thus we have an isomorphism $\mathrm{Gal}(E_1E_2/T) \simeq \mathrm{Gal}(E_1/T) \times \mathrm{Gal}(E_2/T) \simeq V_{R_1} \oplus V_{R_2}$. The extension E_1E_2/T is totally ramified and the degree is p-power. Hence, T is the maximal tamely ramified extension of E in $E_1 \cdot E_2$. Therefore, $T_R = F_R \cap T$. We have the commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(E_1E_2/T) \arrow[r, "\simeq"] \arrow[d] & \mathrm{Gal}(E_1/T) \times \mathrm{Gal}(E_2/T) \arrow[d, "\simeq"] \\
\mathrm{Gal}(F_R/T_R) \arrow[r, "g"] & \mathrm{Gal}(F_1/T_1) \times \mathrm{Gal}(F_2/T_2),
\end{tikzcd}$$

where every map is the restriction map. The right vertical isomorphism follows from Lemma 3.17. Clearly g is injective. The commutative diagram implies that g is bijective. Hence we obtain (1).

We have the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(F_R/T_R) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Gal}(F_R/F) \arrow[r] \arrow[d, "g_1"] & \mathrm{Gal}(T_R/F) \arrow[r] \arrow[d, "g_2"] & 1 \\
1 \arrow[r] & V_{R_1} \oplus V_{R_2} \arrow[r] & \mathrm{Gal}(F_1/F) \times \mathrm{Gal}(F_2/F) \arrow[r] & \mathrm{Gal}(T_1/F) \times \mathrm{Gal}(T_2/F) \arrow[r] & 1,
\end{tikzcd}$$

where the two horizontal sequences are exact. Since g_1 is injective, so is g_2. Hence $T_R = T_1T_2$.

We show (3). Let $r := [E : F]$ and $\mathscr{H}_{d,r} := \mu_d \rtimes (\mathbb{Z}/r\mathbb{Z})$ as in (3.14). We identify $\mathrm{Gal}(T/F)$ with $\mathscr{H}_{d,r}$. Since $T_R \subset T$, the V_R, V_{R_i} are naturally regarded as $\mathbb{F}_p[\mathscr{H}_{d,r}]$-modules. Let α be a primitive d-th root of unity. Let $W := \Phi(\alpha, -1)$. Then we have an isomorphism $V_{R_i} \simeq M(W)$ as $\mathbb{F}_p[\mathscr{H}_{d,r}]$-modules and know that V_{R_i} is of type A by Proposition 3.34(3), Lemma 3.36(1) and $d_{R_1,m_1} = d_{R_2,m_2}$. This induces an isomorphism $V_{R_1} \simeq V_{R_2}$ as $\mathbb{F}_p[\mathscr{H}_{d,r}]$-modules. Hence the claim follows from the assumption that (V_R, ω_R) is completely anisotropic and the definition of $(M(W), 2)$. □

Example 3.45. Assume $p \neq 2$. Let $e = f = 1$, $R_1(x) = x^p$ and $R_2(x) = ax^p \in \mathbb{F}_p[x]\backslash\{0\}$. We assume that $m_1 \neq m_2$ and $d_{R_1,m_1} = d_{R_2,m_2} = p+1$. We have $V_{R_i} = \{x \in \mathbb{F} \mid x^{p^2} + x = 0\}$ for $i = 1, 2$.

Let $W \subset V_{R_1} \oplus V_{R_2}$ be a totally isotropic $\mathbb{F}_p[\mathrm{Gal}(T_R/F)]$-subspace. Assume $W \neq \{0\}$. We take a non-zero element $(x_1, x_2) \in W$. We have $f_{R_1}(x, y) = -xy^p$, $f_{R_2}(x, y) = -axy^p$ and hence $\omega_R((x_1, x_2), (\xi x_1, \xi x_2)) = (x_1^{p+1} + ax_2^{p+1})(\xi - \xi^p) = 0$ for any $\xi \in \mu_{p+1}$. Thus $x_1^{p+1} + ax_2^{p+1} = 0$ and $x_2 \neq 0$. There exists $\eta \in \mathbb{F}$ such that $\eta^{p+1} = -a$ and $x_1 = \eta x_2$. Since $\mathbb{F}_{p^2} = \mathbb{F}_p(\mu_{p+1})$, we have $W_1 := \{(\eta x, x) \mid x \in V_{R_2}\} \subset W$ and $W_2 := \{(\eta^p x, x) \mid x \in V_{R_2}\} \subset W$. Let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. If $W_1 \cap W_2 \neq \{0\}$, we have $\eta \in \mathbb{F}_p$ and $\eta^2 = -a$. This implies $\left(\frac{-a}{p}\right) = 1$.

Assume $\left(\frac{-a}{p}\right) = -1$. Then $W = W_1 \oplus W_2 = V_{R_1} \oplus V_{R_2}$ by $W_1 \cap W_2 = \{0\}$. This is a contradiction. Hence $V_{R_1} \oplus V_{R_2}$ is completely anisotropic if $\left(\frac{-a}{p}\right) = -1$.

If $\left(\frac{-a}{p}\right) = 1$, we have $W_1 = W_2$, which is the unique non-zero totally isotropic $\mathbb{F}_p[\mathscr{H}]$-subspace. Hence $V_{R_1} \oplus V_{R_2}$ is not completely anisotropic.

4. Geometric interpretation of imprimitivity

Through this section, we always assume $p \neq 2$. Our aim in this section is to show Theorem 4.13. To show the theorem, we use the explicit understanding of the automorphism group of C_R and the mechanism of taking quotients of C_R by certain abelian groups, which are developed in [1] and [6].

4.1. Quotient of C_R and description of $\tau_{\psi,R,m}$

Let C_R be as in (2.7). In this subsection, we always assume that there exists a finite étale morphism

$$\phi\colon C_R \to C_{R_1};\ (a, x) \mapsto (a - \Delta(x), r(x)), \tag{4.1}$$

where $\Delta(x) \in \mathbb{F}_q[x]$ and $r(x)$, $R_1(x) \in \mathscr{A}_q$ satisfy $d_{R,m} \mid d_{R_1}$ and $r(\alpha x) = \alpha r(x)$ for $\alpha \in \mu_{d_{R,m}}$. Since ϕ is étale, $r(x)$ is a reduced polynomial. Hence $r'(0) \neq 0$. The above assumption implies that

$$xR(x) = r(x)R_1(r(x)) + \Delta(x)^p - \Delta(x) \tag{4.2}$$

$$r'(0) \neq 0, \quad d_{R,m} \mid d_{R_1}, \quad r(\alpha x) = \alpha r(x) \quad \text{for } \alpha \in \mu_{d_{R,m}}. \tag{4.3}$$

Let e' be a non-negative integer such that $\deg R_1(x) = p^{e'}$ and $e' \leq e$. Then $\deg r(x) = p^{e-e'}$ by (4.2).

We have $\alpha R_1(\alpha x) = R_1(x)$ for $\alpha \in \mu_{d_{R,m}}$ by $d_{R,m} \mid d_{R_1}$ and (2.3). Hence $\Delta(\alpha x) - \Delta(x) \in \mathbb{F}_p$ for $\alpha \in \mu_{d_{R,m}}$ by (4.2). We have $\Delta(\alpha x) = \Delta(x)$, since the constant coefficient of $\Delta(\alpha x) - \Delta(x)$ is zero.

Lemma 4.1. *Let $\varphi\colon C_{R,\mathbb{F}} \to C_{R,\mathbb{F}};\ (x, a) \mapsto (x + c, a + g(x))$ be the automorphism with $g(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then we have $E_R(c) = 0$.*

Proof. From the definition of φ, we have that

$$g(x)^p - g(x) = cR(x) + xR(c) + cR(c). \tag{4.4}$$

Let $\mathcal{P}\colon \mathbb{F}[x] \to \mathbb{F}[x];\ f(x) \mapsto f(x)^p - f(x)$. Since $\mathbb{F}$ is algebraically closed, $cR(c) \equiv 0 \mod \mathcal{P}(\mathbb{F})$. From (4.4) and the definition of $E_R(x)$, it follows that

$$0 \equiv cR(x) + xR(c) + cR(c) \equiv E_R(c)^{1/p^e} x \mod \mathcal{P}(\mathbb{F}[x]).$$

Hence there exists $h(x) \in \mathbb{F}[x]$ such that $h(x)^p - h(x) = E_R(c)^{1/p^e} x$ in $\mathbb{F}[x]$. By considering degrees, we obtain $h(x) = 0$ and $E_R(c) = 0$. □

Lemma 4.2. *We have* $E_{R_1}(r(x)) \mid E_R(x)$.

Proof. Let $\beta \in \mathbb{F}$ be an element such that $E_{R_1}(r(\beta)) = 0$. We take an element $\gamma \in \mathbb{F}$ such that $\gamma^p - \gamma = r(\beta)R_1(r(\beta))$. Let $\varphi\colon C_{R,\mathbb{F}} \to C_{R,\mathbb{F}}$ be the automorphism defined by

$$\varphi(a, x) = \big(a + f_{R_1}(r(x), r(\beta)) + \Delta(x+\beta) - \Delta(x) + \gamma, x + \beta\big).$$

This is well-defined by Lemma 2.2 and (4.2). From Lemma 4.1 it follows that $E_R(\beta) = 0$. Since $E_{R_1}(r(x))$ is separable, the claim follows. □

Lemma 4.3. *Let* $\alpha, \alpha' \in \mu_{d_{R,m}}$. *Assume* $E_{R_1}(r(\alpha y)) = 0$ *for a certain* $y \in \mathbb{F}$. *Then we have the equality*

$$\Delta(\alpha' x + \alpha y) + f_{R_1}(r(\alpha' x), r(\alpha y)) = \Delta(x) + \Delta(y) + f_R(\alpha' x, \alpha y).$$

Proof. By $\Delta(\alpha' x + \alpha y) = \Delta(x + (\alpha/\alpha')y)$ and (2.4), we may assume $\alpha' = 1$ by (4.3). Lemma 4.2 induces that $E_R(\alpha y) = 0$. Let $\Delta_1(x)$ and $\Delta_2(x)$ denote the left and right hand sides of the required equality, respectively. We have $\Delta_1(0) = \Delta(\alpha y) = \Delta(y) = \Delta_2(0)$, since $f_R(0, x') \equiv 0$ in $\mathbb{F}_q[x']$ by definition. Hence it suffices to show $\Delta_1(x)^p - \Delta_1(x) = \Delta_2(x)^p - \Delta_2(x)$. Lemma 4.2 and the assumption imply $E_{R_1}(r(\alpha y)) = E_R(\alpha y) = 0$. Therefore, for each $i = 1, 2$, we have $\Delta_i(x)^p - \Delta_i(x) = (x + \alpha y)R(x + \alpha y) - r(y)R_1(r(y)) - r(x)R_1(r(x))$ according to Lemma 2.2. Hence the claim follows. □

Let

$$U_R := \{x \in \mathbb{F} \mid r(x) = 0\} \subset V'_R := \{x \in \mathbb{F} \mid E_{R_1}(r(x)) = 0\}.$$

We obtain $V'_R \subset V_R$ via Lemma 4.2. Then U_R and V'_R are regarded as $\mathbb{F}_p[\mathscr{H}]$-modules according to $r(x), R_1(x) \in \mathbb{F}_q[x]$ and (4.3).

Lemma 4.4. *We have* $V'_R \subset U_R^{\perp}$. *In particular, the* $\mathbb{F}_p[\mathscr{H}]$*-module* U_R *is totally isotropic.*

Proof. Let β be in U_R and β' be in V'_R so that $r(\beta) = 0$ and $E_{R_1}(r(\beta')) = 0$. From Lemma 4.3, it follows that $f_R(\beta', \beta) = f_R(\beta, \beta') = \Delta(\beta + \beta') - \Delta(\beta) - \Delta(\beta')$. Hence $\omega_R(\beta, \beta') = 0$. □

Let

$$Q'_{R,m} := \{(\alpha,\beta,\gamma) \in Q_{R,m} \mid \beta \in V'_R\}.$$

Then $Q'_{R,m}$ is a subgroup of $Q_{R,m}$ of index $p^{e-e'}$, because of (4.3) and $[V_R : V'_R] = p^{e-e'}$. We have the map

$$\pi \colon Q'_{R,m} \to Q_{R_1,m};\ (\alpha,\beta,\gamma) \mapsto (\alpha, r(\beta), \gamma - \Delta(\beta)).$$

Corollary 4.5. *The map π is a homomorphism.*

Proof. The claim follows from Lemma 4.3 and (4.3). □

We have

$$U'_R := \{(1,\beta,\Delta(\beta)) \in Q'_{R,m} \mid \beta \in U_R\} = \operatorname{Ker} \pi. \tag{4.5}$$

The space V'_R is stable by the q-th power map. Hence we can consider the semidirect product $Q'_{R,m} \rtimes \mathbb{Z}$. The map π induces $\pi' \colon Q'_{R,m} \rtimes \mathbb{Z} \to Q_{R_1,m} \rtimes \mathbb{Z}$.
Quotient of C_R Let ϕ be as in (4.1). We can check that ϕ factors through $C_{R,\mathbb{F}} \to C_{R,\mathbb{F}}/U'_R \xrightarrow{\bar{\phi}} C_{R_1,\mathbb{F}}$ by (2.7). We obtain an isomorphism $\bar{\phi} \colon C_{R,\mathbb{F}}/U'_R \xrightarrow{\sim} C_{R_1,\mathbb{F}}$.

Lemma 4.6. *We have $\phi((a,x)g) = \phi(a,x)\pi'(g)$ for $g \in Q'_{R,m} \rtimes \mathbb{Z}$.*

Proof. The claim follows from Lemma 4.3. □

Let $\tau'_{\psi,R_1,m}$ denote the $Q'_{R,m} \rtimes \mathbb{Z}$-representation which is the inflation of the $Q_{R_1,m} \rtimes \mathbb{Z}$-representation $H^1_{\mathrm{c}}(C_{R_1,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ by π'. We have the homomorphism $\Theta_{R,m,\varpi} \colon W_F \to Q_{R,m} \rtimes \mathbb{Z}$ as in (3.8). We define the W_F-representation $\tau''_{\psi,R_1,m}$ to be the inflation of $\operatorname{Ind}_{Q'_{R,m} \rtimes \mathbb{Z}}^{Q_{R,m} \rtimes \mathbb{Z}} \tau'_{\psi,R_1,m}$ via $\Theta_{R,m,\varpi}$. We have $\dim \tau''_{\psi,R_1,m} = p^e$, since $[Q_{R,m} : Q'_{R,m}] = p^{e-e'}$ and $\dim \tau'_{\psi,R_1,m} = p^{e'}$.

Proposition 4.7. *We have an isomorphism $\tau_{\psi,R,m} \simeq \tau''_{\psi,R_1,m}$ as W_F-representations.*

Proof. Lemma 4.6 induces an injection

$$\tau'_{\psi,R_1,m} = H^1_{\mathrm{c}}(C_{R_1,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi] \xrightarrow{\phi^*} H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$$

of $Q'_{R,m} \rtimes \mathbb{Z}$-representations. Hence we have a non-zero homomorphism

$$\operatorname{Ind}_{Q'_{R,m} \rtimes \mathbb{Z}}^{Q_{R,m} \rtimes \mathbb{Z}} \tau'_{\psi,R_1,m} \to H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi] \tag{4.6}$$

as $Q_{R,m} \rtimes \mathbb{Z}$-representations via Frobenius reciprocity. Since the target is irreducible by Lemma 2.8, the map (4.6) is surjective. We know that (4.6) is an isomorphism by comparing the dimensions. By inflating (4.6) via $\Theta_{R,m,\varpi}$, we obtain the claim. □

We consider the open subgroup $W' := \Theta_{R,m,\varpi}^{-1}(Q'_{R,m} \rtimes \mathbb{Z}) \subset W_F$ of index $p^{e-e'}$. We can write $W' = W_{F'}$ with a finite field extension F'/F of degree $p^{e-e'}$. Let

$$\tau'_{\psi,R_1,m} \colon W_{F'} \xrightarrow{\Theta_{R,m,\varpi}} Q'_{R,m} \rtimes \mathbb{Z} \xrightarrow{\pi'} Q_{R_1,m} \rtimes \mathbb{Z} \to \mathrm{Aut}_{\overline{\mathbb{Q}}_\ell}(H_c^1(C_{R_1,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]) \tag{4.7}$$

be the composite.

Corollary 4.8. *We have an isomorphism $\tau_{\psi,R,m} \simeq \mathrm{Ind}_{W_{F'}}^{W_F} \tau'_{\psi,R_1,m}$ as W_F-representations. If $e' < e$, the W_F-representation $\tau_{\psi,R,m}$ is imprimitive.*

Proof. The assertion follows from Proposition 4.7. □

4.2. Totally isotropic subspace and geometry of C_R

Let $(1, \beta, \gamma) \in H_R$ so, as in Definition 2.3(2), we know that $\gamma^p - \gamma = \beta R(\beta)$. We obtain $(f_R(\beta,\beta) - 2\gamma)^p = f_R(\beta,\beta) - 2\gamma$ by the definition of the pairing ω_R in Lemma 2.6(2). Assume we have that

$$\beta \neq 0, \quad \gamma = \frac{f_R(\beta,\beta)}{2}. \tag{4.8}$$

The following lemma is given in [6, Proposition (13.5)] and [1, Proposition 7.2]. This lemma gives an algorithm of taking quotients of C_R by certain abelian groups.

Lemma 4.9. *Let C_R be as in Definition 2.7. Assume $e \geq 1$.*

(1) *Let*

$$u := x^p - \beta^{p-1}x, \quad v := a + (x/\beta)(\gamma(x/\beta) - f_R(x,\beta)). \tag{4.9}$$

Then there exists $P_1(u) \in \mathscr{A}_{\mathbb{F}}$ of degree p^{e-1} such that $v^p - v = uP_1(u)$.

(2) *Let $U := \{(1, \xi\beta, \xi^2\gamma) \in H_R \mid \xi \in \mathbb{F}_p\} = \langle(1,\beta,\gamma)\rangle$. Then the quotient $C_{R,\mathbb{F}}/U$ is isomorphic to $C_{P_1,\mathbb{F}}$.*

Proof. We show (1). Let $x_1 := x/\beta$ and $u_1 := u/\beta^p$. Then $u_1 = x_1^p - x_1$. We compute

$$\begin{aligned} v^p - v &= xR(x) + \gamma^p x_1^{2p} - \gamma x_1^2 - x_1^p f_R(x,\beta)^p + x_1 f_R(x,\beta) \\ &= xR(x) + \gamma(x_1^{2p} - x_1^2) + \beta^{-2p+1}R(\beta)x^{2p} \\ &\quad - u_1 f_R(x,\beta) - (x/\beta)^p(\beta R(x) + xR(\beta)) \\ &= u\beta^{-p}(-\beta R(x) + \beta^{-p+1}R(\beta)x^p + \gamma(x_1^p + x_1) - f_R(x,\beta)), \end{aligned}$$

where we use $\gamma^p - \gamma = \beta R(\beta)$ and Lemma 2.2 for the second equality. Let $P(x) := \beta^{-p}(-\beta R(x) + \beta^{-p+1}R(\beta)x^p + \gamma(x_1^p + x_1) - f_R(x,\beta))$. Since $P(x)$ is additive, there exists $P_1(u) \in \mathscr{A}_{\mathbb{F}}$ such that $P(x) = P_1(u) + \alpha x$ for a constant

α. By (4.8), we have $P(\beta) = \beta^{-p}(2\gamma - f_R(\beta, \beta)) = 0$. Thus $\alpha = 0$. From $\deg P(x) = p^e$, it follows that $\deg P_1(u) = p^{e-1}$. Hence we obtain (1).

We show (2). We easily check that the finite étale morphism of degree p: $C_{R,\mathbb{F}} \to C_{P_1,\mathbb{F}}$; $(a, x) \mapsto (v, u)$ factors through $C_{R,\mathbb{F}} \to C_{R,\mathbb{F}}/U \to C_{P_1,\mathbb{F}}$. Since $C_{R,\mathbb{F}} \to C_{R,\mathbb{F}}/U$ is a finite étale morphism of degree p, the claim follows. □

Let

$$\Delta_0(x) := -(x/\beta)(\gamma(x/\beta) - f_R(x, \beta)).$$

From Lemma 4.9(1), it follows that

$$xR(x) = uP_1(u) + \Delta_0(x)^p - \Delta_0(x). \tag{4.10}$$

We write $u(x)$ for u.

Let $(1, \beta', \gamma') \in H_R$ be an element satisfying (4.8). Assume $\omega_R(\beta, \beta') = 0$. Then $(1, \beta, \gamma)$ commutes with $(1, \beta', \gamma')$. Hence the action of $(1, \beta', \gamma')$ on $C_{R,\mathbb{F}}$ in (2.7) induces the automorphism of $C_{P_1,\mathbb{F}} \simeq C_{R,\mathbb{F}}/U$.

Lemma 4.10. *Let* $\pi(\beta', \gamma') := (1, u(\beta'), \gamma' - \Delta_0(\beta'))$.

(1) *We have* $\pi(\beta', \gamma') \in H_{P_1}$ *and* $f_{P_1}(u(\beta'), u(\beta')) = 2(\gamma' - \Delta_0(\beta'))$.
(2) *The action of* $(1, \beta', \gamma')$ *on* $C_{R,\mathbb{F}}$ *induces* $\pi(\beta', \gamma')$ *on* $C_{P_1,\mathbb{F}}$.

Proof. Let $\Delta_1(x) := f_R(x, \beta') - \Delta_0(x + \beta') + \Delta_0(x)$. By (4.9), the action of $(1, \beta', \gamma')$ on $C_{R,\mathbb{F}}$ induces the automorphism of $C_{P_1,\mathbb{F}}$ given by $u \mapsto u + u(\beta')$ and $v \mapsto v + \Delta_1(x) + \gamma'$ on $C_{P_1,\mathbb{F}}$. Using (4.8), we can easily check that $\Delta_1(x) - \Delta_1(0)$ is an additive polynomial such that $\Delta_1(\beta) - \Delta_1(0) = \omega_R(\beta, \beta') = 0$. Hence there exists $g(u) \in \mathbb{F}_q[u]$ such that $\Delta_1(x) = g(u(x)) + \Delta_1(0)$. Lemma 4.1 induces that $E_{P_1}(u(\beta')) = 0$. Thus $u(\beta') \in V_{P_1}$. We show (1). The former claim follows from (4.10). Using $\Delta_0(0) = E_{P_1}(u(\beta')) = E_R(\beta') = 0$ in the same way as Lemma 4.3, we have

$$\Delta_0(x + \beta') + f_{P_1}(u(x), u(\beta')) = \Delta_0(x) + \Delta_0(\beta') + f_R(x, \beta'). \tag{4.11}$$

Substituting $x = \beta'$, and using $\Delta_0(2\beta') = 4\Delta_0(\beta')$ and (4.8) for (β', γ'), we obtain the latter claim in (1).

By (4.11),

$$v + f_R(x, \beta') - \Delta_0(x + \beta') + \Delta_0(x) + \gamma' = v + f_{P_1}(u(x), u(\beta')) + \gamma' - \Delta_0(\beta').$$

Hence the claim (2) follows from (2.7). □

Assume that V_R is not completely anisotropic. Let U_R be a non-zero totally isotropic $\mathbb{F}_p[\mathscr{H}]$-submodule in V_R. There exists a monic reduced polynomial $r(x) \in \mathscr{A}_{\mathbb{F}}$ such that $U_R = \{x \in \mathbb{F} \mid r(x) = 0\}$ by [13, Theorem 7]. Since U_R is an $\mathbb{F}_p[\mathscr{H}]$-module, we have

$$r(\alpha x) = \alpha r(x) \text{ for } \alpha \in \mu_{d_{R,m}} \text{ and } r(x) \in \mathbb{F}_q[x] \tag{4.12}$$

by Lemma 3.24. We write $\deg r(x) = p^{e-e'}$ with a non-negative integer $0 \leq e' < e$.

We take a basis $\{\beta_1, \ldots, \beta_{e-e'}\}$ of U_R over $\mathbb{F}_p$. Let $(1, \beta_i, \gamma_i) \in H_R$ be an element satisfying (4.8). Let $U_i := \{(1, \xi\beta_i, \xi^2\gamma_i) \mid \xi \in \mathbb{F}_p\} \subset H_R$, which is a subgroup. Since U_R is totally isotropic, we have $\omega_R(\beta_i, \beta_j) = 0$. Thus $g_i g_j = g_j g_i$ for any $g_i \in U_i$ and $g_j \in U_j$ via Lemma 2.6(2). We consider the abelian subgroup

$$U'_R := U_1 \cdots U_{e-e'} \subset H_R. \tag{4.13}$$

Proposition 4.11. *Assume that V_R is not completely anisotropic. Then there exist $R_1(x) \in \mathscr{A}_{\mathbb{F}}$ of degree $p^{e'}$ and a polynomial $\Delta(x) \in \mathbb{F}[x]$ such that $\Delta(0) = 0$ and the quotient $C_{R,\mathbb{F}}/U'_R$ is isomorphic to the affine curve $C_{R_1,\mathbb{F}}$ and the isomorphism is induced by $\pi : C_{R,\mathbb{F}} \to C_{R_1,\mathbb{F}};\ (a, x) \mapsto (a - \Delta(x), r(x))$. In particular, we have $xR(x) = r(x)R_1(r(x)) + \Delta(x)^p - \Delta(x)$. Furthermore, we have $d_{R,m} \mid d_{R_1}$.*

Proof. By applying Lemmas 4.9 and 4.10 successively, we know that the quotient $C_{R,\mathbb{F}}/U'_R$ is isomorphic to the curve $C_{R_1,\mathbb{F}}$ with some $R_1(x) \in \mathscr{A}_{\mathbb{F}}$, and we obtain $\pi : C_{R,\mathbb{F}} \to C_{R_1,\mathbb{F}};\ (a, x) \mapsto (a - \Delta(x), r(x))$. By (4.9), we have $\Delta(0) = 0$. Since U_R is an $\mathbb{F}_p[\mathscr{H}]$-module, the subgroup $A := \{(\alpha, 0, 0) \in Q_{R,m} \mid \alpha \in \mu_{d_{R,m}}\}$ normalizes U'_R. Hence A acts on the quotient $C_{R_1,\mathbb{F}}$. We recall that $b^p - b = yR_1(y)$ is the defining equation of $C_{R_1,\mathbb{F}}$. Through the morphism π, the action of $A \ni (\alpha, 0, 0)$ on $C_{R_1,\mathbb{F}}$ is given by $b \mapsto b + \Delta(x) - \Delta(\alpha^{-1}x),\ y = r(x) \mapsto r(\alpha^{-1}x) = \alpha^{-1}y$ by (4.12). From [6, Theorem (13.3)] or [1, Theorem 4.3.2], it follows that $\alpha \in \mu_{d_{R_1}}$. Hence the last claim follows. □

Corollary 4.12. *Let the assumption be as in Proposition 4.11. We have $\Delta(x)$, $R_1(x) \in \mathbb{F}_q[x]$.*

Proof. We use the same notation as in Definition 3.23. We consider the equality $xR(x) = r(x)R_1(r(x)) + \Delta(x)^p - \Delta(x)$ in Proposition 4.11. Let $S(x) := -R_1^{\sigma}(x) + R_1(x)$ and $\Pi(x) := \Delta^{\sigma}(x) - \Delta(x)$. Then $S(x) \in \mathscr{A}_{\mathbb{F}}$. Since $r(x), R(x) \in \mathbb{F}_q[x]$,

$$\Pi(x)^p - \Pi(x) = r(x)S(r(x)). \tag{4.14}$$

Assume $S(x) \neq 0$. We have the non-constant morphism $f : \mathbb{A}^1_{\mathbb{F}} \to C_{S,\mathbb{F}};\ x \mapsto (\Pi(x), r(x))$, since $r(x)$ is non-constant. Let $\overline{C}_{S,\mathbb{F}}$ be the smooth compactification of $C_{S,\mathbb{F}}$. The morphism f extends to a non-constant morphism $\mathbb{P}^1_{\mathbb{F}} \to \overline{C}_{S,\mathbb{F}}$. Hence this is a finite morphism. From the Riemann–Hurwitz formula, it follows that the genus of $\overline{C}_{S,\mathbb{F}}$ equals zero. This contradicts to Lemma 2.10. Hence $S(x) \equiv 0$ and $R_1(x) \in \mathbb{F}_q[x]$. We have $\Pi(x) \in \mathbb{F}_p$ by (4.14). As in Proposition 4.11, $\Delta(0) = 0$ induces $\Pi(0) = 0$. Hence $\Pi(x) \equiv 0$. Thus the claim follows. □

4.3. Theorem

Finally, we summarize the contents of 4.1 and 4.2 as a theorem.

Theorem 4.13. *Assume $p \neq 2$. The following conditions are equivalent.*

(1) *There exists a non-trivial finite étale morphism*

$$C_R \to C_{R_1};\ (a, x) \mapsto (a - \Delta(x), r(x)),$$

where $\Delta(x) \in \mathbb{F}_q[x]$ *and* $r(x)$, $R_1(x) \in \mathscr{A}_q$ *satisfy* $d_{R,m} \mid d_{R_1}$ *and* $r(\alpha x) = \alpha r(x)$ *for* $\alpha \in \mu_{d_{R,m}}$.

(2) *The* $\mathbb{F}_p[\mathscr{H}]$*-module* (V_R, ω_R) *is not completely anisotropic.*

(3) *The* W_F*-representation* $\tau_{\psi,R,m}$ *is imprimitive.*

If the above equivalent conditions are satisfied, the W_F*-representation* $\tau_{\psi,R,m}$ *is isomorphic to* $\mathrm{Ind}_{W_{F'}}^{W_F} \tau'_{\psi,R_1,m}$, *where* $\tau'_{\psi,R_1,m}$ *is given in* (4.7).

Proof. Assume (1). The degree of the finite covering $C_R \to C_{R_1}$ equals $\deg r(x)$. Since $C_R \to C_{R_1}$ is not an isomorphism, we have $\deg r(x) > 1$. Thus (2) follows from Lemma 4.4 and $U_R \neq \{0\}$. Assume (2). Then (1) follows from (4.12), Proposition 4.11 and Corollary 4.12.

The equivalence of (2) and (3) follows from Corollary 3.28(1).

The last claim follows from Corollary 4.8. □

Acknowledgements The author would like to thank the referee sincerely for reading previous versions of this paper very carefully and giving many fruitful suggestions to improve them. He would like to thank M. Oi and G. Henniart for their interests on this paper and giving him helpful comments. This work was supported by JSPS KAKENHI Grant Numbers 20K03529/21H00973.

Declarations

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Conflict of interest We have no conflicts of interest to disclose.

References

[1] Bouw, I., Ho, W., Malmskog, B., Scheidler, R., Srinivasan, P., Vincent, C.: Zeta functions of a class of Artin–Schreier curves with many automorphisms, Directions in number theory. Assoc. Women Math. Ser., vol. 3, pp. 87–124. Springer, New York (2016)

[2] Bushnell, C.J., Henniart, G.: The Local Langlands Conjecture for GL(2). A Series of Comprehensive Studies in Mathematics, vol. 335. Springer, New York (2006)

[3] Carlitz, L.: Some theorems on irreducible reciprocal polynomials over a finite field. J. Reine Angew. Math. **227**, 212–220 (1967)

[4] Coulter, R.S., Havas, G., Henderson, M.: On decomposition of sub-linearised polynomials. J. Aust. Math. Soc. **76**(3), 317–328 (2004)

[5] Deligne, P.: Cohomologie étale, Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2. Lect. Notes Math., vol. 569. Springer-Verlag, Berlin (1977)

[6] van der Geer, G., van der Vlugt, M.: Reed–Muller codes and supersingular curves. I. Compos. Math. **84**(3), 333–367 (1992)

[7] Henniart, G.: Représentations du groupe de Weil d'un corps local, Publ. Math. Orsay 79.02, (1979)

[8] Huppert, B.: Endliche Gruppen I. Die Grundlehren der Mathematischen Wissenschaften, vol. 134. Springer-Verlag, Berlin-New York (1967)

[9] Imai, N., Tsushima, T.: Affinoids in the Lubin–Tate perfectoid space and simple supercuspidal representations. II: Wild case. Math. Ann. **380**(1–2), 751–788 (2021)

[10] Imai, N., Tsushima, T.: Local Galois representations of Swan conductor one. Pac. J. Math. **326**(1), 37–83 (2023)

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

[12] Odoni, R.W.K.: On additive polynomials over a finite field. Proc. Edinb. Math. Soc. (2) **42**(1), 1–16 (1999)

[13] Ore, O.: On a special class of polynomials. Trans. Am. Math. Soc. **35**, 559–584 (1933)

[14] Pries, R.: Current Results on Newton Polygons of Curves, Open Problems in Arithmetic Algebraic Geometry. Adv. Lect. Math., vol. 46, pp. 179–207. Int. Press, Somerville (2019)

[15] Rigby, J.F.: Primitive linear groups containing a normal nilpotent subgroup larger than the centre of the group. J. Lond. Math. Soc. **35**, 389–400 (1960)

[16] Serre, J.P.: Corps Locaux. Deuxième édition, Hermann (1968)

[17] Takeuchi, D., Tsushima, T.: Gauss sums and Van der Geer–Van der Vlugt curves. Bull. Lond. Math. Soc. (2023). https://doi.org/10.1112/blms.12953

[18] Tsushima, T.: Good reduction of affinoids in the Lubin–Tate curve in even equal characteristic. I. J. Number Theory **214**, 414–439 (2020)

[19] Weinstein, J.: Semistable models for modular curves of arbitrary level. Invent. Math. **205**(2), 459–526 (2016)