# Iwasawa Theory, Projective Modules, and Modular Representations

Ralph Greenberg

# Contents

**Abstract.** *This paper shows that properties of projective modules over a group ring* $\mathbf{Z}_p[\Delta]$*, where* $\Delta$ *is a finite Galois group, can be used to study the behavior of certain invariants which occur naturally in Iwasawa theory for an elliptic curve* $E$*. Modular representation theory for the group* $\Delta$ *plays a crucial role in this study. It is necessary to make a certain assumption about the vanishing of a* $\mu$*-invariant. We then study* $\lambda$*-invariants* $\lambda_E(\sigma)$*, where* $\sigma$ *varies over the absolutely irreducible representations of* $\Delta$*. We show that there are non-trivial relationships between these invariants under certain hypotheses.*

2000 Mathematics Subject Classification: Primary 11G05, 11R 23 Secondary 20C15, 20C20
Key words and phrases: Iwasawa theory for elliptic curves, Noncommutative Iwasawa theory, Iwasawa invariants, Selmer groups, parity conjecture, root numbers

Research supported in part by National Science Foundation grant DMS-0200785

# 1 Introduction

Let $F$ be a finite extension of $\mathbf{Q}$. Fix a prime $p$ and let $F_\infty$ denote the unique subfield of $F(\mu_{p^\infty})$ such that $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic to $\mathbf{Z}_p$, the additive group of $p$-adic integers. One refers to $F_\infty$ as the cyclotomic $\mathbf{Z}_p$-extension of $F$. Suppose that $K$ is a finite Galois extension of $F$ such that $K \cap F_\infty = F$. Let $K_\infty = KF_\infty$, the cyclotomic $\mathbf{Z}_p$-extension of $K$. Then $K_\infty$ is Galois over $F$ and $G = \mathrm{Gal}(K_\infty/F)$ is isomorphic to $\Delta \times \Gamma$, where $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. Iwasawa theory is often concerned with a compact $\mathbf{Z}_p$-module $X$ which has a natural action of such a Galois group $G$. The questions that we will consider in this paper concern the structure of $X$ just as a $\mathbf{Z}_p[\Delta]$-module. The structure of $X$ as a module over the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\Gamma]]$ will not play a significant role.

Assume that $X$ is a finitely generated, torsion-free $\mathbf{Z}_p$-module and hence a free $\mathbf{Z}_p$-module. This turns out to be so in many interesting cases. Let $\lambda(X)$ denote its $\mathbf{Z}_p$-rank. One can study the action of $\Delta$ on $X$ by considering $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, a vector space over $\mathbf{Q}_p$ of dimension $\lambda(X)$ and a representation space for the group $\Delta$. The module $X$ will be a $\Delta$-invariant $\mathbf{Z}_p$-lattice in $V$. If the order of $\Delta$ is not divisible by $p$, then one sees easily that $X$ is determined up to isomorphism as a $\mathbf{Z}_p[\Delta]$-module by $V$. Furthermore, $X$ will be projective as a $\mathbf{Z}_p[\Delta]$-module. However, if $p\big||\Delta|$, then $V$ can have non-isomorphic $\Delta$-invariant $\mathbf{Z}_p$-lattices and it is possible that none will be projective. If $X$ happens to be a projective $\mathbf{Z}_p[\Delta]$-module, then its isomorphism class is again determined by $V$.

Let $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ denote the set of irreducible representations of $\Delta$ (up to isomorphism) over a field $\mathcal{F}$. We choose $\mathcal{F}$ to be a finite extension of $\mathbf{Q}_p$ containing all $m$-th roots of unity where $m \geq 1$ is divisible by the order of all elements of $\Delta$. Then all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ are absolutely irreducible. For each such $\sigma$, let $W_\sigma$ denote the corresponding $\mathcal{F}$-representation space for $\Delta$ and let $n(\sigma) = \dim_{\mathcal{F}}(W_\sigma)$. One can decompose $V_{\mathcal{F}} = V \otimes_{\mathbf{Q}_p} \mathcal{F}$ as a direct sum of the $W_\sigma$'s, each occurring with a certain multiplicity. We denote this multiplicity by $\lambda(X, \sigma)$. We then have the obvious formula

$$\lambda(X) = \dim_{\mathcal{F}}\big(V_{\mathcal{F}}\big) = \sum_{\sigma} n(\sigma)\lambda(X, \sigma) \tag{1.0.a}$$

where $\sigma$ runs over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. The representation space $V$ is determined by the $\lambda(X, \sigma)$'s. One simple relationship that they satisfy is that $\lambda(X, \sigma) = \lambda(X, \sigma')$ for $\sigma, \sigma' \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ if their characters $\chi_\sigma$ and $\chi_{\sigma'}$ are conjugate over $\mathbf{Q}_p$. We refer to these equalities as the *conjugacy relations*.

Our primary objective in this paper is to study another more subtle type of relationship involving the $\lambda(X, \sigma)$'s which arises when the order of $\Delta$ is divisible by $p$ and $X$ is projective as a $\mathbf{Z}_p[\Delta]$-module. These new relationships, which we refer to as *congruence relations*, owe their existence to the fact that there are more irreducible representations for $\Delta$ in

characteristic 0 than in characteristic $p$ when $p\big||\Delta|$. To be precise, the cardinality of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ is equal to the number of conjugacy classes in the group $\Delta$, which we denote by $s$. Let $\mathcal{O}$ denote the ring of integers of $\mathcal{F}$, $\mathfrak{m}$ denote the maximal ideal of $\mathcal{O}$, and $\mathfrak{f}$ denote the residue field $\mathcal{O}/\mathfrak{m}$, a finite extension of the prime field $\mathbf{F}_p$. Let $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ denote the set of irreducible representations of $\Delta$ over $\mathfrak{f}$. These representations are absolutely irreducible because of the choice of $\mathcal{F}$. The cardinality of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$, which we denote by $t$, is equal to the number of conjugacy classes in $\Delta$ of elements whose order is not divisible by $p$. And so, obviously, $t \leq s$. This inequality is strict if $p\big||\Delta|$.

We will use the notation $\mathrm{Irr}_{\mathcal{F}}(G)$ and $\mathrm{Irr}_{\mathfrak{f}}(G)$ throughout this paper, where $G$ is a finite group. Irreducible representations are always assumed to be absolutely irreducible, unless otherwise mentioned, and it is implicit in the above notation that $\mathcal{F}$ is a finite extension of $\mathbf{Q}_p$ and is sufficiently large so that all irreducible representations of $G$ in characteristic 0 are realizable over $\mathcal{F}$ and all irreducible representations in characteristic $p$ are realizable over its residue field $\mathfrak{f}$. As mentioned earlier, it suffices to have the roots of unity of a certain order in $\mathcal{F}$. We prefer $\mathcal{F}$ to be a finite extension because sometimes it is useful for the ring $\mathcal{O}$ to be compact and Noetherian. This notation is also a simple way of indicating whether the representations being considered are over a field of characteristic 0 or of characteristic $p$.

## 1.1 Congruence Relations.

Let $X_{\mathcal{O}} = X \otimes_{\mathbf{Z}_p} \mathcal{O}$. We can view $X_{\mathcal{O}}$ as an $\mathcal{O}[\Delta]$-module. If we assume that $|\Delta|$ is not divisible by $p$, then formula (1.0.a) is reflected in the following decomposition of $X_{\mathcal{O}}$:

$$X_{\mathcal{O}} \;\cong\; \bigoplus_{\sigma} L_{\sigma}^{\lambda(X,\sigma)} \tag{1.1.a}$$

where $L_\sigma$ is a $\Delta$-invariant $\mathcal{O}$-lattice in $W_\sigma$. Note that $X_{\mathcal{O}}$ and each of the $L_\sigma$'s are projective $\mathcal{O}[\Delta]$-modules. The isomorphism class of $L_\sigma$ is uniquely determined by $\sigma$.

The situation is not as simple if $p$ divides $|\Delta|$. However, under the assumption that $X$ is projective, there is a decomposition of $X_{\mathcal{O}}$ which can be viewed as a natural generalization of (1.1.a). For each $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, let $U_\tau$ denote the underlying $\mathfrak{f}$-representation space for $\tau$ and let $n(\tau) = \dim_{\mathfrak{f}}(U_\tau)$. We can view $U_\tau$ as a simple $\mathcal{O}[\Delta]$-module. There is a projective $\mathcal{O}[\Delta]$-module $P_\tau$ which is characterized (up to isomorphism) as follows: $P_\tau$ has a unique maximal $\mathcal{O}[\Delta]$-submodule and the corresponding quotient module is isomorphic to $U_\tau$. One often refers to $P_\tau$ as the projective hull of $U_\tau$ as an $\mathcal{O}[\Delta]$-module. The $P_\tau$'s are precisely the indecomposable, projective $\mathcal{O}[\Delta]$-modules. Now suppose that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module. Then $X_{\mathcal{O}}$ will be a projective $\mathcal{O}[\Delta]$-module and we will have a decomposition

$$X_{\mathcal{O}} \;\cong\; \bigoplus_{\tau} P_{\tau}^{w(X,\tau)} \tag{1.1.b}$$

where $\tau$ varies over $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ and $w(X,\tau) \geq 0$. This decomposition coincides with that in (1.1.a) if we assume that $|\Delta|$ is not divisible by $p$. Under that assumption, we have $s = t$ and, for every $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, there is a unique $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ such that $L_\sigma/\mathfrak{m}L_\sigma \cong U_\tau$. Furthermore, $P_\tau \cong L_\sigma$ and $w(X,\tau) = \lambda(X,\sigma)$.

The values of the $w(X,\tau)$'s can be determined from the representation space $X_{\mathcal{O}}/\mathfrak{m}X_{\mathcal{O}}$ for $\Delta$ over the field $\mathfrak{f}$. The action of $\Delta$ on this vector space may be non-semisimple, but there is a unique, maximal semisimple quotient space. The characterization of $P_\tau$ implies that $w(X,\tau)$ is equal to the multiplicity of $\tau$ in that semisimple quotient. We will refer to $w(X,\tau)$ as the weight of $\tau$ in $X$. The structure of $X$ as a $\mathbf{Z}_p[\Delta]$-module is completely determined by the $w(X,\tau)$'s.

As an illustration, suppose that $X$ is a free $\mathbf{Z}_p[\Delta]$-module of rank 1. Of course, $X$ is then projective and one can show that $w(X,\tau) = n(\tau)$ for each $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Thus, the $P_\tau$'s are direct summands in $X_{\mathcal{O}}$, which is a free $\mathcal{O}[\Delta]$-module of rank 1. Each $P_\tau$ occurs with multiplicity $n(\tau)$. Note that if $t > 1$, then $P_\tau$ itself will not be free. If $t = 1$, then $\Delta$ is a $p$-group, and projective modules must be free. We will return to this very special case below.

Now consider $P_\tau \otimes_{\mathcal{O}} \mathcal{F}$, a representation space for $\Delta$ over $\mathcal{F}$. Each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ occurs with a certain multiplicity in $P_\tau \otimes_{\mathcal{O}} \mathcal{F}$. We denote this multiplicity by $d(\sigma,\tau)$. We have $V_{\mathcal{F}} \cong X_{\mathcal{O}} \otimes_{\mathcal{O}} \mathcal{F}$ and the multiplicity $\lambda(X,\sigma)$ of $\sigma$ in the $\Delta$-representation space $V_{\mathcal{F}}$ is obviously given by

$$\lambda(X,\sigma) = \sum_{\tau} d(\sigma,\tau) w(X,\tau) \tag{1.1.c}$$

where $\tau$ runs over $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Thus, assuming that one can determine the $d(\sigma,\tau)$'s, formula (1.1.c) shows that the $w(X,\tau)$'s determine the $\lambda(X,\sigma)$'s. The converse is also true, as we will explain below.

Note that the quantities $d(\sigma,\tau)$ are purely group-theoretic in nature and do not depend on $X$. For each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, let $L_\sigma$ denote any $\Delta$-invariant $\mathcal{O}$-lattice in $W_\sigma$. Then $L_\sigma/\mathfrak{m}L_\sigma$ is a representation space for $\Delta$ over $\mathfrak{f}$. We denote the corresponding representation by $\widetilde{\sigma}$. It depends on the choice of $L_\sigma$, but its semisimplification $\widetilde{\sigma}^{ss}$ is determined up to isomorphism by $\sigma$. One of the basic results in modular representation theory is that $d(\sigma,\tau)$, as defined above, coincides with the multiplicity of $\tau$ in $\widetilde{\sigma}^{ss}$. That is, in a composition series for the $\mathcal{O}[\Delta]$-module $L_\sigma/\mathfrak{m}L_\sigma$, the number of composition factors isomorphic to $U_\tau$ is $d(\sigma,\tau)$. Later in this paper we will use the notation $\langle \widetilde{\sigma}^{ss}, \tau \rangle$ instead of $d(\sigma,\tau)$ to denote this multiplicity.

Suppose that $\rho$ is any representation of $\Delta$. We may assume that $\rho$ is defined over $\mathcal{F}$. Just as above, we can realize $\rho$ on a free $\mathcal{O}$-module $L_\rho$ of rank $n(\rho)$. The reduction of $\rho$ modulo $\mathfrak{m}$, which we denote by $\widetilde{\rho}$, gives the action of $\Delta$ on $L_\rho/\mathfrak{m}L_\rho$. Its semisimplification

$\widetilde{\rho}^{ss}$ is uniquely determined by $\rho$ and will be isomorphic to a direct sum of the $\tau$'s with certain multiplicities. Now suppose that we have two representations $\rho_i$, $i = 1, 2$. For each $i$, $\rho_i$ is isomorphic to a direct sum:

$$\rho_i \cong \bigoplus_{\sigma} \sigma^{m_i(\sigma)}$$

for certain multiplicities $m_i(\sigma)$, where $\sigma$ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. Assuming that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module, a *congruence relation* arises whenever we have $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$. Such an isomorphism amounts to the set of equalities: $\sum_\sigma m_1(\sigma)d(\sigma,\tau) = \sum_\sigma m_2(\sigma)d(\sigma,\tau)$ for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Formula (1.1.c) then has the following consequence:

$$\sum_{\sigma} m_1(\sigma)\lambda(X,\sigma) = \sum_{\sigma} m_2(\sigma)\lambda(X,\sigma) \quad . \tag{1.1.d}$$

This is a nontrivial equation if $\rho_1 \not\cong \rho_2$.

We call (1.1.d) a congruence relation because it arises from an isomorphism $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$, which we think of as a kind of congruence modulo $\mathfrak{m}$ between the two representations $\rho_1$ and $\rho_2$. Just as the conjugacy relation mentioned previously arises whenever two representations are conjugate over $\mathbf{Q}_p$ and something which we call a duality relation (mentioned in section 1.3) arises whenever two representations are dual to each other, a congruence relation arises whenever two representations are congruent to each other in the above sense.

Such nontrivial congruence relations will obviously occur if $t < s$. Indeed, let us denote the Grothendieck group of finite-dimensional representations of $\Delta$ over $\mathcal{F}$ by $\mathcal{R}_{\mathcal{F}}(\Delta)$, which can be defined to be the free $\mathbf{Z}$-module on $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. We define $\mathcal{R}_{\mathfrak{f}}(\Delta)$ in the same way. One defines a homomorphism $d : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathcal{R}_{\mathfrak{f}}(\Delta)$ by sending the class $[\rho]$ to the class $[\widetilde{\rho}^{ss}]$. An isomorphism $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$ simply means that $[\rho_1] - [\rho_2] \in \ker(d)$. It is obvious that the $\mathbf{Z}$-rank of $\ker(d)$ is at least $s-t$. The congruence relations that are described by (1.1.d) state that the homomorphism $\lambda_X : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathbf{Z}$ defined by $\lambda_X(\sigma) = \lambda(X,\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ factors through the map $d$. To be precise, define a homomorphism $w_X : \mathcal{R}_{\mathfrak{f}}(\Delta) \to \mathbf{Z}$ by $w_X(\tau) = w(X,\tau)$ for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Then, $\lambda_X = w_X \circ d$. In essence, this is just formula (1.1.c).

A theorem of Brauer asserts that $d$ is surjective. (See [Se77], theorem 33.) It follows that $\ker(d)$ has $\mathbf{Z}$-rank equal to $s - t$. Now $\mathcal{R}_{\mathcal{F}}(\Delta)$ and $\mathcal{R}_{\mathfrak{f}}(\Delta)$ are free $\mathbf{Z}$-modules with bases $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$, respectively. Let $D_p(\Delta)$ denote the matrix for $d$ with respect to those bases, which we refer to as the *decomposition matrix* for $\Delta$ and $p$. Indexing the rows of $D_p(\Delta)$ by $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ and the columns by $\mathrm{Irr}_{\mathcal{F}}(\Delta)$, it is a $t \times s$ matrix and $d(\sigma,\tau)$ is the entry on row $\tau$, column $\sigma$. Since $d$ is surjective, it follows that $D_p(\Delta)$ has rank $t$. Hence one can use (1.1.c) for a certain set of $\sigma$'s (of cardinality $t$) to determine, in principle, the values of the $w(X,\tau)$'s. Thus, all of the $\lambda(X,\sigma)$'s are then determined. A similar remark concerns

the parity of these invariants. Since the reduction of $D_p(\Delta)$ modulo 2 also has rank $t$, one can determine the parity of $\lambda(X,\sigma)$ for all $\sigma$'s if one knows that parity for a suitable subset consisting of $t$ of the $\sigma$'s.

The form of congruence relations depends on the group $\Delta$. We will always denote the trivial representations for $\Delta$ over $\mathcal{F}$ by $\sigma_0$, and the trivial representation over $\mathfrak{f}$ by $\tau_0$, respectively. Of course, $\widetilde{\sigma_0} = \tau_0$. As the first and simplest example, suppose that $\Delta$ is a $p$-group. One can take $\mathcal{F} = \mathbf{Q}_p(\mu_{p^a})$, where $p^a$ is the maximal order of elements in $\Delta$. Then $\mathfrak{f} = \mathbf{F}_p$, $t = 1$, and $\mathrm{Irr}_{\mathfrak{f}}(\Delta) = \{\tau_0\}$. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, then $\widetilde{\sigma}^{ss} \cong \tau_0^{n(\sigma)}$ and $d(\sigma,\tau_0) = n(\sigma)$. If we assume that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module, then we have the congruence relation $\lambda(X,\sigma) = n(\sigma)\lambda(X,\sigma_0)$ for each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. However, in this case, it is not hard to show that $\mathbf{Z}_p[\Delta]$ is a local ring and hence that any projective module $X$ must be free. The above congruence relation is then obvious.

Another relatively simple situation occurs if $\Delta$ is a $p$-solvable group, i.e., if $\Delta$ has a composition series in which each simple subquotient is either of order $p$ or of order prime to $p$. According to the Fong-Swan theorem (theorem 38 in [Se77]), every $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$ is then of the form $\tau = \widetilde{\sigma}$ for some $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. That $\sigma$ may not be uniquely determined by $\tau$, but we will let $\sigma_\tau$ denote one such lifting. Formula (1.1.c) becomes $\lambda(X,\sigma_\tau) = w(X,\tau)$. For an arbitrary $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, we then have

$$\widetilde{\sigma}^{ss} \cong \bigoplus_{\tau} \widetilde{\sigma_\tau}^{\,d(\sigma,\tau)} \qquad \textit{and} \qquad \lambda(X,\sigma) = \sum_{\tau} d(\sigma,\tau)\lambda(X,\sigma_\tau),$$

assuming that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module. The above equation for $\lambda(X,\sigma)$ is precisely the congruence relation (1.1.d) which results from the above isomorphism for $\widetilde{\sigma}^{ss}$. Thus, the $\lambda(X,\sigma_\tau)$'s determine all of the $\lambda(X,\sigma)$'s.

For example, consider $\Delta = D_{2p^r}$, the dihedral group of order $2p^r$, where $p$ is an odd prime and $r \geq 0$. Then $\Delta$ is clearly $p$-solvable. We have $t = 2$. The elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are $\tau_0$ and another 1-dimensional representation $\tau_1$. There are two 1-dimensional representations of $\Delta$ over $\mathcal{F}$, $\sigma_0$ and $\sigma_1$, whose reductions modulo $\mathfrak{m}$ are $\tau_0$ and $\tau_1$, respectively. Those liftings are unique in this case and are the irreducible representations which factor through the unique quotient $\Delta_0$ of $\Delta$ of order 2. All other representations $\sigma$ in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are of dimension 2 and one has $d(\sigma,\tau) = 1$ for both $\tau$'s in $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. For any such $\sigma$ and any projective module $X$, we obtain the congruence relation

$$\lambda(X,\sigma) = \lambda(X,\sigma_0) + \lambda(X,\sigma_1) \quad .$$

However, we should point out that if we use the fact that such a $\sigma$ is induced from a 1-dimensional representation $\pi$ of the Sylow $p$-subgroup $\Pi$ of $\Delta$, then this relation is an easy

consequence of a congruence relation for the $p$-group $\Pi$. To see this, note that $X$ is also a projective $\mathbf{Z}_p[\Pi]$-module and so $\lambda(X,\pi) = \lambda(X,\pi_0)$, where $\pi_0$ is the trivial character of $\Pi$. We have $\sigma \cong \mathrm{Ind}_{\Pi}^{\Delta}(\pi)$ and $\sigma_0 \oplus \sigma_1 \cong \mathrm{Ind}_{\Pi}^{\Delta}(\pi_0)$. Then, using the Frobenius reciprocity law, we have

$$\lambda(X,\sigma) = \lambda(X,\pi) = \lambda(X,\pi_0) = \lambda(X,\sigma_0) + \lambda(X,\sigma_1).$$

A useful general observation is that if $\Delta$ contains a normal $p$-subgroup $\Pi$, then every element $\tau$ of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ must factor through $\Delta/\Pi$. This is clear since $U_\tau^{\Pi}$ is a nontrivial subspace of $U_\tau$ which is $\Delta$-invariant and hence must coincide with $U_\tau$. The groups $D_{2p^r}$ provides a simple illustration. As another interesting example (and one of our main guiding examples for this study), suppose that $p$ is an odd prime and that $\Delta \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for some $r \geq 0$. Let $\Delta_0 = PGL_2(\mathbf{Z}/p\mathbf{Z})$. The kernel $\Pi$ of the obvious homomorphism $\Delta \to \Delta_0$ is a normal $p$-subgroup of $\Delta$. Hence the irreducible representations of $\Delta$ over a finite field of characteristic $p$ factor through $\Delta_0$. They are easily described and all are defined over $\mathbf{F}_p$. One has $t = p+1$. If $p \geq 5$, then $\Delta$ is not $p$-solvable, although it turns out that four of the $\tau$'s can be lifted to representations in characteristic 0. We will return to this example in some detail in chapter 7, along with other examples.

Before turning to the arithmetic side of this paper, we make the following important remark. It will be useful to have a larger class of $\mathbf{Z}_p[\Delta]$-modules for which the congruence relations (1.1.d) hold. We consider only finitely-generated $\mathbf{Z}_p[\Delta]$-modules. If $X$ is such a module, then one can still define the $\lambda(X,\sigma)$'s for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ since they are determined by the $\Delta$-representation space $V = X \otimes_{\mathbf{Z}_p} \mathcal{F}$. Thus, it would actually be sufficient to know that $V$ contains a $\Delta$-invariant $\mathbf{Z}_p$-lattice $Y$ which is projective as a $\mathbf{Z}_p[\Delta]$-module. If that is so, we will then say that $X$ is *strictly quasi-projective*. Equivalently, this means that there is a $\Delta$-homomorphism $X \to Y$ with finite kernel and cokernel. We then have $\lambda(X,\sigma) = \lambda(Y,\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and so by applying formula (1.1.c) to $Y$, we will obtain precisely the same congruence relations (1.1.d) for the $\lambda(X,\sigma)$'s. Furthermore, if we have an exact sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X \longrightarrow 0$$

of finitely-generated $\mathbf{Z}_p[\Delta]$-modules where $X_1$ and $X_2$ are strictly quasi-projective, then we will say that $X$ is *quasi-projective*. Since the congruence relations (1.1.d) hold for the $\lambda(X_1,\sigma)$'s and the $\lambda(X_2,\sigma)'s$, it is clear that they will also hold for the $\lambda(X,\sigma)$'s.

## 1.2 Selmer groups for elliptic curves.

There are situations where a suitably defined module $X$ of arithmetic interest does turn out to be projective or, at least, quasi-projective. We will illustrate the ideas that we have

described above when $X$ is the Pontryagin dual of a Selmer group associated to an elliptic curve $E$ defined over $F$. We assume that $E$ has good, ordinary reduction at all primes of $F$ lying above $p$. Most of the results of this paper will concern this particular example. However, it will be clear that the methods are rather general and could be applied to other "Selmer groups." We will discuss some more general situations in section 3.4.

Let $\mathrm{Sel}_E(K_\infty)_p$ denote the $p$-primary subgroup of the Selmer group for $E$ over $K_\infty$. This can be defined as the kernel of a global-to-local map:

$$\gamma_{K_\infty} : \ H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_v \mathcal{H}_v(K_\infty, E)$$

where $v$ varies over all the primes of $F$. We recall the definition of the local factors $\mathcal{H}_v(K_\infty, E)$ when $v$ is a non-archimedean prime of $F$. The factors corresponding to archimedean primes are trivial except possibly when $p = 2$. We will give the definition of those factors for $p = 2$ in chapter 3. For a non-archimedean prime $v$, define

$$\mathcal{H}_v(K_\infty, E) = \prod_{\eta|v} H^1(K_{\infty,\eta}, E[p^\infty]) \big/ \mathrm{im}(\kappa_\eta)$$

where $\eta$ runs over the finite set of primes of $K_\infty$ lying over $v$, $K_{\infty,\eta}$ is the union of the $\eta$-adic completions of all the finite extension of $F$ contained in $K_\infty$, and $\kappa_\eta$ is the Kummer homomorphism for $E$ over $K_{\infty,\eta}$. Each such prime $\eta$ lies over a prime $w$ of $K$ and a prime $\nu$ of $F_\infty$, both of which, in turn, lie over $v$.

There is a natural action of $\mathrm{Gal}(K_\infty/F)$ on $H^1(K_\infty, E[p^\infty])$ and on each of the groups $\mathcal{H}_v(K_\infty, E)$. Thus, we have commuting actions of both $\Gamma$ and $\Delta$ on those group. They are abelian, $p$-primary groups and so we can regard them as discrete $\Lambda$-modules. The map $\gamma_{K_\infty}$ is a $\Lambda$-module homomorphism and is $\Delta$-equivariant. Hence we can regard $\mathrm{Sel}_E(K_\infty)_p$ as a discrete $\Lambda$-module which has a $\Lambda$-linear action of $\Delta$. It is known that $\mathrm{Sel}_E(K_\infty)_p$ is cofinitely generated as a $\Lambda$-module and it is a conjecture of Mazur [Ma72] that it is $\Lambda$-cotorsion. That is, its Pontryagin dual is finitely generated as a $\Lambda$-module and should be a torsion $\Lambda$-module.

If $v \nmid p$, the definition becomes simple because we then have $\mathrm{im}(\kappa_\eta) = 0$, as is easily seen. Note that any cocycle class $c \in H^1(K_\infty, E[p^\infty])$ will be unramified at all but a finite number of non-archimedean primes of $K_\infty$. If $v \nmid p$ and $\eta|v$, then $K_{\infty,\eta}$ is the unramified $\mathbf{Z}_p$-extension of $K_v$. It is therefore clear that if $c$ is unramified at $\eta$, then $c$ is trivial. This is why the image of $\gamma_{K_\infty}$ is contained in the direct sum. Also, it turns out that

$$H^1(K_{\infty,\eta}, E[p^\infty]) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_\eta}$$

for some $\delta_\eta \geq 0$. Thus the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is a free $\mathbf{Z}_p$-module. Its rank is simply the product of $\delta_\eta$ and the number of primes of $K_\infty$ lying above $v$. It follows that $\mathcal{H}_v(K_\infty, E)$ is a cotorsion $\Lambda$-module and that its $\mu$-invariant is zero.

If $v|p$, then $\mathcal{H}_v(K_\infty, E)$ is quite large; its corank as a $\Lambda$-module (i.e. the rank over $\Lambda$ of its Pontryagin dual) is equal to $[K : F]$. Let $\overline{E}_v$ denote the reduction of $E$ modulo $v$, an ordinary elliptic curve defined over the residue field $f_v$ for $v$. For each prime $\eta$ of $K_\infty$ dividing $v$, one has the corresponding reduction map $E[p^\infty] \longrightarrow \overline{E}_v[p^\infty]$. (This map depends on choosing a prime of $\overline{\mathbf{Q}}$ above $\eta$, but the choice doesn't matter.) As shown in [CoGr] and [Gr89], these maps induce an isomorphism

$$\mathcal{H}_v(K_\infty, E) \xrightarrow{\sim} \prod_{\eta|v} H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty]) \tag{1.2.a}$$

The action of $G_{K_{\infty,\eta}}$ on $\overline{E}_v[p^\infty]$ is unramified and is induced by the above reduction map.

Our theorems concern primarily the *"non-primitive"* Selmer group obtained by omitting the local condition for the primes $v \in \Sigma_0$, where $\Sigma_0$ is a finite set of non-archimedean primes not including primes above $p$. We denote this group by $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. Since $\mathcal{H}_v(K_\infty, E)$ is a cotorsion $\Lambda$-module for $v \nmid p$, the $\Lambda$-coranks of $\mathrm{Sel}_E(K_\infty)_p$ and $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ will be the same. Hence the non-primitive Selmer groups should also be $\Lambda$-cotorsion for any such choice of $\Sigma_0$.

Let $X_E(K_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$. For any $\Sigma_0$ as above, we let $X_E^{\Sigma_0}(K_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. Assuming these $\Lambda$-modules are torsion, we will denote their $\lambda$-invariants (i.e., their $\mathbf{Z}_p$-ranks) by $\lambda_E(K_\infty)$ and $\lambda_E^{\Sigma_0}(K_\infty)$, respectively. Furthermore, for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, we let $\lambda_E(\sigma)$ denote $\lambda(X_E(K_\infty), \sigma)$. We will use a similar notation below for the non-primitive Selmer groups too, indicating the $\Sigma_0$ as a superscript. Thus, we have the general formula

$$\lambda_E(K_\infty) = \sum_\sigma n(\sigma)\lambda_E(\sigma) \ , \tag{1.2.b}$$

where $\sigma$ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. This is just (1.0.a) applied to $X_E(K_\infty)$. A similar formula is valid for $\lambda_E^{\Sigma_0}(K_\infty)$. One sees easily that $\lambda_E(\sigma_0) = \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(F_\infty)_p\big)$, which we denote by $\lambda_E(F_\infty)$. It is one of the terms in (1.2.b).

We are interested in relationships between the $\lambda_E(\sigma)$'s occurring in formula (1.2.b). Apart from the conjugacy relations which result when the character for $\sigma$ has values outside of $\mathbf{Q}_p$, there is another somewhat deep and quite useful type of relationship which we will refer to as the *duality relation*. This is the equality $\lambda_E(\check{\sigma}) = \lambda_E(\sigma)$, where $\check{\sigma}$ is the contragredient of $\sigma$, another irreducible representation for $\Delta$. We will prove it in chapter 10. However, our main results in this paper concern congruence relations and we discuss this now.

Various sets of non-archimedean primes will be singled out in our theorems. If $v$ is a prime of $F$, we denote the ramification index of $v$ in the extension $K/F$ by $e_v(K/F)$. First of all, consider the primes which don't divide $p$. The following subset of the primes which

are ramified in the extension $K/F$ plays an especially important role:

$$\Phi_{K/F} = \{v \mid \ v \text{ is a prime of } F \text{ such that } \ p|e_v(K/F),\ v \nmid p, \text{ and } v \nmid \infty\}$$

We will let $\Psi_E$ denote the set of primes of $F$ where $E$ has bad reduction. Now consider the set of primes of $F$ dividing $p$, which we denote by $\Sigma_p$. For each $v \in \Sigma_p$, let $w$ be a prime of $K$ lying above $v$ and let $k_w$ denote the residue field. The field $k_w$ and the finite group $\overline{E}_v(k_w)$ depend only on $v, E$, and $K$. We say that $v$ is anomalous for $E/K$ if $|\overline{E}_v(k_w)|$ is divisible by $p$; otherwise, we say that $v$ is non-anomalous for $E/K$. If all $v \in \Sigma_p$ are non-anomalous for $E/K$, then we say that $p$ is non-anomalous for $E/K$. This concept and terminology is due to Mazur [Ma72] who first discussed its role in the Iwasawa theory for elliptic curves. Note that if $\eta$ is a prime of $K_\infty$ lying over $w$, then the residue field $k_\eta$ is a finite $p$-extension of $k_w$. Therefore, $p$ divides $|\overline{E}_v(k_\eta)|$ if and only if $p$ divides $|\overline{E}_v(k_w)|$.

We will prove the following theorem.

**Theorem 1.** *Suppose that $E(K)[p] = 0$ and that $p$ is non-anomalous for $E/K$. Suppose also that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Let $\Sigma_0$ be a finite set of non-archimedean primes of $F$ containing $\Phi_{K/F}$, but not containing primes above $p$. Then the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is a projective $\mathbf{Z}_p[\Delta]$-module.*

The finiteness of $\mathrm{Sel}_E(K_\infty)[p]$ is equivalent to the two-fold assertion that $X_E(K_\infty)$ is $\Lambda$-torsion (as conjectured) and also that the $\mu$-invariant for that torsion $\Lambda$-module is zero. The same statements then follow for the Pontryagin dual $X_E^{\Sigma_0}(K_\infty)$ of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. It is quite unfortunate that we must make such an assumption, but our arguments depend crucially on it. Although the vanishing of the $\mu$-invariant is usually conjectured to hold (with certain exceptions), the known results and even the methods to verify it in special cases are extremely limited. The exceptions may not be a serious problem, however. In most cases where the $\mu$-invariant is positive, one can replace $E$ by an isogenous elliptic curve for which the $\mu$-invariant is zero, or at least expected to be zero.

Concerning the other assumptions, we have the following remarks. Assume that $p$ is odd. In that case, if one omits the two assumptions in the first sentence of theorem 1, then we will still prove that $X_E^{\Sigma_0}(K_\infty)$ is quasi-projective. (See proposition 3.2.1.) As we mentioned before, this is good enough for proving the congruence relations. The proofs will make it clear how the various assumptions determine whether $X_E^{\Sigma_0}(K_\infty)$ is projective, quasi-projective, or neither. In particular, the requirement that $\Phi_{K/F} \subseteq \Sigma_0$ cannot be weakened in any significant way, even just for quasi-projectivity. (See proposition 3.3.1)

The prime $p = 2$ requires special attention. Assuming that $E$ has good, ordinary reduction at a prime $v \in \Sigma_2$, we have $\overline{E}_v[2^\infty] \cong \mathbf{Q}_2/\mathbf{Z}_2$ and so $\overline{E}_v$ will have a unique point of order 2. That point must be Galois-invariant and hence rational over the residue field for $v$. Thus,

the prime 2 is anomalous for $E/F$, and hence certainly for $E/K$, and therefore is automatically excluded in theorem 1. However, we will still prove a result about quasi-projectivity if we make the extra assumption that $E(F_v)$ is connected for each archimedean prime $v$ of $F$. This is certainly satisfied if $F$ is totally complex. For a real prime $v$, the assumption that $E(F_v)$ is connected means that $E(F_v)[2]$ has order 2.

## 1.3 Behavior of Iwasawa invariants.

We now describe how theorem 1 can be used for studying the invariants $\lambda_E(\sigma)$. First of all, if one assumes that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, then the global-to-local map $\gamma_{K_\infty}$ is known to be surjective. It follows that

$$\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \big/ \mathrm{Sel}_E(K_\infty)_p \cong \bigoplus_{v\in\Sigma_0} \mathcal{H}_v(K_\infty, E) \tag{1.3.a}$$

Let $\widehat{\mathcal{H}}(K_\infty, E, \Sigma_0)$ denote the Pontryagin dual of the right side in (1.3.a). Then for each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, we have

$$\lambda_E^{\Sigma_0}(\sigma) = \lambda_E(\sigma) + \delta_E^{\Sigma_0}(\sigma) \tag{1.3.b}$$

where we denote $\lambda\big(\widehat{\mathcal{H}}(K_\infty, E, \Sigma_0), \sigma\big)$ by $\delta_E^{\Sigma_0}(\sigma)$, a quantity which can be determined by a purely local calculation. That calculation depends on knowing the restrictions of $\sigma$ to the decomposition subgroups $\Delta_\eta$ of $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ for each $v \in \Sigma_0$, where $\eta$ is a prime of $K_\infty$ lying over $v$. We will discuss that in chapter 5. Thus, in principle, one can determine the difference $\lambda_E^{\Sigma_0}(\sigma) - \lambda_E(\sigma)$ for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$.

Now if $X_E^{\Sigma_0}(K_\infty)$ is projective, or even just quasi-projective, as a $\mathbf{Z}_p[\Delta]$-module, then one can apply formula (1.1.c). This reduces the determination of $\lambda_E^{\Sigma_0}(\sigma)$ to evaluating $d(\sigma, \tau)$ and $w_E^{\Sigma_0}(\tau) = w\big(X_E^{\Sigma_0}(K_\infty), \tau\big)$ for each $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. As remarked before, all of the $w_E^{\Sigma_0}(\tau)$'s can be determined if one knows the $\lambda_E^{\Sigma_0}(\sigma)$'s for a suitable set of $t$ of the $\sigma$'s. One can then obtain relationships between the $\lambda_E(\sigma)$'s by using the congruence relations between the $\lambda_E^{\Sigma_0}(\sigma)$'s together with (1.3.b).

Consider, for example, the case where $\Delta$ is a $p$-group. Assuming that $\Sigma_0$ is suitably chosen, we then have $w_E^{\Sigma_0}(\tau_0) = \lambda_E^{\Sigma_0}(\sigma_0)$. Also, $\lambda_E^{\Sigma_0}(\sigma) = n(\sigma)\lambda_E^{\Sigma_0}(\sigma_0)$ for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. From (1.3.b), one then obtains

$$\lambda_E(\sigma) = n(\sigma)\lambda_E(\sigma_0) + n(\sigma)\delta_E^{\Sigma_0}(\sigma_0) - \delta_E^{\Sigma_0}(\sigma) \tag{1.3.c}$$

for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. As mentioned above, $\lambda_E(\sigma_0) = \lambda_E(F_\infty)$. The relationship between $\lambda_E(K_\infty)$ and $\lambda_E(F_\infty)$ which is derived from (1.3.c) and (1.2.b) is precisely the Riemann-Hurwitz formula proved in [HaMa]. We explain this in chapter 6, using the calculation of

the quantity $\delta_E^{\Sigma_0}(\sigma)$ from chapter 5. The assumptions in [HaMa] are weaker than what we need for projectivity, but sufficient for quasi-projectivity and that is enough to prove the formula. In fact, the arguments in chapters 2 and 3 of this paper follow closely those in [HaMa]. That paper is, in turn, inspired by arguments of Iwasawa [Iwa] concerning the invariants that occur in the study of ideal class groups, specifically Iwasawa's proof of a formula of Kida [Kid].

We certainly expect the congruence relations that we have discussed to be valid even if $\mu_E(K_\infty) \neq 0$. Assume that $X_E(K_\infty)$ is a torsion $\Lambda$-module and that $\Sigma_0$ is chosen to contain $\Phi_{K/F}$. If $p = 2$, assume also that $E(F_v)$ is connected for all $v|\infty$. Let $Z_E^{\Sigma_0}(K_\infty)$ be the $\mathbf{Z}_p$-torsion submodule of $X_E^{\Sigma_0}(K_\infty)$ and let $Y_E^{\Sigma_0}(K_\infty) = X_E^{\Sigma_0}(K_\infty)/Z_E^{\Sigma_0}(K_\infty)$. Tensoring $X_E^{\Sigma_0}(K_\infty)$ and $Y_E^{\Sigma_0}(K_\infty)$ by $\mathbf{Q}_p$ gives isomorphic $\Delta$-representation spaces and so the invariants $\lambda_E^{\Sigma_0}(\sigma)$ are determined by $Y_E^{\Sigma_0}(K_\infty)$. It is reasonable to conjecture that $Y_E^{\Sigma_0}(K_\infty)$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. That quotient is the Pontryagin dual of the maximal divisible subgroup of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. For some small results in this direction, see remark 3.2.3.

## 1.4 Selmer atoms.

Another useful description of the $w_E^{\Sigma_0}(\tau)$'s involves the Galois module $E[p] \otimes_{\mathbf{F}_p} U_\tau$, a vector space over $\mathfrak{f}$ of dimension $2n(\tau)$ and a representation space for $G_F$, which we denote more briefly by $E[p] \otimes \tau$. This description will require an additional assumption about the choice of $\Sigma_0$. First of all, we need to define Selmer groups for such a Galois module. Consider, more generally, an arbitrary finite-dimensional representation $\alpha$ of $\Delta$ over $\mathfrak{f}$ and let $U_\alpha$ denote the underlying $\mathfrak{f}$-vector space. We denote $E[p] \otimes_{\mathbf{F}_p} U_\alpha$ by $E[p] \otimes \alpha$. Assume, as before, that $\Sigma_0$ is a finite set of primes of $F$ not including primes above $p$ or $\infty$. We define a *"Selmer group"* over $F_\infty$ for this Galois module by

$$\mathrm{Sel}_{E[p]\otimes\alpha}^{\Sigma_0}(F_\infty) = \ker\left( H^1(F_\infty, E[p]\otimes\alpha) \longrightarrow \bigoplus_{v\notin\Sigma_0} \mathcal{H}_v(F_\infty, E[p]\otimes\alpha)\right)$$

where one defines $\mathcal{H}_v(F_\infty, E[p]\otimes\alpha)$ for a non-archimedean prime $v$ by

$$\mathcal{H}_v(F_\infty, E[p]\otimes\alpha) = \prod_{\nu|v} H^1(F_{\infty,\nu}, E[p]\otimes\alpha) \quad if\ v\nmid p \ ,$$

$$\mathcal{H}_v(F_\infty, E[p]\otimes\alpha) = \prod_{\nu|v} H^1(F_{\infty,\nu}, \overline{E}_v[p]\otimes\alpha) \quad if\ v\mid p \ .$$

In both products, $\nu$ varies over the finite set of primes of $F_\infty$ lying over $v$. For $v \mid p$, we define $\overline{E}_v[p] \otimes \alpha = \overline{E}_v[p] \otimes_{\mathbf{F}_p} U_\alpha$, considered as an $\mathfrak{f}$-representation space for $G_{F_v}$. The group $\mathcal{H}_v(F_\infty, E[p] \otimes \alpha)$ for archimedean $v$'s will be defined later. As a special case, we can define $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ by just taking $\Sigma_0$ to be empty. We like to refer to the $\mathfrak{f}$-vector spaces $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\tau}(F_\infty)$ for $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$ as *"Selmer atoms"*, either *"primitive"* if $\Sigma_0$ is empty, or *"non-primitive"* otherwise. Under certain assumptions, one can prove the surjectivity of the global-to-local map defining $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ and thereby obtain a relationship analogous to (1.3.b) between the $\mathfrak{f}$-dimensions of the primitive and non-primitive Selmer atoms. (See corollary 4.2.3.)

Chapter 4 will discuss Selmer atoms. The objective is to relate the $\lambda$-invariants associated with the Selmer group for $E$ over the field $K_\infty$ to Selmer groups over the field $F_\infty$ associated with certain finite Galois modules. Formula (1.4.a) below gives such a relationship. The main result is the following theorem which gives a formula for $w_E^{\Sigma_0}(\tau)$ in terms of the dimension of the corresponding non-primitive Selmer atom. It will be necessary to make the extra assumption that $\Sigma_0$ contains $\Psi_E$, the set of primes of $F$ where $E$ has bad reduction.

**Theorem 2.** *Suppose that $\Sigma_0$ contains both $\Phi_{K/F}$ and $\Psi_E$, but no prime lying above $p$ or $\infty$. Suppose also that the following assumptions are satisfied for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$:*

*(i)* $H^0(F, E[p] \otimes \tau) = 0$,

*(ii)* $H^0(F_v, \overline{E}_v[p] \otimes \tau) = 0$ *for all* $v|p$,

*(iii)* $\mathrm{Sel}_{E[p]\otimes\tau}(F_\infty)$ *is finite.*

*Then the Pontryagin dual of* $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ *is a projective* $\mathbf{Z}_p[\Delta]$*-module and, for all* $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$*, we have* $w_E^{\Sigma_0}(\tau) = \dim_{\mathfrak{f}}\big(\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\tau}(F_\infty)\big)$.

Each of the assumptions *(i)* - *(iii)* in theorem 2 turns out to be equivalent to the corresponding one in theorem 1. That is, *(i)* holds for all $\tau$ if and only if $E(K)[p] = 0$, *(ii)* holds for all $\tau$ if and only if $p$ is non-anomalous for $E/K$, and *(iii)* holds for all $\tau$ if and only if $\mathrm{Sel}_E(K_\infty)[p]$ is finite. These equivalences can be found in propositions 4.1.3, 4.1.9, and 4.2.5, respectively. Therefore, the conclusion about $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ follows from theorem 1. It is the formula for $w_E^{\Sigma_0}(\tau)$ that requires the additional assumption that $\Sigma_0$ contain $\Psi_E$.

Theorem 2 and formula (1.1.c) establish a relationship between $\lambda_E^{\Sigma_0}(\sigma)$ and the $\mathfrak{f}$-dimensions of the non-primitive Selmer atoms $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\tau}(F_\infty)$ for the $\tau$'s that occur in $\widetilde{\sigma}^{ss}$ with positive multiplicity, provided that $\Sigma_0$ is chosen to contain $\Phi_{K/F} \cup \Psi_E$. Under the assumptions of theorem 2, we have

$$\lambda_E^{\Sigma_0}(\sigma) = \sum_\tau d(\sigma,\tau)\dim_{\mathfrak{f}}\big(\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\tau}(F_\infty)\big) \tag{1.4.a}$$

The proof that we give in chapter 4 gives a direct connection between the non-primitive Selmer atoms, the $d(\sigma,\tau)$'s, and the $\lambda_E^{\Sigma_0}(\sigma)$'s. Here is a sketch of the argument.

Consider the Galois module $E[p^\infty]\otimes_{\mathbf{Z}_p} L_\sigma$. This is a divisible $\mathcal{O}$-module with $\mathcal{O}$-corank equal to $2n(\sigma)$ and has an action of $G_F$ on it. We denote it more briefly by $E[p^\infty]\otimes\sigma$, although it does depend on the choice of $L_\sigma$ and not just on $\sigma$. We can again define a natural Selmer group over $F_\infty$ for this Galois module, essentially just as before. The notation we will use is $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}(F_\infty)$, and $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)$ for the non-primitive version. We will give the precise definition later.

The first steps are to show the equalities

$$\lambda_E^{\Sigma_0}(\sigma) = \mathrm{corank}_{\mathcal{O}}\big(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)\big) = \dim_{\mathfrak{f}}\big(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)[\mathfrak{m}]\big)\ . \tag{1.4.b}$$

The first equality is rather easy and is valid for any choice of $\Sigma_0$, even the empty set. The second equality depends on showing that if assumptions *(i)* and *(iii)* in theorem 2 are satisfied, then $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)$ is a divisible $\mathcal{O}$-module. This is again valid for any $\Sigma_0$. The next steps are to show the isomorphisms

$$\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)[\mathfrak{m}] \cong \mathrm{Sel}^{\Sigma_0}_{(E[p^\infty]\otimes\sigma)[\mathfrak{m}]}(F_\infty) \cong \mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\widetilde{\sigma}}(F_\infty)\quad . \tag{1.4.c}$$

under the assumptions of theorem 2. The first isomorphism is a kind of control theorem for the Galois $\mathcal{O}$-module $E[p^\infty]\otimes\sigma$ and multiplication by a generator of the ideal $\mathfrak{m}$. Now one sees easily that $(E[p^\infty]\otimes\sigma)[\mathfrak{m}] \cong E[p]\otimes\widetilde{\sigma}$ and the second isomorphism follows from that.

The most interesting step is to show that if one has an exact sequence

$$0 \to U_\alpha \to U_\beta \to U_\gamma \to 0$$

of $\mathfrak{f}$-representation spaces for $\Delta$, then one obtains an exact sequence for the corresponding non-primitive Selmer groups

$$0 \longrightarrow \mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty) \longrightarrow \mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\beta}(F_\infty) \longrightarrow \mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\gamma}(F_\infty) \longrightarrow 0 \tag{1.4.d}$$

under the assumptions of theorem 2. Since each $\tau$ occurs with multiplicity $d(\sigma,\tau)$ in a composition series for $\widetilde{\sigma}$, one deduces formula (1.4.a) from (1.4.b), (1.4.c), and (1.4.d).

In one type of example, which we discuss in detail in chapters 7 and 8, we take $\Delta$ to be isomorphic to $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. If $r$ is large, then an irreducible representation $\sigma$ of $\Delta$ in characteristic zero can have large dimension (in comparison to $p$), but its reduction modulo $\mathfrak{m}$ will give a representation over a field of characteristic $p$ which is highly reducible, with composition factors of dimension at most $p$. Thus, useful information about the Selmer group associated to the twist of $E[p^\infty]$ by $\sigma$ can, in principle, be derived from information about

the Selmer atoms associated to the twists of $E[p]$ by irreducible $\tau$'s. This is a philosophy that we wanted to bring out in this paper. However, in practice, it is often easier to infer the same kind of information by exploiting the congruence relations between various $\sigma$'s directly. Also, the hypotheses that are needed can be weaker.

Assume that $p$ is odd and that all the primes of $F$ lying above $p$ are ramified in the extension $F(\mu_p)/F$. The Selmer atom $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\tau}(F_\infty)$ is then determined by $\Sigma_0, \tau$, and $E[p]$. This is almost clear from the definition. The only point to explain concerns the quotients $\overline{E}_v[p]$ for the primes $v$ of $F$ lying above $p$ that occur in that definition. Of course, one must choose a prime of $F(E[p])$ above $v$ to define that quotient. Having made such a choice for each $v$, one can characterize $\overline{E}_v[p]$ as the maximal unramified quotient of the $G_{F_v}$-module $E[p]$. This is because of the ramification assumption which implies that the inertia subgroup of $G_{F_v}$ acts nontrivially on the kernel of the reduction map $E[p] \to \overline{E}_v[p]$. Thus, if we consider two elliptic curves $E_1$ and $E_2$ which are defined over $F$, which have good ordinary reduction at the primes of $F$ lying over $p$, and such that $E_1[p] \cong E_2[p]$ as $\mathbf{F}_p$-representation spaces for $G_F$, then the Selmer atoms $\mathrm{Sel}^{\Sigma_0}_{E_1[p]\otimes\tau}(F_\infty)$ and $\mathrm{Sel}^{\Sigma_0}_{E_2[p]\otimes\tau}(F_\infty)$ corresponding to any choice of $\Sigma_0$ and $\tau$ will be isomorphic. In particular, if we choose $\Sigma_0$ to contain $\Phi_{K/F} \cup \Psi_{E_1} \cup \Psi_{E_2}$, then one can apply theorem 2 to either elliptic curve. If assumptions *(i), (ii)*, and *(iii)* are satisfied for $E_1$, then they are also satisfied for $E_2$. Under all these assumptions, one can then conclude that $\lambda^{\Sigma_0}_{E_1}(\sigma) = \lambda^{\Sigma_0}_{E_2}(\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. A very similar kind of theorem is proved in [GrVa] for the special case $\sigma = \sigma_0$.

## 1.5 Parity questions.

One of our original motivations for this project was to study parity questions. We denote the contragredient of a representation $\rho$ of any group by $\check{\rho}$. If $\check{\rho} \cong \rho$, then we say that $\rho$ is self-dual. Let $\mathrm{Irr}^{(sd)}_{\mathcal{F}}(\Delta)$ denote the subset of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ consisting of the irreducible, self-dual representations $\sigma$ of $\Delta$ over $\mathcal{F}$. Ideally, the goal would be to derive results concerning the multiplicity $r_E(\sigma)$ of such a $\sigma$ in the $\Delta$-representation space $E(K)\otimes_{\mathbf{Z}}\mathcal{F}$. Conjecturally, $r_E(\sigma)$ should equal the order of vanishing at $s = 1$ for the $L$-function $L(E/F, \sigma, s)$, the Hasse-Weil $L$-function for $E$ over $F$, twisted by the Artin representation $\sigma$. Consequently, the parity of $r_E(\sigma)$ should agree with the sign in the functional equation for $L(E/F, \sigma, s)$. Of course, one must view $\sigma$ as a representation over $\mathbf{C}$ in some way in order to define $L(E/F, \sigma, s)$. The analytic continuation and functional equation for that $L$-function is still just conjectural in general, but there is a precise prediction of the sign in the functional equation which is due to Deligne. We will think of that sign as a factor of $\pm 1$ and denote that predicted factor by $W_{Del}(E, \sigma)$.

A more approachable question concerns the multiplicity of $\sigma$ in the $\Delta$-representation space $X_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$, where $X_E(K)$ is the Pontryagin dual of the $p$-Selmer group $\mathrm{Sel}_E(K)_p$. We denote that multiplicity by $s_{E,p}(\sigma)$. Assuming the finiteness of $Ш_E(K)_p$, the $p$-primary subgroup of the Tate-Shafarevich group for $E$ over $K$, one would have $s_{E,p}(\sigma) = r_E(\sigma)$ for all primes $p$. Thus, at the very least, the parity of $s_{E,p}(\sigma)$ should certainly agree with the value of $W_{Del}(E, \sigma)$. That question has received considerable attention over the years and significant progress has been made by a number of authors. In recent years, this would include Nekovář [Nek1,2,3,4,5], Kim [Kim1,2], Mazur and Rubin [MR07,08], Coates, Fukaya, Kato, and Sujatha [CFKS], and T. and V. Dokchitser [Dok1,2,3,4,5]. Some of the older papers include those of Birch and Stephens [BiSt], Kramer and Tunnell [KrTu], and Monsky [Mon]. However, the approach of this paper is rather different than the ones just mentioned. It is perhaps most closely related to [CFKS]. We will say more about some of the results of the above authors when we discuss various examples in chapter 13.

To describe our contribution to parity questions, consider an arbitrary (possibly reducible) self-dual representation $\rho$ of $\Delta$ over $\mathcal{F}$. For each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, let $m_\rho(\sigma)$ denote the multiplicity of $\sigma$ in $\rho$. Thus, $m_\rho(\check{\sigma}) = m_\rho(\sigma)$. Define

$$W_{Del}(E, \rho) \;=\; \prod_{\sigma}^{(sd)} W_{Del}(E, \sigma)^{m_\rho(\sigma)} \quad ,$$

where the product is over just the $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$. In effect, we have made a definition which is multiplicative for direct sums and where we just regard $W_{Del}(E, \rho)$ to be equal to 1 if $\rho \cong \sigma \oplus \check{\sigma}$ for some non-self-dual $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Of course, the sign in the functional equation for the $L$-function $L(E/F, \rho, s) = L(E/F, \sigma, s)L(E/F, \check{\sigma}, s)$ should certainly be 1.

Continuing to assume that $\rho$ is self-dual, we define an analogous function in terms of the Iwasawa invariants $\lambda_E(\sigma)$, namely

$$W_{Iw_p}(E, \rho) \;=\; \prod_{\sigma}^{(sd)} (-1)^{\lambda_E(\sigma) m_\rho(\sigma)} \quad ,$$

assuming that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion so that the $\lambda$-invariants can be defined. Thus, $W_{Iw_p}(E, \rho)$ is also multiplicative for direct sums and $W_{Iw_p}(E, \sigma) = (-1)^{\lambda_E(\sigma)}$ if $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$. Again, we have implicitly defined $W_{Iw_p}(E, \rho)$ to be 1 if $\rho \cong \sigma \oplus \check{\sigma}$. This is reasonable since it turns out that $\lambda_E(\sigma) = \lambda_E(\check{\sigma})$ for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, a result we will prove in chapter 10, and therefore $\lambda_E(\sigma) + \lambda_E(\check{\sigma})$ is even. With this notation, we will prove the following theorem in chapter 12.

**Theorem 3.** *Assume that $p$ is an odd prime, that $E$ has good ordinary reduction at the primes of $F$ lying above $p$, that $E$ has semistable reduction at the primes of $F$ lying above 2*

*or 3, and that* $\mathrm{Sel}_E(K_\infty)[p]$ *is finite. Suppose that* $\rho_1$ *and* $\rho_2$ *are self-dual representations of* $\Delta$ *over* $\mathcal{F}$ *and that* $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$. *Then* $W_{Iw_p}(E,\rho_1) = W_{Del}(E,\rho_1)$ *if and only if* $W_{Iw_p}(E,\rho_2) = W_{Del}(E,\rho_2)$.

The assumption about reduction at primes $v$ lying over 2 or 3 should not be needed. It is there because the existing formulas for the local root number at such primes don't cover all cases. However, we can weaken the assumption considerably. For example, an alternative assumption would be that $v \notin \Phi_{K/F}$.

One interesting special case concerns extensions $K/F$ where $\Delta = \mathrm{Gal}(K/F)$ is isomorphic to $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for some $r \geq 1$ and an odd prime $p$. We will denote this $\Delta$ by $\Delta_r$ from here on and the corresponding field of definition will be denoted by $\mathcal{F}_r$. It turns out that all representations of $\Delta_r$ are self-dual and orthogonal, i.e., realizable by orthogonal matrices over a sufficiently large field. We prove this in proposition 9.1.1. There is a Galois extension $K_0$ of $F$ contained in $K$ such that $\Delta_0 = \mathrm{Gal}(K_0/F)$ is isomorphic to $PGL_2(\mathbf{Z}/p\mathbf{Z})$. The hypothesis that $\mathrm{Sel}_E(K_\infty)[p]$ is finite turns out to be satisfied if one just assumes that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, where $K_{0,\infty}$ denotes the cyclotomic $\mathbf{Z}_p$-extension of $K_0$. If one makes that assumption and the other stated assumptions, then theorem 3 has the following consequence:

*Suppose that* $W_{Iw_p}(E,\sigma) = W_{Del}(E,\sigma)$ *for all* $\sigma \in \mathrm{Irr}_{\mathcal{F}_0}(\Delta_0)$. *Then* $W_{Iw_p}(E,\sigma) = W_{Del}(E,\sigma)$ *for all* $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$.

To study the relationship of the $W_{Del}(E,\sigma)$'s to $X_E(K)$ which was mentioned before, one uses the Cassels-Tate pairing and the orthogonality to show that the multiplicities of $\sigma$ in $X_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$ and in $X_E(K_\infty) \otimes_{\mathbf{Z}_p} \mathcal{F}$ have the same parity under certain assumptions. (See proposition 10.2.1.) We express this as an equality $W_{Sel_p}(E,\sigma) = W_{Del}(E,\sigma)$, where $W_{Sel_p}(E,\sigma)$ is defined in terms of the multiplicity of $\sigma$ in the $\Delta$-representations space $X_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$.

## 1.6 Other situations.

We now discuss another aspect of Iwasawa theory. On the analytic side of the theory, which concerns $p$-adic $L$-functions, one may consider a $\mathbf{Z}_p$-valued measure on the group $G$. Such a measure corresponds to an element $\theta$ in the completed group ring $\Lambda_G = \mathbf{Z}_p[[G]]$. Starting from $\theta$, one can then consider its image under various ring homomorphisms. For example, suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. We obtain a $\mathbf{Z}_p$-algebra homomorphism from $\mathbf{Z}_p[\Delta]$ to the ring $M_{n(\sigma)}(\mathcal{O})$ of $n(\sigma) \times n(\sigma)$ matrices over $\mathcal{O}$, which we also denote by $\sigma$. Since $\Lambda_G$ is isomorphic to $\Lambda[\Delta] = \mathbf{Z}_p[\Delta] \otimes_{\mathbf{Z}_p} \Lambda$, one can extend $\sigma$ to a $\Lambda$-algebra homomorphism from

$\Lambda_G$ to $M_{n(\sigma)}(\Lambda_{\mathcal{O}})$, where $\Lambda_{\mathcal{O}} = \mathcal{O}[[\Gamma]]$. Thus, $\sigma(\theta)$ is a matrix with entries in $\Lambda_{\mathcal{O}}$. Let us define

$$\mathcal{L}_{\theta,\sigma} \;=\; det\big(\sigma(\theta)\big),$$

an element of $\Lambda_{\mathcal{O}}$. This definition makes sense for an arbitrary representation $\sigma$ of $\Delta$ over $\mathcal{F}$, and is multiplicative for direct sums of such representations. If we fix a topological generator $\gamma_o$ of $\Gamma$, then $\Lambda$ is isomorphic to a formal power series ring $\mathbf{Z}_p[[T]]$ in one variable and $\Lambda_{\mathcal{O}}$ is isomorphic to $\mathcal{O}[[T]]$, where these isomorphisms are defined by sending $\gamma_o - id_\Gamma$ to $T$. If $\mathcal{L}_{\theta,\sigma}$ is a nonzero element of $\Lambda_{\mathcal{O}}$, then we can define its $\lambda$- and $\mu$-invariants as usual. We denote those invariants by $\lambda(\theta,\sigma)$ and $\mu(\theta,\sigma)$

Similarly, we can consider an $\mathbf{F}_p$-valued measure on $G$. This would correspond to an element $\varphi$ of the ring $\widetilde{\Lambda}_G = \mathbf{F}_p[[G]]$. We often think of that ring as $\Lambda_G/p\Lambda_G$. Let $\widetilde{\Lambda} = \Lambda/p\Lambda$. Then $\widetilde{\Lambda}_G$ can be identified with $\widetilde{\Lambda}[\Delta]$. Suppose that $\tau$ is a representation of $\Delta$ over $\mathfrak{f}$, not necessarily irreducible. Then $\tau$ defines a homomorphism from $\mathbf{F}_p[[\Delta]]$ to $M_{n(\tau)}(\mathfrak{f})$. We can extend $\tau$ to a $\widetilde{\Lambda}$-algebra homomorphism from $\widetilde{\Lambda}_G$ to the matrix ring $M_{n(\tau)}\big(\mathfrak{f}[[\Gamma]]\big)$. Thus, $\tau(\varphi)$ is a matrix with entries in $\mathfrak{f}[[\Gamma]]$. We define

$$\mathcal{L}_{\varphi,\tau} \;=\; det\big(\tau(\varphi)\big)$$

which is an element of $\mathfrak{f}[[\Gamma]]$. This ring is isomorphic to the formal power series ring $\mathfrak{f}[[T]]$, a discrete valuation ring. Assuming that $\mathcal{L}_{\varphi,\tau}$ is nonzero, we define $w(\varphi,\tau)$ to be its valuation (normalized so that the valuation of $T$ is 1). It is clear from the definition and properties of determinants that $\mathcal{L}_{\varphi,\tau}$ depends only on the semisimplification $\tau^{ss}$ of $\tau$ and that it is multiplicative for direct sums.

Suppose that $\theta \in \Lambda_G$ and $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Let $\pi$ be a generator of $\mathfrak{m}$. Assume that $\mu(\theta,\sigma) = 0$. This means that $\mathcal{L}_{\theta,\sigma}$ is not divisible by $\pi$ in $\Lambda_{\mathcal{O}}$. Let $\widetilde{\theta}$ denote the image of $\theta$ under the natural homomorphism $\Lambda_G \to \widetilde{\Lambda}_G$. Then it is not difficult to verify that the image of $\mathcal{L}_{\theta,\sigma}$ under the homomorphism $\mathcal{O}[[\Gamma]] \to \mathfrak{f}[[\Gamma]]$ defined by reduction modulo $\mathfrak{m}$ is

$$\mathcal{L}_{\widetilde{\theta},\widetilde{\sigma}} \;=\; \prod_{\tau} \mathcal{L}_{\widetilde{\theta},\tau}^{d(\sigma,\tau)} \quad , \tag{1.6.a}$$

where the product is over all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. As a consequence, $\mathcal{L}_{\widetilde{\theta},\tau}$ is nonzero for all $\tau$'s occurring in $\widetilde{\sigma}^{ss}$ with positive multiplicity and we have

$$\lambda(\theta,\sigma) = \sum_{\tau} d(\sigma,\tau) w(\widetilde{\theta},\tau) \tag{1.6.b}$$

The similarity between (1.6.b) and (1.1.c) can be explained as follows. Consider the cyclic $\Lambda_G$-module $X_\theta = \Lambda_G/\Lambda_G\theta$. We make the assumption that $\mathcal{L}_{\widetilde{\theta},\tau}$ is nonzero for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

That assumption is equivalent to the statement that $\mu(\theta,\sigma)$ is zero for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, as follows from (1.6.a). We will then show that $X_\theta$ is a free $\mathbf{Z}_p$-module of finite rank and is projective as a $\mathbf{Z}_p[\Delta]$-module. Furthermore,

$$\lambda(X_\theta,\sigma) = \lambda(\theta,\sigma), \qquad w(X_\theta,\tau) = w(\widetilde{\theta},\tau) \tag{1.6.c}$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. (See section 2.3.) We will also show that any cyclic $\Lambda_G$-module $X$ which is projective as a $\mathbf{Z}_p[\Delta]$-module is isomorphic to $X_\theta$ for some $\theta \in \Lambda_G$ satisfying the above assumption. A more general result can be found in corollary 2.4.3.

Note that under the assumptions of the previous paragraph, one will have the congruence relation (1.1.d) for the $\mathbf{Z}_p[\Delta]$-module $X_\theta$ whenever one has two representations $\rho_1$ and $\rho_2$ of $\Delta$ satisfying $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$. Therefore, (1.6.c) implies that one will have a corresponding congruence relation for the quantities $\lambda(\theta,\sigma)$. This relation also follows easily from (1.6.b). Furthermore, if $X$ is any finitely generated $\Lambda_G$-module which is torsion as a $\Lambda$-module and projective as a $\mathbf{Z}_p[\Delta]$-module, then there exists a $\theta \in \Lambda_G$ with the following property: *For all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, we have $\mu(\theta,\sigma) = 0$ and $\lambda(\theta,\sigma) = \lambda(X,\sigma)$.* The easy justification will be given in remark 2.4.4.

It is natural to try to extend the kinds of results we study in this paper to the case where $K$ is an infinite Galois extension of $F$. We intend to discuss this in a future paper [Gr09b]. One would want to assume that only finitely many primes of $F$ are ramified in $K/F$, that $K \cap F_\infty = F$, and also that $\Delta = \mathrm{Gal}(K/F)$ is essentially a pro-$p$ group. Of special interest is the case where $\Delta$ is a $p$-adic Lie group. Then $\Delta$ has a normal pro-$p$ subgroup $\Pi$ of finite index. Every irreducible representation of $\Delta$ over a finite field of characteristic $p$ factors through the finite quotient group $\Delta_0 = \Delta/\Pi$. There are only finitely many such irreducible representations. Under our assumptions, one still has $\mathrm{Gal}(K_\infty/F) \cong \Delta \times \Gamma$, where $K_\infty = KF_\infty$. Thus, $\mathrm{Gal}(K_\infty/F)$ is also a $p$-adic Lie group. The Pontryagin dual $X_E(K_\infty)$ of $\mathrm{Sel}_E(K_\infty)_p$ is a module over the completed group ring $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/F)]]$. One kind of result which can be proved is that, under suitable hypotheses, one can make a very precise statement about the structure of $X_E(K_\infty)$ as a $\mathbf{Z}_p[[\Delta]]$-module.

There is another more general setting which we will consider in this paper. Much of what we have described is valid if we just assume that $K_\infty$ is a finite Galois extension of $F_\infty$. We can then let $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$. Nothing is really lost if we assume in addition that $K_\infty$ is Galois over $F$. Then $\Delta$ will be a normal subgroup of $\mathrm{Gal}(K_\infty/F)$. One then sees easily that there is a finite Galois extension $K$ of $F$ such that $K_\infty = KF_\infty$. But, in general, one can't assume that $K \cap F_\infty = F$. That assumption is too restrictive for certain purposes. For example, the quantities $W_{Sel_p}(E,\sigma)$ and $W_{Del}(E,\sigma)$ are defined for all irreducible, self-dual Artin representations $\sigma$ of $G_F$. Such a $\sigma$ will be a faithful representation of $\mathrm{Gal}(K/F)$ for

a certain field $K$, but it can happen that $K \cap F_\infty \neq F$. We will discuss this situation in section 3.5, in the illustration in section 8.4, in chapters 10 and 12, and in section 13.3. We will tend to denote $\mathrm{Gal}(K/F)$ by $D$. Thus, the restriction map identifies $\Delta$ with a normal subgroup of $D$.

## 1.7 Organization and acknowledgements.

Let us briefly summarize the organization of this long paper. Chapters 2 and 3 give the proof of theorem 1. The rather long chapter 4 proves a number of basic results about Selmer atoms. The main objective is to prove theorem 2. The determination of $\delta_E^{\Sigma_0}(\sigma)$ is discussed in chapter 5. Chapters 6 and 8 study special situations and illustrate how the ideas of this paper can be applied. Chapter 7 discusses a wide range of groups which come up naturally as Galois groups and which occur in the illustrations of chapters 8 and 13. Chapter 9 deals with group theoretic questions that are needed for the proof of theorem 3. A fundamental duality theorem is proved in chapter 10. Finally, chapter 11 prepares the way for the proof of theorem 3 which is given in chapter 12. We close with chapter 13 which continues the arithmetic illustrations from chapter 8, but emphasizes parity questions.

This research has been partially supported by a grant from the National Science Foundation. I also want to thank IHES for its hospitality during the summer of 2002. Some of the ideas in this paper began to develop during that visit. One important inspiration was the thesis of Alexandra Nichifor [Nic], where the freeness of certain Iwasawa modules in classical Iwasawa theory is proved when $\Delta$ is cyclic of order $p$. A remark of Cornelius Greither suggesting that a cohomological argument could be used to prove such a freeness result also served as an important hint for me. I am very grateful to David Rohrlich for several helpful discussions concerning root numbers as well as providing most of the proof of Lemma 12.1.2. I have also benefited from various conversations with John Coates, Julia Pevtsova, Robert Pollack, and Karl Rubin. Finally, I want to thank the referee for many valuable suggestions which led to improvements in the organization and exposition of this paper.

# 2 Projective and quasi-projective modules.

Our main objective in this chapter is to give cohomological criteria for the projectivity or quasi-projectivity of a $\mathbf{Z}_p[\Delta]$-module $X$. This is done in section 2.1. In addition, in sections 2.2, 2.3, and 2.4, we will discuss some important points concerning the structure of $X$ as a

$\Lambda_G$-module, where $G$ is the direct product $\Delta \times \Gamma$, or even (in section 2.4) just a semidirect product $\Delta \rtimes \Gamma$.

## 2.1 Criteria for projectivity and quasi-projectivity.

We discuss these criteria in sections **A** and **B**. Some useful remarks will be in section **C**.

**A.** *Projectivity.* Suppose that $X$ is a free $\mathbf{Z}_p$-module of finite rank and that $\Delta$ is a finite group which has a $\mathbf{Z}_p$-linear action on $X$. Let $S = \mathrm{Hom}(X, \mathbf{Q}_p/\mathbf{Z}_p)$, a divisible $\mathbf{Z}_p$-module of finite corank. Of course, $\Delta$ acts on $S$ and the cohomology groups $H^i(\Delta, S)$ for $i \geq 1$ are finite and have $p$-power order. We first give a criterion for projectivity. It is not at all a new result. It is very close to Théorème 7 in [Se68]. That result concerns modules over $\mathbf{Z}[\Delta]$, but the argument found there works for modules over $\mathbf{Z}_p[\Delta]$ as well. The proof below is rather different.

**Proposition 2.1.1.** *Suppose that $H^i(\Delta', S) = 0$ for $i = 1, 2$ and for every subgroup $\Delta'$ of $\Delta$. Then $X$ is projective as a $\mathbf{Z}_p[\Delta]$-module.*

*Proof.* Let $\Pi$ denote a Sylow $p$-subgroup of $\Delta$. We will give an inductive proof to show that $X$ is a free $\mathbf{Z}_p[\Pi]$-module. Suppose at first that $\Pi$ is cyclic of order $p$. In that case, there are three non-isomorphic indecomposable $\mathbf{Z}_p[\Pi]$-modules which are free as $\mathbf{Z}_p$-modules: the free module $\mathbf{Z}_p[\Pi]$, the augmentation ideal $I_\Pi$ in $\mathbf{Z}_p[\Pi]$, and the quotient $\mathbf{Z}_p[\Pi]/I_\Pi \cong \mathbf{Z}_p$ which has a trivial action of $\Pi$. We refer the reader to [Rei] for the proof. That article considers $\mathbf{Z}[\Pi]$-modules which are free as $\mathbf{Z}$-modules, but the argument applies without change to $\mathbf{Z}_p[\Pi]$-modules. The result is simpler in that case because $\mathbf{Z}_p[\mu_p]$ is a PID. The corollary in that article shows that there are just three non-isomorphic, finitely-generated, indecomposable $\mathbf{Z}_p[\Pi]$-modules which are torsion-free as $\mathbf{Z}_p$-modules.

Consequently, $X$ is a direct sum of copies of the above indecomposable modules. We denote their Pontryagin duals by $T, S_1$, and $S_0$, respectively. Thus, $T$ has $\mathbf{Z}_p$-corank $p$, $S_1$ has $\mathbf{Z}_p$-corank $p-1$, and $S_0$ has $\mathbf{Z}_p$-corank 1. We have an isomorphism

$$S \;\cong\; S_0^a \times S_1^b \times T^c$$

as a $\mathbf{Z}_p[\Pi]$-module, where $a, b, c \geq 0$. One sees easily that

$$H^1(\Pi, S_0) \cong \mathbf{Z}/p\mathbf{Z}, \qquad H^2(\Pi, S_1) \cong \mathbf{Z}/p\mathbf{Z}$$

Since we are assuming that $H^1(\Pi, S)$ and $H^2(\Pi, S)$ are both trivial, it follows that $a = b = 0$ and hence that $X \cong \mathbf{Z}_p[\Pi]^c$, proving freeness if $|\Pi| = p$.

Now suppose that $|\Pi| = p^n$, where $n \geq 2$. Let $\Pi'$ be a normal subgroup of $\Pi$ of order $p$. Since $X$ must be $\mathbf{Z}_p[\Pi']$-free, as we just argued, it follows that $S^{\Pi'}$ is a divisible $\mathbf{Z}_p$-module, that $\mathrm{corank}_{\mathbf{Z}_p}(S) = p \cdot \mathrm{corank}_{\mathbf{Z}_p}(S^{\Pi'})$, and that $H^i(\Pi', S) = 0$ for all $i \geq 1$. Also, for any subgroup $\Pi''$ of $\Pi$ containing $\Pi'$, we have exact sequences

$$0 \longrightarrow H^1(\Pi''/\Pi', S^{\Pi'}) \longrightarrow H^1(\Pi'', S), \qquad 0 \longrightarrow H^2(\Pi''/\Pi', S^{\Pi'}) \longrightarrow H^2(\Pi'', S),$$

where the exactness of the second sequence follows from the fact that $H^1(\Pi', S) = 0$. The assumptions in the proposition then imply that $H^i(\Pi''/\Pi', S^{\Pi'}) = 0$ for $i = 1, 2$ and for every such $\Pi''$. We can therefore assume inductively that the Pontryagin dual of $S^{\Pi'}$ is a free $\mathbf{Z}_p[\Pi/\Pi']$-module. This Pontryagin dual is isomorphic to $X_{\Pi'}$, the maximal quotient of $X$ on which $\Pi'$ acts trivially, and so we have

$$X_{\Pi'} \cong \mathbf{Z}_p[\Pi/\Pi']^c$$

for some $c \geq 0$. By Nakayama's lemma, it follows that $X$ can be generated by $c$ elements as a $\mathbf{Z}_p[\Pi]$-module. That is, $X \cong \mathbf{Z}_p[\Pi]^c/Y$ where $Y$ is a submodule of $\mathbf{Z}_p[\Pi]^c$. However, we have

$$\mathrm{rank}_{\mathbf{Z}_p}(X) = p \cdot \mathrm{rank}_{\mathbf{Z}_p}(X_{\Pi'}) = p \cdot c \cdot |\Pi/\Pi'| = c \cdot |\Pi|$$

and this implies that $Y = 0$. Thus, $X \cong \mathbf{Z}_p[\Pi]^c$, as we wanted.

To finish the proof, we recall a standard argument (found in [Alp]) to deduce that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module. Let $m = [\Delta : \Pi]$ and choose a set $\{\delta_j\}_{1 \leq j \leq m}$ of left coset representatives for $\Pi$ in $\Delta$. Note that $p \nmid m$. There is a surjective $\Delta$-homomorphism

$$\psi : \mathbf{Z}_p[\Delta]^r \longrightarrow X$$

for some $r$. Since $X$ is a free $\mathbf{Z}_p[\Pi]$-module, and hence projective, there exists a splitting map $\phi : X \longrightarrow \mathbf{Z}_p[\Delta]^r$ which is a $\Pi$-homomorphism. We have $(\psi \circ \phi)(x) = x$ for all $x \in X$. Define

$$\phi' = \frac{1}{m} \sum_{j=1}^{m} \delta_j \circ \phi \circ \delta_j^{-1} \tag{2.1.a}$$

which is a map from $X$ to $\mathbf{Z}_p[\Delta]^r$ since $m \in \mathbf{Z}_p^\times$. One verifies easily that $\phi'$ is a $\Delta$-homomorphism and that $(\psi \circ \phi')(x) = x$ for all $x \in X$. Thus, $\phi'$ is a splitting map for $\psi$. This shows that $X$ is projective as a $\mathbf{Z}_p[\Delta]$-module. $\square$

**Remark 2.1.2.** The converse of proposition 2.1.1 is obvious. If $X$ is projective, then it is a direct summand in $\mathbf{Z}_p[\Delta]^r$ for some $r$. Hence $S$ is a direct summand in $T^r$, where $T$ denotes

the Pontryagin dual of $\mathbf{Z}_p[\Delta]$. Since $\mathbf{Z}_p[\Delta]$ is a free $\mathbf{Z}_p[\Delta']$-module for any subgroup $\Delta'$ of $\Delta$, it follows that $H^i(\Delta', T) = 0$ for any $i \geq 1$. Hence $H^i(\Delta', S)$ clearly vanishes for $i \geq 1$. $\Diamond$

**B.** *Quasi-projectivity.* Assume that $X$ is a finitely generated $\mathbf{Z}_p[\Delta]$-module, but not necessarily torsion-free as a $\mathbf{Z}_p$-module. We defined the notion of quasi-projectivity in the introduction. To state the definition somewhat differently, we say that $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module if the representation space $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $\Delta$ fits into an exact sequence

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V \longrightarrow 0$$

where $V_1 = Y_1 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, $V_2 = Y_2 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and both $Y_1$ and $Y_2$ are projective $\mathbf{Z}_p[\Delta]$-modules. One verifies easily that this is equivalent to the definition in the introduction. The character $\chi$ of the representation space $V$ for $\Delta$ satisfies the following property:

**(QP)** $\chi(\delta) = 0$ *for all* $\delta \in \Delta$ *of order divisible by* $p$.

This is easy to see. It suffices to check this when $X$ is projective. Suppose $\delta \in \Delta$ has order divisible by $p$. Let $C$ be a cyclic subgroup of $\Delta$ containing $\delta$. Then $X$ is projective as a $\mathbf{Z}_p[C]$-module. Let $C = PQ$, where $P$ is a nontrivial $p$-group and $Q$ has order prime to $p$. Let $\mathcal{O}$ be the extension of $\mathbf{Z}_p$ generated by roots of unity of order $|Q|$, let $\varepsilon$ be any 1-dimensional character of $Q$, and let $e_\varepsilon$ be the idempotent for $\varepsilon$ in $\mathcal{O}[Q]$. Then $X_\mathcal{O} = X \otimes_{\mathbf{Z}_p} \mathcal{O}$ is a projective $\mathcal{O}[C]$-module and is isomorphic to the direct sum of the modules $X^{(\varepsilon)} = e_\varepsilon X_\mathcal{O}$, each of which is also projective as an $\mathcal{O}[C]$-module. It follows that $X^{(\varepsilon)}$ is projective and hence free as a $\mathbf{Z}_p[P]$-module. Let $\mathcal{F}$ be the fraction field of $\mathcal{O}$, $V_\mathcal{F} = V \otimes_{\mathbf{Q}_p} \mathcal{F}$, and $V^{(\varepsilon)} = e_\varepsilon V_\mathcal{F}$, the $\varepsilon$-component of $V$ as a representation space for $Q$. Then $V^{(\varepsilon)}$ is a representation space for $C$, and its restriction to $P$ is a multiple of the regular representation for $P$. The projection of $\delta$ to $P$ is nontrivial and therefore the trace of $\delta$ acting on $V^{(\varepsilon)}$ is 0. Since this is so for every $\varepsilon$, it indeed follows that $\chi(\delta) = 0$.

The converse is also true: If the character of the representation space $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ has the property **(QP)**, then $X$ is quasi-projective. This is proved in [Se77], theorem 36. One of the ingredients in the argument is that the characters of the representations $P_\tau \otimes_{\mathbf{Z}_p} \mathcal{F}$ are $\mathbf{Q}$-linearly independent and must be a basis for the $\mathbf{Q}$-vector space of characters satisfying property **(QP)**, which clearly has dimension $t$. Thus, **(QP)** is a necessary and sufficient condition for $X$ to be quasi-projective. We will use this to prove a criterion for quasi-projectivity in terms of the $\mathbf{Z}_p[\Delta]$-module $S = \mathrm{Hom}(X, \mathbf{Q}_p/\mathbf{Z}_p)$. We will use the same notation $C = PQ$ as above for any cyclic subgroup $C$ of $\Delta$. We let $S^{(\varepsilon)} = e_\varepsilon S_\mathcal{O}$. Here $S_\mathcal{O} = S \otimes_{\mathbf{Z}_p} \mathcal{O}$, which can be defined for any $\mathbf{Z}_p[\Delta]$-module $S$. Let $h_P(A)$ denote the Herbrand quotient $|H^2(P, A)|/|H^1(P, A)|$. In the following, we assume that $X$ is finitely-generated as a $\mathbf{Z}_p$-module.

**Proposition 2.1.3.** *The $\mathbf{Z}_p[\Delta]$-module $X$ is quasi-projective if and only if the following criterion is satisfied: For every cyclic subgroup $C = PQ$ of $\Delta$ and every character $\varepsilon$ of $Q$, we have $h_P(S^{(\varepsilon)}) = 1$.*

*Proof.* The implication in one direction is straightforward. If $X$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module, then there exist finitely-generated, projective $\mathbf{Z}_p[\Delta]$-modules $Y_1$ and $Y_2$ and a sequence

$$0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow \longrightarrow X \longrightarrow 0$$

which exactness at each step only fails by a finite group. If $C = PQ$ is a cyclic subgroup of $\Delta$, then $Y_1$ and $Y_2$ are projective $\mathbf{Z}_p[C]$-modules. It follows that the $\varepsilon^{-1}$-components of both $Y_1 \otimes_{\mathbf{Z}_p} \mathcal{O}$ and $Y_2 \otimes_{\mathbf{Z}_p} \mathcal{O}$ are free $\mathcal{O}[P]$-modules. The fact that the Herbrand quotient is 1 for finite modules and behaves multiplicatively in exact sequences, then implies that $h_P(S^{(\varepsilon)}) = 1$.

For the other implication, we assume the triviality of all the Herbrand quotients. First consider the special case where $\Delta$ is itself a cyclic $p$-group. Let $|\Delta| = p^n$. For each $j$, $0 \leq j \leq n$, let $P_j$ denote the subgroup of $\Delta$ of order $p^j$. For each $k$, $0 \leq k \leq n$, let $W_k$ denote the irreducible representation space for $\Delta$ over $\mathbf{Q}_p$ whose kernel is the subgroup of index $p^k$, i.e., the subgroup $P_{n-k}$. Thus, $W_0$ is the trivial representation space for $\Delta$, $W_1$ is a faithful representation of $\Delta/\Delta^p$ of dimension $p-1$, etc.. One can identify $W_k$ with $\mathbf{Q}_p[\mu_{p^k}]$, where a generator of $\Delta$ acts by multiplication by a generator of $\mu_{p^k}$. Let $n_k = \dim_{\mathbf{Q}_p}(W_k)$. We have $n_k = p^{k-1}(p-1)$ if $k \geq 1$ and $n_0 = 1$. Choose a $\Delta$-invariant $\mathbf{Z}_p$-lattice $L_k$ in $W_k$ and let $S_k = W_k/L_k$. Then $V \cong \bigoplus_{k=0}^n W_k^{\lambda_k}$, say. Therefore,

$$S \approx \bigoplus_{k=0}^{n} S_k^{\lambda_k}$$

where $\approx$ means that there is a $\Delta$-equivariant map with finite kernel and cokernel (which implies that the map is surjective here).

Our assumption is that $h_{P_j}(S) = 1$, or equivalently, $\prod_{k=0}^n h_{P_j}(S_k)^{\lambda_k} = 1$ for all $j$'s. Note that $\prod_{k=0}^n S_k \approx \mathbf{Z}_p[\Delta] \otimes_{\mathbf{Z}_p} (\mathbf{Q}_p/\mathbf{Z}_p)$, a cohomologically trivial module. Hence $\prod_{k=0}^n h_{P_j}(S_k) = 1$ for each $j$. For $1 \leq j \leq n$, $0 \leq k \leq n$, we let $h_{P_j}(S_k) = p^{a_{jk}}$, where $a_{jk} \in \mathbf{Z}$. With this notation, our assumption is that the $\lambda_k$'s satisfy the linear equations

$$\sum_{k=0}^{n} a_{jk}\lambda_k = 0 \tag{2.1.b}$$

for $1 \leq j \leq n$ (ignoring the trivial equation corresponding to $j = 0$). One solution to these equations is $\lambda_0 = \lambda_1 = ... = \lambda_n = 1$. We want to prove that every solution to these equations

is a scalar multiple of that solution. That will imply that $S \approx \left(\mathbf{Z}_p[\Delta] \otimes_{\mathbf{Z}_p} (\mathbf{Q}_p/\mathbf{Z}_p)\right)^{\lambda}$ for some integer $\lambda \geq 0$ and hence that $X$ will indeed be quasi-projective.

We will prove that the coefficient matrix $A = [a_{jk}]$ for the above system of equations has rank $n$ and so the solutions are just constant multiples of the solution given by $\lambda_k = 1$ for $0 \leq k \leq n$, as we want. We can see this by applying some column operation to that $n \times (n+1)$ matrix. For any $k$, $0 \leq k \leq n$, suppose that $j$ satisfies $j + k \leq n$. Then $P_j$ acts trivially on $W_k$ and hence on $S_k$. Hence $H^1(P_j, S_k) = \mathrm{Hom}(P_j, S_k)$ and this has order $p^{jn_k}$, where $n_k$ is as defined above. Also, it is clear that $H^2(P_j, S_k) = 0$. Thus, $a_{jk} = -jn_k$ for such $j$ and $k$. On the other hand, if $k \geq 1$ and $j + k = n + 1$, then $P_j$ acts non-trivially on $S_k$ (through the quotient group of order $p$), $H^1(P_j, S_k) = 0$, and $H^2(P_j, S_k) \cong S_k^{P_j}$, a finite group isomorphic to $\mathbf{Z}_p[\mu_{p^k}]/(\zeta_p - 1)$, where $\zeta_p$ is a generator of $\mu_p$. This finite group has order $p^{p^{k-1}}$ and therefore $a_{jk} = p^{k-1}$. Note that this is positive and so is not equal to $-jn_k$.

Denote the columns in $A$ by $A_0, A_1, ..., A_n$. The first column $A_0$ in $A$ has entries $-1, ..., -n$. For each $k \geq 1$, the $j$-th entry in $B_k = A_k - n_k A_0$ is 0 if $j + k \leq n$, but the $j$-th entry is nonzero when $j + k = n + 1$. Thus, $B_1, ..., B_n$ are linearly independent and so, indeed, $A$ has rank $n$. We remark that for odd $p$, one can give a somewhat simpler argument. Namely, note that the $n_k$'s are even for $k \geq 1$. Thus, the $j$-th entry in $A_k$ is even if $j + k \leq n$, but is odd if $j + k = n + 1$. Hence the matrix with columns $A_1, ..., A_n$ clearly has odd determinant, assuming $p$ is odd, and hence that matrix is nonsingular.

Now assume that $\Delta$ is arbitrary and that $C = PQ$ is a cyclic subgroup of $\Delta$ as notated above. We can apply the result just proved to the cyclic $p$-group $P$ and to $S^{(\varepsilon)}$ for any character $\varepsilon$ of $Q$. It follows that the Pontryagin dual of $S^{(\varepsilon)}$ is quasi-projective as a $\mathbf{Z}_p[P]$-module. Let $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, $V_{\mathcal{F}} = V \otimes_{\mathbf{Q}_p} \mathcal{F}$, as before, and let $\chi$ be the corresponding character (of $C$ or of $\Delta$). Regarding $V_{\mathcal{F}}$ as a representation space for $C$, we now know that $V_{\mathcal{F}}^{(\varepsilon^{-1})} = e_{\varepsilon^{-1}} V_{\mathcal{F}}$ is isomorphic to the tensor product of the representation $\varepsilon^{-1}$ of $Q$ and some multiple of the regular representation of $P$. Thus, the character of this representation of $C$ is identically 0 on the elements of order divisible by $p$. Since this is so for every $\varepsilon$, it follows that $\chi|_C$ has the same property. Consequently, since $C$ is arbitrary, $\chi$ satisfies the property **(QP)** and therefore $X$ is indeed quasi-projective. □

**Remark 2.1.4.** It is proved in [Se77] (corollary 2 to theorem 34) that if $Y$ is a finitely-generated, projective $\mathbf{Z}_p[\Delta]$-module, then the isomorphism class of $Y$ is determined by the $\Delta$-representation space $V = Y \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. We already mentioned this fact at the beginning of the introduction. Consequently, if $X$ is a $\Delta$-invariant $\mathbf{Z}_p$-lattice in $V$ which is not isomorphic to $Y$ as a $\mathbf{Z}_p[\Delta]$-module, then $X$ cannot be projective. However, it is clear from the definition that $X$ will be quasi-projective. Such examples are easy to give. In the special case where $\Delta$ is a $p$-group, a $\mathbf{Z}_p[\Delta]$-module $Y$ is projective if and only if it is free, and so one would just need to check that $X$ is not free.

As a simple example, suppose that $\Delta$ is cyclic of order $p$ and that $Y$ is a free $\mathbf{Z}_p[\Delta]$-module of rank 1. Then $V$ is just the regular representation for $\Delta$ over $\mathbf{Q}_p$. Using the notation in the proof of proposition 2.1.3, we have $V \cong W_0 \oplus W_1$ and $X = L_0 \oplus L_1$ is a $\Delta$-invariant $\mathbf{Z}_p$-lattice in $V$. Thus, $X$ is quasi-projective, but $X \ncong Y$ because $Y$ is a cyclic $\mathbf{Z}_p[\Delta]$-module, but $X$ requires two generators. Hence $X$ is quasi-projective, but not projective. One finds similar examples if one takes $\Delta$ to be cyclic of order $p^n$. In fact, the number of isomorphism classes of $\Delta$-invariant $\mathbf{Z}_p$-lattices increases with $n$.

If $\Delta$ is a $p$-group, then a finitely-generated $\mathbf{Z}_p[\Delta]$-module $X$ is quasi-projective if and only if $X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a free $\mathbf{Q}_p[\Delta]$-module. This follows easily from the definition. Consequently, $X$ is quasi-projective if and only if there exists a free $\mathbf{Z}_p[\Delta]$-module $Y$ and a $\mathbf{Z}_p[\Delta]$-homomorphism $X \to Y$ with finite kernel and cokernel. In general, for an arbitrary finite group $\Delta$, a strictly quasi-projective module (as defined at the end of section 1.1) is certainly quasi-projective. However, the converse is not always true. The issue is whether or not property (**QP**) implies that a representation space $V$ contains a $\Delta$-invariant $\mathbf{Z}_p$-lattice which is projective as a $\mathbf{Z}_p[\Delta]$-module. We refer the reader to chapter 16.3 in [Se77] for a discussion of this issue. Theorem 38 there shows that quasi-projectivity and strict quasi-projectivity are equivalent if $\Delta$ is a $p$-solvable group. $\Diamond$

Suppose that $X$ is a finitely-generated $\mathbf{Z}_p[\Delta]$-module. As in the introduction, we can define $\lambda_X : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathbf{Z}$ to be the unique group homomorphism satisfying $\lambda_X(\sigma) = \lambda(X, \sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Recall that $\lambda(X, \sigma)$ is the multiplicity of $\sigma$ in the representation space $V_{\mathcal{F}} = X \otimes_{\mathbf{Z}_p} \mathcal{F}$ for $\Delta$. The next proposition gives another criterion for quasi-projectivity. The first part was already pointed out in the introduction. For brevity, we let $\mathrm{Rep}_{\mathcal{F}}(\Delta)$ denote the set of representations for $\Delta$ over $\mathcal{F}$, considered as a subset of $\mathcal{R}_{\mathcal{F}}(\Delta)$.

**Proposition 2.1.5.** *Suppose that $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module. Then the following statement is true:*

*If $\rho_1,\ \rho_2 \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$ and $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$, then $\lambda_X(\rho_1) = \lambda_X(\rho_2)$ .*

*Conversely, if this statement is true, then $X$ is quasi-projective.*

*Proof.* We just need to consider the converse. So suppose that the function $\lambda_X$ has the stated property. This means that $\lambda_X$ factors through the decomposition homomorphism $d : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathcal{R}_{\mathfrak{f}}(\Delta)$ and so there is a function $w_X : \mathcal{R}_{\mathfrak{f}}(\Delta) \to \mathbf{Z}$ such that $\lambda_X = w_X \circ d$. We can assume that $w_X(\tau) \geq 0$ for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$ without loss of generality just by replacing $X$ by $X \oplus \mathbf{Z}_p[\Delta]^t$ for a sufficiently large value of $t$, if necessary. Making that assumption, consider $Y = \oplus_\tau P_\tau^{w_X(\tau)}$, a projective $\mathbf{Z}_p[\Delta]$-module. Then

$$\lambda(Y, \sigma) \ = \ \sum_\tau \ w_X(\tau) d(\sigma, \tau) \ = \ \lambda(X, \sigma)$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and hence $Y \otimes_{\mathbf{Z}_p} \mathcal{F} \cong X \otimes_{\mathbf{Z}_p} \mathcal{F}$ as $\mathcal{F}$-representation spaces for $\Delta$. It follows that $X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $Y \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ are isomorphic as $\mathbf{Q}_p$-representation spaces for $\Delta$, proving that $X$ is indeed quasi-projective. $\square$

**C.** *Useful remarks.* Suppose that we have finitely-generated $\mathbf{Z}_p$-modules $X_j$ for $j = 1, 2, 3$ which have $\mathbf{Z}_p$-linear actions of $\Delta$. Let $S_j = \mathrm{Hom}(X_j, \mathbf{Q}_p/\mathbf{Z}_p)$. Suppose that these discrete modules fit into an exact sequence

$$0 \longrightarrow S_1 \longrightarrow S_2 \longrightarrow S_3 \longrightarrow 0$$

of $\mathbf{Z}_p[\Delta]$-modules. Then proposition 2.1.3 together with the multiplicativity of Herbrand quotients in exact sequences implies the following result:

**Remark 2.1.6.** *If any two of the modules $X_j$ are quasi-projective, then so is the third.*

This is also obvious from considering the characters of the representation spaces $X_j \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. If two of the characters satisfy property **(QP)**, then so does the third. $\lozenge$

Assume now that $X_j$ is a free $\mathbf{Z}_p$-module of finite rank for $j = 1, 2, 3$ and that the Pontryagin duals $S_j$ fit into an exact sequence as above. Of course, the $X_j$'s also fit into a similar exact sequence, but in the reverse order. Then the following result is true:

**Remark 2.1.7.** *If any two of the modules $X_j$ are projective as $\mathbf{Z}_p[\Delta]$-modules, then so is the third.*

By definition, if $X_1$ is assumed to be projective, then the exact sequence splits and we have an isomorphism $X_2 \cong X_1 \oplus X_3$. Therefore, $X_2$ is projective if and only if $X_3$ is projective. Assume instead that $X_3$ is a projective $\mathbf{Z}_p[\Delta]$-module. Then, for any subgroup $\Delta'$ of $\Delta$, we have $H^i(\Delta', S_3) = 0$ for $i \geq 1$. Also, $X_3$ will be a direct summand in a free $\mathbf{Z}_p[\Delta']$-module. It follows easily that $H^0(\Delta', S_3)$ is a divisible $\mathbf{Z}_p$-module. Using this together with the fact that $H^1(\Delta', S_1)$ is finite, we see that the map $H^0(\Delta', S_2) \to H^0(\Delta', S_3)$ must be surjective. Consequently, one has $H^i(\Delta', S_1) \cong H^i(\Delta', S_2)$ for all $i \geq 1$. Thus, by proposition 2.1.1 and remark 2.1.2, the projectivity of $X_1$ and $X_2$ as $\mathbf{Z}_p[\Delta]$-modules will be equivalent. $\lozenge$

**Remark 2.1.8.** This concerns induction from a subgroup $\Delta_*$ of $\Delta$. Suppose that $X_*$ is a free $\mathbf{Z}_p$-module with a $\mathbf{Z}_p$-linear actions of $\Delta_*$. Let $X = X_* \otimes_{\mathbf{Z}_p[\Delta_*]} \mathbf{Z}_p[\Delta]$. It is easy to see that if $X_*$ is a projective $\mathbf{Z}_p[\Delta_*]$-module, then $X$ is a projective $\mathbf{Z}_p[\Delta]$-module. As a consequence, a similar statement is true for strictly quasi-projective modules. Using the fact that induction is an exact functor for representation spaces, the same statement follows for quasi-projective modules. One can also easily justify this assertion by using property **(QP)**. In particular, suppose that $|\Delta_*|$ is not divisible by $p$. Let $V_* = X_* \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and let $V = \mathrm{Ind}_{\Delta_*}^{\Delta}(V_*)$ be the

induced representation of $\Delta$. Then every $\Delta$-invariant $\mathbf{Z}_p$-lattice in $V$ will be quasi-projective as a $\mathbf{Z}_p[\Delta]$-module.

One other simple remark concerning induction has nothing to do with projectivity. Suppose that $X$ is a finitely generated $\mathbf{Z}_p[\Delta]$-module and that $\sigma_* \in \mathrm{Irr}_{\mathcal{F}}(\Delta_*)$. Suppose that

$$\mathrm{Ind}_{\Delta_*}^{\Delta}(\sigma_*) \;\cong\; \bigoplus_{\sigma} \sigma^{m(\sigma)} \quad ,$$

where $\sigma$ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $m(\sigma) \geq 0$. Then

$$\sum_{\sigma} m(\sigma)\lambda(X,\sigma) \;=\; \lambda(X,\sigma_*) \quad ,$$

where $\lambda(X,\sigma_*)$ is defined by viewing $X$ as a $\mathbf{Z}_p[\Delta_*]$-module. This equality is an immediate consequence of Frobenius reciprocity. In particular, if $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\sigma \cong \mathrm{Ind}_{\Delta_*}^{\Delta}(\sigma_*)$, then $\lambda(X,\sigma) \;=\; \lambda(X,\sigma_*)$. $\Diamond$

**Remark 2.1.9.** This remark also concerns induction. Suppose that $C = PQ$ is a finite cyclic group as in proposition 2.1.3 and that $C_*$ is a subgroup of $C$. We then have $C_* = P_*Q_*$, where $P_* = P \cap C_*$ and $Q_* = Q \cap C_*$, cyclic groups of $p$-power order and of order prime to $p$, respectively. Suppose that $\mathcal{A}_*$ is a $\mathbf{Z}_p[C_*]$-module which has the discrete topology and is a torsion $\mathbf{Z}_p$-module. We will assume that the cohomology groups $H^i(P_*, \mathcal{A}_*)$ for $i \geq 1$ are all finite. Let $\mathcal{A} = \mathrm{Ind}_{C_*}^{C}(\mathcal{A}_*)$. Let $\varepsilon$ be an $\mathcal{O}^{\times}$-valued character of $Q$ and let $\varepsilon_* = \varepsilon|_{Q_*}$. Then

$$h_P\big(\mathcal{A}^{(\varepsilon)}\big) \;=\; h_{P_*}\big(\mathcal{A}_*^{(\varepsilon_*)}\big) \quad . \tag{2.1.c}$$

We will later apply this equality in a situation where $C$ is a Galois group, $C_*$ is the decomposition subgroup of $C$ for some prime, and $\mathcal{A}_*$ may have infinite $\mathbf{Z}_p$-corank. Thus, proposition 2.1.3 may not be useful in such a situation.

For the justification, we may assume that $\mathcal{A}_*$ is already an $\mathcal{O}$-module. Furthermore, for a fixed $\varepsilon$, the $\varepsilon$-components for the action of $Q$ on $\mathcal{A}$ and on $\mathrm{Ind}_{C_*}^{C}(\mathcal{A}^{(\varepsilon_*)})$ are isomorphic as $\mathcal{O}[C]$-modules. Hence we can simply reduce to the case where $Q_*$ acts on $\mathcal{A}_*$ by the character $\varepsilon_*$. Also, if we let $\mathcal{B}_* = \mathcal{A}_* \otimes \varepsilon_*^{-1}$, then $\mathcal{B} = \mathrm{Ind}_{C_*}^{C}(\mathcal{B}_*)$ is isomorphic to $\mathcal{A} \otimes \varepsilon^{-1}$. The $\varepsilon$-component of $\mathcal{A}$ is isomorphic to the $\varepsilon_0$-component of $\mathcal{B}$ for the action of $P$, where $\varepsilon_0$ is the trivial character of $Q$. Hence the corresponding Herbrand quotients are equal. A similar statement is true for the action of $P_*$ on the corresponding components of $\mathcal{A}_*$ and $\mathcal{B}_*$. Thus, by replacing $\mathcal{A}_*$ by $\mathcal{B}_*$ if necessary, we can simply consider the case where $Q_*$ acts trivially on $\mathcal{A}_*$. Then, by replacing $C$ by $C/Q_*$ and $C_*$ by $C_*/Q_*$, we can therefore reduce to the case where $Q_*$ is trivial and $C_* = P_*$.

Let $\mathcal{A}_P = \mathrm{Ind}_{P_*}^{P}(\mathcal{A}_*)$. Shapiro's lemma states that $H^i(P, \mathcal{A}_P) \cong H^i(P_*, \mathcal{A}_*)$ for all $i$. Let $\varepsilon$ be any character of $Q$. Since $\mathcal{A} = \mathrm{Ind}_{P}^{C}(\mathcal{A}_P)$, one sees easily that $\mathcal{A}^{(\varepsilon)} \cong \mathcal{A}_P$ as an $\mathcal{O}[P]$-module. It follows that $H^i(P, \mathcal{A}^{(\varepsilon)}) \cong H^i(P_*, \mathcal{A}_*)$ for all $i$. The stated equality of the Herbrand quotients follows from this. $\Diamond$

## 2.2 Nonzero $\mu$-invariant.

We have assumed so far in this chapter that $X$ is a finitely-generated, free $\mathbf{Z}_p$-module (in proposition 2.1.1) or just finitely-generated as a $\mathbf{Z}_p$-module (in proposition 2.1.3), and that there is a $\mathbf{Z}_p$-linear action of $\Delta$ on $X$. Our primary interest is in examples where $X$ is also a $\Lambda$-module and the action of $\Delta$ on $X$ is $\Lambda$-linear. Here $\Lambda = \mathbf{Z}_p[[\Gamma]]$, as in the introduction, and such a module $X$ can be regarded as a $\Lambda_G$-module, where $G = \Delta \times \Gamma$ and $\Lambda_G$ is the corresponding completed $\mathbf{Z}_p$-group algebra. We have $\Lambda_G \cong \Lambda[\Delta]$.

It would be useful to be able to consider any finitely-generated, torsion $\Lambda$-module $X$ with such an action of $\Delta$. For such a $\Lambda$-module, the $\mathbf{Z}_p$-torsion subgroup is a $\Lambda$-submodule and has bounded exponent. More precisely, for any $m \geq 1$, let $X[p^m] = \{x \in X \mid p^m x = 0\}$. Then, for some $m$, the $\mathbf{Z}_p$-torsion subgroup of $X$ is $X[p^m]$ and the quotient $X/X[p^m]$ is a free $\mathbf{Z}_p$-module of finite rank. If the $\mu$-invariant $\mu(X)$ is positive (or equivalently, if the $\mathbf{Z}_p$-torsion submodule of $X$ is infinite), then $X[p]$ will be infinite and $X$ will not be finitely-generated as a $\mathbf{Z}_p$-module. The propositions in section 2.1 will fail in general. However, it is still possible for $X/X[p^m]$ to be projective or quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. If that is so, then we will obtain the same congruence relations for the invariants $\lambda(X, \sigma)$. Those invariants depend only on $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. The only positive result we can prove is the following.

**Proposition 2.2.1.** *Suppose that $X$ is a $\Lambda[\Delta]$-module which is finitely-generated and torsion as a $\Lambda$-module. Let $S$ denote the Pontryagin dual of $X$. Assume that $X/X[p]$ is finitely-generated as a $\mathbf{Z}_p$-module and that $H^1(P, S)$ and $H^2(P, S)$ are finite for every cyclic $p$-subgroup $P$ of $\Delta$. Then $X/X[p]$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module if and only if the following criterion is satisfied: $h_P(S^{(\varepsilon)}) = 1$ for every $P$ and $\varepsilon$ (as in proposition 2.1.3).*

It turns out that an extremely similar result was proved in [HaSh]. (See the lemmas for the proof of their theorem 2.1. ) Our proof is somewhat different, although close in its essential idea.

*Proof.* Our assumptions imply that, for all $P$'s and $\varepsilon$'s, $H^1(P, S^{(\varepsilon)})$ and $H^2(P, S^{(\varepsilon)})$ are both finite. This is because $S^{(\varepsilon)}$ is a direct summand in $S_{\mathcal{O}}$, which in turn is a direct sum of a finite number of copies of $S$, all considered as $\mathbf{Z}_p[P]$-modules. Hence $h_P(S^{(\varepsilon)})$ is defined. Consider the $\Lambda[\Delta]$-submodule $pS$ of $S$. Then $pS$ is isomorphic to the Pontryagin dual of

$X/X[p]$ and, by assumption, is a cofinitely-generated $\mathbf{Z}_p$-module. Thus, $h_P(pS^{(\varepsilon)})$ is also defined for all $P$ and $\varepsilon$. We can apply proposition 2.1.3: $X/X[p]$ is quasi-projective if and only if $h_P(pS^{(\varepsilon)}) = 1$ for all $P$'s and $\varepsilon$'s. Thus, we must just prove that $h_P(pS^{(\varepsilon)}) = h_P(S^{(\varepsilon)})$. Equivalently, we must show that $h_P(U^{(\varepsilon)}) = 1$, where $U = S/pS$. Note that $U$ is isomorphic to the Pontryagin dual of $X[p]$.

Fix a $P$ and $\varepsilon$. Let $n = |P|$, a power of the prime $p$. It is easy to see that $H^i(P, pS^{(\varepsilon)})$ is finite for all $i \geq 1$. This is simply because $pS^{(\varepsilon)}$ has only finitely many elements killed by $n$. It follows that $H^i(P, U^{(\varepsilon)})$ is also finite for $i = 1, 2$. We will study the corresponding Herbrand quotient.

The Pontryagin dual of $U^{(\varepsilon)}$ is $X[p]^{(\varepsilon^{-1})}$, which is a finitely-generated module over the ring $\mathbf{F}_p[[\Gamma \times P]]$. Now $P$ is a cyclic $p$-group. Let $g$ be a generator for $P$ and let $\gamma$ be a topological generator for $\Gamma$. Thus, $\gamma$ and $g$ generate $\Gamma \times P$ topologically. We can regard $X[p]^{(\varepsilon^{-1})}$ as a finitely-generated module over the formal power series ring $R = \mathbf{F}_p[[x, y]]$ by letting $x$ act as $\gamma - id_\Gamma$ and $y$ act as $g - id_P$. Since $g$ has order $n$, this module is annihilated by $y^n$ and hence is a torsion $R$-module. The standard classification theorem for torsion modules over $R$ (which is a regular local ring of Krull dimension 2 and residue field $\mathbf{F}_p$) implies that $X[p]^{(\varepsilon^{-1})}$ is pseudo-isomorphic to a direct sum of modules of the form $E_a = R/(y^a)$, where $1 \leq a \leq n$. Pseudo-null $R$-modules are finite in this case. Thus, for some $t \geq 0$ and $a_1, ..., a_t$ satisfying $0 \leq a_j \leq n$, there is an $R$-module homomorphism

$$U^{(\varepsilon)} \longrightarrow \bigoplus_{j=1}^{t} \mathrm{Hom}(E_{a_j}, \mathbf{F}_p) \tag{2.2.a}$$

of discrete $R$-modules with finite kernel and cokernel. (In fact, the cokernel must be trivial.)

Our assumptions imply that $H^i(P, U^{(\varepsilon)})$ is finite for $i = 1, 2$, as we mentioned above. It follows that $H^i\big(P, \mathrm{Hom}(E_{a_j}, \mathbf{F}_p)\big)$ is also finite for $i = 1, 2$ and for each $j$. By taking Pontryagin duals, this implies that, for each of the summands $E_a$ occurring above, the groups $H^i(P, E_a)$ are also finite. Note that the map defined by $g - id_P$ is multiplication by $y$ and the norm map for $P$ corresponds to multiplication by $y^{n-1}$. Hence, we have

$$H^1(P, E_a) = Ker(y^{n-1} : E_a \to E_a)/yE_a \ , \qquad H^2(P, E_a) = Ker(y : E_a \to E_a)/y^{n-1}E_a \ .$$

If $a < n$, then both of these groups will be infinite. Thus, we must have $a_j = n$ for $1 \leq j \leq t$. But $E_n$ is a free module of rank 1 over the ring $R/(y^n) \cong \mathbf{F}_p[[x]][P]$ and both of the cohomology groups will be trivial in that case. Hence, the Herbrand quotient will be 1. The Herbrand quotients for the kernel and cokernel of the map (2.2.a) will be 1 too. It follows that we indeed have $h_P(U^{(\varepsilon)}) = 1$. This will be so for all choices of $P$ and $\varepsilon$. $\square$

**Remark 2.2.2.** The kind of result just proved can fail if $X[p^2]/X[p]$ is infinite. We have no substitute in such a case. Consider the following specific example (which can also be

found in [HaSh]). Suppose that $\Delta = P$ is cyclic of order $p$. Identify $\Lambda$ with $\mathbf{Z}_p[[T]]$. Suppose that $X = \Lambda/(p^2T)$. Let the generator $g$ for $P$ act on $X$ as multiplication by $1+pT$, which is indeed an automorphism of $X$ of order $p$. One sees easily that $X/X[p^2] \cong \mathbf{Z}_p$ and that $P$ acts trivially on that quotient. Thus, $X/X[p^2]$ is not quasi-projective as a $\mathbf{Z}_p[P]$-module. In fact, one has $\lambda(X, \sigma_0) = 1$, but $\lambda(X, \sigma) = 0$ for the other irreducible representations $\sigma$ of $P$. However, if $S = \mathrm{Hom}(X, \mathbf{Q}_p/\mathbf{Z}_p)$, then it turns out that $H^1(P, S) = H^2(P, S) = 0$. To see this, note that $g-1$ acts on $X$ as multiplication by $pT$ and the norm $N_P$ acts on $X$ as multiplication by

$$\sum_{j=0}^{p-1} (1+pT)^j \;=\; pu$$

where $u \in \Lambda^\times$. Hence $ker(N_P) = (pT)/(p^2T) = im(g-1)$. This implies that $H^2(P, S) = 0$. Also, $im(N_P) = (p)/(p^2T) = ker(g-1)$, which implies that $H^1(P, S) = 0$. $\Diamond$

## 2.3 The structure of $\Lambda_G/\Lambda_G\theta$.

The module $X$ occurring in remark 2.2.2 can alternatively be described as follows. Let $\theta = g - 1 - pT$, viewed as an element of $\Lambda_G$ for $G = \Delta \times \Gamma$. Then $X = \Lambda_G/\Lambda_G\theta$. Now we discuss modules of this same form, justifying the statements made in section 1.6. Suppose that $\theta$ is any nonzero element of $\Lambda_G$ and let $X = \Lambda_G/\Lambda_G\theta$. This $\Lambda_G$-module was denoted by $X_\theta$ in the introduction. It is obviously finitely-generated as a $\Lambda$-module.

Recall that $\Lambda_{\mathcal{O}} = \mathcal{O}[[\Gamma]]$. We identify $\Lambda_G \otimes_{\mathbf{Z}_p} \mathcal{O}$ with $\Lambda_{\mathcal{O}}[\Delta]$. Let $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Then we have an $\mathcal{O}$-algebra homomorphism $\mathcal{O}[\Delta] \longrightarrow M_{n(\sigma)}(\mathcal{O})$. Tensoring with $\Lambda_{\mathcal{O}}$, we obtain a continuous $\Lambda_{\mathcal{O}}$-algebra homomorphism which we also denote by $\sigma$:

$$\sigma : \; \Lambda_{\mathcal{O}}[\Delta] \;\longrightarrow\; M_{n(\sigma)}(\Lambda_{\mathcal{O}}) \;\;,$$

The image of $\sigma$ is a $\Lambda_{\mathcal{O}}$-subalgebra of $M_{n(\sigma)}(\Lambda_{\mathcal{O}})$ which we denote by $R_\sigma$. The cokernel of $\sigma$ is a torsion-group of exponent dividing $|\Delta|$ which we denote by $Z_\sigma$. It is a two-sided $R_\sigma$-module. As in the introduction, we will denote $det\big(\sigma(\theta)\big)$ by $\mathcal{L}_{\theta,\sigma}$. One sees easily that $X$ is a torsion $\Lambda$-module if and only if $\mathcal{L}_{\theta,\sigma} \neq 0$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$.

Let $I_\sigma = \ker(\sigma)$, an ideal in $\Lambda_{\mathcal{O}}[\Delta]$. Let $X_{\mathcal{O}} = X \otimes_{\mathbf{Z}_p} \mathcal{O} \cong \Lambda_{\mathcal{O}}[\Delta]/\Lambda_{\mathcal{O}}[\Delta]\theta$. We define

$$X_\sigma \;=\; X_{\mathcal{O}}/I_\sigma X_{\mathcal{O}}, \qquad\qquad S_\sigma = \mathrm{Hom}_\Delta(X,\; W_\sigma/L_\sigma),$$

where $W_\sigma$ is the underlying $\mathcal{F}$-representation space for $\sigma$ and $L_\sigma$ is a $\Delta$-invariant $\mathcal{O}$-lattice in $W_\sigma$. Assume that $X$ is a torsion $\Lambda$-module. Then, as $\Lambda_{\mathcal{O}}$-modules, $X_\sigma$ is finitely-generated

and torsion, $S_\sigma$ is cofinitely-generated and cotorsion. The elements of $S_\sigma$ factor through $X_\sigma$. We have the following isomorphism:

$$X_\sigma \;\cong\; R_\sigma \big/ R_\sigma\sigma(\theta) \quad .$$

Assume that $\mathcal{L}_{\theta,\sigma} \neq 0$. Right multiplication by $\sigma(\theta)$ defines $\Lambda_\mathcal{O}$-module endomorphisms of $R_\sigma, M_{n(\sigma)}(\Lambda_\mathcal{O})$, and $Z_\sigma$, considered as left modules. The snake lemma then gives an exact sequence of $\Lambda_\mathcal{O}$-modules

$$0 \longrightarrow Z_\sigma[\sigma(\theta)] \longrightarrow R_\sigma \big/ R_\sigma\sigma(\theta) \longrightarrow M_{n(\sigma)}(\Lambda_\mathcal{O}) \big/ M_{n(\sigma)}(\Lambda_\mathcal{O})\sigma(\theta) \longrightarrow Z_\sigma \big/ Z_\sigma\sigma(\theta) \longrightarrow 0$$

from which one easily deduces that the $\Lambda_\mathcal{O}$-modules $M_{n(\sigma)}(\Lambda_\mathcal{O}) \big/ M_{n(\sigma)}(\Lambda_\mathcal{O})\sigma(\theta)$ and $X_\sigma$ have the same characteristic ideals. However, $M_{n(\sigma)}(\Lambda_\mathcal{O})$ is a direct sum of $n(\sigma)$ right ideals, each isomorphic to $\Lambda_\mathcal{O}^{n(\sigma)}$ as right $M_{n(\sigma)}(\Lambda_\mathcal{O})$-modules. If $A \in M_{n(\sigma)}(\Lambda_\mathcal{O})$ and has rank $n(\sigma)$, then the cokernel of right multiplication by the matrix $A$ on $\Lambda_\mathcal{O}^{n(\sigma)}$ is a torsion $\Lambda_\mathcal{O}$-module and the characteristic ideal of that module is generated by $det(A)$. These remarks imply that the characteristic ideal of $X_\sigma$ is generated by $\mathcal{L}_{\theta,\sigma}^{n(\sigma)}$.

The $\mathcal{O}$-rank of $X_\sigma$ is equal to $n(\sigma)\lambda(X,\sigma)$ by definition. On the other hand, that $\mathcal{O}$-rank is also equal to $n(\sigma)\lambda(\theta,\sigma)$. The first equality in (1.6.c) follows. Note also that the $\mathcal{O}$-corank of $S_\sigma$ is equal to $\lambda(X,\sigma)$.

Let $\widetilde{X} = X/pX \cong \widetilde{\Lambda}_G \big/ \widetilde{\Lambda}_G\widetilde{\theta}$. If $\tau \in \mathrm{Irr}_\mathfrak{f}(\Delta)$, then $\tau$ is absolutely irreducible and hence the $\mathfrak{f}$-algebra homomorphism $\mathfrak{f}[\Delta] \to M_{n(\tau)}(\mathfrak{f})$ is surjective. This extends to a continuous $\mathfrak{f}[[\Gamma]]$-algebra homomorphism

$$\tau : \; \mathfrak{f}[[\Gamma]][\Delta] \;\longrightarrow\; M_{n(\tau)}(\mathfrak{f}[[\Gamma]])$$

which is also surjective. Let $I_\tau$ denote its kernel. Define $\widetilde{X}_\mathfrak{f} = \widetilde{X} \otimes_{\mathbf{F}_p} \mathfrak{f}$. Then we have an isomorphism

$$\widetilde{X}_\tau = \widetilde{X}_\mathfrak{f} \big/ I_\tau \widetilde{X}_\mathfrak{f} \;\cong\; M_{n(\tau)}(\mathfrak{f}[[\Gamma]]) \big/ M_{n(\tau)}(\mathfrak{f}[[\Gamma]])\tau(\widetilde{\theta})$$

of $\mathfrak{f}[[\Gamma]]$-modules. This quotient is a torsion $\mathfrak{f}[[\Gamma]]$-module, and hence finite, if and only if $\mathcal{L}_{\widetilde{\theta},\tau} = det\big(\tau(\widetilde{\theta})\big) \neq 0$.

In fact, $\mu(X) = 0$ (i.e., $\widetilde{X}$ is finite) if and only if $\mathcal{L}_{\widetilde{\theta},\tau} \neq 0$ for all $\tau \in \mathrm{Irr}_\mathfrak{f}(\Delta)$. One direction is clear. For the other direction, the nonvanishing of all the $\mathcal{L}_{\widetilde{\theta},\tau}$'s implies that $\widetilde{X}_\tau$ is finite for all $\tau$. It is not difficult to deduce that $\widetilde{X}$ is finite and hence that indeed $\mu(X) = 0$. The argument is in the proof of proposition 4.1.6. The part about an $\mathfrak{f}$-representation space Ш for $\Delta$ is applicable here. Now $\Lambda_G$ is a free $\Lambda$-module of rank $|\Delta|$, and therefore so is $\Lambda_G\theta$. It follows that the corresponding quotient module $X$ has no nonzero, finite $\Lambda$-submodules.

Assuming that $\mu(X) = 0$, it follows that $X$ must be torsion-free and therefore free as a $\mathbf{Z}_p$-module. Furthermore, by propositions 2.1.1 and 2.4.1 (to be proved below), it follows that $X$ is a projective $\mathbf{Z}_p[\Delta]$-module.

We want to now justify the second equality in (1.6.c). Since $X$ is projective as a $\mathbf{Z}_p[\Delta]$-module, the weight $w(X,\tau)$ can be defined as the multiplicity of $\tau$ in the maximal semisimple quotient of $\widetilde{X}_\mathfrak{f}$, viewed as an $\mathfrak{f}$-representation space for $\Delta$. The $\tau$-component of that representation space is the maximal quotient annihilated by $I_\tau$, which is $\widetilde{X}_\tau$ and is isomorphic to $M_{n(\tau)}(\mathfrak{f}[[\Gamma]])\big/M_{n(\tau)}(\mathfrak{f}[[\Gamma]])\tau(\widetilde{\theta})$ as a left $M_{n(\tau)}(\mathfrak{f})$-module. Now $M_{n(\tau)}(\mathfrak{f}[[\Gamma]])$ is isomorphic to a direct sum of $n(\tau)$ right ideals, all isomorphic to $\mathfrak{f}[[\Gamma]]^{n(\tau)}$ as right $M_{n(\tau)}(\mathfrak{f}[[\Gamma]])$-modules. If $A \in M_{n(\tau)}(\mathfrak{f}[[\Gamma]])$ and has rank $n(\tau)$, then the cokernel of right multiplication by the matrix $A$ on $\mathfrak{f}[[\Gamma]]^{n(\tau)}$ is a torsion $\mathfrak{f}[[\Gamma]]$-module and hence is finite. Its characteristic ideal is generated by $det(A)$, and that determines its $\mathfrak{f}$-dimension. Taking $A = \tau(\widetilde{\theta})$, that cokernel has $\mathfrak{f}$-dimension $w(\widetilde{\theta},\tau)$. These remarks imply that the $\mathfrak{f}$-dimension of $\widetilde{X}_\tau$ is $n(\tau)w(\widetilde{\theta},\tau)$. Thus, the multiplicity of $\tau$ in $\widetilde{X}_\tau$ is $w(\widetilde{\theta},\tau)$, which therefore indeed is equal to $w(X,\tau)$.

## 2.4 Projective dimension.

A module $X$ of the form considered in the previous section obviously has a free resolution of length 1 because $X$ is isomorphic to the cokernel of the map $\Lambda_G \to \Lambda_G$ defined by multiplication by $\theta$ on the right. Regarding $\Lambda_G$ as a left $\Lambda_G$-module, it is free and the above map is a $\Lambda_G$-module homomorphism. The results in this section give such a free resolution under certain assumptions. We will consider a somewhat more general situation. We still assume that $\Gamma \cong \mathbf{Z}_p$ and that $\Delta$ is finite, but we just suppose that $G$ is an extension of $\Gamma$ by $\Delta$. That is, we have an exact sequence

$$1 \longrightarrow \Delta \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$$

and so $\Delta$ is a normal subgroup of $G$. This group extension is easily seen to be split. Hence $G \cong \Delta \rtimes \Gamma$, where the semidirect product corresponds to a certain unspecified homomorphism $\Gamma \to \mathrm{Aut}(\Delta)$. Thus, we can regard $\Gamma$ as a subgroup of $G$ and any $\Lambda_G$-module can also be regarded as a $\Lambda$-module.

The following result gives a direct relationship between the cohomological triviality (with respect to $\Delta$) of a $\Lambda_G$-module (or its dual) and the projective dimension of the module (as a $\Lambda_G$-module), specifically whether or not that projective dimension is 1. A rather different proof of such a relationship (at least in the case where $G$ is abelian) can be found in a paper by Greither. It is part of the proof of proposition 2.4 in [Gre].

**Proposition 2.4.1.** *Suppose that $X$ is a finitely-generated $\Lambda_G$-module. Assume that $X$ is a torsion $\Lambda$-module and that $X$ has no nonzero, finite $\Lambda$-submodules. Let $S$ denote the Pontryagin dual of $X$. Then $X$ has a free resolution of length 1 as a $\Lambda_G$-module if and only if $H^i(\Delta', S) = 0$ for every subgroup $\Delta'$ of $\Delta$ and for all $i \geq 1$.*

*Proof.* We start with some general remarks about cofree, cofinitely-generated $\Lambda_G$-modules, where $G$ is any profinite group. Assume that $A$ is such a module. That means that its Pontryagin dual $\widehat{A}$ is isomorphic to $\Lambda_G^r$ for some $r \geq 0$. Note that the Pontryagin dual of $A[p]$ is isomorphic to $\widetilde{\Lambda}_G^r$, where $\widetilde{\Lambda}_G \cong \Lambda_G/p\Lambda_G$, the completed group algebra for $G$ over $\mathbf{F}_p$. It follows that for every closed subgroup $G'$ of $G$ and for all $i \geq 1$, we have

$$H^i(G', A) \ = \ 0, \qquad H^i(G', A[p]) \ = \ 0 \ .$$

Furthermore, $H^0(G', A)$ is a divisible group. The vanishing statements are easily reduced to the case where $G$ is finite. In that case, it suffices to note that $\mathbf{Z}_p[G]$ and $\mathbf{F}_p[G]$ are free-modules over $\mathbf{Z}_p[G']$ and $\mathbf{F}_p[G']$, respectively. Hence their Pontryagin duals are cohomologically trivial as $G'$-modules, as is any direct sum of those modules. If $G$ is profinite and $N$ is an open, normal subgroup of $G$, then $A^N$ and $A[p]^N$ are cofree modules over the rings $\mathbf{Z}_p[G/N]$ and $\mathbf{F}_p[G/N]$, respectively. Hence the cohomology groups $H^i(G'N/N, A^N)$ and $H^i(G'N/N, A[p]^N)$ vanish for all $i \geq 1$. Since $G'$ is the inverse limit of groups of the form $G'N/N$, the above vanishing statements follow simply by taking direct limits. Now $A$ is a divisible group and so we obtain the divisibility of $H^0(G', A)$ from the fact that $H^1(G', A[p]) = 0$.

Now assume that $X$ is a finitely-generated $\Lambda_G$-module which has a free resolution of length 1. This means that there is an exact sequence

$$0 \longrightarrow S \longrightarrow S_1 \longrightarrow S_2 \longrightarrow 0 \tag{2.4.a}$$

of cofinitely-generated, discrete $\Lambda_G$-modules where $S_1$ and $S_2$ are cofree $\Lambda_G$-modules. If $G'$ is any closed subgroup of $G$, then it follows that $H^i(G', S) = 0$ for all $i \geq 2$. Also, since $H^0(G', S_2)$ is a divisible group, it follows that the same is true for $H^1(G', S)$. In particular, if $G'$ is a finite subgroup of $G$, then $H^1(G', S)$ must have finite exponent and therefore we have $H^1(G', S) = 0$. The "only if" part of the proposition follows from these remarks.

For the converse, we assume $G = \Delta \rtimes \Gamma$. We think of $\Gamma$ as a subgroup of $G$ as well as a quotient group. For some $k \geq 0$, the action of $\Gamma_k$ on $\Delta$ is trivial. Thus, $\Gamma_k$ is a subgroup of the center of $G$. It is an open, normal subgroup of $G$. We assume the vanishing of the cohomology groups $H^i(\Delta', S) = 0$ for all $\Delta'$ and $i$, as stated. Suppose that $X$ can be generated by $m$ elements as a $\Lambda_G$-module. Then $S$ fits into an exact sequence (2.4.a), where

$S_1$ is the Pontryagin dual of $\Lambda_G^m$. We will prove the same statement about the Pontryagin dual of $S_2$, which we denote by $Y$. We regard $Y$ as a $\Lambda_G$-submodule of $\Lambda_G^m$. Thus we have

$$X \;\cong\; \Lambda_G^m/Y$$

as $\Lambda_G$-modules. Since $\Lambda_G$ is a free $\Lambda$-module and $X$ has no nonzero, finite $\Lambda$-submodules,it follows that $Y$ is a reflexive $\Lambda$-module. Hence $Y$ is free and $S_2$ is cofree as $\Lambda$-modules. It follows that $H^i(\Gamma_k, S_2) = 0$ for all $i \geq 1$ and that $H^0(\Gamma_k, S_2)$ is a divisible group.

Suppose that $G'$ is a closed subgroup of $G$ such that $\Gamma_k \subseteq G'$. Let $\Delta' = G' \cap \Delta$, a normal subgroup of $G'$, and let $\Gamma' = G'/\Delta'$, which is isomorphic to a subgroup of $\Gamma$. Since $H^i(\Delta', S) = 0$ for all $i \geq 1$, the inflation map

$$H^i(\Gamma', S^{\Delta'}) \;\longrightarrow\; H^i(G', S)$$

is an isomorphism for all $i \geq 1$ and hence $H^i(G', S) = 0$ for all $i \geq 2$. It follows that $H^i(G', S_2) = 0$ for all $i \geq 1$. In particular, $H^i(\Gamma_k, S_2) = 0$ and consequently the inflation map

$$H^i(G'/\Gamma_k, S_2^{\Gamma_k}) \;\longrightarrow\; H^i(G', S_2)$$

is an isomorphism for all $i \geq 1$. Now $S_2^{\Gamma_k}$ is cofree as a $\mathbf{Z}_p$-module and we have

$$\mathrm{corank}_{\mathbf{Z}_p}\big(S_2^{\Gamma_k}\big)\big) \;=\; p^k \mathrm{corank}_{\Lambda}\big(S_2\big) \;=\; p^k \mathrm{rank}_{\Lambda}(Y) \;=\; m|\Delta|p^k \quad .$$

We can apply proposition 2.1.1 to conclude that the Pontryagin dual $Y_{\Gamma_k}$ of $S_2^{\Gamma_k}$ is a projective module for the group ring $\mathbf{Z}_p[G/\Gamma_k]$. Note that $G/\Gamma_k$ has order $|\Delta|p^k$.

We now show that $Y_{\Gamma_k}$ is a free $\mathbf{Z}_p[G/\Gamma_k]$-module. Since it is a projective, it is sufficient to show that $Y_{\Gamma_k} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a free $\mathbf{Q}_p[G/\Gamma_k]$-module. We have an exact sequence

$$0 \;\longrightarrow S^{\Gamma_k} \;\longrightarrow\; S_1^{\Gamma_k} \;\longrightarrow\; S_2^{\Gamma_k} \;\longrightarrow\; H^1(\Gamma_k, S) \;\longrightarrow 0 \quad .$$

The maps are equivariant for the action of $G/\Gamma_k$. Let $\gamma_k$ be a topological generator for $\Gamma_k$ (which is isomorphic to $\mathbf{Z}_p$). Then we have $H^1(\Gamma_k, S) \cong S\big/(\gamma_k - 1)S$. The Pontryagin duals of $S^{\Gamma_k}$ and $S\big/(\gamma_k - 1)S$ are $X\big/(\gamma_k - 1)X$ and $X^{\Gamma_k}$, respectively. Tensoring those $\mathbf{Z}_p$-modules with $\mathbf{Q}_p$ gives $V\big/(\gamma_k - 1)V$ and $V^{\Gamma_k}$, respectively, where $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, a finite-dimensional $\mathbf{Q}_p$-representation space for $G$.

Since $\gamma_k$ is in the center of $G$, the map $v \to (\gamma_k - 1)v$ is a $G$-homomorphisms from $V$ to itself. Consequently, the kernel and cokernel of that map have the same composition factors. This implies that $V^{\Gamma_k}$ and $V\big/(\gamma_k - 1)V$ are isomorphic as $\mathbf{Q}_p$-representation spaces for $G/\Gamma_k$. Therefore, it follows that the $\mathbf{Q}_p$-representations spaces $Y_{\Gamma_k} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $\big(\widehat{S}_1\big)_{\Gamma_k} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for

$G/\Gamma_k$ are isomorphic. But the latter representation space is isomorphic to $\mathbf{Q}_p[G/\Gamma_k]^m$. Therefore, $Y_{\Gamma_k} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a direct sum of $m$ copies of the regular representation for $G/\Gamma_k$.

The above observations imply that $Y_{\Gamma_k} \cong \mathbf{Z}_p[G/\Gamma_k]^m$ as a $\mathbf{Z}_p[G/\Gamma_k]$-module. Therefore, $Y_{\Gamma_k}$ can be generated by $m$ elements as a $\mathbf{Z}_p[G/\Gamma_k]$-module. One can then apply Nakayama's lemma (for $\Lambda$-modules) to conclude that $Y$ can be generated by $m$ elements as a $\Lambda_G$-module. Thus, $Y$ is a quotient of a free $\Lambda_G$-module of rank $m$. Now $X$ is a torsion $\Lambda$-module and so $Y$ and $\Lambda_G^m$ have the same $\Lambda$-rank. Consequently, it is clear that we actually have $Y \cong \Lambda_G^m$. Therefore, $X$ indeed has a free resolution of length 1 as a $\Lambda_G$-module. $\square$

**Remark 2.4.2.** The following well-known properties of $\Lambda$-modules can be found in [NSW], propositions 5.3.20 and 5.5.3: *(a) If $X$ is a finitely-generated $\Lambda$-module, then $X$ has projective dimension at most 2*, and *(b) If $X$ has no nonzero, finite $\Lambda$-submodules, then its projective dimension is at most 1.* In *(b)*, $X$ will have a free resolution of length 1 as a $\Lambda$-module since any finitely-generated projective $\Lambda$-module must be free. This result is the special case of proposition 2.4.1 where $\Delta$ is trivial. The essential ingredient in the proof is the fact that any reflexive $\Lambda$-module must be free, which we also used in a crucial way in the above argument. $\lozenge$

The following corollary follows immediately from proposition 2.4.1. Note that $m = 1$ if $X$ is a cyclic $\Lambda_G$-module.

**Corollary 2.4.3.** *Suppose that $X$ is a $\Lambda_G$-module which is finitely-generated and projective as a $\mathbf{Z}_p[\Delta]$-module. Then $X$ has a free resolution of length 1 as a $\Lambda_G$-module. In particular, if $X$ is a cyclic $\Lambda_G$-module, then $X \cong \Lambda_G/\Lambda_G\theta$ for some nonzero element $\theta \in \Lambda_G$.*

**Remark 2.4.4.** Suppose that $\tau$ is an irreducible representation of $\Delta$ over $\mathbf{F}_p$. For this remark, we don't want to assume $\tau$ is absolutely irreducible. It is still true that there is an indecomposable, projective $\mathbf{Z}_p[\Delta]$-module $P_\tau$ that has $U_\tau$, the underlying $\mathbf{F}_p$-representation space for $\tau$, as its unique simple quotient. Furthermore, $P_\tau$ is a direct summand in $\mathbf{Z}_p[\Delta]$ (as a module) and hence is a cyclic $\mathbf{Z}_p[\Delta]$-module. All of this follows from proposition 41 in [Se77]. Let $G = \Delta \times \Gamma$. We let $G$ act on $P_\tau$ by letting $\Gamma$ act trivially. Then $P_\tau$ becomes a cyclic $\Lambda_G$-module. Corollary 2.4.3 implies that $P_\tau \cong \Lambda_G/\Lambda_G\theta_\tau$, where $\theta_\tau$ is in $\Lambda_G$. By section 2.3, we have $\mu(\theta_\tau, \sigma) = 0$ and $\lambda(\theta_\tau, \sigma) = \lambda(P_\tau, \sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ (where $\mathcal{F}$ is sufficiently large as usual). Now if $X$ is any finitely-generated $\Lambda_G$-module which is torsion as a $\Lambda$-module and projective as a $\mathbf{Z}_p[\Delta]$-module, we can forget the action of $\Gamma$ and express $X$ as a direct sum of the $P_\tau$'s with certain multiplicities. Let $\theta \in \Lambda_G$ be the corresponding product of the $\theta_\tau$'s. Then, by definition, we have $\mu(\theta, \sigma) = 0$ and $\lambda(\theta, \sigma) = \lambda(X, \sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$.

We would like to find such a $\theta \in \Lambda_G$ which reflects the action of $G$ on $X$ more fully, not just the action of $\Delta$. An illustration of what we mean by this is contained in remark 3.1.3, which only concerns the case where $G$ is commutative. We have not succeeded in finding a way to do this when $G$ is non-commutative. $\Diamond$

# 3 Projectivity or quasi-projectivity of $X_E^{\Sigma_0}(K_\infty)$.

We take $F, K, F_\infty, K_\infty, \Sigma_0$, and $E$ exactly as in the introduction. Let $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$. In this chapter we will apply propositions 2.1.1 and 2.1.3 to the $\mathbf{Z}_p[\Delta]$-module $X_E^{\Sigma_0}(K_\infty)$. This requires verifying the appropriate hypotheses for $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. We will study the relevant cohomology groups by using the exact sequence defining the non-primitive Selmer group. Each of the verifications requires a certain subset of the assumptions we need for the main results, which are propositions 3.1.1 and 3.2.1. The arguments apply with only minor modifications in the formulations to a more general situation. It suffices to assume that $K_\infty$ is a Galois extension of $F$ containing the cyclotomic $\mathbf{Z}_p$-extension $F_\infty$ of $F$ and that $[K_\infty : F_\infty]$ is finite. Section 3.5 is devoted to a discussion of this generalization. .

## 3.1 The proof of theorem 1.

The proof is in a series of steps culminating in proposition 3.1.1, which is theorem 1.

**A.** *Surjectivity of the global-to-local maps.* We need only assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion. This is conjectured to always be true. Since we are including $p = 2$, we first describe $\mathcal{H}_v(K_\infty, E)$ when $v$ is an archimedean prime of $F$. There will then be infinitely many primes of $K_\infty$ lying over $v$. If $\eta$ is such a prime, then $\mathrm{im}(\kappa_\eta) = 0$. The local factor $\mathcal{H}_\infty(K_\infty, E)$ is trivial when $p$ is odd, but can be nontrivial when $p = 2$. It is defined by

$$\mathcal{H}_v(K_\infty, E) = \varinjlim_{F'} \Big( \bigoplus_{v'|v} H^1(F'_{v'}, E[p^\infty]) \Big)$$

where $F'$ varies over all finite extensions of $F$ contained in $K_\infty$, partially ordered by inclusion, and $v'$ runs over the primes of $F'$ lying over $v$. We can restrict to $F'$'s containing $K$ (i.e., the layers in the $\mathbf{Z}_p$-extension $K_\infty/K$), and then the completions $F'_{v'}$ are either all isomorphic to $\mathbf{R}$ or to $\mathbf{C}$, depending on $K$ and $v$. The group $\mathcal{H}_v(K_\infty, E)$ is nontrivial only when $F_v = \mathbf{R}$, $v$ splits completely in $K/F$, and $H^1(F_v, E[p^\infty]) \neq 0$, which occurs only when $p = 2$ and $E(F_v)$ has two connected components. In that case, $H^1(F_v, E[p^\infty])$ is of order 2 and $\mathcal{H}_v(K_\infty, E)$

is infinite, but of exponent 2. Its Pontryagin dual is a $\Lambda$-module with $\mu$-invariant equal to $[K : F]$.

We will first recall why the map $\gamma_{K_\infty}$ is surjective, as stated in the introduction. Let $\Sigma$ be a set of primes of $F$ containing all the primes where $E$ has bad reduction, or where $K/F$ is ramified, or which divide $p$ or $\infty$. Consider the map

$$H^1(F_\Sigma/K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{v\in\Sigma} \mathcal{H}_v(K_\infty, E) \tag{3.1.a}$$

where $F_\Sigma$ is the maximal extension of $F$ unramified outside $\Sigma$. Note that $K_\infty \subset F_\Sigma$. It is easy to see that $\mathrm{Sel}_E(K_\infty)_p$ is the kernel of (3.1.a), just assuming that $\Sigma$ is chosen as stated. Now, according to lemma 4.6 of [Gr99], if $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, then the map (3.1.a) is surjective. By letting $\Sigma$ vary, the surjectivity of $\gamma_{K_\infty}$ follows. One immediate consequence is that for any set $\Sigma_0$ of primes of $F$, the global-to-local map

$$\gamma_{K_\infty}^{\Sigma_0} : \ H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{v\notin\Sigma_0} \mathcal{H}_v(K_\infty, E)$$

is also surjective. By definition, $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \ker(\gamma_{K_\infty}^{\Sigma_0})$.

**B.** *Divisibility of Selmer groups.* The assumptions that we need are that $\mathrm{Sel}_E(K_\infty)[p]$ is finite and that $E(K)[p] = 0$. To apply the criteria of section 2.1, we need to show that $X_E^{\Sigma_0}(K_\infty)$ is a free $\mathbf{Z}_p$-module of finite rank or, equivalently, that $\mathrm{Sel}_E(K_\infty)_p$ is divisible and of finite $\mathbf{Z}_p$-corank. The assumption that $\mathrm{Sel}_E(K_\infty)[p]$ is finite implies that $X_E(K_\infty)$ is a finitely generated, torsion $\Lambda$-module and that its $\mu$-invariant is zero. It follows that $X_E(K_\infty)$ is a finitely generated $\mathbf{Z}_p$-module. We can now use proposition 4.14 from [Gr99] which requires the additional assumption that $E(K)[p] = 0$. It then follows that $X_E(K_\infty)$ has no nonzero finite $\Lambda$-submodules. Hence the $\mathbf{Z}_p$-torsion submodule must be zero. This implies that $X_E(K_\infty)$ is $\mathbf{Z}_p$-free of finite rank, as needed. Equivalently, $\mathrm{Sel}_E(K_\infty)_p$ is divisible and of finite $\mathbf{Z}_p$-corank.

Now for any non-archimedean prime $v \nmid p$, and a prime $\eta$ of $K_\infty$ lying over $v$, the local cohomology groups $H^1(K_{\infty,\eta}, E[p^\infty])$ is also divisible and of finite $\mathbf{Z}_p$-corank. The divisibility follows from the fact that $K_{\infty,\eta}$ has $p$-cohomological dimension 2, and so $H^2(K_{\infty,\eta}, E[p]) = 0$. The fact that $H^1(K_{\infty,\eta}, E[p^\infty])$ has finite $\mathbf{Z}_p$-corank follows from proposition 2 of [Gr89]. Therefore, for $v \nmid p$, $\mathcal{H}_v(K_\infty, E)$ is divisible and of finite $\mathbf{Z}_p$-corank. The surjectivity of $\gamma_{K_\infty}$ now implies that $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is indeed divisible and of finite $\mathbf{Z}_p$-corank.

**C.** *Basic cohomology sequences.* Continuing to assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, the global-to-local map $\gamma_{K_\infty}^{\Sigma_0}$ is surjective and gives the following exact sequence:

$$0 \longrightarrow \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \longrightarrow H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{v\notin\Sigma_0} \mathcal{H}_v(K_\infty, E) \longrightarrow 0 \tag{3.1.b}$$

We have already explained the surjectivity of the global-to-local map $\gamma_{K_\infty}^{\Sigma_0}$. The maps in the sequence (3.1.b) are $\Delta$-equivariant and so we obtain the following exact sequences of cohomology groups.

$$H^1(K_\infty, E[p^\infty])^\Delta \xrightarrow{\delta} \bigoplus_{v\notin\Sigma_0} \mathcal{H}_v(K_\infty, E)^\Delta \longrightarrow H^1\big(\Delta, \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big) \longrightarrow H^1\big(\Delta, H^1(K_\infty, E[p^\infty])\big)$$

and

$$\bigoplus_{v\notin\Sigma_0} H^1\big(\Delta, \mathcal{H}_v(K_\infty, E)\big) \longrightarrow H^2\big(\Delta, \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big) \longrightarrow H^2\big(\Delta, H^1(K_\infty, E[p^\infty])\big)$$

Theorem 1 will be proved by studying each of the terms in these sequences. To prove that $H^1\big(\Delta, \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big) = 0$, it suffices to show that $H^1\big(\Delta, H^1(K_\infty, E[p^\infty])\big) = 0$ and that the map labeled $\delta$ in the first sequence is surjective. To prove that $H^2\big(\Delta, \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big) = 0$, it suffices to show that $H^2\big(\Delta, H^1(K_\infty, E[p^\infty])\big) = 0$ and that $H^1\big(\Delta, \mathcal{H}_v(K_\infty, E)\big) = 0$ for all $v \notin \Phi_{K/F}$. For each of these statements, some subset of the assumptions in theorem 1 will be needed.

**D.** *Surjectivity of $\delta$.* We will need to assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, that $\Phi_{K/F}$ is a subset of $\Sigma_0$, and that either $p$ is non-anomalous for $E/K$ or that none of the $e_v(K/F)$'s for $v \in \Sigma_p$ is divisible by $p$. The kernel of the restriction map $H^1(F_\infty, E[p^\infty]) \to H^1(K_\infty, E[p^\infty])$ is isomorphic to $H^1\big(\Delta, E(K_\infty)[p^\infty]\big)$, which is easily seen to be finite. Thus, the kernel of the map $\mathrm{Sel}_E(F_\infty)_p \to \mathrm{Sel}_E(K_\infty)_p$ must be finite. Since we assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, it follows that the same is true for $\mathrm{Sel}_E(F_\infty)_p$. Therefore, the map $\gamma_{F_\infty}$ is surjective and so is the global-to-local map defining $\mathrm{Sel}_E^{\Sigma_0}(F_\infty)_p$. This shows the exactness of the first row in the following commutative diagram.

$$\begin{array}{ccccc} H^1(F_\infty, E[p^\infty]) & \longrightarrow & \bigoplus_{v\notin\Sigma_o} \mathcal{H}_v(F_\infty, E) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ H^1(K_\infty, E[p^\infty])^\Delta & \xrightarrow{\delta} & \bigoplus_{v\notin\Sigma_o} \mathcal{H}_v(K_\infty, E)^\Delta & & \end{array}$$

where the vertical maps are the obvious restriction maps. To prove the surjectivity of the map in the second row, it suffices to show the surjectivity of the second vertical map, or, equivalently, that the map $\beta_v : \mathcal{H}_v(F_\infty, E) \longrightarrow \mathcal{H}_v(K_\infty, E)^\Delta$ is surjective for each $v \notin \Sigma_o$.

For any prime $\eta$ of $K_\infty$ lying above $v$, let $\Delta_\eta$ denote the corresponding decomposition subgroup of $\Delta$. Thus, $\Delta_\eta \cong \mathrm{Gal}(K_{\infty,\eta}/F_{\infty,\nu})$, where $\nu$ is the prime of $F_\infty$ lying below $\eta$. Of course, $\Delta$ permutes the primes of $K_\infty$ above $v$. We can take one $\eta$ in each orbit. If $v|\infty$,

the surjectivity of $\beta_v$ is clear because either $K_{\infty,\eta} \cong \mathbf{C}$, in which case $\mathcal{H}_v(K_\infty, E) = 0$, or $K_{\infty,\eta} \cong \mathbf{R}$, in which case each $\Delta_\eta$ is trivial and the map $\beta_v$ is an isomorphism. Now assume that $v \nmid p, \infty$. For such $v$ and any $\eta|v$, it suffices to prove that the map

$$H^1(F_{\infty,\nu}, E[p^\infty]) \longrightarrow H^1(K_{\infty,\eta}, E[p^\infty])^{\Delta_\eta}$$

is surjective. The cokernel of this map is isomorphic to $H^2\big(\Delta_\eta, H^0(K_{\infty,\eta}, E[p^\infty])\big)$. But this cohomology group vanishes if we assume that $v \notin \Sigma_0$. To see that, note that $F_{\infty,\nu}$ is the unramified $\mathbf{Z}_p$-extension of $F_v$, since $v \nmid p$, and hence any unramified extension of $F_{\infty,\nu}$ has degree prime to $p$. Now $e_v(K/F)$ is the order of the inertia subgroup of $\Delta_\eta$, which is assumed to be prime to $p$, and so the same is true for $|\Delta_\eta|$ itself. The vanishing follows from that fact.

Suppose now that $v|p$. Then we must prove the surjectivity of the map

$$H^1(F_{\infty,\nu}, \overline{E}_v[p^\infty]) \longrightarrow H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{\Delta_\eta} \quad .$$

The cokernel of this map is isomorphic to $H^2\big(\Delta_\eta, H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])\big) = H^2\big(\Delta_\eta, \overline{E}_v(k_\eta)[p^\infty]\big)$. This cohomology group obviously vanishes if $\overline{E}_v(k_\eta)[p] = 0$ or, equivalently, as we pointed out in the introduction, if $v$ is non-anomalous for $E/K$. Under that assumption, it follows that $\beta_v$ is surjective.

The map $\beta_v$ will also be surjective if we assume that $p \nmid e_v(K/F)$. To see this, let $\Upsilon_\eta$ denote the inertia subgroup of $\Delta_\eta$, whose order will also be prime to $p$. It will be that slightly weaker assumption that we actually need. It follows that $H^i(\Upsilon_\eta, \overline{E}_v(k_\eta)[p^\infty]) = 0$ for $i = 1, 2$. We therefore have exact sequences

$$0 \longrightarrow H^i(\Delta_\eta/\Upsilon_\eta, \overline{E}_v(k_\eta)[p^\infty]) \longrightarrow H^i(\Delta_\eta, \overline{E}_v(k_\eta)[p^\infty]) \longrightarrow 0 \tag{3.1.c}$$

Thus, taking $i = 2$, the vanishing of $H^2(\Delta_\eta, \overline{E}_v(k_\eta)[p^\infty])$, and therefore the surjectivity of $\beta_v$, follows from the fact that $H^2\big(k_\eta/f_\nu, \overline{E}_v(k_\eta)\big) = 0$ for any finite extension of finite fields $k_\eta/f_\nu$. Here we take $f_\nu$ to be the residue field for $\nu$.

**E.** *The Hochschild-Serre spectral sequence.* We will use a special case. Assume that $G$ is a profinite group, $N$ is a closed, normal subgroup of finite index, and let $\Delta = G/N$. Suppose that $A$ is a discrete, $p$-primary $G$-module. Let us assume that $H^i(N, A) = 0$ for $i \geq 2$. The Hochschild-Serre spectral sequence then simplifies considerably. See exercise 5 in [NSW], page 96, which is based on theorem 2.1.5. The simplification occurs because only the bottom two rows of objects in the spectral sequence can be nonzero. What we will need are the following exact sequences for $j \geq 1$. Mainly, we will need this for $j = 2$ and $j = 3$. The last map for each $j$ is the inflation map.

$$H^j(G, A) \longrightarrow H^{j-1}\big(\Delta, H^1(N, A)\big) \longrightarrow H^{j+1}(\Delta, A^N) \longrightarrow H^{j+1}(G, A) \tag{3.1.d}$$

As a consequence, if $H^i(G,A)=0$ for $i\geq 2$, then we obtain isomorphisms:

$$H^{j-1}\big(\Delta, H^1(N,A)\big)\cong H^{j+1}(\Delta, A^N) \tag{3.1.e}$$

for $j\geq 2$. We will apply this to cases where $G$ and $N$ are global or local Galois groups which have $p$-cohomological dimension 2. Thus, at least for $i\geq 3$, the vanishing of both $H^i(N,A)$ and $H^i(G,A)$ will be assured.

**F.** *Vanishing of $H^i\big(\Delta, H^1(K_\infty, E[p^\infty])\big)$ for $i\geq 1$.* We assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion and that $E(K)[p]=0$. For $p=2$, we will need the additional assumption that $E(F_v)$ is connected for all $v|\infty$. We will use the Hochschild-Serre spectral sequence, taking $G=G_{F_\infty}$, $N=G_{K_\infty}$, and $A=E[p^\infty]$. We first assume that $p$ is odd. It is then known that $H^i(F_\infty, E[p^\infty])$ and $H^i(K_\infty, E[p^\infty])$ both vanish for $i\geq 3$. This follows from the fact that the $p$-cohomological dimension for the Galois groups $G_{F_\infty}$ and $G_{K_\infty}$ is equal to 2 when $p$ is odd.

That vanishing statement is also known for $i=2$ under the assumption that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion. That result is contained in [Gr99], although it is unfortunately not explicitly stated. One first deduces that $H^1(K_\infty, E[p^\infty])$ has $\Lambda$-corank equal to $[K:\mathbf{Q}]$. That assertion and its justification can be found on pages 94-95 in [Gr99]. The vanishing of $H^2(K_\infty, E[p^\infty])$ for an odd prime $p$ then follows from proposition 4.12 in that paper. Since $\mathrm{Sel}_E(F_\infty)_p$ will also be $\Lambda$-cotorsion, the vanishing of $H^2(F_\infty, E[p^\infty])$ also follows.

The assumptions needed for (3.1.e) are therefore satisfied when $p$ is odd. Hence we obtain isomorphisms

$$H^{j-1}\big(\Delta, H^1(K_\infty, E[p^\infty])\big)\cong H^{j+1}\big(\Delta, H^0(K_\infty, E[p^\infty])\big), \tag{3.1.f}$$

for $j\geq 2$. The assumption that $E(K)[p]=0$ implies that $H^0(K_\infty, E[p^\infty])=0$ since $\mathrm{Gal}(K_\infty/K)$ is pro-$p$. The stated vanishing of $H^i\big(\Delta, H^1(K_\infty, E[p^\infty])\big)$ then follows by taking $j=i+1$.

We now assume that $p=2$, that $v$ is an archimedean prime of $F$, and that $E(F_v)$ is connected. That assumption is obviously satisfied for any complex prime $v$, but may fail if $v$ is real. An equivalent statement is that $H^i(F_v, E[2^\infty])=0$ for all $i\geq 1$. If $w|v$, then $E(K_w)$ will also be connected and so we have the corresponding vanishing for $K_w$ too. By theorem 8.6.13 in [NSW], we have isomorphisms

$$H^i(F_\infty, E[2^\infty])\cong \bigoplus_{v|\infty}\mathcal{H}^i_v(F_\infty, E), \qquad H^i(K_\infty, E[2^\infty])\cong \bigoplus_{v|\infty}\mathcal{H}^i_v(K_\infty, E) \tag{3.1.g}$$

for $i\geq 3$. Here the $\mathcal{H}^i_v$'s for $v|\infty$ are defined just as in part **A**, except that $H^1$ is replaced by $H^i$. These isomorphisms are proved in [NSW] for finite extensions and for finite Galois modules, but they can be extended easily to the above situation by taking direct limits.

The arguments and results in [Gr99] cited above imply that $H^2(K_\infty, E[2^\infty])$ is $\Lambda$-cotorsion, and more precisely that it is a cofree module over $\Lambda/2\Lambda$. This again requires the assumption that $\mathrm{Sel}_E(K_\infty)_2$ is $\Lambda$-cotorsion. The proof of proposition 4.12 in that paper shows that, under that same assumption, the isomorphisms (3.1.g) hold even for $i = 2$. The connectedness assumption implies that $\mathcal{H}^i_v(F_\infty, E)$ and $\mathcal{H}^i_v(K_\infty, E)$ both vanish for all $v|\infty$. Therefore, it follows that $H^i(F_\infty, E[p^\infty])$ and $H^i(K_\infty, E[p^\infty])$ must also vanish when $i \geq 2$. Hence the Hochschild-Serre sequence again gives us the identifications (3.1.f). The vanishing of $H^i\big(\Delta, H^1(K_\infty, E[2^\infty])\big)$ follows as before.

**G.** *Vanishing of* $H^i\big(\Delta, \mathcal{H}_v(K_\infty, E)\big)$ *for* $v \notin \Phi_{K/F} \bigcup \Sigma_p$ *and* $i \geq 1$. No extra assumptions about such $v$ are needed. First suppose that $v \nmid \infty$. We will then show that the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is actually projective as a $\mathbf{Z}_p[\Delta]$-module. The fact that $H^i\big(\Delta, \mathcal{H}_v(K_\infty, E)\big) = 0$ for any $i \geq 1$ is a consequence. Since $\mathcal{H}_v(K_\infty, E)$ is a direct product over all $\eta|v$, we can consider each $\Delta$-orbit separately. Fix one $\eta$. Let $\nu$ be the prime of $F_\infty$ lying below $\eta$. Then

$$\prod_{\eta|\nu} H^1(K_{\infty,\eta}, E[p^\infty]) \cong \mathrm{Ind}_{\Delta_\eta}^{\Delta}\big(H^1(K_{\infty,\eta}, E[p^\infty])\big) \tag{3.1.h}$$

It therefore suffices to show that the Pontryagin dual of $H^1(K_{\infty,\eta}, E[p^\infty])$ is projective as a $\mathbf{Z}_p[\Delta_\eta]$-module. Since $v \notin \Phi_{K/F}$, $|\Delta_\eta|$ is not divisible by $p$, and hence a $Z_p[\Delta_\eta]$-module is projective if it is finitely-generated and torsion-free as a $\mathbf{Z}_p$-module. Since $v \nmid p$, $H^1(K_{\infty,\eta}, E[p^\infty])$ is cofinitely generated as a $\mathbf{Z}_p$-module. (See proposition 2 in [Gr89].) It is also a divisible $\mathbf{Z}_p$-module, a consequence of the fact that $G_{K_{\infty,\eta}}$ has $p$-cohomological dimension 1. We refer the reader to the discussion following lemma 4.5 in [Gr99] for the proof of divisibility. Thus, the Pontryagin dual of $H^1(K_{\infty,\eta}, E[p^\infty])$ is indeed a finitely-generated, torsion-free $\mathbf{Z}_p$-module.

Now suppose that $v|\infty$. If the primes of $K$ above $v$ are complex, then $\mathcal{H}_v(K_\infty, E) = 0$ and so the result is obvious. On the other hand, if those primes are real, then the primes $\eta$ of $K_\infty$ lying above $v$ are also real and hence $v$ splits completely in $K_\infty/F$. Thus, $\mathcal{H}_v(K_\infty, E)$ is isomorphic to $H^1(K_{\infty,\eta}, E[p^\infty]) \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\Delta]$, and this is cohomologically trivial.

**H.** *Vanishing of* $H^i\big(\Delta, \mathcal{H}_v(K_\infty, E)\big)$ *for* $v \in \Sigma_p$ *and* $i \geq 1$. We need to assume that either $v$ is non-anomalous for $E/K$ or that $p \nmid e_v(K_\infty/F_\infty)$. Again, $\Delta$ permutes the primes of $K_\infty$ above $v$ and so one must prove that $H^1\big(\Delta_\eta, H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])\big) = 0$ for any $\eta|v$. Just as before, one can use the Hochschild-Serre spectral sequence since it is known that the $p$-cohomological dimension of both $G_{K_{\infty,\eta}}$ and $G_{F_{\infty,\nu}}$ is 1. We have

$$H^i\big(\Delta_\eta, H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])\big) \cong H^{i+2}\big(\Delta_\eta, H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])\big)$$

But $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty]) = \overline{E}_v[p^\infty]^{G_{K_{\infty,\eta}}}$. This is trivial if we assume that $\overline{E}_v(k_\eta)[p] = 0$.

On the other hand, if $v$ is anomalous for $E$ and $K$, then we can still prove the vanishing if we assume that $p \nmid e_v(K/F)$, i.e., that $v$ is tamely ramified in the extension $K/F$. To show this, suppose that $\eta$ be a prime of $K_\infty$ and $\nu$ is the prime of $F_\infty$ lying below $\eta$. Then the residue fields $k_\eta$ and $f_\nu$ are finite. It is known that $H^j(k_\eta/f_\nu, \overline{E}_v(k_\eta)) = 0$ for $j \geq 1$. Assuming that $p \nmid e_v(K/F)$, it follows from (3.1.c) that we indeed have $H^{i+2}\big(\Delta_\eta, H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])\big) = 0$ for all $i \geq 1$. In fact, it suffices to assume that $e_v(K_\infty/F_\infty)$ is not divisible by $p$.

The following proposition summarizes what the above results show. The final conclusion about projectivity then follows from proposition 2.1.1. We just apply the first conclusion to any subgroup $\Delta'$ of $\Delta$, taking $i = 1$ and $i = 2$. Theorem 1 is a consequence.

**Proposition 3.1.1.** *Assume that* $\mathrm{Sel}_E(K_\infty)_p$ *is* $\Lambda$*-cotorsion. Let us also make the following assumptions:*

*(a)* $E(K)[p] = 0$,

*(b) For each* $v|p$, *either* $v$ *is non-anomalous for* $E/K$ *or* $v$ *is tamely ramified in* $K/F$.

*(c)* $\Sigma_o$ *contains* $\Phi_{K/F}$, *but no primes above* $p$ *or* $\infty$.

*(d) If* $p = 2$, *then* $E(F_v)$ *is connected for all archimedean primes* $v$.

*Then* $H^i\big(\Delta, \mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p\big) = 0$ *for* $i \geq 1$.

*If, in addition, we assume that*

*(e)* $\mathrm{Sel}_E(K_\infty)[p]$ *is finite,*

*then* $\mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p$ *is a divisible, cofinitely generated* $\mathbf{Z}_p$*-module and* $X_E^{\Sigma_o}(K_\infty)$ *is a projective* $\mathbf{Z}_p[\Delta]$*-module.*

**Remark 3.1.2.** The assumption that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion together with assumption *(a)* is sufficient to imply that $X_E(K_\infty)$ has no nonzero, finite $\Lambda$-submodules and hence is a $\Lambda$-module of projective dimension 1. The first statement is proposition 4.14 in [Gr99]. For the second, see remark 2.4.2. The same assertions will also be true for $X_E^{\Sigma_0}(K_\infty)$. The above proposition together with proposition 2.4.1 implies that $X_E^{\Sigma_0}(K_\infty)$ actually has projective dimension 1 as a $\Lambda[\Delta]$-module if assumptions *(b)*, *(c)*, and *(d)* are also satisfied. However, without those assumptions, the proofs show that sometimes (although not always), we can have $H^i\big(\Delta', \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big) \neq 0$ for some subgroup $\Delta'$ of $\Delta$ and $i = 1$ or 2. In such a case, it is clear that $X_E^{\Sigma_0}(K_\infty)$ has infinite projective dimension as a $\Lambda[\Delta]$-module. $\Diamond$

**Remark 3.1.3.** Assume that $K_\infty/F$ is an abelian extension. Thus $G = \mathrm{Gal}(K_\infty/F)$ is isomorphic to $\Delta \times \Gamma$, where $\Delta$ is a finite, abelian group. Corollary 2.4.3 has an interesting

consequence in that case. Let us make the assumptions in proposition 3.1.1. It follows that $X = X_E^{\Sigma_0}(K_\infty)$ is projective as a $\mathbf{Z}_p[\Delta]$-module. Therefore, $X$ is isomorphic as a $\Lambda_G$-module to the cokernel of a $\Lambda_G$-linear map $\Theta : \Lambda_G^n \longrightarrow \Lambda_G^n$ for some $n \geq 1$. The ring $\Lambda_G$ is commutative. Let $\theta = det(\Theta)$, an element of $\Lambda_G$. One can think of $\theta$ as a $\mathbf{Z}_p$-valued measure on $G$.

Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Then $n(\sigma) = 1$ and we can extend $\sigma$ to a surjective $\mathbf{Z}_p$-algebra homomorphism from $\mathbf{Z}_p[\Delta]$ to $\mathcal{O}$, which we also will denote by $\sigma$. Let $I_\sigma = ker(\sigma)$, an ideal in $\mathbf{Z}_p[\Delta]$. Let $X_{\mathcal{O}} = X \otimes_{\mathbf{Z}_p} \mathcal{O}$. We define the $\sigma$-component of $X_{\mathcal{O}}$ as the quotient $X_{\mathcal{O}}^{(\sigma)} = X_{\mathcal{O}}/I_\sigma X_{\mathcal{O}}$, which we can consider as a $\Lambda_{\mathcal{O}}$-module, where $\Lambda_{\mathcal{O}} = \mathcal{O}[[\Gamma]]$. As in the introduction, we can extend $\sigma$ to a $\Lambda$-algebra homomorphism from $\Lambda_G$ to $\Lambda_{\mathcal{O}}$, which we still denote by $\sigma$. Then it is not difficult to verify that $\sigma(\theta)$ is a generator of the characteristic ideal of the $\Lambda_{\mathcal{O}}$-module $X_{\mathcal{O}}^{(\sigma)}$. Thus, all of these characteristic ideals have generators which are *"interpolated"* by $\theta$.

Such an element $\theta \in \Lambda_G$ could also conceivably exist if we just make the assumptions in proposition 3.2.1. Then $X = X_E^{\Sigma_0}(K_\infty)$ is merely quasi-projective. Suppose that $X$ is actually strictly quasi-projective. In that case, there exists a projective $\mathbf{Z}_p[\Delta]$-module $Y$ such that $Y \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \cong X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ as a representation space for $\mathrm{Gal}(K_\infty/F)$. If $Y$ can be chosen to be $\Gamma$-invariant, then one can apply corollary 2.4.3 to the $\Lambda_G$-module $Y$. Such a $\theta$ would then exist because, for every $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, the $\Lambda_{\mathcal{O}}$-modules $X_{\mathcal{O}}^{(\sigma)}$ and $Y_{\mathcal{O}}^{(\sigma)}$ are pseudo-isomorphic and hence have the same characteristic ideal. However, we do not know when it is possible to find a $\Gamma$-invariant $Y$ as described above. $\Diamond$

## 3.2 Quasi-projectivity.

For proving quasi-projectivity of $X_E^{\Sigma_0}(K_\infty)$, it suffices to just make the assumptions *(c)*, *(d)*, and *(e)* from proposition 3.1.1, as we will now explain.

**A.** *Herbrand quotients for* $H^1(K_\infty, E[p^\infty])$. We assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion and, if $p = 2$, that $E(F_v)$ is connected for all $v|\infty$. Then, as explained in **F** of section 3.1, we can make the identifications (3.1.f). However, we need a slight refinement. Suppose that $C = PQ$ is a cyclic subgroup of $\Delta$, using the notation from section 2.1, part **B**. Let $\varepsilon$ be a character of $Q$. We will let $\otimes\varepsilon$ denote tensoring over $\mathbf{Z}_p$ with $L_\varepsilon$, a free $\mathcal{O}$-module of rank 1 on which $Q$ acts by $\varepsilon$. We can make the identifications

$$H^1(K_\infty, E[p^\infty])^{(\varepsilon)} \;\cong\; \big(H^1(K_\infty, E[p^\infty]) \otimes \varepsilon^{-1}\big)^Q$$

$$\cong H^1(K_\infty, E[p^\infty] \otimes \varepsilon^{-1})^Q \;\cong\; H^1(K_\infty^Q, E[p^\infty] \otimes \varepsilon^{-1})$$

where the last isomorphism comes from the inflation-restriction sequence together with the fact that $|Q|$ is prime to $p$. If $p$ is odd, then the assumptions for applying (3.1.e) are still satisfied and so we get

$$H^i\big(P, H^1(K_\infty, E[p^\infty])^{(\varepsilon)}\big) \cong H^i\big(P, H^1(K_\infty^Q, E[p^\infty] \otimes \varepsilon^{-1})\big) \cong H^{i+2}\big(P, H^0(K_\infty^Q, E[p^\infty] \otimes \varepsilon^{-1})\big)$$

for $i = 1, 2$. Now $H^0(K_\infty^Q, E[p^\infty] \otimes \varepsilon^{-1})$ can be identified with $H^0(K_\infty, E[p^\infty])^{(\varepsilon)}$, which is a subgroup of $E(K_\infty)[p^\infty] \otimes_{\mathbf{Z}_p} \mathcal{O}$ and hence is finite. Also, $P$ is cyclic and hence the cohomology is periodic with period 2. Therefore,

$$h_P\big(H^1(K_\infty, E[p^\infty])^{(\varepsilon)}\big) = h_P\big(H^0(K_\infty, E[p^\infty])^{(\varepsilon)}\big) = 1$$

at least if $p$ is odd. If $p = 2$, then we must show that if $F_v \cong \mathbf{R}$, then $H^i(F_v, E[p^\infty] \otimes \varepsilon^{-1})) = 0$. But since $\varepsilon$ will have odd order, it is enough to consider $H^i(F_v, E[p^\infty] \otimes_{\mathbf{Z}_p} \mathcal{O})$ and this vanishes because of the assumption that $E(F_v)$ is connected. Hence we can again apply (3.1.e).

**B.** *Herbrand quotients for $\mathcal{H}_v(K_\infty, E)$ when $v \notin \Phi_{K/F}$.* For any archimedean prime $v$, we have $\mathcal{H}_v(K_\infty, E) = 0$ and so there is nothing to prove. Assume that $v$ is non-archimedean and that $v \notin \Phi_{K/F}$. First suppose that $v \nmid p$. Then, as shown in part **G** of section 3.1, the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is projective. The Herbrand quotients $h_P(\mathcal{H}_v(K_\infty, E)^{(\varepsilon)})$ which occur in proposition 2.1.3 must then all be equal to 1.

Now suppose that $v|p$. Let $C = PQ$ be any cyclic subgroup of $\Delta$ and let $\varepsilon$ be a character of $Q$. Just as in (3.1.h), but replacing $\Delta$ by $C$, we can express $\mathcal{H}_v(K_\infty, E)$ as a direct product of $\mathbf{Z}_p[C]$-modules of the form

$$\mathcal{A} \;=\; \mathrm{Ind}_{C_\eta}^{C}\big(\mathcal{A}_\eta\big), \qquad \text{where} \quad \mathcal{A}_\eta \;=\; H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty]) \quad .$$

Here $\eta$ is a prime of $K_\infty$ lying above $v$ and $C_\eta$ is the corresponding decomposition subgroup of $C$. According to remark 2.1.9, $h_P(\mathcal{A}^{(\varepsilon)}) = 1$ if and only if $h_{P_\eta}(\mathcal{A}_\eta^{(\varepsilon_\eta)}) = 1$, where $P_\eta$ is the decomposition subgroup of $P$ for $\eta$ and $\varepsilon_\eta$ is the restriction of $\varepsilon$ to $Q_\eta$, the decomposition subgroup of $Q$ for $\eta$.

Just as in part **A**, the inflation-restriction sequence gives a canonical isomorphism

$$\mathcal{A}_\eta^{(\varepsilon_\eta)} \;=\; H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)} \;\cong\; H^1(K_{\infty,\eta}^{Q_\eta}, \overline{E}_v[p^\infty] \otimes \varepsilon_\eta^{-1})\big)$$

as $\mathcal{O}[P_\eta]$-modules. Since subgroups of $G_{F_{\infty,v}}$ have $p$-cohomological dimension 1, we can apply (3.1.e) to obtain

$$H^i(P_\eta, H^1(K_{\infty,\eta}^{Q_\eta}, \overline{E}_v[p^\infty] \otimes \varepsilon_\eta^{-1})\big) \;\cong\; H^{i+2}\big(P_\eta, H^0(K_{\infty,\eta}^{Q}, \overline{E}_v[p^\infty] \otimes \varepsilon_\eta^{-1})\big)$$

for any $i \geq 1$. The residue field for $K_{\infty,\eta}$ is finite. It follows that

$$H^0(K_{\infty,\eta}^{Q_\eta}, \overline{E}_v[p^\infty] \otimes \varepsilon_\eta^{-1})) \;\cong\; H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)}$$

is finite too. Since the cohomology of a finite cyclic group is periodic with period 2, it follows that

$$h_{P_\eta}\big(H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)}\big) \;=\; h_{P_\eta}\big(H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty]^{(\varepsilon_\eta)}\big) \;=\; 1$$

and therefore we have shown that $h_P\big(\mathcal{H}_v(K_\infty, E)\big) = 1$ for all primes $v$ of $F$ which are not in $\Phi_{K/F}$.

Using the results in **A** and **B**, we can now deduce the following result concerning quasi-projectivity for the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. Note that the assumption that $\mathrm{Sel}_E(K_\infty)[p]$ be finite implies that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion.

**Proposition 3.2.1.** *Assume that (c), (d), and (e) from proposition 3.1.1 are satisfied. Then $X_E^{\Sigma_0}(K_\infty)$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module.*

*Proof.* Suppose that $C = PQ$ is any cyclic subgroup of $\Delta$ and $\varepsilon$ is any character of $Q$. Then we have the following exact sequence of $\mathbf{Z}_p[P]$-modules:

$$0 \longrightarrow \big(\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big)^{(\varepsilon)} \longrightarrow \big(H^1(K_\infty, E[p^\infty])\big)^{(\varepsilon)} \longrightarrow \bigoplus_{v \notin \Sigma_0} \mathcal{H}_v(K_\infty, E)^{(\varepsilon)} \longrightarrow 0 \tag{3.2.a}$$

Using **A** and **B**, it is clear that $h_P\left(\big(\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p\big)^{(\varepsilon)}\right) = 1$. Proposition 2.1.3 then implies that the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is indeed quasi-projective. □

The following corollary follows immediately.

**Corollary 3.2.2.** *Assume that $\Phi_{K/F}$ is empty and that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. If $p = 2$, assume that $E(F_v)$ is connected for all archimedean primes $v$. Then $X_E(K_\infty)$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module.*

The hypotheses in this corollary are not uncommonly satisfied. Suppose that $\Pi$ is a Sylow $p$-subgroup of $\Delta$. We consider the fixed field $L = K^\Pi$ for $\Pi$. Then the assumption that $\Phi_{K/F}$ is empty just means that only primes of $L$ lying above $p$ or $\infty$ can ramify in the extension $K/L$. If one starts by choosing a finite extension $L$ of $F$ of degree prime to $p$, then there may be many finite $p$-extensions $K$ of $L$ which are ramified only at primes lying over $p$ and $\infty$. This is certainly true if $L$ is not totally real. We also want $K$ to be Galois over $F$ and $K \cap F_\infty = F$. Such examples are abundant. In any case, under the assumptions of the

corollary, we can take $\Sigma_0$ to be empty so that $\lambda_E^{\Sigma_0}(\sigma) = \lambda_E(\sigma)$ for all $\sigma$'s. Thus, we obtain the congruence relations for the $\lambda_E(\sigma)$'s just as described in the introduction.

Here are some specific types of examples. Suppose that $F = \mathbf{Q}$ and $L$ is an imaginary quadratic field. Suppose that $p$ is odd. Then one could take $K$ to be any layer in the anticyclotomic $\mathbf{Z}_p$-extension of $L$. Or one could take $K$ to be the $p$-Hilbert class field of $L$, or any layer in the $p$-Hilbert class field tower of $L$. (See [MR08] for a study of this type of example.) One other interesting type of example arises from an elliptic curve $A$ defined over $F$ whose $j$-invariant is an algebraic integer. The curve $A$ will have potentially good reduction at all primes of $F$. If $p \geq 5$, one could take $K$ to be any finite Galois extension of $F$ contained in $F(A[p^\infty])$ satisfying $K \cap F_\infty = F$. The ramification index for any $v \nmid p$ will be a divisor of 24 and hence not divisible by $p$. Thus, indeed, $\Phi_{K/F}$ will then be empty. This type of example will be discussed in section 8.1.

**Remark 3.2.3.** Suppose that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, but that $\mathrm{Sel}_E(K_\infty)[p]$ is infinite. Suppose that $\Sigma_0$ contains $\Phi_{K/F}$. If $p = 2$, suppose that $E(F_v)$ is connected for all archimedean primes $v$ of $F$. Consider the maximal divisible subgroup of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. Its Pontryagin dual is a $\mathbf{Z}_p[\Delta]$-module and, as a $\mathbf{Z}_p$-module, it is free of finite rank. That module should be quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. We mention two situations in which that assertion would be true. First of all, suppose that $E$ is isogenous over $F$ to an elliptic curve $E'$ such that $\mathrm{Sel}_{E'}(K_\infty)[p]$ is finite. Then it is quite easy to prove the assertion by applying proposition 3.2.1 to $E'$. Secondly, one can apply proposition 2.2.1 to $S = \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ if one knows that $\mathrm{Sel}_E(K_\infty)[p^2]/\mathrm{Sel}_E(K_\infty)[p]$ is finite, thus proving the assertion in that case. The needed assumptions about the Herbrand quotients are verified in the proof of proposition 3.2.1. $\Diamond$

## 3.3 Partial converses.

It is natural to ask if $X_E(K_\infty)$ itself can be projective or quasi-projective as a $\mathbf{Z}_p[\Delta]$-module when $\Phi_{K/F}$ is nonempty. It is certainly possible for this to happen because one could have $\mathcal{H}_v(K_\infty, E) = 0$ for all $v \in \Phi_{K/F}$. If that is so, then, taking $\Sigma_0 = \Phi_{K/F}$, one has $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \mathrm{Sel}_E(K_\infty)_p$. Thus, if all the other assumptions in propositions 3.1.1 and 3.2.1 are satisfied, except for the assumption that $\Sigma_0$ contains $\Phi_{K/F}$, then the projectivity or quasi-projectivity of $X_E(K_\infty)$ would follow. The vanishing of $\mathcal{H}_v(K_\infty, E)$ is not uncommon. We will discuss this in chapter 5. However, apart from this observation, one cannot really improve the propositions significantly, at least for $p \geq 5$, as the following result shows. We continue to assume good, ordinary reduction at all $v \in \Sigma_p$. We will prove the following proposition, using some results to be proved in chapter 5.

**Proposition 3.3.1** *Suppose that $\Sigma_o$ is a finite set of non-archimedean primes of $F$ which contains no prime over $p$. Let $\Sigma_1 = \Sigma_o \bigcup \Phi_{K/F}$.*

*(i) Assume that all of the assumptions in proposition 3.1.1 are satisfied except for the inclusion $\Phi_{K/F} \subseteq \Sigma_o$. If the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p$ is projective as a $\mathbf{Z}_p[\Delta]$-module, then $\mathcal{H}_v(K_\infty, E) = 0$ for all $v \in \Sigma_1 - \Sigma_o$ and therefore $\mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p = \mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$.*

*(ii) Suppose that $p \geq 5$. If the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module, then $\mathcal{H}_v(K_\infty, E) = 0$ for all $v \in \Sigma_1 - \Sigma_o$ and therefore $\mathrm{Sel}_E^{\Sigma_o}(K_\infty)_p = \mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$.*

*Proof.* For part *(i)*, proposition 3.1.1 implies that the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$ is a projective $\mathbf{Z}_p[\Delta]$-module. We have an exact sequence

$$0 \longrightarrow \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \longrightarrow \mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p \longrightarrow \prod_{v \in \Sigma_1 - \Sigma_0} \mathcal{H}_v(K_\infty, E) \longrightarrow 0 \quad .$$

If the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is also projective as a $\mathbf{Z}_p[\Delta]$-module, then it follows immediately that the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is also projective for each $v \in \Sigma_1 - \Sigma_0$. However, we will show later (in section 5.3) that, for any $v \in \Phi_{K/F}$, the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is projective if and only if $\mathcal{H}_v(K_\infty, E) = 0$.

For part *(ii)*, the assumption implies that $X_E^{\Sigma_0}(K_\infty)$ is a finitely-generated $\mathbf{Z}_p$-module. Therefore $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)[p]$ is finite, and hence so is $\mathrm{Sel}_E(K_\infty)[p]$. Thus, by proposition 3.2.1, $X_E^{\Sigma_1}(K_\infty)$ will then be quasi-projective. Using the above exact sequence and remark 2.1.6, it follows that the Pontryagin dual of $\prod_{v \in \Sigma_1 - \Sigma_0} \mathcal{H}_v(K_\infty, E)$ is also quasi-projective. Therefore, for any cyclic $p$-subgroup $P$ of $\Delta$, we have $\prod_{v \in \Sigma_1 - \Sigma_0} h_P(\mathcal{H}_v(K_\infty, E)) = 1$. However, as we will also show in section 5.3, if $p \geq 5$, then $h_P(\mathcal{H}_v(K_\infty, E)) \leq 1$ for all $P$ and all nonarchimedean $v \nmid p$. Thus, it follows that $h_P(\mathcal{H}_v(K_\infty, E)) = 1$ for all $v \in \Sigma_1 - \Sigma_0$, which is a subset of $\Phi_{K/F}$. However, for such $v$, proposition 5.3.1 also asserts that if $h_P(\mathcal{H}_v(K_\infty, E)) = 1$ for all $P$, then $\mathcal{H}_v(K_\infty, E) = 0$. The proposition follows from this. □

**Remark 3.3.2.** If $p < 5$, then the conclusion in part *(ii)* of proposition 3.3.1 can fail to be true. It is possible to have $h_P(\mathcal{H}_v(K_\infty, E)) > 1$ for some $v$. This can only happen if $E$ has additive reduction at $v$. We refer to remark 5.3.2 for more explanation. Thus, in some cases, the product of Herbrand quotients over $v \in \Sigma_1 - \Sigma_0$ occurring in the above proof can be 1, even though some factors are not 1. In such an unusual example, there will be a set $\Sigma_0$ with the following properties: The Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)$ is quasi-projective, $\Sigma_0$ does not contain $\Phi_{K/F}$, and $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is a proper subgroup of $\mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$. ◊

## 3.4 More general situations.

**A.** The results that we have described can be extended to a more general class of elliptic curves. First consider any elliptic curve $E$ with potentially good ordinary reduction at all the primes of $F$ lying above $p$. If $v$ is such a prime, then there exists a finite extension of $F_v$ over which $E$ has good ordinary reduction. The kernel of the reduction map is a subgroup of $E[p^\infty]$ which we denote by $F_v^+E[p^\infty]$. That subgroup is easily seen to be $G_{F_v}$-invariant. It is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$, as is the quotient group $E[p^\infty]/F_v^+E[p^\infty]$, which we will denote by $\overline{E}_v[p^\infty]$. By definition, the inertia subgroup of $G_{F_v}$ acts on $\overline{E}_v[p^\infty]$ through a finite quotient group. With this notation, the Selmer group $\mathrm{Sel}_E(K_\infty)_p$ can be defined just as in the introduction. The crucial point is that the isomorphism (1.2.a) is still valid, as proved in [CoGr]. (See proposition 4.3.) It is still true that $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])$ is finite. The proof of proposition 3.2.1 then goes through with virtually no change. As for proposition 3.1.1, one must just replace assumption *(b)* by the assumption that $H^0(K_w, \overline{E}_v[p^\infty]) = 0$ for all $v \in \Sigma_p$. Here $w$ is any prime of $K$ lying over $p$.

If $E$ has multiplicative or potentially multiplicative reduction at some $v$ lying over $p$, then the situation is different. One still has a canonical $G_{F_v}$-invariant subgroup $F_v^+E[p^\infty]$ isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group. We again denote the corresponding quotient group by $\overline{E}_v[p^\infty]$. The definition of $\mathrm{Sel}_E(K_\infty)_p$ remains the same as in the introduction. However, $G_{F_v}$ acts on $\overline{E}_v[p^\infty]$ either trivially or through a quotient group of order 2. If the action of $G_{K_{\infty,\eta}}$ is nontrivial and $p$ is odd, then $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty]) = 0$ and so the argument in this case works just as if $E$ were non-anomalous for any prime $w$ of $K$ lying above $v$. Even if $p = 2$, $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])$ would still be finite. However, if $E$ has split multiplicative reduction over $K_{\infty,\eta}$, then $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty]) \cong \mathbf{Q}_p/\mathbf{Z}_p$ and so the argument in part **D** of section 3.1 breaks down if $H^2(\Delta'_\eta, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$ for some subgroup $\Delta'_\eta$ of $\Delta_\eta$. The argument in part **H** breaks down if $p \big| |\Delta_\eta|$. For if $\Delta'_\eta$ is a subgroup of $\Delta_\eta$ of order $p$, then has $H^3(\Delta'_\eta, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$. The argument in section 3.2, part **B**, also breaks down if $p \big| |\Delta_\eta|$ since if $P_\eta$ is a cyclic subgroup of order $p^t$, then $h_{P_\eta}(\mathbf{Q}_p/\mathbf{Z}_p) = p^{-t}$.

One does have a useful analogue of proposition 3.2.1 which applies under the assumption that $E$ has potentially good or multiplicative reduction at all primes of $F$ lying above $p$. One must just replace $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ by the possibly larger group

$$\widetilde{\mathrm{Sel}}_E^{\Sigma_0}(K_\infty)_p \;=\; \ker\Big(H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{v \notin \Sigma_0} \widetilde{\mathcal{H}}_v(K_\infty, E)\Big)$$

where $\widetilde{\mathcal{H}}_v(K_\infty, E)$ is defined as follows. If $v \notin \Sigma_p$, we let $\widetilde{\mathcal{H}}_v(K_\infty, E) = \mathcal{H}_v(K_\infty, E)$. If $v \in \Sigma_p$ and $\eta | v$, let $I_\eta$ denote the inertia subgroup of $G_{K_{\infty,\eta}}$. We then let $\widetilde{\mathcal{H}}_v(K_\infty, E)$ be the image

of $\mathcal{H}_v(K_\infty, E)$ under the homomorphism

$$\prod_{\eta|v} H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty]) \;\longrightarrow\; \prod_{\eta|v} H^1(I_\eta, \overline{E}_v[p^\infty])$$

induced by the restriction maps. Thus, $\widetilde{\mathcal{H}}_v(K_\infty, E) \cong \mathcal{H}_v(K_\infty, E)/\mathcal{T}_v$, where $\mathcal{T}_v$ is a certain $\mathrm{Gal}(K_\infty/F)$-invariant subgroup of $\mathcal{H}_v(K_\infty, E)$. We now describe that subgroup. Note that for each $\eta|v$, we have

$$\ker\Big(H^1\big(K_{\infty,\eta}, \overline{E}_v[p^\infty]\big) \;\longrightarrow\; H^1\big(I_\eta, \overline{E}_v[p^\infty]\big)\Big) \;\cong\; H^1\big(K_{\infty,\eta}^{unr}/K_{\infty,\eta}, \overline{E}_v[p^\infty]^{I_\eta}\big)$$

and this group is finite (and trivial if $p$ is odd) unless $E$ has split multiplicative reduction over $K_{\infty,\eta}$. In the latter case, the kernel is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group. This doesn't depend on the choice of $\eta$ lying over $v$. Thus, as a group, $\mathcal{T}_v$ would be isomorphic to a direct sum of $\mathbf{Q}_p/\mathbf{Z}_p$'s, one for each $\eta$.

To discuss the action of $\Delta$ on $\mathcal{T}_v$, note that $G_{F_{\infty,v}}$ acts on $\overline{E}_v[p^\infty]$ by a character $\varepsilon_v$ of order 1 or 2. (We write $F_{\infty,v}$ instead of $F_{\infty,\nu}$ because this extension of $F_v$ doesn't depend on the choice of $\nu$ lying over $v$. Similarly, we write $\varepsilon_v$ instead of $\varepsilon_\nu$.) The group $\mathcal{T}_v$ is nontrivial (or infinite if $p = 2$) if and only if $\varepsilon_v$ factors through the quotient $\Delta_\eta$. Now $\Delta_\eta$ acts trivially on $\mathrm{Gal}(K_{\infty,\eta}^{unr}/K_{\infty,\eta}) \cong \widehat{\mathbf{Z}}$ and hence the above kernel is isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)(\varepsilon_v)$, the group $\mathbf{Q}_p/\mathbf{Z}_p$ on which $\Delta_\eta$ acts by $\varepsilon_v$. For any prime $\nu$ of $F_\infty$ lying over $v$, the primes $\eta$ of $K_\infty$ lying over $\nu$ form an orbit for the action of $\Delta$. Let $g_v$ denote the number of such orbits. Thus, assuming that $\varepsilon_v$ factors through $\Delta_\eta$, it follows that $\mathcal{T}_v$ is isomorphic to a direct sum of $g_v$ copies of $\mathrm{Ind}_{\Delta_\eta}^{\Delta}\big((\mathbf{Q}_p/\mathbf{Z}_p)(\varepsilon_v)\big)$ as $\mathbf{Z}_p[\Delta]$-modules. The corresponding quotient of $\mathcal{H}_v(K_\infty, E)$ is isomorphic to $\widetilde{\mathcal{H}}_v(K_\infty, E)$.

It is reasonable to believe that $\mathrm{Sel}_E(K_\infty)_p$ is a cotorsion $\Lambda$-module if $E$ has potentially good or multiplicative reduction at the primes of $F$ lying above $p$. Assuming this is the case, the global-to-local map defining $\mathrm{Sel}_E(K_\infty)_p$ is again surjective. One deduces that

$$\widetilde{\mathrm{Sel}}_E^{\Sigma_0}(K_\infty)_p/\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \;\cong\; \prod_{v|p} \mathcal{T}_v \tag{3.4.a}$$

for any finite set $\Sigma_0$ of primes not dividing $p$.

We want to prove the analogue of proposition 3.2.1 for the Pontryagin dual of the modified Selmer group $\widetilde{\mathrm{Sel}}_E^{\Sigma_0}(K_\infty)_p$. The argument is essentially the same and relies on parts **A** and **B** of section 3.2. The arguments in **A** work without change. As for **B**, we must show that the relevant Herbrand quotients for $\widetilde{\mathcal{H}}_v(K_\infty, E)$ are all equal to 1. It suffices to prove that

$$h_P\big(\mathcal{H}_v(K_\infty, E)^{(\varepsilon)}\big) \;=\; h_P\big(ker(\mathcal{H}_v(K_\infty, E)^{(\varepsilon)} \longrightarrow \widetilde{\mathcal{H}}_v(K_\infty, E)^{(\varepsilon)}\big)$$

for all $v \in \Sigma_p$, for every cyclic subgroup $C = PQ$ of $\Delta$, and every character $\varepsilon$ of $Q$. For that equality implies immediately that $h_P\big(\widetilde{\mathcal{H}}_v(K_\infty, E)^{(\varepsilon)}\big) = 1$. The proof then proceeds just as before.

As in section 3.2, part **B**, it is sufficient to prove that the Herbrand quotients for

$$H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)}, \quad \textit{and} \quad ker\big(H^1(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)} \longrightarrow H^1(I_\eta, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)}\big)$$

are equal, where now $C_\eta = P_\eta Q_\eta$ is a cyclic subgroup of $\Delta_\eta$. Equivalently, we must show

$$h_{P_\eta}\big(H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])^{(\varepsilon_\eta)}\big) \;=\; h_{P_\eta}\big(H^1(K_{\infty,\eta}^{unr}/K_{\infty,\eta}, \overline{E}_v[p^\infty]^{I_\eta})^{(\varepsilon_\eta)}\big) \quad .$$

This is not hard. First of all, $\overline{E}_v[p^\infty]$ is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ as a group and so if $G_{K_{\infty,\eta}}$ acts nontrivially on $\overline{E}_v[p^\infty]$, then both $H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty])$ and $H^1(K_{\infty,\eta}^{unr}/K_{\infty,\eta}, \overline{E}_v[p^\infty]^{I_\eta})$ are finite. The above Herbrand quotients are then both equal to 1. On the other hand, if $G_{K_{\infty,\eta}}$ acts trivially on $\overline{E}_v[p^\infty]$, then we have isomorphisms

$$H^0(K_{\infty,\eta}, \overline{E}_v[p^\infty]) \;\cong\; \overline{E}_v[p^\infty], \qquad H^1(K_{\infty,\eta}^{unr}/K_{\infty,\eta}, \overline{E}_v[p^\infty]^{I_\eta}) \;\cong\; \overline{E}_v[p^\infty]$$

which are equivariant for the action of $\Delta_\eta$. For the second isomorphism, one uses the fact that $K_{\infty,\eta}^{unr}/F_{\infty,v}$ is abelian and so $\Delta_\eta$ acts trivially on $\mathrm{Gal}(K_{\infty,\eta}^{unr}/K_{\infty,\eta})$. It follows that for every choice of $C_\eta = P_\eta Q_\eta$ and $\varepsilon_\eta$, the corresponding $\varepsilon_\eta$-components are isomorphic. Consequently, the equality of Herbrand quotients is obvious.

These observations prove the following result:

**Proposition 3.4.1.** *Assume that $E$ has potentially good, ordinary reduction or potentially multiplicative reduction at all primes of $F$ lying above $p$. Assume also that (c), (d), and (e) from proposition 3.1.1 are satisfied. Then the Pontryagin dual of the modified Selmer group $\widetilde{\mathrm{Sel}}_E^{\Sigma_0}(K_\infty)_p$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module.*

For every $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, let $\widetilde{\lambda}_E^{\Sigma_0}(\sigma) = \lambda\big(\widetilde{X}_E^{\Sigma_0}(K_\infty), \sigma\big)$, where $\widetilde{X}_E^{\Sigma_0}(K_\infty)$ denotes the Pontryagin dual of $\widetilde{\mathrm{Sel}}_E^{\Sigma_0}(K_\infty)_p$. This is defined if one assumes that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion and $\Sigma_0$ is a finite set of primes not including primes over $p$ and $\infty$. Under the assumptions of proposition 3.4.1, one gets nontrivial congruence relations for the $\widetilde{\lambda}_E^{\Sigma_0}(\sigma)$'s if $|\Delta|$ is divisible by $p$. By (3.4.a) and Frobenius reciprocity, we have the following formula

$$\widetilde{\lambda}_E^{\Sigma_0}(\sigma) \;-\; \lambda_E^{\Sigma_0}(\sigma) \;=\; \sum_{v \in \Sigma_p} g_v \langle \sigma|_{\Delta_\eta},\ \varepsilon_v \rangle$$

where the multiplicity $\langle \sigma|_{\Delta_\eta},\ \varepsilon_v \rangle$ is interpreted to be 0 if $\varepsilon_v$ doesn't factor through $\Delta_\eta$. Note that this multiplicity doesn't depend on the choice of $\eta$ lying over $v$. Also, one should really put the contragredient of $\varepsilon_v$ in the above formula, but since $\varepsilon_v$ has order 2, it defines a self-dual representation.

Formula (1.3.b) still holds in this more general context. Thus, the difference $\widetilde{\lambda}_E^{\Sigma_0}(\sigma) - \lambda_E(\sigma)$ can be expressed in terms of quantities defined purely locally at the primes in $\Sigma_p \cup \Sigma_0$.

**B.** We now consider an even more general situation. One can associate Selmer groups to Galois modules of the form $A = V/T$, where $V$ is a finite-dimensional $\mathbf{Q}_p$-representation space for $G_F$ and $T$ is a Galois-invariant $\mathbf{Z}_p$-lattice in $V$. This Selmer group can be defined if one makes certain assumptions of a local nature about $V$. This topic is discussed in detail in [Gr89]. Selmer groups are introduced there if one assumes a certain ordinariness condition at the primes of $F$ lying above $p$. Chapter 5 in that paper is even more general. We will use the notation $S_A(K_\infty)$, although the notation in [Gr89] is slightly different and more precise. The Selmer group $S_A(K_\infty)$ is defined as the kernel of a certain global-to-local map $\gamma_{A,K_\infty}$. Under the assumption that $V$ is *"p-critical"*, one shows that if $S_A(K_\infty)$ is $\Lambda$-cotorsion, then $\mathcal{C}_A(K_\infty) = coker\big(\gamma_{A,K_\infty}\big)$ is also $\Lambda$-cotorsion.

In the special case where $A = E[p^\infty]$ and $E$ has good, ordinary reduction at the primes of $K$ lying above $p$, we have $S_A(K_\infty) = \mathrm{Sel}_E(K_\infty)_p$. In contrast, if $E$ has split, multiplicative reduction at some of the primes of $K$ lying above $p$, then $S_A(K_\infty) = \widetilde{\mathrm{Sel}}_E(K_\infty)_p$, the modified Selmer group defined in remark 3.4, and this will be strictly bigger than $\mathrm{Sel}_E(K_\infty)_p$, assuming that it is $\Lambda$-cotorsion. In this case, $\mathrm{Sel}_E(K_\infty)_p$ coincides with the so-called *"strict Selmer group"* $S_A^{str}(K_\infty)$ which is also defined in [Gr89]. Actually, one has $\mathrm{Sel}_E(K_\infty)_p = S_A^{str}(K_\infty)$ just under the assumption that $E$ doesn't have potentially supersingular reduction at any prime above $p$. If one assumes that $\mathrm{Sel}_E(K_\infty)_p$ is $\Lambda$-cotorsion, then one has $\mathcal{C}_A(K_\infty) = 0$.

The most significant difference in the general setting is that it is possible for $\mathcal{C}_A(K_\infty)$ to be non-trivial. Assuming that $V$ is $p$-critical and that $S_A(K_\infty)$ is $\Lambda$-cotorsion, it turns out that the Pontryagin dual of $coker\big(\gamma_{A,K_\infty}\big)$ is pseudo-isomorphic to $H^0(K_\infty, T^*)$ as a $\Lambda[\Delta]$-module. Here, as in [Gr89], we define $T^* = \mathrm{Hom}\big(A, \mu_{p^\infty}\big)$, a free $\mathbf{Z}_p$-module of rank $n = dim(V)$. We cannot give a good reference for this, but the necessary arguments can essentially be found in the proof of proposition 4.13 in [Gr99].

Surjectivity of the global-to-local map plays an important role in the proofs of propositions 3.1.1 and 3.2.1. Thus, if $\mathcal{C}_A(K_\infty) \neq 0$, then the proofs break down. One remedy for this difficulty is to consider the non-primitive Selmer group $S_A^{\Sigma_0}(K_\infty)$, defined to be the kernel of a map $\gamma_{A,K_\infty}^{\Sigma_0}$, where one omits the local conditions for primes in $\Sigma_0$. We assume as usual that $\Sigma_0$ is a finite set of primes not containing primes above $p$ or $\infty$. If one assumes that $V$ is $p$-critical, that $S_A(K_\infty)$ is $\Lambda$-cotorsion, and that $\Sigma_0$ is non-empty, then it turns out that $\gamma_{A,K_\infty}^{\Sigma_0}$ is surjective. (See the comment following proposition 4.13 in [Gr99].) Thus, one can

then prove analogues of propositions 3.1.1 or 3.2.1 under suitable sets of assumptions. We have not carefully checked what the needed assumptions are in this general setting. Under all of these assumptions, one has the following exact sequence

$$0 \longrightarrow \mathrm{Sel}_A(K_\infty) \longrightarrow \mathrm{Sel}_A^{\Sigma_0}(K_\infty) \longrightarrow \prod_{v\in\Sigma_0} \mathcal{H}_v(K_\infty, A) \longrightarrow \mathcal{C}_A(K_\infty) \longrightarrow 0 \tag{3.4.b}$$

Therefore, one obtains an equation analogous to (1.3.b). One must just modify it by including an additional term which takes into account the action of $\Delta$ on $H^0(K_\infty, T^*)$. Of course, that term is subtracted on the right side of the equation.

## 3.5 $\Delta \rtimes \Gamma$-extensions.

We now consider a different type of generalization. We return to the situation where $E$ is an elliptic curve defined over $F$ with good, ordinary reduction at the primes above $p$. Propositions 3.1.1, 3.2.1, 3.3.1, and corollary 3.2.2 are all valid almost exactly as stated in the following situation. Just as before, let us assume that $K_\infty = KF_\infty$, where $K$ is a finite Galois extension of $F$. However, we won't necessarily assume that $K \cap F_\infty = F$. Thus, $K_\infty$ is the cyclotomic $\mathbf{Z}_p$-extension of $K$ and is a finite Galois extension of $F_\infty$. Let $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$. Then $\Delta$ acts on $\mathrm{Sel}_E(K_\infty)_p$, but there may not be a well-defined action of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on that Selmer group. Nevertheless, for the conclusions in the above propositions to be valid, one only needs to replace the assumption that $\mathrm{Sel}_E(K_\infty)_p$ be $\Lambda$-cotorsion by the assumption that $\mathrm{Sel}_E(K_\infty)_p$ be cotorsion over the ring $\mathbf{Z}_p[[\Gamma_K]]$, where $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. Assumption *(e)* in proposition 3.1.1 would certainly suffice because it implies that $\mathrm{Sel}_E(K_\infty)_p$ has finite $\mathbf{Z}_p$-corank which, in turn, implies that $\mathrm{Sel}_E(K_\infty)_p$ is $\mathbf{Z}_p[[\Gamma_K]]$-cotorsion.

If $K \cap F_\infty = F$, then the restriction map defines an isomorphism of $\Gamma_K$ to $\Gamma$. However, in general, we would have $K \cap F_\infty = F_m$ for some $m \geq 0$, where $F_m$ is the unique subfield of $F_\infty$ such that $[F_m : F] = p^m$. The restriction map is then an isomorphism of $\Gamma_K$ to $\Gamma_m = \mathrm{Gal}(F_\infty/F_m)$. Note that $\Gamma_m = \Gamma^{p^m}$. The restriction map also gives an injective homomorphism of $\Delta$ to $\mathrm{Gal}(K/F)$. The image is $\mathrm{Gal}(K/F_m)$ and the cokernel is isomorphic to $\mathrm{Gal}(F_m/F)$, a cyclic group of order $p^m$. We will often use the notation $D$ for $\mathrm{Gal}(K/F)$ to distinguish it from $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$.

Note that if we replace the base field $F$ by $F_m$, then we are in the earlier situation. We have $\mathrm{Gal}(K_\infty/F_m) \cong \Delta \times \Gamma_m$. In that isomorphism, $\Gamma_m$ is identified with $\Gamma_K$. We can replace the set $\Sigma_0$ by the set $\Sigma_{o,m}$ consisting of the primes of $F_m$ lying over primes in $\Sigma_0$. Only primes above $p$ are ramified in $F_m/F$ and hence $\Phi_{K/F_m}$ contains just the primes of $F_m$ lying above primes in $\Phi_{K/F}$. Also, $F_m$ and $F$ have the same completions at archimedean primes.

Alternatively, one can start by just assuming that $K_\infty$ is a Galois extension of $F$ which contains $F_\infty$ and that $[K_\infty : F_\infty]$ is finite. We then have an exact sequence

$$1 \longrightarrow \Delta \longrightarrow \mathrm{Gal}(K_\infty/F) \longrightarrow \Gamma \longrightarrow 1 \quad .$$

where $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$ and $\Gamma = \mathrm{Gal}(F_\infty/F)$. One sees easily that this group extension is split. Hence there exists a subfield $K'$ of $K_\infty$ containing $F$ such that $\mathrm{Gal}(K_\infty/K') \cong \Gamma$, $K' \cap F_\infty = F$, and $K'F_\infty = K_\infty$. One has $[K' : F] = |\Delta|$, but $K'$ may fail to be a Galois extension of $F$. One can choose the splitting so that $K'$ is Galois over $F$ if and only if the natural homomorphism $\Gamma \to \mathrm{Aut}(\Delta)/\mathrm{Inn}(\Delta)$ is trivial. Here $\mathrm{Aut}(\Delta)$ is the group of automorphisms of $\Delta$ and $\mathrm{Inn}(\Delta)$ is the subgroup of inner automorphisms. In general, let $K$ be the compositum of all the conjugates of $K'$ over $F$. Then $K/F$ is a finite Galois extension and we do indeed have $K_\infty = KF_\infty$. If $K'/F$ is not Galois, then $K \cap F_\infty = F_m$, where $m \geq 1$.

One could easily formulate the propositions just in terms of $F_\infty$ and $K_\infty$ without even referring to $\Gamma$. One defines $\Delta$ to be $\mathrm{Gal}(K_\infty/F_\infty)$ as before. The proofs would be virtually unchanged, although the fact that those fields are the cyclotomic $\mathbf{Z}_p$-extensions of number fields enters in an important way in some of the steps. It is worth noting that $p$ is anomalous for $E/K$ if and only if $p$ is anomalous for $E/K_\infty$, which is what the arguments actually use. Also, it is obvious that $E(K)[p] = 0$ if and only if $E(K_\infty)[p] = 0$, which is another ingredient.

Since $\mathrm{Gal}(K_\infty/F)$ is isomorphic to the semidirect product $\Delta \rtimes \Gamma$, where $\Gamma$ acts on $\Delta$ by some homomorphism $\Gamma \to \mathrm{Aut}(\Delta)$, we will refer to $K_\infty/F$ as a $(\Delta \rtimes \Gamma)$-extension. In the special case where one can choose $\Gamma$ so that its action on $\Delta$ is trivial, we will call $K_\infty/F$ a $(\Delta \times \Gamma)$-extension. In the general case, the above discussion shows that if $\mathrm{Gal}(K_\infty/F)$ is a $\Delta \rtimes \Gamma$-extension, then $K_\infty/F_m$ is a $(\Delta \times \Gamma_m)$-extension for some $m \geq 0$.

Suppose that $K_\infty/F$ is a $(\Delta \rtimes \Gamma)$-extension, that $K$ is defined as above, and that $D = \mathrm{Gal}(K/F)$. Let $G = \mathrm{Gal}(K_\infty/F)$. Thus, $\Delta$ is a normal subgroup of $G$ and $D$ is a certain quotient group. There is a fairly simple relationship between the irreducible representations of $D$ and $\Delta$. To describe this, we identify $\Delta$ with its image in $D$. It is a normal subgroup and $D/\Delta \cong \mathbf{Z}/p^m\mathbf{Z}$. Suppose that $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$. Of course, $\rho|_\Delta$ may be reducible. We let $Orb_\rho$ denote the set of irreducible constituents in $\rho|_\Delta$. We use that notation for the following reason. Conjugation gives a well-defined action of $D/\Delta$ on the set $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $Orb_\rho$ is one of the orbits. The cardinality of $Orb_\rho$ divides $p^m$, where $m$ is as above. Furthermore, if $\sigma \in Orb_\rho$, then the multiplicity of $\sigma$ in $\rho|_\Delta$ is 1. This last assertion follows from proposition (9.12) in [Fei], using the fact that $D/\Delta$ is cyclic.

In this situation, one does not have a well-defined action of $D$ on $\mathrm{Sel}_E(K_\infty)_p$. However, it seems natural to make the following definitions. Fix a set $\Sigma_0$ of primes as usual. We can

define $\lambda_E^{\Sigma_0}(\sigma)$ for every $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ just as before. We can extend this to the Grothendieck group $\mathcal{R}_{\mathcal{F}}(\Delta)$ to have a homomorphism $\lambda_E^{\Sigma_0} : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathbf{Z}$. We then define

$$\lambda_E^{\Sigma_0}(\rho) \;=\; \lambda_E^{\Sigma_0}\big(\rho|_\Delta\big) \;=\; \sum_{\sigma \in Orb_\rho} \lambda_E^{\Sigma_0}(\sigma) \tag{3.5.a}$$

for all $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$. Of course, if $\Sigma_0$ is empty, we omit it from the notation. These definitions can be extended to give homomorphisms from $\mathcal{R}_{\mathcal{F}}(D)$ to $\mathbf{Z}$. It is important to note that if $\sigma, \sigma' \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ are in the same orbit under the action of $\Gamma$ (or equivalently, under the action of $D/\Delta$), then one can show that $\lambda_E^{\Sigma_0}(\sigma) = \lambda_E^{\Sigma_0}(\sigma')$ for any choice of $\Sigma_0$. This is not difficult to prove. Consequently, $\lambda_E^{\Sigma_0}(\rho) = |Orb_\rho| \cdot \lambda_E^{\Sigma_0}(\sigma)$ for any $\sigma \in Orb_\rho$.

Suppose that $\rho_1$ and $\rho_2$ are representations of $D$ over $\mathcal{F}$ and that $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$. We then have a similar isomorphism for the restrictions of $\rho_1$ and $\rho_2$ to $\Delta$. Therefore, if the hypotheses in proposition 3.2.1 are satisfied, then we have a congruence relation $\lambda_E^{\Sigma_0}(\rho_1) = \lambda_E^{\Sigma_0}(\rho_2)$.

As a final remark, assume that hypotheses *(a), (b), (c)*, and *(d)* in proposition 3.1.1 are satisfied. One can then apply proposition 2.4.1 to conclude that $X_E^{\Sigma_0}(K_\infty)$ has a free resolution of length 1 as a $\Lambda_G$-module. Thus, its projective dimension is 1.

# 4 Selmer atoms.

Let $\Sigma$ be a finite set of primes of $F$ containing the set $\Sigma_p$ of primes lying over $p$, the set $\Sigma_\infty$ of archimedean primes of $F$, the set $\Psi_E$ of primes where $E$ has bad reduction, as well as the set $\mathrm{Ram}(K/F)$ of primes which are ramified in $K/F$. Thus, the maximal extension $F_\Sigma$ of $F$ unramified outside of $\Sigma$ contains $K_\infty$ and $F(E[p^\infty])$. We will assume in this chapter that $K \cap F_\infty = F$. Everything we discuss can be reduced to that case by replacing $F$ by $K \cap F_\infty$ if necessary. (See section 3.5.)

Let $\mathrm{Rep}_{\mathfrak{f}}(\Delta)$ denote the set of finite-dimensional representations of $\Delta = \mathrm{Gal}(K/F)$ over $\mathfrak{f}$, up to isomorphism. If $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$, we will denote the underlying representation space for $\alpha$ by $U_\alpha$. For any such $\alpha$, consider $E[p] \otimes_{\mathbf{F}_p} U_\alpha$, a representation space for $\mathrm{Gal}(F_\Sigma/F)$ over $\mathfrak{f}$ of dimension $2n(\alpha)$. We denote it more briefly by $E[p] \otimes \alpha$. The action of $\mathrm{Gal}(F_\Sigma/F)$ on $E[p] \otimes \alpha$ factors through the quotient group $\mathrm{Gal}\big(K(E[p])/F\big)$.

The definition of $\mathrm{Sel}_{E[p]\otimes\alpha}^{\Sigma_0}(F_\infty)$ was given in section 1.4. One can see easily that it is a subgroup of $H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ and is defined by the local triviality conditions for the primes $v \in \Sigma - \Sigma_0$. All of the cohomology groups $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ can be naturally considered as modules over the group ring $\mathfrak{f}[[\Gamma]]$, where $\Gamma = \mathrm{Gal}(F_\infty/F)$. Different aspects

of their structure are discussed in section 4.1. The Selmer groups are also modules over that ring and their structure is the subject of section 4.2.

Our main objective in this chapter is to prove Theorem 2, which follows the outline in the introduction and will be completed only in section 4.4. Hypothesis *(ii)* in that result implies that $p$ is odd. We will simply make the blanket assumption in this chapter that $p$ is an odd prime, although it is not actually needed in many of the steps. In some parts, we will make brief comments concerning the case $p = 2$. We will mostly assume that $E$ has good, ordinary reduction at the primes of $F$ lying over $p$. That assumption is not needed until part **D** of section 4.1.

## 4.1 Various cohomology groups. Coranks. Criteria for vanishing.

**A.** *Coranks of* $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ *over* $\mathfrak{f}[[\Gamma]]$. We can relate these coranks for $i = 1, 2$ to each other by studying the growth of $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)^{\Gamma_n}$ as $n$ varies. Here $\Gamma_n$ is the unique subgroup of $\Gamma$ of index $p^n$. Thus, $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, where $F_n$ is a cyclic extension of $F$ of degree $p^n$, the $n$-th layer in the $\mathbf{Z}_p$-extension $F_\infty/F$. Consider the restriction maps

$$\rho_n^{(i)} : \ H^i(F_\Sigma/F_n, E[p] \otimes \alpha) \ \longrightarrow \ H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)^{\Gamma_n} \quad .$$

It turns out that $\rho_n^{(i)}$ is surjective. This follows for $i = 1$ from the usual inflation-restriction sequence since $H^2\big(\Gamma_n, H^0(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big) = 0$.

For $i = 2$, one can also use an exact sequence derived from the Hochschild-Serre spectral sequence. The objects $E_2^{ab} = H^a\big(\Gamma_n, H^b(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big)$ in that spectral sequence vanish when $a \geq 2$. This is because $\Gamma_n$ has $p$-cohomological dimension 1. Consequently, $E_2^{ab} \cong E_\infty^{ab}$ for all $a$ and $b$, and this vanishes when $a \geq 2$. Hence only the first two columns of objects in the spectral sequence can be nonzero. The filtration on $H^2(F_\Sigma/F_n, E[p] \otimes \alpha)$ collapses to just a subgroup isomorphic to $E_2^{11}$ (which will be the kernel of $\rho_n^{(2)}$) and a quotient group isomorphic to $E_2^{02} = H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)^{\Gamma_n}$, where the isomorphism is induced by $\rho_n^{(2)}$. Thus, $\mathrm{coker}(\rho_n^{(2)}) = 0$.

It is known that $H^i(F_\Sigma/F, E[p] \otimes \alpha)$ is finite for any $i$. Applying the above result for $n = 0$ and $i = 1, 2$ then shows that $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)^\Gamma$ is also finite. It follows that $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ is cofinitely generated as a $\mathfrak{f}[[\Gamma]]$-module. The same is true for $H^0(F_\Sigma/F_\infty, E[p] \otimes \alpha)$, which is obviously finite and hence is cotorsion as a module over $\mathfrak{f}[[\Gamma]]$. Although it won't be needed, we remark that $H^i(F_\Sigma/F_\infty, E[p] \otimes \alpha) = 0$ for $i \geq 3$ if $p$ is odd or if $p = 2$ and $E(F_v)$ is connected for all archimedean primes $v$ of $F$. It could be nontrivial otherwise, but will still be cofinitely generated.

To study the growth of $H^i(F_\Sigma/F_\infty, E[p]\otimes\alpha)^{\Gamma_n}$, we will need the isomorphisms

$$\ker(\rho_n^{(1)}) \cong H^1(\Gamma_n, A), \qquad \ker(\rho_n^{(2)}) \cong H^1(\Gamma_n, B)$$

where we let $A = H^0(F_\Sigma/F_\infty, E[p]\otimes\alpha) = (E[p]\otimes\alpha)^{G_{F_\infty}}$ and $B = H^1(F_\Sigma/F_\infty, E[p]\otimes\alpha)$ for brevity. The first isomorphism follows from the inflation-restriction sequence. The second follows from the above remarks since $H^1(\Gamma_n, B) = E_2^{11}$. It follows that $\ker(\rho_n^{(1)})$ is finite and has bounded order. In fact, for $n$ sufficiently large, we have $|\ker(\rho_n^{(1)})| = |A|$ since $A$ is finite.

The $\mathfrak{f}[[\Gamma]]$-module $B$ is cofinitely generated. Let $h_1$ denote its corank. Since $\mathfrak{f}[[\Gamma]]$ is a PID, the Pontryagin dual $\widehat{B}$ of $B$ is isomorphic to the direct sum of a free $\mathfrak{f}[[\Gamma]]$-module of rank $h_1$ and a finitely-generated torsion-module. The torsion-module will be finite. Thus $B$ contains a cofree $\mathfrak{f}[[\Gamma]]$-submodule, which we denote by $B_{div}$, such that the quotient module $B/B_{div}$ is finite. We use this notation because $B_{div}$ is precisely the maximal divisible $\mathfrak{f}[[\Gamma]]$-submodule of $B$. Also, we have $B \cong B_{div}\oplus B/B_{div}$ as a $\mathfrak{f}[[\Gamma]]$-module. One sees easily that $H^1(\Gamma_n, B_{div}) = 0$ for all $n \geq 0$. Hence $H^1(\Gamma_n, B) = H^1(\Gamma_n, B/B_{div})$. It follows that $\ker(\rho_n^{(2)})$ is finite and has bounded order. In fact, if $n$ is sufficiently large, $\Gamma_n$ acts trivially on $B/B_{div}$ and hence we then have $|\ker(\rho_n^{(2)})| = |B/B_{div}|$.

We have already proved the first part of the following result.

**Proposition 4.1.1.** *The cohomology groups $H^i(F_\Sigma/F_\infty, E[p]\otimes\alpha)$ are cofinitely generated as modules over the ring $\mathfrak{f}[[\Gamma]]$ for $0 \leq i \leq 2$. The module $H^0(F_\Sigma/F_\infty, E[p]\otimes\alpha)$ is cotorsion. We have*

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^1(F_\Sigma/F_\infty, E[p]\otimes\alpha)\big) \;=\; \mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^2(F_\Sigma/F_\infty, E[p]\otimes\alpha)\big) \;+\; n(\alpha)[F:\mathbf{Q}] \quad .$$

*Furthermore, $H^2(F_\Sigma/F_\infty, E[p]\otimes\alpha)$ is a cofree $\mathfrak{f}[[\Gamma]]$-module.*

*Proof.* If $H$ is an $\mathfrak{f}[[\Gamma]]$-module of corank $h$, then one sees easily that $\dim_{\mathfrak{f}}\big(H^{\Gamma_n}\big) = hp^n + O(1)$ as $n\to\infty$. We have $\dim_{\mathfrak{f}}\big(H^{\Gamma_n}\big) \geq hp^n$ for all $n$ and equality holds for at least one $n$ if and only if $H$ is a cofree $\mathfrak{f}[[\Gamma]]$-module. This can be seen by using the fact that $\mathfrak{f}[[\Gamma]]$ is a PID. For $0 \leq i \leq 2$, let $h_i = \mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^i(F_\Sigma/F_\infty, E[p]\otimes\alpha)\big)$. It is obvious that $h_0 = 0$. Using the notation and the remarks described above, if $n$ is sufficiently large, we have

$$\dim_{\mathfrak{f}}\big(H^0(F_\Sigma/F_n, E[p]\otimes\alpha)\big) \;=\; \dim_{\mathfrak{f}}(A) \quad ,$$

$$\dim_{\mathfrak{f}}\big(H^1(F_\Sigma/F_n, E[p]\otimes\alpha)\big) \;=\; h_1p^n \;+\; \dim_{\mathfrak{f}}\big(B/B_{div}\big) \;+\; \dim_{\mathfrak{f}}(A) \quad .$$

We have used the fact that $\dim_{\mathfrak{f}}\big(\ker(\rho_n^{(1)})\big) = \dim_{\mathfrak{f}}(A)$ if $n >> 0$. The Euler-Poincaré characteristic for the $\mathrm{Gal}(F_\Sigma/F_n)$-module $E[p]\otimes\alpha$, by which we mean the alternating sum of the $\mathfrak{f}$-dimensions of the cohomology groups $H^i(F_\Sigma/F_n, E[p]\otimes\alpha)$, can be expressed as

$$\dim_{\mathfrak{f}}(A) - \Big(h_1p^n + \dim_{\mathfrak{f}}\big(B/B_{div}\big) + \dim_{\mathfrak{f}}(A)\Big) \;+\; \dim_{\mathfrak{f}}\Big(H^2(F_\Sigma/F_n, E[p]\otimes\alpha)\Big) \quad . \tag{4.1.a}$$

One can calculate this from the standard formula for finite Galois modules, as given in proposition 8.6.14 in [NSW], for example. The formula involves contributions from all of the archimedean primes of $F_n$. The contribution to the value of (4.1.a) from the complex primes is $-2n(\alpha)$. For each real prime, one notes that the $+1$ and $-1$ eigenspaces for the action of complex conjugation on $E[p]$ are both 1-dimensional over $\mathbf{F}_p$. It follows that each eigenspace for the action of complex conjugation on $E[p] \otimes \alpha$ has $\mathfrak{f}$-dimension $n(\alpha)$, and the corresponding contribution to (4.1.a) is $-n(\alpha)$. Thus, the Euler-Poincaré characteristic (4.1.a) turns out to equal $-n(\alpha)[F_n : \mathbf{Q}]$. As a consequence, we have

$$\dim_{\mathfrak{f}}(A) - \Big(h_1 p^n + \dim_{\mathfrak{f}}\big(B/B_{div}\big) + \dim_{\mathfrak{f}}(A)\Big) + \dim_{\mathfrak{f}}\Big(H^2(F_\Sigma/F_n, E[p] \otimes \alpha)\Big) \;=\; -n(\alpha)[F_n : \mathbf{Q}]$$

and we therefore find that

$$\dim_{\mathfrak{f}}\big(H^2(F_\Sigma/F_n, E[p] \otimes \alpha)\big) \;=\; \Big(h_1 - n(\alpha)[F : \mathbf{Q}]\Big)p^n \;+\; \dim_{\mathfrak{f}}\big(B/B_{div}\big) \quad .$$

for sufficiently large $n$. We also have $\dim_{\mathfrak{f}}\big(\ker(\rho_n^{(2)})\big) = \dim_{\mathfrak{f}}\big(B/B_{div}\big)$. Therefore,

$$\dim_{\mathfrak{f}}\big(H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)^{\Gamma_n}\big) \;=\; \Big(h_1 - n(\alpha)[F : \mathbf{Q}]\Big)p^n$$

for sufficiently large $n$. This implies two things: $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ has $\mathfrak{f}[[\Gamma]]$-corank $h_2 = h_1 - n(\alpha)[F : \mathbf{Q}]$ and is actually $\mathfrak{f}[[\Gamma]]$-cofree. The proposition follows. □

**Corollary 4.1.2.** *We have the inequality*

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big) \;\geq\; n(\alpha)[F : \mathbf{Q}] \quad .$$

*Equality holds if and only if* $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha) = 0$.

The above proofs work without change if $p = 2$. However, in that case, there may be a lower bound on the $\mathfrak{f}[[\Gamma]]$-corank of $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big)$ coming from the real archimedean primes. Suppose that $v$ is such a prime and that $E(F_v)$ has two connected components. The action of $G_{F_v}$ on $E[2]$ will then be trivial and we will have $|H^i(F_v, E[2]| = 4$ for all $i \geq 1$. Hence it is possible for $H^i(F_v, E[p] \otimes \alpha)$ to be nontrivial. Its order (and hence its $\mathfrak{f}$-dimension) will then be independent of $i$. For every $i \geq 1$ and $n \geq 0$, there is a map

$$H^i(F_\Sigma/F_n, E[p] \otimes \alpha) \;\longrightarrow\; \prod_{\nu|v} H^i(F_{n,\nu}, E[p] \otimes \alpha)$$

where $\nu$ varies over the primes of $F_n$ lying above $v$ and $F_{n,\nu}$ denotes the $\nu$-adic completion of $F_n$. This map is an isomorphism for $i \geq 3$. It is surjective for $i = 1, 2$. In particular, since $v$ splits completely in $F_\infty/F$, we get a lower bound

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^2(F_\Sigma/F_n, E[p] \otimes \alpha)\big) \;\geq\; \sum_{v|\infty} \dim_{\mathfrak{f}}\big(H^2(F_v, E[p] \otimes \alpha)\big)$$

and so one may have a lower bound on $\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big)$ which is strictly larger than $n(\alpha)[F : \mathbf{Q}]$.

**B.** *Vanishing of $H^0(F, E[p] \otimes \alpha)$.* Since $G_K$ acts trivially on $\alpha$, we have an isomorphism $E[p] \otimes \alpha \cong (E[p] \otimes \mathfrak{f})^{n(\alpha)}$ as $\mathfrak{f}$-representation spaces for $G_K$. If we make the assumption that $E(K)[p] = H^0(K, E[p])$ vanishes, then it follows that $H^0(F, E[p] \otimes \alpha) = 0$ for any $\alpha$. On the other hand, if $E(K)[p] \neq 0$, then we can regard $E(K)[p] \otimes \mathfrak{f}$ as a nontrivial $\mathfrak{f}$-representation space for $\Delta$. It contains a $\Delta$-invariant subspace $U$ on which $\Delta$ acts irreducibly. Thus, for some $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, we have $U \cong U_{\check{\tau}}$, the underlying representation space for the contragredient representation $\check{\tau}$ for $\tau$. Then, for that $\tau$,

$$H^0(F,\; E[p] \otimes \tau) \;\cong\; H^0\big(F,\; \mathrm{Hom}(U_{\check{\tau}}, \mathfrak{f}) \otimes E[p])\big) \;\cong\; H^0\big(F,\; \mathrm{Hom}(U_{\check{\tau}}, E[p] \otimes \mathfrak{f})\big)$$

will be nontrivial. The following proposition summarizes these observations. It is valid even for $p = 2$.

**Proposition 4.1.3.** *The following statements about $E[p]$ are equivalent:*

*(i)* $E(K)[p] = 0$,
*(ii)* $H^0(F, E[p] \otimes \alpha) = 0$ *for all* $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$,
*(iii)* $H^0(F, E[p] \otimes \tau) = 0$ *for all* $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

*Furthermore, $H^0(F_\infty, E[p] \otimes \alpha) = 0$ if and only if $H^0(F, E[p] \otimes \alpha) = 0$ and $E(K_\infty)[p] = 0$ if and only if $E(K)[p] = 0$.*

The final statement is true just because $\mathrm{Gal}(F_\infty/F)$ and $\mathrm{Gal}(K_\infty/K)$ are pro-$p$ groups.

**C.** *Vanishing of $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$.* We have $H^2(F_{\infty,v}, E[p] \otimes \alpha) = 0$ for all $v$. This is true for non-archimedean primes $v$ because $G_{F_{\infty,v}}$ always has $p$-cohomological dimension 1, It is true for archimedean primes $v$ because $p$ is odd. In particular, we see that

$$H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha) \;=\; Ш^2(F_\Sigma/F_\infty, E[p] \otimes \alpha) \quad ,$$

the group of everywhere locally trivial 2-cocycle classes. We can relate this group to $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$, the group of locally trivial 1-cocycle classes, by using one of the Poitou-Tate duality theorems. The result is the following proposition.

**Proposition 4.1.4.** *Suppose that $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$. With the above assumptions, the following statements are equivalent:*

*(i)* $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha) = 0$,

*(ii)* $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ *is finite,*

*(iii)* $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$ *is finite.*

*Proof.* We know that *(i)* and *(ii)* are equivalent by the last part of proposition 4.1.1. Let $F_n$ denote the $n$-th layer in the $\mathbf{Z}_p$-extension $F_\infty/F$ as before. To use the Poitou-Tate duality theorems, note that

$$\mathrm{Hom}\big(E[p] \otimes \alpha,\ \mu_p\big) \cong E[p] \otimes \check{\alpha} \tag{4.1.b}$$

by the Weil pairing and standard canonical isomorphisms from linear algebra. Thus, for every $n$, we have a perfect pairing of the $\mathfrak{f}$-vector spaces

$$Ш^1(F_\Sigma/F_n, E[p] \otimes \check{\alpha}) \times Ш^2(F_\Sigma/F_n, E[p] \otimes \alpha) \longrightarrow \mathbf{F}_p \quad ,$$

which we refer to as the Poitou-Tate pairing.

Assume that *(ii)* is satisfied. Since $\ker(\rho_n^{(2)})$ has bounded order, it follows that the order of $H^2(F_\Sigma/F_n, E[p] \otimes \alpha)$ is bounded as $n \to \infty$. Therefore, the same thing is true for the order of $Ш^2(F_\Sigma/F_n, E[p] \otimes \alpha)$ and hence $Ш^1(F_\Sigma/F_n, E[p] \otimes \check{\alpha})$. Thus, $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$ is finite, and so *(iii)* is satisfied.

Assume that *(iii)* is satisfied. Consider the map $\check{\rho}_n^{(1)}$ which is defined just as $\rho_n^{(1)}$, but for the Galois module $E[p] \otimes \check{\alpha}$ instead of $E[p] \otimes \alpha$. Its kernel has bounded order, and so it follows that $Ш^1(F_\Sigma/F_n, E[p] \otimes \check{\alpha})$ and hence $Ш^2(F_\Sigma/F_n, E[p] \otimes \alpha)$ have bounded order. Thus, $Ш^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ is finite, and so *(ii)* is satisfied. □

**Remark 4.1.5.** In the above proofs, the restriction maps play a role. We can say a little more about them. For $m \geq n$ (including the possibility that $m = \infty$), consider

$$r_{m/n}^{(i)} :\ Ш^i(F_\Sigma/F_n, E[p] \otimes \alpha) \longrightarrow Ш^i(F_\Sigma/F_m, E[p] \otimes \alpha)$$

for $i = 1, 2$. We first discuss the case when $i = 1$. The restriction maps then turn out to be injective if $n$ is sufficiently large. Of course, it suffices to show this for $m = \infty$. The inflation-restriction sequence implies that

$$H^1(\Gamma_n, A) \ \cong\ \ker\big(H^1(F_\Sigma/F_n, E[p] \otimes \alpha) \longrightarrow H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big) \quad ,$$

where $A = H^0(F_\infty, E[p] \otimes \alpha)$ and $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$. We will identify $H^1(\Gamma_n, A)$ with its image in $H^1(F_\Sigma/F_n, E[p] \otimes \alpha)$. To prove the injectivity of $r^{(1)}_{\infty/n}$ for large $n$, we must show that the intersection of $H^1(\Gamma_n, A)$ with $Ш^1(F_\Sigma/F_n, E[p] \otimes \alpha)$ is trivial. For that purpose, suppose that $\pi$ is a prime of $F_\infty$ lying over $p$. Then $\pi$ is ramified in $F_\infty/F$ and totally ramified in $F_\infty/F_n$ for sufficiently large $n$. For such $n$, we can identify $\Gamma_n$ with $\Gamma_{n,\pi} = \mathrm{Gal}(F_{\infty,\pi}/F_{n,\pi})$. Thus, $H^1(\Gamma_n, A) \cong H^1(\Gamma_{n,\pi}, A)$. On the other hand, let $A_\pi = H^0(F_{\infty,\pi}, E[p] \otimes \alpha)$. Consider the composite map

$$H^1(\Gamma_n, A) \longrightarrow H^1(\Gamma_{n,\pi}, A_\pi) \longrightarrow H^1(F_{n,\pi}, E[p] \otimes \alpha) \quad ,$$

where the second map is the inflation map and is certainly injective. Now $A \subseteq A_\pi$ and $\Gamma_{n,\pi}$ acts trivially on $A_\pi$ if $n$ is sufficiently large, since $A_\pi$ is finite. The first map is then clearly injective since 1-cocycles with values in $A$ or $A_\pi$ are just homomorphisms. Thus, for large $n$, any nontrivial element of $\ker\big(H^1(F_\Sigma/F_n, E[p] \otimes \alpha) \longrightarrow H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)\big)$ is locally nontrivial at $\pi$. Hence, indeed, $r^{(1)}_{\infty/n}$ will be injective.

Now consider $i = 2$. The map $r^{(2)}_{m/n}$ can fail to be injective. In fact, if one assumes that $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$ is finite, then one can deduce that $r^{(2)}_{m/n}$ is the zero-map for $m > n >> 0$, which gives an alternative proof of the equivalence of that assumption to the vanishing of $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$. It is possible for $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$ to be finite, but nontrivial. Then, for $m >> n >> 0$, $H^2(F_\Sigma/F_n, E[p] \otimes \alpha)$ will be nontrivial and will coincide with $\ker\big(r^{(2)}_{m/n}\big)$.

The argument is as follows. The assumption that $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \check{\alpha})$ is finite and the injectivity of the restriction maps (which we now denote by $\check{r}^{(1)}_{m/n}$) implies that the order of $Ш^1(F_\Sigma/F_n, E[p] \otimes \check{\alpha})$ stabilizes and $\check{r}^{(1)}_{m/n}$ is an isomorphism if $m > n >> 0$. Consider the corestriction map

$$\check{c}^{(1)}_{m/n} : \ Ш^1(F_\Sigma/F_m, E[p] \otimes \check{\alpha}) \longrightarrow Ш^1(F_\Sigma/F_n, E[p] \otimes \check{\alpha}) \quad .$$

Since $\check{c}^{(1)}_{m/n} \circ \check{r}^{(1)}_{m/n}$ is simply multiplication by $p^{m-n}$, it follows that, for $n$ sufficiently large and $m > n$, the map $\check{c}^{(1)}_{m/n}$ will be the zero-map. Under the Poitou-Tate pairing, $r^{(2)}_{m/n}$ and $\check{c}^{(1)}_{m/n}$ are adjoints of each other. It follows therefore that $r^{(2)}_{m/n}$ is indeed the zero-map if $n$ is large enough and $m > n$. $\Diamond$

The group $Ш^1(F_\Sigma/K_\infty, E[p^\infty])$ occurring in the next proposition is the group of locally trivial 1-cocycle classes for the Galois module $E[p^\infty]$. It is a $\Lambda$-submodule of $\mathrm{Sel}_E(K_\infty)_p$, called the *"fine Selmer group"* in [CS05], where it is denoted by $R(E/K_\infty)$. Coates and

Sujatha conjecture that the $\mu$-invariant for this $\Lambda$-module (or its Pontryagin dual) is zero, which means precisely that $Ш^1(F_\Sigma/K_\infty, E[p^\infty])[p]$ is finite. This does seem like a reasonable conjecture, and so the statements *(i), (ii), (iii)* in the following proposition are likely to hold in general. See also remark 4.1.7. Statement *(iv)* is also likely to hold if $p$ is odd. For $p = 2$, one certainly needs the hypothesis that $E(F_v)$ is connected for all real primes $v$ of $F$, as discussed at the end of part **A**.

**Proposition 4.1.6.** *The following statements are equivalent:*

*(i)* $Ш^1(F_\Sigma/K_\infty, E[p^\infty])[p]$ *is finite,*

*(ii)* $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ *is finite for all* $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$,

*(iii)* $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \tau)$ *is finite for all* $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$,

*(iv)* $H^2(F_\Sigma/K_\infty, E[p]) = 0$.

*Proof.* In comparing the various cohomology groups over $F_\infty$ and over $K_\infty$, the kernels of the global and local restriction maps are involved. The Galois module might be of the form $A = E[p] \otimes \alpha$, where $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$, and so will be finite. The kernels will be of the form $H^1(\Delta, A)$ or $H^1(\Delta_v, A)$ for $v \in \Sigma$. These groups are all clearly finite. To show that *(i)* implies *(ii)*, first note that $G_{K_\infty}$ acts trivially on $\alpha$ and hence

$$E[p] \otimes \alpha \;\cong\; E[p]^{n(\alpha)[\mathfrak{f}:\mathbf{F}_p]}$$

as a Galois module over $K_\infty$. Thus, assuming that $n(\alpha) > 0$, $Ш^1(F_\Sigma/K_\infty, E[p] \otimes \alpha)$ is finite if and only if $Ш^1(F_\Sigma/K_\infty, E[p])$ is finite . Therefore, if we assume that $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ is infinite for some $\alpha \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$, then $Ш^1(F_\Sigma/K_\infty, E[p])$ would be infinite too. The map

$$H^1(F_\Sigma/K_\infty, E[p]) \longrightarrow H^1(F_\Sigma/K_\infty, E[p^\infty])[p] \tag{4.1.c}$$

has a finite kernel. Hence, the same is true for the kernel of the natural map

$$Ш^1(F_\Sigma/K_\infty, E[p]) \longrightarrow Ш^1(F_\Sigma/K_\infty, E[p^\infty])[p] \quad , \tag{4.1.d}$$

and so the latter group would also be infinite. This proves that *(i)* implies *(ii)*.

The fact that *(ii)* implies *(iii)* is obvious. Now we prove *(i)*, assuming *(iii)*. The map (4.1.c) is surjective. To prove that the cokernel of the map (4.1.d) is finite, it is sufficient to note that, for each $v \in \Sigma$, the local map

$$H^1(K_{\infty,v}, E[p]) \longrightarrow H^1(K_{\infty,v}, E[p^\infty])[p]$$

has a finite kernel. This is easy to verify. Thus, to prove *(i)*, it suffices to show that $Ш^1(F_\Sigma/K_\infty, E[p])$ is finite.

Suppose that Ш is any representation space for $\Delta$ over $\mathfrak{f}$, possibly of infinite dimension. However, assume that $(Ш \otimes \tau)^{\Delta}$ is finite for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Thus, for each such $\tau$, there is a maximal integer $m(\check{\tau})$ such that Ш contains a $\Delta$-invariant subspace isomorphic to $U_{\check{\tau}}^{m(\check{\tau})}$. We will let $\mathcal{U}$ denote the sum over all $\tau$'s of those subspaces. Thus, $\mathcal{U}$ is a $\Delta$-invariant subspace of Ш which has finite dimension over $\mathfrak{f}$, $\mathcal{U}$ is semisimple as a representation space for $\Delta$, and $\mathcal{U}$ is the maximum such subspace of Ш. Let $u$ denote the $\mathfrak{f}$-dimension of $\mathcal{U}$. Now suppose that $\mathcal{V}$ is any $\Delta$-invariant, finite-dimensional subspace of Ш containing $\mathcal{U}$. We will view these spaces, and their duals, as modules over the finite ring $R = \mathfrak{f}[\Delta]$. Let $I$ denote the Jacobson radical of that ring. The dual space $\check{\mathcal{U}}$ is then a quotient space of $\check{\mathcal{V}}$, namely the maximal semisimple quotient as an $R$-module. That is, $\check{\mathcal{V}}/I\check{\mathcal{V}} \cong \check{\mathcal{U}}$. Therefore, we can get a set of generators of $\check{\mathcal{V}}$ by choosing lifts of the elements in an $\mathfrak{f}$-basis of $\check{\mathcal{U}}$. Hence, $\check{\mathcal{V}}$ has $u$ generators as an $R$-module and so $\dim_{\mathfrak{f}}(\mathcal{V}) = \dim_{\mathfrak{f}}(\check{\mathcal{V}})$ is bounded by $u|\Delta|$. However, Ш is the union of all its finite-dimensional, $\Delta$-invariant subspaces $\mathcal{V}$, and therefore it follows that Ш is finite-dimensional.

It is clear that $Ш^1(F_\Sigma/K_\infty, E[p]) \otimes \tau = Ш^1(F_\Sigma/K_\infty, E[p] \otimes \tau)$ since $G_{K_\infty}$ acts trivially on $U_\tau$. Therefore, it is now sufficient to show that $\big(Ш^1(F_\Sigma/K_\infty, E[p] \otimes \tau)\big)^{\Delta}$ is finite for every $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Consider the restriction map

$$Ш^1(F_\Sigma/F_\infty, E[p] \otimes \tau) \longrightarrow Ш^1(F_\Sigma/K_\infty, E[p] \otimes \tau)^{\Delta} \quad . \tag{4.1.e}$$

The groups $Ш^1(F_\Sigma/F_\infty, E[p] \otimes \tau)$ are assumed to be finite for all $\tau$'s, and so we must just show that the cokernel of the (4.1.e) is finite too. For each such $\tau$, we have an exact sequence

$$H^1(F_\Sigma/F_\infty, E[p] \otimes \tau) \longrightarrow H^1(F_\Sigma/K_\infty, E[p] \otimes \tau)^{\Delta} \longrightarrow H^2\big(\Delta, (E[p] \otimes \tau)^{\Delta}\big)$$

which is part of the inflation-restriction sequence. The last group is certainly finite and hence so is the cokernel of the first map. However, our initial remarks then imply the finiteness of the cokernel of the map (4.1.e). Thus, we have proved that *(iii)* implies *(i)*.

Finally, if we apply proposition 4.1.4 to $F_\infty = K_\infty$, then we see that $H^2(F_\Sigma/K_\infty, E[p]) = 0$ is equivalent to the finiteness of $Ш^1(F_\Sigma/K_\infty, E[p])$. In the course of the above proof, it was shown that this finiteness is equivalent to *(i)* and so to all three statements. □

**Remark 4.1.7.** Let $L_\infty$ denote the maximal, abelian pro-$p$ extension of $K_\infty$ such that all primes of $K_\infty$ are unramified. Then $X = \mathrm{Gal}(L_\infty/K_\infty)$ is a $\Lambda$-module, one of the main objects of study in classical Iwasawa theory. It is a finitely generated, torsion $\Lambda$-module. A well-known conjecture of Iwasawa asserts that $\mu(X) = 0$. This is known to be true if $K$ is a finite, abelian extension of $\mathbf{Q}$, a theorem of Ferrero and Washington [FeWa], but is open in general. Note that all primes $v$ of $K_\infty$ not lying over $p$ split completely in $L_\infty/K_\infty$. Let $L'_\infty$ denote the maximal subfield of $L_\infty$ in which the primes above $p$ split completely and let

$X' = \mathrm{Gal}(L_\infty/K_\infty)$, which is also a $\Lambda$-module. Those two modules can differ; the restriction map $X \to X'$ is surjective and its kernel is finitely generated over $\mathbf{Z}_p$. Hence $\mu(X') = \mu(X)$.

As pointed out at the end of the proof, the statements considered in proposition 4.1.6 are equivalent to the statement that $Ш^1(F_\Sigma/K_\infty, E[p])$ is finite. If we choose $K$ so that $F(E[p]) \subseteq K$, then $H^1(F_\Sigma/K_\infty, E[p]) = \mathrm{Hom}(\mathrm{Gal}(F_\Sigma/K_\infty, E[p])$. It then follows that $Ш^1(F_\Sigma/K_\infty, E[p]) = \mathrm{Hom}(X', E[p])$. The finiteness of that group is equivalent to the vanishing of $\mu(X')$, and hence to Iwasawa's conjecture for $K_\infty$. Thus, if Iwasawa's conjecture is true for all ground fields $K$, then the statements in proposition 4.1.6 are also valid. Essentially the same point is made in [CS05], corollary 3.5. $\Diamond$

If $p = 2$ and $E(F_v)$ is connected for all archimedean primes $v$ of $F$, then proposition 4.1.4 and 4.1.6 are valid as stated. That assumption implies that $E[2]$ is a projective $\mathbf{F}_2[G_{F_v}]$-module, and hence so is $E[2] \otimes \alpha$. It then follows that $H^i(F_{\infty,v}, E[p] \otimes \alpha) = 0$ for all $i \geq 1$. However, for greater generality, one can simply replace $H^2(F_\Sigma/K_\infty, E[p])$ and $H^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$ by $Ш^2(F_\Sigma/K_\infty, E[p])$ and $Ш^2(F_\Sigma/F_\infty, E[p] \otimes \alpha)$, respectively, in those propositions. The difference comes entirely from the local conditions at the archimedean primes.

**D.** *The local cohomology groups.* We first discuss the coranks of the local cohomology groups of interest in this chapter as modules over the group ring $\mathfrak{f}[[\Gamma]]$. For a nonarchimedean prime $v$ of $F$, and any $\alpha \in \mathrm{Rep}_\mathfrak{f}(\Delta)$, we will use the notation $\mathcal{H}_v(F_\infty, E[p] \otimes \alpha)$ to represent

$$\prod_{\nu|v} H^1(F_{\infty,\nu}, E[p] \otimes \alpha) \qquad or \qquad \prod_{\nu|v} H^1(F_{\infty,\nu}, \overline{E}_v[p] \otimes \alpha) \ ,$$

the first if $v \nmid p$, the second if $v|p$. Note that these products are finite. They are the groups that occur in the definition of the Selmer groups for $E[p] \otimes \alpha$. The result about coranks is more definitive then in the global case. We have

**Proposition 4.1.8.** *Suppose that $\alpha \in \mathrm{Rep}_\mathfrak{f}(\Delta)$ and that $v$ is a nonarchimedean prime of $F$. If $v|p$, we have*

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(\mathcal{H}_v(F_\infty, E[p] \otimes \alpha)\big) \ = \ [F_v : \mathbf{Q}_p] n(\alpha) \quad .$$

*If $v \nmid p$, then $\mathcal{H}_v(F_\infty, E[p] \otimes \alpha)$ is finite and hence has $\mathfrak{f}[[\Gamma]]$-corank zero.*

*Proof.* There are only finitely many primes of $F_\infty$ lying above a given nonarchimedean prime $v$ of $F$. Let $F_{n,v}$ and $F_{\infty,v}$ denote the completions of $F_n$ and $F_\infty$ at any one of the primes above $v$. Let $\Gamma_{n,v} = \mathrm{Gal}(F_{\infty,v}/F_{n,v})$. The group $\Gamma_v = \Gamma_{0,v}$ can be identified with the

decomposition subgroup of $\Gamma$ for any of the primes lying above $v$. The index $g_v = [\Gamma : \Gamma_v]$ is the number of primes of $F_\infty$ lying above $v$.

The proof is easy if $v \nmid p$. It suffices to point out that $H^1(F_{n,v}, E[p] \otimes \alpha)$ has bounded order as $n$ varies. The Euler-Poincaré characteristic of the Galois module $E[p] \otimes \alpha$ is zero. That is, we have

$$\sum_{i=0}^{2} (-1)^i \dim_{\mathfrak{f}}\big(H^i(F_{n,v}, E[p] \otimes \alpha)\big) \;=\; 0 \quad .$$

Obviously, the order of $H^0(F_{n,v}, E[p] \otimes \alpha)$ is bounded by that of $H^0(F_{\infty,v}, E[p] \otimes \alpha)$, which is finite, and so the $\mathfrak{f}$-dimension of $H^0(F_{n,v}, E[p] \otimes \alpha)$ stabilizes for sufficiently large $n$. Now, by local Tate duality, $H^2(F_{n,v}, E[p] \otimes \alpha)$ is the Pontryagin dual of $H^0(F_{n,v}, E[p] \otimes \check{\alpha})$ and so its order and $\mathfrak{f}$-dimension also stabilize. Thus, indeed, the $\mathfrak{f}$-dimension of $H^1(F_{n,v}, E[p] \otimes \alpha)$ stabilizes. To get a precise result about $H^1(F_{\infty,v}, E[p] \otimes \alpha)$, we use the inflation-restriction sequence. Let $A_v = H^0(F_{\infty,v}, E[p] \otimes \alpha)$. Then we have an exact sequence

$$0 \;\longrightarrow\; H^1(\Gamma_{n,v}, A_v) \;\longrightarrow\; H^1(F_{n,v}, E[p] \otimes \alpha) \;\longrightarrow\; H^1(F_{\infty,v}, E[p] \otimes \alpha)^{\Gamma_{n,v}} \;\longrightarrow\; 0 \quad .$$

If $n$ is large enough, then $\Gamma_{n,v}$ acts trivially on $A_v$ and also on $H^1(F_{\infty,v}, E[p] \otimes \alpha)$. We then have $|H^1(\Gamma_{n,v}, A_v)| = |A_v|$. Consequently,

$$\dim_{\mathfrak{f}}\big(\mathcal{H}_v(F_\infty, E[p] \otimes \alpha)\big) \;=\; g_v \dim_{\mathfrak{f}}\big(H^0(F_{\infty,v}, E[p] \otimes \check{\alpha})\big) \tag{4.1.f}$$

for any nonarchimedean $v$ not lying over $p$.

Now suppose $v|p$. With the same notation as above, the relevant Euler-Poincaré characteristic is now

$$\sum_{i=0}^{2} (-1)^i \dim_{\mathfrak{f}}\big(H^i(F_{n,v}, \overline{E}_v[p] \otimes \alpha)\big) \;=\; -\,[F_{n,v} : \mathbf{Q}_p] n(\alpha)$$

since $\overline{E}_v[p]$ has $\mathbf{F}_p$-dimension 1. The order of $H^0(F_{n,v}, \overline{E}[p] \otimes \alpha)$ stabilizes as $n$ varies. So does the order of $H^2(F_{n,v}, \overline{E}_v[p] \otimes \alpha)$ since that group is again isomorphic to the Pontryagin dual of $H^0(F_{n,v}, \overline{E}_v[p] \otimes \check{\alpha})$. Also, just as above, the order of the kernel of the restriction map stabilizes. Thus, we have

$$\dim_{\mathfrak{f}}\big(H^1(F_{\infty,v}, \overline{E}_v[p] \otimes \alpha)^{\Gamma_{n,v}}\big) \;=\; [F_{n,v} : \mathbf{Q}_p] n(\alpha) \;+\; O(1)$$

as $n \to \infty$. Suppose that $g_v = p^{n_0}$. Then $F_{n_0,v} = F_v$ and $\Gamma_v = \Gamma_{n_0,v}$. Also, we have $[F_{n,v} : F_v] = [\Gamma_v : \Gamma_{n,v}]$ for $n \geq n_0$. It follows that

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma_v]]}\big(H^1(F_{\infty,v}, \overline{E}_v[p] \otimes \alpha)\big) \;=\; [F_v : \mathbf{Q}_p] n(\alpha)$$

Therefore, the $\mathfrak{f}[[\Gamma_v]]$-corank of $\mathcal{H}_v(F_\infty, E[p]\otimes\alpha)$ is equal to $g_v[F_v:\mathbf{Q}_p]n(\alpha)$. Since $[\Gamma:\Gamma_v] = g_v$, it follows that the $\mathfrak{f}[[\Gamma]]$-corank of $\mathcal{H}_v(F_\infty, E[p]\otimes\alpha)$ is $[F_v:\mathbf{Q}_p]n(\alpha)$. $\square$

Assume that $v\in\Sigma_p$. As defined in the introduction, $v$ is anomalous for $E/K$ if and only if $H^0(K_w, \overline{E}_v[p]) \neq 0$, where $w$ is a prime of $K$ lying above $v$. The argument in the proof of proposition 4.1.3 applies to this group with little change. Thus, we have the following result:

**Proposition 4.1.9.** *The following statements are equivalent:*

*(i)* $H^0(K_w, \overline{E}_v[p]) = 0$.
*(ii)* $H^0(F_v, \overline{E}_v[p]\otimes\alpha) = 0$ *for all* $\alpha\in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$,
*(iii)* $H^0(F_v, \overline{E}_v[p]\otimes\tau) = 0$ *for all* $\tau\in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

Proposition 4.1.8 is valid as stated for $p=2$. Proposition 4.1.9 is vacuously true for $p=2$; the three statements there are never satisfied. Archimedean primes split completely in $F_\infty/F$. For such a prime $v$, one defines $\mathcal{H}_v(F_\infty, E[p]\otimes\alpha)$ as a direct limit over the $F_n$'s, just as in section 3.1, part **A**. One then proves the following result:

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(\mathcal{H}_v(F_\infty, E[p]\otimes\alpha)\big) \;=\; \dim_{\mathfrak{f}}\big(H^1(F_v, E[p]\otimes\alpha)\big) \quad .$$

One sees easily that for any nonzero $\alpha$, $H^1(F_v, E[p]\otimes\alpha) = 0$ if $E(F_v)$ is connected, and is nonzero otherwise.

## 4.2 Selmer groups for $E[p]\otimes\alpha$.

**A.** *Definition and equivalences for finiteness.* The definition of $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty)$ was given at the beginning of section 1.4 for the base field $F_\infty$. However, for proving the next two propositions, it will be helpful to have an alternative description of the local cohomology groups occurring in the definition. If $F'$ is any finite extension of $F$ contained in $F_\Sigma$, consider the localization map:

$$H^1(F_\Sigma/F', E[p]\otimes\alpha) \;\xrightarrow{loc}\; P^1_\Sigma(F', E[p]\otimes\alpha) \quad ,$$

where

$$P^1_\Sigma(F', E[p]\otimes\alpha) \;=\; \prod_{v\in\Sigma}\Big(\prod_{v'|v} H^1(F'_{v'}, E[p]\otimes\alpha)\Big) \quad .$$

Here $v'$ runs over all the primes of $F'$ lying above a prime $v$ which, in turn, varies over the primes in $\Sigma$. For each such $v'$, let $I_{v'}$ denote the inertia subgroup of $G_{F'_{v'}}$. We define $L^1(F'_{v'}, E[p] \otimes \alpha)$ to be the kernel of one of the following maps

$$H^1(F'_{v'}, E[p] \otimes \alpha) \longrightarrow H^1(I_{v'}, E[p] \otimes \alpha) \qquad or \qquad H^1(F'_{v'}, E[p] \otimes \alpha) \longrightarrow H^1(F'_{v'}, \overline{E}[p] \otimes \alpha) \ ,$$

the first if $v \nmid p$, the second if $v|p$. Thus, $L^1(F'_{v'}, E[p] \otimes \alpha)$ is a subgroup of $H^1(F'_{v'}, E[p] \otimes \alpha)$. We then define $\mathrm{Sel}_{E[p]\otimes\alpha}(F')$ as the kernel of the composite map

$$H^1(F_\Sigma/F', E[p] \otimes \alpha) \stackrel{loc_{F'}}{\longrightarrow} P^1_\Sigma(F', E[p] \otimes \alpha) \stackrel{red_{F'}}{\longrightarrow} P^1_\Sigma(F', E[p] \otimes \alpha)\big/L^1_\Sigma(F', E[p] \otimes \alpha)$$

where we have put

$$L^1_\Sigma(F', E[p] \otimes \alpha) \ = \ \prod_{v\in\Sigma} \left( \prod_{v'|v} L^1(F'_{v'}, E[p] \otimes \alpha) \right) \ .$$

Thus, $\mathrm{Sel}_{E[p]\otimes\alpha}(F') = \ker(red_{F'} \circ loc_{F'})$. Note that the contribution to $P^1_\Sigma(F', E[p] \otimes \alpha)$ and $L^1_\Sigma(F', E[p] \otimes \alpha)$ coming from archimedean primes is trivial since $p$ is odd. Thus, there is no local condition in the definition of the Selmer group for those primes.

Suppose that $F'$ and $F''$ are finite extensions of $F$ such that $F' \subset F'' \subset F_\Sigma$. Then one has a natural map (the restriction map) from $\mathrm{Sel}_{E[p]\otimes\alpha}(F')$ to $\mathrm{Sel}_{E[p]\otimes\alpha}(F'')$. For an infinite extension of $F$ contained in $F_\Sigma$, one defines the corresponding Selmer group for $E[p] \otimes \alpha$ to be just the direct limit of the Selmer groups for $E[p] \otimes \alpha$ over all the subfields of finite degree over $F$. In particular, if $F_\infty = \cup_n F_n$ is the cyclotomic $\mathbf{Z}_p$-extension of $F$, then

$$\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty) \ = \ \ker\left( H^1(F_\Sigma/F_\infty, E[p] \otimes \alpha) \longrightarrow P^1_\Sigma(F_\infty, E[p] \otimes \alpha)\big/L^1_\Sigma(F_\infty, E[p] \otimes \alpha) \right) \ ,$$

where $P^1_\Sigma(F_\infty, E[p] \otimes \alpha)$ and $L^1_\Sigma(F_\infty, E[p] \otimes \alpha)$ are defined in the same way as above. One can also define these $\mathfrak{f}[[\Gamma]]$-modules as direct limits

$$P^1_\Sigma(F_\infty, E[p] \otimes \alpha) = \varinjlim_n P^1_\Sigma(F_n, E[p] \otimes \alpha), \qquad L^1_\Sigma(F_\infty, E[p] \otimes \alpha) = \varinjlim_n L^1_\Sigma(F_n, E[p] \otimes \alpha) \ .$$

The map whose kernel is $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ will be denoted by $red_\infty \circ loc_\infty$, with the obvious meaning for $red_\infty$ and $loc_\infty$. The corresponding maps at the $n$-th level will be denoted by $red_n$ and $loc_n$. Results from section 4.1 imply that

$$\text{(4.2.a)} \qquad \mathrm{corank}_{\mathfrak{f}[[\Gamma]]} \left( P^1_\Sigma(F_\infty, E[p] \otimes \alpha) \Big/ L^1_\Sigma(F_\infty, E[p] \otimes \alpha) \right) \ = \ [F : \mathbf{Q}] n(\alpha) \ .$$

To see this, note that for $v|p$, the map $H^1(F_{\infty,v}, E[p]\otimes\alpha) \longrightarrow H^1(F_{\infty,v}, \overline{E}[p]\otimes\alpha)$ is surjective and hence

$$H^1(F_{\infty,v}, E[p]\otimes\alpha)/L^1(F_{\infty,v}, E[p]\otimes\alpha) \;\cong\; H^1(F_{\infty,v}, \overline{E}[p]\otimes\alpha) \quad .$$

The contribution to $P^1_\Sigma(F_\infty, E[p]\otimes\alpha)/L^1_\Sigma(F_\infty, E[p]\otimes\alpha)$ coming from primes $v$ not lying over $p$ will be finite and hence of $\mathfrak{f}[[\Gamma]]$-corank 0. Although we don't need it right now, we remark that for any $v \in \Sigma$ not dividing $p$ and for any prime $\nu$ of $F_\infty$ lying above such a $v$, we have $L_1(F_{\infty,\nu}, E[p]\otimes\alpha) = 0$. This is true because $G_{F_{\infty,\nu}}/I_\nu$ has profinite order prime to $p$. Thus, the corresponding factor in $P^1_\Sigma(F_\infty, E[p]\otimes\alpha)/L^1_\Sigma(F_\infty, E[p]\otimes\alpha)$ is simply $H_1(F_{\infty,\nu}, E[p]\otimes\alpha)$. The $\mathfrak{f}$-dimension of the contribution from all $\nu|v$ is given by (4.1.f).

On the other hand, corollary 4.1.2 states that $H^1(F_\Sigma/F_\infty, E[p]\otimes\alpha)$ has $\mathfrak{f}[[\Gamma]]$-corank bounded below by $[F:\mathbf{Q}]n(\alpha)$, with equality if and only if $H^2(F_\Sigma/F_\infty, E[p]\otimes\alpha) = 0$. Using this fact in conjunction with (4.2.a) and the definition of the Selmer group, we have the following proposition.

**Proposition 4.2.1.** *The following statements are equivalent:*

*(i)* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ *is finite.*

*(ii)* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_n)$ *has bounded order as* $n \to \infty$.

*(iii)* $H^2(F_\Sigma/F_\infty, E[p]\otimes\alpha) = 0$ *and the cokernel of the map* $red_\infty \circ loc_\infty$ *is finite.*

*(iv)* $Ш^1(F_\Sigma/F_\infty, E[p]\otimes\check{\alpha})$ *is finite and the cokernel of the map* $red_n \circ loc_n$ *is finite and has bounded order as* $n \to \infty$.

If $\Sigma_0$ is a subset of $\Sigma$ which contains only nonarchimedean primes not lying above $p$, then we will also consider the nonprimitive Selmer groups $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_n)$ and $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty)$ obtained by omitting the local conditions at all primes lying above $v \in \Sigma_0$. We will next prove that, under certain mild hypotheses, $\mathrm{coker}(red_\infty \circ loc_\infty)$ is trivial. This will have an immediate consequence concerning the $\mathfrak{f}$-dimension of $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty)/\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$.

**B.** *Surjectivity of the global-to-local map.* We prove the following result:

**Proposition 4.2.2.** *Assume that* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ *is finite and that* $H^0(F, E[p]\otimes\check{\alpha}) = 0$. *Then the map*

$$H^1(F_\Sigma/F_\infty, E[p]\otimes\alpha) \longrightarrow P^1_\Sigma(F_\infty, E[p]\otimes\alpha)/L^1_\Sigma(F_\infty, E[p]\otimes\alpha)$$

*is surjective.*

*Proof.* We will use the following abbreviated notation in this proof. The Selmer groups and other groups associated with $E[p]\otimes\alpha$ for the field $F_n$ and the fixed set $\Sigma$ will be denoted

by $S_{n,\alpha}$, $H^1_{n,\alpha}$, $H^2_{n,\alpha}$, $Ш^1_{n,\alpha}$, $Ш^2_{n,\alpha}$, $P^1_{n,\alpha}$, and $L^1_{n,\alpha}$. Also, we let $G_{n,\alpha}$ denote the image of the map $loc_n : H^1_{n,\alpha} \longrightarrow P^1_{n,\alpha}$. The corresponding groups over $F_\infty$ will just have a subscript $\infty, \alpha$. We will use a similar notation for the groups associated to $E[p] \otimes \check{\alpha}$.

By proposition 4.2.1, we know that $Ш^1_{n,\check{\alpha}}$ has bounded order as $n \to \infty$. The cokernel of $red_n \circ loc_n$ is isomorphic to $P^1_{n,\alpha}/G^1_{n,\alpha}L^1_{n,\alpha}$. We also know that this group will be finite and of bounded order as $n$ varies. Now, according to the Poitou-Tate duality theorems, there is a perfect pairing

$$P^1_{n,\alpha} \times P^1_{n,\check{\alpha}} \longrightarrow \mathbf{F}_p$$

for each $n \geq 0$. Also, the orthogonal complements of $L^1_{n,\alpha}$ and $G^1_{n,\alpha}$ are $L^1_{n,\check{\alpha}}$ and $G^1_{n,\check{\alpha}}$, respectively. The Pontryagin dual of $P^1_{n,\alpha}/G^1_{n,\alpha}L^1_{n,\alpha}$ is isomorphic to $G^1_{n,\check{\alpha}} \cap L^1_{n,\check{\alpha}}$, which therefore has bounded order as $n \to \infty$.

Surjectivity of the global-to-local map means that $P^1_{\infty,\alpha}/G^1_{\infty,\alpha}L^1_{\infty,\alpha} = 0$. It suffices to show that $\varinjlim_n P^1_{n,\alpha}/G^1_{n,\alpha}L^1_{n,\alpha}$ is trivial. Now that direct limit is defined by the natural local restriction maps as $n$ varies. Equivalently, we must show that the inverse limit $\varprojlim_n G^1_{n,\check{\alpha}} \cap L^1_{n,\check{\alpha}}$ defined by the corestriction maps is trivial. We will use the isomorphism

$$G^1_{n,\check{\alpha}} \cap L^1_{n,\check{\alpha}} \cong S_{n,\check{\alpha}}/Ш^1_{n,\check{\alpha}}$$

which follows from the definition of $S_{n,\check{\alpha}}$. We have already pointed out that $Ш^1_{n,\check{\alpha}}$ has bounded order. But $S_{n,\check{\alpha}}/Ш^1_{n,\check{\alpha}}$ also has bounded order and hence so does $S_{n,\check{\alpha}}$.

We are assuming that $H^0(F, E[p] \otimes \check{\alpha}) = 0$. The inflation-restriction sequence then implies that the restriction maps $r\check{e}s_{m/n} : S_{n,\check{\alpha}} \longrightarrow S_{m,\check{\alpha}}$ for $m > n \geq 0$ are injective. It follows that these maps are isomorphisms if $n$ is sufficiently large. Hence so are the restriction maps $Ш^1_{n,\check{\alpha}} \longrightarrow Ш^1_{m,\check{\alpha}}$. Therefore, the induced maps on the quotients $S_{n,\check{\alpha}}/Ш^1_{n,\check{\alpha}} \longrightarrow S_{m,\check{\alpha}}/Ш^1_{m,\check{\alpha}}$ will also be isomorphisms if $n$ is large enough. For the associated corestriction maps $c\check{o}r_{m/n}$, the map $c\check{o}r_{m/n} \circ r\check{e}s_{m/n}$ is multiplication by $p^{m-n}$. Hence the maps $S_{m,\check{\alpha}}/Ш^1_{m,\check{\alpha}} \longrightarrow S_{n,\check{\alpha}}/Ш^1_{n,\check{\alpha}}$ induced by $c\check{o}r_{m/n}$ will be the zero map if $m > n >> 0$. This proves that the inverse limit of the groups $G^1_{n,\check{\alpha}} \cap L^1_{n,\check{\alpha}}$ is zero and hence the same is true for the direct limit of the groups $P^1_{n,\alpha}/G^1_{n,\alpha}L^1_{n,\alpha}$, as we needed to prove. □

The following result follows immediately from the above proposition and (4.1.f).

**Corollary 4.2.3.** *Assume that* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ *is finite and that* $H^0(F, E[p]\otimes\check{\alpha}) = 0$. *Suppose that* $\Sigma_o$ *is a finite subset of* $\Sigma$ *which contains no primes lying above* $p$ *or* $\infty$. *Then*

$$\mathrm{Sel}^{\Sigma_o}_{E[p]\otimes\alpha}(F_\infty)/\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty) \cong \prod_{v\in\Sigma_o} \mathcal{H}_v(F_\infty, E[p]\otimes\alpha) \quad .$$

*Therefore,*

$$\dim_{\mathfrak{f}}\Big(\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty)/\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)\Big) \;=\; \sum_{v\in\Sigma_0} g_v \dim_{\mathfrak{f}}\big(H^0(F_{\infty,v}, E[p]\otimes\check{\alpha})\big)\ .$$

**Remark 4.2.4.** The proof of proposition 4.2.2 includes the following assertion:

*If* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ *is finite, then so is* $\mathrm{Sel}_{E[p]\otimes\check{\alpha}}(F_\infty)$.

We also remark that the finiteness of $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ and of $\mathrm{Sel}^{\Sigma_0}_{E[p]\otimes\alpha}(F_\infty)$ are equivalent. $\Diamond$

**C.** *Finiteness of* $\mathrm{Sel}_E(K_\infty)[p]$. The following result is the analogue of proposition 4.1.6 for $\mathrm{Sel}_E(K_\infty)_p$. However, as we discuss in section 4.5, there are situations where the statements fail to be true.

**Proposition 4.2.5.** *The following statements are equivalent:*

*(i)* $\mathrm{Sel}_E(K_\infty)[p]$ *is finite,*

*(ii)* $\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty)$ *is finite for all* $\alpha\in\mathrm{Rep}_{\mathfrak{f}}(\Delta)$,

*(iii)* $\mathrm{Sel}_{E[p]\otimes\tau}(F_\infty)$ *is finite for all* $\tau\in\mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

*Proof.* The proof is similar to that for proposition 4.1.6. We just sketch the steps. First of all, the restriction map

$$\mathrm{Sel}_{E[p]\otimes\alpha}(F_\infty) \;\longrightarrow\; \mathrm{Sel}_{E[p]\otimes\alpha}(K_\infty)^\Delta \tag{4.2.b}$$

has finite kernel. Also, $\mathrm{Sel}_{E[p]\otimes\alpha}(K_\infty)\cong\mathrm{Sel}_{E[p]}(K_\infty)^{n(\alpha)[\mathfrak{f}:\mathbf{F}_p]}$. Here $\mathrm{Sel}_{E[p]}(K_\infty)$ is defined exactly as previously, just taking $F_\infty=K_\infty$ and tensoring by the trivial representation. The map (4.1.c) has finite kernel and hence so does the map

$$\mathrm{Sel}_{E[p]}(K_\infty) \;\longrightarrow\; \mathrm{Sel}_E(K_\infty)[p]\ . \tag{4.2.c}$$

It follows that *(i)* implies *(ii)*. Clearly, *(ii)* implies *(iii)*.

The cokernel of the map (4.2.b) is finite. Just as in the proof of proposition 4.1.6, it is a matter of showing that the local restriction maps for $v\in\Sigma$ have finite kernels. One must check this also for $v|p$, where the relevant kernel is $H^1(\Delta_v,\overline{E}_v[p]\otimes\alpha)$, and that is clearly finite. Assume that *(iii)* is true. It then follows that $\big(\mathrm{Sel}_{E[p]}(K_\infty)\otimes\tau\big)^\Delta$ is finite for all $\tau\in\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Consequently, as in the earlier proof, $\mathrm{Sel}_{E[p]}(K_\infty)$ is finite-dimensional over $\mathfrak{f}$.

To deduce *(i)*, assuming *(iii)*, it suffices now to show that the map (4.2.c) has finite cokernel. But this follows just as before. The only additional ingredient is the fact that, for all $v|p$, the map $H^1(K_{\infty,v},\overline{E}_v[p])\longrightarrow H^1(K_{\infty,v},\overline{E}_v)[p^\infty])$, which is induced by the inclusion map $\overline{E}_v[p]\longrightarrow\overline{E}_v[p^\infty]$, has finite kernel. $\square$

## 4.3 Justification of (1.4.b) and (1.4.c).

**A.** *The corank of* $\mathrm{Sel}^{\Sigma_o}_{E[p^\infty]\otimes\sigma}(F_\infty)$. We take $\Sigma_0$ to be any subset of $\Sigma$ not containing primes above $p$ or $\infty$. First of all, $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)$ is a subgroup of $H^1(F_\Sigma/F_\infty, E[p^\infty]\otimes\sigma)$. Here, as in the introduction, $L_\sigma$ is a $\Delta$-invariant $\mathcal{O}$-lattice in the underlying representation space $W_\sigma$ for $\sigma$ and $E[p^\infty]\otimes\sigma = E[p^\infty]\otimes L_\sigma$ by definition. This tensor product is over $\mathbf{Z}_p$ and the resulting group is an $\mathcal{O}$-module on which $\mathrm{Gal}(F_\Sigma/F)$ acts $\mathcal{O}$-linearly. We will denote various other tensor products with $L_\sigma$ similarly in the following discussion. The local conditions defining $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)$ are that a cocycle class have trivial image in $H^1(F_{\infty,v}, E[p^\infty]\otimes\sigma)$ for all non-archimedean $v\in\Sigma$ which are not in $\Sigma_p\cup\Sigma_0$ and in $H^1(F_{\infty,v}, \overline{E}_v[p^\infty]\otimes\sigma)$ for all $v\in\Sigma_p$. We prove the following proposition justifying the first equality in (1.4.b).

**Proposition 4.3.1.** *Suppose that* $\sigma\in\mathrm{Irr}_{\mathcal{F}}(\Delta)$ *and that* $\Sigma_o$ *is any subset of* $\Sigma$ *containing no primes of* $F$ *lying above* $p$ *or* $\infty$. *Then we have*

$$\lambda_E^{\Sigma_o}(\sigma) \;=\; \mathrm{corank}_{\mathcal{O}}\big(\mathrm{Sel}^{\Sigma_o}_{E[p^\infty]\otimes\sigma}(F_\infty)\big) \quad .$$

*Proof.* First of all, the kernel and the cokernel of the restriction map

$$H^1(F_\infty, E[p^\infty]\otimes\sigma) \;\longrightarrow\; H^1(K_\infty, E[p^\infty]\otimes\sigma)^\Delta \;\cong\; \big(H^1(K_\infty, E[p^\infty])\otimes\sigma\big)^\Delta \tag{4.3.a}$$

are finite. The isomorphism in (4.3.a) arises from the fact that $G_{K_\infty}$ acts trivially on $L_\sigma$ and the canonical isomorphism $H^1(K_\infty, E[p^\infty]\otimes\sigma) \;\cong\; H^1(K_\infty, E[p^\infty])\otimes\sigma$ is $\Delta$-equivariant. We identify the two groups.

We can define $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(K_\infty)$ just as above. It is a subgroup of $H^1(K_\infty, E[p^\infty]\otimes\sigma)$ and can be identified with $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(K_\infty)\otimes\sigma = \mathrm{Sel}_E(K_\infty)_p\otimes\sigma$. Consider the map

$$\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty) \;\longrightarrow\; \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(K_\infty)^\Delta \;=\; \big(\mathrm{Sel}^{\Sigma_0}_E(K_\infty)_p\otimes\sigma\big)^\Delta \;. \tag{4.3.b}$$

This map has finite kernel and cokernel because the kernels of the relevant local restriction maps are all finite. Thus, we have

$$\mathrm{corank}_{\mathcal{O}}\big(\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)\big) \;=\; \mathrm{corank}_{\mathcal{O}}\big((\mathrm{Sel}^{\Sigma_0}_E(K_\infty)_p\otimes\sigma)^\Delta\big) \quad .$$

To see that the last $\mathcal{O}$-corank is equal to $\lambda_E(\sigma)$, we have

$$\mathrm{Sel}^{\Sigma_0}_E(K_\infty)_p\otimes\sigma \;\cong\; \mathrm{Hom}_{\mathbf{Z}_p}(X^{\Sigma_0}_E(K_\infty),\; L_\sigma\otimes\mathbf{Q}_p/\mathbf{Z}_p) \;\cong\; \mathrm{Hom}_{\mathbf{Z}_p}(X^{\Sigma_0}_E(K_\infty),\; W_\sigma/L_\sigma) \quad .$$

The second isomorphism results from the fact that $W_\sigma/L_\sigma = \bigcup_m \left(\frac{1}{p^m}L_\sigma/L_\sigma\right)$. It follows that

$$\begin{aligned}\mathrm{corank}_{\mathcal{O}}\big((\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \otimes \sigma)^\Delta\big) &= \mathrm{rank}_{\mathbf{Z}_p}\big(\mathrm{Hom}_{\mathbf{Z}_p}(X_E^{\Sigma_0}(K_\infty),\ W_\sigma)^\Delta\big) \\ &= \dim_{\mathcal{F}}\big(\mathrm{Hom}_{\mathcal{F}}(X_E^{\Sigma_0}(K_\infty)\otimes\mathcal{F},\ W_\sigma)^\Delta\big).\end{aligned}$$

Since $\sigma$ is absolutely irreducible over $\mathcal{F}$ and $X_E^{\Sigma_0}(K_\infty)\otimes\mathcal{F}$ is a semisimple representation, the above $\mathcal{F}$-dimension is indeed equal to the multiplicity $\lambda_E(\sigma)$. □

**Remark 4.3.2.** Virtually the same proof demonstrates the following useful result about the Pontryagin dual $X_E^{\Sigma_0}(K)$ of $\mathrm{Sel}_E^{\Sigma_0}(K)_p$. Let $s_E^{\Sigma_0}(\sigma)$ denote the multiplicity of $\sigma$ in the $\Delta$-representation space $X_E^{\Sigma_0}(K)\otimes_{\mathbf{Z}_p}\mathcal{F}$ over $\mathcal{F}$. We then have

$$s_E^{\Sigma_0}(\sigma) \;=\; \mathrm{corank}_{\mathcal{O}}\big(\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F)\big)\quad,$$

where the non-primitive Selmer group over $F$ occurring here is defined in a completely analogous way as over $F_\infty$. This remark applies to $s_E(\sigma)$ by taking $\Sigma_0$ to be empty. ◊

**B.** *Divisibility of* $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$. We will prove that the Pontryagin dual of $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$ has no nontrivial, finite $\Lambda$-submodule under certain assumptions. As a consequence, if one assumes that $\mu_E(K_\infty)=0$, it would then follow that $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$ is a divisible group. In part **B** of section 3.1, we discussed a similar statement for $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$, based on results in [Gr99] and [Gr89]. Although we didn't mention it there, the assumption that $E(K)[p]=0$ is not needed if $\Sigma_0$ is non-empty. The proof is essentially the same as the proof of proposition 4.15, part *(i)*, in [Gr99] (which is found on page 104 of that paper). The arguments given for propositions 4.14 and 4.15 there are easily extended to Galois modules of the form $E[p^\infty]\otimes\sigma$. Those arguments rely on the assumption that the corresponding Selmer groups are $\Lambda$-cotorsion, and start by proving a general form of Cassels' theorem concerning the cokernel of the global-to-local maps defining Selmer groups. That is proposition 4.13 in [Gr99]. Since the arguments are so similar, we simply state the result.

**Proposition 4.3.3.** *Suppose that $\Sigma_0$ is any subset of $\Sigma$ containing no primes above $p$ or $\infty$. If $E(K)[p]=0$ and $\mathrm{Sel}_E(K_\infty)[p]$ is finite, then $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$ is a divisible group. The same conclusion is valid without the assumption that $E(K)[p]=0$ if one assumes additionally that $\Sigma_0$ is non-empty.*

Under the assumptions in proposition 4.3.3, the Pontryagin dual of $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$ will be finitely-generated as a $\mathbf{Z}_p$-module. Now $\mathrm{Sel}_{E[p^\infty]\otimes\sigma}^{\Sigma_0}(F_\infty)$ is an $\mathcal{O}$-module, and if it is divisible

as a group, then it is also divisible as an $\mathcal{O}$-module. Its Pontryagin dual will then be a free $\mathcal{O}$-module of finite rank. The rank of a free $\mathcal{O}$-module $X$ is equal to the $\mathfrak{f}$-dimension of $X/\mathfrak{m}X$. Therefore, we obtain the following corollary which gives the second equality in (1.4.b).

**Corollary 4.3.4.** *Suppose that $\Sigma_o$ is any subset of $\Sigma$ containing no primes above $p$ or $\infty$, that $\mathrm{Sel}_E(K_\infty)[p]$ is finite, and that either $E(K)[p] = 0$ or $\Sigma_o$ is non-empty. Then*

$$\mathrm{corank}_{\mathcal{O}}\big(\mathrm{Sel}^{\Sigma_o}_{E[p^\infty]\otimes\sigma}(F_\infty)\big) \;=\; \dim_{\mathfrak{f}}\big(\mathrm{Sel}^{\Sigma_o}_{E[p^\infty]\otimes\sigma}(F_\infty)[\mathfrak{m}]\big) \quad .$$

**C.** *Two isomorphisms.* We now establish the two isomorphisms stated in (1.4.c). The second isomorphism is essentially a matter of definition. Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. The inclusion $E[p] \subset E[p^\infty]$ induces a canonical isomorphism $E[p]\otimes\sigma \cong (E[p^\infty]\otimes\sigma)[p]$ as Galois modules over $\mathcal{O}$. The maximal submodules killed by $\mathfrak{m}$ will be canonically isomorphic. Thus, $E[p]\otimes\widetilde{\sigma} = (E[p]\otimes\sigma)[\mathfrak{m}]$ will be isomorphic to $(E[p^\infty]\otimes\sigma)[\mathfrak{m}]$ as representation spaces for $G_F$ over $\mathfrak{f}$.

In defining Selmer groups over $F_\infty$ for those isomorphic Galois modules, the local conditions for primes $v$ not dividing $p$ are the same. Cocycles are required to be trivial when restricted to $G_{F_{\infty,v}}$. If $v$ divides $p$, then note that the map $E[p^\infty] \to \overline{E}_v[p^\infty]$ induces (by restriction) the map $E[p] \to \overline{E}_v[p]$. It follows that the map $E[p^\infty]\otimes\sigma \to \overline{E}_v[p^\infty]\otimes\sigma$ induces the map $E[p]\otimes\sigma \to \overline{E}_v[p]\otimes\sigma$. We refer to those maps as the reduction maps. Just as above, the $\mathfrak{f}$-representation spaces $(\overline{E}_v[p^\infty]\otimes\sigma)[\mathfrak{m}]$ and $\overline{E}_v[p]\otimes\widetilde{\sigma}$ for $G_{F_v}$ will be canonically isomorphic . The obvious commutative square involving the reduction maps and the above canonical isomorphisms of $G_{F_v}$-modules is commutative. We have already described the local condition at $v$ in the definition of $\mathrm{Sel}_{E[p]\otimes\widetilde{\sigma}}(F_\infty)$. A cocycle class satisfies that Selmer condition if its image in $H^1(F_{\infty,v}, \overline{E}_v[p]\otimes\widetilde{\sigma})$ is trivial. We haven't yet specified the local condition at $v$ for defining $\mathrm{Sel}^{\Sigma_0}_{(E[p^\infty]\otimes\sigma)[\mathfrak{m}]}(F_\infty)$, but we simply require that a cocycle class have trivial image in $H^1(F_{\infty,v}, (\overline{E}_v[p^\infty]\otimes\sigma)[\mathfrak{m}])$. With this definition, the canonical isomorphism $(E[p^\infty]\otimes\sigma)[\mathfrak{m}] \cong E[p]\otimes\widetilde{\sigma}$ induces the second isomorphism in (1.4.c).

The first isomorphism in (1.4.c) requires the assumptions in theorem 2.

**Proposition 4.3.5.** *The inclusion map $(E[p^\infty]\otimes\sigma)[\mathfrak{m}] \to E[p^\infty]\otimes\sigma$ induces an isomorphism*

$$\mathrm{Sel}^{\Sigma_o}_{(E[p^\infty]\otimes\sigma)[\mathfrak{m}]}(F_\infty) \;\cong\; \mathrm{Sel}^{\Sigma_o}_{E[p^\infty]\otimes\sigma}(F_\infty)[\mathfrak{m}] \quad .$$

*under the assumptions in theorem 2. This isomorphism is $\Gamma$-equivariant.*

*Proof.* Suppose that $\pi$ is a generator of $\mathfrak{m}$. The $\mathcal{O}$-module $E[p^\infty] \otimes \sigma$ is divisible and multiplication by $\pi$ induces a surjective $\Gamma$-equivariant map

$$H^1(F_\Sigma/F, (E[p^\infty] \otimes \sigma)[\mathfrak{m}]) \longrightarrow H^1(F_\Sigma/F, E[p^\infty] \otimes \sigma)[\mathfrak{m}] \quad .$$

This map is also injective because $H^0(F_\infty, E[p^\infty] \otimes \sigma) = 0$. That fact follows from assumption *(i)* in theorem 2 and proposition 4.1.3. Thus, the map

$$\mathrm{Sel}^{\Sigma_0}_{(E[p^\infty]\otimes\sigma)[\mathfrak{m}]}(F_\infty) \longrightarrow \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]\otimes\sigma}(F_\infty)[\mathfrak{m}] \tag{4.3.c}$$

is injective. It is also $\Gamma$-equivariant. The surjectivity will be proved by showing that the corresponding maps for the local cohomology groups occurring in the definitions of these Selmer groups are injective. The assumption that $\Sigma_0$ contains $\Phi_{K/F} \cup \Psi_E$ is important here.

If $v \in \Sigma$ and $v \notin \Sigma_p \cup \Sigma_0$, then the action of $G_{F_v}$ on $E[p^\infty]$ will be unramified. Hence $G_{F_{\infty,v}}$ acts through a finite quotient group of order prime to $p$. The action of $G_{F_{\infty,v}}$ on $L_\sigma$ factors through $\Delta_v$, which also has order prime to $p$. Thus the action of $G_{F_{\infty,v}}$ on $E[p^\infty] \otimes \sigma$ is through a finite group of order prime to $p$ and therefore $H^0(F_{\infty,v}, E[p^\infty] \otimes \sigma)$ is a divisible $\mathcal{O}$-module. This proves the injectivity of the map

$$H^1(F_{\infty,v}, (E[p^\infty] \otimes \sigma)[\mathfrak{m}]) \longrightarrow H^1(F_{\infty,v}, E[p^\infty] \otimes \sigma)[\mathfrak{m}]$$

for those $v$'s. Now suppose that $v \in \Sigma_p$. We want to show that the map

$$H^1(F_{\infty,v}, (\overline{E}[p^\infty] \otimes \sigma)[\mathfrak{m}]) \longrightarrow H^1(F_{\infty,v}, \overline{E}[p^\infty] \otimes \sigma)[\mathfrak{m}]$$

is injective. The $\mathcal{O}$-module $\overline{E}[p^\infty] \otimes \sigma$ is again divisible. The map is induced by multiplication by $\pi$. Its kernel will be trivial because assumption *(ii)* in theorem 2, together with proposition 4.1.9, implies that $H^0(F_{\infty,v}, \overline{E}[p^\infty] \otimes \sigma) = 0$. Since $p$ is odd, the local cohomology groups for archimedean primes are trivial. The surjectivity of (4.3.c) follows. □

## 4.4 Justification of (1.4.d) and the proof of theorem 2.

Assume that $Ш^1(F_\Sigma/K_\infty, E[p^\infty])[p]$ is finite. Propositions 4.1.4 and 4.1.6 then imply that $H^2(F_\Sigma/F, E[p] \otimes \alpha) = 0$ for all $\alpha$. Assume also that $E(K)[p] = 0$. Then proposition 4.1.3 implies that $H^0(F_\Sigma/F, E[p] \otimes \alpha) = 0$ for all $\alpha$. Suppose that we have an exact sequence

$$0 \longrightarrow U_\alpha \longrightarrow U_\beta \longrightarrow U_\gamma \longrightarrow 0$$

of finite-dimensional representation spaces for $\Delta$ over $\mathfrak{f}$. Tensoring with $E[p]$, or with $\overline{E}_v[p]$, will give exact sequences. We consider the corresponding cohomology sequences, both global

and local. The results just cited imply that the first row in the diagram below is exact. The second row involves the product of groups of the form $\mathcal{H}_v(F_\infty, \cdot)$ over all $v$ which are in $\Sigma$, but not in $\Sigma_0$. For brevity, we denote that product by $\mathcal{P}_\Sigma^{\Sigma_0}(F_\infty, \cdot)$.
(4.4.a)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(F_\Sigma/F_\infty, E[p]\otimes\alpha) & \longrightarrow & H^1(F_\Sigma/F_\infty, E[p]\otimes\beta) & \longrightarrow & H^1(F_\Sigma/F_\infty, E[p]\otimes\gamma) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{P}_\Sigma^{\Sigma_0}(F_\infty, E[p]\otimes\alpha) & \longrightarrow & \mathcal{P}_\Sigma^{\Sigma_0}(F_\infty, E[p]\otimes\beta) & \longrightarrow & \mathcal{P}_\Sigma^{\Sigma_0}(F_\infty, E[p]\otimes\gamma) & \longrightarrow & 0 \end{array}$$

The vertical maps are the global-to-local maps defining the non-primitive Selmer groups. All the maps are $\mathfrak{f}[[\Gamma]]$-module homomorphisms. We now prove the exactness of the second row.

Since we are assuming that $p$ is non-anomalous for $E/F$, proposition 4.1.9 implies that $H^0(F_{\infty.v}, \overline{E}_v[p]\otimes\gamma) = 0$ for all $v|p$. The fact that $G_{F_{\infty,v}}$ has $p$-cohomological dimension 1implies that $H^2(F_{\infty.v}, \overline{E}_v[p]\otimes\alpha) = 0$ for those $v$'s. The cohomological dimension argument also implies that $H^2(F_{\infty.v}, E[p]\otimes\alpha) = 0$ for any non-archimedean prime $v$. Now assume that $v \notin \Sigma_p \cup \Phi_{K/F} \cup \Psi_E$. Then the action of $G_{F_{\infty,v}}$ on $E[p]$ is unramified and hence through a finite quotient group of order prime to $p$. The same is true for the action of $G_{F_{\infty,v}}$ on $\alpha, \beta$, and $\gamma$ since $|\Delta_v|$ is prime to $p$, and therefore for the action on $E[p]\otimes\alpha$, $E[p]\otimes\beta$ and $E[p]\otimes\gamma$. Suppose that all of these actions factor through $G$, a finite group of order prime to $p$. Then $H^1(G, E[p]\otimes\alpha) = 0$. Therefore, we have the following exact sequence

$$H^0(F_{\infty,v}, E[p]\otimes\beta) \longrightarrow H^0(F_{\infty,v}, E[p]\otimes\gamma) \longrightarrow 0 \quad .$$

The exactness of the second row in (4.4.a) follows from these observations.

The vertical arrows are surjective by proposition 4.2.2. The exactness of the sequence (1.4.d) then follows by applying the snake lemma, completing the proof of theorem 2. □

## 4.5 Finiteness of Selmer atoms.

We believe that the Selmer atoms we have been considering are usually finite dimensional over $\mathfrak{f}$. But there are exceptions. The exceptions we know of correspond to cases where $E[p]\otimes\tau$ is reducible as a representation space over $\mathfrak{f}$. As before, we assume that $\mathfrak{f}$ is large enough so that all irreducible representations over $\mathfrak{f}$ of the finite groups that we consider are absolutely irreducible. We want to make the following conjecture:

**Conjecture 4.5.1.** *Suppose that $p$ is odd and that $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. If $E[p]\otimes\tau$ is an irreducible $G_F$-representation space over $\mathfrak{f}$, then $\mathrm{Sel}_{E[p]\otimes\tau}(F_\infty)$ is finite.*

The irreducibility of $E[p] \otimes \tau$ over $F_\infty$ obviously implies the irreducibility over $F$. The converse is true too.

**Proposition 4.5.2.** *If $G_F$ acts irreducibly on the $\mathfrak{f}$-representation space $E[p] \otimes \tau$, then so does $G_{F_\infty}$.*

*Proof.* We can regard $E[p] \otimes \tau$ as a representation space for $\mathrm{Gal}(L/F)$, where $L = K(E[p])$, a finite Galois extension of $F$. It suffices to show that $L \cap F_\infty = F$. If that is not true, then clearly $F_1 \subseteq L$ and so $K_1 \subseteq L$. Hence $K_1 \subset L \cap K_\infty$. Since $p^2 \nmid [L : K]$, it would follow that $L \cap K_\infty = K_1$. Hence $\mathrm{Gal}(L/K)$ has a normal subgroup of index $p$. But $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup $H$ of $GL_2(\mathbf{F}_p)$. The simplicity of $SL_2(\mathbf{F}_p)/\{\pm I\}$ implies that $H$ cannot contain $SL_2(\mathbf{F}_p)$. The Sylow theorems imply that $H$ contains either one or all of the $p+1$ Sylow $p$-subgroups of $GL_2(\mathbf{F}_p)$. Those subgroups are of order $p$ and generate $SL_2(\mathbf{F}_p)$. Therefore, one sees that $H$ has a unique subgroup $P$ of order $p$. It is clear that $P$ is a normal subgroup of $\mathrm{Gal}(L/F)$. Therefore, $E[p]^P$ is invariant under the action of $\mathrm{Gal}(L/F)$. This would imply that $E[p]$ is reducible as a representation space for $G_F$, and hence so is $E[p] \otimes \tau$, contrary to the hypothesis. □

**A.** *The case where $G_F$ acts irreducibly on $E[p] \otimes \tau_0$.* Suppose that $G_F$ acts irreducibly on $E[p] \otimes_{\mathbf{F}_p} \mathfrak{f}$. If $K \cap F(E[p]) = F$, then it follows that $G_F$ acts irreducibly on $E[p] \otimes \tau$ for any $\tau$ in $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. This is so because the action of $G_F$ on $E[p] \otimes \tau$ factors through the direct product $\mathrm{Gal}(K(E[p])/F) \cong \mathrm{Gal}(F(E[p])/F) \times \Delta$, and is therefore just the tensor product of irreducible representations of each direct factor. However, if $K \cap F(E[p]) \neq F$, it is not uncommon for $E[p] \otimes \tau$ to be reducible. For example, suppose that $K = F(E[p])$ and that $\Delta \cong GL_2(\mathbf{F}_p)$. Then, the action of $G_F$ on $E[p]$ factors through $\Delta$ and defines an irreducible representation of $\Delta$ of dimension 2. One can take $\mathfrak{f} = \mathbf{F}_p$ in this example since all the irreducible representations of $\Delta$ are isomorphic to $sym^a(E[p]) \otimes det^b$ for non-negative integers $a$ and $b$. If $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta)$ and $n(\tau) > 1$, then the representation space $E[p] \otimes \tau$ of $\Delta$ over $\mathbf{F}_p$ is actually reducible. A similar phenomenon can happen if $\Delta$ is a proper subgroup of $GL_2(\mathbf{F}_p)$. We will discuss one such example (due to Drinen) in part **C** below, where $\Delta$ is a nonabelian subgroup of order prime to $p$. It is clear that $\Delta$ will still act irreducibly on $E[p] \otimes \tau_0$.

**B.** *The case where $E[p]$ is reducible.* We consider the simpler situation where $E[p] \otimes \tau$ is reducible just because $E[p]$ is itself reducible. This means that $E$ has an isogeny of degree $p$ defined over $F$. Let $\Phi$ denote the kernel of that isogeny. Then $E[p]$ is reducible as a representation space for $G_F$ over $\mathbf{F}_p$ and $\Phi$ is a $G_F$-invariant, 1-dimensional subspace of $E[p]$. Hence $\Phi \otimes \tau$ is a $G_F$-invariant $\mathfrak{f}$-subspace of $E[p] \otimes \tau$ of dimension $n(\tau)$, and so $E[p] \otimes \tau$ is reducible as a $G_F$-representation space over $\mathfrak{f}$.

For simplicity, we will now assume that $F = \mathbf{Q}$. Thus, $E$ is assumed to be defined over $\mathbf{Q}$ and to have good ordinary reduction at $p$. The reduction of $E$ modulo $p$ is denoted by $\overline{E}_p$. If $\pi$ is a prime of $\mathbf{Q}(E[p])$ lying above $p$, then the reduction map $E[p] \to \overline{E}_p[p]$ is a surjective homomorphism. We denote its kernel by $F_\pi^+ E[p]$, following the notation in [Dri]. Thus, $F_\pi^+ E[p]$ is a 1-dimensional subspace of $E[p]$. In general, only the orbit of $F_\pi^+ E[p]$ under the action of $G_{\mathbf{Q}}$ is well-defined. The next proposition deals with the case where $F_\pi^+ E[p]$ is fixed by the action of $G_{\mathbf{Q}}$.

The cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ is denoted by $\mathbf{Q}_\infty$. Suppose that $K/\mathbf{Q}$ is a finite Galois extension, that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$, that $\Delta = \mathrm{Gal}(K/\mathbf{Q})$, and that $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. For any $G_{\mathbf{Q}}$-representation space $A$ over $\mathfrak{f}$, we let $n^{(\pm)}(A)$ denote the $\mathfrak{f}$-dimension of the $(\pm 1)$-eigenspace for a complex conjugation in $G_{\mathbf{Q}}$. With this notation, we will prove the following result.

**Proposition 4.5.3.** *Suppose that $E$ is defined over $\mathbf{Q}$ and has an isogeny of degree $p$ defined over $\mathbf{Q}$. Suppose that $\Phi$ is the kernel of that isogeny and that the extension $\mathbf{Q}(\Phi)/\mathbf{Q}$ is ramified at $p$. Let $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. Then*

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)\big) \;\geq\; n^-(\Phi \otimes \tau) \quad .$$

*In particular, if $n^-(\Phi \otimes \tau) \geq 1$, then $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ is infinite.*

*Proof.* The set $\Sigma$ consists of primes of $\mathbf{Q}$ now. For $m \geq 0$, let $\mathbf{Q}_m$ denote the $m$-th layer in $\mathbf{Q}_\infty/\mathbf{Q}$. The Euler-Poincaré characteristic for the $\mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q}_m)$-module $\Phi\otimes\tau$ is $n^-(\Phi\otimes\tau)p^m$. Thus the $\mathfrak{f}$-dimension of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_m, \Phi \otimes \tau)$ is at least $n^-(\Phi \otimes \tau)p^m$. The restriction maps

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_m, \Phi \otimes \tau) \;\longrightarrow\; H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi \otimes \tau)^{\Gamma_m}$$

are surjective and the kernels are finite of bounded order (and usually trivial). It follows that the corank of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi\otimes\tau)$ as an $\mathfrak{f}[[\Gamma]]$-module is at least $n^-(\Phi\otimes\tau)$. We will denote the maximal divisible $\mathfrak{f}[[\Gamma]]$-submodule of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi\otimes\tau)$ by $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi\otimes\tau)_{div}$. Consider the maps

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi \otimes \tau)_{div} \;\longrightarrow\; H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E[p] \otimes \tau) \;\longrightarrow \prod_{v\in\Sigma} \mathcal{H}_v(F_\infty, E[p] \otimes \tau) \quad .$$

The first map has a finite kernel and its image is still $\mathfrak{f}[[\Gamma]]$-divisible. Denote that image by $\mathcal{S}$. For any prime $v \neq p$, the $\mathfrak{f}[[\Gamma]]$-module $\mathcal{H}_v(F_\infty, E[p] \otimes \tau)$ is finite, and hence its maximal $\mathfrak{f}[[\Gamma]]$-divisible submodule is trivial. Therefore the image of $\mathcal{S}$ in $\mathcal{H}_v(F_\infty, E[p] \otimes \tau)$ is trivial.

Now suppose that $v = p$. The assumption about $\mathbf{Q}(\Phi)/\mathbf{Q}$ implies that the action of $G_{\mathbf{Q}_p}$ on $\Phi$ is ramified. Therefore, we have $\Phi = F_\pi^+ E[p]$ for a prime $\pi$ of $\mathbf{Q}(E[p])$ lying over $p$ (and hence for all such primes). This implies that the image of $\Phi \otimes \tau$ in $\overline{E}_p[p] \otimes \tau$ is trivial.

Consequently, the image of $\mathcal{S}$ in $\mathcal{H}_v(F_\infty, E[p]\otimes\tau)$ is trivial. Therefore, we have the following inclusion:

$$\mathcal{S} = im\big(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi\otimes\tau)_{div}\big) \ \subseteq \ \mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty) \ .$$

The stated inequality follows from this since the $\mathfrak{f}[[\Gamma]]$-corank of $\mathcal{S}$ is at least $n^-(\Phi\otimes\tau)$. $\square$

**Remark 4.5.4.** It is very likely that the inequality in proposition 4.5.3 is an equality. This assertion follows from Iwasawa's conjecture that the classical $\mu$-invariant for the cyclotomic $\mathbf{Z}_p$-extension $L_\infty$ of any number field $L$ vanishes. That conjecture asserts that $Cl(L_n)[p]$ is of bounded order as $n\to\infty$, where $Cl(L_n)$ denotes the ideal class group of $L_n$, the $n$-th layer in $L_\infty/L$. It has been proven if $L/\mathbf{Q}$ is abelian, a theorem of Ferrero and Washington [FeWa]. If Iwasawa's conjecture is assumed to be true for all number fields $L$, then one can deduce that

$$\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Phi\otimes\tau)\big) \ = \ n^-(\Phi\otimes\tau)$$

for all $\tau\in\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. This is proved in [Gr99], lemma 5.9, for the special case $\tau=\tau_0$, but the same argument (which is rather long) works in general. Furthermore, $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)/\mathcal{S}$ would then be finite, where $\mathcal{S}$ is as in the proof of proposition 4.5.3. It would therefore follow that the $\mathfrak{f}[[\Gamma]]$-corank of $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ is indeed equal to $n^-(\Phi\otimes\tau)$. The Ferrero-Washington theorem implies this statement for all 1-dimensional $\tau$'s.

As an example, suppose that $E$ is the elliptic curve $X_0(11)$, which is 11A1 in Cremona's tables. Let $p=5$. Then $E$ has good, ordinary reduction at $p$ and there are two cyclic isogenies of $E$ of degree $p$ defined over $\mathbf{Q}$. For one of them, the kernel $\Phi$ satisfies the assumption in the above proposition. In fact, $\Phi\cong\mu_p$ as a Galois module. For any $\tau\in\mathrm{Irr}_{\mathfrak{f}}(\Delta)$, we have $n^-(\Phi\otimes\tau) = n^+(U_\tau)$, which will be a lower bound on the $\mathfrak{f}[[\Gamma]]$-corank of $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$. Iwasawa's conjecture for the base field $L=K(\mu_p)$ implies equality. $\lozenge$

**Remark 4.5.5.** The ramification hypothesis in proposition 4.5.3 is not preserved by isogeny. As an example, let $E$ again be 11A1 in [Cre], let $E'$ be 11A3, and let $p=5$. Then $E'[p]$ has a unique $G_{\mathbf{Q}}$-invariant subgroup $\Phi'$ of order $p$. It is generated by a point on $E'(\mathbf{Q})$ of order $p$ and so $\mathbf{Q}(\Phi') = \mathbf{Q}$. In general, suppose that $E$ is any elliptic curve over $\mathbf{Q}$ with good ordinary reduction at a prime $p$ which has an isogeny over $\mathbf{Q}$ of degree $p$. It is not hard to see that the isogeny class of $E$ over $\mathbf{Q}$ contains at least one curve $E'$ where the hypothesis fails: $E'[p]$ will have just one $G_{\mathbf{Q}}$-invariant subgroup $\Phi'$ of order $p$ and the action of $G_{\mathbf{Q}}$ on $\Phi'$ will be unramified at $p$. It is then reasonable to conjecture that all the Selmer atoms $\mathrm{Sel}_{E'[p]\otimes\tau}(\mathbf{Q}_\infty)$ are finite. Some results in this direction are proved in [Tri], mostly taking $\tau=\tau_0$ and assuming that the kernel of the isogeny is generated by a point of $E'(\mathbf{Q})$. That conjecture means that, for any Galois extension $K/\mathbf{Q}$, it should be true that $\mathrm{Sel}_{E'}(K_\infty)[p]$ is finite. Thus, in the situation of the above proposition, and assuming the conjecture, one should be able to apply all our results to $E'$ in place of $E$.

Now one has $X_E^{\Sigma_0}(K_\infty)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p \cong X_{E'}^{\Sigma_0}(K_\infty)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$ for any choice of $\Sigma_0$. Thus, one certainly has $\lambda_E^{\Sigma_0}(\sigma) = \lambda_{E'}^{\Sigma_0}(\sigma)$ for all $\sigma$. Furthermore, assuming that $\mathrm{Sel}_{E'}(K_\infty)[p]$ is indeed finite, it would follow from proposition 3.2.1 that $X_{E'}^{\Sigma_0}(K_\infty)$ is quasi-projective if $\Sigma_0$ is suitably chosen. Therefore, one would expect to have exactly the same congruence relations for the $\lambda_E^{\Sigma_0}(\sigma)$'s as described in the introduction.

If we take an arbitrary base field $F$, one can prove an analogue of proposition 4.5.3. The formulation is somewhat more involved. We refer the reader to [Dri] for a thorough discussion of this. Results in that paper suggest that the preceding discussion in this remark should apply with no change under the assumption that $E$ is defined over $\mathbf{Q}$ and has a cyclic isogeny of degree $p$ defined over $\mathbf{Q}$. In particular, if $X = X_E^{\Sigma_0}(K_\infty)$, then one would conjecture that $X/X[p^t]$ is quasi-projective for a suitably chosen set $\Sigma_0$ and a sufficiently large $t$. $\Diamond$

**C.** *Drinen's example.* Now we come to a more surprising kind of example, but one which seems exceedingly rare. It was found by M. Drinen, although our explanation is from the point of view of Selmer atoms and is somewhat different than that given in [Dri]. The idea is that if $E[p]\otimes\tau$ is reducible and if $\Psi$ is a $G_{\mathbf{Q}}$-invariant subspace, then one can consider the map

$$\mu : H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Psi)_{div} \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E[p]\otimes\tau) \quad . \tag{4.5.a}$$

The kernel of the map $\mu$ is finite. One has $\mathrm{corank}_{\mathfrak{f}[[\Gamma]]}\big(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty,\Psi)\big) \geq n^-(\Psi)$, which could easily be positive. The $\mathfrak{f}[[\Gamma]]$-corank of $\mathrm{im}(\mu)$ is the same. One can then consider $\mathrm{im}(\mu)\cap \mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$, which sometimes will also have positive $\mathfrak{f}[[\Gamma]]$-corank, thereby giving an example where $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ is infinite. This is precisely what happens in the proof of proposition 4.5.3, where we take $\Psi = \Phi\otimes\tau$.

Drinen's example is as follows. Let $E$ be any one of the elliptic curves in the isogeny classes 338D or 338E in Cremona's tables. Let $p = 3$, $K = \mathbf{Q}(E[p])$, and $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. Now the representation of $G_{\mathbf{Q}}$ on $E[p]$ is irreducible, but the image of $G_{\mathbf{Q}}$ in the automorphism group $GL_2(\mathbf{F}_p)$ is small, just a dihedral group of order 8. We identify that image with $\Delta$. We can clearly take $\mathfrak{f} = \mathbf{F}_p$ in this case. Thus, $\Delta$ has just one 2-dimensional irreducible representation over $\mathbf{F}_p$, which we call $\tau_{\mathbf{2}}$. It is precisely the representation giving the action of $\Delta$ on $E[p]$. Now $\Delta$ also has four 1-dimensional representations over $\mathbf{F}_p$ and $E[p]\otimes\tau_{\mathbf{2}}$ is easily seen to be isomorphic to the direct sum of those representations. The action of $\Delta$ on $E[p]\otimes\tau_{\mathbf{2}}$ is through the quotient $\Delta^{ab}$, which is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$. In fact, the maximal abelian extension of $\mathbf{Q}$ contained in $K$ is the biquadratic field $\mathbf{Q}(\sqrt{13},\sqrt{-3})$. Two of the four 1-dimensional representations of $\Delta$ are odd, say $\varepsilon$ and $\varepsilon'$. Define $\Psi$ to be the

sum of the $\varepsilon$- and $\varepsilon'$-components in $E[p] \otimes \tau_{\mathbf{2}}$. Hence $n(\Psi) = n^-(\Psi) = 2$. It follows that the $\mathbf{F}_p[[\Gamma]]$-corank of $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Psi)$ is at least 2. In fact, that corank is exactly 2.

As in the proof of proposition 4.5.3, if $\mu$ is the map (4.5.a), then $\mathrm{im}(\mu)$ satisfies the local conditions defining $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ for all $v \neq p$. For the local condition at the unique prime of $\mathbf{Q}_\infty$ lying above $p$, one chooses an embedding of $\mathbf{Q}_\Sigma$ into $\overline{\mathbf{Q}}_p$. Let $\pi$ be the associated prime of $K$. We then define $F_\pi^+\Psi = \Psi \bigcap \big(F_\pi^+ E[p] \otimes \tau_{\mathbf{2}}\big)$. If $\gamma$ is a cocycle class in $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, \Psi)$, then a sufficient condition for $\mu(\gamma)$ to satisfy the local condition for $p$ is that the image of $\gamma$ in $H^1(\mathbf{Q}_{\infty,p}, \Psi/F_\pi^+\Psi)$ is trivial. We will show that $F_\pi^+\Psi$ is 1-dimensional, and hence so is $\Psi/F_\pi^+\Psi$. It then follows that the $\mathbf{F}_p[[\Gamma]]$-corank of $H^1(\mathbf{Q}_{\infty,p}, \Psi/F_\pi^+\Psi)$ is equal to 1, and consequently, $\mathrm{im}(\mu) \cap \mathrm{Sel}_{E[p]\otimes\tau_{\mathbf{2}}}(\mathbf{Q}_\infty)$ has positive $\mathbf{F}_p[[\Gamma]]$-corank.

Let $C = \mathrm{Gal}\big(K/\mathbf{Q}(\sqrt{13})\big)$, a subgroup of $\Delta$ of order 4. If $c \in C$ denotes a complex conjugation, then $c$ acts on $E[p]$ with eigenvalues $\pm 1$. However, $C$ also contains the center of $\Delta$, which has order 2 and is generated by the element acting on $E[p]$ as the scalar $-1$. Therefore, $C$ can be identified with the diagonal subgroup of $GL_2(\mathbf{F}_p)$ and $\Delta$ with its normalizer in $GL_2(\mathbf{F}_p)$. The group $C$ fixes two subspaces of $E[p]$. Since $p$ is unramified in $\mathbf{Q}(\sqrt{13})/\mathbf{Q}$, the inertia subgroup $I_\pi$ of $\Delta$ for any prime $\pi$ of $K$ above $p$ will be a subgroup of $C$ which acts nontrivially on $F_\pi^+E[p]$ and trivially on $E[p]/F_\pi^+E[p]$. Thus, $I_\pi$ has order 2 and a generator acts with eigenvalues $\pm 1$. It is then clear that $F_\pi^+E[p]$ is one of the two subspaces of $E[p]$ fixed by $C$. We can choose a complex conjugation $c$ so that it is a generator of $I_\pi$. Then $c$ acts on $F^+E[p] \otimes \tau_{\mathbf{2}}$ with eigenvalues $\pm 1$. It follows that $F^+\Psi$ is indeed 1-dimensional.

One can find infinitely many examples of the above type when $p = 3$. Twists of $E$ by a quadratic character $\varepsilon$ of conductor prime to $p$ would give more examples. The field $K$ can change, but the biquadratic subfield contained in $K$ will be the same. In addition, one can apply a theorem in [RuSi] which asserts that there are infinitely many elliptic curves $E'$ defined over $\mathbf{Q}$ such that $E'[p] \cong E[p]$. Then the field $K$ remains the same. That theorem applies because $p \leq 5$. It seems likely that more examples exist for $p = 3$. However, it is not so clear what to expect for $p \geq 5$. The above argument can be made to work under the following hypothesis: The prime $p$ is odd, the image of $G_{\mathbf{Q}}$ in $\mathrm{Aut}(E[p]) \cong GL_2(\mathbf{F}_p)$ is the normalizer $N$ of a split Cartan subgroup $C$, and the subfield of $\mathbf{Q}(E[p])$ fixed by $C$ is real and unramified at $p$. If $p \geq 5$, one shows that for certain 2-dimensional, irreducible representations $\tau$ of $\Delta$, $E[p] \otimes \tau$ has a $\Delta$-invariant subspace $\Psi$ such that $n(\Psi) = n^-(\Psi) = 2$. The subspace $\Psi$ will now be irreducible, but the rest of the argument is essentially the same as in the above example for $p = 3$. Examples of such elliptic curves $E$ for $p > 3$ haven't yet been exhibited.

**D.** *Some verifiable cases.* We will end this chapter by discussing some cases where the Selmer atoms are provably finite. We continue to assume that $F = \mathbf{Q}$. Suppose that $K$ is

a finite, abelian extension of $\mathbf{Q}$ and $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. A theorem of Kato (theorem 17.4 in [Kat]) asserts that the $\Lambda$-module $X = X_E(K_\infty)$ is torsion and that its characteristic ideal $I_X$ contains an element $p^t\theta(E/K)$, where $t \geq 0$ and $\theta(E/K) \in \Lambda$ is the measure on $\Gamma$ associated with the $p$-adic $L$-function for $E$ over $K$. The element $\theta(E/K)$ can be computed quite accurately in practice. In particular, if one can verify that $I_X$ contains $\theta(E/K)$ itself and that $p \nmid \theta(E/K)$, then it follows that $\mu(X) = 0$. The Selmer atoms $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ will then be finite for all $\tau \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ according to proposition 4.2.5. Kato proves that $\theta(E/K) \in I_X$ if $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \cong GL_2(\mathbf{F}_p)$. The assertion that $p \nmid \theta(E/K)$ has been verified for numerous examples, especially when $K$ is a quadratic field or $K = \mathbf{Q}(\mu_p)$. The first such verifications are given in [MaSw] for the elliptic curves $X_0(11)$ and $X_0(17)$. They consider the good, ordinary primes $p$ in the range $7 \leq p \leq 347$ for the first curve and in the range $5 \leq p \leq 179$ for the second. Those calculations are for $K = \mathbf{Q}(\mu_p)$ and include the determination of the corresponding $\lambda$-invariants for each character of $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. To be precise, it is only the *"analytic"* $\lambda$-invariants that are determined. Similar calculations have been done by T. McCabe for various elliptic curves and primes $p$. R. Pollack has produced extensive tables which give $\lambda$- and $\mu$-invariants over $\mathbf{Q}_\infty$. They includes quadratic twists for many elliptic curves. Those tables can be found on Pollack's webpage at Boston University.

Proposition 5.10 in [Gr99] gives one situation where it is known that $\mu\big(X_E(K_\infty)\big) = 0$. The assumptions are that $E$ has an isogeny of degree $p$ defined over $\mathbf{Q}$, that the character $\phi : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ giving the action of $G_{\mathbf{Q}}$ on the kernel $\Phi$ of the isogeny is even and is ramified at $p$, and that $K$ is a finite, abelian, totally real extension of $\mathbf{Q}$. That result is a consequence of the Ferrero-Washington theorem. It is equivalent to the assertion that $\mathrm{Sel}_{E[p]\otimes\tau}(\mathbf{Q}_\infty)$ is finite for all $\tau \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, where $\Delta = \mathrm{Gal}(K/F)$. Unfortunately, the assumption that $K$ is totally real is crucial in the proof.

# 5 The structure of $\mathcal{H}_v(K_\infty, E)$.

Our main objective in this chapter is to discuss the determination of the quantity $\delta_E^{\Sigma_0}(\sigma)$ which occurs in formula (1.3.b). For each $v \in \Sigma_0$, the group $\mathcal{H}_v(K_\infty, E)$ defined in the introduction is the direct product of the groups $H^1(K_{\infty,\eta}, E[p^\infty])$, where $\eta$ varies over all primes of $K_\infty$ lying above $v$. This is so since $v \nmid p$ and hence $\mathrm{im}(\kappa_\eta) = 0$. For each such $\eta$, let $\Delta_\eta$ denote the decomposition subgroup of $\Delta$ for $\eta$. It is determined up to conjugacy by $v$. Let $g_v$ denote the number of primes $\nu$ of $F_\infty$ lying over $v$. As a $\Delta$-module, $\mathcal{H}_v(K_\infty, E)$ is the direct product over all those $\nu$'s of the $\Delta$-modules

$$\mathcal{H}_\nu(K_\infty, E) \;=\; \prod_{\eta|\nu} H^1(K_{\infty,\eta}, E[p^\infty]) \;\cong\; \mathrm{Ind}_{\Delta_\eta}^{\Delta}\big(H^1(K_{\infty,\eta}, E[p^\infty])\big)\ , \tag{5.0.a}$$

where $\eta$ varies over the primes of $K_\infty$ lying over $\nu$. Those primes $\eta$ are permuted transitively by $\Delta$. For the induced module in (5.0.a), we simply fix one $\eta|\nu$ for each $\nu$. We identify $\Delta_\eta$ with $\mathrm{Gal}(K_{\infty,\eta}/F_{\infty,\nu})$. That group acts naturally on $H^1(K_{\infty,\eta}, E[p^\infty])$.

Let $\widehat{\mathcal{H}}_\nu(K_\infty, E)$ denote the Pontryagin dual of $\mathcal{H}_\nu(K_\infty, E)$. For each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, one sees easily that $\lambda(\widehat{\mathcal{H}}_\nu(K_\infty, E), \sigma)$ is independent of the choice of $\nu$ lying above $v$. We denote that quantity by $\delta_{E,v}(\sigma)$. Then

$$\delta_E^{\Sigma_0}(\sigma) \;=\; \sum_{v\in\Sigma_0} g_v \delta_{E,v}(\sigma)\ . \tag{5.0.b}$$

The $g_v$'s depend only on $F_\infty/F$ and not on $E$. They are not difficult to determine, but the $\delta_{E,v}(\sigma)$'s are more subtle.

All of the quantities that we define in this chapter are independent of the choice of the primes $\eta$ and $\nu$ dividing $v$. In particular, the extensions $F_{\infty,\nu}$ and $K_{\infty,\eta}$ are determined by $v$ and $K$. Thus, to simplify notation, we will denote these fields by $F_{\infty,v}$ and $K_{\infty,v}$ from here on, and we will usually write $\Delta_v$ instead of $\Delta_\eta$ for $\mathrm{Gal}(K_{\infty,v}/F_{\infty,v})$. We will sometimes revert back to the previous notation if there is a possibility of confusion. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, then we denote their restrictions to the subgroup $\Delta_v$ of $\Delta$ by $\sigma_v$ and $\tau_v$, respectively. Various Galois groups will arise in our arguments. We will use the following notation throughout for a few of them.

$$\mathcal{G}_v \;=\; G_{F_{\infty,v}}\ , \qquad \mathcal{N}_v \;=\; G_{K_{\infty,v}}\ , \qquad \mathcal{I}_v \;=\; G_{K_v^{unr}}\ ,$$

where $K_v^{unr}$ is the maximal unramified extension of $K_v$. Since $K_{\infty,v}/K_v$ is unramified, $\mathcal{I}_v$ is the inertia subgroup of $\mathcal{N}_v$. Note that $\Delta_v$ is isomorphic to the quotient group $\mathcal{G}_v/\mathcal{N}_v$. We will often regard representations of $\Delta_v$ as representations of $\mathcal{G}_v$.

Another notation that we will use is the following. Suppose that $G$ is a group, that $\alpha$ is an absolutely irreducible representation for $G$ over a field $\mathfrak{F}$, and that $\beta$ is any representation for $G$ over $\mathfrak{F}$. We assume these representations are finite-dimensional. Let $\mathcal{V}_\alpha$ and $\mathcal{V}_\beta$ be the underlying representation spaces for $\alpha$ and $\beta$, respectively. Suppose that $m$ is the largest nonnegative integer such that $\mathcal{V}_\beta$ contains a $G$-invariant subspace isomorphic to $\mathcal{V}_\alpha^m$. We denote this $m$ by $\langle\beta,\alpha\rangle_G$, or just by $\langle\beta,\alpha\rangle$. Equivalently,

$$\langle\beta,\alpha\rangle \;=\; \langle\beta,\alpha\rangle_G \;=\; \dim_{\mathfrak{F}}\big(\mathrm{Hom}_G(\mathcal{V}_\alpha, \mathcal{V}_\beta)\big)\ .$$

If $G$ is a quotient of another group $\mathcal{G}$, then one can view $\alpha$ and $\beta$ as representations of $\mathcal{G}$, but $\langle\beta,\alpha\rangle$ is unchanged. Thus, $\langle\beta,\alpha\rangle_G = \langle\beta,\alpha\rangle_{\mathcal{G}}$. We often suppress the subscripts because specifying $\alpha$ and $\beta$ should be sufficient.

If $G$ is finite and $\mathfrak{F}$ has characteristic 0, then $\langle \beta, \alpha \rangle$ is just the usual multiplicity of $\alpha$ in $\beta$. If $G$ is infinite, it may happen that $\beta$ is not semisimple. Its semisimplification is denoted by $\beta^{ss}$. Then, in a composition series for $\mathcal{V}_\beta$ consisting of $G$-invariant subspaces, the number of composition factors isomorphic to $\mathcal{V}_\alpha$ is equal to $\langle \beta^{ss}, \alpha \rangle$, which may be different than $\langle \beta, \alpha \rangle$. Notice that we are taking the second variable in this notation to be irreducible. This is usually what we will do. However, if $G$ is finite and $\mathfrak{F}$ has characteristic zero, then all finite-dimensional representations over $\mathfrak{F}$ are semisimple. We may then sometimes want to regard $\langle \beta, \alpha \rangle$ as a $\mathbf{Z}$-bilinear form on $\mathcal{R}_{\mathfrak{F}}(G)$. We assume that all irreducible representations over $\mathfrak{F}$ are absolutely irreducible. The form is symmetric, $\mathbf{Z}$-valued, nondegenerate, and is characterized by defining $\langle \beta, \alpha \rangle$ just as before when $\alpha$ and $\beta$ are both irreducible, equal to 1 if $\beta \cong \alpha$ and equal to 0 otherwise.

## 5.1 Determination of $\delta_{E,v}(\sigma)$.

To determine $\delta_{E,v}(\sigma)$, it is sufficient to study $H^1(K_{\infty,v}, E[p^\infty]) = H^1(\mathcal{N}_v, E[p^\infty])$ as a $\Delta_v$-module. The $\delta_{E,v}(\sigma)$'s can then be determined by the Frobenius reciprocity law. More precisely, let $\widehat{H}_{E,v}$ denote the Pontryagin dual of $H^1(\mathcal{N}_v, E[p^\infty])$. We will assume that $\mathcal{F}$ is chosen as in the introduction. We can regard $\widehat{H}_{E,v} \otimes_{\mathbf{Z}_p} \mathcal{F}$ as a representation space for $\Delta_v$. Furthermore, each $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ will be absolutely irreducible. We will temporarily write $h_v(E, \chi)$ to denote the multiplicity of $\chi$ in $\widehat{H}_{E,v} \otimes_{\mathbf{Z}_p} \mathcal{F}$. Then (5.0.a) implies that $\delta_{E,v}(\sigma)$ is equal to the multiplicity of $\sigma$ in

$$\bigoplus_{\chi \in \mathrm{Irr}_v} \mathrm{Ind}_{\Delta_v}^{\Delta}(\chi)^{h_v(E,\chi)} \quad ,$$

where $\chi$ runs over $\mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ (abbreviated as $\mathrm{Irr}_v$ here and in the summation below). By Frobenius reciprocity, the multiplicity of $\sigma$ in $\mathrm{Ind}_{\Delta_v}^{\Delta}(\chi)$ is equal to $\langle \sigma_v, \chi \rangle$. Therefore, we have the formula

$$\delta_{E,v}(\sigma) \;=\; \sum_{\chi \in \mathrm{Irr}_v} \langle \sigma_v, \chi \rangle h_v(E, \chi) \quad . \tag{5.1.a}$$

The quantities $\langle \sigma_v, \chi \rangle$ are group-theoretic in nature and will be discussed for various examples in later chapters. We will now study the $h_v(E, \chi)$'s in some detail. The next proposition is needed for that purpose. Let $V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $T_p(E)$ denotes the Tate module for $E$ and $p$. We consider $V_p(E)$ as a representation space for $\mathcal{G}_v$.

**Proposition 5.1.1.** *The $\mathbf{Q}_p$-representations spaces $\widehat{H}_{E,v} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $H^0\big(K_{\infty,v}, V_p(E)\big)$ for $\Delta_v$ are isomorphic.*

*Proof.* One has a tower of fields

$$F_v \ \subset \ K_v \ \subset \ K_{\infty,v} \ \subset \ K_v^{unr} \ \subset \ K_v^{tr} \ \subset \ \overline{K}_v,$$

where $K_v^{unr}$ is the maximal unramified extension and $K_v^{tr}$ is the maximal tamely ramified extension of $K_v$, all subfields of an algebraic closure $\overline{K}_v$ of $K_v$. All these extensions are Galois over $F_v$. We have already defined $\mathcal{I}_v, \mathcal{N}_v$, and $\mathcal{G}_v$. Let $\mathcal{R}_v = G_{K_v^{tr}}$, the wild ramification subgroup of $\mathcal{N}_v$. In this proof, we will suppress the subscript $v$ and just write $\mathcal{N}, \mathcal{I}$, and $\mathcal{R}$.

Now $\mathrm{Gal}(K_v^{unr}/K_v) \cong \widehat{\mathbf{Z}}$ and $\mathrm{Gal}(K_{\infty,v}/K_v) \cong \mathbf{Z}_p$, where $\widehat{\mathbf{Z}}$ denotes the profinite completion of $\mathbf{Z}$. Hence $\mathcal{N}/\mathcal{I} \cong \widehat{\mathbf{Z}}/\mathbf{Z}_p$, a topologically cyclic group of profinite order prime to $p$. By local class field theory, we also have an isomorphism $\mathcal{I}/\mathcal{R} \cong \widehat{\mathbf{Z}}/\mathbf{Z}_\ell$, where $\ell$ is the residue field characteristic for $v$. We are assuming that $\ell \neq p$. Hence $\mathcal{I}$ contains a unique subgroup $\mathcal{P}$ containing $\mathcal{R}$ such that $\mathcal{P}/\mathcal{R} \cong \mathbf{Z}_p$. The subgroup $\mathcal{P}$ is normal in $\mathcal{N}$, and actually even normal in $G_{F_v}$. The profinite order of $\mathcal{N}/\mathcal{P}$ is prime to $p$. Furthermore, $\mathcal{R}$ is a pro-$\ell$ group and hence also has profinite order prime to $p$.

For brevity, we will let $A = E[p^\infty]$ and $B = A^{\mathcal{R}} = E(K_v^{tr})[p^\infty]$ in this proof. If $n \in \mathbf{Z}$, the notation $A(n)$ and $B(n)$ will denote the twists of $A$ and $B$ by $\chi_p^n$, where $\chi_p$ is the $p$-power cyclotomic character of $G_{F_v}$. Note that $\ker(\chi_p)$ contains $\mathcal{I}$. Local class field theory implies that the natural action of $G_{F_v}/\mathcal{P}$ on $\mathcal{P}/\mathcal{R}$ (by inner automorphisms) is given by the character $\chi_p$. For that reason, we write $\mathcal{P}/\mathcal{R} \cong \mathbf{Z}_p(1)$.

The group $\widehat{H}_{E,v}$ is the Pontryagin dual of $H^1(\mathcal{N}, A)$. We have the following isomorphisms

$$H^1(\mathcal{N}, A) \ \xrightarrow{\sim} \ H^1(\mathcal{N}/\mathcal{R}, B) \ \xrightarrow{\sim} \ H^1(\mathcal{P}/\mathcal{R}, B)^{\mathcal{N}/\mathcal{P}} \quad .$$

The first isomorphism is the inverse of the inflation map corresponding to the normal subgroup $\mathcal{R}$ of $\mathcal{N}$, which is an isomorphism because $H^1(\mathcal{R}, A) = 0$. The second isomorphism is the restriction map corresponding to the normal subgroup $\mathcal{P}/\mathcal{R}$ of $\mathcal{N}/\mathcal{R}$. It is an isomorphism because $H^i(\mathcal{N}/\mathcal{P}, B^{\mathcal{P}}) = 0$ for $i = 1, 2$.

The group $\mathcal{R}$ acts trivially on $B$. The maximal quotient $B_{\mathcal{P}}$ of $B$ on which $\mathcal{P}$ acts trivially is $B/(\varpi - 1)B$, where $\varpi$ is a topological generator for $\mathcal{P}/\mathcal{R}$. We then have isomorphisms

$$H^1(\mathcal{P}/\mathcal{R}, B) \ \cong \ \mathrm{Hom}(\mathcal{P}/\mathcal{R}, B_{\mathcal{P}}) \ \cong \ \mathrm{Hom}(\mathbf{Z}_p, B(-1)_{\mathcal{P}}) \ \cong \ B(-1)_{\mathcal{P}} \quad .$$

We have used the fact that $\mathcal{P} \subset \ker(\chi_p)$ and so $B_{\mathcal{P}}(-1) = B(-1)_{\mathcal{P}}$. Combining the above observations, we have now shown that $H^1(\mathcal{N}, A)$ is isomorphic to the maximal subgroup of $B(-1)_{\mathcal{P}}$ on which $\mathcal{N}/\mathcal{P}$ acts trivially.

Recall the following easily proved fact. Suppose that $G$ is a profinite group which has profinite order prime to $p$. Suppose that $C$ is a $p$-primary group on which $G$ acts. Then

$C^G$ is a direct summand of $C$ and is therefore canonically isomorphic to $C_G$. We apply this first to $C = B(-1)_{\mathcal{P}}$ and $G = \mathcal{N}/\mathcal{P}$. It follows that $H^1(\mathcal{N}, A)$ is isomorphic to $B(-1)_{\mathcal{N}}$. Similarly, we also have $B(-1) \cong A(-1)_{\mathcal{R}}$. Therefore, we have an isomorphism

$$H^1(\mathcal{N}, A) \;\cong\; A(-1)_{\mathcal{N}} \quad .$$

The Weil pairing implies that the Tate module $T_p(E)$ is isomorphic to the Pontryagin dual of $E[p^\infty](-1) = A(-1)$. Hence the Pontryagin dual of $A(-1)_{\mathcal{N}}$ is isomorphic to the maximal subgroup $T_p(E)^{\mathcal{N}}$ of $T_p(E)$ on which $\mathcal{N}$ acts trivially.

The isomorphisms given above are all $G_{F_v}$-equivariant. Thus, we obtain a $\mathrm{Gal}(K_{\infty,v}/F_v)$-equivariant isomorphism from the Pontryagin dual of $H^1(\mathcal{N}_v, E[p^\infty])$, which is $\widehat{H}_{E,v}$, to $T_p(E)^{\mathcal{N}_v}$. Tensoring by $\mathbf{Q}_p$ gives the isomorphism in the proposition. $\square$

**Corollary 5.1.2.** *Suppose that $v$ is a nonarchimedean prime of $F$ and that $v \nmid p$. The following statements are equivalent:*

*(i)* $\mathcal{H}_v(K_\infty, E) = 0$,

*(ii)* $\delta_{E,v}(\sigma) = 0$ *for all* $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$,

*(iii)* $H^0\big(K_{\infty,v}, V_p(E)\big) = 0$,

*(iv)* $E(K_{\infty,v})[p^\infty]$ *is finite.*

*The following statement implies (i) - (iv):*

*(v)* $E(K_v)[p] = 0$.

*Statement (v) is equivalent to the other four statements if $E$ has good reduction over $K_v$ or if $p \geq 5$ and $E$ has potentially good reduction at $v$.*

*Proof.* For the equivalence of *(i)* and *(ii)*, note that $\mathcal{H}_v(K_\infty, E)$ is a divisible group. Hence $\mathcal{H}_v(K_\infty, E) = 0$ if and only if the $\mathbf{Z}_p$-rank of its Pontryagin dual is zero. Each of the groups $\mathcal{H}_\nu(K_\infty, E)$ for $\nu|v$ has the same $\mathbf{Z}_p$-corank. By definition, its Pontryagin dual has $\mathbf{Z}_p$-rank zero if and only if all the multiplicities $\delta_{E,v}(\sigma)$ are zero. The equivalence of *(iii)* and *(iv)* is clear. Proposition 5.1.1 and (5.0.a) imply the equivalence of *(i)* and *(iii)*.

Since $\mathrm{Gal}(K_{\infty,v}/K_v)$ is pro-$p$, *(v)* is equivalent to $E(K_{\infty,v})[p] = 0$ and hence equivalent to $E(K_{\infty,v})[p^\infty] = 0$. Thus, *(v)* obviously implies *(iv)*. As for the converse, assume that $E(K_v)[p] \neq 0$. Then $E(K_{\infty,v})[p] \neq 0$. Under the assumptions about $E$ stated in the last sentence of the proposition, the action of $\mathcal{N}_v$ on $V_p(E)$ and on $E[p^\infty]$ will factor through a finite quotient group of $\mathcal{N}_v$ of order prime to $p$. (More details about the action of $\mathcal{G}_v$ are given below. We apply them to $\mathcal{N}_v$. ) Thus, the action of $\mathcal{N}_v$ on $E[p]$ is semisimple. Since we assume that $E(K_v)[p] \neq 0$, the $\mathbf{F}_p$-representation space $E[p]$ for $\mathcal{N}_v$ contains the

trivial representation as a constituent. It follows that the trivial representation occurs as a constituent in the $\mathbf{Q}_p$-representation space $V_p(E)$ for $\mathcal{N}_v$. Hence, it does indeed follow that $H^0\big(K_{\infty,v}, V_p(E)\big)$ has positive dimension. Therefore, *(iii)*, and hence *(iv)*, implies *(v)*. $\square$

## 5.2 Determination of $\langle \rho_{E,v}, \chi \rangle$.

We will use proposition 5.1.1 to reduce the determination of the $h_v(E,\chi)$'s to studying $V_p(E)_{\mathcal{F}} = V_p(E) \otimes_{\mathbf{Q}_p} \mathcal{F}$ as a representation space for $\mathcal{G}_v$. We denote this representation of $\mathcal{G}_v$ by $\rho_{E,v}$. It is not necessarily semisimple. If $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$, then we can regard $\chi$ as an irreducible representation of $\mathcal{G}_v$. For any such $\chi$, let $V_p(E)_{\mathcal{F}}^{(\chi)}$ denote the maximal subspace of $V_p(E)_{\mathcal{F}}$ on which $\mathcal{G}_v$ acts by $\chi$. Obviously,

$$V_p(E)_{\mathcal{F}}^{(\chi)} \ \subseteq \ H^0\big(K_{\infty,v}, V_p(E)_{\mathcal{F}}\big) \ = \ H^0\big(K_{\infty,v}, V_p(E)\big) \otimes_{\mathbf{Q}_p} \mathcal{F} \quad .$$

Consequently, we have $h_v(E,\chi) = \langle \rho_{E,v}, \chi \rangle$ for any $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$. It therefore suffices to discuss the $\langle \rho_{E,v}, \chi \rangle$'s. There are four cases to consider, corresponding to different reduction types over $F_v$.

**$E$ has good reduction at $v$.** Then the action of $G_{F_v}$ on $V_p(E)$ is unramified. The Frobenius automorphism over $F_v$ acts with eigenvalues $\alpha_v, \beta_v$, the roots of a quadratic polynomial $x^2 - a_v x + N(v)$, where $a_v,\ N(v) \in \mathbf{Z}$. Here $N(v)$ is the cardinality of the residue field for $v$ and $1 - a_p + N(v)$ is the cardinality of the set of points on the reduction of $E$ over that residue field. Those eigenvalues lie in a quadratic extension of $\mathbf{Q}_p$, possibly in $\mathbf{Q}_p$ itself. They must be units in that field. We will let $\widetilde{\alpha}_v,\ \widetilde{\beta}_v$ denote the unique roots of unity of order prime to $p$ in their residue classes. The orders of $\widetilde{\alpha}_v$ and $\widetilde{\beta}_v$ divide $p^2 - 1$. Now $F_{\infty,v}$ is the unramified $\mathbf{Z}_p$-extension of $F_v$. The eigenvalues of the Frobenius automorphism in $\mathcal{G}_v$ acting on $V_p(E)$ are the roots of unity $\widetilde{\alpha}_v$ and $\widetilde{\beta}_v$. Thus, for a suitable $\mathcal{F}$, $V_p(E)_{\mathcal{F}}$ is the direct sum of two one-dimensional subspaces on which $\mathcal{G}_v$ acts by unramified characters $\varphi_v,\ \psi_v$ of order dividing $p^2 - 1$. Those characters are determined entirely by the integers $a_v$ and $N(v)$.

The action of $G_{F_v}$ on $\mathbf{Q}_p(1)$ is also unramified. The Frobenius acts by $N(v)$, a $p$-adic unit. The Frobenius in $\mathcal{G}_v$ acts by the unique $(p-1)$-st root of unity in the residue class of $N(v)$. Thus, $\mathcal{G}_v$ acts on $\mathbf{Q}_p(1)$ by a character $\omega_v$ of order dividing $p-1$. The Weil pairing on $V_p(E)$ implies that $\varphi_v \psi_v = \omega_v$. If $\chi \in \{\varphi_v, \psi_v\}$, then $\langle \rho_{E,v}, \chi \rangle = 1$ if $\psi_v \neq \varphi_v$ and $\langle \rho_{E,v}, \chi \rangle = 2$ if $\psi_v = \varphi_v$. For any other $\chi$, we have $\langle \rho_{E,v}, \chi \rangle = 0$.

**$E$ has multiplicative reduction at $v$.** This case is somewhat simpler. The action of $\mathcal{G}_v$ on $V_p(E)$ is not semisimple. There is a unique one-dimensional $\mathcal{G}_v$-invariant subspace. The

character giving the action of $\mathcal{G}_v$ on that subspace will be denoted by $\varphi_v$. Then, $\varphi_v = \omega_v$ if $E$ has split multiplicative reduction at $v$ and $\varphi_v = \omega_v\varepsilon_v$, where $\varepsilon_v$ is unramified of order 2, if $E$ has nonsplit multiplicative reduction at $v$. If $p = 2$, then the second case cannot occur and $\varphi_v$ is trivial. We have $\langle\rho_{E,v}, \chi\rangle = 0$ unless $\chi = \varphi_v$ in which case $\langle\rho_{E,v}, \chi\rangle = 1$. Note that the order of $\varphi_v$ is not divisible by $p$.

**$E$ has potentially multiplicative reduction at $v$.** In this case, $V_p(E)$ will also have a unique one-dimensional $\mathcal{G}_v$-invariant subspace. If $\varphi_v$ denotes the corresponding character, then $\varphi_v\omega_v^{-1}$ will be a ramified quadratic character of $\mathcal{G}_v$, assuming that $E$ doesn't have multiplicative reduction over $F_{\infty,v}$. As above, we have $\langle\rho_{E,v}, \chi\rangle = 1$ if $\chi = \varphi_v$ and $\langle\rho_{E,v}, \chi\rangle = 0$ otherwise. The order of $\varphi_v$ is not divisible by $p$ if $p \geq 3$.

**$E$ has potentially good reduction at $v$.** We assume that $E$ actually has bad reduction at $v$. There are a number of distinct possibilities for the action of $\mathcal{G}_v$. However, the image of $\mathcal{G}_v$ under $\rho_{E,v}$ is finite and hence the representation is semisimple. We let $\Theta_v$ denote the image of the inertia subgroup under $\rho_{E,v}$. Then $\Theta_v$ is a normal subgroup of $\rho_{E,v}(\mathcal{G}_v)$ and $\rho_{E,v}(\mathcal{G}_v)/\Theta_v$ is cyclic of order prime to $p$. The possibilities for $\Theta_v$ are described in [SeTa]. The order of $\Theta_v$ has no prime factor $\geq 5$. If $\rho_{E,v}(\mathcal{G}_v)$ is abelian, then the action of $\mathcal{G}_v$ on $V_p(E)_{\mathcal{F}}$ is given by two one dimensional characters of $\mathcal{G}_v$, which we denote by $\varphi_v$ and $\psi_v$. Since $\varphi_v\psi_v = \omega_v$, which is unramified, it follows that the restrictions of $\varphi_v$ and $\psi_v$ to $\Theta_v$ are both faithful. Note that it is possible for $\varphi_v$ and $\psi_v$ to be equal, just as in the case of good reduction. If the image of $\rho_{E,v}$ is nonabelian, then $\rho_{E,v}$ is absolutely irreducible and we denote it by $\varphi_v$. Hence, there may be at most two one-dimensional $\chi$'s for which $\langle\rho_{E,v}, \chi\rangle > 0$, or just one two-dimensional $\chi$. If one of those $\chi$'s factors through $\Delta_v$, then $E$ has good reduction over $K_v$. If $E$ has good reduction over $K_v$, then $\varphi_v$ (and $\psi_v$) factor through $\mathrm{Gal}(K_v^{unr}/F_v)$.

One useful remark is that if $p \geq 5$, then the action of $\mathcal{G}_v$ on $V_p(E)$ factors through a finite quotient group of order prime to $p$. This follows from what we have said above, but it is also quite clear directly since an element of order $p$ can act nontrivially on a 2-dimensional $\mathbf{Q}_p$-vector space only if $p \leq 3$.

For each $v \in \Sigma_0$, let $\mathrm{Irr}_v = \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ as before. Then (5.0.b) and (5.1.a) imply the formula

$$\delta_E^{\Sigma_0}(\sigma) \;=\; \sum_{v\in\Sigma_0} g_v \left( \sum_{\chi\in\mathrm{Irr}_v} \langle\sigma_v, \chi\rangle\langle\rho_{E,v}, \chi\rangle \right) . \tag{5.2.a}$$

The inner sum is precisely $\delta_{E,v}(\sigma)$. For each $v$, there are at most two irreducible representations $\chi$ of $\mathcal{G}_v$ for which $\langle\rho_{E,v}, \chi\rangle > 0$. Thus, at most two terms in each inner sum could be

nonzero. Those $\chi$'s might or might not factor through $\Delta_v$. Even if they do, the multiplicity $\langle \sigma_v, \chi \rangle$ might be 0.

## 5.3 Projectivity and Herbrand quotients.

The missing steps for the proof of proposition 3.3.1 are contained in the following result.

**Proposition 5.3.1** *(i) For any $v \in \Phi_{K/F}$, the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$ is projective as a $\mathbf{Z}_p[\Delta]$-module if and only if $\mathcal{H}_v(K_\infty, E) = 0$. (ii) Suppose that $p \geq 5$ or that $E$ has good or multiplicative reduction at $v$. Then, for every cyclic $p$-subgroup $P$ of $\Delta$, we have $h_P\big(\mathcal{H}_v(K_\infty, E)\big) \leq 1$. If $v \in \Phi_{K/F}$, then $h_P\big(\mathcal{H}_v(K_\infty, E)\big) = 1$ for all $P$'s if and only if $\mathcal{H}_v(K_\infty, E) = 0$.*

*Proof.* For any $p$-subgroup $P$ of $\Delta$ and for any $v$, let $P_v$ be the corresponding decomposition subgroup. (Recall that $P_v$ is actually the decomposition subgroup for some prime $\eta$ of $K_\infty$ lying above $v$.) Just as for $\Delta$ itself, we can write $\mathcal{H}_v(K_\infty, E)$ as a direct product of modules of the form $A = \mathrm{Ind}_{P_v}^{P}\big(H^1(K_{\infty,v}, E[p^\infty])\big)$. As a $\mathbf{Z}_p[P_v]$-module, $H^1(K_{\infty,v}, E[p^\infty])$ is a direct summand of $A$. If $v \in \Phi_{K/F}$, then we can choose a cyclic $p$-subgroup $P$ so that $P_v$ is nontrivial.

Part *(i)* is now quite easy. It suffices to show that if $v \in \Phi_{K/F}$, if $P$ is chosen so that $P_v$ is nontrivial, and if $H^1(K_{\infty,v}, E[p^\infty]) \neq 0$, then the Pontryagin dual of $H^1(K_{\infty,v}, E[p^\infty])$ cannot be projective as a $\mathbf{Z}_p[P_v]$-module. Recall that projective $\mathbf{Z}_p[P_v]$-modules must be free. Hence their $\mathbf{Z}_p$-rank must be divisible by $|P_v|$. But the $\mathbf{Z}_p$-corank of $H^1(K_{\infty,v}, E[p^\infty])$ is at most 2 according to proposition 5.1.1. Thus, *(i)* is proven except for the case where $P_v$ has order 2 and $H^0\big(K_{\infty,v}, V_p(E)\big) = V_p(E)$. So we now suppose that $p = 2$. It is clear that $\omega_v|_{P_v}$ is trivial. Thus, a generator of $P_v$ will act on $V_p(E)$ with determinant 1. Therefore, its eigenvalues will either both be equal to 1, or both equal to -1. The same thing will be true for its action on the Pontryagin dual of $H^1(K_{\infty,v}, E[p^\infty])$, and so that $\mathbf{Z}_p[P_v]$-module cannot be projective.

Now consider part *(ii)*. Let $P$ be a cyclic $p$-subgroup of $\Delta$ and let $A$ be as above. Shapiro's lemma implies that the Herbrand quotient $h_P(A)$ is equal to $h_{P_v}\big(H^1(K_{\infty,v}, E[p^\infty])\big)$. Of course, $P_v$ is a subgroup of $\Delta_v$ and could be any cyclic $p$-subgroup. If $P_v$ is nontrivial, then apart from the trivial representation, any irreducible representation for $P_v$ over $\mathbf{Q}_p$ has degree at least $p-1$. Thus, assuming that $p \geq 5$, the action of $P_v$ on the $\mathbf{Q}_p$-vector space $H^0\big(K_{\infty,v}, V_p(E)\big)$ must be trivial. By proposition 5.1.1 and the fact that $H^1(K_{\infty,v}, E[p^\infty])$ is divisible, the action of $P_v$ on that group must also be trivial. Therefore,

$$h_{P_v}\big(H^1(K_{\infty,v}, E[p^\infty])\big) = |P_v|^{-r} \ , \tag{5.3.a}$$

where $r$ denotes the $\mathbf{Z}_p$-corank of $H^1(K_{\infty,v}, E[p^\infty])$, proving the first statement for $p \geq 5$.

If $E$ has good or multiplicative reduction at $v$, then the characters $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ for which $\langle \rho_{E,v}, \chi \rangle > 0$ are of order prime to $p$. Thus, the restriction of such $\chi$'s to a $p$-subgroup will be trivial. That is, for any $P$, the action of $P_v$ on $H^1(K_{\infty,v}, E[p^\infty])$ will again be trivial. Just as above, one has (5.3.a) and the first statement again follows.

If $v \in \Phi_{K/F}$, then one can clearly choose $P$ so that $P_v$ is nontrivial. Furthermore, if $h_P\big(\mathcal{H}_v(K_\infty, E)\big) = 1$, then $h_{P_v}\big(H^1(K_{\infty,v}, E[p^\infty])\big) = 1$. It follows from (5.3.a) that $r = 0$. However, $H^1(K_{\infty,v}, E[p^\infty])$ is a divisible group. Therefore, $H^1(K_{\infty,v}, E[p^\infty]) = 0$, and hence indeed $\mathcal{H}_v(K_\infty, E) = 0$. The other implication in the second assertion is obvious. □

**Remark 5.3.2.** As a complement to the above proposition, we will discuss the second part of the above proposition when $p \leq 3$ and $E$ does not have good or multiplicative reduction at $p$. We use the notation as in the proof. The case of potentially multiplicative reduction is the easiest. Suppose first that $p = 3$. Then $\varphi_v$ is a ramified character of order 2. The action of $P_v$ on $H^1(K_{\infty,v}, E[p^\infty])$ will again be trivial. Hence the proof works without change. We could indeed have included this case in the proposition.

Suppose now that $p = 2$ and that $E$ has potentially multiplicative reduction at $v$. Then $\varphi_v$ is a ramified character of order 2. Since $v \nmid 2$, the character $\varphi_v$ is tamely ramified and hence is uniquely determined. If $v \in \Phi_{K/F}$, then $\varphi_v$ does factor through $\Delta_v$ and has a nontrivial restriction to $P_v$ for some cyclic $p$-subgroup $P$ of $\Delta$. The $\mathbf{Z}_p$-corank of $H^1(K_{\infty,v}, E[p^\infty])$ is equal to 1 and one finds that $h_{P_v}\big(H^1(K_{\infty,v}, E[p^\infty])\big) = p$, Therefore, the first conclusion in part *(ii)* of proposition 5.3.1 could fail in this case. One can easily find examples where $h_P\big(\mathcal{H}_v(K_\infty, E)\big) > 1$.

In the case of potentially good reduction, and $p = 2$ or 3, it might or might not be the case that $|\Theta_v|$ is divisible by $p$. If $p$ doesn't divide $|\Theta_v|$, then the characters $\chi$ for which $\langle \rho_{E,v}, \chi \rangle > 0$ will be of order prime to $p$, and so the proof of proposition 5.3.1 still works. On the other hand, assume that $p$ divides $|\Theta_v|$. If $\varphi_v$ or $\psi_v$ factor through $\Delta_v$, then $\Theta_v$ is isomorphic to a subgroup of $\Delta_v$ and hence, for some $P$, we will have $P_v \subseteq \Theta_v$. The action of $P_v$ on $H^1(K_{\infty,v}, E[p^\infty])$ will then be nontrivial. In such a case, the Herbrand quotient will again be greater than 1. It is then possible to have $h_P\big(\mathcal{H}_v(K_\infty, E)\big) > 1$. This can happen for either $p = 2$ or $p = 3$. ◊

# 6 The case where $\Delta$ is a $p$-group.

Formula (1.3.c) is based on the fact that if $\Delta$ is a $p$-group, then $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ contains only the trivial representation $\tau_0 = \widetilde{\sigma}_0$. By using the results of chapter 5, we can refine that formula. One of the additional simplifying features in this case is that $\Delta_\eta$ will also be a $p$-group for

any prime $\eta$ of $K_\infty$ (reverting back to the notation in the beginning of chapter 5). Assuming that $\eta \mid v$, where $v \nmid p, \infty$, it is clear that $\Delta_\eta$ is actually the inertia subgroup of $\Delta$ for $\eta$. This is because $F_{\infty,v}$ is the unramified $\mathbf{Z}_p$-extension of $F_v$ and hence there are no nontrivial unramified $p$-extensions of $F_{\infty,v}$. Thus $\Delta_\eta$ is nontrivial if and only if $v \in \Phi_{K/F}$. We let $e_\eta = |\Delta_\eta|$, the ramification index for $\eta$ in the extension $K_\infty/F_\infty$. The ramification is tame and so $e_\eta$ divides $N(\eta) - 1$, where $N(\eta)$ denotes the cardinality of the residue field for $\eta$. It follows that if $v \in \Phi_{K/F}$, then $\mu_p \subset K_{\infty,v}$. Since $\Delta_\eta$ is a $p$-group, it acts trivially on $\mu_p$ and hence the character $\omega_v$ is trivial. That is, we have $\mu_p \subset F_{\infty,v}$.

Another simplifying feature is that for $\eta$ and $v$ as above, if $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_\eta)$ is a nontrivial representation, then usually $\langle \rho_{E,v}, \chi \rangle = 0$. This is true if $p \geq 5$ or if $E$ has good or multiplicative reduction at $v$, because, as pointed out in chapter 5, $\langle \rho_{E,v}, \chi \rangle > 0$ implies that $\chi$ factors through a group of order prime to $p$. However, if $p = 2$ or 3, one can sometimes have $\langle \rho_{E,v}, \chi \rangle > 0$ for a nontrivial $\chi$.

We will prove the following proposition. It is assumed that $E$ has good, ordinary reduction at the primes of $F$ lying over $p$. The trivial character of $\Delta_\eta$ is just the restriction of $\sigma_0$, which we will denote by $\sigma_{0,v}$. But we will also sometimes use the notation $\chi_{0,v}$ when it seems more appropriate.

**Proposition 6.1.** *Suppose that $p \geq 5$, that $\Delta$ is a $p$-group. and that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Assume also that $\mathrm{Sel}_E(F_\infty)[p]$ is finite. Let $\Sigma_0 = \Phi_{K/F}$. Then*

$$\lambda_E(\sigma) \;=\; n(\sigma)\lambda_E(\sigma_0) + \sum_{v \in \Sigma_0} g_v\big(n(\sigma) - \langle \sigma_v, \chi_{0,v} \rangle\big)\langle \rho_{E,v}, \chi_{0,v} \rangle \;.$$

*Furthermore, for $v \in \Sigma_0$, $\langle \rho_{E,v}, \chi_{0,v} \rangle = 2$ if $E$ has good reduction at $v$ and $E(F_v)[p] \neq 0$, $\langle \rho_{E,v}, \chi_{0,v} \rangle = 1$ if $E$ has split multiplicative reduction at $v$, and $\langle \rho_{E,v}, \chi_{0,v} \rangle = 0$ otherwise.*

*Proof.* It is proved in [HaMa] that if $\mathrm{Sel}_E(F_\infty)[p]$ is finite, then $\mathrm{Sel}_E(K_\infty)[p]$ is also finite. (See also chapter 4 for an argument using the concept of a Selmer atom.) The other assumptions in proposition 3.2.1 are clearly satisfied and so we can apply formula (1.3.c). Together with formula (5.2.a), we have in general

$$\lambda_E(\sigma) \;=\; n(\sigma)\lambda_E(\sigma_0) \;+\; \sum_{v \in \Sigma_0} g_v \left( \sum_{\chi \in \mathrm{Irr}_v} \big(n(\sigma)\langle \sigma_{0,v}, \chi \rangle - \langle \sigma_v, \chi \rangle\big)\langle \rho_{E,v}, \chi \rangle \right) \;.$$

Since $p \geq 5$, we have $\langle \rho_{E,v}, \chi \rangle = 0$ if $\chi \neq \chi_{0,v}$. Here $\sigma_{0,v} = \sigma_0|_{\Delta_\eta}$ and obviously $\langle \sigma_{0,v}, \chi_{0,v} \rangle = 1$. This gives the formula in the proposition.

Assume that $E$ has good reduction at $v$. Then $\langle \rho_{E,v}, \chi_{0,v} \rangle > 0$ if and only if $\chi_{0,v}$ is equal to $\varphi_v$ or $\psi_v$. However, $\varphi_v \psi_v = \omega_v$, which is trivial, and so $\chi_{0,v} = \varphi_v$ means that both $\varphi_v$ and

$\psi_v$ are equal to $\chi_{0,v}$ and that $\langle \rho_{E,v}, \chi_{0,v} \rangle = 2$. Since the action of $\mathcal{G}_v$ on $E[p]$ is unramified and factors through a group of order prime to $p$, we have the equivalences

$$\langle \rho_{E,v}, \chi_{0,v} \rangle = 2 \quad \Longleftrightarrow \quad \varphi_v = \chi_{0,v} \quad \Longleftrightarrow \quad E(F_{\infty,v})[p] \neq 0 \ .$$

Actually, these statements are equivalent to the assertion that $E[p] \subset E(F_{\infty,v})$. Since $F_{\infty,v}/F_v$ is a $\mathbf{Z}_p$-extension, $E(F_{\infty,v})[p] \neq 0$ if and only if $E(F_v)[p] \neq 0$. Therefore, we see that $\langle \rho_{E,v}, \chi_{0,v} \rangle = 2$ if $E(F_v)[p] \neq 0$ and $\langle \rho_{E,v}, \chi_{0,v} \rangle = 0$ otherwise. The assumption that $p \geq 5$ is not needed for this assertion.

Now assume that $E$ has multiplicative or potentially multiplicative reduction at $v$. Since $\omega_v = \chi_{0,v}$, it follows that $\varphi_v = \chi_{0,v}$ if and only if $E$ has split multiplicative reduction at $v$. Hence $\langle \rho_{E,v}, \chi_{0,v} \rangle = 1$ just in that case and $\langle \rho_{E,v}, \chi_{0,v} \rangle = 0$ otherwise. Again, this assertion is valid for all $p$.

Finally, assume that $E$ has additive reduction at $v$. Then $\langle \rho_{E,v}, \chi \rangle > 0$ implies that $\chi$ is ramified at $v$. Thus, $\chi \neq \chi_{0,v}$. However, if $p \geq 5$, then $\langle \rho_{E,v}, \chi \rangle > 0$ implies that $\chi$ factors through a quotient of $\mathcal{G}_v$ of order prime to $p$. Hence, if $\chi$ also factors through the $p$-group $\Delta_v$, then $\chi = \chi_{0,v}$. Therefore, it follows that $\langle \rho_{E,v}, \chi \rangle = 0$ for all $\chi \in \mathrm{Irr}_v$. $\square$

**Remark 6.1.1.** In the above proposition, suppose that $\Delta$ is a cyclic group of order $p^r$ where $r \geq 1$ and that $\sigma$ is a faithful character of $\Delta$. We also take $\Sigma_0 = \Phi_{K/F}$ and $p \geq 5$. Then the formula takes the following simple form:

$$\lambda_E(\sigma) = \lambda_E(\sigma_0) + \sum_{v \in \Sigma_0} g_v \langle \rho_{E,v}, \chi_{0,v} \rangle \ .$$

This is clear since $n(\sigma) = 1$ and $\sigma_v$ is nontrivial for any $v \in \Phi_{K/F}$. $\Diamond$

**Remark 6.1.2.** The formula proved in [HaMa] follows from proposition 6.1. We make the same assumptions and let $\sigma$ vary over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. We use formulas (1.2.b) and (1.3.c) which give

$$\lambda_E(K_\infty) \ = \ \sum_\sigma n(\sigma) \lambda_E(\sigma) \ = \ \sum_\sigma n(\sigma)^2 \lambda_E(\sigma_0) \ + \ \sum_\sigma n(\sigma)^2 \delta_E^{\Sigma_0}(\sigma_0) \ - \ \sum_\sigma n(\sigma) \delta_E^{\Sigma_0}(\sigma) \ .$$

Of course, $\sum_\sigma n(\sigma)^2 = |\Delta|$ and $\lambda_E(\sigma_0) = \lambda_E(F_\infty)$. Thus, the first sum on the right is equal simply to $|\Delta| \lambda_E(F_\infty)$. The second sum is

$$|\Delta| \sum_{v \in \Sigma_0} g_v \langle \rho_{E,v}, \chi_{0,v} \rangle \ = \ \sum_{v \in \Sigma_0} [\Delta : \Delta_\eta] g_v e_\eta \langle \rho_{E,v}, \chi_{0,v} \rangle \ .$$

Note that for each $v \in \Sigma_0$, the quantity $[\Delta : \Delta_\eta]g_v$ is equal to the cardinality of the set of primes of $K_\infty$ lying over $v$. The third sum is

$$\sum_\sigma n(\sigma)\delta_E^{\Sigma_0}(\sigma) \;=\; \sum_{v\in\Sigma_0} g_v\langle\rho_{E,v},\chi_{0,v}\rangle\left(\sum_\sigma n(\sigma)\langle\sigma_v,\chi_{0,v}\rangle\right) \;=\; \sum_{v\in\Sigma_0}\langle\rho_{E,v},\chi_{0,v}\rangle g_v[\Delta:\Delta_\eta]$$

since $\langle\sigma_v,\chi_{0,v}\rangle$ is the multiplicity of $\sigma$ in the induced representation $\mathrm{Ind}_{\Delta_\eta}^{\Delta}(\chi_{0,v})$ and the dimension of that representation is $[\Delta:\Delta_\eta]$. Thus the second and third contributions are

$$\sum_{v\in\Sigma_0}\langle\rho_{E,v},\chi_{0,v}\rangle[\Delta:\Delta_\eta]g_v\big(e_\eta-1\big)\ .$$

Therefore, the formula that we derive is

$$\lambda_E(K_\infty) \;=\; |\Delta|\lambda_E(F_\infty) \;+\; \sum_{\eta\in\Sigma_1}(e_\eta-1) \;+\; 2\sum_{\eta\in\Sigma_2}(e_\eta-1)$$

where $\Sigma_1$ denotes the set of primes of $K_\infty$ lying over a $v\in\Sigma_0$ where $E$ has split multiplicative reduction and $\Sigma_2$ denotes the set of primes of $K_\infty$ lying over a $v\in\Sigma_0$ where $E$ has good reduction and $E(F_v)[p]\neq 0$. This is exactly the formula proved in [HaMa].

Conversely, the formula proved in [HaMa] implies proposition 6.1. One must apply the formula to all intermediate fields $F'$ for the $p$-extension $K/F$. The non-primitive version of that formula takes the following form:

$$\lambda_E^{\Sigma_0}(F'_\infty) \;=\; [F':F]\lambda_E^{\Sigma_0}(F_\infty) \;=\; [F':F]\lambda_E^{\Sigma_0}(\sigma_0)\ .$$

This is valid even if $F'/F$ is not Galois since there will be a tower of subfields of $F'$, starting from $F$, ending with $F'$, each Galois over the preceding field. This is so because $\Delta$ is a $p$-group. If $\Delta' = \mathrm{Gal}(K/F')$, then it follows that

$$\lambda_E^{\Sigma_0}(\mathbf{1}_{\Delta'}) \;=\; [\Delta:\Delta']\lambda_E^{\Sigma_0}(\sigma_0)\quad .$$

The characters of irreducible representation of $\Delta$ over $\mathbf{Q}$ can be expressed as linear combinations of the characters for the induced representations $\mathrm{Ind}_{\Delta'}^{\Delta}(\mathbf{1}_{\Delta'})$. Using this together with the second part of remark 2.1.8, one deduces that

$$\sum_\sigma\ \lambda_E^{\Sigma_0}(\sigma) \;=\; \left(\sum_\sigma n(\sigma)\right)\lambda_E^{\Sigma_0}(\sigma_0)\quad ,$$

where $\sigma$ varies over any $\mathbf{Q}$-conjugacy class of irreducible representations of $\Delta$. However, if $\sigma_1$ and $\sigma_2$ are conjugate over $\mathbf{Q}$, then they are also conjugate over $\mathbf{Q}_p$ and hence it follows that $\lambda_E^{\Sigma_0}(\sigma_1) = \lambda_E^{\Sigma_0}(\sigma_2)$. Of course, $n(\sigma_1) = n(\sigma_2)$ too. Therefore, we indeed have

$$\lambda_E^{\Sigma_0}(\sigma) = n(\sigma)\lambda_E^{\Sigma_0}(\sigma_0)$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. $\Diamond$

**Remark 6.1.3.** We will discuss the dihedral group $\Delta = D_{2p^r}$ here because it requires just a simple application of remark 6.1.1. We still assume that $p \geq 5$. The quadratic extension of $F$ contained in $K$ is $K^{\Pi}$, the fixed field for the Sylow $p$-subgroup $\Pi$ of $\Delta$, which we will denote by $K_0$. The order of $\Pi$ is $p^r$. Suppose that $r \geq 1$ and that $\sigma$ is a faithful element of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. Then $\sigma = \mathrm{Ind}_{\Pi}^{\Delta}(\pi)$, where $\pi$ is a faithful character of $\Pi$. We have $\lambda_E(\pi) = \lambda_E(\sigma)$ and $\lambda_E(\pi_0) = \lambda_E(\sigma_0) + \lambda_E(\sigma_1)$, where $\sigma_0$ and $\sigma_1$ are the two 1-dimensional representations of $\Delta$ and $\pi_0$ is the trivial character of $\Pi$. (See remark 2.1.8.) Applying remark 6.1.1 to $\pi$, we obtain the formula

$$\lambda_E(\sigma) = \lambda_E(\sigma_0) + \lambda_E(\sigma_1) + \sum_{v \in \Sigma_0} g_v\big(\langle \rho_{E,v}, \sigma_{0,v}\rangle + \langle \rho_{E,v}, \sigma_{1,v}\rangle\big) \quad .$$

There may be one or two primes of $K_0$ lying above each $v$, and one checks both possibilities to verify this formula. Note that, in remark 6.1.1, the $g_v$ is $g_v(K_0)$, whereas in the formula just stated, $g_v = g_v(F)$. $\Diamond$

# 7 Other specific groups.

We will discuss the determination of congruence relations for certain groups $\Delta$ and primes $p$. As previously, the trivial representations of $\Delta$ over $\mathcal{F}$ and $\mathfrak{f}$ will always be denoted by $\sigma_0$ and $\tau_0$, respectively. The other representations will be denoted with double-subscripts $\boldsymbol{n}, i$, where $\boldsymbol{n}$ indicates the dimension $n(\sigma)$ or $n(\tau)$, written in boldface, and where $i \geq 1$. However, if there is only one nontrivial representation of a given dimension, we will suppress the second subscript.

In section 7.1, we first consider the solvable groups $A_4$ and $S_4$. For any prime $p$, they are $p$-solvable and that simplifies the discussion. We also discuss the non-solvable group $S_5$. In each example, we will specify the smallest field $\mathcal{F}$ over which the representations are realizable, possibly significantly smaller than the $\mathcal{F}$ specified in the introduction. In section 7.2, we discuss the group $PGL_2(\mathbf{Z}/p\mathbf{Z})$ and describe the representation theory and congruence relations rather completely. In sections 7.3 and 7.4, we discuss interesting families

of groups which will come up in some of our later illustrations. However, although the discussion will include many of the irreducible representations of those groups, it is still somewhat incomplete.

One fact in modular representation theory that we will use frequently has to do with induced representations. Suppose that $\Theta$ is a subgroup of $\Delta$. One can regard $\mathrm{Ind}_\Theta^\Delta$ as a homomorphism from $\mathcal{R}_\mathcal{F}(\Theta)$ to $\mathcal{R}_\mathcal{F}(\Delta)$ or as a homomorphism from $\mathcal{R}_\mathfrak{f}(\Theta)$ to $\mathcal{R}_\mathfrak{f}(\Delta)$. Those induction maps commute with the decomposition maps for the groups $\Theta$ and $\Delta$. One can find a proof of this commutativity on page 502 in [CuRe], volume 1. We will often use the following consequence.

*Suppose that $\theta_1$ and $\theta_2$ are representations of $\Theta$. Let $\rho_1 = \mathrm{Ind}_\Theta^\Delta(\theta_1)$ and $\rho_2 = \mathrm{Ind}_\Theta^\Delta(\theta_2)$. If $\widetilde{\theta_1}^{ss} \cong \widetilde{\theta_2}^{ss}$, then $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$.*

We want to give an alternative justification here by using character theory. As in [Se77], let $\Delta_{reg}$ denote the set of elements of $\Delta$ whose order is prime to $p$. Define $\Theta_{reg}$ in the same way. If $\chi$ is a character of a representation $\rho$ over $\mathcal{F}$, then Brauer proved that $\widetilde{\rho}^{ss}$ is determined up to isomorphism by $\chi|_{\Delta_{reg}}$. This is corollary 1 to theorem 42 in [Se77]. Furthermore, if $\rho = \mathrm{Ind}_\Theta^\Delta(\theta)$, then there is a standard formula for $\chi$ in terms of the character $\psi$ of $\theta$. That formula shows that $\chi|_{\Delta_{reg}}$ is determined by $\psi|_{\Theta_{reg}}$. Therefore, up to isomorphism, $\widetilde{\rho}^{ss}$ is determined by $\widetilde{\theta}^{ss}$.

## 7.1 The groups $A_4$, $S_4$, and $S_5$.

**A.** $\Delta = A_4$. We have $s = 4$. We can take $\mathcal{F} = \mathbf{Q}(\mu_3)$. The elements of $\mathrm{Irr}_\mathcal{F}(\Delta)$ are $\sigma_0$, $\sigma_{\mathbf{1},1}$ and $\sigma_{\mathbf{1},2}$ (the last two of which are the characters of order 3), and $\sigma_\mathbf{3}$ (of dimension 3). The group $\Delta$ has a normal subgroup $\Pi$ of order 4, the Klein 4-group, and $\sigma_\mathbf{3} \cong \mathrm{Ind}_\Pi^\Delta(\chi)$, where $\chi$ is any one of the three nontrivial characters of $\Pi$. Note that $\sigma_\mathbf{3}$ is defined over $\mathbf{Q}$. The prime divisors of $|\Delta|$ are 2 and 3. The determinant of $\sigma_\mathbf{3}$ is $\sigma_0$.

Consider first $p = 2$. Then $\mathfrak{f} = \mathbf{F}_4$ and $t = 3$. The three elements of $\mathrm{Irr}_\mathfrak{f}(\Delta)$ factor through the abelian quotient group $\Delta/\Pi$ and are $\tau_0 = \widetilde{\sigma_0}$, $\tau_{\mathbf{1},1} = \widetilde{\sigma_{\mathbf{1},1}}$, and $\tau_{\mathbf{1},2} = \widetilde{\sigma_{\mathbf{1},2}}$. We have $\widetilde{\sigma_\mathbf{3}}^{ss} \cong \tau_0 \oplus \tau_{\mathbf{1},1} \oplus \tau_{\mathbf{1},2}$. Thus, for any projective $\mathbf{Z}_2[\Delta]$-module $X$, we have the congruence relation

$$\lambda(X, \sigma_\mathbf{3}) \;=\; \lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{1},1}) + \lambda(X, \sigma_{\mathbf{1},2})$$

This equation becomes fairly obvious if one uses the fact that $X$ must be a free $\mathbf{Z}_2[\Pi]$-module. Its $\mathbf{Z}_2[\Pi]$-rank $r$ will be equal to the $\mathbf{Z}_p$-rank of $X^\Pi$, and that is just the sum of the multiplicities of the 1-dimensional representations $\sigma_0$, $\sigma_{\mathbf{1},1}$ and $\sigma_{\mathbf{1},2}$ in $V_\mathcal{F} = X \otimes_{\mathbf{Z}_p} \mathcal{F}$.

But $\dim_{\mathcal{F}}(V_{\mathcal{F}}) = 4r$ and hence the contribution of the 3-dimensional representation $\sigma_{\mathbf{3}}$ has $\mathcal{F}$-dimension $3r$, and therefore multiplicity $r$. Note that we also have the conjugacy relation $\lambda(X, \sigma_{\mathbf{1},1}) = \lambda(X, \sigma_{\mathbf{1},2})$.

For $p = 3$, we have $t = 2$ and $\mathfrak{f} = \mathbf{F}_3$. The two elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are $\tau_0 = \widetilde{\sigma_0}$ and $\tau_{\mathbf{3}} = \widetilde{\sigma_{\mathbf{3}}}$. We have $\widetilde{\sigma_{\mathbf{1},1}} \cong \widetilde{\sigma_{\mathbf{1},2}} \cong \tau_0$. Thus, for a projective $\mathbf{Z}_3[\Delta]$-module $X$, we have the two congruence relations

$$\lambda(X, \sigma_0) = \lambda(X, \sigma_{\mathbf{1},1}) = \lambda(X, \sigma_{\mathbf{1},2})$$

which are also obvious from the fact that $\sigma_0, \sigma_{\mathbf{1},1}$ and $\sigma_{\mathbf{1},2}$ factor through the quotient $\Delta/\Pi$, a 3-group. The second equality is also a conjugacy relation.

**B.** $\Delta = S_4$. We have $s = 5$ and can take $\mathcal{F} = \mathbf{Q}$. The elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are $\sigma_0$ and $\sigma_{\mathbf{1}}$, both one-dimensional (the trivial and sign characters), one two-dimensional representation $\sigma_{\mathbf{2}}$, whose kernel is the Klein 4-group $\Pi$, and two three-dimensional representations $\sigma_{\mathbf{3},1}$ and $\sigma_{\mathbf{3},2} = \sigma_{\mathbf{3},1} \otimes \sigma_{\mathbf{1}}$. Those two representations are induced from nontrivial characters of a Sylow 2-subgroup of $\Delta$. We let $\sigma_{\mathbf{3},1}$ be the representation whose determinant is $\sigma_0$. Thus, $det(\sigma_{\mathbf{3},2}) = \sigma_{\mathbf{1}}$.

First $p = 2$. We have $t = 2$. The elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are $\tau_0$ and a 2-dimensional representation $\tau_{\mathbf{2}} = \widetilde{\sigma_{\mathbf{2}}}$. Clearly, $\widetilde{\sigma_0} \cong \widetilde{\sigma_{\mathbf{1}}} \cong \tau_0$. Also, $\widetilde{\sigma_{\mathbf{3},1}}^{ss} \cong \widetilde{\sigma_{\mathbf{3},2}}^{ss} \cong \tau_0 \oplus \tau_{\mathbf{2}}$. The three independent congruence relations for a projective $\mathbf{Z}_2[\Delta]$-module $X$ are

$$\lambda(X, \sigma_{\mathbf{1}}) = \lambda(X, \sigma_0), \qquad \lambda(X, \sigma_{\mathbf{3},1}) = \lambda(X, \sigma_{\mathbf{3},2}) = \lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{2}}).$$

For $p = 3$, we have $t = 4$. There are two elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ of dimension 1, namely $\tau_0 = \widetilde{\sigma_0}$ and $\tau_{\mathbf{1}} = \widetilde{\sigma_{\mathbf{1}}}$, and two representations of dimension 3, namely $\tau_{\mathbf{3},1} = \widetilde{\sigma_{\mathbf{3},1}}$ and $\tau_{\mathbf{3},2} = \widetilde{\sigma_{\mathbf{3},2}}$. We have $\widetilde{\sigma_{\mathbf{2}}}^{ss} \cong \tau_0 \oplus \tau_{\mathbf{1}}$. For a projective $\mathbf{Z}_3[\Delta]$-module $X$, we have

$$\lambda(X, \sigma_{\mathbf{2}}) = \lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{1}}) \ ,$$

which is actually just the congruence relation for the projective $\mathbf{Z}_3[\Delta/\Pi]$-module $X^{\Pi}$.

**C.** $\Delta = S_5$. We have $s = 7$ and can take $\mathcal{F} = \mathbf{Q}$. The elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are of dimensions 1, 4, 5, and 6, two of each dimension except for 6. We denote them by $\sigma_0$, $\sigma_{\mathbf{1}}$, $\sigma_{\mathbf{4},1}$, $\sigma_{\mathbf{4},2}$, $\sigma_{\mathbf{5},1}$, $\sigma_{\mathbf{5},2}$, and $\sigma_{\mathbf{6}}$. Tensoring by $\sigma_{\mathbf{1}}$ interchanges the two representations of each of the dimensions 1, 4, and 5. We identity $S_4$ with a subgroup $H$ of $S_5$ in any way. Thus, we can regard $S_5$ as the group of permutations on the left cosets of $H$ in $S_5$. Choose $\sigma_{\mathbf{4},1}$ so that its restriction to $H$ contains the trivial representation. That is, $\sigma_{\mathbf{4},1}$ is the 4-dimensional irreducible constituent in the permutation representation $\mathrm{Ind}_H^{S_5}(\mathbf{1}_H)$.

Its determinant is $\sigma_{\mathbf{1}}$. Of course, $\sigma_{\mathbf{4},2}$ has the same determinant. The determinant of $\sigma_{\mathbf{6}}$ is also $\sigma_{\mathbf{1}}$. However, it will be convenient to take $\sigma_{\mathbf{5},1}$ to be the 5-dimensional irreducible representation with determinant $\sigma_0$. And so the determinant of $\sigma_{\mathbf{5},2}$ will be $\sigma_{\mathbf{1}}$. A reference for the decomposition matrix information that we will now cite is [J-K], which contains useful tables for the symmetric groups.

For $p = 2$, we have $t = 3$. The elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are of dimension 1 and 4: $\tau_0, \tau_{\mathbf{4},1}$ and $\tau_{\mathbf{4},2}$. In fact, $\widetilde{\sigma_{\mathbf{4},1}}$ is irreducible and we take that reduction to be $\tau_{\mathbf{4},1}$. We also have $\widetilde{\sigma_{\mathbf{4},2}} \cong \tau_{\mathbf{4},1}$. As for $\tau_{\mathbf{4},2}$, it isn't of the form $\widetilde{\sigma}$ for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, but it is a direct summand in $\widetilde{\sigma_{\mathbf{5},1}}^{ss}$, $\widetilde{\sigma_{\mathbf{5},2}}^{ss}$, and $\widetilde{\sigma_{\mathbf{6}}}^{ss}$. The complementary summands are $\tau_0$'s. Thus, we have the following congruence relations for a projective $\mathbf{Z}_2[\Delta]$-module $X$:

$$\lambda(X, \sigma_{\mathbf{1}}) = \lambda(X, \sigma_0), \qquad \lambda(X, \sigma_{\mathbf{4},2}) = \lambda(X, \sigma_{\mathbf{4},1}), \qquad \lambda(X, \sigma_{\mathbf{5},2}) = \lambda(X, \sigma_{\mathbf{5},1})$$

$$\lambda(X, \sigma_{\mathbf{6}}) = \lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{5},1}) \ .$$

In this example, $\tau_0$ and $\tau_{\mathbf{4},1}$ have liftings $\sigma_0$ and $\sigma_{\mathbf{4},1}$, respectively, and so we recover the corresponding weights quite easily: $w(X, \tau_0) = \lambda(X, \sigma_0)$, $w(X, \tau_{\mathbf{4},1}) = \lambda(X, \sigma_{\mathbf{4},1})$. However, for $\tau_{\mathbf{4},2}$, we have $w(X, \tau_{\mathbf{4},2}) = \lambda(X, \sigma_{\mathbf{5},1}) - \lambda(X, \sigma_0)$.

If $p = 3$, then $t = 5$. The elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are of dimension 1, 4, and 6, two of each dimension except 6. All of the elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ can be lifted to elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ (even though $S_5$ is not 3-solvable). They are $\tau_0 = \widetilde{\sigma_0}$, $\tau_{\mathbf{1}} = \widetilde{\sigma_{\mathbf{1}}}$, $\tau_{\mathbf{4},1} = \widetilde{\sigma_{\mathbf{4},1}}$, $\tau_{\mathbf{4},2} = \widetilde{\sigma_{\mathbf{4},2}}$, and $\tau_{\mathbf{6}} = \widetilde{\sigma_{\mathbf{6}}}$. The 5-dimensional representations of $\Delta$ have reducible reductions: $\widetilde{\sigma_{\mathbf{5},1}}^{ss} \cong \tau_{\mathbf{4},1} \oplus \tau_{\mathbf{1}}$ and $\widetilde{\sigma_{\mathbf{5},2}}^{ss} \cong \tau_{\mathbf{4},2} \oplus \tau_0$. Thus, for a projective $\mathbf{Z}_3[\Delta]$-module $X$, the congruence relations are

$$\lambda(X, \sigma_{\mathbf{5},1}) = \lambda(X, \sigma_{\mathbf{1}}) + \lambda(X, \sigma_{\mathbf{4},1}), \qquad \lambda(X, \sigma_{\mathbf{5},2}) = \lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{4},2}) \ .$$

In this example, every $\tau$ in $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ has a unique lifting $\sigma$ in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and we then have $w(X, \tau) = \lambda(X, \sigma)$.

For $p = 5$, we have $t = 6$. However, $S_5 \cong PGL_2(\mathbf{F}_5)$. This example is included in the next section which considers the family of groups $PGL_2(\mathbf{F}_p)$, where $p$ is any odd prime. In fact, $S_4 \cong PGL_2(\mathbf{F}_3)$, which was already discussed above for $p = 3$ and is also a special case of section 7.2.

**D.** *Blocks.* We want to briefly discuss an important aspect of modular representation theory, although it will not play a real role in the present paper. It does shed some light on congruence relations. For a given finite group $\Delta$ and a prime $p$, the sets $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ can both be partitioned into blocks in a standard way. This corresponds to writing the matrix $D_p(\Delta)$ in a block form. Let $\mathcal{S}_1, ..., \mathcal{S}_k$ denote the distinct blocks in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$, $\mathcal{T}_1, ..., \mathcal{T}_k$ the corresponding blocks in $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. For each $i$ (with $1 \leq i \leq k$), if $\sigma$ is in $\mathcal{S}_i$, then every $\tau$

such that $d(\sigma,\tau) > 0$ will be in $\mathcal{T}_i$. If $\tau \in \mathcal{T}_i$, then every $\sigma$ such that $d(\sigma,\tau) > 0$ will be in $\mathcal{S}_i$. The blocks provide the finest partitions of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ with these two properties. (We refer the reader to chapter 9 in [CuRe] for a complete discussion.)

If $s_i = |\mathcal{S}_i|$ and $t_i = |\mathcal{T}_i|$, then the corresponding submatrix in $D_p(\Delta)$ is a $t_i \times s_i$ matrix. The rank of that submatrix is $t_i$ because $\sum_{i=1}^{k} t_i = t$ and the matrix $D_p(\Delta)$ itself has rank $t$ according to the theorem of Brauer cited in section 1.1. Therefore, we have $t_i \leq s_i$ for all $i$. The congruence relations can be found block-by-block, each block $\mathcal{S}_i$ contributing $s_i - t_i$ independent relations.

For the groups $A_4$ and $S_4$, the congruence relations involve just the irreducible representations of the block that contains the trivial representation $\sigma_0$, the so-called *"principal block"*. However, for $S_5$ and $p = 2$, there are two blocks and the non-principal block $\{\sigma_{\mathbf{4},1}, \sigma_{\mathbf{4},2}\}$ gives one of the four congruence relations. The other three come from the principal block $\{\sigma_0, \sigma_{\mathbf{1}}, \sigma_{\mathbf{5},1}, \sigma_{\mathbf{5},2}, \sigma_{\mathbf{6}}\}$. For $p = 3$, there are three blocks and the two congruence relations come from the principal block and the block for $\sigma_{\mathbf{1}}$. Those two blocks are $\{\sigma_0, \sigma_{\mathbf{4},2}, \sigma_{\mathbf{5},2}\}$ and $\{\sigma_{\mathbf{1}}, \sigma_{\mathbf{4},1}, \sigma_{\mathbf{5},1}\}$. The third block is simply $\{\sigma_{\mathbf{6}}\}$.

Other illustrations involving congruence relations and blocks are discussed in remark 7.2.8, remark 7.3.2, and at the end of part **B** of section 7.4.

## 7.2 The group $PGL_2(\mathbf{F}_p)$.

We consider $\Delta = PGL_2(\mathbf{F}_p)$, where $p$ is any odd prime. We will discuss in some detail the modular representation theory for $\Delta$ and for the prime $p$.

**A.** *Representations in characteristic 0.* First we describe thet irreducible representations of $\Delta$ over a sufficiently large field $\mathcal{F}$ (of characteristic zero). They are of dimension 1, $p-1$, $p$ and $p+1$. By counting characteristic polynomials, one finds that $s = p+2$. The commutator subgroup $\Delta'$ of $\Delta$ has index 2 and so there are two elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ of dimension 1, the two characters $\sigma_0$ and $\sigma_{\mathbf{1}}$ which factor through $\Delta/\Delta'$. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, then so is $\sigma \otimes \sigma_{\mathbf{1}}$, which has the same dimension. One of the two $p$-dimensional elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ is the Steinberg representation. We denote this by $\sigma_{st}$. It can be defined by the isomorphism $\sigma_0 \oplus \sigma_{st} \cong \mathrm{Ind}_B^{\Delta}(\mathbf{1}_B)$, where $B$ denotes the image of the group of upper triangular matrices in $\Delta$ and $\mathbf{1}_B$ is the trivial representation of $B$. Viewing $\mathrm{Ind}_B^{\Delta}(\mathbf{1}_B)$ as the permutation representation of $\Delta$ on the set of 1-dimensional subspaces of $\mathbf{F}_p^2$, one easily sees that the determinant of $\sigma_{st}$ is $\sigma_{\mathbf{1}}$. The other $p$-dimensional irreducible representation of $\Delta$ is $\sigma_{st} \otimes \sigma_{\mathbf{1}}$ which has determinant $\sigma_0$. We will let $\sigma_{\boldsymbol{p},1} = \sigma_{st} \otimes \sigma_{\mathbf{1}}$ and $\sigma_{\boldsymbol{p},2} = \sigma_{st}$.

All of the other elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ have even dimension. There are $\frac{p-3}{2}$ of dimension $p+1$, which we denote by $\sigma_{\boldsymbol{p+1},j}$, where $1 \leq j \leq \frac{p-3}{2}$. These are of the form $\mathrm{Ind}_B^{\Delta}(\psi)$ where $\psi$

is a 1-dimensional character of $B$ such that $\psi \neq \psi^{-1}$. Both $\psi$ and $\psi^{-1}$ give the same induced representation. To make the notation more precise, we will define a canonical character $\beta : B \longrightarrow \mathbf{Z}_p^\times$ and then we let $\sigma_{\boldsymbol{p+1},j}$ denote $\mathrm{Ind}_B^\Delta(\beta^j)$ for $1 \leq j \leq \frac{p-3}{2}$. The definition of $\beta$ is very simple and natural. Consider the action by inner automorphisms of $B$ on its Sylow $p$-subgroup $\Pi$, a normal subgroup of $B$ of order $p$. That action defines a homomorphism $\widetilde{\beta} : B \longrightarrow \mathbf{F}_p^\times$ whose kernel is $\Pi$. Thus, if $b \in B$ is represented by the matrix $\begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}$, then $\widetilde{\beta}(b) = b_{11}b_{22}^{-1}$. Define the character $\beta : B \longrightarrow \mathbf{Z}_p^\times$ to be the unique lifting of $\widetilde{\beta}$. Thus, $\beta$ is a character of $B$ of order $p-1$ and hence $\psi = \beta^j$ satisfies $\psi \neq \psi^{-1}$ for $1 \leq j \leq \frac{p-3}{2}$.

As for the elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ of dimension $p-1$, there are $\frac{p-1}{2}$ of those, which we denote by $\sigma_{\boldsymbol{p-1},j}$, where $1 \leq j \leq \frac{p-1}{2}$. To make the notation more precise for those representations, we will first need to consider their reductions modulo $\mathfrak{m}$. The following result will be helpful for that purpose. Since $s - t = 1$ in this example, it will also give the one independent congruence relation that exists.

**Proposition 7.2.1.** *Suppose that $\Delta = PGL_2(\mathbf{F}_p)$, where $p$ is an odd prime. Then we have*

$$\widetilde{\sigma_0} \oplus \widetilde{\sigma_{\mathbf{1}}} \oplus \bigoplus_{j=1}^{\frac{p-3}{2}} \widetilde{\sigma_{\boldsymbol{p+1},j}}^{ss} \;\cong\; \bigoplus_{j=1}^{\frac{p-1}{2}} \widetilde{\sigma_{\boldsymbol{p-1},j}}^{ss}.$$

*Consequently, if $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module, then we have the congruence relation*

$$\lambda(X, \sigma_0) + \lambda(X, \sigma_{\mathbf{1}}) + \sum_{j=1}^{\frac{p-3}{2}} \lambda(X, \sigma_{\boldsymbol{p+1},j}) \;=\; \sum_{j=1}^{\frac{p-1}{2}} \lambda(X, \sigma_{\boldsymbol{p-1},j}).$$

*Proof.* Let $B$ and $\Pi$ be as above. The group $B$ has $p-1$ representations of dimension 1, namely the distinct powers of the character $\beta$, as well as one irreducible representation of dimension $p-1$, which we will denote by $\gamma$ in this proof. Let $\beta_0$ denote the trivial representation. The other *"self-inverse"* character of $B$ is $\beta^{\frac{p-1}{2}}$. But this coincides with $\sigma_{\mathbf{1}}|_B$ and so we will denote it simply by $\beta_{\mathbf{1}}$. The representation $\gamma$ is $\mathrm{Ind}_\Pi^B(\pi)$, where $\pi$ is any nontrivial character of $\Pi$. Frobenius reciprocity implies that $\sigma_{\boldsymbol{p+1},j}|_B$ has $\beta^j$ and $\beta^{-j}$ as its 1-dimensional constituents and hence $\gamma$ as another constituent, all with multiplicity 1. If $\sigma$ is any one of the elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ of dimension $p-1$, then $\sigma|_B$ has no 1-dimensional constituents and hence must be precisely $\gamma$. The restriction of the 1-dimensional representations to $B$ are obvious (namely, $\beta_0$ and $\beta_{\mathbf{1}}$), and the restrictions of $\sigma_{\boldsymbol{p},1}$ or $\sigma_{\boldsymbol{p},2}$ to

$B$ contain $\gamma$ as one constituent and $\beta_1$ or $\beta_0$, respectively, as the other, all with multiplicity 1. Thus, every element of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ occurs in $\mathrm{Ind}_{\Pi}^{\Delta}(\pi) = \mathrm{Ind}_{B}^{\Delta}(\gamma)$ with multiplicity 1, except for $\sigma_0$ and $\sigma_{\mathbf{1}}$ which don't occur at all.

On the other hand, if $\pi_0$ denotes the trivial character of $\Pi$, then every 1-dimensional representation of $B$ occurs as a constituent in $\mathrm{Ind}_{\Pi}^{B}(\pi_0)$ with multiplicity 1, but $\gamma$ does not occur. Therefore, the representations $\sigma_0,\ \sigma_{\mathbf{1}},\ \sigma_{\boldsymbol{p},1},\ \sigma_{\boldsymbol{p},2}$ occur with multiplicity 1 in $\mathrm{Ind}_{\Pi}^{\Delta}(\pi_0)$, each of the $\sigma_{\boldsymbol{p+1},j}$'s occur with multiplicity 2, but none of the $\sigma_{\boldsymbol{p-1},j}$'s occur.

Now, as representations of $\Pi$, we have $\widetilde{\pi} \cong \widetilde{\pi}_0$. Thus, if we consider the definition of the induced representation by monomial matrices, it is clear that

$$\widetilde{\mathrm{Ind}_{\Pi}^{\Delta}(\pi)}^{ss} \ \cong\ \widetilde{\mathrm{Ind}_{\Pi}^{\Delta}(\pi_0)}^{ss}.$$

If we compare the constituents and their multiplicities, as described above, then we obtain the stated isomorphism. The congruence relation follows immediately. $\square$

**Remark 7.2.2.** It is worth pointing out that the irreducible representations of $B$ are the 1-dimensional representations $\beta^j$, where $0 \leq j \leq p-2$, and the single $(p-1)$-dimensional representation $\gamma$ which occurred in the above proof. $\lozenge$

**Remark 7.2.3.** Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Then $det(\sigma)$ is determined by $\sigma|_B$. Of course, $det(\sigma)$ is either $\sigma_0$ or $\sigma_{\mathbf{1}}$. We already know $det(\sigma)$ for the four odd-dimensional $\sigma$'s. If $\gamma$ is as above, then $det(\gamma) = \sigma_{\mathbf{1}}|_B$. The remarks in the above proof about $\sigma|_B$ imply that $det(\sigma) = \sigma_{\mathbf{1}}$ when $n(\sigma) = p{+}1$ or $p-1$. Thus, the determinant of all the even-dimensional and two of the four odd-dimensional elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ is equal to $\sigma_{\mathbf{1}}$. $\lozenge$

**B.** *Characteristic p.* Now we come to the irreducible representations of $\Delta$ in characteristic $p$. The elements of order $p$ in $\Delta$ form one conjugacy class, represented by any generator of $\Pi$. All other elements of $\Delta$ have order prime to $p$. Thus, we have $t = p{+}1$. The elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are of odd dimensions varying from 1 to $p$, two for each such dimension, interchanged by tensoring by the nontrivial character of dimension 1. We denote them by $\tau_{\boldsymbol{j},k}$ where $j \in \{1, 3, ..., p\}$ and $k \in \{1, 2\}$. The two 1-dimensional irreducible representations will also be denoted, as usual, just by $\tau_0$ and $\tau_{\mathbf{1}}$. For each possible dimension $j$, one of the representations has determinant $\tau_0$ and we denote that by $\tau_{\boldsymbol{j},1}$. Thus, $\tau_{\boldsymbol{j},2}$ has determinant $\tau_{\mathbf{1}}$. All of these representations are defined over $\mathbf{F}_p$ and will be described in terms of the symmetric powers of the tautological 2-dimensional representation of $GL_2(\mathbf{F}_p)$. For any $n \geq 0$, let $sym^n$ denote the $n$-th symmetric power. We will view $sym^n$ in the following way. Let $\mathcal{P}_n$ be the $\mathbf{F}_p$-subspace of the polynomial ring $\mathbf{F}_p[x, y]$ consisting of all homogeneous polynomials of degree $n$. Then $GL_2(\mathbf{F}_p)$ acts on $\mathcal{P}_n$ by linear substitutions. The $\mathbf{F}_p$-dimension of $\mathcal{P}_n$ is $n+1$. In order to obtain representations which factor through the quotient group $\Delta = PGL_2(\mathbf{F}_p)$, we

must twist by a suitable power of the determinant homomorphism $det : GL_2(\mathbf{F}_p) \longrightarrow \mathbf{F}_p^\times$. This is possible if $n$ is even. For any $j \in \{1, 3, ..., p\}$, we define

$$\tau_{\boldsymbol{j},1} \;=\; sym^{j\text{-}1} \otimes det^{-\frac{j-1}{2}}, \qquad\qquad \tau_{\boldsymbol{j},2} \;=\; \tau_{\boldsymbol{j},1} \otimes \tau_{\mathbf{1}} \quad .$$

The determinant of $\tau_{\boldsymbol{j},1}$, as just defined, is indeed seen to be $\tau_0$. Note that $\tau_{\mathbf{1}} = det^{\frac{p-1}{2}}$ and so $\tau_{\boldsymbol{j},2}$ is also a twist of $sym^{j\text{-}1}$ by a suitable power of $det$.

It will be useful to have a somewhat different characterization for the elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. We consider their restrictions to $B$ and to the $p$-subgroup $\Pi$. Let $u$ be the generator of $\Pi$ represented by the matrix $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, where 1 is written for the identity in $\mathbf{F}_p$. Suppose that $0 \leq n \leq p-1$ and that $n$ is even. The underlying vector space for $sym^n \otimes det^{-\frac{n}{2}}$ will be denoted by $\mathcal{P}_n(-\frac{n}{2})$. There is a descending filtration on that space defined by the subspaces $(u - id_P)^k \mathcal{P}_n(-\frac{n}{2})$ for $0 \leq k \leq n+1$. Each of these subspaces is invariant under the action of $B$ and has codimension 1 in the preceding subspace. This filtration is the unique composition series for $\mathcal{P}_n(-\frac{n}{2})$ as a representation space for $\Pi$, and also for $B$. The top subquotient $\mathcal{P}_n(-\frac{n}{2})/(u - id_P)\mathcal{P}_n(-\frac{n}{2})$ is represented by $y^n$, the next subquotient is represented by $xy^{n-1}$, etc. The bottom subquotient is $(u - id_P)^n \mathcal{P}_n(-\frac{n}{2})$ and is represented by $x^n$, which is killed by $u - 1$. Note that if $b \in B$ is represented by a diagonal matrix with diagonal entries $b_{11}, b_{22}$, then all the monomials $x^i y^j$, where $i + j = n$, are eigenvectors for $b$. The eigenvalue for $y^n$ is $b_{22}^n (b_{11} b_{22})^{-\frac{n}{2}} = \widetilde{\beta}(b)^{-\frac{n}{2}}$. The eigenvalue for $x^n$ is $\widetilde{\beta}(b)^{\frac{n}{2}}$. The eigenvalue for $x^{\frac{n}{2}} y^{\frac{n}{2}}$ is 1 (in $\mathbf{F}_p$). All other eigenvalues occur in pairs whose product is 1. Thus, it is clear that the action of $B$ on the successive subquotients in the above filtration on $\mathcal{P}_n(-\frac{n}{2})$ is given by powers of $\widetilde{\beta}$, varying from $\widetilde{\beta}^{-\frac{n}{2}}$ at the top to $\widetilde{\beta}^{\frac{n}{2}}$ at the bottom. The exponent of the power of $\widetilde{\beta}$ increases by 1 at each step. There is an odd number of steps in the filtration, the action of $B$ on the middle step is given by $\tau_0|_B$, and so it follows that the determinant of this representation, restricted to $B$, is trivial. The element of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ just described is of dimension $n+1$ and has determinant $\tau_0$. It is precisely $\tau_{\boldsymbol{n}+1,1}$. If we twist by $\tau_{\mathbf{1}}$, then we obtain $\tau_{\boldsymbol{n}+1,2}$ and the action of $B$ on each subquotient of the corresponding composition series has been twisted by $\tau_{\mathbf{1}}|_B = \widetilde{\beta}^{\frac{p-1}{2}}$.

We can define a function $ch : \mathrm{Irr}_{\mathfrak{f}}(\Delta) \longrightarrow \mathrm{Irr}_{\mathfrak{f}}(B)$ as follows. For each $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, let $U_\tau$ denote the underlying $\mathfrak{f}$-representation space. Let $ch(\tau)$ be the character of $B$ giving the action of $B$ on the highest subquotient in the filtration on $U_\tau$ described above. Thus, if $j \in \{1, 3, ..., p\}$, then

$$ch(\tau_{\boldsymbol{j},1}) \;=\; \widetilde{\beta}^{-\frac{j-1}{2}}, \qquad\qquad ch(\tau_{\boldsymbol{j},2}) \;=\; \widetilde{\beta}^{\frac{p-j}{2}}$$

It is clear that the map $ch$ is surjective and that $\tau$ is determined by $ch(\tau)$ except when

$n(\tau) = 1$ or $p$. We have

$$ch(\tau_{\boldsymbol{p},1}) = ch(\tau_{\mathbf{1}}) = \widetilde{\beta}^{\frac{p-1}{2}} = \tau_{\mathbf{1}}|_B = \widetilde{\beta_{\mathbf{1}}}, \qquad ch(\tau_{\boldsymbol{p},2}) = ch(\tau_0) = \widetilde{\beta}_0 \ .$$

If $1 < n(\tau) < p$ and if $ch(\tau) = \widetilde{\psi}$, then the characters of $B$ which occur in the filtration for $U_\tau$ are $\{\widetilde{\psi}, \widetilde{\psi}\widetilde{\beta}, ..., \widetilde{\psi}^{-1}\}$. One has $\widetilde{\psi} \neq \widetilde{\psi}^{-1}$ and every character of $B$ occurring can be paired with its inverse, except for the character for the middle of the filtration which will be either $\beta_0$ or $\beta^{\frac{p-1}{2}}$. The determinant of $\tau$ is determined by this middle character. Of course, the number of characters that occur is $n(\tau)$. If $n(\tau) = 1$, then $ch(\tau) = \tau|_B$. If $n(\tau) = p$, then $ch(\tau) = \widetilde{\psi}$ will be one of the two characters satisfying $\widetilde{\psi} = \widetilde{\psi}^{-1}$, which occurs twice, and the middle character will be the other self-inverse (or self-dual) character of $B$, and again this middle character determines the determinant of $\tau$.

We remark in passing that each $\tau$ is self-dual. This is clear because the elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ are determined by their dimension and determinant. The determinant is a character of order 1 or 2 and so, letting $\check{\tau}$ denote the contragredient of any element $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, we have $det(\check{\tau}) = det(\tau)^{-1} = det(\tau)$. Obviously, $n(\check{\tau}) = n(\tau)$ and so indeed $\check{\tau} \cong \tau$. The restriction of $\tau$ to $B$ will also be self-dual and so the symmetry in the powers of $\widetilde{\beta}$ occurring in the filtration for $U_\tau$, which we saw above, is to be expected. The character occurring in the middle step must be self-inverse, i.e., either $\beta_0$ or $\beta_{\mathbf{1}}$. Correspondingly, $det(\tau)$ is then $\tau_0$ or $\tau_{\mathbf{1}}$, respectively.

**C.** *The decomposition numbers, indecomposable projective modules, and blocks.* We can now obtain rather complete information about the decomposition matrix $D_p(\Delta)$ for $\Delta$. There are only four odd-dimensional representations in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and their reductions are irreducible. Namely, we have $\widetilde{\sigma_0} \cong \tau_0$, $\widetilde{\sigma_{\mathbf{1}}} \cong \tau_{\mathbf{1}}$, $\widetilde{\sigma_{\boldsymbol{p},1}} \cong \tau_{\boldsymbol{p},1}$, and $\widetilde{\sigma_{\boldsymbol{p},2}} \cong \tau_{\boldsymbol{p},2}$. Thus, the only elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ which can be lifted to characteristic 0 are the ones of dimension 1 or of dimension $p$. As for the other representations $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, it turns out that $\widetilde{\sigma}$ has just two composition factors which we will now determine. The following describes what they are for each of the $(p+1)$-dimensional representations $\sigma_{\boldsymbol{p+1},j}$. For those of dimension $p-1$, the proposition specifies what they are and also serves as the definition of the index $j$ which was left undefined above.

**Proposition 7.2.4.** *Suppose that $\Delta = PGL_2(\mathbf{F}_p)$ and that $1 \leq j \leq \frac{p-3}{2}$. Then*

$$\widetilde{\sigma_{\boldsymbol{p+1},j}}^{ss} \cong \tau \oplus \tau' \ ,$$

*where $\tau$ and $\tau'$ are the unique elements in $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ such that $ch(\tau) = \widetilde{\beta}^j$ and $ch(\tau') = \widetilde{\beta}^{-j}$. Also, suppose that $1 \leq j \leq \frac{p-1}{2}$. Then*

$$\widetilde{\sigma_{\boldsymbol{p-1},j}}^{ss} \cong \tau \oplus \tau' \ ,$$

*where $\tau$ and $\tau'$ are the unique elements in $\mathrm{Irr}_{\mathsf{f}}(\Delta)$ of dimension at most $p-2$ such that $ch(\tau) = \widetilde{\beta}^{j}$ and $ch(\tau') = \widetilde{\beta}^{1\text{-}j}$.*

*Proof.* As mentioned in the proof of proposition 7.2.1, $\sigma_{\boldsymbol{p+1},j}|_B$ has $\beta^j$ and $\beta^{\text{-}j}$ as its 1-dimensional constituents and hence $\gamma$ as another constituent, all with multiplicity 1. Now $\widetilde{\gamma}$ has all of the powers of $\widetilde{\beta}$ as its 1-dimensional constituents. Thus, the restriction of $\widetilde{\sigma_{\boldsymbol{p+1},j}}^{ss}$ to $B$ is isomorphic to the direct sum of all the distinct powers of $\widetilde{\beta}$, all with multiplicity 1 except for $\widetilde{\beta}^{j}$ and $\widetilde{\beta}^{\text{-}j}$, which have multiplicity 2. In particular, the self-inverse characters $\widetilde{\beta_0}$ and $\widetilde{\beta_{\mathbf{1}}}$ occur with multiplicity 1 each. This last fact implies that there are exactly two irreducible constituents in $\widetilde{\sigma_{\boldsymbol{p+1},j}}^{ss}$. Furthermore, in order for $\widetilde{\beta}^{j}$ and $\widetilde{\beta}^{\text{-}j}$ to occur with multiplicity 2, the irreducible constituents must be precisely the ones described in the proposition.

Now suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and has dimension $p-1$. We then have $\sigma|_B \cong \gamma$. Hence, the restriction of $\widetilde{\sigma}^{ss}$ to $B$ is isomorphic to the direct sum of all the distinct powers of $\widetilde{\beta}$, all with multiplicity 1. This implies that $\widetilde{\beta_0}$ and $\widetilde{\beta_{\mathbf{1}}}$ occur with multiplicity 1 each, and so again there are exactly two irreducible constituents in $\widetilde{\sigma}^{ss}$. In order for each power of $\widetilde{\beta}$ to occur with multiplicity 1 in $\widetilde{\sigma}^{ss}$, the two irreducible constituents must be precisely the ones described in the proposition for *some* value of $j$. The inequality $1 \leq j \leq \frac{p-1}{2}$ uniquely determines that $j$. Proposition 7.2.1 implies that each of those irreducible constituents will occur in $\widetilde{\sigma}^{ss}$ for exactly one of the $\sigma$'s of dimension $p-1$. And so, each $j$ occurs just once and we can denote the given $\sigma$ by $\sigma_{\boldsymbol{p\text{-}1},j}$. It is determined by $j$ up to isomorphism. □

**Corollary 7.2.5.** *All elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ can be realized over $\mathbf{Q}_p$.*

*Proof.* It is clear from the definitions that the elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ of dimension 1 or $p$ can be realized over $\mathbf{Q}$. The $\sigma_{\boldsymbol{p+1},j}$'s are induced from 1-dimensional representations $\psi$ of $B$. Each such $\psi$ is a character of order dividing $p-1$ and so has values in $\mathbf{Q}_p^{\times}$. Hence the corresponding induced representation is realizable over $\mathbf{Q}_p$.

If $\sigma$ is of dimension $p-1$, one can use the fact that every $\tau \in \mathrm{Irr}_{\mathsf{f}}(\Delta)$ is actually defined over $\mathbf{F}_p$. Suppose that $\sigma_a$ and $\sigma_b$ are of dimension $p-1$ and conjugate over $\mathbf{Q}_p$. Then their reductions $\widetilde{\sigma_a}^{ss}$ and $\widetilde{\sigma_b}^{ss}$ would be conjugate over $\mathbf{F}_p$ and hence isomorphic. However, proposition 7.2.4 implies that $\sigma$ is determined up to isomorphism by the constituents $\tau$ and $\tau'$ in $\widetilde{\sigma}^{ss}$. Hence $\sigma_a$ and $\sigma_b$ would be isomorphic. Thus, for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ of dimension $p-1$, the character of $\sigma$ has values in $\mathbf{Q}_p$.

Finally, we must show that the Schur index for $\sigma$ over $\mathbf{Q}_p$ is 1. Consider the representation $\gamma$ of $B$ defined earlier. It is realizable over $\mathbf{Q}_p$ (and even over $\mathbf{Q}$). Hence $\mathrm{Ind}_B^{\Delta}(\gamma)$ is a representation of $\Delta$ over $\mathbf{Q}_p$. But $\sigma|_B \cong \gamma$ and hence $\sigma$ occurs with multiplicity 1 in $\mathrm{Ind}_B^{\Delta}(\gamma)$. The assertion about the Schur index follows from this. □

The indecomposable, projective $\mathcal{O}[\Delta]$-modules $P_\tau$ are direct summands (as left ideals) in $\mathcal{O}[\Delta]$. The multiplicity of $P_\tau$ is $n(\tau)$. The following result gives their $\mathcal{O}$-ranks. It is easily derived from proposition 7.2.4 by using the fact that each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ contributes $n(\sigma)d(\sigma,\tau)$ to the $\mathcal{O}$-rank.

**Corollary 7.2.6.** *Suppose that* $\tau \in \mathrm{Irr}_{\mathrm{f}}(\Delta)$. *We have* $\mathrm{rank}_{\mathcal{O}}\big(P_\tau\big) = p$ *if* $n(\tau) = 1$ *or* $n(\tau) = p$, *and* $\mathrm{rank}_{\mathcal{O}}\big(P_\tau\big) = 2p$ *for all other* $\tau$*'s.*

**Remark 7.2.7.** Note that the $\mathcal{F}$-representation space $P_\tau \otimes_{\mathcal{O}} \mathcal{F}$ for $\Delta$ is irreducible if $n(\tau) = p$, and is a direct sum of two distinct irreducible representations of $\Delta$ for all other $\tau$'s. One of those representation spaces has dimension $p-1$; the other has dimension 1 or $p+1$. Each of the irreducible representations of dimension $p-1$ or $p+1$ occurs as a summand in $P_\tau \otimes_{\mathcal{O}} \mathcal{F}$ for exactly two $\tau$'s, precisely as indicated in proposition 7.2.4. $\Diamond$

**Remark 7.2.8.** Proposition 7.2.1 provides another illustration of the fact that congruence relations arise from the individual blocks, just as described in part **D** of section 7.1. In this case, it is the principal block which gives the congruence relation. To explain this, note that proposition 7.2.4 allows us to determine the blocks for $\Delta = PGL_2(\mathbf{F}_p)$ and $p$. There are two nonprincipal blocks, which are just the singletons $\{\sigma_{\boldsymbol{p},1}\}$ and $\{\sigma_{\boldsymbol{p},2}\}$. Note that those representations are realizable on $\mathcal{F}$-vector spaces which contain projective $\Delta$-invariant $\mathcal{O}$-lattices, namely $P_{\tau_{\boldsymbol{p},1}}$ and $P_{\tau_{\boldsymbol{p},2}}$, respectively. The principal block consists of all of the other elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. One can verify this by repeatedly using proposition 7.2.4. If $\sigma_1, \sigma_2 \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ are such that $\widetilde{\sigma_1}^{ss}$ and $\widetilde{\sigma_2}^{ss}$ have an irreducible constituent in common, then we will say that they are *"linked"*. If so, then $\sigma_1$ and $\sigma_2$ are in the same block. Thus, in order, we have the following linked pairs:

$$\text{(7.2.a)} \qquad \sigma_0,\ \sigma_{\boldsymbol{p}\text{-}1,1}, \qquad \sigma_{\boldsymbol{p}\text{-}1,1},\ \sigma_{\boldsymbol{p}+1,1}, \quad \ldots, \quad \sigma_{\boldsymbol{p}\text{-}1,1},\ \sigma_{\mathbf{1}}$$

and all the elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$, except for the two of degree $p$, are easily seen to be included in the list and hence in the principal block. Following this same approach, one can also express the $w(X,\tau)$'s in terms of the $\lambda(X,\sigma)$'s for any projective $\mathbf{Z}_p[\Delta]$-module $X$. $\Diamond$

**D.** *The representations* $\rho$, $\zeta$, *and* $\kappa$. It will be useful for proposition 7.3.1 below to discuss the following three representations of $\Delta$:

$$\rho \ = \ \bigoplus_{\sigma} \sigma^{n(\sigma)}, \qquad \zeta \ = \ \mathrm{Ind}_B^{\Delta}(\gamma), \qquad \kappa \ = \ \sigma_0 \oplus \sigma_{\mathbf{1}} \oplus \sigma_{\boldsymbol{p},1} \oplus \sigma_{\boldsymbol{p},2} \oplus \bigoplus_{j=1}^{\frac{p-3}{2}} \sigma^2_{\boldsymbol{p}+\mathbf{1},j} \ .$$

Of course, $\rho$ is just the regular representation for $\Delta$ over $\mathcal{F}$ and $n(\rho) = |\Delta| = p(p+1)(p-1)$. Also, $n(\zeta) = n(\kappa) = (p+1)(p-1)$. We can describe $\zeta$ and $\kappa$ in the following ways:

$$\zeta \;\cong\; \bigoplus_{n(\sigma)>1} \sigma \qquad \textit{and} \qquad \kappa \;\cong\; \bigoplus_{j=0}^{p\text{-}2} \sigma_{\boldsymbol{p+1},j},$$

where we are using the notation $\sigma_{\boldsymbol{p+1},j}$ for the representation $\mathrm{Ind}_B^{\Delta}(\beta^j)$ for *any* $j$ in the range $0 \le j \le p-2$, and not just for $1 \le j \le \frac{p\text{-}3}{2}$ as before. Thus, $\beta^j$ can be any power of $\beta$. The justification for the first isomorphism is that if $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $n(\sigma) > 1$, then $\sigma|_B$ has $\gamma$ as a constituent with multiplicity 1. One then applies Frobenius reciprocity. The justification for the second isomorphism is again Frobenius reciprocity. It follows from what we have described previously concerning the $\beta^j$'s which occur in the restrictions $\sigma|_B$ for $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Note that $\sigma_{\boldsymbol{p+1},j}$ is reducible for two values of $j$. For $j = 0$, it is isomorphic to $\sigma_0 \oplus \sigma_{\boldsymbol{p},2}$. For $j = \frac{p\text{-}1}{2}$, it is isomorphic to $\sigma_{\boldsymbol{1}} \oplus \sigma_{\boldsymbol{p},1}$.

The reductions modulo $\mathfrak{m}$ of $\kappa$, $\zeta$, and $\rho$ are related as follows:

$$\widetilde{\kappa}^{ss} \;\cong\; \widetilde{\zeta}^{ss}, \qquad \widetilde{\rho}^{ss} \;\cong\; \left(\widetilde{\kappa}^{ss}\right)^p \quad . \tag{7.2.b}$$

The first isomorphism follows from the fact that $\widetilde{\gamma}^{ss} \cong \bigoplus_{j=0}^{p\text{-}2} \widetilde{\beta}^j$ as a representation of $B$. The second follows easily from proposition 7.2.1.

We also recall the following notation from the introduction. If $X$ is a finitely-generated $\mathbf{Z}_p[\Delta]$-module, then we obtain a group homomorphism $\lambda_X : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathbf{Z}$. This is determined by $\lambda_X(\sigma) = \lambda(X, \sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. For example, we have

$$\lambda_X(\kappa) \;=\; \lambda_X(\sigma_0) \;+\; \lambda_X(\sigma_{\boldsymbol{1}}) \;+\; \lambda_X(\sigma_{\boldsymbol{p},1}) \;+\; \lambda_X(\sigma_{\boldsymbol{p},2}) \;+\; 2\sum_{j=1}^{\frac{p\text{-}3}{2}} \lambda_X(\sigma_{\boldsymbol{p+1},j}) \quad . \tag{7.2.c}$$

**Remark 7.2.9.** One can use proposition 7.2.4 to determine the multiplicity of $\tau$ in $\widetilde{\kappa}^{ss}$ for any $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. It is given by $\langle \widetilde{\kappa}^{ss}, \tau \rangle = 1$ if $n(\tau) = 1$ or $p$, $\langle \widetilde{\kappa}^{ss}, \tau \rangle = 2$ if $1 < n(\tau) < p$. $\Diamond$

## 7.3 The groups $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \ge 1$.

Suppose that $r \ge 1$ and that $p$ is an odd prime. We let $\Delta_r = PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. We have already discussed the representation theory of $\Delta_0 = PGL_2(\mathbf{Z}/p\mathbf{Z})$ in section 7.2. Since the

kernel of the map $\Delta_r \to \Delta_0$ is a normal $p$-subgroup of $\Delta_r$, we therefore know the irreducible representations of $\Delta_r$ in characteristic $p$.

**A.** *Characteristic zero.* We will now summarize some results about the representation theory of $\Delta_r$. They are extracted from [Sil]. The irreducible complex representations are described there, but the results apply to an extension $\mathcal{F}$ of $\mathbf{Q}_p$ containing enough roots of unity, as in the introduction. The field $\mathcal{F}$ may depend on $r$ and we denote it by $\mathcal{F}_r$. An element of $\mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ is called $r$-primitive if it doesn't factor through the quotient group $\Delta_{r\text{-}1}$. There are exactly $p^{r+1}$ such representations. Their dimensions will be one of the following possibilities

$$\text{(7.3.a)} \qquad a_r = (p+1)p^r, \qquad b_r = (p-1)p^r, \qquad c_r = (p+1)(p-1)p^{r\text{-}1} \quad .$$

Let $\mathcal{A}_r$, $\mathcal{B}_r$, and $\mathcal{C}_r$ denote the corresponding subsets of $\mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$. Then

$$\text{(7.3.b)} \qquad |\mathcal{A}_r| = \tfrac{1}{2}(p-1)^2 p^{r\text{-}1}, \qquad |\mathcal{B}_r| = \tfrac{1}{2}(p-1)(p+1)p^{r\text{-}1}, \qquad |\mathcal{C}_r| = p^r \ .$$

The representations in $\mathcal{A}_r$ are easily described. Let $B_r$ denote the image of the $2 \times 2$ upper triangular matrices over $\mathbf{Z}/p^{r+1}\mathbf{Z}$ in $\Delta_r$ and let $U_r$ denote the image of the upper triangular matrices with 1's along the main diagonal. Thus $U_r$ is a normal subgroup of $B_r$ and $U_r \cong \mathbf{Z}/p^{r+1}\mathbf{Z}$. Also, $B_r/U_r \cong (\mathbf{Z}/p^{r+1}\mathbf{Z})^\times$. Every $\sigma \in A_r$ is of the form $\sigma = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi)$, where $\psi$ is a primitive character of $(\mathbf{Z}/p^{r+1}\mathbf{Z})^\times$, viewed as a 1-dimensional representation of $B_r$. If $\psi'$ is a 1-dimensional representation of $B_r$, then the corresponding induced representation is isomorphic to $\sigma$ if and only if $\psi' \in \{\psi, \psi^{-1}\}$. The cardinality of $\mathcal{A}_r$ is just the number of such pairs of primitive characters. We denote these representations by $\sigma_{\boldsymbol{a_r},j}$, where $1 \le j \le |\mathcal{A}_r|$. Each has degree $a_r$ because $[\Delta_r : B_r] = a_r$. The irreducible representations just described are the elements of the so-called *"principal series."* This phrase also includes the irreducible representations of $\Delta_0$ of dimension $p+1$.

We won't describe the other $r$-primitive elements of $\mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ at all, except for the so-called Steinberg representation. It is a constituent in $\mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r})$, which we denote by $\sigma_{st}^{(r)}$, and is characterized by the isomorphism

$$\mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r}) \ \cong \ \sigma_{st}^{(r)} \ \oplus \ \mathrm{Ind}_{B_{r\text{-}1}}^{\Delta_{r\text{-}1}}(\mathbf{1}_{B_{r\text{-}1}}) \ ,$$

where we view the second summand as a representation of $\Delta_r$ through the canonical homomorphism $\Delta_r \to \Delta_{r\text{-}1}$. Alternatively, letting $N_{r\text{-}1}$ denote the kernel of that homomorphism, one can identify the second summand with the representation of $\Delta_r$ induced from the trivial representation of $B_r N_{r\text{-}1}$. One sees easily that $n(\sigma_{st}^{(r)}) = c_r$ and therefore $\sigma_{st}^{(r)}$ is in $\mathcal{C}_r$. The elements of $\mathcal{B}_r$ are the irreducible representations in the so-called *"unramified discrete series"* which also includes all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ with $n(\sigma) = p-1$.

A number of different subgroups of $\Delta_r$ will intervene in the following discussion. We've already defined $B_r, U_r$ and $N_{r\text{-}1}$. For any $s$, $0 \leq s \leq r-1$, we define $N_s$ to be the "congruence subgroup" $\ker\big(\Delta_r \to \Delta_s\big)$. Thus, $N_s$ is the image of $I + p^s M_2(\mathbf{Z}_p)$ in $\Delta_r$ under the obvious map $GL_2(\mathbf{Z}_p) \to \Delta_r$. Here $M_2(\mathbf{Z}_p)$ denotes the ring of $2 \times 2$ matrices over $\mathbf{Z}_p$. In the proof of proposition 7.3.1 below, we will define other subgroups of $\Delta_r$, denoted by $H_r$, $C_r$, and $\Pi_r$.

**B.** *Decomposition numbers, congruence relations, and the indecomposable projectives.* We now discuss the modular representation theory for $\Delta_r$ and the prime $p$. All of the irreducible representations of $\Delta_r$ over $\mathfrak{f}$ are actually defined over $\mathbf{F}_p$. They all factor through $\Delta_0$ and were described completely in section 7.2. We now want to obtain the decomposition numbers $d(\sigma, \tau)$ for $\sigma$ in $\mathcal{A}_r$ and $\mathcal{C}_r$. We will describe the results in terms of the representations $\kappa$ and $\sigma_{\boldsymbol{p+1},j}$ of $\Delta_0$ which were defined in section 7.2, part **D**. The decomposition numbers for those two representations are given in remark 7.2.9 for $\kappa$ and in proposition 7.2.4 for $\sigma_{\boldsymbol{p+1},j}$. We can regard them as representations of $\Delta_r$. We also will refer to the character $\beta$ of the group that was denoted by $B$ in section 7.2, and which we now will denote by $B_0$. Since $B_0$ is a quotient of $B_r$, we can also regard $\beta$ as a character of $B_r$. It factors through $B_r/U_r$.

Since we are now considering the family of groups $\Delta_r$, where $r$ is allowed to vary, it is important to note that the $\lambda$-invariants for a given $\sigma$ are well-defined. To be precise, suppose that $\sigma$ is an irreducible representation of a finite group $G$ over $\mathcal{F}$ and that $X$ is a finitely-generated $\mathbf{Z}_p[G]$-module. We can then define the invariants $\lambda(X, \sigma)$ as before. If $N$ is a normal subgroup of $G$ such that $N \subseteq \ker(\sigma)$, and if we also regard $\sigma$ as a representation of $G/N$, then we have $\lambda(X, \sigma) = \lambda(X_N, \sigma)$, where $X_N$ is the largest quotient of $X$ on which $N$ acts trivially. If $X$ is a projective $\mathbf{Z}_p[G]$-module, then $X_N$ is a projective $\mathbf{Z}_p[G/N]$-module. These statements are easily verified.

We will sometimes use the following abbreviated notation. If $\rho_1$ and $\rho_2$ are representations of a group $G$ over $\mathcal{F}$, then we will write $\rho_1 \approx \rho_2 \pmod{\mathfrak{m}}$ if $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$ as $\mathfrak{f}$-representations of $G$. We will also use the notation $\sigma_{\boldsymbol{p+1},j}$ as in part **D** of section 7.2, where we allow $j$ to be in the range $0 \leq j \leq p-2$. This representation of $\Delta_0$ is reducible for $j = 0$ and $j = \frac{p\text{-}1}{2}$. For the other $j$'s, the representation is irreducible, but the isomorphism class only determines the pair $\{j, p\text{-}1\text{-}j\}$.

**Proposition 7.3.1.** *Suppose that $r \geq 1$. If $\sigma \in \mathcal{C}_r$, then we have an isomorphism*

$$\widetilde{\sigma}^{ss} \;\cong\; \big(\widetilde{\kappa}^{ss}\big)^{p^{r\text{-}1}} \quad .$$

*Furthermore, suppose that $\psi$ is any character of $B_r/U_r$ (primitive or not) and that $\widetilde{\psi} = \widetilde{\beta}^j$,*

*where* $0 \leq j \leq p-2$. *Let* $d_r = \frac{p^r\text{-}1}{p\text{-}1}$. *Then, if* $\sigma = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi)$, *we have*

$$\widetilde{\sigma}^{ss} \;\cong\; \left(\widetilde{\kappa}^{ss}\right)^{d_r} \oplus \widetilde{\sigma_{\boldsymbol{p+1},j}}^{ss} \quad .$$

*In particular, if* $\sigma \in \mathcal{A}_r$, *then this isomorphism for* $\widetilde{\sigma}^{ss}$ *will hold for the value of* $j$ *determined as follows: the character* $\psi$ *will be primitive and can be uniquely chosen so that* $\widetilde{\psi} = \widetilde{\beta}^j$, *where* $0 \leq j \leq \frac{p-1}{2}$.

*Suppose that* $X$ *is a quasi-projective* $\mathbf{Z}_p[\Delta_r]$*-module and that* $k = \lambda_X(\kappa)$, *the quantity defined in (7.2.c). We then have the following congruence relations: If* $\sigma \in \mathcal{C}_r$, *then* $\lambda(X, \sigma) = p^{r\text{-}1}k$. *If* $\sigma \in \mathcal{A}_r$, *then* $\lambda(X, \sigma) = d_r k + \lambda(X, \sigma_{\boldsymbol{p+1},j})$, *where* $j$ *is as above.*

*Proof.* The stated congruence relations follow from the isomorphisms. We will prove the first isomorphism for $\sigma = \sigma_{st}^{(r)}$ and then extend it to all $\sigma \in \mathcal{C}_r$ by using the following result (whose proof will only be given in remark 7.4.7): *If* $\sigma_1,\ \sigma_2 \in \mathcal{C}_r$, *then* $\widetilde{\sigma_1}^{ss} \cong \widetilde{\sigma_2}^{ss}$.

Let $H_r$ denote the inverse image of $B_0$ under the canonical homomorphism $\Delta_r \to \Delta_0$. Thus, $H_r$ is a subgroup of $\Delta_r$ containing $B_r$ and we have $[\Delta_r : H_r] = p+1,\ [H_r : B_r] = p^r$. The group $H_r$ will play an important role in this proof. Note that $H_r$ has a normal subgroup $\Pi_r$ of index $p-1$ which is a $p$-group. In fact, $\Pi_r$ is a Sylow $p$-subgroup of $\Delta_r$ and $H_r$ is a semidirect product of $\Pi_r$ with a subgroup $C_r$ of order $p-1$. We can take $C_r$ to be the image in $\Delta_r$ of the group of matrices of the form $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ where $c \in (\mathbf{Z}/p^{r+1}\mathbf{Z})^\times$ has order dividing $p-1$. Thus, $C_r$ is cyclic of order $p-1$.

Consider the representation $\varepsilon_r = \mathrm{Ind}_{B_r}^{H_r}(\mathbf{1}_{B_r})$ of $H_r$. We have $n(\varepsilon_r) = p^r$. We regard the powers of $\beta$ as characters of $B_0$ and hence of $H_r$ (without a change of notation). Then $\widetilde{\varepsilon_r}^{ss}$ is a direct sum of the $\widetilde{\beta}^j$'s with certain multiplicities. To determine those multiplicities, it suffices to consider the restriction $\varepsilon_r|_{C_r}$. We must look at the action of $C_r$ on the left coset space $H_r/B_r$. An element of $C_r$ acts as the permutation of the left cosets induced by left multiplication.

Each left coset in $H_r/B_r$ has a unique representative of the form $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, where 1 and $a$ are in $\mathbf{Z}/p^{r+1}\mathbf{Z}$ and $a$ is divisible by $p$. If one multiplies that matrix (on the left) by $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$, which is a representative for some element of $C_r$, then one obtains $\begin{pmatrix} 1 & 0 \\ ca & c \end{pmatrix}$ which is in the same left coset as $\begin{pmatrix} 1 & 0 \\ ca & 1 \end{pmatrix}$. Thus the action of $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ as a permutation of $H_r/B_r$ corresponds to the action of $c$ on the set $p\mathbf{Z}/p^{r+1}\mathbf{Z}$ by multiplication. It is clear that there is one orbit of length 0 and $d_r$ orbits of length $p-1$. This means that $\varepsilon_r|_{C_r}$ is isomorphic to the direct sum of $\mathbf{1}_{C_r}$ and $d_r$ copies of the regular representation of $C_r$. Consequently, the

multiplicity of $\widetilde{\beta}^j$ in $\widetilde{\varepsilon}_r^{\,ss}$ is $d_r$ except when $\widetilde{\beta}^j$ is the trivial character. The multiplicity is then $d_r + 1$.

We will use the abbreviated notation $\rho_1 \approx \rho_2 \pmod{\mathfrak{m}}$ described before in the rest of this proof. We have $\varepsilon_r \approx \gamma^{d_r} \oplus \beta_0 \pmod{\mathfrak{m}}$ as representations of $H_r$. Recall that $\gamma$ is an irreducible representation of $B_0$ and that $\widetilde{\gamma}^{ss}$ is isomorphic to the direct sum of the $\widetilde{\beta}^j$'s for $0 \le j \le p-2$. It follows that

$$\mathrm{Ind}_{H_r}^{\Delta_r}(\varepsilon_r) \;\approx\; \left(\mathrm{Ind}_{B_0}^{\Delta_0}(\gamma)\right)^{d_r} \oplus \sigma_{\boldsymbol{p+1},0} \;\approx\; \zeta^{d_r} \oplus \sigma_{\boldsymbol{p+1},0} \quad (\mathrm{mod}\ \mathfrak{m}) \ .$$

as representations of $\Delta_r$. We have used the fact that we can regard $\gamma$ as a representation of $H_r$ which factors through $B_0$ and so $\zeta = \mathrm{Ind}_{B_0}^{\Delta_0}(\gamma)$ can be identified with $\mathrm{Ind}_{H_r}^{\Delta_r}(\gamma)$. Of course, since induction is transitive, $\mathrm{Ind}_{H_r}^{\Delta_r}(\varepsilon_r) \cong \mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r})$. Consequently, using (7.2.b), we have

$$\mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r}) \;\approx\; \kappa^{d_r} \oplus \sigma_{\boldsymbol{p+1},0} \quad (\mathrm{mod}\ \mathfrak{m})$$

for any $r \ge 1$. The fact that $d_r - d_{r\text{-}1} = p^{r\text{-}1}$ then implies the first isomorphism in the proposition for the special case where $\sigma = \sigma_{st}^{(r)}$. As mentioned above, the isomorphism then follows for all $\sigma \in \mathcal{C}_r$.

For the second isomorphism, we consider the restrictions of $\beta^j$, viewed as a character of $H_r$, to $B_r$. Then we have

$$\varepsilon_r \otimes \beta^j \;\cong\; \mathrm{Ind}_{B_r}^{H_r}(\beta^j|_{B_r})$$

and so

$$\mathrm{Ind}_{B_r}^{H_r}(\psi) \;\approx\; \varepsilon_r \otimes \beta^j \;\approx\; \gamma^{d_r} \oplus \beta^j \quad (\mathrm{mod}\ \mathfrak{m}) \ .$$

Inducing from $H_r$ to $\Delta_r$ then gives the stated isomorphism. □

**Remark 7.3.2.** The decomposition numbers $d(\sigma, \tau)$ can now be easily determined for all $\sigma$ in $\mathcal{A}_r$ or $\mathcal{C}_r$ and for any $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta_r) = \mathrm{Irr}_{\mathfrak{f}}(\Delta)$. (Such $\tau$'s are defined over $\mathbf{F}_p$, but we simply take $\mathfrak{f}$ to be the residue field for $\mathcal{F}_r$, which is independent of $r$.) First note that $d(\kappa, \tau) = 1$ for the four $\tau$'s satisfying $n(\tau) = 1$ or $p$, and $d(\kappa, \tau) = 2$ for all other $\tau$'s. We then have $d(\sigma, \tau) = p^{r\text{-}1} d(\kappa, \tau)$ for all $\sigma \in \mathcal{C}_r$. For $\sigma \in \mathcal{A}_r$, one can use the second isomorphism in proposition 7.3.1 together with proposition 7.2.4 which gives the decomposition numbers $d(\sigma_{\boldsymbol{p+1},j}, \tau)$.

It is interesting to note that if $\sigma$ is in $\mathcal{A}_r$ or $\mathcal{C}_r$, where $r \ge 1$, then $d(\sigma, \tau) \ge 1$ for all $\tau$. This implies that all other elements of $\mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ are in the same block as $\sigma$. Therefore, there is only one block for the group $\Delta_r$ and the prime $p$, assuming that $r \ge 1$. ◊

**Remark 7.3.3.** We haven't said anything about the $\sigma$'s in $\mathcal{B}_r$ when $r \ge 1$. For any such $\sigma$, we will later show that $\sigma|_{B_r}$ is the unique faithful, irreducible representation of $B_r$. This

will be proved in proposition 7.4.1. It will then be clear that $\sigma|_{H_r} \approx \gamma^{p^r}$ as representations of $H_r$. This puts a strong constraint on the possibilities for $\widetilde{\sigma}^{ss}$. We omit the details, but one finds that

$$\widetilde{\sigma}^{ss} \;\cong\; \bigoplus_{j=1}^{\frac{p-1}{2}} \left(\widetilde{\sigma_{\boldsymbol{p-1},j}}^{ss}\right)^{m_j} \;\oplus\; \left(\widetilde{\sigma_{\boldsymbol{p},1}}^{ss} \ominus \widetilde{\sigma_{\mathbf{1}}}\right)^{u} \;\oplus\; \left(\widetilde{\sigma_{\boldsymbol{p},2}}^{ss} \ominus \widetilde{\sigma}_0\right)^{v} .$$

This should be interpreted as an equality in the Grothendieck group $\mathcal{R}_{\mathfrak{f}}(\Delta_r)$. Here, the multiplicities $m_1, ..., m_{\frac{p-1}{2}}$, $u$, and $v$ are nonnegative integers whose sum is $p^r$. However, we don't know which possibilities actually occur. In any case, if $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module and if $\sigma \in \mathcal{B}_r$, then $\lambda(X, \sigma)$ is determined if one knows the quantities

$$\lambda(X, \sigma_{\boldsymbol{p-1},j}) \;\; for\; 1 \le j \le \frac{p\text{-}1}{2}, \qquad \lambda(X, \sigma_{\boldsymbol{p},1}) - \lambda(X, \sigma_{\mathbf{1}}), \quad and \quad \lambda(X, \sigma_{\boldsymbol{p},2}) - \lambda(X, \sigma_0) \;\; ,$$

together with the corresponding multiplicities $m_1, ..., m_{\frac{p-1}{2}}$, $u$, and $v$. $\Diamond$

**Remark 7.3.4.** Howe [How] completely determines $det(\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ and all $r \ge 0$. He assumes that $p$ is odd as we do. It turns out that we can recover his result by using remark 7.2.3 for $r = 0$ and the modular representation theory for $\Delta_r$ when $r \ge 1$. Proposition 7.3.1 suffices for the $\sigma$'s covered by that result. Recall that $det(\sigma_{\boldsymbol{p},1}) = \sigma_0$ and $det(\sigma_{\boldsymbol{p},2}) = \sigma_{\mathbf{1}}$. The definition of $\kappa$ then makes it clear that $det(\kappa) = \sigma_0$. Since $p$ is odd, $det(\sigma)$ is determined by $det(\widetilde{\sigma}^{ss})$, as one easily sees. It follows that $det(\sigma) = \sigma_0$ for all $\sigma \in \mathcal{C}_r$. As for any of the induced representations $\sigma$ covered in proposition 7.3.1, we have $det(\sigma) = \sigma_{\mathbf{1}}$. This follows because the same thing is true for the $\sigma_{\boldsymbol{p+1},j}$'s. In particular, $det(\sigma) = \sigma_{\mathbf{1}}$ for all $\sigma \in \mathcal{A}_r$. Later, in remark 7.4.8, we will give a modular representation proof that $det(\sigma) = \sigma_{\mathbf{1}}$ for all $\sigma \in \mathcal{B}_r$. $\Diamond$

**Remark 7.3.5.** The congruence relations in proposition 7.3.1 give some simple parity statements which will be useful later. Note that $d_r \equiv r \pmod 2$. For compactness, we let

$$\lambda_0(X) \;=\; \lambda(X, \sigma_0), \qquad \lambda_{\mathbf{1}}(X) \;=\; \lambda(X, \sigma_{\mathbf{1}}), \qquad and \qquad \lambda_{\boldsymbol{n},j}(X) \;=\; \lambda(X, \sigma_{\boldsymbol{n},j})$$

for the dimensions $n = p,\; p-1$ or $p+1$ and the appropriate $j$'s. The representations listed here all factor through $\Delta_0$. We take $X$ to be a $\mathbf{Z}_p[\Delta_r]$-module, but if $X_0$ denotes the maximal quotient of $X$ on which $N = ker(\Delta_r \to \Delta_0)$ acts trivially, then those invariants can also be defined in terms of the $\mathbf{Z}_p[\Delta_0]$-module $X_0$. (See the remark before proposition 7.3.1.)

If $r \ge 1$, we will consider the following irreducible representations of $\Delta_r$. Suppose that $\theta$ is a character of $B_r/U_r$ of order exactly $p^r$. For any $t$ satisfying $1 \le t \le \frac{p-3}{2}$, let $\psi_t = \beta^t\theta$.

We also consider $\beta_{\mathbf{1}}\theta$. All of these characters of $B_r/U_r$ are primitive and the following representations are all in $\mathcal{A}_r$:

$$\sigma_\theta^{(r)} = \mathrm{Ind}_{B_r}^{\Delta_r}(\theta), \qquad \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}} = \mathrm{Ind}_{B_r}^{\Delta_r}(\beta_{\mathbf{1}}\theta), \qquad \sigma_{\psi_t}^{(r)} = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi_t) \quad .$$

We assume $r \geq 1$. Then, if $X$ is a quasi-projective $\mathbf{Z}_p[\Delta_r]$-module, we have

**1.** $\lambda(X, \sigma_\theta^{(r)}) \equiv (r+1)\Big(\lambda_0(X) + \lambda_{\boldsymbol{p},2}(X)\Big) + r\Big(\lambda_{\mathbf{1}}(X) + \lambda_{\boldsymbol{p},1}(X)\Big) \pmod 2$ ,

**2.** $\lambda(X, \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}}) \equiv r\Big(\lambda_0(X) + \lambda_{\boldsymbol{p},2}(X)\Big) + (r+1)\Big(\lambda_{\mathbf{1}}(X) + \lambda_{\boldsymbol{p},1}(X)\Big) \pmod 2$ ,

**3.** $\lambda\big(X, \sigma_{\psi_t}\big) \equiv \lambda_0(X) + \lambda_{\mathbf{1}}(X) + \lambda_{\boldsymbol{p},1}(X) + \lambda_{\boldsymbol{p},2}(X) + \lambda_{\boldsymbol{p}+\mathbf{1},t}(X) \pmod 2$ .

For $\sigma \in \mathcal{C}_r$, the congruence is even simpler. We then have

**4.** $\lambda(X, \sigma) \equiv \lambda_0(X) + \lambda_{\mathbf{1}}(X) + \lambda_{\boldsymbol{p},1}(X) + \lambda_{\boldsymbol{p},2}(X) \pmod 2$ .

Thus, if we let $\lambda = \lambda(X, \sigma_0) + \lambda(X, \sigma_{\boldsymbol{p},2})$ and $\lambda' = \lambda(X, \sigma_{\mathbf{1}}) + \lambda(X, \sigma_{\boldsymbol{p},1})$, then the parities of $\lambda(X, \sigma_\theta^{(r)})$ and $\lambda(X, \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}})$ are completely determined by the parities of $\lambda$ and $\lambda'$. The other elements of $\mathcal{A}_r$ are of the form $\sigma = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi)$, where $\widetilde{\psi} \neq \widetilde{\beta_0}$ or $\widetilde{\beta_{\mathbf{1}}}$. We then again obtain a parity result for $\lambda(X, \sigma)$, but this time the parity of $\lambda(X, \sigma_{\boldsymbol{p}+\mathbf{1},j})$ is also involved. However, for $\sigma \in \mathcal{C}_r$, the parity of $\lambda(X, \sigma)$ is determined just by the parity of the single quantity $\lambda + \lambda'$. $\Diamond$

We now prove a result about the indecomposable projective modules for $\mathbf{Z}_p[\Delta_r]$. In the introduction, we consider the corresponding modules for the group ring over the integers $\mathcal{O}$ in a sufficiently large, finite extension $\mathcal{F}$ of $\mathbf{Q}_p$, which we have been denoting by $\mathcal{F}_r$. However, in this example, $\mathcal{O}$ and $\mathcal{F}$ would vary with $r$. This is rather inconvenient. Now the elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta_r) = \mathrm{Irr}_{\mathfrak{f}}(\Delta_0)$ are actually realizable over $\mathbf{F}_p$. Thus, for every $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta_r)$, we can define an indecomposable, projective $\mathbf{Z}_p[\Delta_r]$-module $P_\tau^{(r)}$ whose unique simple quotient is isomorphic to $U_\tau$, the $\mathbf{F}_p$-irreducible representation space of $\Delta_r$ corresponding to $\tau$. It is uniquely determined up to isomorphism as a $\mathbf{Z}_p[\Delta_r]$-module. (See chapter 14.4, proposition 42, in [Se77].) Then, for any $\mathcal{O}$ as above, the corresponding indecomposable, projective $\mathcal{O}[\Delta]$-module is $P_\tau^{(r)} \otimes_{\mathbf{Z}_p} \mathcal{O}$, which has $U_\tau \otimes_{\mathbf{F}_p} \mathfrak{f}$ as its unique simple quotient. In particular, the $\mathbf{Z}_p[\Delta_0]$ module $P_\tau^{(0)}$ has $\mathbf{Z}_p$-rank $p$ or $2p$, just as indicated in corollary 7.2.6.

We also use the following notation. If $r_1 > r_2 \geq 0$, then there is a surjective group homomorphism $\Delta_{r_1} \to \Delta_{r_2}$ whose kernel is $\mathrm{Gal}(K_{r_1}/K_{r_2})$. This can be extended to a $\mathbf{Z}_p$-algebra homomorphism $\mathbf{Z}_p[\Delta_{r_1}] \to \mathbf{Z}_p[\Delta_{r_2}]$ whose kernel will be denoted by $I_{(r_1/r_2)}$. The first part of the following result extends corollary 7.2.6.

**Proposition 7.3.6.** *Suppose that* $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta_0)$ *and* $r \geq 0$. *We have* $\mathrm{rank}_{\mathbf{Z}_p}\big(P_\tau^{(r)}\big) = p^{3r+1}$ *if* $n(\tau) = 1$ *or* $n(\tau) = p$, *and* $\mathrm{rank}_{\mathbf{Z}_p}\big(P_\tau^{(r)}\big) = 2p^{3r+1}$ *for all other* $\tau$*'s. Furthermore, for* $r_1 > r_2 \geq 0$, *we have an isomorphism*

$$P_\tau^{(r_1)} \big/ I_{(r_1/r_2)} P_\tau^{(r_1)} \;\cong\; P_\tau^{(r_2)}$$

*as* $\mathbf{Z}_p[\Delta_{r_2}]$*-modules.*

*Proof.* First note that $I_{(r/0)}$ annihilates $U_\tau$. This is clear because the action of $\Delta_r$ on $U_\tau$ factors through $\Delta_0$. Thus, for any $r_1 > r_2 \geq 0$, $I_{(r_1/r_2)}$ annihilates $U_\tau$. Therefore, $P_\tau^{(r_1)} \big/ I_{(r_1/r_2)} P_\tau^{(r_1)}$ has $U_\tau$ as a quotient module. This is the only nontrivial semisimple quotient of $P_\tau^{(r_1)} \big/ I_{(r_1/r_2)} P_\tau^{(r_1)}$. If $X$ is a free $\mathbf{Z}_p[\Delta_{r_1}]$-module, then it is clear that $X/I_{(r_1/r_2)}X$ is a free $\mathbf{Z}_p[\Delta_{r_2}]$-module. It follows that if $P$ is a projective $\mathbf{Z}_p[\Delta_{r_1}]$-module, then $P/I_{(r_1/r_2)}P$ is a projective $\mathbf{Z}_p[\Delta_{r_2}]$-module. Therefore, as a $\mathbf{Z}_p[\Delta_{r_2}]$-module, $P_\tau^{(r_1)} \big/ I_{(r_1/r_2)} P_\tau^{(r_1)}$ has the properties which characterize $P_\tau^{(r_2)}$, and so the two are indeed isomorphic.

Let $N_{(r_1/r_2)} = \ker(\Delta_{r_1} \to \Delta_{r_2})$. We regard $P_\tau^{(r_1)}$ as a $\mathbf{Z}_p[N_{(r_1/r_2)}]$-module. It is a free module because it is projective and $N_{(r_1/r_2)}$ is a $p$-group. Now

$$P_\tau^{(r_1)} \big/ I_{(r_1/r_2)} P_\tau^{(r_1)} \;=\; \big(P_\tau^{(r_1)}\big)_{N_{(r_1/r_2)}} \quad .$$

Since $P_\tau^{(r_1)}$ is free over $\mathbf{Z}_p[N_{(r_1/r_2)}]$ and $N_{(r_1/r_2)}$ has order $p^{3(r_1\text{-}r_2)}$, we have

$$\mathrm{rank}_{\mathbf{Z}_p}\big(P_\tau^{(r_1)}\big) \;=\; p^{3(r_1\text{-}r_2)} \cdot \mathrm{rank}_{\mathbf{Z}_p}\big((P_\tau^{(r_1)})_{N_{(r_1/r_2)}}\big) \quad .$$

The statement about ranks then follows immediately from corollary 7.2.6. □

**Remark 7.3.7.** Let $\Delta_\infty = PGL_2(\mathbf{Z}_p)$ and let $\mathbf{Z}_p[[\Delta_\infty]]$ be the completed group algebra for $\Delta_\infty$ over $\mathbf{Z}_p$. These are the inverse limits of the $\Delta_r$'s and their group algebras $\mathbf{Z}_p[\Delta_r]$ under the maps mentioned above, respectively. For every $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta_0)$, there exists a projective indecomposable $\mathbf{Z}_p[[\Delta_\infty]]$-module $P_\tau^{(\infty)}$ which has $U_\tau$ as a quotient. It is uniquely determined up to isomorphism. The existence follows from proposition 7.3.6 since we can define $P_\tau^{(\infty)}$ as the inverse limit of the $P_\tau^{(r)}$'s. One sees that this is a direct summand in $\mathbf{Z}_p[[\Delta_\infty]]$, and hence projective. The uniqueness can be deduced from the corresponding fact for the $P_\tau^{(r)}$'s. One also sees that if $\Pi_\infty$ is a Sylow pro-$p$ subgroup of $\Delta_\infty$, then $P_\tau^{(\infty)}$ is a free $\mathbf{Z}_p[[\Pi_\infty]]$-module of rank 1 if $n(\tau) = 1$ or $n(\tau) = p$, and of rank 2 for all other $\tau$'s. Furthermore, any finitely-generated projective $\mathbf{Z}_p[[\Delta_\infty]]$ is isomorphic to a finite direct sum of those projective indecomposable modules. ◊

## 7.4 Extensions of $(\mathbf{Z}/p\mathbf{Z})^\times$ by a $p$-group.

Assume that $p$ is odd. We will consider various groups $\Delta$ which are extensions of $(\mathbf{Z}/p\mathbf{Z})^\times$ by a finite $p$-group $\Pi$. Thus, $\Pi$ will be a Sylow $p$-subgroup of $\Delta$ and will be normal. We then have an exact sequence

$$1 \longrightarrow \Pi \longrightarrow \Delta \longrightarrow \Omega \longrightarrow 1 \ , \tag{7.4.a}$$

where we will fix an isomorphism $\Omega \to (\mathbf{Z}/p\mathbf{Z})^\times$. That isomorphism will be of the form $\widetilde{\omega}$, where $\omega : \Omega \to \mathbf{Z}_p^\times$ is an injective homomorphism. In illustration 8.3 of the next chapter, we will take $\Omega = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ and $\omega$ will be the Teichmüller character. We will regard the powers $\omega^i$, $0 \le i \le p-2$, as representations of $\Omega$ and also of $\Delta$. The irreducible representations of $\Delta$ over a field of characteristic $p$ factor through $\Omega$ and are all defined over $\mathbf{F}_p$. They are the powers $\tau_i = \widetilde{\omega}^i$, where $0 \le i \le p-2$. The trivial representation will be denoted by $\tau_0$.

We will refer to such a group $\Delta$ as a $\Pi\Omega$-group. It will be understood that $\Pi$ is a $p$-group and that $\Omega$ is as above. We have a well-defined homomorphism $\Omega \to \mathrm{Aut}(\Pi)/\mathrm{Inn}(\Pi)$ in this situation, where $\mathrm{Inn}(\Pi)$ is the subgroup of $\mathrm{Aut}(\Pi)$ consisting of inner automorphisms of $\Pi$. This action is defined by conjugation. The group $\Delta$ is isomorphic to a semidirect product; one can identify $\Omega$ with a subgroup of $\Delta$ (non-canonically) and one then has a homomorphism $\Omega \to \mathrm{Aut}(\Pi)$. Such an identification will sometimes be helpful in the discussion. We then have $\Delta \cong \Pi \rtimes \Omega$.

**A.** *Relationship between* $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ *and* $\mathrm{Irr}_{\mathcal{F}}(\Pi)$. The homomorphism $\Omega \to \mathrm{Aut}(\Pi)/\mathrm{Inn}(\Pi)$ defines an action of $\Omega$ on the set $\mathrm{Irr}_{\mathcal{F}}(\Pi)$. Each orbit for that action has length dividing $p-1$. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, then $\sigma|_\Pi$ is isomorphic to a direct sum of irreducible representations of $\Pi$. Those summands constitute one orbit. Since $\Omega$ is cyclic, it follows that each summand occurs in $\sigma|_\Pi$ with multiplicity 1. (See [Fei], proposition 9.12.) Their degrees are equal and must divide $|\Pi|$. If $\pi$ is any one of these irreducible constituents in $\sigma|_\Pi$, then $n(\pi) = p^a$, where $a \ge 0$, and $n(\sigma) = dp^a$, where $d$ is the length of the corresponding orbit. Suppose that $N$ is the unique subgroup of $\Delta$ containing $\Pi$ and of index $d$. Then there exists an irreducible representation $\eta$ of $N$ such that $\eta|_\Pi \cong \pi$ and $\mathrm{Ind}_N^\Delta(\eta) \cong \sigma$. (See proposition 9.11 in [Fei].) Furthermore, the irreducible constituents of $\mathrm{Ind}_\Pi^\Delta(\pi)$ are the twists $\sigma \otimes \omega^j$, where $0 \le j < \frac{p-1}{d}$. They are not isomorphic because their determinants are distinct.

There is a natural action of $\Omega$ on $\mathrm{Irr}_{\mathcal{F}}(\Pi)$. Let $\widehat{\Omega}$ denote the character group of $\Omega$, which is just $\mathrm{Irr}_{\mathbf{Q}_p}(\Omega)$ and consists of the distinct powers of $\omega$. There is also a natural action of $\widehat{\Omega}$ on $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ which is defined as follows. If $\alpha \in \widehat{\Omega}$, then $\alpha$ defines a permutation of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ by sending any $\sigma$ to $\sigma \otimes \alpha$. To summarize the remarks in the previous paragraph, there is a one-to-one correspondence between the set of $\Omega$-orbits in $\mathrm{Irr}_{\mathcal{F}}(\Pi)$ and the set of $\widehat{\Omega}$-orbits in

$\mathrm{Irr}_{\mathcal{F}}(\Delta)$. The correspondence is defined by induction in one direction, and restriction in the other, as described above. In this correspondence, the product of the orbit lengths is $p-1$.

**B.** $\Pi$-*induced irreducible representations.* We will be especially interested in the case where $n(\sigma) = (p-1)p^a$. Then $\sigma \cong \mathrm{Ind}_{\Pi}^{\Delta}(\pi)$, where $\pi$ is an irreducible representation of $\Pi$ and $n(\pi) = p^a$. This occurs precisely when the orbit of $\pi$ under the action of $\Omega$ has length $p-1$. We will then say that $\sigma$ is *"$\Pi$-induced."* Thus, we have a one-to-one correspondence between the $\Omega$-orbits in $\mathrm{Irr}_{\mathcal{F}}(\Pi)$ of length $p-1$ and the $\Pi$-induced elements $\sigma$ in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. One property that such $\sigma$'s have is that

$$\widetilde{\sigma}^{ss} \;\cong\; \left(\bigoplus_{i=0}^{p-2} \tau_i\right)^{p^a} \quad . \tag{7.4.b}$$

The reason is that $\widetilde{\pi}^{ss} \cong (\widetilde{\pi}_0)^{p^a}$, where $\pi_0$ is the trivial representation of $\Pi$, and $\mathrm{Ind}_{\Pi}^{\Delta}(\pi_0)$ is just the regular representation of $\Omega$, regarded as a representation of $\Delta$. The congruence relations for $\Pi$-induced irreducible representations take a rather simple form. Suppose that $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ is $\Pi$-induced, we then have

$$\lambda(X,\sigma) \;=\; \frac{n(\sigma)}{p-1}\left(\sum_{i=0}^{p-2} \lambda(X,\omega^i)\right) \quad . \tag{7.4.c}$$

Alternatively, one can also deduce (7.4.c) from the equalities

$$\lambda(X,\sigma) = \lambda(X,\pi), \qquad \sum_{i=0}^{p\text{-}2} \lambda(X,\omega^i) = \lambda(X,\pi_0)$$

which follow from Frobenius Reciprocity. (See remark 2.1.8.) One then uses the equality $\lambda(X,\pi) = n(\pi)\lambda(X,\pi_0)$, a consequence of the fact that $X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a free $\mathbf{Q}_p[\Pi]$-module.

Of course, it may be that $\Delta$ has many irreducible representations which are not $\Pi$-induced. Some of the examples below will have no $\Pi$-induced irreducible representations; others will have many. Suppose that $\mathcal{Z}$ is the center of $\Pi$. Then $\Omega$ acts on the abelian group $\mathcal{Z}$ and on the dual of that group. Suppose that $\zeta$ is a character of $\mathcal{Z}$ whose orbit under the action of $\Omega$ has length $p-1$. Such $\zeta$'s exist if and only if the map $\Omega \to \mathrm{Aut}(\mathcal{Z})$ is injective. If $\pi$ is any irreducible constituent of $\mathrm{Ind}_{\mathcal{Z}}^{\Pi}(\zeta)$, then $\mathcal{Z}$ acts on the underlying space of $\pi$ by $\zeta$. That is, $\pi$ has $\zeta$ as its central character. The orbit of $\pi$ under the action of $\Omega$ also has length $p-1$. It follows that if $\sigma$ is any irreducible constituent in $\mathrm{Ind}_{\mathcal{Z}}^{\Delta}(\zeta)$, then $\sigma$ is $\Pi$-induced.

We remark that if $\Delta$ has at least one $\Pi$-induced representation $\sigma$, then $\Delta$ has just one block. This is so because $\widetilde{\sigma}^{ss}$ has all the elements of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ as its constituents.

**C.** *The indecomposable projective modules.* Before discussing the examples, we make some remarks about the indecomposable projective $\mathbf{Z}_p[\Delta]$-modules $P_{\tau_i}$. These are defined for $0 \leq i \leq p-2$. Their direct sum is a free $\mathbf{Z}_p[\Delta]$-module of rank 1. Each of the $P_{\tau_i}$'s is a free $\mathbf{Z}_p[\Pi]$-module of rank 1. Furthermore, one has

$$P_{\tau_i} \;\cong\; P_{\tau_0} \otimes \omega^i \tag{7.4.d}$$

as $\mathbf{Z}_p[\Delta]$-modules. Here, when we write $P \otimes \omega^i$, where $P$ is a $\mathbf{Z}_p[\Delta]$-module, we mean $P \otimes_{\mathbf{Z}_p} L_{\omega^i}$, where $L_{\omega^i}$ is a free $\mathbf{Z}_p$-module of rank 1 on which $\Delta$ acts by $\omega^i$. Thus, $P_{\tau_i}$ is just a twist of $P_{\tau_0}$. The justification is simply to observe that the $\mathbf{Z}_p[\Delta]$-module on the right side of (7.4.d) has $U_{\tau_i}$ as a quotient module and that it is projective and indecomposable. The last fact follows by noting that it is a free $\mathbf{Z}_p[\Pi]$-module of rank 1.

The $P_{\tau_i}$'s have the following description which was suggested by R. Pollack. For each $i$, the idempotent $e_{\omega^i} \in \mathbf{Z}_p[\Omega]$ can be regarded as an element of $\mathbf{Z}_p[\Delta]$. The left ideal $\mathbf{Z}_p[\Delta]e_{\omega^i}$ of the ring $\mathbf{Z}_p[\Delta]$ is a direct summand and hence is a projective $\mathbf{Z}_p[\Delta]$-module. The maximal semisimple quotient of $\mathbf{Z}_p[\Delta]$ is isomorphic to the direct sum of all the $U_{\tau_j}$'s, each with multiplicity 1. The maximal semisimple quotient of $\mathbf{Z}_p[\Delta]e_{\omega^i}$ is then seen to be $U_{\tau_i}$. Thus, $\mathbf{Z}_p[\Delta]e_{\omega^i}$ is indeed isomorphic to the projective hull of $U_{\tau_i}$, which is $P_{\tau_i}$. In effect, $P_{\tau_i}$ can be described as $\mathrm{Ind}_{\Omega}^{\Delta}(L_{\omega^i})$. The fact that the direct sum of these modules (over $0 \leq i \leq p-2$) is a free $\mathbf{Z}_p[\Delta]$-module of rank 1 follows immediately from the fact that the direct sum of the $L_{\omega^i}$'s is a free $\mathbf{Z}_p[\Omega]$-module of rank 1.

**D.** *Various families of* $\Pi\Omega$*-groups.* We consider certain specific families of groups in the rest of this chapter. We are primarily interested in these groups because they can arise as Galois groups in a natural way.

The simplest examples occur when $\Pi$ is cyclic. For each $i$, $0 \leq i \leq p-2$, we will let $\Gamma_i$ denote a group isomorphic to $\mathbf{Z}_p$ on which $\Omega$ acts by the character $\omega^i : \Omega \to \mathbf{Z}_p^{\times}$. We will use a multiplicative notation for $\Gamma_i$. For any $r \geq 0$, we let $\Pi = \Gamma_i/\Gamma_i^{p^{r+1}}$. We then have an action of $\Omega$ on $\Pi$. The corresponding semidirect product $\Delta = \Pi \rtimes \Omega$ has order $(p-1)p^{r+1}$ and is a quotient of the profinite group $\Gamma_i \rtimes \Omega$. The representation theory of $\Delta$ is rather easy to describe. Let $d_i$ denote the order of the character $\omega^i$. Then, apart from the orbit of $\pi_0$, the orbits in $\mathrm{Irr}_{\mathcal{F}}(\Pi)$ for the action of $\Omega$ have length $d_i$. Thus, the irreducible representations of $\Delta$ are either of degree 1 or of degree $d_i p^a$ where $a \geq 0$. If $gcd(i, p-1) = 1$, then $d_i = p-1$ and every $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ is either a power of $\omega$ or is $\Pi$-induced. Somewhat more general examples occur if $\Pi$ is a direct product of groups of the form $\Gamma_i/\Gamma_i^{p^j}$ for various $i$'s and $j$'s.

The next example gives generalizations of the profinite groups $\Gamma_i$ and $\Gamma_i \rtimes \Omega$. Suppose that $\boldsymbol{t} = (t_0, ..., t_{p\text{-}2})$ is a $(p-1)$-tuple of nonnegative integers. Let $g = \sum_{i=0}^{p-2} t_i$. We will let $\Gamma_{\boldsymbol{t}}$ denote a free pro-$p$ group on $g$ generators with an action of $\Omega$ defined as follows. Fix

the generating set $G$. Partition $G$ as a disjoint union of $p-1$ subsets $G_i$, each of cardinality $t_i$, where $0 \leq i \leq p-2$. If $\alpha \in \Omega$ and $x \in G_i$, we define $\alpha(x)$ to be $x^{\omega^i(\alpha)}$. Since $\Gamma_{\boldsymbol{t}}$ is free, $\alpha$ extends uniquely to a continuous automorphism of $\Gamma_{\boldsymbol{t}}$. This defines a homomorphism $\Omega \to \mathrm{Aut}(\Gamma_{\boldsymbol{t}})$. The semidirect product $\Gamma_{\boldsymbol{t}} \rtimes \Omega$ is a profinite $\Pi\Omega$-group, where one takes $\Pi = \Gamma_{\boldsymbol{t}}$.

**D1.** *The groups $B_r$.* Next we consider the groups $B_r$ which occurred in section 7.3. We let $\beta$ be as defined there. The Sylow $p$-subgroup of $B_r$ is precisely $ker(\beta)$. We will denote it by $P_r$. It is normal and $\beta$ gives an isomorphism $B_r/P_r \cong (\mathbf{Z}/p\mathbf{Z})^\times$. (We use $\beta$ instead of $\omega$ here to avoid confusion in section 8.3. In fact, $\beta$ and $\omega$ will not necessarily be the same.) We will continue to use the notation from section 7.3. Thus, we let $\Delta_r$ denote $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$. For $r = 0$, $B_0$ is the group $B$ discussed in section 7.2. See remark 7.2.2 for its irreducible representations. The representation $\gamma$ defined there will now be denoted by $\gamma_0$.

Assume that $r \geq 1$ from here on. The subgroup $U_r$ of $B_r$ is normal and is cyclic of order $p^{r+1}$. The quotient group $B_r/U_r$ is cyclic of order $(p-1)p^r$ and acts faithfully on $U_r$. All the characters of $U_r$ of order $p^{r+1}$ are conjugate by this action. The number of such characters is $(p-1)p^r$. Suppose that $u_r$ is one of those characters. Let

$$\gamma_r \;=\; \mathrm{Ind}_{U_r}^{B_r}(u_r) \quad ,$$

a representation of $B_r$ of degree $b_r = (p-1)p^r$. If $\gamma'$ is any irreducible constituent of $\gamma_r$, then $\gamma'|_{U_r}$ has $u_r$ and all of its conjugates as constituents. Hence $\gamma'$ has degree at least $b_r$. It follows that $\gamma_r$ is an irreducible representation of $B_r$. It is also clear that if $\rho$ is an irreducible representation of $B_r$ such that $\rho|_{U_r}$ is faithful, then $\rho \cong \gamma_r$. One sees easily that $\gamma_r$ is faithful and is therefore the unique irreducible representation of $B_r$ with that property. It will play an important role for studying representations of other groups.

If $0 \leq s < r$, then we have a natural surjective homomorphism $B_r \to B_s$ and so $\gamma_s$ can be considered as an irreducible representation of $B_r$. The irreducible representations of $B_r$ are of the following types: the one-dimension representations $\psi$ corresponding to the characters of $B_r/U_r$, the representations of the form $\gamma_s \otimes \psi$, where $0 \leq s \leq r$ and $\psi$ is one-dimensional. The second type have degree divisible by $p-1$ and hence are $P_r$-induced. Furthermore, If $\psi$ and $\psi'$ are one-dimensional, then $\gamma_s \otimes \psi \cong \gamma_s \otimes \psi'$ if and only if $\psi'\psi^{-1}$ factors through $B_s$. The above remarks are easily verified. They also follow from a standard theorem about the irreducible representations of a semidirect product. (See [Se77], chapter 8.2.) In this case, $B_r$ is the semidirect product of $T_r$ and $U_r$, where $T_r$ is the subgroup of $\Delta_r$ represented by diagonal matrices.

Apart from $\gamma_r$, the kernels of all of the other irreducible representations of $B_r$ contain $U_r[p]$, the unique subgroup of $U_r$ of order $p$. This subgroup $U_r[p]$ is the center of $P_r$. It will be useful to define $\Omega_r$ to be the unique subgroup of $T_r$ of order $p-1$. It is the group denoted

by $C_r$ in the proof of proposition 7.3.1 and is identified with $B_r/P_r$ in the obvious way. One sees easily that $\Omega_r$ acts on $U_r$, and hence on $U_r[p]$, by the character $\beta$.

**D2.** *Some groups containing $B_r$.* Fix an $r \geq 1$. Assume that $H$ is a subgroup of $\Delta_r$ which contains $B_r$. We will also assume that the image of $H$ in $\Delta_0$ is precisely $B_0$. Let $\Pi$ denote the inverse image of $U_0$, which is the Sylow $p$-subgroup of $H$. Thus, $\Pi$ is a normal subgroup and $H/\Pi \cong \Omega$. It is not difficult to show that any such subgroup $H$ is the inverse image of $B_s$ under the map $\Delta_r \to \Delta_s$, where $0 \leq s \leq r$. The kernel of that map is precisely the image of $I + p^{s+1}M_2(\mathbf{Z}_p)$ in $\Delta_r$, where we let $M_2(\mathbf{Z}_p)$ denote the ring of $2 \times 2$ matrices over $\mathbf{Z}_p$ and $I$ denotes its identity element.

One of the main examples that we have in mind is the group $H_r$ defined in the proof of proposition 7.3.1, which corresponds to $s = 0$. Another example corresponds to $s = 1$, the inverse image of $B_1$ under the map $\Delta_r \to \Delta_1$. We denote that group by $H'_r$. Both groups will occur naturally as Galois groups in section 8.3. In particular, see the remarks following proposition 8.3.7. We denote their Sylow $p$-subgroups by $\Pi_r$ and $\Pi'_r$, respectively.

The following result singles out a special class of irreducible representations of any $H$ satisfying the above assumptions. The notation in the statement and proof comes from the preceding discussion of the irreducible representations of $B_r$. The properties of $\gamma_r$ play an important role, especially the facts that $n(\gamma_r) = (p-1)p^r$ and that this is equal to $b_r$, the degree of the elements of $\mathcal{B}_r$. The results concern irreducible representations $\xi$ of $H$ which are $r$-primitive. This just means that $\xi$ does not factor through the image of $H$ under the map $\Delta_r \to \Delta_{r\text{-}1}$.

**Proposition 7.4.1.** *Suppose that $\xi$ is an irreducible representation of $H$. Then we have the inequality $n(\xi) \leq (p-1)p^r$. The following statements are equivalent:*

$$(i)\ \ n(\xi) = (p-1)p^r, \qquad (ii)\ \ \xi \text{ is faithful}, \qquad (iii)\ \ \xi|_{B_r} \cong \gamma_r \ \ .$$

*If $\xi$ satisfies any of these statements, then $\xi$ is $r$-primitive and $\Pi$-induced.*

*If $\sigma$ is any $r$-primitive, irreducible representation of $\Delta_r$, then $\sigma|_H$ has exactly one irreducible constituent $\xi$ which has degree $(p-1)p^r$. The multiplicity of $\xi$ in $\sigma|_H$ is 1. If $\sigma \in \mathcal{B}_r$, then $\sigma|_H$ is irreducible.*

*If $\xi$ is any $r$-primitive, irreducible representation of $H$, then $\xi$ is a constituent in $\sigma|_H$ for some $r$-primitive, irreducible representation $\sigma$ of $\Delta_r$. If $\xi$ has degree $(p-1)p^r$, then the number of such $\sigma$'s is at most $[\Delta_r : H]$.*

*Proof.* Suppose that $\xi$ is an irreducible representation of $H$. If $\xi|_{B_r}$ has a constituent $\psi$ of degree 1, then $\xi$ is a constituent in $\mathrm{Ind}_{B_r}^H(\psi)$. We would then have $n(\xi) \leq p^r$ since $[H : B_r]$

divides $[H_r : B_r] = p^r$. On the other hand, if none of the irreducible constituents in $\xi|_{B_r}$ has degree 1, then their degrees are divisible by $p-1$ and hence the same is true for the degree of $\xi$. Since $n(\xi)$ divides $|H|$, we therefore have $n(\xi) = (p-1)p^t$ for some $t \geq 0$. Now any such $\xi$ will be a constituent in $\sigma|_H$ for some $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_r)$. One can just take $\sigma$ to be any irreducible constituent in $\mathrm{Ind}_H^{\Delta_r}(\xi)$. It follows that

$$n(\xi) \ \leq \ n(\sigma) \ \leq \ a_r \ = \ (p+1)p^r \quad .$$

One deduces that $t \leq r$. In both cases, we have $n(\xi) \leq (p-1)p^r$.

The equivalence of *(i)* and *(iii)* is obvious. If *(ii)* is true, then $\xi|_{B_r}$ is also faithful and must therefore contains $\gamma_r$ as an irreducible constituent. Otherwise, we would have $U_r[p] \subseteq \ker(\xi)$. We've shown that $n(\xi) \leq (p-1)p^r$. Since $n(\gamma_r) = (p-1)p^r$ too, we must have $\xi|_{B_r} \cong \gamma_r$. Therefore, *(ii)* implies *(iii)*. For the opposite implication, we assume temporarily that $H = H_r$, which slightly simplifies the argument. Assume that $\xi$ satisfies *(iii)*. Then $\xi|_{B_r}$ is faithful. Thus, so are $\xi|_{\Omega_r}$ and $\xi|_{U_r}$. Since all subgroups of $H_r$ of order prime to $p$ are conjugate to a subgroup of $\Omega_r$, it follows that $\ker(\xi)$ is a $p$-group. Thus, $\ker(\xi)$ is a normal subgroup of $\Pi_r$. Let $\mathcal{Z}_r$ be the center of the $p$-group $\Pi_r$. If $\ker(\xi)$ is nontrivial, then so is $\ker(\xi) \cap \mathcal{Z}_r$. However, we will next show that $\mathcal{Z}_r = U_r[p]$. Since $\ker(\xi)$ can't contain $U_r[p]$, it follows that $\ker(\xi)$ is indeed trivial, and so *(ii)* is true. Also, it is then clear that $\xi$ is $r$-primitive. Its degree is divisible by $p-1$ and so $\xi$ is also $\Pi$-induced.

Let $N_s$ be the kernel of the map $\Delta_r \to \Delta_s$ for $0 \leq s \leq r-1$. In fact, $N_s$ is the image of $I + p^{s+1}M_2(\mathbf{Z}_p)$ in $\Delta_r$, as previously mentioned. Then $N_0$ is a $p$-group and it is easy to verify that the center of $N_0$ is precisely $N_{r\text{-}1}$ and consists of the elements of order dividing $p$ in $N_0$. (Note that for $p = 3$, $\Delta_r$ contains elements of order $p$ which are not in $N_0$.) We have $N_0 \subset \Pi_r$ and the index is $p$. There is a well-defined action (by conjugation) of $\Pi_r/N_0$ on the 3-dimensional $\mathbf{F}_p$-vector space $N_{r\text{-}1}$. Now $\Pi_r/N_0$ can be identified with the image of $\Pi_r$ in $B_0$, which is just the subgroup $U_0$ of $B_0$. One verifies easily that $N_{r\text{-}1}^{U_0} = U_r[p]$. Thus, $U_r[p]$ is indeed the center of $\Pi_r$.

For the rest, we need some observations about $\sigma|_{B_r}$, where $\sigma$ is an $r$-primitive, irreducible representation of $\Delta_r$. The restriction $\sigma|_{U_r}$ must be faithful. To see this, consider the normal subgroup $N_{r\text{-}1}$ of $\Delta_r$ defined above. It is a vector space over $\mathbf{F}_p$ of dimension 3. The action of $\Delta_r$ (by conjugation) on $N_{r\text{-}1}$ factors through $\Delta_0$ and coincides with $\tau_{\mathbf{3},1}$ (in the notation from part **B** of section 7.2). Thus $\Delta_r$ acts irreducibly on $N_{r\text{-}1}$ and hence there are no proper subgroups of $N_{r\text{-}1}$ which are normal in $\Delta_r$. In particular, since $\ker(\sigma)$ doesn't contain $N_{r\text{-}1}$, $\sigma|_{N_{r\text{-}1}}$ is faithful. The unique subgroup $U_r[p]$ of $U_r$ of order $p$ is contained in $N_{r\text{-}1}$. Therefore, $\sigma|_{U_r}$ is indeed faithful.

It follows that $\sigma|_{B_r}$ must contain $\gamma_r$ as a constituent. Otherwise, $\ker(\sigma)$ would contain $U_r[p]$. Furthermore, $\sigma|_{B_r}$ has degree $n(\sigma) = a_r$, $b_r$, or $c_r$ (as defined in section 7.3) and $\gamma_r$

has degree $b_r$. We have the inequalities

$$b_r \ < \ c_r \ < \ a_r \ \leq \ 2b_r \ . \tag{7.4.e}$$

Also, if $\sigma \in \mathcal{A}_r$, then $\sigma|_{B_r}$ contains two 1-dimensional representations of $B_r$. It follows that the multiplicity $\langle \sigma|_{B_r}, \gamma_r \rangle$ must be 1. (For $p \geq 5$, this can be seen more easily because the last inequality in (7.4.e) is then strict.) If $\sigma \in \mathcal{B}_r$, then $n(\sigma) = n(\gamma_r)$ and so we obviously have $\sigma|_{B_r} \cong \gamma_r$.

Still assuming that $\sigma$ is an $r$-primitive element of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$, consider $\sigma|_H$. Exactly one irreducible constituent $\xi$ in $\sigma|_H$ will have the property that $\xi|_{B_r}$ has $\gamma_r$ as an irreducible constituent. However, since $n(\xi) \leq n(\gamma_r)$, it is clear that we have $\xi|_{B_r} \cong \gamma_r$, that $\xi$ is the unique constituent in $\sigma|_H$ satisfying *(iii)*, or the equivalent statement *(i)*. That $\xi$ will be referred to as the "$\gamma_r$-constituent" of $\sigma|_H$ in the rest of this argument. It has multiplicity 1. If $\sigma \in \mathcal{B}_r$, then we clearly have $\sigma|_H \cong \xi$.

Now suppose that $\xi$ is any irreducible representation of $H$. Let $\sigma$ be an irreducible constituent in $\mathrm{Ind}_H^{\Delta_r}(\xi)$. Then Frobenius Reciprocity implies that $\xi$ is an irreducible constituent in $\sigma|_H$. If $\xi$ is $r$-primitive, then $\sigma$ will clearly be $r$-primitive too. If $n(\xi) = (p-1)p^r$, then $\xi$ must be the $\gamma_r$-constituent in $\sigma|_H$. We can now show that $\xi$ satisfies *(ii)*. For it is clear that $\xi$ is the restriction to $H$ of the $\gamma_r$-constituent of $\sigma|_{H_r}$, which we've shown is faithful. The restriction $\xi$ to $H$ will also be faithful.

Finally, if we assume that $n(\xi) = b_r$, then the degree of $\mathrm{Ind}_H^{\Delta_r}(\xi)$ is $[\Delta_r : H]b_r$. Each irreducible constituent is $r$-primitive and hence has degree at least $b_r$. Therefore, the number of such constituents is at most $[\Delta_r : H]$ as stated. □

**Remark 7.4.2.** If $H = H_r$ and $\xi$ satisfies $n(\xi) = b_r$, then each irreducible constituent in $\mathrm{Ind}_H^{\Delta_r}(\xi)$ will be $r$-primitive and hence of degree $a_r, b_r$, or $c_r$. The triplet $(x, y, z)$ giving the number of constituents of each type will satisfy the equation

$$a_r x + b_r y + c_r z \ = \ (p+1)b_r$$

and one finds that there are just the following possible triplets:

$$(0,\ 0,\ p), \qquad (0,\ p+1,\ 0), \qquad (p-1,\ 0,\ 0), \qquad (\ \tfrac{1}{2}(p-1),\ \tfrac{1}{2}(p+1),\ 0) \ .$$

We don't know if all these possibilities occur. ◊

**Remark 7.4.3.** We will introduce another type of irreducible representation of $H$. Suppose that $\psi$ is a primitive character of $B_r/U_r$ and that $H$ is a subgroup of $\Delta_r$ of the kind considered in proposition 7.4.1. Let $\xi_{H,\psi}$ denote $\mathrm{Ind}_{B_r}^{H}(\psi)$. Since $\mathrm{Ind}_H^{\Delta_r}(\xi_{H,\psi})$ is isomorphic to the irreducible representation $\sigma = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi)$ of $\Delta_r$, it follows that $\xi_{H,\psi}$ is an irreducible

representation of $H$. It is an irreducible constituent in $\sigma|_H$ which must be different than the faithful irreducible constituent $\xi$ described in proposition 7.4.1. This is simply because $n(\xi_{H,\psi}) = [H : B_r]$, which is a power of $p$. Also, note that $\xi_{H,\psi}|_{B_r}$ has $\psi$ as a constituent. This implies that $\xi_{H,\psi}$ is $r$-primitive.

Now $\psi^{-1}$ is also a constituent in $\sigma|_{B_r}$ and hence $\xi_{H,\psi^{-1}}$ is another irreducible constituent in $\sigma|_H$. Both $\xi_{H,\psi}$ and $\xi_{H,\psi^{-1}}$ have degree equal to $[H : B_r]$, which is a power of $p$, but they are not isomorphic. To see this, note that $\psi = \beta^j\theta$, where $0 \leq j \leq p-2$ and $\theta$ is a character of $B_r/U_r$ of order $p^r$. Here $\beta$ is the basic character of $B_0$ defined in section 7.2, viewed as a character of $B_r$ and also of $H$. If $\mathrm{Ind}_{B_r}^H(\psi) \cong \mathrm{Ind}_{B_r}^H(\psi^{-1})$, then $\mathrm{Ind}_{B_r}^H(\beta^{2j}\theta) \cong \mathrm{Ind}_{B_r}^H(\theta^{-1})$. We would then have $\mathrm{Ind}_{B_r}^{\Delta_r}(\beta^{2j}\theta) \cong \mathrm{Ind}_{B_r}^{\Delta_r}(\theta^{-1})$. Such an isomorphism can only occur if $\beta^{2j}\theta$ and $\theta^{-1}$ are either equal or inverses of each other, neither of which is possible since $p$ is odd and $r \geq 1$.

It follows that $\psi$ is the only 1-dimensional constituent of $\xi_{H,\psi}|_{B_r}$. A similar statement is true for $\xi_{H,\psi^{-1}}$. Furthermore, the 1-dimensional constituents in $\sigma|_{B_r}$ are just $\psi$ and $\psi^{-1}$. All other irreducible constituents in $\sigma|_{B_r}$ have degree divisible by $p-1$. Therefore, all the other irreducible constituents in $\sigma|_H$ have degree divisible by $p-1$. Those degrees must be of the form $(p-1)p^s$ and hence those constituents are certainly $\Pi$-induced. In contrast, since $\xi_{H,\psi}$ and $\xi_{H,\psi^{-1}}$ are of degree $p^s$ for some $s$, their restrictions to $\Pi$ must remain irreducible.

In summary, if $[H : B_r] = p^s$, then $H$ has $(p-1)^2p^{r-1}$ non-isomorphic, $r$-primitive irreducible representations of degree $p^s$. They all occur as constituents in $\sigma|_H$ for some $\sigma \in \mathcal{A}_r$. $\Diamond$

**D3.** *The groups $H_r$ and $H_r'$.* We continue to assume that $r \geq 1$. The following result about the irreducible constituents of $\sigma|_{H_r}$, where $\sigma$ is any $r$-primitive element in $\mathrm{Irr}_{\mathcal{F}}(\Delta_r)$, gives complete information about the degrees of the $r$-primitive, irreducible representations of $H_r$.

**Proposition 7.4.4.** *If $\sigma \in \mathcal{A}_r$, then $\sigma|_{H_r}$ has three non-isomorphic irreducible constituents, two of degree $p^r$ and one of degree $(p-1)p^r$. If $\sigma \in \mathcal{B}_r$, then $\sigma|_{H_r}$ is irreducible. If $\sigma \in \mathcal{C}_r$, then $\sigma|_{H_r}$ has two irreducible constituents, one of degree $(p-1)p^r$, the other of degree $(p-1)p^{r-1}$. All of the above irreducible representations of $H_r$ are $r$-primitive. Up to isomorphism, there are $p^r$ of degree $(p-1)p^r$, $p^r$ of degree $(p-1)p^{r-1}$, and $(p-1)^2p^{r-1}$ of degree $p^r$.*

*Proof.* Remark 7.4.3 and proposition 7.4.1 show that if $\sigma \in \mathcal{A}_r$, then $\sigma|_{H_r}$ indeed has at least three irreducible constituents and their degrees are as stated. No others constituents exist because the sum of those degrees is $n(\sigma)$. They are indeed $r$-primitive. The irreducibility of $\sigma|_{H_r}$ for $\sigma \in \mathcal{B}_r$ is already in proposition 7.4.1. That representation is faithful and hence certainly $r$-primitive. Suppose now that $\sigma \in \mathcal{C}_r$. Let $\xi$ be the faithful, irreducible constituent

of $\sigma|_{H_r}$. Then

$$\sigma|_{H_r} \;\cong\; \xi \;\oplus\; \xi'$$

where $n(\xi') = c_r - b_r = (p-1)p^{r-1}$. Observe that if $\xi''$ is an irreducible constituent of $\xi'$, then Frobenius Reciprocity implies that $\sigma$ is a constituent in $\mathrm{Ind}_{H_r}^{\Delta_r}(\xi'')$, a representation of degree $(p+1)n(\xi'')$. Hence

$$n(\xi'') \;\geq\; \frac{n(\sigma)}{p+1} \;=\; (p-1)p^{r\text{-}1} \;=\; n(\xi')$$

and therefore $\xi'' = \xi'$. This proves the irreducibility of $\xi'$. We also see that $\sigma \cong \mathrm{Ind}_{H_r}^{\Delta_r}(\xi')$. Now since $r \geq 1$, $H_r$ contains $N_{r\text{-}1} = \ker(\Delta_r \to \Delta_{r\text{-}1})$. This subgroup of $\Delta_r$ is normal and hence, if $N_{r\text{-}1} \subseteq \ker(\xi')$, then $N_{r\text{-}1}$ is also contained in the kernel of $\mathrm{Ind}_{H_r}^{\Delta_r}(\xi') = \sigma$. Since this isn't possible, $\xi'$ must indeed be $r$-primitive.

Concerning the numbers of irreducible, $r$-primitive representation of the three possible degrees, the stated result follows in a straightforward way by using the fact that for any finite group $H$, we have $\sum_\xi n(\xi)^2 = |H|$, where $\xi$ varies over $\mathrm{Irr}_{\mathcal{F}}(H)$. The $\xi$'s where $n(\xi) = (p-1)p^r$ are characterized as follows: they are the irreducible representations of $H_r$ which do not factor through $H_r/U_r[p]$. Hence, if $\xi$ varies over just those representations, then $\sum_\xi n(\xi)^2 = |H_r| \cdot \left(1 - \frac{1}{p}\right)$. For the $\xi$'s such that $n(\xi) = p^r$, they are of the form $\xi_{H_r,\psi}$, where $\psi$ is a uniquely determined primitive character of $(\mathbf{Z}/p^{r+1}\mathbf{Z})^\times$. Their number is obviously as stated. The remaining $\xi$'s all have degree $n(\xi) = (p-1)p^{r\text{-}1}$, and their number is then easily determined since if $\xi$ varies over *all* the $r$-primitive, irreducible representations of $H_r$, then $\sum_\xi n(\xi)^2 = |H_r| - |H_{r\text{-}1}|$. $\square$

**Remark 7.4.5.** The above result shows the existence of $p^r$ irreducible representations $\xi$ of $H_r$ of degree $b_r = p^r(p-1)$. These are precisely the faithful, irreducible representations. We don't have an equally precise statement about $H_r'$. However, there are also many faithful, irreducible representations of $H_r'$ according to proposition 7.4.1. Every such $\xi$ is a constituent in $\sigma|_{H_r'}$ for some irreducible, $r$-primitive representation $\sigma$ of $\Delta_r$, and has multiplicity 1. Furthermore, the number of such $\sigma$'s is at most $[\Delta_r : H_r'] = (p+1)p$. It follows that the number of isomorphism classes of such $\xi$'s is bounded below by $c_1 p^r$ and above by $c_2 p^r$ for some positive constants $c_1,\ c_2$. We also have many irreducible representations of $H_r'$ of degree $[H_r' : B_r] = p^{r\text{-}1}$. The number of isomorphism classes has similar upper and lower bounds. $\Diamond$

**Remark 7.4.6.** The $H_r$'s form an inverse system under the obvious maps. We will let $H_\infty$ denote the corresponding inverse limit. The surjectivity of those maps shows that all of the $H_r$'s are quotients of the profinite groups $H_\infty$. Thus, proposition 7.4.4 gives us the

degrees of the irreducible representations of $H_\infty$ with open kernel. Each such representation is $r$-primitive for a certain value of $r$. Similarly, we will let $H'_\infty$ denote the inverse limit of the $H'_r$'s and consider representations of $H'_r$ for $r \geq 0$ as representations of $H'_\infty$. Both of those groups are examples of $p$-adic Lie groups of dimension 3. We also will consider $B_\infty$, the inverse limit of the $B_r$'s under the obvious maps. We can identify $B_\infty$ with a subgroup of $H'_\infty$, which in turn is a subgroup of $H_\infty$. However, $B_\infty$ is a $p$-adic Lie group of dimension 2. We also define $U_\infty$ to be the inverse limit of the $U_r$'s, which is a normal subgroup of $B_\infty$. It is clear that $U_\infty$ is isomorphic to the additive group of $\mathbf{Z}_p$ and is a $p$-adic Lie group of dimension 1. $\Diamond$

**Remark 7.4.7.** The proof of proposition 7.4.4 shows that if $\sigma \in \mathcal{C}_r$, then $\sigma \cong \mathrm{Ind}_{H_r}^{\Delta_r}(\xi')$, where $\xi'$ is an irreducible representation of $H_r$ of degree divisible by $p-1$. Since $\xi'$ must be $\Pi_r$-induced, if one lets $\pi'$ be any irreducible constituent in $\xi'|_{\Pi_r}$, then $\sigma \cong \mathrm{Ind}_{\Pi_r}^{\Delta_r}(\pi')$. We have $n(\pi') = p^{r\text{-}1}$. Furthermore, $\widetilde{\pi'}^{ss} \cong \widetilde{\pi}_0^{\,n(\pi')}$. Therefore, we have

$$\sigma \;\approx\; \mathrm{Ind}_{\Pi_r}^{\Delta_r}(\pi_0)^{p^{r\text{-}1}}$$

for any $\sigma \in \mathcal{C}_r$. Here we use the notation from the proof of proposition 7.3.1. Consequently, it follows that $\widetilde{\sigma}^{ss}$ is the same for all such $\sigma$'s, a fact already used in the proof of proposition 7.3.1. $\Diamond$

**Remark 7.4.8.** Suppose that $\sigma \in \mathcal{B}_r$. We can use proposition 7.4.4 to determine $det(\sigma)$, which was left unresolved in remark 7.3.4. Of course, $det(\sigma)$ is either $\sigma_0$ or $\sigma_{\mathbf{1}}$. Thus, it is clearly determined by the irreducible representation $\xi = \sigma|_{H_r}$ of $H_r$. The abelianization of $H_r$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^\times$. It follows that the determinant of any representation of $H_r$ is a power of $\beta$ and is determined completely by the reduced representation. Thus, it suffices to determine $det(\widetilde{\xi})$. Since $\xi$ is $\Pi_r$-induced, we can apply (7.4.b). It follows that

$$det(\widetilde{\xi}) \;=\; \left(\widetilde{\omega}^{\frac{p-1}{2}}\right)^{p^r} \;=\; \widetilde{\omega}^{\frac{p-1}{2}}$$

which has order 2. Consequently, $det(\sigma) = \sigma_{\mathbf{1}}$ for all $\sigma \in \mathcal{B}_r$. That assertion can also be deduced easily just using the fact that $\sigma|_{B_r} \cong \gamma_r$.

The same argument shows that if $\xi$ is any irreducible representation of $H_r$ of degree divisible by $p-1$, then $det(\xi)$ is the quadratic character of $H_r$. $\Diamond$

**Remark 7.4.9.** Now we discuss the congruence relations for $H_r$. One can simply apply (7.4.c) for the representations which have degree divisible by $p-1$. The remaining irreducible representations are of the form $\xi_{H_r,\psi}$ and have degree $p^r$. The congruence relations for those irreducible representations are somewhat different, but also easily described. We refer to the

very end of the proof of proposition 7.3.1. Let $d_r = \frac{p^r-1}{p-1}$ as in that proposition. Suppose that $\psi$ is a primitive character of $B_r/U_r$ and let $j$ be such that $\widetilde{\psi} = \widetilde{\beta}^j$. Then we have

$$\xi_{H_r,\psi} \;\approx\; \left(\bigoplus_{i=0}^{p-2} \beta^i\right)^{d_r} \;\oplus\; \beta^j \quad .$$

As before, we fix an isomorphism $\omega : \Omega \to (\mathbf{Z}/p\mathbf{Z})^\times$. The map $\beta$ will be a power $\omega^b$ for some $b$ satisfying $gcd(b, p-1) = 1$. Thus, if $X$ is a quasi-projective $\mathbf{Z}_p[H_r]$-module, then one has the congruence relation

$$\lambda\big(X, \xi_{H_r,\psi}\big) \;=\; d_r \sum_{i=0}^{p-2} \lambda(X, \omega^i) + \lambda(X, \omega^{bj}) \quad . \tag{7.4.f}$$

Similar comments apply to the group $H'_r$ for all the irreducible representations which have degree divisible by $p-1$ and for the additional ones of the form $\xi_{H'_r,\psi}$. $\Diamond$

# 8 Some arithmetic illustrations.

We will discuss a number of special cases illustrating the results of the previous chapters under various sets of simplifying assumptions. We will not strive for generality. We always assume that $E$ has good, ordinary reduction at $p$. Our objective is mainly to describe the behavior of $\lambda_E(\sigma)$ for various families of irreducible Artin representations $\sigma$ of $G_F$. It will be useful to note that $\lambda_E(\sigma)$ really depends just on $\sigma$ and $E$. That is, if $\Delta = \mathrm{Gal}(K/F)$ and if $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ factors through $\Delta' = \mathrm{Gal}(K'/F)$, where $K'$ is a subfield of $K$ and is Galois over $F$, then the multiplicities of $\sigma$ in $X_E(K_\infty) \otimes_{\mathbf{Z}_p} \mathcal{F}$ and in $X_E(K'_\infty) \otimes_{\mathbf{Z}_p} \mathcal{F}$ are equal. This follows immediately from proposition 4.3.1. A similar remark is true for the invariants $\lambda_E^{\Sigma_0}(\sigma)$.

## 8.1 An illustration where $\Sigma_0$ is empty.

One of the principal examples that we have in mind arises in the following way. We assume that $p \geq 5$. Suppose that $A$ is an elliptic curve defined over $F$ (which might or might not be related to $E$). We will use $A$ just to generate interesting extensions of $F$. Assume that $A$ is non-CM and that $p$ is a prime for which the representation $\rho_A : G_F \longrightarrow \mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(A)\big)$ is surjective. This will be true for all but finitely many primes $p$ by a well-known theorem of

Serre [Se72]. Therefore, for every $r \geq 0$, $\mathrm{Gal}\big(F(A[p^{r+1}])/F\big) \cong GL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. We denote the fixed field for the center of this group by $K_r$. Thus, we can identify $\mathrm{Gal}(K_r/F)$ with the group $\Delta_r = PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ studied in section 7.2 and 7.3. Since $\rho_A$ is assumed to be surjective, the Weil pairing implies that $F(\mu_p) \subset F(A[p])$ and that $[F(\mu_p) : F] = p - 1$. Let $F^\sharp = F(\mu_p) \cap K_r$. That field doesn't depend on $r$. In fact, one sees easily that $[F^\sharp : F] = 2$ and that $F^\sharp = F(\sqrt{d})$, where $d = p$ if $p \equiv 1 \pmod 4$ and $d = -p$ if $p \equiv 3 \pmod 4$. For any $r \geq 0$, $F^\sharp$ is the maximal abelian extension of $F$ contained in $K_r$. Since $p$ is odd, we have $K_r \cap F_\infty = F$.

We will also consider the intermediate field $J_r = K_r^{B_r}$, which is a non-Galois extension of $F$ of degree $p^r(p+1)$. Now $B_r$ has a unique subgroup of index 2. The fixed field for that subgroup is the quadratic extension $J_r^\sharp = J_r F^\sharp$ of $J_r$. The fields $J_r$ form an increasing tower and $[J_r : J_{r\text{-}1}] = p$ for all $r \geq 1$. A similar statement is true for the fields $J_r^\sharp$.

Let $j_A$ denote the $j$-invariant of $A$. The simplest situation to consider is when $j_A$ is an algebraic integer and $p \geq 5$. Then, if $v$ is a prime of $F$ and $v \notin \Sigma_p \cup \Sigma_\infty$, the ramification index for $v$ in $K_r/F$ divides 24, and hence is prime to $p$. Thus, $\Phi_{K_r/F}$ is empty and we will take $\Sigma_0$ to be empty in applying proposition 3.2.1. We will assume that $E$ is an elliptic curve defined over $F$ with good, ordinary reduction at the primes of $F$ lying over $p$.

For each $r \geq 0$, let $K_{r,\infty}$, $J_{r,\infty}$, and $J^\sharp_{r,\infty}$ denote the cyclotomic $\mathbf{Z}_p$-extensions of $K_r$, $J_r$, and $J_r^\sharp$, respectively. We will assume that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. By proposition 4.2.5, it then follows that the Selmer atoms $\mathrm{Sel}_{E[p]\otimes\tau}(F_\infty)$ are finite for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta_0)$. That same proposition then implies that $\mathrm{Sel}_E(K_{r,\infty})[p]$ is finite for any $r \geq 0$. One could also see this by using one of the results from [HaMa] since $K_r/K_0$ is a $p$-extension. Consequently, the Pontryagin dual $X_E(K_{r,\infty})$ is quasi-projective as a $\mathbf{Z}_p[\Delta_r]$-module. Proposition 7.3.1 then implies the following result.

**Proposition 8.1.1.** *Assume that $j_A$ is an algebraic integer, that $E$ has good ordinary reduction at the primes of $F$ lying above $p$, and that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. Let*

$$k \;=\; \lambda_E(\sigma_0) \;+\; \lambda_E(\sigma_{\mathbf{1}}) \;+\; \lambda_E(\sigma_{\boldsymbol{p},1}) \;+\; \lambda_E(\sigma_{\boldsymbol{p},2}) \;+\; 2\sum_{j=1}^{\frac{p-3}{2}} \lambda_E(\sigma_{\boldsymbol{p}+\mathbf{1},j}) \quad .$$

*Then $\lambda_E(K_{r,\infty}) = p^{3r+1}k$ for $r \geq 0$. For the other fields defined above, we have*

$$\lambda_E(J_{r,\infty}) \;=\; d_r k \;+\; \lambda_E(\sigma_0) \;+\; \lambda_E(\sigma_{\boldsymbol{p},2}) \quad ,$$

$$\lambda_E(J^\sharp_{r,\infty}) \;=\; 2d_r k \;+\; \lambda_E(\sigma_0) \;+\; \lambda_E(\sigma_{\mathbf{1}}) \;+\; \lambda_E(\sigma_{\boldsymbol{p},1}) \;+\; \lambda_E(\sigma_{\boldsymbol{p},2})$$

*for all $r \geq 0$, where $d_r = \frac{p^r\text{-}1}{p-1}$. If $\sigma \in \mathcal{A}_r$, then $\sigma = \mathrm{Ind}_{B_r}^{\Delta_r}(\psi)$, where $\psi$ is a primitive character of $B_r/U_r$. We can choose $\psi$ so that $\widetilde{\psi} = \widetilde{\beta}^j$, where $0 \leq j \leq \frac{p\text{-}1}{2}$. Then*

$$\lambda_E(\sigma) \;=\; d_r k \;+\; \lambda_E(\sigma_{\boldsymbol{p}+\mathbf{1},j}) \quad .$$

*for all $r \geq 0$. For $\sigma \in \mathcal{C}_r$, where $r \geq 1$, we have $\lambda_E(\sigma) \;=\; p^{r\text{-}1}k$.*

*Proof.* To simplify notation, we define $\lambda_E(\phi)$ for all $\mathcal{F}$-representations $\phi$ of $\Delta_r$ by letting it be additive for direct sums. Under the stated assumptions, $X_E(K_{0,\infty})$ is a quasi-projective $\mathbf{Z}_p[\Delta_0]$-module, and hence $V_0 = X_E(K_{0,\infty}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is free as a $\mathbf{Q}_p[\Pi_0]$-module, where $\Pi_0$ is the Sylow $p$-subgroup of $B_0$. This explains why $\lambda_E(K_{0,\infty})$ is divisible by $p$. That divisibility and the value of $k$ follow from the second isomorphism in (7.2.b), which gives $\lambda_E(K_{0,\infty}) = \lambda_E(\rho) = p\lambda_E(\kappa)$. Thus, we should take $k = \lambda_E(\kappa)$. This is indeed the value stated above. The relationship between $\lambda_E(K_{r,\infty})$ and $k$ follows from the Riemann-Hurwitz formula proved in [HaMa]. It also follows from chapter 6 of this paper, by using the facts that $[K_r : K] = p^{3r}$ and that $\Sigma_0$ is empty. If $\sigma \in \mathcal{A}_r$, or if $r \geq 1$ and $\sigma \in \mathcal{C}_r$, then the stated relationships between $\lambda_E(\sigma)$ and $k$ follow immediately from proposition 7.3.1.

To prove the results concerning $J_{r,\infty}$, note that the restriction map

$$\mathrm{Sel}_E(J_{r,\infty})_p \;\longrightarrow \mathrm{Sel}_E(K_{r,\infty})_p^{B_r}$$

has finite kernel and cokernel. Therefore, the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(J_{r,\infty})_p$ is equal to the multiplicity of $\mathbf{1}_{B_r}$ in the representation space $V_r = X_E(K_{r,\infty}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $B_r$. We can regard $V_r$ as a representation space for $\Delta_r$. If $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$, then the multiplicity of $\sigma$ in $V_r$ is $\lambda_E(\sigma)$. It follows that

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(J_{r,\infty})_p\big) \;=\; \sum_{\sigma} \langle \sigma|_{B_r}, \mathbf{1}_{B_r} \rangle \quad .$$

Now $\langle \sigma|_{B_r}, \mathbf{1}_{B_r} \rangle = \langle \sigma, \mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r}) \rangle$, which is equal to 1 if $\sigma = \sigma_{st}^{(j)}$ for $1 \leq j \leq r$ and if $\sigma \in \{\sigma_0, \sigma_{\boldsymbol{p},2}\}$, but this multiplicity is equal to 0 for all other $\sigma$'s. In particular, we have $\lambda_E(J_{0,\infty}) = \lambda_E(\sigma_0) + \lambda_E(\sigma_{p,2})$ and

$$\lambda_E(J_{r,\infty}) \;=\; \lambda_E(\sigma_0) \;+\; \lambda_E(\sigma_{\boldsymbol{p},2}) \;+\; \sum_{j=1}^{r} \lambda_E(\sigma_{st}^{(j)}) \;,$$

from which the stated result follows easily. One uses the fact that $\sigma_{st}^{(j)} \in \mathcal{C}_j$ for $j \geq 1$ together with the formula already proven for those $\sigma$'s.

If $B_r^\sharp$ is the unique subgroup of $B_r$ of index 2, then

$$\mathrm{Ind}_{B_r^\sharp}^{\Delta_r}(\mathbf{1}_{B_r^\sharp}) \;\cong\; \mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r}) \;\oplus\; \big(\mathrm{Ind}_{B_r}^{\Delta_r}(\mathbf{1}_{B_r}) \otimes \sigma_{\mathbf{1}}\big) \quad .$$

The formula for $\lambda_E(J_{r,\infty}^\sharp)$ can then be derived exactly as above. One uses the facts that $\sigma_{\boldsymbol{p},2} \otimes \sigma_{\mathbf{1}} \cong \sigma_{\boldsymbol{p},1}$ and that $\sigma_{st}^{(j)} \otimes \sigma_{\mathbf{1}} \cong \sigma_{st}^{(j)}$ for all $j \geq 1$. $\square$

**Remark 8.1.2.** In principle, under the assumptions in the above proposition, one can determine the invariants $\lambda_E(\sigma)$ for all $r$ and all irreducible representations $\sigma$ of $\Delta_r$ just from the $\lambda_E(\sigma)$'s for the irreducible representations $\sigma$ of $\Delta_0$. One can then determine the invariants $\lambda_E(M_\infty)$ for any extension $M$ of $F$ contained in any of the $K_r$'s. The above proposition partially illustrates this principle. However, we also see that knowing $\lambda_E(M_\infty)$ for certain subfields $M$ of $K_0$ suffices to determine some of the $\lambda_E(\sigma)$'s. A theorem of Artin states that every rational-valued character of a finite group $\Delta$ can be expressed as a $\mathbf{Q}$-linear combination of characters for representations of the form $\mathrm{Ind}_H^\Delta(\mathbf{1}_H)$, where $H$ varies over all subgroups (or even just cyclic subgroups) of $\Delta$. (See theorem 17, chapter 9.2 in [Se77].) Thus, one can determine $\lambda_E(\rho)$ for all $\rho$'s with rational-valued character from the $\lambda_E(M_\infty)$'s. In fact, it suffices to consider subfields $M$ of $K_0$. In particular, the useful quantities

$$\lambda_E(\sigma_{\boldsymbol{p}+\mathbf{1},0}) \;=\; \lambda_E(\sigma_0) + \lambda_E(\sigma_{\boldsymbol{p},2}), \qquad \lambda_E(\sigma_{\boldsymbol{p}+\mathbf{1},\frac{p-1}{2}}) \;=\; \lambda_E(\sigma_{\mathbf{1}}) + \lambda_E(\sigma_{\boldsymbol{p},1})$$

associated to the induced representations $\mathrm{Ind}_{B_0}^{\Delta_0}(\beta_0)$ and $\mathrm{Ind}_{B_0}^{\Delta_0}(\beta_{\mathbf{1}})$ are determined by $\lambda_E(J_{0,\infty})$ and $\lambda_E(J_{0,\infty}^\sharp)$ under the assumptions of proposition 8.1.1. This is clear since $d_r = 0$ for $r = 0$. Of course, $\lambda_E(\sigma_0) = \lambda_E(F_\infty)$ and $\lambda_E(\sigma_{\mathbf{1}}) = \lambda_E(F_\infty^\sharp) - \lambda_E(F_\infty)$. Thus, the four quantities $\lambda_E(\sigma_0)$, $\lambda_E(\sigma_{\mathbf{1}})$, $\lambda_E(\sigma_{\boldsymbol{p},1})$, and $\lambda_E(\sigma_{\boldsymbol{p},2})$ are determined by the four quantities $\lambda_E(F_\infty)$, $\lambda_E(F_\infty^\sharp)$, $\lambda_E(J_{0,\infty})$, and $\lambda_E(J_{0,\infty}^\sharp)$, again under the assumptions of the above proposition. Furthermore, $k$ is obviously determined by $\lambda_E(K_{0,\infty})$. $\Diamond$

**Remark 8.1.3.** We make the assumptions in proposition 8.1.1. If $k \geq 1$, then $\lambda_E(\sigma)$ will be positive for many $\sigma$'s, including all $\sigma \in \mathcal{A}_r$ and the Steinberg representations $\sigma_{st}^{(r)}$ for $r \geq 1$. In fact, all those $\lambda$-invariants would then be unbounded as $r \to \infty$. By definition, $k \geq 1$ if and only if $\lambda_E(\sigma) \geq 1$ for at least one $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ with $n(\sigma) \neq p-1$. A sufficient condition for $k \geq 1$ is that $\lambda_E(\sigma) \geq 1$ for at least one $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ with $n(\sigma) = p-1$. That follows from proposition 7.2.1.

Suppose that we are in a situation where $X_E(K_{0,\infty})$ is known to be projective, or at least strictly quasi-projective. Then the $\Delta_0$-representation space $V_0 = X_E(K_{0,\infty}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is isomorphic to a direct sum of representations of the form $P_\tau \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta_0)$. If $n(\tau) \neq p$, then $P_\tau \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a direct sum of two irreducible representations $\sigma$ and $\sigma'$ such that one of them has dimension $p-1$, and the other has dimension 1 or $p+1$. We referred to such a pair $\sigma, \sigma'$ of irreducible representations of $\Delta_0$ as a *"linked pair"* in remark 7.2.8. Remark 7.2.7 leads to the following conclusion under the above assumption about $X_E(K_{0,\infty})$.

*If $\lambda_E(\sigma) \geq 1$ for some $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ of dimension $p+1$, then there are two non-isomorphic representations $\sigma' \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ of dimension $p-1$ linked to $\sigma$, and $\lambda_E(\sigma') \geq 1$ for at least one*

*of them. If $\lambda_E(\sigma) \geq 1$ for some $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ of dimension $p-1$, then there are two non-isomorphic representations $\sigma' \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ of dimension 1 or $p+1$ linked to $\sigma$, and $\lambda_E(\sigma') \geq 1$ for at least one of them.*

One gets a more precise result if $\lambda_E(\sigma) \geq 1$ for either one of the two $\sigma$'s of dimension 1. Such a $\sigma$ is linked to just one irreducible representation $\sigma'$, namely $\sigma' = \sigma_{\boldsymbol{p\text{-}1},1}$ if $\sigma = \sigma_0$ or $\sigma' = \sigma_{\boldsymbol{p\text{-}1},\frac{p-1}{2}}$ if $\sigma = \sigma_{\mathbf{1}}$. This follows from proposition 7.2.4. We therefore obtain the inequalities

$$\lambda_E(\sigma_{\boldsymbol{p\text{-}1},1}) \ \geq \ \lambda_E(\sigma_0), \qquad \lambda_E\big(\sigma_{\boldsymbol{p\text{-}1},\frac{p-1}{2}}\big) \ \geq \ \lambda_E(\sigma_{\mathbf{1}})$$

under the assumptions in proposition 8.1.1. Not much more can be said. For example, if it turned out that $V_0 \cong P_{\tau_0} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, then one would simply have $\lambda_E(\sigma_0) = \lambda_E(\sigma_{\boldsymbol{p\text{-}1},1}) = 1$, $\lambda_E(\sigma) = 0$ for all the other $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$, and $k = 1$. As another illustration, suppose that $V_0 \cong (P_{\tau_0} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p) \oplus (P_{\tau_{\boldsymbol{p\text{-}2},2}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$. Proposition 7.2.4 and the fact that $ch(\tau_{\boldsymbol{p\text{-}2},2}) = \widetilde{\beta}^1$ imply that $\lambda_E(\sigma_0) = 1$, $\lambda_E(\sigma_{\boldsymbol{p\text{-}1},1}) = 2$, $\lambda_E(\sigma_{\boldsymbol{p+1},1}) = 1$, and $\lambda_E(\sigma) = 0$ for all the other $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. Also, $k = 3$ in that example. $\Diamond$

The $\mathbf{Q}_p$-representation spaces $V_r$ for $\Delta_r$ occurring in the above proof are also determined up to isomorphism by the $\lambda_E(\sigma)$'s for $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. However, we can make the following considerably more precise statement under some mild additional assumptions about $A, E$ and $p$. We use the notation from proposition 7.3.6 for the indecomposable, projective $\mathbf{Z}_p[\Delta_r]$-modules.

**Proposition 8.1.4.** *In addition to the assumptions in proposition 8.1.1 about $A$, $E$, and $p$, assume that (i) $A$ does not have supersingular or potentially supersingular reduction at $p$, (ii) $E(F^\sharp)[p] = 0$, (iii) $p$ is non-anomalous for $E/F$, and (iv) $F(\mu_p)/F$ is totally ramified at all $v \in \Sigma_p$. For each $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta_0)$, let $w_0(\tau)$ denote $w(X_E(K_{0,\infty}), \tau)$. Then, for all $r \geq 0$,*

$$X_E(K_{r,\infty}) \ \cong \ \bigoplus_{\tau} \ \big(P_\tau^{(r)}\big)^{w_0(\tau)} \ .$$

*as $\mathbf{Z}_p[\Delta_r]$-modules. Thus, the isomorphism class of the $\mathbf{Z}_p[\Delta_r]$-module $X_E(K_{r,\infty})$ is determined for all $r$ by the weights $w_0(\tau)$ for $\tau \in \mathrm{Irr}_{\mathbf{F}_p}(\Delta_0)$.*

*Proof.* The first point is that if $v \in \Sigma_p$, then assumption *(i)* implies that the residue field for any prime of $K_0$ lying above $v$ coincides with the residue field for $v$ itself. That is, the corresponding decomposition and inertia subgroups of $\Delta_0$ coincide. To see this, note that the decomposition subgroup of $\mathrm{Gal}(F(E[p])/F)$ can be identified with a subgroup of the group of triangular matrices $\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ and the inertia subgroup of $\mathrm{Gal}(F(E[p])/F)$ can

be identified with a subgroup of $\left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\}$. Furthermore, the inertia subgroup has order divisible by $p-1$ because of assumption *(iv)*. This is sufficient to imply that the images of those two subgroups in $\Delta_0$ indeed coincide. It follows from assumption *(iii)* that $p$ is non-anomalous for $E/K_0$, and therefore, by proposition 4.1.9, also for $E/K_r$ for all $r \geq 1$.

Secondly, note that $E(K_0)[p]$ is a representation space for $\Delta_0$ over $\mathbf{F}_p$. Since $K_0$ is a proper subfield of $F(E[p])$, the $\mathbf{F}_p$-dimension of $E(K_0)[p]$ is at most 1. Hence if $E(K_0)[p] \neq 0$, then the action of $\Delta_0$ on $E(K_0)[p]$ is by a 1-dimensional character. Now $\Delta_0$ has two 1-dimensional characters, the two characters which factor through $\mathrm{Gal}(F^\sharp/F)$. Hence $E(K_0)[p] = E(F^\sharp)[p]$, and this is trivial by assumption *(ii)*. It then follows that $E(K_r)[p] = 0$ for all $r \geq 0$, using either proposition 4.1.3 or the fact that $\mathrm{Gal}(K_r/K_0)$ is a $p$-group.

The hypotheses in Proposition 3.1.1 (or theorem 1) are satisfied. Hence $X_E(K_{r,\infty})$ is a projective $\mathbf{Z}_p[\Delta_r]$-module for all $r \geq 0$. Therefore, $X_E(K_{r,\infty})$ is a direct sum of the $P_\tau^{(r)}$'s and we must just show that the corresponding multiplicities are independent of $r$. This will follow from proposition 7.3.6 if we show that

$$X_E(K_{r_1,\infty})/I_{(r_1/r_2)}X_E(K_{r_1,\infty}) \;\cong X_E(K_{r_2,\infty})$$

for $r_1 \geq r_2 \geq 0$. This statement amounts to proving that the restriction map

$$\mathrm{Sel}_E(K_{r_2,\infty})_p \;\longrightarrow\; \mathrm{Sel}_E(K_{r_1,\infty})_p^{N_{(r_1/r_2)}}$$

is an isomorphism. However, the argument for this is quite standard. The kernel and cokernel of the inflation-restriction map

$$H^1(K_{r_2,\infty}, E[p^\infty]) \;\longrightarrow\; H^1(K_{r_1,\infty}, E[p^\infty])^{N_{(r_1/r_2)}}$$

are both trivial because $H^0(K_{r,\infty}, E[p^\infty]) = 0$ for all $r$. It remains to show that the local restriction maps are injective. For primes above $p$, this is so because $p$ is non-anomalous for $E/K_r$. For all other primes $v \in \Sigma$, the injectivity holds because the local degree for the extension $K_{r_1,\infty}/K_{r_2,\infty}$ is prime to $p$. □

**Remark 8.1.5.** In terms of the notation in the above proposition, one sees easily that

$$k \;=\; \sum_\tau w_0(\tau) k_\tau$$

where $k_\tau = 1$ if $n(\tau) = 1$ or $p$, $k_\tau = 2$ for all other $\tau$'s in $\mathrm{Irr}_{\mathbf{F}_p}(\Delta_0)$. ◊

**Remark 8.1.6.** Instead of considering the fields obtained from $p$-power division points on an elliptic curve $A$, one gets other interesting examples from modular forms. As an example,

consider the normalized cusp form $f_{12}$ of weight 12 for $SL_2(\mathbf{Z})$. Then, for every prime $p$, there is an associated representation $\rho_p$ of $G_{\mathbf{Q}}$ with values in $GL_2(\mathbf{Z}_p)$. If $p \notin \{2,3,5,7,23,691\}$, then the image of $\rho_p$ coincides with the set of matrices whose determinant is in $(\mathbf{Z}_p^{\times})^{11}$. It follows that the corresponding projective representation is surjective. That is, except for the six listed primes, the field cut out by the representation $\rho_p$ contains a tower of subfields $K_r$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. The only prime ramified in $K_r/\mathbf{Q}$ is $p$. Thus, propositions 8.1.1 and 8.1.4 and the associated remarks apply exactly as stated. $\Diamond$

## 8.2 An illustration where $\Sigma_0$ is non-empty.

We continue discussing the situation in the previous illustration, but now we assume that $j_A$ is not an algebraic integer. We still assume that $p \geq 5$ and that $\rho_A$ is surjective. Let

$$\Sigma_0 \;=\; \{v \;\big|\; v \nmid p, \infty \;\; \textit{and} \;\; \mathrm{ord}_v(j_A) < 0 \;\} \quad .$$

Thus, $A$ has multiplicative or potentially multiplicative reduction at all $v \in \Sigma_0$. The field $K_r$ is unchanged if one replaces $A$ by a quadratic twist over $F$. Thus, the field $K_r$ actually depends only on $j_A$. By replacing $A$ by a suitable quadratic twist, we can therefore simply assume that $A$ has split multiplicative reduction at all $v \in \Sigma_0$. One then sees that the $v$-adic completion of $K_{r,\infty}$ is $F_v(\mu_{p^\infty}, q_v^{p^{-(r+1)}})$. Here $q_v$ is the Tate period for $A$ over $F_v$. One has $ord_p(j_A) = -ord_p(q_v)$. Also, $F_v(\mu_{p^\infty}) = F_{\infty,v}(\mu_p)$, an unramified, cyclic extension of $F_{\infty,v}$. Let $w_v = [F_{\infty,v}(\mu_p) : F_{\infty,v}]$, a divisor of $p-1$. As in chapter 5, we let $\mathcal{G}_v = G_{F_{\infty,v}}$. Then $\mathcal{M}_v = G_{F_{\infty,v}(\mu_p)}$ is a normal subgroup of $\mathcal{G}_v$ of index $w_v$. The character $\omega_v$ is a faithful representation of $\mathcal{G}_v/\mathcal{M}_v$ and has order $w_v$.

Note that $\Phi_{K_r/F} \subseteq \Sigma_0$ for all $r \geq 0$ and that equality holds if $r$ is sufficiently large. We make the simplifying assumption that $\mathrm{ord}_v(j_A) \not\equiv 0 \pmod{p}$ for all $v \in \Sigma_0$. This implies that $\Phi_{K_r/F} = \Sigma_0$ for all $r \geq 0$. Let $\Delta_{r,v}$ denote the decomposition subgroup of $\Delta_r$ for a prime of $K_{r,\infty}$ lying above $v$, which is determined up to conjugacy in $\Delta_r$. Identifying $\Delta_r$ with $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$, and choosing a prime above $v$ suitably, we can identify $\Delta_{r,v}$ with the unique subgroup of $B_r$ containing $U_r$ such that $[\Delta_{r,v} : U_r] = w_v$. Recall that $U_r \cong \mathbf{Z}/p^{r+1}\mathbf{Z}$. Thus, the inertia subgroup of $\Delta_{r,v}$ is identified with $U_r$. The corresponding quotient group is $\mathrm{Gal}(F_{\infty,v}(\mu_p)/F_{\infty,v})$ and $\omega_v$ can be regarded as a character of $\Delta_{r,v}$ whose kernel is $U_r$.

As in section 8.1, we want to study the behavior of the $\lambda_E(\sigma)$'s. We always assume that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. The $\lambda_E^{\Sigma_0}(\sigma)$'s then behave just as described in proposition 8.1.1 since $X_E^{\Sigma_0}(K_{r,\infty})$ will be quasi-projective as a $\mathbf{Z}_p[\Delta_r]$-module. The corresponding value of $k$ is now

$$k \;=\; \lambda_E^{\Sigma_0}(\kappa) \;=\; \lambda_E(\kappa) + \sum_{v \in \Sigma_0} g_v \delta_{E,v}(\kappa) \tag{8.2.a}$$

where we define $\lambda_E^{\Sigma_0}(\phi), \lambda_E(\phi)$, and $\delta_{E,v}(\phi)$ for an arbitrary $\mathcal{F}$-representation $\phi$ of $\Delta_r$ by making it additive for direct sums. Alternatively, we have

$$k \;=\; \frac{1}{p}\lambda_E^{\Sigma_0}(K_{0.\infty}) \;=\; \frac{1}{p}\Big(\lambda_E(K_{0,\infty}) \;+\; \sum_{v\in\Sigma_0} \dim_{\mathbf{Q}_p}\big(\mathcal{H}_v(K_{0,\infty},E)\big)\Big)$$

Proposition 5.1.1 can be used to determine the $\mathbf{Q}_p$-dimension of $\mathcal{H}_v(K_{0,\infty},E)$.

Since we assume that $p \geq 5$, the representations $\chi$ of $\mathcal{G}_v$ for which $\langle \rho_{E,v}, \chi\rangle \geq 1$ factor through a quotient group of $\mathcal{G}_v$ of order prime to $p$. Such a $\chi$ factors through $\Delta_{r,v}$ if and only if $\chi = \omega_v^j$ for some integer $j$. This means that $\chi$ must be 1-dimensional, unramified, and of order dividing $w_v$. In the notation of section 5.2, this rules out the possibilities where $\chi = \varphi_v$ is 2-dimensional or where $\chi = \varphi_v$ is 1-dimensional, but ramified. Thus, if $E$ has additive reduction at $v$, then $\mathcal{H}_v(K_{r,\infty},E) = 0$. If $E$ has non-split multiplicative reduction at $v$, then $\varphi_v = \omega_v\varepsilon_v$, where $\varepsilon_v$ is unramified and has order 2. Hence $\varphi_v$ factors through $\Delta_{r,v}$ if and only if $w_v$ is even. If $E$ has split multiplicative reduction at $v$, then $\varphi_v = \omega_v$ which does factor through $\Delta_{r,v}$.

Finally, we discuss the case where $E$ has good reduction at $v$. There are then two characters $\varphi_v$ and $\psi_v$ to consider, both unramified. We have $\varphi_v\psi_v = \omega_v$ and so if one of the characters factors through $\Delta_{r,v}$, then so does the other. As discussed in section 5.2, those characters are determined by the two roots of the polynomial $c_v(x) = x^2 - a_v x + b_v$, where $b_v = N(v)$, the cardinality of the residue field for $v$, and where $1 - a_v + b_v$ is the cardinality of the set of points on $\overline{E}_v$ over the residue field for $v$. It suffices to know the roots of $\widetilde{c}_v(x) \in \mathbf{F}_p[x]$, the reduction of $c_v(x)$ modulo $p$. The two roots are in $\mathbf{F}_{p^2}^\times$ in general. Now $w_v$, the order of $\omega_v$, is just the order of $\widetilde{b}_v$ in $\mathbf{F}_p^\times$. These remarks show that $\varphi_v$ factors through $\Delta_{r,v}$ if and only if some power of $\widetilde{b}_v$ is a root of $\widetilde{c}_v(x)$. Then the other root will also be a power of $\widetilde{b}_v$. This is a stringent requirement. If $p = 5$, only 6 of the 20 polynomials of the form $x^2 - \widetilde{a}x + \widetilde{b}$ in $\mathbf{F}_p[x]$, with $\widetilde{b} \neq 0$, have powers of $\widetilde{b}$ as its roots. For $p = 7$, the property is satisfied by 12 out of the 42 polynomials of that form.

In summary, we have proved the following result, where we implicitly make the assumptions described above. However, the assumption that $ord_v(j_A) \not\equiv 0 \pmod{p}$ is not needed. Note also that the conditions for the nonvanishing of $\mathcal{H}_v(K_{r,\infty},E)$ don't involve $r$. This is so because we are assuming that $p \geq 5$, and therefore a character $\chi$ for which $\langle \rho_{E,v}, \chi\rangle \geq 1$ has order prime to $p$. If $\chi$ factors through $\Delta_{r,v}$, then $\chi$ also factors through $\Delta_{0,v}$.

**Proposition 8.2.1.** *Assume that $p \geq 5$. Suppose that $v \in \Sigma_o$. Then $\mathcal{H}_v(K_{r,\infty},E) \neq 0$ if and only if one of the following statements is true:*

*(i) E has split multiplicative reduction at v,*

*(ii) $E$ has non-split multiplicative reduction at $v$ and $w_v$ is even,*

*(iii) $E$ has good reduction at $v$ and the roots of $\widetilde{c}_v(x) = x^2 - \widetilde{a_v}x + \widetilde{b_v}$ are powers of $\widetilde{b_v}$.*

*In case (i), $\langle \rho_{E,v}, \chi \rangle = 1$ for $\chi = \omega_v$. In case (ii), $\langle \rho_{E,v}, \chi \rangle = 1$ for $\chi = \omega_v \varepsilon_v$, where $\varepsilon_v$ is the unramified character of order 2. In case (iii), one either has $\langle \rho_{E,v}, \chi \rangle = 1$ for exactly two $\chi$'s, namely $\chi = \varphi_v$ and $\chi = \psi_v$ if $\varphi_v \neq \psi_v$, or $\langle \rho_{E,v}, \chi \rangle = 2$ for exactly one $\chi$, namely $\chi = \varphi_v$ if $\varphi_v = \psi_v$. We have $\langle \rho_{E,v}, \chi \rangle = 0$ for all other $\chi$'s.*

If it turns out that $\mathcal{H}_v(K_{r,\infty}, E) = 0$ for all $v \in \Sigma_0$ and if $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, then $X_E(K_{r,\infty})$ is quasi-projective as a $\mathbf{Z}_p[\Delta_r]$-module for all $r \geq 0$. Consequently, all of the congruence relations for the $\lambda_E(\sigma)$'s stated in proposition 8.1.1 would then hold. On the other hand, if *(i), (ii),* or *(iii)* is satisfied, then proposition 3.3.1 implies that $X_E(K_{r,\infty})$ is not quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. In particular, $X_E(K_{r,\infty}) \neq 0$. Assuming that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, it would then follow that $\lambda_E(\sigma) \geq 1$ for at least one $\sigma$. We will make some more precise statements below.

In formula (5.2.a) for $\delta_E^{\Sigma_0}(\sigma)$, the contribution for each $v \in \Sigma_0$ involves terms of the form $g_v \langle \sigma_v, \chi \rangle \langle \rho_{E,v}, \chi \rangle$. Thus, we need only consider cases *(i), (ii), (iii)* and we may assume that $\chi$ is such that $\langle \rho_{E,v}, \chi \rangle \geq 1$. In cases *(i)* and *(ii)*, there is one such $\chi$. In case *(iii)*, there will be one or two such $\chi$'s. The factor $g_v$ is an elementary invariant and depends only on $v$ and $F$. It remains to discuss $\langle \sigma_v, \chi \rangle$ for $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_{r,v})$, which will be positive for some $\sigma$'s. The assumption that $ord_v(j_A) \not\equiv 0 \pmod{p}$ for all $v \in \Sigma_0$ will now be useful for simplifying the discussion. The problem is purely group theoretic. The value of $w_v$ plays an important role. Note that the $\chi$'s now being considered are 1-dimensional and their kernel contains $U_r$.

For $r = 0$, the discussion in section 7.2 gives complete information. The decomposition of $\sigma|_{B_0}$ is given there for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. One can then deduce the value of $\langle \sigma_v, \chi \rangle$. For that purpose, it is useful to note that $\gamma|_{U_0}$ is isomorphic to the direct sum of the nontrivial characters of $U_0$. Here $\gamma$ denotes the irreducible $(p-1)$-dimensional representation of $B_0$. It follows that $\chi$ is not a constituent in $\gamma|_{\Delta_{0,v}}$. One can then see that the value of $\langle \sigma_v, \chi \rangle$ is 0, 1, or 2. The possibilities for $\langle \sigma_v, \chi \rangle$ depend on $n(\sigma)$ in the following way:

If $n(\sigma) = p - 1$, then $\langle \sigma_v, \chi \rangle = 0$. Thus, $\delta_{E,v}(\sigma) = 0$.

If $n(\sigma) = 1$ or $p$, then $\langle \sigma_v, \chi \rangle = 0$ unless $\chi = \chi^{-1}$. In cases *(i)* or *(ii)*, $\chi = \chi^{-1}$ if and only if $w_v \leq 2$. In case *(iii)*, there may be one or two $\chi$'s, and the condition for $\chi = \chi^{-1}$ for one or both is a simple congruence condition on $a_v$ and $b_v$ modulo $p$. We have the following results in these cases. If $\chi = \chi_0$, then $\langle \sigma_v, \chi \rangle = 1$ for either two or all four of those $\sigma$'s, depending on whether $(p\text{-}1)/w_v$ is odd or even, respectively. If $\chi$ has order 2, then $\langle \sigma_v, \chi \rangle = 1$ for either none or two of those $\sigma$'s, depending on whether $(p\text{-}1)/w_v$ is even or odd, respectively. Otherwise, $\langle \sigma_v, \chi \rangle = 0$.

Finally, if $n(\sigma) = p+1$, then $\sigma|_{B_0}$ has two 1-dimensional constituents $\psi$ and $\psi^{-1}$, where $\psi \neq \psi^{-1}$. One can view those constituents as characters of the cyclic group $B_0/U_0$. The value of $\langle \sigma_v, \chi \rangle$ is determined by the restrictions of $\psi$ and $\psi^{-1}$ to the subgroup $\Delta_{0,v}/U_0$ of order $w_v$. Either one of those restrictions might or might not turn out to be $\chi$. Thus, the value of $\langle \sigma_v, \chi \rangle$ is 0, 1,or 2 when $n(\sigma) = p+1$.

In all cases, for $r = 0$, the possible values of $\delta_{E,v}(\sigma)$ are $0, 1, 2$, or 4. Furthermore, if $\mathcal{H}_v(K_{0,\infty}) \neq 0$, then $\delta_{E,v}(\sigma) \geq 1$ for at least one $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. For such a $\sigma$, we have $n(\sigma) \neq p-1$. However, in all cases, there exists such a $\sigma$ with $n(\sigma) = 1$ or $p+1$.

If $r \geq 1$ and $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$, then $\langle \sigma_v, \chi \rangle$ can be determined if one knows the characters of $B_r/U_r$ which occur in $\sigma|_{B_r}$, and their multiplicities. The number of such characters, counting multiplicity, is $\langle \sigma|_{U_r}, \mathbf{1}_{U_r} \rangle$. For example, if $\sigma \in \mathcal{A}_r$, then there are just two such characters, $\psi$ and $\psi^{-1}$, where $\psi$ is a primitive character of $B_r/U_r$. The value of $\langle \sigma_v, \chi \rangle$ just depends on the restrictions of $\psi$ and $\psi^{-1}$ to the unique subgroup of $B_r/U_r$ of order $w_v$. That restriction is determined by $\widetilde{\psi}$. Thus, $\langle \sigma_v, \chi \rangle$ is 0, 1, or 2 if $\sigma \in \mathcal{A}_r$.

Note that $\langle \sigma|_{U_r}, \mathbf{1}_{U_r} \rangle$ is closely related to the Artin conductor of $\sigma$, which we denote by $\mathfrak{c}_\sigma$. It is clear that $\sigma$ is tamely ramified at $v$ (since $v \nmid p$) and so, if we let $I_v$ denote the inertia subgroup of $G_{F_v}$, then the image of $I_v$ in $\Delta_r$ is conjugate to $U_r$ (under our assumption that $ord_v(j_A)$ is not divisible by $p$) and we therefore have

$$ord_v\big(\mathfrak{c}_\sigma\big) \;=\; \dim_{\mathcal{F}}\big(W_\sigma\big) \;-\; \dim_{\mathcal{F}}\big(W_\sigma^{I_v}\big) \;=\; n(\sigma) \;-\; \langle \sigma|_{U_r}, \mathbf{1}_{U_r} \rangle \;\; .$$

In particular, if $ord_v\big(\mathfrak{c}_\sigma\big) = n(\sigma)$, then $\delta_{E,v}(\sigma) = 0$. For example, this remark applies to any $\sigma \in \mathcal{B}_r$ since we then have $\sigma|_{B_r} \cong \gamma_r$. In contrast, if $\sigma \in \mathcal{A}_r$, then $ord_v\big(\mathfrak{c}_\sigma\big) = n(\sigma) - 2$ and $\delta_{E,v}(\sigma)$ can be positive. For $\sigma \in \mathcal{C}_r$, the value of $ord_v\big(\mathfrak{c}_\sigma\big)$ depends on $\sigma$.

In particular, if $\sigma = \sigma_{st}^{(r)}$ and $r \geq 1$, then it turns out that $\langle \sigma|_{U_r}, \mathbf{1}_{U_r} \rangle = (p-1)p^{[(r\text{-}1)/2]}$. More precisely, every character of $B_r/U_r$ which factors through the unique quotient of order $(p-1)p^{[(r\text{-}1)/2]}$ occurs in $\sigma|_{B_r}$ with multiplicity 1; no others characters occur. (See [Sil], the last part of theorem 3.3, page 59. I thank Ryota Matsuura for this reference.) Thus, every character $\chi$ of $\Delta_{r,v}/U_r$ occurs in $\sigma_v$. To be precise, we have

$$\langle \sigma_v, \chi \rangle \;=\; \frac{p-1}{w_v} \cdot p^{[(r\text{-}1)/2]} \tag{8.2.b}$$

which is unbounded as $r \to \infty$. Thus, if *(i), (ii)*, or *(iii)* in proposition 8.2.1 is satisfied for at least one $v \in \Sigma_0$, then $\delta_E^{\Sigma_0}(\sigma_{st}^{(r)}) = ap^{[(r\text{-}1)/2]}$ for all $r \geq 1$, where $a$ is some positive constant. It follows that $\lambda_E^{\Sigma_0}(\sigma_{st}^{(r)})$ is nonzero and hence that $k \geq 1$. Therefore, $\lambda_E^{\Sigma_0}(\sigma_{st}^{(r)}) \geq p^{r\text{-}1}$. As a consequence, we see that $\lambda_E(\sigma_{st}^{(r)}) \to \infty$ as $r \to \infty$. Some other conclusions are given in the following result.

**Proposition 8.2.2.** *Assume that $j_A$ is not an algebraic integer, that $p \nmid ord_v(j_A)$ for all $v \in \Sigma_0$, that $E$ has good ordinary reduction at the primes of $F$ lying above $p$, and that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. Assume also that (i), (ii), or (iii) in proposition 8.2.1 is satisfied for at least one $v \in \Sigma_0$. Then $\lambda_E(\sigma) \geq 1$ for at least one $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ such that $n(\sigma) = p-1$. If $\lambda_E^{\Sigma_0}(\sigma_0) \geq 1$, then $\lambda_E(\sigma_{\boldsymbol{p\text{-}1},1}) \geq 1$. If $\lambda_E^{\Sigma_0}(\sigma_{\mathbf{1}}) \geq 1$, then $\lambda_E(\sigma_{\boldsymbol{p\text{-}1},\frac{p-1}{2}}) \geq 1$. Furthermore, the integer $k$ defined in (8.2.a) is positive and we have*

$$\lambda_E(\sigma) \;=\; d_r k + O(1)$$

*for all $r \geq 1$ and all $\sigma \in \mathcal{A}_r$. Also, $\lambda_E(\sigma_{st}^{(r)}) = p^{r-1}k + O(p^{r/2})$.*

*Proof.* The Pontryagin dual $X_E^{\Sigma_r}(K_{r,\infty})$ of $\mathrm{Sel}_E^{\Sigma_0}(K_{r,\infty})$ is a quasi-projective $\mathbf{Z}_p[\Delta_r]$-module for any $r \geq 0$. Let

$$V_r = X_E(K_{r,\infty}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \qquad V_r^{\Sigma_0} = X_E^{\Sigma_0}(K_{r,\infty}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \qquad U_r^{\Sigma_0} = \bigoplus_{v \in \Sigma_0} \widehat{\mathcal{H}_v}(K_{r,\infty}, E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \;\; .$$

We then have the following isomorphisms of $\mathbf{Q}_p$-representation spaces of $\Delta_r$.

$$V_r^{\Sigma_0} \;\cong\; V_r \;\oplus\; U_r^{\Sigma_0} \;\;\; .$$

First consider $r = 0$. The assumption that *(i), (ii)*, or *(iii)* holds for at least one $v \in \Sigma_0$ implies that $U_0^{\Sigma_0} \neq 0$. As remarked above, it follows that $U_0^{\Sigma_0}$ has at least one constituent $\sigma$ with $n(\sigma) = 1$ or $p$. Choose such a $\sigma$. That $\sigma$ is obviously a constituent in $V_0^{\Sigma_0}$. Now $V_0^{\Sigma_0}$ is a direct sum of representation spaces of the form $P_\tau \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $\tau \in \mathrm{Irr}_{\mathrm{f}}(\Delta_0)$. If $P_\tau \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ contains $\sigma$ as a constituent, then it also contains a constituent $\sigma'$ such that $n(\sigma') = p-1$. (See remark 7.2.7.) However, that $\sigma'$ is not a constituent in $U_0^{\Sigma_0}$ and hence must be a constituent in $V_0$. This means that $\lambda_E(\sigma') \geq 1$.

If $\lambda_E^{\Sigma_0}(\sigma_0) \geq 1$, then $P_{\tau_0} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a direct summand in $V_0^{\Sigma_0}$. Thus, the linked irreducible representation $\sigma_{\boldsymbol{p\text{-}1},1}$ must also be a constituent in $V_0^{\Sigma_0}$. (See (7.2.a.) Just as above, it follows that $\lambda_E(\sigma_{\boldsymbol{p\text{-}1},1}) \geq 1$. The same argument works if $\lambda_E^{\Sigma_0}(\sigma_{\mathbf{1}}) \geq 1$.

Now consider $r \geq 1$. We have already observed that $k \geq 1$ under the stated assumptions. Thus, we have $\lambda_E^{\Sigma_0}(\sigma) = d_r k + O(1)$ as $r \to \infty$ for any $\sigma \in \mathcal{A}_r$ according to proposition 7.3.1. However, for each $v \in \Sigma_0$ and each such $\sigma$, $g_v$ is fixed and $\delta_{E,v}(\sigma) \leq 4$. Hence $\delta_E^{\Sigma_0}(\sigma)$ is bounded as $\sigma$ varies over $\mathcal{A}_r$ for $r \geq 1$. The final result follows from the equation

$$\lambda_E(\sigma_{st}^{(r)}) \;=\; \lambda_E^{\Sigma_0}(\sigma_{st}^{(r)}) \;-\; \delta_E^{\Sigma_0}(\sigma_{st}^{(r)}) \;=\; p^{r\text{-}1}k \;-\; ap^{[(r\text{-}1)/2]}$$

which was pointed out before. □

**Remark 8.2.3.** We have made the simplifying assumption that $ord_v(j_A)$ is not divisible by $p$. Suppose that this assumption is not satisfied. Let $p^a$ be the highest power of $p$ dividing $ord_v(j_A)$, where $a \geq 1$. Then $\Delta_{r,v}$ will be a somewhat smaller subgroup of $B_r$. In fact, one can show that $\Delta_{r,v}$ is conjugate to a subgroup of $B_r$. Choosing $v$ suitably, we can assume that $\Delta_{r,v} \subset B_r$ and we will then have $\Delta_{r,v} \cap U_r = U_r^{p^a}$. This may have a possibly significant effect on the value of $\delta_{E,v}(\sigma)$. $\Diamond$

## 8.3 An illustration where the $\widetilde{\sigma}^{ss}$'s have abelian image.

First of all, note that if $\Delta$ is any finite group and if $\widetilde{\sigma}^{ss}$ has an abelian image for all $\sigma$ in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$, then $\Delta$ must have a normal Sylow $p$-subgroup $\Pi$ and $\Delta/\Pi$ must be abelian. Indeed, one sees that each $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$ must have an abelian image of order prime to $p$ and that $\Pi = \bigcap_\tau ker(\tau)$ has the stated properties, where $\tau$ varies over $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$. The converse is also clear. Furthermore, if $\Omega = \Delta/\Pi$, then $\Omega$ has order prime to $p$ and every element of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ factors through $\Omega$. If $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Omega)$, then there exists a unique $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Omega)$ such that $\widetilde{\sigma} \cong \tau$. Thus, if $X$ is a quasi-projective $\mathbf{Z}_p[\Delta]$-module, then one can determine (in principle) all the invariants $\lambda(X, \sigma)$ for $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ if one knows those invariants for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Omega)$. The special case where $\Omega \cong (\mathbf{Z}/p\mathbf{Z})^\times$ was discussed in some detail in section 7.4. We will concentrate on that special case in this illustration. Also, it is sometimes convenient to assume that $\Omega$ has been identified with a subgroup of $\Delta$ in some way. We will then have a certain homomorphism $\Omega \to \mathrm{Aut}(\Pi)$.

This situation is easily realized in the setting where $\Delta$ is a Galois group. For simplicity, we will take $p$ to be any odd prime, $F = \mathbf{Q}$, and $L = \mathbf{Q}(\mu_p)$ throughout this illustration. We can take $K$ to be any finite $p$-extension of $L$ which is Galois over $\mathbf{Q}$. Then $\Omega = \mathrm{Gal}(L/\mathbf{Q})$ is cyclic of order $p-1$. We let $\omega : \Omega \to \mathbf{Z}_p^\times$ be the Teichmüller character which is characterized by the fact that $\widetilde{\omega}$ gives the action of $\Omega$ on $\mu_p$. The elements of $\mathrm{Irr}_{\mathcal{F}}(\Omega)$ are the powers $\omega^i,\ 0 \leq i \leq p-2$.

Many such $K$'s exist. We will first consider examples where only $p$ is allowed to ramify. Later, starting in part **D**, we will allow more primes to be ramified. One simple type of example is the following. Class field theory shows that $L$ has $\frac{p+1}{2}$ independent $\mathbf{Z}_p$-extensions which are Galois over $\mathbf{Q}$. One of them is the cyclotomic $\mathbf{Z}_p$-extension $L_\infty = \mathbf{Q}(\mu_{p^\infty})$ of $L$. The others are characterized as Galois extensions $L_\infty^{(i)}$ of $\mathbf{Q}$ containing $L$ such that $\mathrm{Gal}(L_\infty^{(i)}/\mathbf{Q})$ is isomorphic to a semi-direct product $\Gamma_i \rtimes \Omega$, where $\Gamma_i \cong \mathbf{Z}_p$ and $\Omega$ acts on $\Gamma_i$ by $\omega^i$. Such a $\mathbf{Z}_p$-extension of $L$ exists for every odd $i,\ 1 \leq i \leq p-2$. We identify $\Gamma_i$ with $\mathrm{Gal}(L_\infty^{(i)}/L)$. One can take $K$ to be a layer in any one of the $L_\infty^{(i)}$'s for odd $i$. Then $K \cap \mathbf{Q}_\infty = \mathbf{Q}$ and $K/\mathbf{Q}$ is ramified only at $p$ and $\infty$.

Since the only ramified prime in $L/\mathbf{Q}$ is $p$, it is clear that if $l$ is a prime and $l \neq p$, then $l \in \Phi_{K/\mathbf{Q}}$ if and only if $l$ is ramified in $K/\mathbf{Q}$. For the examples in the previous paragraph, $\Phi_{K/\mathbf{Q}}$ is empty. We now consider the most general examples with that property. Equivalently, we consider arbitrary finite Galois extensions $K$ of $\mathbf{Q}$ such that $L \subseteq K \subset M$, where $M$ denotes the maximal pro-$p$ extension of $L$ such that only the prime of $L$ above $p$ is ramified. Thus, $M$ contains the compositum of all $\mathbf{Z}_p$-extensions of $L$. Furthermore, if $K'$ is a finite extension of $L$ contained in $M$, then $M$ also contains all $\mathbf{Z}_p$-extensions of $K'$. It is clear that $M$ is Galois over $\mathbf{Q}$ and so $\Omega$ acts on $\mathrm{Gal}(M/L)$. (This action is only well-defined modulo inner automorphisms.)

One can take $K$ to be the fixed field for any open, normal subgroup of $\mathrm{Gal}(M/L)$ which is $\Omega$-invariant. If one wants to have $K \cap \mathbf{Q}_\infty = \mathbf{Q}$, then one can equivalently make a certain requirement about the action of $\Omega$ on the quotient $\overline{\Pi} = \Pi\big/\Phi(\Pi)$, where $\Phi(\Pi)$ is the Frattini subgroup of $\Pi$. The action of $\Omega$ on $\overline{\Pi}$ by conjugation is well-defined and we can regard $\overline{\Pi}$ as a representation space over $\mathbf{F}_p$ for $\Omega$. One sees easily that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$ if and only if $\overline{\Pi}^\Omega$ is trivial. The assumption that $K \subset M$ is needed for this equivalence.

**A.** *Congruence relations.* Under the assumption that $\Phi_{K/\mathbf{Q}}$ is empty, the congruence relations take a simple form. One can even describe $X_E(K_\infty)$ as a $\mathbf{Z}_p[\Delta]$-module rather concretely if one makes an additional mild assumption. Here, just as in section 3.5, we let

$$\Delta \;=\; \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty) \qquad \textit{and} \qquad D \;=\; \mathrm{Gal}(K/\mathbf{Q}) \quad . \tag{8.3.a}$$

We will avoid making the assumption that $K \cap \mathbf{Q}_\infty = \mathbf{Q}$, although this will be satisfied in a number of our later examples. We just assume that $L \subseteq K \subset M$. Note that both of the groups $\Delta$ and $D$ are extensions of $\Omega$ by a pro-$p$ subgroup. We will usually use the letter $\sigma$ for an irreducible representation of either group, although sometimes we follow the notation of section 3.5, using $\rho$ for elements of $\mathrm{Irr}_{\mathcal{F}}(D)$ and $\sigma$ for elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$.

Suppose that $E$ is an elliptic curve over $\mathbf{Q}$ with good, ordinary reduction at $p$. We will assume that $\mathrm{Sel}_E(L_\infty)[p]$ is finite. Then all the invariants $\lambda_E(\sigma)$ for $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ can be determined if one just knows the invariants $\lambda_E(\omega^i)$ for $0 \leq i \leq p-2$. An especially simple case is described in the next proposition.

**Proposition 8.3.1.** *Assume that $L \subseteq K \subset M$ and that $\mathrm{Sel}_E(L_\infty)[p]$ is finite. Then $X_E(K_\infty)$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ is of degree divisible by $p-1$, then*

$$\lambda_E(\sigma) \;=\; \frac{n(\sigma)}{p-1} \cdot k \;, \qquad \textit{where} \;\; k \;=\; \sum_{i=0}^{p\text{-}2} \lambda_E(\omega^i) \;=\; \lambda_E(L_\infty) \quad .$$

*Furthermore, if one assumes that $p$ is non-anomalous for $E/\mathbf{Q}$ and that $E$ has no $\mathbf{Q}$-isogeny of degree $p$, then $X_E(K_\infty)$ is projective as a $\mathbf{Z}_p[\Delta]$-module. One has an isomorphism*

$$X_E(K_\infty) \;\cong\; P_{\tau_0} \otimes_{\mathbf{Z}_p} X_E(L_\infty)$$

*of $\mathbf{Z}_p[\Delta]$-modules, where $P_{\tau_0}$ is the indecomposable projective $\mathbf{Z}_p[\Delta]$-module corresponding to $\tau_0$ and $X_E(L_\infty)$ is regarded as a $\mathbf{Z}_p[\Delta]$-module via the natural homomorphism $\mathbf{Z}_p[\Delta] \to \mathbf{Z}_p[\Omega]$.*

If $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$, then we can still define $\lambda_E(\rho)$ as explained in section 3.5. We have

$$\lambda_E(\rho) \;=\; \frac{n(\rho)}{p-1} \cdot k \tag{8.3.b}$$

if $n(\rho)$ is divisible by $p-1$. Here $k$ is just as in the above proposition. This formula follows immediately from the proposition by using (3.5.a) and noticing that any $\sigma \in Orb_\rho$ will also have degree divisible by $p-1$. The ratio $n(\rho)/n(\sigma)$ is a power of $p$.

*Proof.* The first statement follows from proposition 3.2.1. One can take $\Sigma_0$ to be empty. The congruence relation then follows from the fact that if $n(\sigma)$ is divisible by $p-1$, then $\sigma$ is $\Pi$-induced. See formula (7.4.c). Actually, this congruence relation can be deduced just by using the formula of Hachimori and Matsuno for $p$-extensions. This follows by using remarks 2.1.8 and 6.1.2.

For projectivity, note first that the residue field for the unique prime of $L$ lying above $p$ is just $\mathbf{F}_p$. Hence if $p$ is non-anomalous for $E/\mathbf{Q}$, then the same is true for $E/L$ and therefore even for $E/K$ since $K/L$ is a $p$-extension. Also, if $E(K)[p] \neq 0$, then $E(L)[p] \neq 0$. Obviously, $E(L)[p]$ is $G_{\mathbf{Q}}$-invariant. If $E(L)[p]$ has order $p$, then that subgroup defines a $\mathbf{Q}$-isogeny of degree $p$. If $E(L)[p] = E[p]$, then $E[p]$ is an $\mathbf{F}_p$-representation space for $\Omega$. It must be reducible and semi-simple. Hence $E$ would then have two distinct $\mathbf{Q}$-isogenies of degree $p$. Therefore, the stated assumptions imply that the hypotheses in proposition 3.1.1 are satisfied. Hence, $X_E(K_\infty)$ is indeed projective as a $\mathbf{Z}_p[\Delta]$-module.

Thus, under the assumptions in the last part, and using (7.4.d), we have isomorphisms

$$X_E(K_\infty) \;\cong\; \bigoplus_{i=0}^{p\text{-}2} P_{\tau_i}^{w_E(\tau_i)} \;\cong\; P_{\tau_0} \otimes_{\mathbf{Z}_p} X, \qquad \textit{where} \quad X \;\cong\; \bigoplus_{i=0}^{p\text{-}2} \left(\mathbf{Z}_p \otimes \omega^i\right)^{w_E(\tau_i)}$$

of $\mathbf{Z}_p[\Delta]$-modules. Here we have written $\mathbf{Z}_p \otimes \omega^i$ for a free $\mathbf{Z}_p$-module of rank 1 on which $\Omega$ acts by $\omega^i$. We view it as a $\mathbf{Z}_p[\Delta]$-module on which $\Delta$ acts through the homomorphism $\Delta \to \Omega$. Finally, since $\omega^i$ is a lifting of $\tau_i$, we have $w_E(\tau_i) = \lambda_E(\omega^i)$ for all $i$. Thus, $X \cong X_E(L_\infty)$ as $\mathbf{Z}_p[\Omega]$-modules. The last statement follows from these remarks. $\square$

**Remark 8.3.2.** Instead of assuming that $E$ has no $\mathbf{Q}$-isogeny of degree $p$, it is sufficient to assume that $E'(\mathbf{Q})[p] = 0$ for every $E'$ which is $\mathbf{Q}$-isogenous to $E$. That assumption implies that $E(L)[p] = 0$ and hence that $E(K)[p] = 0$. To see this, assume to the contrary that $E(L)[p] \neq 0$. Now $\Omega$ acts semisimply on $E(L)[p]$ and so $E[p]$ must contain a subgroup $\Phi$ of order $p$ such that $\Phi \subseteq E(L)$ and $\Phi$ is $\Omega$-invariant. Thus, $\Omega$ acts on $\Phi$ by an $\mathbf{F}_p^\times$-valued character $\varphi$. Since $E$ has good, ordinary reduction at $p$, either $\varphi$ or $\omega\varphi^{-1}$ must be unramified at $p$. Since $p$ is totally ramified in $L/\mathbf{Q}$, either $\varphi$ is trivial or $\varphi = \omega$. In the first case, we would have $E(\mathbf{Q})[p] \neq 0$. In the second case, we would have $E'(\mathbf{Q})[p] \neq 0$, where $E' = E/\Phi$. $\Diamond$

**B.** *Letting $K$ and $\sigma$ vary.* We regard $\lambda_E(\sigma)$ as a function of $\sigma$ and study its behavior as $\sigma$ varies. We can let $K$ vary since $\lambda_E(\sigma)$ depends only on $E$ and $\sigma$ (assuming that $p$ is fixed), but not on $K$, as we remarked at the beginning of this chapter. Thus, we might simply consider all the irreducible Artin representations $\sigma$ of $\mathrm{Gal}(M/\mathbf{Q})$. However, describing all those representations in a useful way would be difficult. Irreducible representations $\sigma$ whose degree is divisible by $p-1$ seem to be quite ubiquitous. Such a representation is induced from an irreducible Artin representation $\pi$ of the normal, pro-$p$ subgroup $\mathrm{Gal}(M/L)$, as explained in part **A** of section 7.4. That is, if $p-1$ divides $n(\sigma)$, then $\sigma$ is $\Pi$-induced, where $\Pi = \mathrm{Gal}(M/L)$. Any irreducible Artin representation $\sigma$ of $\mathrm{Gal}(M/\mathbf{Q})$ is at least a constituent in such an induced representation, along with all the twists $\sigma \otimes \omega^i$. To be precise, there is a one-to-one correspondence between the set of $\Omega$-orbits of irreducible Artin representations of $\mathrm{Gal}(M/L)$ and the set of $\widehat{\Omega}$-orbits of irreducible Artin representations of $\mathrm{Gal}(M/\mathbf{Q})$. The $\Omega$-orbits of length $p-1$ correspond to the irreducible representations of $\mathrm{Gal}(M/\mathbf{Q})$ which are induced from $\mathrm{Gal}(M/L)$.

Rather than considering all the irreducible Artin representations, we tend to restrict to more manageable families. For example, choose a fixed tower $K_0, K_1, ..., K_r, ...$ of subfields of $M$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$ for $r \geq 0$. Note that $K_r \cap \mathbf{Q}_\infty = \mathbf{Q}$ for each $r$ in this situation because the group $H_r$ has no nontrivial quotient of order $p$. We can consider the various irreducible representations of the $H_r$'s which were described in proposition 7.4.4 as Artin representations of $\mathrm{Gal}(M/\mathbf{Q})$. Their degrees are unbounded. The inverse limit $H_\infty$ of the $H_r$'s can be identified with an open subgroup of $PGL_2(\mathbf{Z}_p)$ of index $p+1$. Its Sylow pro-$p$ subgroup $\Pi_\infty$ is normal, the corresponding quotient group is isomorphic to $\Omega$, and the action of $\Omega$ on the Frattini quotient $\overline{\Pi}_\infty$ can be determined. These are ingredients in the proof of the following proposition. The assumption that $p$ is regular is important in that it implies that $\mathrm{Gal}(M/L)$ is a free pro-$p$ group, a result which is proved in [MoNg], and that fact allows us to easily define homomorphisms of $\mathrm{Gal}(M/L)$ onto $\Pi_\infty$. Carefully taking into account the action of $\Omega$ on $\overline{\Pi}_\infty$, it turns out that we can define homomorphisms which can be extended to $\mathrm{Gal}(M/\mathbf{Q})$. The argument will be presented in [Gr09a]. We state the result

here because it shows that many towers of extensions $K_r$ of the above type exist, at least when $p$ is a regular prime. In general, we do not know if such a tower exists if $p$ is irregular.

**Proposition 8.3.3.** *Suppose that $p$ is an odd, regular prime. Then there exist an uncountable family of surjective homomorphisms $f : \mathrm{Gal}(M/\mathbf{Q}) \to H_\infty$, all with distinct kernels.*

**Remark 8.3.4.** Each such homomorphism $f$ would determine a tower of fields $K_0, K_1, ...$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$ and $\bigcup_r K_r = M^{\ker(f)}$. That subfield of $M$ is an extension of $L$ with Galois group isomorphic to $\Pi_\infty$ and an extension of $\mathbf{Q}$ with Galois group isomorphic to $H_\infty$. Two different $f$'s correspond to distinct subfields of $M$. In fact, since the Lie algebra of the $p$-adic Lie group $\Pi_\infty$ is $\mathfrak{sl}_2(\mathbf{Q}_p)$, which is simple, the intersection of any two of those subfields will just be a finite extension of $L$. Hence the fields $K_r$ in the corresponding towers must differ for sufficiently large $r$. $\Diamond$

Another quite different approach is to consider Artin representations of a given degree. It is known that finite $p$-groups are monomial groups. That is, if $\pi \in \mathrm{Irr}_{\mathcal{F}}(\Pi)$, then there exists a subgroup $\Pi'$ of $\Pi$ and a 1-dimensional representation $\pi'$ of $\Pi'$ such that $\pi \cong \mathrm{Ind}_{\Pi'}^{\Pi}(\pi')$. Thus, if $\sigma$ is any irreducible representation of $\Delta$ which is $\Pi$-induced, then $\sigma$ is induced from a 1-dimensional representation of some subgroup of $\Pi$. The index is determined by $n(\sigma)$. Even if $\sigma$ is not $\Pi$-induced, the direct sum of all the distinct (non-isomorphic) twists of $\sigma$ by powers of $\omega$ will be isomorphic to $\mathrm{Ind}_{\Pi'}^{\Delta}(\pi')$ for some choice of $\Pi'$ and 1-dimensional $\pi'$.

To simplify the discussion, we modify the notation for induced representations. Suppose that $L'$ is a finite extension of $L$ contained in $M$. If $\pi'$ is any representation of $\mathrm{Gal}(M/L')$, then we let $\mathrm{Ind}_{L'}^{\mathbf{Q}}(\pi')$ denote the representation of $\mathrm{Gal}(M/\mathbf{Q})$ induced from $\pi'$. Assuming that $n(\pi') = 1$, this induced representation has degree $[L' : \mathbf{Q}] = (p-1)p^a$, where $p^a = [L' : L]$. We will use the notation $\mathcal{L}'$ for the maximal abelian extension of $L'$ contained in $M$. We continue to assume for simplicity that $p$ is a regular prime. Then $\mathrm{Gal}(\mathcal{L}'/L')$ is a free $\mathbf{Z}_p$-module of rank $\frac{p-1}{2}p^a + 1$. Thus, $\mathcal{L}'$ is just the compositum of all $\mathbf{Z}_p$-extensions of $L'$. Let $\mathcal{C}_{L'}$ denote the group of Artin characters of $\mathrm{Gal}(\mathcal{L}'/L')$, which is simply the Pontryagin dual of $\mathrm{Gal}(\mathcal{L}'/L')$. Thus, $\mathcal{C}_{L'}$ is a cofree $\mathbf{Z}_p$-module of that same corank. If one fixes the field $L'$, then one obtains a family of Artin representations of $\mathrm{Gal}(M/\mathbf{Q})$ parametrized by $\mathcal{C}_{L'}$, all of degree $(p-1)p^a$. Namely, if $\pi' \in \mathcal{C}_{L'}$, then one obtains the representation $\mathrm{Ind}_{L'}^{\mathbf{Q}}(\pi')$. One can view this from a *"deformation theory"* point of view. Namely, consider the completed group ring $R_{L'} = \mathbf{Z}_p[[\mathrm{Gal}(\mathcal{L}'/L')]]$ (which is isomorphic to a formal power series ring over $\mathbf{Z}_p$ in $\frac{p-1}{2}p^a + 1$ variables). One has the natural injective homomorphism $\kappa_{L'} : \mathrm{Gal}(\mathcal{L}'/L') \to GL_1(R_{L'})$. One then obtains the induced representation $\mathrm{Ind}_{L'}^{\mathbf{Q}}(\kappa_{L'}) : \mathrm{Gal}(\mathcal{L}'/\mathbf{Q}) \to GL_n(R_{L'})$, where $n = (p-1)p^a$. Now every $\pi' \in \mathcal{C}_{L'}$ can be extended to a continuous, $\mathbf{Z}_p$-algebra homomorphism

from $R_{L'}$ to the ring of integers of $\mathcal{F}$, where $\mathcal{F}$ is generated over $\mathbf{Q}_p$ by the values of the character $\pi'$. We refer to this homomorphism as *"specialization"* at $\pi'$. Then $\mathrm{Ind}_{L'}^{\mathbf{Q}}(\pi')$ is just the corresponding *"specialization"* of $\mathrm{Ind}_{L'}^{\mathbf{Q}}(\kappa_{L'})$. Of course, there will usually be repetitions since different $\pi'$'s can have isomorphic specializations.

We believe that *"almost all"* of these specializations will be irreducible. To explain what this means, let $P_{\pi'}$ denote the kernel of the specialization homomorphism corresponding to some $\pi'$ in $\mathcal{C}_{L'}$. Of course, $P_{\pi'}$ is a prime ideal of $R_{L'}$. If $I'$ is an ideal in $R_{L'}$, then we say that $\pi'$ vanishes on $I'$ if $I' \subseteq P_{\pi'}$. With this terminology, we believe that there should exist a nonzero ideal $I'$ in $R_{L'}$ with the following property:

$\mathrm{Ind}_{L'}^{\mathbf{Q}}(\pi')$ *is irreducible for all* $\pi'$ *which do not vanish on* $I'$.

The following proposition implies this assertion if we make the extra assumption that $L'/\mathbf{Q}$ is Galois.

**Proposition 8.3.5.** *Suppose that $J$ is a finite, totally complex, Galois extension of $\mathbf{Q}$. Let $\mathcal{J}$ denote the compositum of all $\mathbf{Z}_p$-extensions of $J$ and let $R_J = \mathbf{Z}_p[[\mathcal{J}/J)]]$. Let $\mathcal{C}_J$ denote the Pontryagin dual of $\mathrm{Gal}(\mathcal{J}/J)$. Then there exists a nonzero ideal $I$ of $R_J$ with the following property: If $\phi \in \mathcal{C}_J$ and $\mathrm{Ind}_J^{\mathbf{Q}}(\phi)$ is reducible, then $\phi$ vanishes on $I$.*

*Proof.* Let $G = \mathrm{Gal}(J/\mathbf{Q})$ and let $N = \mathrm{Gal}(\mathcal{J}/J)$, a normal subgroup of $\mathcal{G} = \mathrm{Gal}(\mathcal{J}/\mathbf{Q})$. Let $n = |G|$. Thus, $G$ acts on $\mathcal{C}_J$ by conjugation and each orbit has length dividing $n$. The representation $\mathrm{Ind}_J^{\mathbf{Q}}(\phi)$ has degree $n$. Suppose that $\mathrm{Ind}_J^{\mathbf{Q}}(\phi)$ is reducible and that $\rho$ is one of its irreducible constituents. Then $n(\rho) < n$. Now $\phi$ and all of its conjugates under the action of $G$ are constituents in $\rho|_N$. Consequently, the $G$-orbit of $\phi$ has length $< n$. Thus, the stabilizer of $\phi$ is nontrivial. Let $H$ be a nontrivial cyclic subgroup of that stabilizer. The character $\phi$ of $N$ factors through the maximal quotient $N_H$ on which $H$ acts trivially. There is a ring homomorphism

$$R_J = \mathbf{Z}_p[[N]] \longrightarrow \mathbf{Z}_p[[N_H]]$$

whose kernel $I_H$ is the ideal generated by elements $g - id_N$, where $g$ varies over a set of topological generators for the kernel of the homomorphism $N \to N_H$. We will show that $H$ acts nontrivially on $N$. That fact implies that $I_H$ is a nonzero ideal. It is clear that $\phi$ vanishes on $I_H$.

Consider $N \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ as a representation space for $G$. Its dimension is bounded below by $\frac{1}{2}[J : \mathbf{Q}] + 1$; Leopoldt's conjecture for $J$ and $p$ asserts that equality holds. However, by class field theory, one can at least say that $N \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ has $\mathrm{Ind}_{G_\eta}^{G}(\varepsilon)$ as a direct summand. Here $\eta$ is an archimedean prime of $J$, $G_\eta$ is the corresponding decomposition subgroup of $G$, and $\varepsilon$ is the nontrivial character of $G_\eta$. It suffices to show that any nontrivial element $h$ of $G$ acts nontrivially on $\mathrm{Ind}_{G_\eta}^{G}(\varepsilon)$. This is rather easy. For if $h$ acts trivially, then $h$ induces a trivial

permutation of the left coset space $G/G_\eta$. Hence, $h \in G_\eta$. However, $h$ then acts by $\varepsilon(h)$ on some subspace of $\mathrm{Ind}_{G_\eta}^{G}(\varepsilon)$, and hence acts nontrivially on that subspace.

Let $I = \bigcap_H I_H$, where $H$ varies over all nontrivial cyclic subgroups of $G$. Then $I$ is a nonzero ideal of $R_J$ and has the property stated in the proposition. $\square$

**C.** *Some specific examples.* We return now to Selmer groups. We continue to take $L = \mathbf{Q}(\mu_p)$ throughout this illustration. Then $L_\infty = \mathbf{Q}(\mu_{p^\infty})$. As we pointed out at the end of chapter 4, it is possible to verify the finiteness of $\mathrm{Sel}_E(L_\infty)[p]$ for specific elliptic curves and primes $p$ by calculating the coefficients in a certain expansion of the $p$-adic $L$-functions $L_p(s, E, \omega^i)$ associated to $E$ and the characters $\omega^i$. Such calculations were done many years ago by T. McCabe and more recently by R. Pollack. Actually, the first such calculations can be found in [MaSw]. All of those calculations deal with the analytic $\lambda$- and $\mu$-invariants, which we will denote by $\lambda_E^{anal}(\omega^i)$ and $\mu_E^{anal}(\omega^i)$. The calculations verify that $\mu_E^{anal}(\omega^i) = 0$ for all $i$ in the cases where that is expected to be so. The value of the $\lambda_E^{anal}(\omega^i)$'s is also determined. If the map $G_{\mathbf{Q}} \to \mathrm{Aut}\big(T_p(E)\big)$ is surjective, then one can use theorem 17.4 in [Kat] to conclude that $\mathrm{Sel}_E(L_\infty)[p]$ is indeed finite. But one only gets the inequality $\lambda_E(\omega^i) \le \lambda_E^{anal}(\omega^i)$ for the $\lambda$-invariants. Kato's theorem establishes that inequality even without the assumption of surjectivity. Recent work of Skinner and Urban should give the opposite inequality under rather general assumptions.

Our main example will concern the three elliptic curves of conductor 11 and various choices of the prime $p$. Those curves are related by isogenies of degree 5 and so the $\lambda$ and $\mu$-invariants actually don't depend on which curve we choose, except for $p = 5$. However, we will consider that prime first.

*Conductor 11, $p = 5$.* It is convenient to choose $E$ to be the curve defined by the equation $y^2 + y = x^3 - x^2$. That is the curve 11A3 in [Cre]. It is verified in [CS00] that $\mathrm{Sel}_E(L_\infty)_p = 0$. Therefore we can apply proposition 8.3.1 to $E$. We have $k = 0$. Consequently, it follows that $\lambda_E(\sigma) = 0$ for all Artin representations $\sigma$ of $\mathrm{Gal}(M/\mathbf{Q})$. In this situation, exactly the same result follows directly from the main theorems in [HaMa]. We remark that the $\mu$-invariants for 11A1 and 11A2, the other two elliptic curves of conductor 11, are actually positive. One can't apply proposition 8.3.1 directly to those curves. However, the $\lambda$-invariants are unchanged by isogeny and so the conclusion is the same. If $E'$ is any one of those elliptic curves, then $\lambda_{E'}(\sigma) = 0$ for all $\sigma$ as above.

We will consider a few other primes based on calculations of Mazur and Swinnerton-Dyer. Table 5 on page 58 of [MaSw] gives the values of the $\lambda_E^{anal}(\omega^i)$'s for all primes $p$ where $E$ has good, ordinary reduction in the range $7 \le p \le 347$. They verified that $\mu_E^{anal}(\omega^i) = 0$ for those primes and all $i$, $0 \le i \le p-2$. Now the map $G_{\mathbf{Q}} \to \mathrm{Aut}\big(T_p(E)\big)$ is surjective for all $p \ge 7$. (This is verified in section 5.5.1 of [Se72].) Thus, Kato's theorem can be

applied and so $\mathrm{Sel}_E(L_\infty)[p]$ is indeed finite for all those $p$'s. As for the $\lambda$-invariants, the table shows nonzero values of some of the $\lambda_E^{anal}(\omega^i)$'s for 49 of the 69 primes $p$ in the above range. Thus, for the remaining 20 primes, one has $k = 0$ and therefore we have $\lambda_E(\sigma) = 0$ for all irreducible Artin representations $\sigma$ of $\mathrm{Gal}(M/\mathbf{Q})$. For the other primes, one expects to have $k \geq 1$. The list includes 14 of the 17 irregular primes in the range of the table. We select regular primes so that we can apply proposition 8.3.3.

*Conductor 11, $p = 7$.* The first case where $k \geq 1$ is $p = 7$. The table gives $\lambda_E^{anal}(\omega^3) = 1$ and $\lambda_E^{anal}(\omega^i) = 0$ for $i \in \{0, 1, 2, 4, 5\}$. Thus, $\lambda_E(\omega^i) = 0$ except possibly for $i = 3$. For $i = 3$, we use the fact that the Mordell-Weil group of the quadratic twist $E_7$ ( which is one of the curves 539D) turns out to have rank 1. Thus, $\mathrm{Sel}_{E_7}(\mathbf{Q})$ contains a subgroup isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$ and hence so does $\mathrm{Sel}_{E_7}(\mathbf{Q}_\infty)$. Since the quadratic character of conductor 7 is $\omega^3$, we have $1 \leq \lambda_E(\omega^3) \leq \lambda_E^{anal}(\omega^3)$ and hence $\lambda_E(\omega^3) = 1$. Thus, $k = 1$ for $p = 7$. As a consequence, using proposition 8.3.1, it follows that

$$\lambda_E(\sigma) = \frac{n(\sigma)}{6} \tag{8.3.c}$$

for all the irreducible representations of $\mathrm{Gal}(M/\mathbf{Q})$ with degree divisible by $p - 1 = 6$.

Continuing to take $p = 7$, we consider certain irreducible Artin representations $\sigma$ of degree $p^r$. Consider any quotient of $\mathrm{Gal}(M/\mathbf{Q})$ isomorphic to $H_r$ and a representation $\sigma$ of the form $\xi_{H_r,\psi}$, where $\psi$ is a primitive character of $B_r/U_r$. Such representations were described in remark 7.4.3. The corresponding congruence relations were discussed in remark 7.4.9. There are $p - 1 = 6$ possibilities for $\widetilde{\psi}$. We have

$$\lambda_E(\xi_{H_r,\psi}) \;=\; d_r + 1 \quad \textit{if } \widetilde{\psi} \cong \widetilde{\omega}^3 \;, \qquad \lambda_E(\sigma) \;=\; d_r \quad \textit{otherwise} \quad . \tag{8.3.d}$$

This follows immediately from (7.4.f).

The prime $p = 7$ is non-anomalous for $E/\mathbf{Q}$. (In fact, if $p > 5$, then $p$ is non-anomalous for $E/\mathbf{Q}$. See lemma 5.2 in [Gr99].) Proposition 8.3.1 implies that if $K$ is any finite Galois extension of $\mathbf{Q}$ contained in $M$, then $X_E(K_\infty)$ is projective as a $\mathbf{Z}_p[\mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)]$-module. The same remark applies to all the other primes $p$ in the range $7 \leq p \leq 347$.

*Conductor 11, $p = 127$.* The largest value of $k$ indicated in the table is for $p = 127$. The table gives $\lambda_E^{anal}(\omega^i) = 1$ for $i = 29, 63, 97$, and also for all $i$'s such that $\omega^i$ has order 9. For the other $i$'s, one has $\lambda_E^{anal}(\omega^i) = 0$. This suggests that $k = 9$. Except for $i = 29$ and 97, the contribution to $\mathrm{Sel}_E(L_\infty)_p$ probably comes from the Mordell-Weil group $E(L)$. This is stated in [MaSw] as likely, but not verified. Assuming this is so, it then follows (just as for $p = 7$) that $\lambda_E(\omega^i) = 1$ for at least those seven values of $i$. The contribution for $i \in \{29, 97\}$ should come from the Tate-Shafarevich group (although this is mislabeled in [MaSw]) and

so it is not clear how to verify that $\lambda_E(\omega^i) = 1$ for those two $i$'s. Thus, applying Kato's theorem gives the inequality $7 \leq k \leq 9$ under the above assumption about the Mordell-Weil group for $E$ over $L$. In fact, we would have $k = 7$ or $k = 9$ because $\lambda_E(\omega^{29}) = \lambda_E(\omega^{97})$. Thus, those $\lambda$-invariants are either both 1 (which is conjecturally so) or both 0.

We have just used the symmetry in the $\lambda$-invariants. One always has the equalities $\lambda_E^{anal}(\omega^i) = \lambda_E^{anal}(\omega^{p\text{-}1\text{-}i})$. This is a consequence of the functional equation for the twisted Hasse-Weil $L$-functions, and their $p$-adic analogues. On the algebraic side, the analogous equalities $\lambda_E(\omega^i) = \lambda_E(\omega^{p\text{-}1\text{-}i})$ also hold. This result is a special case of corollary 10.1.3 since the dual of $\omega^i$ is $\omega^{p\text{-}1\text{-}i}$.

Assuming one has determined $k$, one then gets exact formulas for $\lambda_E(\sigma)$ for every irreducible Artin representation $\sigma$ of $\mathrm{Gal}(M/\mathbf{Q})$ which is induced from $\mathrm{Gal}(M/L)$, just as described in proposition 8.3.1. In principle, one can get formulas for other $\sigma$'s too. For example, one can use (7.4.f) for some $\sigma$'s, assuming that the above value for $\lambda_E(\omega^{29})$ has been confirmed.

*Conductor 11,* $p = 211$. The table gives $\lambda_E^{anal}(\omega^i) = 1$ for $i \in \{23, 41, 90, 105, 120, 169, 187\}$ and $\lambda_E^{anal}(\omega^i) = 0$ for the other $i$'s. Thus, one should have $k = 7$, but this seems difficult to verify. However, as remarked above, recent work of Skinner and Urban may settle this. In this case, only one of those nonzero $\lambda$-invariants comes from the Mordell-Weil group, namely $\lambda_E(\omega^{105})$. Note that $\omega^{105}$ is the quadratic character of conductor 211.

**D.** *Allowing more ramification. The $\mathcal{H}$-trivial case.* The assumption that $K/\mathbf{Q}$ be ramified only at $p$ is rather restrictive. One can usually weaken that assumption considerably and still find that the conclusions in proposition 8.3.1 are valid. Although it is not essential, we assume that $p \geq 5$ to simplify the statements and discussion. We will now consider extensions $K/\mathbf{Q}$ where $\Phi_{K/\mathbf{Q}}$ may be nonempty. Let $\Sigma_0$ be a finite set of primes of $\mathbf{Q}$ not containing $p$ or $\infty$ and let $\Sigma = \Sigma_0 \cup \{p, \infty\}$. Let $\mathbf{Q}_\Sigma$, the maximal extension of $\mathbf{Q}$ unramified outside of $\Sigma$ and let $M_\Sigma$ denote the maximal pro-$p$ extension of $L$ contained in $\mathbf{Q}_\Sigma$. Then $L \subset M \subseteq M_\Sigma$, with equality only if $\Sigma_0$ is empty. We will now assume that $K$ is a finite, Galois extension of $\mathbf{Q}$ and that $L \subseteq K \subset M_\Sigma$. We let $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ as before.

Suppose that $E$ is an elliptic curve over $\mathbf{Q}$ with good, ordinary reduction at $p$. We now consider examples where the set $\Sigma_0$ is chosen so that the primitive and non-primitive Selmer groups that we consider actually coincide. The following proposition describes when this is the case.

**Proposition 8.3.6.** *Assume that $p \geq 5$ and that every $l$ in $\Sigma_o$ satisfies one of the following conditions:*

*(a) $E$ has non-split, multiplicative reduction at $l$ and $l$ has odd order modulo $p$,*

*(b)* *$E$ has good reduction at $l$ and no power of $\widetilde{l}$ is a root of $x^2 - \widetilde{a}_l x + \widetilde{l}$,*

*(c)* *$E$ has additive reduction at $l$.*

*Then $\mathcal{H}_l(K_\infty, E) = 0$ for all $l \in \Sigma_0$. Consequently, $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \mathrm{Sel}_E(K_\infty)_p$. If $\mathrm{Sel}_E(L_\infty)[p]$ is finite, then the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module and all of the conclusions stated in proposition 8.3.1 are valid.*

A set $\Sigma_0$ satisfying the above hypothesis will be said to be *"$\mathcal{H}$-trivial for $E$ and $p$"*. In *(b)*, the quadratic polynomial is in $\mathbf{F}_p[x]$ and is just as in proposition 8.2.1, taking $F = \mathbf{Q}$. It is that condition which sometimes allows for an $\mathcal{H}$-trivial set to be arbitrarily large.

*Proof.* The proof of the vanishing of $\mathcal{H}_l(K_\infty, E)$ is essentially the same as for proposition 8.2.1 and depends just on the fact that the completion of $K$ at a prime above $l$ is a $p$-extension of $\mathbf{Q}_l(\mu_p)$. The stated conditions guarantee that we have $\langle \rho_{E,l}, \omega_l^j \rangle = 0$ for all $j$. We also have the inclusion $\Phi_{K/\mathbf{Q}} \subseteq \Sigma_0$ since we are assuming that $K \subset M_\Sigma$. The assumption that $\mathrm{Sel}_E(L_\infty)[p]$ is finite implies the finiteness of $\mathrm{Sel}_E(K_\infty)[p]$ since $K/L$ is a $p$-extension. Proposition 3.2.1 then implies that the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ is quasi-projective as a $\mathbf{Z}_p[\Delta]$-module. □

Under the assumptions of the above proposition, all of the congruence relations described before for the case where $\Sigma_0$ is empty will be valid for the larger class of Artin representations which factor through $\mathrm{Gal}(K/\mathbf{Q})$ for some $K$ chosen as above. In particular, if $\sigma$ is such an Artin representation and has degree divisible by $p-1$, then the formula for $\lambda_E(\sigma)$ given in proposition 8.3.1 applies.

*Conductor 11, $p = 7$ again.* Returning to the special case where $E$ has conductor 11, here is an example of an $\mathcal{H}$-trivial set for $E$ and $p = 7$:

$$\Sigma_0 \;=\; \{2, 3, 13, 17, 23, 29, 41, 43, 53, 59, 61, 67, 71, 79, 83, 101, 103, 107, 109, 127\} \quad .$$

The set of primes $l$ for which *(b)* fails to be satisfied has a positive Dirichlet density. We've included the first 20 such primes in $\Sigma_0$. One can find arbitrarily large $\mathcal{H}$-trivial sets for $E$ and all the other primes $p$ too, except for $p = 5$. In that case, one easily sees that the roots of $x^2 - \widetilde{a}_l x + \widetilde{l}$ are $\widetilde{1}$ and $\widetilde{l}$. Hence it is not possible to find a nonempty $\mathcal{H}$-trivial set $\Sigma_0$ for $E$ and $p = 5$.

Let $\Sigma = \Sigma_0 \cup \{p, \infty\}$. We continue to consider $p = 7$. Suppose that $A$ is an elliptic curve defined over $\mathbf{Q}$ whose conductor is divisible only by primes in $\Sigma$. Suppose also that $A(\mathbf{Q})[p] \neq 0$. It then follows that $\mathbf{Q}(A[p^\infty]) \subset M_\Sigma$. It also follows that $\rho_A$ is not surjective. In fact, for a suitable basis of $T_p(A)$, we have $\widetilde{\rho}_A = \begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix}$. Many such $A$'s exist and

so this construction provides an ample source of specific Galois extensions $K/\mathbf{Q}$ satisfying the assumptions in this illustration. Here are some choices of $A$ found by perusing [Cre]: 26B, 174B, 258F, 294B, 546F, 574I, and 762G. For each of those curves and for any $r \geq 0$, we have $L \subseteq \mathbf{Q}(A[p^{r+1}]) \subset M_\Sigma$. It turns out that the image of $G_\mathbf{Q}$ in $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ is isomorphic to $H_r$ for all of those elliptic curves, as we will explain below. Therefore one obtains certain quotients of $\mathrm{Gal}(M_\Sigma/\mathbf{Q})$ isomorphic to $H_r$ and our earlier remarks apply to the Artin representations that factor through those quotients. In particular, either (8.3.c) or (8.3.d) will valid for each such Artin representation, depending just on the degree.

The next rather general proposition shows that under certain assumptions the image of $\rho_A$ is determined by the image of $\widetilde{\rho}_A$. It implies the assertion made above. The proof will be given in [Gr09a]. This result is probably not new, although we haven't found it stated in the literature. Some version of it was previously pointed out by T. Fisher. One can also include $p = 5$ in the statement, but only by making additional assumptions.

Suppose that $A$ is an elliptic curve defined over $\mathbf{Q}$ which has a $\mathbf{Q}$-isogeny of degree $p$. Let $\Phi$ denote the kernel of the isogeny and let $\Psi = A[p]/\Phi$. The actions of $G_\mathbf{Q}$ on $\Phi$ and $\Psi$ are described by $\mathbf{F}_p^\times$-valued characters $\varphi$ and $\psi$, respectively. The statement below refers to a Sylow pro-$p$ subgroup of $\mathrm{Aut}\big(T_p(A)\big)$. One can identify $\mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(A)\big)$ and $\mathrm{Aut}_{\mathbf{F}_p}\big(T_p(A)/pT_p(A)\big)$ with $GL_2(\mathbf{Z}_p)$ and $GL_2(\mathbf{F}_p)$, respectively, by choosing a basis for $T_p(A)$ over $\mathbf{Z}_p$ and the image of that basis in $T_p(A)/pT_p(A) \cong A[p]$. One Sylow pro-$p$ subgroup of $GL_2(\mathbf{Z}_p)$ is the group of matrices whose image in $GL_2(\mathbf{F}_p)$ is upper triangular and unipotent. The others are conjugate to that subgroup. Note also that $\varphi\psi = \omega$ is an odd character. Therefore, $\varphi\psi^{-1}$ is also odd and hence its order is even.

**Proposition 8.3.7.** *Assume that $p \geq 7$. Assume also that $\varphi\psi^{-1}$ is not of order 2. Then the image of $\rho_A$ contains a Sylow pro-$p$ subgroup of* $\mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(A)\big)$.

Of course, $\mathrm{im}(\rho_A) \cong \mathrm{Gal}\big(\mathbf{Q}(A[p^\infty])/\mathbf{Q}\big)$. For any $r \geq 0$, we can also interpret the image of $\mathrm{im}(\rho_A)$ in $\Delta_r = PGL_2(\mathbf{Z}/p^{r+1})$ as a Galois group. We let $K_r$ denote the corresponding Galois extension of $\mathbf{Q}$ and identify $\mathrm{Gal}(K_r/\mathbf{Q})$ with the corresponding subgroup of $\Delta_r$. Under the assumptions of the above proposition, and choosing a suitable basis for $T_p(A)$, the Sylow $p$-subgroup of $\mathrm{Gal}(K_r/\mathbf{Q})$ is normal and is identified with the subgroup $\Pi_r$. The corresponding fixed field is an extension of $\mathbf{Q}$ of degree dividing $p-1$ and is precisely the fixed field for $\ker(\varphi\psi^{-1})$. If this field turns out to be $L$, then the fields $K_r$ are extensions of exactly the kind we are considering in this illustration. It turns out that we even have $K_r \cap \mathbf{Q}_\infty = \mathbf{Q}$, although this is not really needed. (See section 3.4.)

One case where $\varphi\psi^{-1}$ is not of order 2 occurs if $A(\mathbf{Q})[p] \neq 0$ and $p \geq 5$. We can then

take $\varphi$ to be trivial and $\psi = \omega$. Assuming that $p \geq 7$, proposition 8.3.7 implies that

$$\mathrm{im}(\rho_A) \;=\; \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a \in 1 + p\mathbf{Z}_p,\ b \in \mathbf{Z}_p,\ c \in p\mathbf{Z}_p,\ d \in \mathbf{Z}_p^\times \right\} \quad .$$

The image of that group in $PGL_2(\mathbf{Z}_p)$ is precisely the group $H_\infty$ defined in remark 7.4.6 and the image in $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for any $r \geq 0$ is precisely $H_r$, as mentioned above. More generally, under the assumptions of the proposition, the image of $G_\mathbf{Q}$ in $PGL_2(\mathbf{Z}_p)$ arising from $\rho_A$ is equal to $H_\infty$ if and only if $\varphi\psi^{-1}$ has order $p-1$. 0therwise, the image will be the unique subgroup of $H_\infty$ of index $(p-1)/e$, where $e$ denotes the order of $\varphi\psi^{-1}$.

We've already listed a number of examples where $A(\mathbf{Q})[p] \neq 0$ when $p = 7$. Such examples are abundant. If $p > 7$, then $A(\mathbf{Q})[p] = 0$ and such examples can't exist. However, for $p = 11$, we can take $A$ to be one of the curves 121A or 121C in [Cre]. Each has a $\mathbf{Q}$-isogeny of degree 11. For one of them, one finds that $\varphi = \omega^7,\ \psi = \omega^4$ and hence the ratio is $\omega^3$ which has order $p - 1 = 10$. Thus, if $A$ is any one of those curves, then $\mathbf{Q}(A[11^\infty])$ contains a tower of subfields $K_r$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$. Furthermore, we do actually have $L \subset K_r \subset M$ and so we can simply take $\Sigma_0$ to be empty.

On the other hand, if $A$ is one of the curves 121B, then $A$ has complex multiplication by the ring of integers in $\mathbf{Q}(\sqrt{-11})$ and hence has a $\mathbf{Q}$-isogeny of degree $p$. For one of them, one finds that $\varphi = \omega^8,\ \psi = \omega^3$ and hence the ratio is $\omega^5$ which has order 2. (This must be so in the CM-case.) The image of $\rho_A$ is just a 2-dimensional $p$-adic Lie group. Its image in $PGL_2(\mathbf{Z}_p)$ is not even of finite index.

If $p > 11$, then it is still possible for $\varphi\psi^{-1}$ to have order $p-1$. One sees easily that this will be true if the conductor of $A$ is not divisible by $p$. This happens for $p = 37$. If $A$ is either one of the two elliptic curves of conductor 1225 which have a $\mathbf{Q}$-isogeny of degree 37, then $A$ has good, ordinary reduction at 37. Thus, even when one restricts $\varphi\psi^{-1}$ to an inertia group for 37, its order is $p - 1 = 36$. We can then apply proposition 8.3.7 to $\rho_A$ to obtain a tower of extensions $K_r$ of $\mathbf{Q}$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$ for all $r \geq 0$. However, the fields $K_r$ don't quite fit into this illustration. Although the fixed field for $\Pi_r$ is a cyclic extension of $\mathbf{Q}$ of degree $p - 1 = 36$, that field is ramified at 5, 7, and 37, and can't be $L = \mathbf{Q}(\mu_{37})$. Similar remarks can be made if $p = 17$. There exist elliptic curves $A$ of conductor $2 \cdot 5^2 \cdot 17^2$ which have a cyclic $\mathbf{Q}$-isogeny of degree $p$. Since $\varphi\psi = \omega$ has order $p - 1 = 16$, one sees easily that $\varphi\psi^{-1}$ also has order 16. Hence proposition 8.3.7 can again be applied to $\rho_A$. However, $\varphi\psi^{-1}$ is ramified at 5 and 17, and hence the corresponding cyclic extension of $\mathbf{Q}$ cannot be $L$.

For $p = 5$, there is a variant of proposition 8.3.7. If $A(\mathbf{Q})[5] \neq 0$, then there exists a tower of Galois extensions $K_r$ of $\mathbf{Q}$ which are $p$-extensions of $L$ and such that $\mathrm{Gal}(K_r/\mathbf{Q})$ is isomorphic to either $H_r$ or to $H_r'$. Examples of both possibilities abound. If we take $A$ to be

in 38B in [Cre], then it turns out that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$, but if we take $A$ to be 11A3, then we have $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r'$. This will also be discussed in [Gr09a].

**E.** *Allowing arbitrary ramification.* Suppose now that $\Sigma = \Sigma_0 \cup \{p, \infty\}$ is an arbitrary finite set of primes containing $p$ and $\infty$. We assume again that $K$ is a finite Galois extension of $\mathbf{Q}$ and that $L \subseteq K \subset M_\Sigma$. There may be primes $l \in \Sigma_0$ such that $\mathcal{H}_l(K_\infty, E) \neq 0$. If so, then we will have $\lambda_E^{\Sigma_0}(\sigma) > \lambda_E(\sigma)$ for some irreducible Artin representations $\sigma$ of $\mathrm{Gal}(M_\Sigma/\mathbf{Q})$. The difference $\lambda_E^{\Sigma_0}(\sigma) - \lambda_E(\sigma)$ involves the quantities $\delta_{E,l}(\sigma)$, where $l$ varies over $\Sigma_0$. We will use the notation from the beginning of section 8.2, where we are now taking $F = \mathbf{Q}$ and $v = l$. Let $w_l$ denote the order of the character $\omega_l$ of $G_{\mathbf{Q}_l}$. Thus, $w_l$ is the order of $l$ modulo $p$. We will usually regard $\omega_l$ as a character of $\mathcal{G}_l = G_{\mathbf{Q}_{\infty,l}}$. Let $\mathcal{M}_l \subseteq \mathcal{G}_l$ denote its kernel, a normal subgroup of $\mathcal{G}_l$ of index $w_l$.

We assume that $l \neq p$. Let $I_l$ denote the inertia subgroup of $\mathrm{Gal}(M_\Sigma/\mathbf{Q})$ for some fixed prime of $M_\Sigma$ lying above $l$. Its choice will not be important. Then $I_l \subset \mathrm{Gal}(M_\Sigma/L_\infty)$ and $I_l \cong \mathbf{Z}_p$ as a group. We will assume as before that $p \geq 5$. According to the discussion in chapter 5, if $\chi$ is an irreducible representation of $\mathcal{G}_l$ such that $\langle \rho_{E,l}, \chi \rangle \geq 1$, then $\chi$ must be of degree 1, unramified, and of order prime to $p$. The decomposition subgroup of $\mathrm{Gal}(M_\Sigma/\mathbf{Q})$ (for the fixed prime above $l$) can be identified with a certain quotient group of $\mathcal{G}_l$, namely $\mathcal{G}_l/\mathcal{J}_l$, where $\mathcal{J}_l$ is characterized as follows: $\mathcal{J}_l$ is the smallest closed normal subgroup of $\mathcal{M}_l$ such that $\mathcal{M}_l/\mathcal{J}_l$ is a pro-$p$ group. In fact, by local class field theory, one sees that $\mathcal{M}_l/\mathcal{J}_l \cong \mathbf{Z}_p$ and can be identified with $I_l$. With this notation, the fixed field of $\mathcal{M}_l$ is $\mathbf{Q}_{\infty,l}(\mu_p)$ and the fixed field for $\mathcal{J}_l$ is the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}_{\infty,l}(\mu_p)$.

Suppose that $\sigma$ is an irreducible Artin representation of $\mathrm{Gal}(M_\Sigma/\mathbf{Q})$. Let $W_\sigma$ be the underlying $\mathcal{F}$-representation space for $\sigma$. We can regard $\sigma_l$ as a representation of $\mathcal{G}_l$. However, $\sigma_l$ factors through the quotient group $\mathcal{G}_l/\mathcal{J}_l$. Its irreducible constituents are of two types, either unramified or ramified, depending just on whether their restriction to $\mathcal{M}_l$ is trivial or nontrivial. The unramified constituents are precisely the irreducible constituents in $W_\sigma^{I_l}$. They are 1-dimensional. In fact, any such constituent must be a character of $\mathcal{G}_l$ which factors through $\mathcal{G}_l/\mathcal{M}_l$ and so must be a power of $\omega_l$.

The definition of $\delta_E^{\Sigma_0}(\sigma)$ involves the quantities $\delta_{E,l}(\sigma)$ which, in turn, involve terms of the form $\langle \sigma_l, \chi \rangle \langle \rho_{E,l}, \chi \rangle$. The above remarks show that we need only consider terms where $\chi = \omega_l^j$ for some $j$. Thus, we have

$$\delta_E^{\Sigma_0}(\sigma) \;=\; \sum_{l \in \Sigma_0} g_l \delta_{E,l}(\sigma)\ , \qquad \textit{where} \quad \delta_{E,l}(\sigma) \;=\; \sum_{j=0}^{w_l - 1} \langle \sigma_l, \omega_l^j \rangle \langle \rho_{E,l}, \omega_l^j \rangle \quad .$$

The factor $g_l$ is a power of $p$, the highest power dividing the Fermat quotient $(l^{p-1}-1)/p$. The expression for $\delta_{E,l}(\sigma)$ sometimes takes a simpler form. If $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, then $n(\sigma) = dp^a$

for some $a \geq 0$, where $d$ is a divisor of $p-1$. We denote $d$ by $d(\sigma)$. With this notation, we have the following result.

**Proposition 8.3.8.** *Assume that $p \geq 5$ and that $gcd\left(\frac{p-1}{d(\sigma)}, w_l\right) = 1$. Then*

$$\delta_{E,l}(\sigma) \;=\; \frac{\dim_{\mathcal{F}}\left(W_\sigma^{I_l}\right)}{w_l} \cdot \alpha(E,l)$$

*where $\alpha(E,l) = 0$ if any of the conditions (a), (b), or (c) in proposition 8.3.6 is satisfied, $\alpha(E,l) = 1$ if either $E$ has split, multiplicative reduction at $l$ or if $E$ has nonsplit, multiplicative reduction at $l$ and $l$ has even order modulo $p$, and $\alpha(E,l) = 2$ if $E$ has good reduction at $l$ and the roots of the polynomial $x^2 - \widetilde{a}_l x + \widetilde{l}$ are powers of $\widetilde{l}$.*

*Proof.* As mentioned above, the constituents in the $\mathcal{G}_l$-representation space $W_\sigma^{I_l}$ are powers of $\omega_l$. We know that $\sigma \otimes \omega^j \cong \sigma$ if $\omega^j$ has order dividing $d = d(\sigma)$. This just means that $j$ is divisible by $(p-1)/d$. We have $\sigma_l \otimes \omega_l^j \cong \sigma_l$ for all such $j$. The stated assumption then implies that $\sigma_l \otimes \omega_l \cong \sigma_l$. Thus, all of the multiplicities $\langle \sigma_l, \omega_l^j \rangle$ are equal. Consequently, we have

$$\delta_{E,l}(\sigma) \;=\; \frac{\dim_{\mathcal{F}}\left(W_\sigma^{I_l}\right)}{w_l} \cdot \sum_{j=0}^{w_l\text{-}1} \langle \rho_{E,l}, \omega_l^j \rangle \quad .$$

However, the sum is precisely $\alpha(E,l)$. □

**Remark 8.3.9.** Since $l$ is tamely ramified in $M_\Sigma/\mathbf{Q}$, there is a simple relationship between the dimension of $W_\sigma^{I_l}$ and the power of $l$ dividing the Artin conductor $\mathfrak{c}_\sigma$ for $\sigma$:

$$\mathrm{ord}_l\left(\mathfrak{c}_\sigma\right) \;=\; n(\sigma) \;-\; \dim_{\mathcal{F}}\left(W_\sigma^{I_l}\right) \quad .$$

This is true by definition. Thus, $\delta_{E,l}(\sigma)$ is closely related to $\mathfrak{c}_\sigma$. We can pick a field $K$ containing $L$ such that $\sigma$ factors through $\mathrm{Gal}(K/\mathbf{Q})$. The image of $I_l$ in $\mathrm{Gal}(K/\mathbf{Q})$ is the inertia subgroup for some prime above $l$, a cyclic subgroup $I_l(K/\mathbf{Q})$ of $\mathrm{Gal}(K/L)$. Hence, $\dim_{\mathcal{F}}\left(W_\sigma^{I_l}\right)$ is just the multiplicity of $\mathbf{1}_{I_l(K/\mathbf{Q})}$ in $\sigma|_{I_l(K/\mathbf{Q})}$.

As an example, suppose that $\Delta = H_r$ for some $r \geq 1$, that $I_l(K/\mathbf{Q})$ is conjugate to $U_r$, and that $\sigma$ is an irreducible representation of $H_r$ of degree $(p-1)p^r$. Thus, $\sigma|_{U_r}$ is faithful, we have $\dim_{\mathcal{F}}\left(W_\sigma^{U_r}\right) = 0$, and therefore $\delta_{E,l}(\sigma) = 0$ in that case. In contrast, suppose that $\sigma$ is the irreducible constituent in $\sigma_{st}^{(r)}|_{H_r}$ of degree $(p-1)p^{r\text{-}1}$. (See proposition 7.4.4.) Then, as mentioned in the discussion before proposition 8.2.2, we have $\dim_{\mathcal{F}}\left(W_\sigma^{U_r}\right) = (p-1)p^{[(r\text{-}1)/2]}$ and hence $\delta_{E,l}(\sigma)$ will be positive if $\alpha(E,l) \neq 0$, and is unbounded as $r$ increases. Note that $I_l(K/\mathbf{Q})$ is determined only up to conjugacy as a subgroup of $H_r$. The simplest case is when

$I_l(K/\mathbf{Q})$ is conjugate to $U_r$. A necessary condition for this is that the image of $I_l(K/\mathbf{Q})$ under the map $H_r \to B_0$ is nontrivial. That condition is also easily seen to be sufficient. If it holds, then we can simply assume that we have the equality $I_l(K/\mathbf{Q}) = U_r$. $\Diamond$

*Conductor 11, $p = 7$ again.* We will discuss an example where $\Sigma_0$ is not quite $\mathcal{H}$-trivial for $E$ and $p = 7$. There is one elliptic curve $A$ of conductor $678 = 2 \cdot 3 \cdot 113$ such that $A(\mathbf{Q})[p] \neq 0$. Suppose that $r \geq 0$. The discussion following proposition 8.3.7 tells us that $\mathbf{Q}(A[p^{r+1}])$ contains a subfield $K_r$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r$. Fixing such an isomorphism, we identify the two groups. The irreducible representations $\sigma$ of $\mathrm{Gal}(K_r/\mathbf{Q})$ correspond to those of $H_r$. Proposition 7.4.4 describes those representations. We will determine $\lambda_E(\sigma)$ for all of them.

We can take $\Sigma_0 = \{2, 3, 113\}$ and $\Sigma = \{p, \infty\} \cup \Sigma_0$. The set $\Sigma_0$ is not $\mathcal{H}$-trivial for $E$ and $p$, although the subset $\{2,\ 3\}$ is. We have $\delta_{E,l}(\sigma) = 0$ for $l = 2$ and $l = 3$ and all $\sigma$ factoring through $\mathrm{Gal}(K_r/\mathbf{Q})$. Now $w_{113} = 1$ and so we can use proposition 8.3.8 to determine $\delta_{E,113}(\sigma)$. One finds that $\alpha(E, 113) = 2$. We will also need the fact that $ord_{113}(j_A) \not\equiv 0 \pmod 7$. This tells us that the image of the inertia group $I_{113}$ in $H_r$ is conjugate to $U_r$. We can assume that the prime above $l = 113$ (in $K_r$) is chosen so that this image is precisely $U_r$. These remarks together with the fact that $g_{113} = 1$ give us the formula

$$\lambda_E^{\Sigma_0}(\sigma) \ = \ \lambda_E(\sigma) \ + \ 2\mathrm{dim}_{\mathcal{F}}\big(W_\sigma^{U_r}\big) \tag{8.3.e}$$

for any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(H_r)$.

As stated before, we have $\lambda_E(\omega^3) = 1$, but $\lambda_E(\omega^i) = 0$ for $i \in \{0, 1, 2, 4, 5\}$. Since the $\omega^i$'s are unramified at $l = 113$, their kernels contain $U_r$. Thus, (8.3.e) implies that

$$\lambda_E^{\Sigma_0}(\omega^i) \ = \ \begin{cases} 2 & if\ i = 0, 1, 2, 4, or\ 5 \\ 3 & if\ i = 3 \end{cases} \tag{8.3.f}$$

and therefore that $\lambda_E^{\Sigma_0}(L_\infty) = 13$.

The proof of proposition 8.3.1 shows that $X_E^{\Sigma_0}(K_{r,\infty})$ is a projective $\mathbf{Z}_7[H_r]$-module. If $\sigma$ has degree divisible by $p - 1 = 6$, then $\sigma$ is $\Pi_r$-induced and we therefore have the following congruence relation for the non-primitive $\lambda$-invariant:

$$\lambda_E^{\Sigma_0}(\sigma) \ = \ \frac{n(\sigma)}{6} \cdot \sum_{i=0}^{5} \lambda_E^{\Sigma_0}(\omega^i) \ = \ \frac{n(\sigma)}{6} \cdot \lambda_E^{\Sigma_0}(L_\infty) \ = \ \frac{13}{6} n(\sigma) \quad .$$

Hence we find the following formula for the primitive $\lambda$-invariant:

$$\lambda_E(\sigma) \ = \ \frac{13}{6} n(\sigma) \ - \ 2\mathrm{dim}_{\mathcal{F}}\big(W_\sigma^{U_r}\big)$$

for any irreducible representation of $H_r$ of degree divisible by 6. Remark 8.3.9 includes some comments about the quantity $\dim_{\mathcal{F}}\big(W_\sigma^{U_r}\big)$. It is interesting to note that $\lambda_E(\sigma)$ is odd for all such $\sigma$. The significance of this will be pointed out in chapter 13.

Now consider a representation of the form $\rho_{H_r,\psi}$ of $H_r$. This has degree $7^r$. We have $\widetilde{\psi} = \widetilde{\omega}^i = \tau_i$ for a unique integer $i$ in the range $0 \le i \le 5$. We then have the formula

$$\lambda_E\big(\rho_{H_r,\psi}\big) \;=\; 13 \cdot \frac{7^r - 1}{6} \;+\; \begin{cases} 0 & if\ \widetilde{\psi} \in \{\tau_0, \tau_1, \tau_2, \tau_4, \tau_5\} \\ 1 & if\ \widetilde{\psi} = \tau_3 \end{cases}$$

To see this, one applies the congruence relation (7.4.f) to $X = X_E^{\Sigma_o}(K_{r,\infty})$. One then uses (8.3.e) for $\sigma = \rho_{H_r,\psi}$. Note that $\mathbf{1}_{U_r}$ occurs as a constituent in $\rho_{H_r,\psi}|_{U_r}$ with multiplicity 1, a consequence of the fact that $\rho_{H_r,\psi}|_{B_r}$ has only one irreducible constituent of degree 1. For the final term, one uses (8.3.f).

*Conductor 11, $p = 5$ again.* As before, we let $E$ be the curve 11A3. However, we will now take $A = E$. It turns out that $\mathbf{Q}(E[p^\infty])$ contains a tower of subfields $K_r$ such that $\mathrm{Gal}(K_r/\mathbf{Q}) \cong H_r'$ for all $r \ge 1$. We mentioned this before and will discuss this further in [Gr09a]. However, it is also a consequence of a result in [Fis]. We clearly have $L \subset K_r \subset M_\Sigma$, where $\Sigma = \{\infty, 5, 11\}$. We take $\Sigma_0 = \{11\}$.

As mentioned before, we have $X_E(L_\infty) = 0$. Thus, $\lambda_E(\omega^i) = \mu_E(\omega^i) = 0$ for $0 \le i \le 3$. Now $w_{11} = 1$ and $g_{11} = 1$. Also, identifying $\mathrm{Gal}(K_r/\mathbf{Q})$ with $H_r'$, we can assume that the image of the inertia group $I_{11}$ in $\mathrm{Gal}(K_r/\mathbf{Q})$ is precisely $U_r$. This is because $5 \nmid \mathrm{ord}_{11}(j_A)$. As a consequence of these facts, we have

$$\delta_E^{\Sigma_0}(\sigma) \;=\; \dim\big(W_\sigma^{U_r}\big)$$

for all irreducible representations of $\mathrm{Gal}(K_r/\mathbf{Q})$. In particular, for the 1-dimensional representations $\omega^i$, where $0 \le i \le 3$, we have $\lambda_E^{\Sigma_0}(\omega^i) = \delta_E^{\Sigma_0}(\omega^i) = 1$. Thus, $\lambda_E^{\Sigma_0}(L_\infty) = 4$.

If $\sigma$ is a faithful, irreducible representation of $H_r'$, then $\sigma$ is $\Pi_r'$-induced and $W_\sigma^{U_r} = 0$. It follows that

$$\lambda_E(\sigma) \;=\; \lambda_E^{\Sigma_0}(\sigma) \;=\; \frac{n(\sigma)}{4} \cdot \lambda_E^{\Sigma_0}(L_\infty) \;=\; n(\sigma)$$

for all the faithful $\sigma$'s. More generally, this formula is valid whenever $\sigma|_{B_r}$ has no irreducible constituents of degree 1. The irreducible representations of the form $\sigma = \xi_{H_r',\psi}$ have the property that $\sigma|_{B_r}$ has exactly one irreducible constituent of degree 1, the character $\psi$. Thus, we have the formula

$$\lambda_E(\xi_{H_r',\psi}) \;=\; \lambda_E^{\Sigma_0}(\xi_{H_r',\psi}) - 1 \;=\; \frac{5^{r\text{-}1} - 1}{4} \cdot \lambda_E^{\Sigma_0}(L_\infty) - 1 \;=\; 5^{r\text{-}1} - 2$$

since $\xi_{H_r',\psi}$ has degree $5^{r\text{-}1}$.

## 8.4 False Tate extensions of Q.

Now we consider a class of examples where the Galois groups are isomorphic to the $B_r$'s discussed in part **D1** of section 7.4. Thus, we will continue to be in the situation of section 8.3. Fix an integer $m$. For simplicity, we will assume that $p \nmid ord_q(m)$ for all primes $q$ which divide $m$. If $r \geq 0$, we will let

$$K_r \;=\; \mathbf{Q}\big(\mu_{p^{r+1}},\; \sqrt[p^{r+1}]{m}\;\big) \quad , \tag{8.4.a}$$

a Galois extension of $\mathbf{Q}$ with $\mathrm{Gal}(K_r/\mathbf{Q}) \cong B_r$. We will identify the two groups to simplify the discussion and we will use the notation from section 7.4, part **D1**. Letting $\mathbf{Q}_r$ denote the $r$-th layer in the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$, we then have

$$K_r^{U_r} \;=\; \mathbf{Q}(\mu_{p^{r+1}}) \;=\; \mathbf{Q}_r(\mu_p), \qquad K_r^{P_r} = \mathbf{Q}(\mu_p) = L \quad .$$

Thus, we can identify $\mathrm{Gal}\big(K_r/\mathbf{Q}_r(\mu_p)\big)$ with $U_r$ and $\mathrm{Gal}\big(\mathbf{Q}_r(\mu_p)/\mathbf{Q}\big)$ with the quotient group $B_r/U_r$. Our assumption about $m$ implies that if $q$ is a prime dividing $m$, and $q \neq p$, then the inertia subgroup $I_q(K_r/\mathbf{Q})$ of $\mathrm{Gal}(K_r/\mathbf{Q})$ for a prime lying above $q$ is precisely $U_r$.

Now let $E$ be an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at $p$. Assume that $\mathrm{Sel}_E(L_\infty)[p]$ is finite and that $p \geq 5$. We take $\Sigma_0 = \{l \;\big|\; l|m,\; l \neq p\}$. Then $X_E^{\Sigma_0}(K_{r,\infty}/\mathbf{Q}_\infty)$ is quasi-projective as a $\mathbf{Z}_p[B_r]$-module. Note that $K_r \cap \mathbf{Q}_\infty = \mathbf{Q}_r$ and so, if $r \geq 1$, then we are in the situation discussed in section 3.5. As explained there, if $\rho$ is an irreducible representation of $B_r$, then we can still define $\lambda_E(\rho)$ and $\lambda_E^{\Sigma_0}(\rho)$ even though $B_r = \mathrm{Gal}(K_r/\mathbf{Q})$ doesn't actually act on $X_E(K_{r,\infty})$ and $X_E^{\Sigma_0}(K_{r,\infty})$.

Note that $B_r$ is a $\Pi\Omega$-group, with $\Pi = P_r$. We have described the irreducible representations of $B_r$ in section 7.4, part **D1**. The unique faithful irreducible representation is $\gamma_r$ and has degree $(p-1)p^r$. The others have smaller degree and those degrees are also divisible by $p-1$, except for the 1-dimensional representations, all of which factor through $\mathrm{Gal}(\mathbf{Q}_r(\mu_p)/\mathbf{Q})$. It follows that all of the irreducible representations of $B_r$ of degree $> 1$ are $P_r$-induced. We obtain

$$\lambda_E^{\Sigma_0}(\rho) \;=\; \frac{n(\rho)}{p-1}\Big(\sum_{i=0}^{p-2} \lambda_E^{\Sigma_0}(\omega^i)\Big) \;=\; \frac{n(\rho)}{p-1} \cdot \lambda_E^{\Sigma_0}(L_\infty)$$

by applying (7.4.c) together with the remark following proposition 8.3.1 to all those $\rho$'s.

To determine $\lambda_E^{\Sigma_0}(\rho) - \lambda_E(\rho)$, we apply proposition 8.3.8. Assume that $p \geq 5$. That proposition doesn't apply to the powers of $\omega$ unless $l \equiv 1 \pmod p$. However, the argument does apply without change to the direct sum of the $\omega^i$'s and gives us the formula

$$\sum_{i=0}^{p\text{-}1} \delta_{E,l}(\omega^i) \;=\; \frac{p-1}{w_l} \cdot \alpha(E,l) \quad .$$

Furthermore, if $\rho$ is any irreducible representation of $B_r$ which is not 1-dimensional, then we have $\langle \rho|_{U_r}, \mathbf{1}_{U_r} \rangle = 0$. It follows that $\delta_E^{\Sigma_0}(\rho) = 0$ and therefore that $\lambda_E(\rho) = \lambda_E^{\Sigma_0}(\rho)$. Combining these remarks, and assuming that $p \geq 5$, we obtain the formula

$$\lambda_E(\rho) \;=\; \frac{n(\rho)}{p-1} \cdot \lambda_E(L_\infty) \;+\; n(\rho) \cdot \sum_{l \in \Sigma_0} g_l \cdot \frac{\alpha(E,l)}{w_l} \tag{8.4.b}$$

for any irreducible representation $\rho$ of $\mathrm{Gal}(K_r/\mathbf{Q})$ which is not 1-dimensional.

It is interesting that the above formula takes the very simple form $\lambda_E(\rho) = c \cdot n(\rho)$, where $c$ is a certain rational constant depending on $E$, $p$, and $m$. The denominator of $c$ divides $p-1$. If we view this example from the point of view of section 3.5, the behavior becomes even simpler. The group $B_r$ plays the role of $D$ and $\Delta_r$ plays the role of $\Delta$. The restriction map identifies $\Delta_r$ with the unique subgroup of $B_r$ containing $U_r$ and such that $\Delta_r/U_r$ has order $p-1$. Note that $\Delta_r$ is isomorphic to the semidirect product $\left(\Gamma_1/\Gamma_1^{p^{r+1}}\right) \rtimes \Omega$. Here we are using the notation from the beginning of section 7.4, part **D**, and so $\Gamma_1$ is isomorphic to $\mathbf{Z}_p$ as a group and $\Omega$ acts by the character $\omega$. Apart from the $p-1$ representations of $\Delta_r$ of degree 1, all the other irreducible representations $\sigma$ of $\Delta_r$ have degree $p-1$. Furthermore, every such $\sigma$ is a constituent in $\rho|_{\Delta_r}$ for some irreducible representation $\rho$ of $B_r$ with $n(\rho) \neq 1$. The definition of $\lambda_E(\rho)$ in section 3.5 implies that

$$\frac{\lambda_E(\rho)}{\lambda_E(\sigma)} \;=\; \frac{n(\rho)}{n(\sigma)}$$

and therefore we have the formula $\lambda_E(\sigma) = c \cdot \lambda_E(\sigma) = c(p-1)$ for any irreducible representation $\sigma$ of $\Delta_r$ which is not 1-dimensional.

The union $\mathcal{K}_m = \bigcup_r K_r$ is called a "false Tate extension" in [CFKS]. It is a Galois extension of $\mathbf{Q}$ and $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q})$ is isomorphic to $B_\infty$, a two-dimensional $p$-adic Lie group which is defined in remark 7.4.6. The Artin representations $\rho$ which factor through $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q})$ correspond to the irreducible representations of the $B_r$'s for $r \geq 0$. They are described completely in part **D1** of section 7.4. Ignoring the 1-dimensional representations, which factor through $\mathrm{Gal}\big(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}\big)$, we have $n(\rho) = (p-1)p^t$ for all the others, where $t \geq 0$. Of course, $t$ varies over all the nonnegative integers. However, the restriction of $\rho$ to $G_{\mathbf{Q}_\infty}$ breaks up as a direct sum of $p^t$ irreducible representations, all of degree $p-1$. As mentioned above, the invariant $\lambda_E(\sigma)$ is actually constant as $\sigma$ varies over all such irreducible representations of $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q}_\infty)$.

There is an interpretation of that constant $c(p-1)$. It coincides with an invariant defined in chapter 4 of [CFKS] whose definition we will now recall. Consider the Selmer group $\mathrm{Sel}_E(\mathcal{K}_m)_p$, which one can regard as a discrete module over the completed $\mathbf{Z}_p$-group

algebra $\mathbf{Z}_p[[B_\infty]]$. Here we will fix an identification of $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q})$ with $B_\infty$ to simplify the discussion. The subgroup $U_\infty$ of $B_\infty$ is then identified with $\mathrm{Gal}(\mathcal{K}_m/L_\infty)$ and so we can also regard $\mathrm{Sel}_E(\mathcal{K}_m)_p$ as a module over the ring $\mathbf{Z}_p[[U_\infty]]$. Since $U_\infty \cong \mathbf{Z}_p$, that ring is isomorphic to a formal power series ring over $\mathbf{Z}_p$ in one variable. The assumption that $\mathrm{Sel}_E(L_\infty)[p]$ is finite implies that the Pontryagin dual $X_E(\mathcal{K}_m)$ of $\mathrm{Sel}_E(\mathcal{K}_m)_p$ is a finitely-generated module over $\mathbf{Z}_p[[U_\infty]]$. Its rank is denoted by $\tau$ in [CFKS]. We will denote it by $\tau(E,m)$.

One then has $\lambda_E(\sigma) = \tau(E,m)$ for all the irreducible representations $\sigma$ of $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q}_\infty)$ of degree $> 1$. Since this is proved in [CFKS], we will simply mention the various ingredients used in verifying this fact.

(**1**) The Sylow pro-$p$ subgroup of $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q}_\infty)$ is the normal subgroup $U_\infty$. Its index is $p-1$. Each irreducible constituent in $\sigma|_{U_\infty}$ is 1-dimensional, nontrivial, and occurs with multiplicity 1. If $u$ is one of them, then $\lambda_E(\sigma) = \lambda_E(u)$. This follows from Frobenius Reciprocity.

(**2**) There is a control theorem for the behavior of the Selmer groups for $E$ in the $\mathbf{Z}_p$-extension $\mathcal{K}_m/L_\infty$, almost like the case of a $\mathbf{Z}_p$-extension of a number field. However, one finds that the cokernel of the restriction map can be infinite, but that $U_\infty$ acts trivially on that cokernel. Thus, if $u$ is a nontrivial character of $U_\infty$, then $\lambda_E(u)$ is equal to the multiplicity of $u$ in the $\mathbf{Q}_p$-representation space

$$X_E(\mathcal{K}_m)_{U_\infty^{p^t}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \quad , \tag{8.4.c}$$

where $p^t$ is the order of the character $u$.

(**3**) Our assumptions about $E$ imply that $X_E(\mathcal{K}_m)$ is a torsion-free $\mathbf{Z}_p[[U_\infty]]$-module. This is a consequence of the fact that $X_E(\mathcal{K}_m)$ has no nonzero, pseudo-null $\mathbf{Z}_p[[B_\infty]]$-submodules. (See theorem 3.1 in [HaVe].) Hence the multiplicity of $u$ in (8.4.c) is indeed equal to the rank $\tau(E,m)$.

As a consequence, we get a nice formula for $\tau(E,m)$. This formula can also be found in [CFKS] (where it is mentioned in the proof of proposition 4.1.8) as well as in theorem 3.1 in [HaVe]. The above remarks and the formula for $\lambda_E(\rho)$ show that

$$\tau(E,m) \;=\; c(p-1) \;=\; \lambda_E(L_\infty) \;+\; \sum_l \; g_l \cdot \frac{p-1}{w_l} \cdot \alpha(E,l)$$

where $l$ runs over the primes dividing $m$, excluding $l = p$ if $p|m$. Note that the factor $g_l \frac{p-1}{w_l}$ is just the number of primes of $L_\infty = \mathbf{Q}(\mu_{p^\infty})$ lying over $l$. The derivation of this formula in [CFKS] proceeds from a quite different point of view. Also, it is proved there for more general base fields (and not just $\mathbf{Q}$) and under the following more general assumption. We state it using the above notation. The subscript *div* indicates the maximal divisible subgroup.

**Assumption A:** $\left(\mathrm{Sel}_E(\mathcal{K}_m)_p\right)_{div}$ *is cofinitely-generated as a* $\mathbf{Z}_p[[U_\infty]]$*-module.*

Our assumption that $\mathrm{Sel}_E(L_\infty)[p]$ is finite implies that $\mathrm{Sel}_E(\mathcal{K}_m)_p$ itself is a cofinitely-generated $\mathbf{Z}_p[[U_\infty]]$-module. Furthermore, if $E$ is $\mathbf{Q}$-isogenous to an elliptic curve $E'$ for which $\mathrm{Sel}_{E'}(L_\infty)[p]$ is finite, then assumption **A** is also easily seen to hold. However, the converse is not known to be true. Our argument would also work in that more general context, but only with our assumption about the vanishing of the $\mu$-invariant for $E$ over $L_\infty$.

Note that $\tau(E,m)$ depends only on the set of primes $q$ which divide $m$, and not on $ord_q(m)$. The parity of $\tau(E,m)$ determines the parity of all the $\lambda_E(\rho)$'s, where $\rho$ is any irreducible Artin representation of $\mathrm{Gal}(\mathcal{K}_m/\mathbf{Q})$ of degree divisible by $p-1$. This follows from the formula

$$\lambda_E(\rho) \;=\; \frac{n(\rho)}{p-1}\cdot\tau(E,m) \quad ,$$

which holds for all such $\rho$'s, together with the fact that $\frac{n(\rho)}{p-1}$ is a power of the odd prime $p$.

As a specific example, suppose that $E$ is one of the elliptic curves of conductor 11 and that $p=7$. We know that $\mathrm{Sel}_E(L_\infty)[p]$ is finite and that $\lambda_E(L_\infty)=1$. The fact that $w_{11}=3$ implies that $\tau(E,m)$ is odd for all $m$. We have previously listed 20 values of $l$ for which $\alpha(E,l)=0$, starting with $l=2$, 3, 13, 23, and 29, which we refer to as $\mathcal{H}$-trivial primes for $E$ and $p$. If $m$ is any product of such primes, then $\tau(E,m)=1$. 0therwise, $\tau(E,m)\geq 3$. One has $\tau(E,m)=3$ for $m=11$ and also for $m=q$, where $q$ is any prime where $\alpha(E,q)=2$, $w_q=6$, and $g_q=1$. For example, $\tau(E,5)=3$. The next prime for which $\alpha(E,q)=2$ is $q=19$. One has $w_{19}=6$, but $g_{19}=49$, and so $\tau(E,19)=99$. Thus, $\lambda_E(\rho)=99\cdot\frac{n(\rho)}{p-1}$ for any irreducible Artin representation $\rho$ of $\mathrm{Gal}(\mathcal{K}_{19}/\mathbf{Q})$ of degree $>1$. The reason this is so large is that there are 49 primes of $L_\infty$ lying above 19.

# 9 Self-dual representations.

For any representation $\rho$ of $\Delta$ over $\mathcal{F}$, we let $\check{\rho}$ denote the contragredient representation. If $W_\rho$ denotes the underlying representation space for $\rho$, then $W_{\check{\rho}}=\mathrm{Hom}(W_\rho,\mathcal{F})$ is the underlying representation space for $\check{\rho}$, where the action of $\Delta$ on $W_{\check{\rho}}$ is defined in the usual way. We say that $\rho$ is self-dual if $\rho$ and $\check{\rho}$ are isomorphic representations. Thus, there would then be a non-degenerate, $\Delta$-invariant pairing $B: W_\rho\times W_\rho\longrightarrow\mathcal{F}$. If $\rho$ is also absolutely irreducible, then one easily sees that this pairing $B$ is unique up to a factor in $\mathcal{F}^\times$. As a consequence, if one composes $B$ with the map $(a,b)\rightarrow(b,a)$ of $W_\rho\times W_\rho$ to itself, then one obtains another non-degenerate, $\Delta$-invariant pairing $B'$ and one must have $B'=\varepsilon B$, where

$\varepsilon \in \{\pm 1\}$. If $\varepsilon = +1$, then $B$ is symmetric and one then says that $\rho$ is *"orthogonal"*. If $\varepsilon = -1$, then $B$ is skew-symmetric and one then says that $\rho$ is *"symplectic"*.

## 9.1 Various classes of groups.

Certain groups $\Delta$ have the property that all elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are self-dual, and even orthogonal. The dihedral groups and the symmetric groups have both properties. We will see other examples of such groups below. If all elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are self-dual, then we will say that $\Delta$ has property **(SD)**. A simple characterization is:

**(SD)** *Every element of $\Delta$ is conjugate to its inverse.*

This condition is easily verified for the dihedral and symmetric groups. A group satisfying **(SD)** is sometimes said to be *ambivalent*. An abelian group $\Delta$ is ambivalent if and only if $\Delta$ is an elementary abelian 2-group. The alternating group $A_n$ is ambivalent if and only if $n = 1, 2, 5, 6, 10$ or 14. (See 1.2.12 in [J-K].)

We will say that $\Delta$ has property **(SDO)** if all elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ are self-dual *and* orthogonal. An equivalent characterization is the following counting property:

$$\textbf{(SDO)} \qquad \sum_{\sigma} n(\sigma) \;=\; \left|\{\ \delta \in \Delta \;\middle|\; \delta^2 = id_\Delta\ \}\right| \ ,$$

where $\sigma$ runs over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $id_\Delta$ denotes the identity element of $\Delta$. This characterization is an immediate consequence of a theorem of Frobenius and Schur. That result and its proof can be found in proposition 3.7 in [Fei]. We will adopt the notation in [Ro07] to state it. Let

$$\vartheta(\Delta) \;=\; \sum_{\sigma}^{(sd)} n(\sigma) \;=\; \vartheta_{orth}(\Delta) \;+\; \vartheta_{symp}(\Delta) \quad ,$$

where $\sigma$ varies over $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ in the sum, which we then break up into the separate sums over the orthogonal and symplectic elements of $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$. Proposition 3.7 in [Fei]

$$\vartheta_{orth}(\Delta) \;-\; \vartheta_{symp}(\Delta) \;=\; \left|\{\ \delta \in \Delta \;\middle|\; \delta^2 = id_\Delta\ \}\right| \quad .$$

We refer to this equation as the Frobenius-Schur identity.

If $U_\alpha$ is the underlying vector space for a representation $\alpha$ of $\Delta$ over $\mathfrak{f}$, then the dual (or contragredient) representation $\check{\alpha}$ gives the action of $\Delta$ on $U_{\check{\alpha}} = \mathrm{Hom}(U_\alpha, \mathfrak{f})$. A necessary and sufficient condition to have $\check{\tau} \cong \tau$ for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$ is the following variation on **(SD)**:

($\mathbf{SD}_p$) *Every element of $\Delta$ of order prime to $p$ is conjugate to its inverse.*

For example, if $\Delta$ is a $p$-group, then $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ consists just of the self-dual representation $\tau_0$ and ($\mathbf{SD}_p$) is obviously satisfied, but **(SD)** is not satisfied if $p$ is odd (unless $|\Delta| = 1$). It is sometimes satisfied if $p = 2$. Obviously, for any $p$, **(SD)** implies ($\mathbf{SD}_p$) .

**Proposition 9.1.1.** *For any odd prime $p$ and for any $r \geq 0$, the group $\Delta_r = PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ satisfies property* **(SDO)**.

*Proof.* For $\Delta_0 = PGL_2(\mathbf{F}_p)$, the elements of order 2 fall into two conjugacy classes, one of cardinality $\frac{1}{2}p(p+1)$, represented by a diagonal matrix with eigenvalues 1 and -1, the other of cardinality $\frac{1}{2}p(p-1)$, represented by a matrix whose eigenvalues are $\alpha, -\alpha$, where $\alpha^2 \in \mathbf{F}_p^\times$, but $\alpha \notin \mathbf{F}_p^\times$. Thus, $\{\ \delta \in \Delta \ \big|\ \delta^2 = id_\Delta\ \}$ has cardinality $p^2+1$. On the other hand, the results summarized in part **A** of section 7.2 show that $\sum_\sigma n(\sigma)$ is also $p^2+1$.

Now assume that $r \geq 1$. We first sum over the primitive $\sigma$'s, obtaining

$$|\mathcal{A}_r|a_r + |\mathcal{B}_r|b_r + |\mathcal{C}_r|c_r \ = \ p^{2(r+1)} - p^{2r}$$

Hence $\sum_\sigma n(\sigma) = p^{2(r+1)} + 1$. If $\delta \in \Delta$ has order 2, let $\delta_0$ denote its image in $\Delta_0$. Now $\delta_0$ generates a subgroup of $\Delta_0$ of order 2 and the inverse image of that subgroup under the map $\Delta \longrightarrow \Delta_0$ is a subgroup of $\Delta$ of order $2p^{3r}$. Call this subgroup $H_{\delta_0}$. It contains a subgroup of index 2, namely $\ker(\Delta_r \to \Delta_0)$, which consists of elements represented by matrices of the form $I + pA$, where $A \in M_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. All elements of order 2 in $H_{\delta_0}$ (including $\delta$ itself) map to $\delta_0$ and are conjugate in that group. The cardinality of that conjugacy class is the index $[H_{\delta_0} : Z_\delta]$, where $Z_\delta$ is the centralizer of $\delta$ in $H_{\delta_0}$. The order of $Z_\delta$ can be determined by a matrix argument and turns out to be $2p^r$. Thus, the conjugacy class of $\delta$ has cardinality $p^{2r}$. There are $p^2$ choices for $\delta_0$ and so, altogether, the cardinality of $\{\ \delta \in \Delta \ \big|\ \delta^2 = id_\Delta\ \}$ is $p^{2(r+1)} + 1$. This verifies property (**SDO**).

The matrix argument alluded to above reduces to determining the cardinality of

$$\{A \in M_2(\mathbf{Z}/p^{r+1}\mathbf{Z}) \ \big|\ DAD^{-1} = A\ \} \quad .$$

Here $D$ is a matrix representing $\delta$ and so its square is a scalar matrix. Thus, $D$ defines an involution on $M_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ by conjugation. The $(\pm 1)$-eigenspaces are direct summands and both are isomorphic to $(\mathbf{Z}/p^{r+1}\mathbf{Z})^2$. One checks this separately for both types of elements $\delta_0$ of order 2 in $\Delta_0$. Noting that the Sylow $p$-subgroup of $Z_\delta$ (which has index 2 in $Z_\delta$ ) is precisely the image of the group of matrices of the form $I + pA$, where $A$ is in the $(+1)$-eigenspace, and that the subgroup consisting of scalar matrices has order $p^r$, the statement about the order of $Z_\delta$ follows easily. $\square$

The fact that $\Delta_r$ satisfies property **(SD)** could also be verified directly by a straightforward matrix argument.

As we've already mentioned, the dihedral groups, symmetric groups, and elementary abelian 2-groups also satisfy **(SDO)**. An example of a group which satisfies **(SD)**, but not **(SDO)** is the quaternionic group of order 8. Its single 2-dimensional irreducible representation is symplectic. Of course, groups which do not satisfy **(SD)** are very common.

If $\Delta$ has odd order, then a theorem of Burnside states that $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ consists only of the trivial representation $\sigma_0$. Groups of odd order are simple examples of groups with the following property: *Every self-dual irreducible representation of $\Delta$ is orthogonal.* We will refer to this as property **(O)**. It can also be characterized by a counting property:

$$\textbf{(O)} \qquad \vartheta(\Delta) \;=\; \left|\{\; \delta \in \Delta \;\middle|\; \delta^2 = id_\Delta \;\}\right| \,.$$

The equivalence follows immediately from the Frobenius-Schur identity. In addition to groups of odd order, finite abelian groups satisfy property **(O)**. Another family of examples is $GL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$ and $p$ odd. Most of the self-dual representations of that group factor through $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$, and so are orthogonal by proposition 9.1.1. For any others, the restriction to the center must be the character of order 2. Such self-dual representations exist, exactly one which is primitive for each $r$. These are described by Rohrlich in [Ro06]. They are all realizable over $\mathbf{Q}$ and so are certainly orthogonal. (We recall that any finite subgroup of $GL_n(\mathbf{R})$ is conjugate to a subgroup of the orthogonal group $O_n(\mathbf{R})$. Hence any representation of a finite group which is realizable over $\mathbf{R}$ must be an orthogonal, self-dual representation.)

## 9.2 $\Pi\Omega$ groups.

Certain subgroups of $GL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ satisfy property **O**. This question is studied in some detail in [Ro07] for subgroups whose image in $\Delta_0$ is contained in $B_0$. Assume that $G$ is an open subgroup of $GL_2(\mathbf{Z}_p)$ and let $G_r$ denote its image in $GL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$. Assume that the elements of $G_0$ are upper triangular and that $G_0$ contains a matrix whose eigenvalues are $+1$ and $-1$. Proposition 9 in [Ro07] implies that $G_r$ satisfies property **(O)**. Rohrlich also obtains asymptotic information on the behavior of $\vartheta(G_r)$ as $r$ varies. This implies that the number of $r$-primitive representations of $G_r$ is bounded above and below by positive constant multiples of $p^r$. These same results apply to the image of $G_r$ in $\Delta_r$. This image will be a subgroup of $H_r$ by definition. As an example, the groups $H_r$ and $B_r$ (defined in section 7.4, part **D**) satisfy property **(O)**.

We can verify these facts for $H_r$ by using proposition 7.4.4, which gives specific families of orthogonal irreducible representations. All of the irreducible representations of $H_r$, except for those whose degree is a power of $p$, are self-dual. To see this, it is enough to consider just the $r$-primitive representations. We know that each such $\rho$ occurs as a constituent in $\sigma|_{H_r}$ for some $r$-primitive irreducible representation $\sigma$ of $\Delta_r$ and, if we assume that $n(\rho)$ is not a power of $p$, then $\rho$ is the only constituent of its dimension. Since $\sigma$ is self-dual, so is $\sigma|_{H_r}$. It follows that $\rho$ must be self-dual too. Furthermore, $\rho$ must be orthogonal. To see this, note that since $\sigma$ is orthogonal, so is $\sigma|_{H_r}$. Remark 9.3.2 below then implies that $\rho$ must be orthogonal. Therefore, $H_r$ indeed satisfies property **(O)**. The number of self-dual, $r$-primitive, irreducible representations of $H_r$ is $2p^r$ according to proposition 7.4.4.

For the group $H'_r$, one can at least say something about the faithful, irreducible representations $\rho$ whose degree is $b_r = (p-1)p^r$. Those representations also must be self-dual and orthogonal. The reason is that each such $\rho$ occurs with multiplicity 1 in $\sigma|_{H'_r}$ for some irreducible representation $\sigma$ of $\Delta_r$ and is the unique irreducible constituent of degree $b_r$. Remark 7.4.5 points out that the number of such representations of $H'_r$ is bounded above and below by positive constant multiples of $p^r$.

The situation is much simpler for the group $B_r$. Referring to the discussion in **D1** of section 7.4, there is a unique faithful, irreducible representation $\gamma_r$. Obviously, $\gamma_r$ is self-dual. If $0 \leq s < r$, then we also get a self-dual representation of $B_r$ by regarding $\gamma_s$ as a representation of $B_r$ via the homomorphism $B_r \to B_s$. All the other irreducible representations of $B_r$ are of the form $\gamma_s \otimes \psi$, where $\psi$ is a character of $B_r$ which has a nontrivial restriction to the subgroup $\ker(B_r \to B_s)$. That restriction has $p$-power order. The contragredient of $\gamma_s \otimes \psi$ is $\gamma_s \otimes \psi^{-1}$. The two representations are not isomorphic. This is so because $p$ is odd and hence the restrictions of $\psi$ and $\psi^{-1}$ to $\ker(B_r \to B_s)$ will be different. Therefore, the irreducible, self-dual representations of $B_r$ are just the representations $\gamma_s$ where $0 \leq s \leq r$. The fact that those are all orthogonal follows by a simple application of the Frobenius-Schur identity, or from the fact that $\gamma_s$ is the restriction to $B_s$ (or $B_r$) of a representation $\sigma \in \mathcal{B}_s$.

The groups $H_r$, $H'_r$, and $B_r$ have the property that all of their self-dual irreducible representations, excluding the two of dimension 1, have degree divisible by $p-1$. This statement (for the first two groups, at least) is actually a special case of a general theorem proved in [CFKS]. Consider an open subgroup $G$ of $PGL_2(\mathbf{Z}_p)$ whose image in $\Delta_0$ is contained in $B_0$. Then $G$ has a normal pro-$p$ subgroup $P$ such that $G/P$ is isomorphic to a subgroup of $(\mathbf{Z}/p\mathbf{Z})^\times$. Consider an irreducible representation $\xi$ which factors through a finite quotient group of $G$. Proposition 6.8 in [CFKS] implies that if $\xi$ is self-dual and $n(\xi) > 1$, then $\xi$ is $P$-induced. This general theorem applies to the $H_r$'s and $H'_r$'s by taking $G$ to be $H_\infty$ or $H'_\infty$. Such a result implies that $\widetilde{\xi}^{ss}$ is isomorphic to a multiple of the regular representation

of $G/P$ over $\mathfrak{f}$. The argument is the same as for the isomorphism (7.4.b). [CFKS] proves the same result in corollary 6.9 and exploits it in a way which seems quite parallel to the way it has been used in this paper.

The group $H_r$ has the unusual property that all of its irreducible representations of degree divisible by $p-1$ are self-dual. This is not true for $H'_r$ and $B_r$ if $r \geq 1$. We should also point out a direct reason why the irreducible representations $\xi_{H_r,\psi}$ of $H_r$ described in remark 7.4.3 are not self-dual. It is clear that the contragredient of $\xi_{H_r,\psi}$ is $\xi_{H_r,\psi^{-1}}$, which was shown not to be isomorphic to $\xi_{H_r,\psi}$.

**Remark 9.2.1.** If $p \equiv 3 \pmod 4$, then any $\Pi\Omega$-group $\Delta$ will satisfy property **(O)**. This follows from the lemma after proposition 3 in [Ro07], a very special case of which asserts that if $\Delta$ is a finite group which contains a normal subgroup of odd order and index 2, then $\Delta$ satisfies property **(O)**. We can give another argument based on modular representation theory if $\Delta$ is a $\Pi\Omega$-group. Of course, $\Pi$ is a normal subgroup of $\Delta$ and we will regard $\Omega$ as a subgroup of $\Delta$. Let $\Omega'$ be the subgroup of $\Omega$ of order 2 and let $\Delta' = \Pi\Omega'$, which contains $\Pi$ as a subgroup of index 2. We let $\eta_0$ and $\eta_1$ denote the two characters of $\Delta'/\Pi$.

We will first show that $\Delta'$ satisfies property **(O)**. This is true for any odd prime $p$. Suppose that $\rho$ is a self-dual irreducible representation of $\Delta'$ over $\mathcal{F}$. Assume that $\rho$ doesn't factor through $\Delta'/\Pi$. Now $\Pi$ has odd order and hence its only irreducible, self-dual representation is $\pi_0 = \mathbf{1}_\Pi$. Therefore, $\rho|_\Pi$ is reducible. We must have $\rho|_\Pi \cong \pi \oplus \check{\pi}$, where $\pi \in \mathrm{Irr}_{\mathcal{F}}(\Pi)$ and $\pi \neq \pi_0$. Thus, it follows that $\rho \cong \mathrm{Ind}_\Pi^{\Delta'}(\pi)$. Now $n(\pi) = p^a$ for some $a \geq 0$. We then have $\widetilde{\pi}^{ss} \cong \widetilde{\pi}_0^{p^a}$ as representations of $\Pi$ over $\mathfrak{f}$. Since $\mathrm{Ind}_\Pi^{\Delta'}(\pi_0) \cong \eta_0 \oplus \eta_1$, it follows that

$$\widetilde{\rho}^{ss} \;\cong\; \widetilde{\eta}_0^{p^a} \;\oplus\; \widetilde{\eta}_1^{p^a} \quad .$$

Now consider $\rho|_{\Omega'}$. It follows that the multiplicities of $\eta_0|_{\Omega'}$ and $\eta_1|_{\Omega'}$ in $\rho|_{\Omega'}$ are both equal to $p^a$. Now we use proposition 9.3.1 below. The representation $\eta_0|_{\Omega'}$ is orthogonal and occurs with odd multiplicity in $\rho|_{\Omega'}$. Therefore, the underlying representation space for $\rho|_{\Omega'}$ cannot have a nondegenerate $\Omega'$-invariant, symplectic pairing. It follows that $\rho$ itself cannot be symplectic and hence is orthogonal.

If $p \equiv 3 \pmod 4$, then $[\Delta : \Delta'] = \frac{p-1}{2}$ is odd. One can use proposition 9.3.4 below to see that $\Delta$ indeed satisfies property **(O)**. However, if $p \equiv 1 \pmod 4$, then one can easily give examples of $\Pi\Omega$-groups which fail to satisfy property **(O)**. For example, if $\Pi$ is cyclic of order $p$ and if one defines the map $\theta : \Omega \to \mathrm{Aut}(\Pi)$ so that $\ker(\theta) = \Omega'$, then $\Delta = \Pi \rtimes_\theta \Omega$ has just one element of order 2. Since $\Omega'$ is in the center of $\Delta$, it is a normal subgroup. One sees easily that $\Delta/\Omega'$ has at least one irreducible, self-dual representation of degree $> 1$, and hence so does $\Delta$. The two self-dual representations of degree 1 which factor through $\Delta/\Pi$ are obviously orthogonal. The Frobenius-Schur identity then shows that $\Delta$ must have at least one irreducible, symplectic representation. $\Diamond$

**Remark 9.2.2.** Assume that $\Delta$ is a $\Pi\Omega$-group and let $\Delta' = \Pi\Omega'$ as defined in remark 9.2.1. Thus, $\Delta/\Delta' \cong \Omega/\Omega'$, a cyclic group of order $\frac{p-1}{2}$. There is a certain subset of $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ which is closely related to $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta')$. If $\sigma$ is any irreducible representation of $\Delta$, then $\sigma|_{\Delta'}$ decomposes as a direct sum of irreducible representations of $\Delta'$, each occurring with multiplicity 1. Those summands form an orbit for the action of $\Omega/\Omega'$. (These remarks follow from propositions 9.10 and 9.12 in [Fei].) If $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$, then we will say that $\sigma$ is *"$\Delta'$-orthogonal"* if every irreducible constituent in $\sigma|_{\Delta'}$ is self-dual. Those constituents will be orthogonal since $\Delta'$ satisfies property **(O)**. It would be sufficient to require that just one irreducible constituent be self-dual. Note that there are two self-dual 1-dimensional representation of $\Delta$. They factor through $\Omega$ and will be denoted by $\sigma_0$ and $\sigma_{\mathbf{1}}$. Both are $\Delta'$-orthogonal by definition.

Proposition 9.3.1 below has the following consequence. Assume that $\sigma$ is an irreducible, self-dual representation of $\Delta$. If $\sigma$ is $\Delta'$-orthogonal, then $\sigma$ is orthogonal. However, the converse is not true in general.

Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Let $\rho$ be an irreducible constituent of $\sigma|_{\Delta'}$. Let $\pi$ be an irreducible constituent of $\rho|_{\Pi}$ and hence of $\sigma|_{\Pi}$. The set of irreducible constituents of $\sigma|_{\Pi}$ is the orbit of $\pi$ under the action of $\Omega$. The stabilizer for $\pi$ under this action will be denoted by $\Omega_\pi$ and will be called the $\Omega$-stabilizer for $\pi$. If $d = d(\sigma)$ is the length of this orbit, then $n(\sigma) = dp^a$ for some $a \geq 0$. Furthermore, one has an action of $\widehat{\Omega}$ on $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ defined by tensoring. More precisely, the action is described by the map $\widehat{\Omega} \times \mathrm{Irr}_{\mathcal{F}}(\Delta) \to \mathrm{Irr}_{\mathcal{F}}(\Delta)$ defined by sending $(\chi, \sigma)$ to $\sigma \otimes \chi$ for $\chi \in \widehat{\Omega}$ and $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. The $\widehat{\Omega}$-orbit of $\sigma$ has cardinality $\frac{p-1}{d}$ and consists of the irreducible constituents in $\mathrm{Ind}_{\Pi}^{\Delta}(\pi)$. The stabilizer of $\sigma$ under the action of $\widehat{\Omega}$ is the unique subgroup of $\widehat{\Omega}$ of order $d$. These facts are explained in part **A** of section 7.4. We let $\widehat{\Omega}(2)$ denote the Sylow 2-subgroup of $\widehat{\Omega}$.

Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$. With the above notation, we will show that the following statements are equivalent:

1. *The representation $\sigma$ is $\Delta'$-orthogonal and $n(\sigma) > 1$.*
2. *The ratio $\frac{p-1}{d(\sigma)}$ is odd.*
3. *The $\Omega$-stabilizer of $\pi$ has odd order.*
4. *The $\widehat{\Omega}$-stabilizer of $\sigma$ contains $\widehat{\Omega}(2)$.*
5. *The $\Omega'$-orbit of $\pi$ has length 2 and consists of $\pi$ and $\check{\pi}$.*

In statement 1, the inequality $n(\sigma) > 1$ just means that $\sigma$ doesn't factor through $\Omega$. Thus, $\pi \neq \pi_0$. Statements 2 and 3 are obviously equivalent. As remarked above, the $\widehat{\Omega}$-stabilizer of $\sigma$ is the subgroup of $\widehat{\Omega}$ of order $d(\sigma)$. Thus, statement 4 means that $|\widehat{\Omega}(2)|$ divides $d(\sigma)$, which is equivalent to statement 2.

Assume that statement 3 is satisfied. Let $\Omega_\pi$ denote the $\Omega$-stabilizer of $\pi$. Then $\Omega' \not\subset \Omega_\pi$ and hence the $\Omega'$-orbit of $\pi$ has length 2. Since $\sigma$ is self-dual, the $\Omega$-orbit of $\pi$ contains $\check{\pi}$. Thus, for some $\alpha \in \Omega$, we have $\check{\pi} \cong \pi \circ \varphi_\alpha$, where we let $\varphi_\alpha$ denote the automorphism of $\Pi$ defined by conjugation by $\alpha$. In fact, $\check{\pi} \cong \pi \circ \varphi_\alpha$ is true for all $\alpha$'s in a certain coset of $\Omega_\pi$. The contragredient of $\pi \circ \varphi_\alpha$ is $\check{\pi} \circ \varphi_\alpha$. Thus,

$$\pi \;\cong\; \check{\pi} \circ \varphi_\alpha \;\cong\; \pi \circ \varphi_\alpha^2 \;\cong\; \pi \circ \varphi_{\alpha^2} \quad .$$

Thus $\alpha^2 \in \Omega_\pi$ and hence $\alpha \in \Omega'\Omega_\pi$. Note that $\check{\pi} \ncong \pi$ since $\Pi$ has odd order and $\pi \neq \pi_0$. It follows that one can take $\alpha$ to be the nontrivial element of $\Omega'$, and so statement 5 is true. Conversely, if statement 5 is true, then the $\Omega'$-orbit of $\pi$ has length 2. Therefore, $\Omega' \not\subset \Omega_\pi$ which implies statement 3.

Statement 5 implies that $\mathrm{Ind}_\Pi^{\Delta'}(\pi)$ is a self-dual, irreducible representation of $\Delta'$. (See remark 9.2.1.) It is the unique irreducible representation of $\Delta'$ whose restriction to $\Pi$ contains $\pi$ as a constituent. Thus, $\mathrm{Ind}_\Pi^{\Delta'}(\pi)$ is an irreducible constituent in $\sigma|_{\Delta'}$. All the irreducible constituents are of that form and hence are self-dual. Therefore, statement 1 is true. Conversely, statement 1 means that every irreducible constituent of $\sigma|_{\Delta'}$ is isomorphic to $\mathrm{Ind}_\Pi^{\Omega'}(\pi)$ for some $\pi$ whose $\Omega'$-orbit contains $\check{\pi}$. Clearly, $\pi$ is an irreducible constituent in $\sigma|_\Pi$. It is clear that statement 5 is then true.

The above equivalences have now been justified. As an additional comment, suppose that $\rho$ is an irreducible, self-dual representation of $\Delta'$ and that $n(\rho) > 1$. We then have $\rho \cong \mathrm{Ind}_\Pi^{\Omega'}(\pi)$, where $\pi$ satisfies statement 5. The $\Omega$-stabilizer of $\pi$ has odd order and therefore every irreducible constituent $\sigma$ in $\mathrm{Ind}_\Pi^{\Delta}(\pi)$ satisfies statement 2. Thus, the number of such irreducible constituents is odd. Since $\mathrm{Ind}_\Pi^{\Delta}(\pi)$ is self-dual, at least one such constituent (say, $\sigma$) will be self-dual. The other constituents are isomorphic to twists $\sigma \otimes \chi$, where $\chi \in \widehat{\Omega}$. If $\sigma \otimes \chi$ is also self-dual, then $\sigma \otimes \chi^2 \cong \sigma$. Since the $\widehat{\Omega}$-stabilizer of $\sigma$ has index $\frac{p-1}{d(\sigma)}$, which is again odd, it follows that $\sigma \otimes \chi \cong \sigma$. Therefore, $\mathrm{Ind}_\Pi^{\Delta}(\pi) \cong \mathrm{Ind}_{\Delta'}^{\Delta}(\sigma)$ has exactly one irreducible, self-dual constituent. That is, there exists exactly one self-dual representations $\sigma$ of $\Delta$ such that $\sigma|_{\Delta'}$ has $\rho$ an one of its irreducible constituents. By definition, that representation $\sigma$ is $\Delta'$-orthogonal. Both $\Delta$ and $\Delta'$ have two 1-dimensional, self-dual representations, although $\sigma_0$ and $\sigma_{\mathbf{1}}$ have the same restriction to $\Delta'$ if $p \equiv 1 \pmod 4$.

We use the notation $\theta_{\Delta'\text{-}orth}(\Delta)$ to denote $\sum n(\sigma)$, where $\sigma$ varies over all of the $\Delta'$-orthogonal irreducible representations of $\Delta$. Since $\sigma$ and $\sigma|_{\Delta'}$ have the same degree, the remarks in the previous paragraph give the following relationship:

$$\theta_{\Delta'\text{-}orth}(\Delta) \;=\; \theta_{orth}(\Delta') \quad .$$

Note also that all the elements of order 2 in $\Delta$ are in $\Delta'$. Furthermore, $\theta_{symp}(\Delta') = 0$

according to remark 9.2.1. The Frobenius-Schur identity then implies that

$$\theta_{orth}(\Delta) \;=\; \theta_{\Delta'\text{-}orth}(\Delta) \;+\; \theta_{symp}(\Delta)$$

and hence that $\Delta$ satisfies property **(O)** if and only if every irreducible, self-dual representation of $\Delta$ is $\Delta'$-orthogonal. $\Diamond$

## 9.3 Some parity results concerning multiplicities.

Our next results concern the parity of the multiplicity for $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ in an $\mathcal{F}$-representation space $V$ for $\Delta$. In the formulation, saying that an $\mathcal{F}$-bilinear form $B$ on $V$ is $\Delta$-invariant means that $B(\delta v_1, \delta v_2) = B(v_1, v_2)$ for all $\delta \in \Delta$ and all $v_1, v_2 \in V$.

**Proposition 9.3.1.** *Suppose that $V$ is a finite-dimensional representation space for $\Delta$ over $\mathcal{F}$ and that there is a non-degenerate, skew-symmetric, $\Delta$-invariant, $\mathcal{F}$-bilinear form $B$ on $V$. Suppose that $\sigma$ is an orthogonal, irreducible representation of $\Delta$. Then the multiplicity of $\sigma$ in $V$ is even.*

*Proof.* For any subspace $W$ of $V$, we will let $W^\perp$ denote the maximal subspace orthogonal to $W$ under the pairing for $B$. Suppose that the multiplicity of $\sigma$ in $V$ is positive. Let $W$ be a $\Delta$-invariant subspace of $V$ isomorphic to $W_\sigma$, the underlying representation space for $\sigma$. The restriction of $B$ to $W$ is still skew-symmetric. Since $\sigma$ is orthogonal, that restriction must be trivial. That is, $W \subseteq W^\perp$. Now $W^\perp$ is also $\Delta$-invariant and so we get a non-degenerate $\Delta$-invariant pairing $W \times V/W^\perp \longrightarrow \mathcal{F}$. Thus, $V/W^\perp$ is a representation space for $\Delta$ isomorphic to $W_{\check{\sigma}}$. Since $\sigma$ is self-dual, we see that the multiplicity of $\sigma$ in $V$ is at least 2. Let $V' = W^\perp/W$. Then $V'$ is also a representation space for $\Delta$ and the multiplicity for $\sigma$ has been reduced by exactly 2. Now $B$ induces a bilinear form $B'$ on $V'$ in the obvious way, and that form is nondegenerate, skew-symmetric, and $\Delta$-invariant. The proposition follows by induction. $\square$

**Remark 9.3.2.** A virtually identical proof gives the following result.

*Assume that $V$ has a $\Delta$-invariant, $\mathcal{F}$-bilinear, non-degenerate pairing which is symmetric. Let $\sigma$ be a symplectic, irreducible representation of $\Delta$. Then the multiplicity of $\sigma$ in $V$ must be even.*

We also remark that the proofs of both results are valid for representations over any field of characteristic 0, or even odd characteristic. We will later apply proposition 9.3.1 to a

situation where $V$ is a $\mathbf{Q}_p$-representation for $\Delta$. We obtain an $\mathcal{F}$-representation space $V_{\mathcal{F}}$ by extending scalars: $V_{\mathcal{F}} = V \otimes_{\mathbf{Q}_p} \mathcal{F}$. By definition, if $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, then the multiplicity of $\sigma$ in $V$ refers to the multiplicity of $W_\sigma$ as a direct summand in $V_{\mathcal{F}}$. Also, note that a $\mathbf{Q}_p$-bilinear form $B$ on $V$ extends uniquely to an $\mathcal{F}$-bilinear form $B_{\mathcal{F}}$ on $V_{\mathcal{F}}$. Of course, $B_{\mathcal{F}}$ is $\Delta$-invariant if and only if $B$ is $\Delta$-invariant. Similarly, $B_{\mathcal{F}}$ is non-degenerate, symmetric, or skew-symmetric if and only if $B$ is non-degenerate, symmetric, or skew-symmetric, respectively. $\Diamond$

**Remark 9.3.3.** If $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$, then its Schur index over $\mathbf{Q}_p$ will be 1 or 2. This follows from the Brauer-Speiser theorem which states that the Schur index over $\mathbf{Q}$ is at most 2 when $\sigma$ is self-dual. If the Schur index for $\sigma$ over $\mathbf{Q}_p$ is 2 and if $V$ is a $\mathbf{Q}_p$-representation space for $\Delta$,then the multiplicity of $\sigma$ in $V$ will be even. The Schur index over $\mathbf{Q}_p$ can turn out to be 2 for either orthogonal or symplectic $\sigma$'s. In contrast, if one considers an irreducible, self-dual representation $\sigma$ over $\mathbf{C}$, its character is real-valued and its Schur index over $\mathbf{R}$ is 1 if $\sigma$ is orthogonal and is 2 if $\sigma$ is symplectic. (See [Se77], chapter 13.2.) $\Diamond$

We end this chapter with some results which will be useful in chapters 10 and 12. In particular, we will sometimes apply the next two propositions to the groups $G = D$ and $N = \Delta$, in the notation of section 3.5.

**Proposition 9.3.4.** *Suppose that $G$ is a finite group and that $N$ is a normal subgroup of $G$ such that $G/N$ is a cyclic group of odd order. Suppose that $\rho$ is a self-dual irreducible representation of $G$. Let $\sigma$ be an irreducible constituent in $\rho|_N$. Then $\sigma$ is self-dual. If $\rho$ is orthogonal, then so is $\sigma$. If $\rho$ is symplectic, then so is $\sigma$.*

*Furthermore, if $\sigma$ is a self-dual irreducible representation of $N$, then there exists exactly one self-dual irreducible representation $\rho$ of $G$ such that $\rho|_N$ has $\sigma$ as a constituent. If $\sigma$ is orthogonal, then so is $\rho$. If $\sigma$ is symplectic, then so is $\rho$.*

*Proof.* The irreducible constituents in $\rho|_N$ form an orbit in $\mathrm{Irr}_{\mathcal{F}}(N)$ under the action of $G/N$ defined by conjugation. Since $\rho$ is self-dual, so is $\rho|_N$. Therefore, if $\sigma$ is one of the irreducible constituents of $\rho|_N$, then $\check{\sigma}$ is also an irreducible constituent. The number of constituents is odd and therefore at least one must be self-dual. It then follows that they are all self-dual.

All of the irreducible constituents in $\rho|_N$ occur with equal multiplicity and that multiplicity is known to be 1 if $G/N$ is cyclic. This is proved in proposition 9.12 in [Fei]. Now if $\rho$ is orthogonal (respectively, symplectic), then we can apply proposition 9.3.1 or remark 9.3.2 to $\rho|_N$ to conclude that $\sigma$ is orthogonal (respectively, symplectic). We remark that we only need to know that $\sigma$ has odd multiplicity in $\rho|_N$, and this is known to be true if we just assume that $G/N$ has odd order.

For the second part, note that if $\rho$ is any irreducible constituent in $\mathrm{Ind}_N^G(\sigma)$, where $\sigma$ is an irreducible representation of $N$, then $n(\rho) = dn(\sigma)$, where $d$ is the cardinality of the orbit of $\sigma$. Each of those irreducible constituents has multiplicity 1 by Frobenius Reciprocity. The number of such constituents is therefore odd. If $\sigma$ is self-dual, then so is $\mathrm{Ind}_N^G(\sigma)$. Pairing each of those constituents with their contragredients, it follows that at least one of them is self-dual. Call that constituent $\rho$. By the first part, $\rho$ is orthogonal if and only if $\sigma$ is orthogonal.

Now suppose that $\rho'$ is a self-dual constituent in $\mathrm{Ind}_N^G(\sigma)$. Then $\rho \otimes \rho'$ is also self-dual. We will show that $\rho \otimes \rho'$ contains $\mathbf{1}_G$ as a constituent, and therefore that $\rho' \cong \check{\rho} \cong \rho$. First of all, $\rho \otimes \rho'|_N$ does contain $\mathbf{1}_N$ as a constituent. That is so because $\sigma \otimes \sigma$ contains $\mathbf{1}_N$. The multiplicity is 1. This is true for all the irreducible constituents in $\rho|_N \cong \rho'|_N$. It follows easily that $\rho \otimes \rho'|_N$ contains $\mathbf{1}_N$ as a constituent with multiplicity $d$. Thus, there exists at least one irreducible constituent $\chi$ in $\rho \otimes \rho'$ such that $\chi|_N$ has $\mathbf{1}_N$ as a constituent. However, using 9.12 in [Fei] again, it follows that $\chi$ must be of degree 1 and so $\chi|_N = \mathbf{1}_N$. This means that $ker(\chi)$ contains $N$. The number of such constituents $\chi$ in $\rho \otimes \rho'$ must be $d$. Each of them can regarded as a character of $G/N$. Since $d$ is odd, at least one of those $\chi$'s must be self-dual. However, $\rho \otimes \rho'$ is self-dual. Hence, at least one of the $\chi$'s must be self-dual. Since $G/N$ has odd order, their is only one self-dual character of $G/N$, namely the trivial character. Consequently, $\rho \otimes \rho'$ does indeed have $\mathbf{1}_G$ as a constituent. □

The next result will be stated in terms of the usual multiplicity pairing $\langle \rho, \rho' \rangle_G$, which is defined for all $\rho, \rho' \in \mathcal{R}_{\mathcal{F}}(G)$. It is a $\mathbf{Z}$-bilinear pairing. If $\rho$ and $\rho'$ are absolutely irreducible, one has $\langle \rho, \rho' \rangle_G = 1$ if $\rho \cong \rho'$ and $\langle \rho, \rho' \rangle_G = 0$ otherwise. The pairing $\langle \cdot, \cdot \rangle_N$ on $\mathcal{R}_{\mathcal{F}}(N)$, where $N$ is a subgroup of $G$, is defined in the same way.

**Proposition 9.3.5.** *Suppose that $G$ is a finite group and that $N$ is a normal subgroup of $G$ such that $G/N$ has odd order. Suppose that $\rho$ and $\rho'$ are self-dual representation of $G$. Then*

$$\langle \rho|_N,\ \rho'|_N \rangle_N \ \cong\ \langle \rho,\ \rho' \rangle_G \qquad (\mathrm{mod}\ 2)\ .$$

*Proof.* Since $N$ is a normal subgroup of $G$, $\mathrm{Ind}_N^G(\mathbf{1}_N)$ is isomorphic to the regular representation of $G/N$, viewed as a representation of $G$. It follows that

$$\mathrm{Ind}_N^G(\rho'|_N) \ \cong\ \bigoplus_{\varepsilon} (\rho' \otimes \varepsilon)^{n(\varepsilon)}\ ,$$

where $\varepsilon$ runs over all the irreducible representations of $G/N$. We use Frobenius Reciprocity, obtaining the following equalities:

$$\langle \rho|_N, \rho'|_N \rangle_N = \langle \rho,\ \mathrm{Ind}_N^G(\rho'|_N)\ \rangle_G = \langle \rho,\ \bigoplus_{\varepsilon} (\rho' \otimes \varepsilon)^{n(\varepsilon)}\ \rangle_G = \sum_{\varepsilon}\ n(\varepsilon) \langle \rho,\ \rho' \otimes \varepsilon \rangle_G\ .$$

The term where $\varepsilon = \varepsilon_0$ gives the contribution $\langle \rho, \rho' \rangle_G$. There is a theorem of Burnside which asserts that a nontrivial absolutely irreducible representation of a finite group of odd order cannot be self-dual. Thus, the terms where $\varepsilon \neq \varepsilon_0$ occur in pairs: $\varepsilon$ and $\check{\varepsilon}$. However, since $\rho'$ is self-dual, the contragredient of $\rho' \otimes \varepsilon$ is isomorphic to $\rho' \otimes \check{\varepsilon}$. Also, since $\rho$ is self-dual, we have

$$\langle \rho,\ \rho' \otimes \check{\varepsilon} \rangle_G \ = \ \langle \rho,\ \rho' \otimes \varepsilon \rangle_G$$

where we use the fact that $\langle \check{\alpha},\ \check{\beta} \rangle_G = \langle \alpha,\ \beta \rangle_G$ for any two representations $\alpha$ and $\beta$ of $G$. The stated congruence follows immediately. $\square$

## 9.4 Self-dual representations and the decomposition map.

Let $\Delta$ be a finite group. There is a refinement of the theorem of Brauer asserting that the decomposition map $d : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathcal{R}_{\mathfrak{f}}(\Delta)$ is surjective. It will be useful in the proof of corollary 12.1.3. As in Brauer's theorem, we assume that $\mathcal{F}$ contains the $m$-th roots of unity, where $m$ is divisible by the orders of all elements of $\Delta$. The groups $\mathcal{R}_{\mathcal{F}}(\Delta)$ and $\mathcal{R}_{\mathfrak{f}}(\Delta)$ have natural involutions defined by sending an irreducible representation to its contragredient. Thus, both groups have an action of a cyclic group $C$ of order 2. We denote $\mathcal{R}_{\mathcal{F}}(\Delta)^C$ and $\mathcal{R}_{\mathfrak{f}}(\Delta)^C$ by $\mathcal{R}^{(sd)}_{\mathcal{F}}(\Delta)$ and $R^{(sd)}_{\mathfrak{f}}(\Delta)$, respectively. If $\rho \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$, then $[\rho] \in \mathcal{R}^{(sd)}_{\mathcal{F}}(\Delta)$ if and only if $\rho$ is self-dual. If $\upsilon \in \mathrm{Rep}_{\mathfrak{f}}(\Delta)$, then $[\upsilon] \in \mathcal{R}^{(sd)}_{\mathfrak{f}}(\Delta)$ if and only if $\check{\upsilon}^{ss} \cong \upsilon^{ss}$. Now consider the induced map

$$d^{(sd)} :\ \mathcal{R}^{(sd)}_{\mathcal{F}}(\Delta) \longrightarrow \mathcal{R}^{(sd)}_{\mathfrak{f}}(\Delta) \quad .$$

It turns out that this map is also surjective. The proof relies on another well-known theorem of Brauer - his characterization of elements of $\mathcal{R}_{\mathcal{F}}(\Delta)$ in terms of their restrictions to elementary subgroups of $\Delta$.

We can identify $\mathcal{R}_{\mathcal{F}}(\Delta)$ with the character ring for $\Delta$. This is a subring of the ring of class functions on $\Delta$ with values in $\mathbf{Z}[\zeta]$, where $\zeta$ is a primitive $m$-th root of unity. If $\rho$ is any representation of $\Delta$ over $\mathcal{F}$, we will denote its character by $\chi_\rho$. The elements of $\mathcal{R}_{\mathcal{F}}(\Delta)$ are differences $\chi_{\rho_1} - \chi_{\rho_2}$, where $\rho_1$ and $\rho_2$ are representations of $\Delta$. We could write this as $\chi_\rho$, where $\rho = \rho_1 \ominus \rho_2$ is a "virtual" representation. One identifies a virtual representation $\rho$ with its character $\chi_\rho$. The ring $\mathbf{Z}[\zeta]$ has an involution $\iota$ induced by $\zeta \to \zeta^{-1}$. Let $\mathbf{Z}[\zeta]^+$ denote the subring of $\mathbf{Z}[\zeta]$ fixed by that involution. If $f$ is any function with values in $\mathbf{Z}[\zeta]$, then we will let $\overline{f}$ denote $\iota \circ f$. In particular, if $\rho \in \mathcal{R}_{\mathcal{F}}(\Delta)$, then it is well-known that $\chi_{\check{\rho}} = \overline{\chi}_\rho$. Hence, $\rho \in \mathcal{R}^{(sd)}_{\mathcal{F}}(\Delta)$ if and only if $\chi_\rho$ has values in $\mathbf{Z}[\zeta]^+$. We then say that $\chi_\rho$ is real-valued.

Let $\Delta_{reg}$ be the set of elements in $\Delta$ of order prime to $p$. The ring $\mathcal{R}_{\mathfrak{f}}(\Delta)$ can be identified with the ring of Brauer characters, which is a subring of the $\mathbf{Z}[\zeta]$-valued class functions on $\Delta_{reg}$. If $\upsilon$ is a representation of $\Delta$ over $\mathfrak{f}$, then its Brauer character $\chi_\upsilon$ determines and is determined by the isomorphism class of $\upsilon^{ss}$, i.e., by the class $[\upsilon]$ in $\mathcal{R}_{\mathfrak{f}}(\Delta)$. We can define $\chi_\upsilon$ if $\upsilon$ is a virtual representations for $\Delta$ just as above. It is again true that $\chi_{\check{\upsilon}} = \overline{\chi}_\upsilon$ and so $\upsilon \in \mathcal{R}_{\mathfrak{f}}^{(sd)}(\Delta)$ if and only if $\chi_\upsilon$ is real-valued. To show that $d^{(sd)}$ is surjective, it suffices to show that if $[\upsilon] \in \mathcal{R}_{\mathfrak{f}}^{(sd)}(\Delta)$, then there exists a $\rho \in \mathcal{R}_{\mathcal{F}}(\Delta)$ such that $\chi_\rho$ is real-valued and $\chi_\rho|_{\Delta_{reg}} = \chi_\upsilon$. But this assertion is an immediate consequence of theorem 43 in [Se77]. One defines a class function $\chi$ on $\Delta$ as follows: If $g \in \Delta$, one can write $g = rs$, where $r \in \Delta_{reg}$, $s$ has $p$-power order, and $rs = sr$. Obviously, $r$ and $s$ are uniquely determined by $g$. Define $\chi : \Delta \to \mathbf{Z}[\zeta]$ by $\chi(g) = \chi_\upsilon(r)$. It is clear that $\chi$ is a class function on $\Delta$, that $\chi$ is real-valued, and that $\chi|_{\Delta_{reg}} = \chi_\upsilon$. Using the characterization theorem of Brauer, Serre verifies that there is indeed a $\rho \in \mathcal{R}_{\mathcal{F}}(\Delta)$ such that $\chi = \chi_\rho$.

# 10 A duality theorem.

Suppose that $K/F$ is a finite Galois extension and let $D = \mathrm{Gal}(K/F)$. Suppose that $E$ is any elliptic curve defined over $F$. Fix a prime $p$. The weak Mordell-Weil theorem tells us that $\mathrm{Sel}_E(K)_p$ has finite $\mathbf{Z}_p$-corank. The Kummer map

$$E(K) \otimes_{\mathbf{Z}} \left(\mathbf{Q}_p/\mathbf{Z}_p\right) \longrightarrow \mathrm{Sel}_E(K)_p$$

is an injective $D$-equivariant map. Its cokernel is isomorphic to $Ш_E(K)_p$. Let $X_E(K)$ denote the Pontryagin dual of $\mathrm{Sel}_E(K)_p$ and $Y_E(K)$ denote the Pontryagin dual of $E(K) \otimes_{\mathbf{Z}} \left(\mathbf{Q}_p/\mathbf{Z}_p\right)$. We then have a surjective map $X_E(K) \to Y_E(K)$ which is $D$-equivariant. Therefore, $Y_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a quotient of $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ as a $\mathbf{Q}_p$-representation space for $D$. Of course, the conjecture that $Ш_E(K)_p$ is finite implies that those two spaces are isomorphic.

Both $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $Y_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ are self-dual representation spaces for $D$. This is obvious for $Y_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ since it is dual to $E(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p$ and the character of that representation space has values in $\mathbf{Q}$. The fact that $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is self-dual is proved in [Dok4] by studying the change in Selmer groups under an isogeny. One can also give a proof based directly on the Poitou-Tate duality theorems. One must show that if $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$, then $\rho$ and $\check{\rho}$ have the same multiplicities in $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. According to remark 4.3.2, those multiplicities are equal to the $\mathcal{O}$-coranks of the Selmer groups $\mathrm{Sel}_{E[p^\infty]\otimes\rho}(F)$ and $\mathrm{Sel}_{E[p^\infty]\otimes\check{\rho}}(F)$, respectively. One can compare those $\mathcal{O}$-coranks by using the duality theorems. A proof of the equality of those $\mathcal{O}$-coranks is found in [Nek2], proposition 12.5.9.5. Nekovář

assumes that $n(\rho) = 1$, but this is not really necessary in his argument. Proposition 2 in [Gr94a] also implies the equality, but that result is only proved for the base field $F = \mathbf{Q}$. The argument is quite general in nature and can easily be modified to work over any number field $F$.

Suppose that $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$. Let $r_E(\rho)$ denote the multiplicity of $\rho$ in the $\mathcal{F}$-representation space $E(K) \otimes_{\mathbf{Z}} \mathcal{F}$, or equivalently, in the representation space $Y_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$. Let $s_E(\rho)$ denote the multiplicity of $\rho$ in $X_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$. Of course, $s_E(\rho)$ might conceivably depend on $p$. If the Tate-Shafarevich group $Ш_E(K)$ turns out to be finite, then $s_E(\rho) = r_E(\rho)$, which is independent of $p$. Conjecturally, this is so. As a consequence of self-duality, we have

$$r_E(\check{\rho}) \;=\; r_E(\rho), \qquad \textit{and} \qquad s_E(\check{\rho}) \;=\; s_E(\rho) \tag{10.0.a}$$

for all $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$. One can extend the definitions of $r_E(\rho)$ and $s_E(\rho)$ to all representations $\rho$ of $D$ so that those functions behave additively for direct sums. Clearly, the equalities (10.0.a) will continue to be true.

## 10.1 The main result.

Now assume that $E$ has good, ordinary reduction at $p$. The main result of this chapter concerns the $\mathbf{Q}_p$-representation space $V = X_E(K_\infty) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $G = \mathrm{Gal}(K_\infty/F)$, where $K_\infty$ is the cyclotomic $\mathbf{Z}_p$-extension of $K$. We will let $\Gamma_K$ denote $\mathrm{Gal}(K_\infty/K)$. If $\mathrm{Sel}_E(K_\infty)_p$ is a cotorsion $\mathbf{Z}_p[[\Gamma_K]]$-module, then $V$ is finite-dimensional. We will show that $V$ is then self-dual. However, the result is more precise. In the formulation, let $K_n$ denote the $n$-th layer in $K_\infty/K$, where $n \geq 0$. Thus, $\mathrm{Gal}(K_n/K)$ is cyclic of order $p^n$. We let $\Gamma_{K_n} = \mathrm{Gal}(K_\infty/K_n)$, the subgroup of index $p^n$ in $\Gamma_K$. It will not be necessary to make the assumption that $K \cap F_\infty = F$. As in section 3.5, we will continue to denote $\mathrm{Gal}(K_\infty/F_\infty)$ by $\Delta$. We can identify $\Delta$ with a subgroup of $D$. In particular, if $K \cap F_\infty = F$, we will have $\Delta = D$. Here is our main result. It is true even if $p = 2$.

**Proposition 10.1.1.** *Suppose that* $\mathrm{Sel}_E(K_\infty)_p$ *is cotorsion as a* $\mathbf{Z}_p[[\Gamma_K]]$*-module. Let* $G$ *and* $V$ *be as defined above. Then* $V$ *is a finite-dimensional, self-dual* $\mathbf{Q}_p$*-representation space for* $G$*. Furthermore, if* $t$ *is chosen large enough so that* $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_t)_p\big)$ *is maximal, then the* $\mathbf{Q}_p$*-representation space*

$$W \;=\; \ker\big(V \longrightarrow V_{\Gamma_{K_t}}\big)$$

*for* $G$ *admits a* $\mathbf{Q}_p$*-bilinear, non-degenerate, skew-symmetric,* $G$*-invariant pairing.*

As we will point out in the proof, $V_{\Gamma_{K_t}}$ is isomorphic to $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ as a $\mathbf{Q}_p$-representation space for $\mathrm{Gal}(K_t/F)$ and is therefore self-dual. That fact is one ingredient in

the proof. Another ingredient is the Cassels-Tate pairing on $Ш_E(K_n)_p$ for $n \geq t$, which is skew-symmetric. The existence of the skew-symmetric pairing on $W$ will be derived from the existence of the Cassels-Tate pairing for a sufficiently large value of $n$. The following lemma is the key step in doing that. It concerns the existence of bilinear forms of a certain type. We consider only skew-symmetric forms, which is what we will actually need, but the analogous result is true for symmetric forms too, with essentially the same proof. We will just assume that $\Delta$ is a finite group, that $G$ is a profinite group which contains $\Delta$ as a normal subgroup, and that $G/\Delta \cong \Gamma$. 0f course, we have in mind the situation discussed in section 3.5.

If $R$ is a commutative ring and $B$ is an $R$-bilinear form on some $R$-module $N$, then we will understand implicitly that the values of $B$ are in $R$. If $B$ is symmetric or skew-symmetric, then $\{n \in N \mid B(n, N) = 0\}$ will be called the radical of $B$. It is an $R$-submodule of $N$. If $R = \mathbf{Z}_p$ and the radical of $B$ is trivial, then $B$ extends to a non-degenerate $\mathbf{Q}_p$-bilinear form on the vector space $N \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

**Lemma 10.1.2.** *Suppose that $W$ is a $\mathbf{Q}_p$-representation space for $\Delta$ and that $L$ is a $\Delta$-invariant $\mathbf{Z}_p$-lattice in $W$. For every $n \geq 1$, suppose that there exists a $(\mathbf{Z}/p^n\mathbf{Z})$-bilinear form $\widetilde{B}_n$ on $L/p^nL$ which is $\Delta$-invariant and skew-symmetric, and whose radical has bounded exponent as $n \to \infty$. Then there exists a $\mathbf{Q}_p$-bilinear form $B$ on $W$ which is $\Delta$-invariant, skew-symmetric, and non-degenerate. Furthermore, suppose that $W$ is a representation space for $G$, that $L$ is invariant under the action of $G$, and that the forms $\widetilde{B}_n$ can be chosen to be $G$-invariant. Then the form $B$ can also be chosen to be $G$-invariant.*

*Proof.* Let $\mathfrak{B}$ be the $\mathbf{Z}_p$-module consisting of all skew-symmetric, $\mathbf{Z}_p$-bilinear forms on $L$. Any element $B \in \mathfrak{B}$ induces a skew-symmetric $\mathbf{Q}_p$-bilinear form on $W$. The group $\Delta$ acts naturally on $\mathfrak{B}$. If $\delta \in \Delta$, then the value of $\delta(B)$ at $(x, y)$ is $B(\delta^{-1}x, \delta^{-1}y)$. We must prove the existence of an element $B \in \mathfrak{B}$ which is $\Delta$-invariant and such that the bilinear form on $W$ induced by $B$ is non-degenerate.

For $n \geq 1$, let $\mathfrak{B}_n$ denote the $\mathbf{Z}_p$-module consisting of skew-symmetric, $(\mathbf{Z}/p^n\mathbf{Z})$-bilinear forms on $L/p^nL$. The group $\Delta$ acts on $\mathfrak{B}_n$ and the natural reduction map $\beta_n : \mathfrak{B} \to \mathfrak{B}_n$ is a surjective, $\Delta$-equivariant homomorphism. Suppose that $\widetilde{B}_n \in \mathfrak{B}_n$ satisfies the hypotheses in the proposition. Let $B'_n \in \mathfrak{B}$ be any inverse image of $\widetilde{B}_n$ under the map $\beta_n$. Define $B_n = N_\Delta(B'_n)$, where $N_\Delta$ is the norm map for the action of $\Delta$ on $\mathfrak{B}$. Then $B_n$ is $\Delta$-invariant. The image of $B_n$ under $\beta_n$ is $|\Delta|\widetilde{B}_n$. We must just show that the radical of $B_n$ is trivial if $n$ is sufficiently large. Then we take $B$ to be the extension of $B_n$ to $W$.

If the radical $M$ of $B_n$ is nonzero, then $M$ is a $\mathbf{Z}_p$-submodule of $L$ and must obviously be a direct summand. Hence the image of $M$ in $L/p^nL$ has exponent $p^n$. However, the image

of $M$ is contained in the radical of $|\Delta|\widetilde{B}_n$, which has bounded exponent as $n \to \infty$. Thus, if $n$ is sufficiently large, the radical of $B_n$ is indeed trivial.

For the second part, the group $G$ is assumed to act on $W$ continuously. Now $G$ also acts continuously on $\mathfrak{B}$ and the $\mathbf{Z}_p$-submodule $\mathfrak{B}^\Delta$ is invariant under that action. The set $\mathfrak{B}^\Delta$ is a closed subset of $\mathfrak{B}$ and hence is compact. It is sequentially compact. It is also a direct summand of $\mathfrak{B}$ as a $\mathbf{Z}_p$-module. The action of $G$ on $\mathfrak{B}^\Delta$ factors through $\Gamma$. Let $\gamma$ be a topological generator of $\Gamma$ and let $T = \gamma - id_\Gamma$, viewed as a $\mathbf{Z}_p$-linear map on $\mathfrak{B}^\Delta$. Assume that the forms $\widetilde{B}_n$ are $G$-invariant. Then $B_n$, as defined above, is in $\mathfrak{B}^\Delta$ and $TB_n \in p^n\mathfrak{B}^\Delta$. There exists a subsequence of the $B_n$'s which converges. Let $B_\infty \in \mathfrak{B}^\Delta$ be the limit of such a subsequence. Then $TB_\infty = 0$. It is clear that $B_\infty$ is $G$-invariant. Also, by using essentially the same argument as above, one can verify that the radical of $B_\infty$ is trivial. We obtain the desired $B$ by extending $B_\infty$ to $W$. $\square$

*Proof of proposition 10.1.1.* Mazur's control theorem for the extension $K_\infty/K$ asserts that the restriction map

$$s_n : \ \mathrm{Sel}_E(K_n)_p \ \longrightarrow \ \mathrm{Sel}_E(K_\infty)_p^{\Gamma_{K_n}}$$

has finite kernel and cokernel, both of bounded order. (See [Ma72] or [Gr99].) It is also a $\mathrm{Gal}(K_n/F)$-equivariant map. The assumption that $\mathrm{Sel}_E(K_\infty)_p$ is cotorsion as a $\mathbf{Z}_p[[\Gamma_K]]$-module implies that the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K_n)_p$ is bounded as $n \to \infty$, and hence becomes constant for sufficiently large $n$. Let $M_n$ denote the maximal divisible subgroup of $\mathrm{Sel}_E(K_n)_p$ and let $A_n = \mathrm{Sel}_E(K_n)_p/M_n$, a finite group. It follows that if $t$ is chosen as in the proposition, and if $m \geq n \geq t$, then the map $M_n \to M_m$ is surjective. Let $M_\infty = s_t(M_t)$ and let $A_\infty = \mathrm{Sel}_E(K_\infty)_p/M_\infty$. The map $s_n$ induces a map $a_n : A_n \to A_\infty$. The above remarks imply that $|ker(a_n)| \leq |ker(s_n)|$ for $n \geq t$ and hence $|ker(a_n)|$ is bounded as $n \to \infty$. Let

$$\lambda = \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_\infty)_p\big), \qquad \lambda_0 = \mathrm{corank}_{\mathbf{Z}_p}\big(M_\infty\big), \qquad \lambda_1 = \mathrm{corank}_{\mathbf{Z}_p}\big(A_\infty\big) \ .$$

Then $\lambda = \mathrm{rank}_{\mathbf{Z}_p}\big(X_E(K_\infty)\big) = \dim_{\mathbf{Q}_p}(V)$ and $\lambda_0 + \lambda_1 = \lambda$.

Suppose that $n \geq t$. The restriction map $s_n$ induces the dual map

$$\hat{s}_n : \ X_E(K_\infty)_{\Gamma_{K_n}} \ \longrightarrow \ X_E(K_n) \ ,$$

which also has finite kernel and cokernel. Since $s_n$ is $\mathrm{Gal}(K_n/F)$-equivariant, so is $\hat{s}_n$. Hence,

$$V_{\Gamma_{K_n}} \ \cong \ X_E(K_n) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

as representation spaces for $\mathrm{Gal}(K_n/F)$. The theorem in [Dok4] cited previously therefore implies that $V_{\Gamma_{K_n}}$ is a self-dual representation space for $\mathrm{Gal}(K_n/F)$. For $n \geq t$, we have $\dim_{\mathbf{Q}_p}(V_{\Gamma_{K_n}}) = \lambda_0$. Also, $\dim_{\mathbf{Q}_p}(W) = \lambda_1$.

We now study $W$. Assume that $n \geq t$. From the definitions, we have

$$s_n(M_n) \;=\; M_\infty \;\subseteq\; \mathrm{Sel}_E(K_\infty)_p^{\Gamma_{K_n}} \;\subseteq\; \mathrm{Sel}_E(K_\infty)_p$$

and correspondingly, we have surjective maps

$$X_E(K_\infty) \;\longrightarrow\; X_E(K_\infty)_{\Gamma_{K_n}} \;\longrightarrow\; \widehat{M}_\infty \quad .$$

The kernel of the second map is finite and the kernel of the composite map is isomorphic to $\widehat{A}_\infty$. Therefore, we have an isomorphism

$$W \;\cong\; \widehat{A}_\infty \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

as representation spaces for $G$. If $\mu\big(X_E(K_\infty)\big) > 0$, then the $\mathbf{Z}_p$-torsion subgroup of $X_E(K_\infty)$ would be infinite, but it would be of bounded exponent. Let $A_{\infty,div}$ be the maximal divisible subgroup of $A_\infty$. Then $A_{\infty,div}$ has finite $\mathbf{Z}_p$-corank, which is equal to $\dim_{\mathbf{Q}_p}(W)$, and the corresponding quotient $A_\infty/A_{\infty,div}$ has finite exponent, say $p^u$. Let $L$ be the image of $\widehat{A}_\infty$ in $W$. It is clear that $L$ is a Galois-invariant $\mathbf{Z}_p$-lattice in $W$ and that $L \cong \widehat{A}_{\infty,div}$. We will use lemma 10.1.2 to get a bilinear pairing on $W$ with the stated properties.

Note that for any $n \geq 1$, $L/p^nL$ is the Pontryagin dual of $A_{\infty,div}[p^n]$. To define a bilinear form on $L/p^nL$ with certain properties, it suffices to define such a form on $A_{\infty,div}[p^n]$. We will omit the justification, which is not completely trivial. One helpful remark is that if $\mathfrak{B}_n$ is as in the proof of lemma 10.1.2, then the Pontryagin dual of $(\mathfrak{B}_n)^\Delta$ is $(\widehat{\mathfrak{B}_n})_\Delta$, which may have a different structure than $(\widehat{\mathfrak{B}_n})^\Delta$. However, it is enough to show that the kernel and cokernel of the map $(\mathfrak{B}_n)^\Delta \to (\mathfrak{B}_n)_\Delta$ has bounded order as $n \to \infty$, which is not difficult.

Now we have a map $a_n : A_n \to A_\infty$ whose kernel is of bounded order as $n$ varies. The Cassels-Tate pairing on the group $A_n$ defines a non-degenerate, skew-symmetric, $\mathbf{Z}_p$-bilinear form on that group. That form is $\mathrm{Gal}(K_n/F)$-invariant. We will use it to define a suitable bilinear form on $A_{\infty,div}[p^n]$. Note that $a_n\big(p^uA_n\big) \subset A_{\infty,div}$. We will show that the subgroup $a_n\big(p^uA_n\big)$ of $A_{\infty,div}$ is an approximation to $A_{\infty,div}[p^n]$ in some sense.

Suppose that we have two sequences $\{G_n\}$ and $\{H_n\}$ of finite abelian groups and a sequence of homomorphisms $f_n : G_n \to H_n$. We will say that this sequence $\{f_n\}$ of maps is *kc*-bounded if the groups $ker(f_n)$ and $coker(f_n)$ have bounded exponent as $n \to \infty$. If such a sequence $\{f_n\}$ exists, we will write $\{G_n\} \sim \{H_n\}$. One example we need is the following. For brevity, we write $\Lambda_K$ for $\mathbf{Z}_p[[\Gamma_K]]$. As usual, we can identify that ring with the formal power series ring $\mathbf{Z}_p[[T_K]]$, where $T_K = \gamma_K - id_{\Gamma_K}$ and $\gamma_K$ is a fixed topological generator of $\Gamma_K$. Suppose that $X = X_E(K_\infty)$, a finitely generated, torsion $\Lambda_K$-module. One can use the classification theorem for such modules to study the growth of the groups $X_{\Gamma_{K_n}}$ as $n$ varies.

One does this factor-by-factor, reducing to modules of the form $\Lambda_K/\big(\theta(T_K)\big)$, where $\theta(T_K)$ is a power of an irreducible polynomial in $\Lambda_K$. This is rather straightforward to do. Some special attention is needed for factors where the roots of $\theta(T_K)$ are of the form $\zeta-1$, $\zeta$ being a $p$-power root of unity. We will omit the details. Applying this to $X = X_E(K_\infty)$, we see that the $\mathbf{Z}_p$-rank of $X_{\Gamma_{K_n}}$ stabilizes and is equal to $\lambda_0$ for $n \geq t$. For the $\mathbf{Z}_p$-torsion submodules, one can show that $\{(X_{\Gamma_{K_n}})_{tors}\} \sim \{\big(\mathbf{Z}/p^n\mathbf{Z}\big)^{\lambda_1}\}$. The corresponding $kc$-bounded sequence of maps $f_n$ is not canonical. A second example that we need is that $\{(X_{\Gamma_{K_n}})_{tors}\} \sim \{\widehat{A}_n\}$. This follows from Mazur's control theorem. Also, $\widehat{A}_n \cong A_n$ as a group. Hence, in summary, we have $\{A_n\} \sim \{\big(\mathbf{Z}/p^n\mathbf{Z}\big)^{\lambda_1}\}$. Note that $A_{\infty,div}[p^n] \cong \big(\mathbf{Z}/p^n/\mathbf{Z}\big)^{\lambda_1}$.

The maps $a_n$ defined above are canonical, and hence Galois-equivariant. The above discussion shows that one can choose an integer $v \geq u$ so that $a_n(p^v A_n) \subseteq A_{\infty,div}[p^n]$. Consider the map $b_n = p^v a_n$, which is a Galois-equivariant map from $A_n$ to $A_{\infty,div}[p^n]$. Furthermore, the sequence $\{b_n\}$ of maps is $kc$-bounded. The last fact follows from the remarks in the previous paragraph and the fact that $ker(a_n)$ is of bounded order.

The assertion that $W$ has a pairing with the stated properties is easily deduced from lemma 10.1.2. We need to define $(\mathbf{Z}/p^n\mathbf{Z})$-bilinear, skew-symmetric, Galois-equivariant pairings on the $A_{\infty,div}[p^n]$'s and this can be done using the maps $b_n$. One uses the following two observations: (1) Assume that one has a non-degenerate, bilinear form $B_1$ on a finite abelian group $A_1$ and that $A_1'$ is a subgroup of $A_1$ of exponent $e$. Then $eB_1$ defines a bilinear form $B_2$ on $A_2 = A_1/A_1'$. The radical of $B_2$ will have exponent at most $e$. (2) Assume that one has a bilinear form $B_2$ on a finite abelian group $A_2$, that the radical of $B_2$ has exponent $e$, that $A_3$ is an abelian group containing $A_2$ as a subgroup, and that $A_3/A_2$ has exponent $f$. Then one obtains a bilinear form $B_3$ on $A_3$ by composing the map $A_3 \times A_3 \longrightarrow A_2 \times A_2$ defined by multiplication by $f$ with the form $B_2$. The radical of the form $B_3$ has exponent at most $ef^2$. One uses observation (1) for the form $B_1$ defined by the Cassels-Tate pairing on $A_n$ to obtain a bilinear form $B_2$ on $im(b_n)$. One uses the form $B_2$ and observation (2) to obtain a bilinear form $B_3$ on $A_{\infty,div}[p^n]$. It is clear that $B_3$ will be skew-symmetric, Galois-invariant, and that its radical will have exponent which is bounded as $n$ varies.

Having shown that $W$ has a non-degenerate, $G$-invariant, skew-symmetric, $\mathbf{Q}_p$-bilinear form, it follows that $W$ is self-dual as a representation space for $G$. Since $V/W$ is also self-dual, it follows that $V$ is self-dual. □

The following corollary includes the duality relation mentioned in section 1.2. For the second part, recall that $\lambda_E(\rho)$ is defined for $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$ by the formula (3.5.a).

**Corollary 10.1.3.** *Suppose that* $\mathrm{Sel}_E(K_\infty)_p$ *is a cotorsion* $\mathbf{Z}_p[[\Gamma_K]]$*-module. If* $\sigma$ *is an*

*irreducible representation of* $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$*, then* $\lambda_E(\check{\sigma}) = \lambda_E(\sigma)$*. Also, if* $\rho$ *is an irreducible representation of* $D = \mathrm{Gal}(K/F)$*, then* $\lambda_E(\check{\rho}) = \lambda_E(\rho)$*.*

*Proof.* The fact that $V$ is self-dual as a $\Delta$-representation space gives the first assertion. The second follows immediately because the contragredient of $\rho|_\Delta$ is $\check{\rho}|_\Delta$. □

## 10.2 Consequences concerning the parity of $s_E(\rho)$.

We want to now discuss the parity of $s_E(\rho)$ for self-dual representations $\rho$. We will assume that $p$ is odd. We continue to let $D = \mathrm{Gal}(K/F)$ and $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$. The first part of the following proposition concerns self-dual, irreducible representations $\rho$ of $D$. In the last part, $\rho$ may be reducible.

**Proposition 10.2.1.** *Suppose that* $p$ *is odd and that* $\mathrm{Sel}_E(K_\infty)_p$ *is* $\mathbf{Z}_p[[\Gamma_K]]$*-cotorsion. Suppose that* $\rho$ *is a self-dual, irreducible representation of* $D$ *and that* $\rho$ *is orthogonal. Suppose that* $\sigma$ *is an irreducible constituent in* $\rho|_\Delta$*. Then*

$$s_E(\rho) \equiv \lambda_E(\rho) \equiv \lambda_E(\sigma) \pmod 2 \quad .$$

*If* $\rho$ *is any self-dual, orthogonal representation of* $\Delta$*, then* $s_E(\rho) \equiv \lambda_E(\rho) \pmod 2$*.*

*Proof.* We assume that $\rho$ is irreducible until the last part of the proof. First of all, by definition, we have $\lambda_E(\rho) = |Orb_\rho| \cdot \lambda_E(\sigma)$. Since $|Orb_\rho|$ is a power of $p$, and hence odd, the second congruence is obvious. Let $t$ be as in proposition 10.1.1 and let $\Delta_t$ denote the image of $\Delta$ in $D_t = \mathrm{Gal}(K_t/F)$. We identify $\Delta$ with $\Delta_t$. Thus, $\Delta_t$ is a normal subgroup of $D_t$ and the order of $D_t/\Delta_t$ is a power of $p$. Consider the representation space $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $D_t$, which we will denote by $\rho'$ in this proof. We know that $\rho'$ is self-dual. Regarding $\rho$ as a representation of $D_t$, it is clear that its multiplicity as a constituent in $\rho'$ is equal to $s_E(\rho)$. According to proposition 9.3.5, we have the congruence

$$s_E(\rho) = \langle \rho,\ \rho' \rangle_{D_t} \equiv \langle \rho|_{\Delta_t},\ \rho'|_{\Delta_t} \rangle_{\Delta_t} \pmod 2 \quad .$$

However, regarding $\sigma$ as a representation of $\Delta_t$, it is an irreducible constituent in $\rho|_{\Delta_t}$ and its orbit under the action of $D_t/\Delta_t$ is just $Orb_\rho$. Also, if $\sigma_1$ and $\sigma_2$ are in that orbit, then one sees easily that $s_E(\sigma_1) = s_E(\sigma_2)$, where these quantities are defined in terms of the action of $\Delta_t$ on $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Thus,

$$\langle \rho|_{\Delta_t},\ \rho'|_{\Delta_t} \rangle_{\Delta_t} = |Orb_\rho| \cdot \langle \sigma,\ \rho'|_{\Delta_t} \rangle_{\Delta_t} \equiv s_E(\sigma) \pmod 2$$

since $|Orb_\rho|$ is odd. Hence $s_E(\rho)$ and $s_E(\sigma)$ have the same parity. We must prove that $s_E(\sigma)$ and $\lambda_E(\sigma)$ also have the same parity.

We now use proposition 10.1.1. Let $W$ be as defined there. Note that since $\rho$ is orthogonal, proposition 9.3.4 implies that $\sigma$ is orthogonal. Consequently, by proposition 9.3.1, the multiplicity of $\sigma$ in the $\Delta$-representation space $W$ is even. Also, $V_{\Gamma_{K_t}}$ is isomorphic to $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ as a representation space for $\Delta$. It follows that $\lambda_E(\sigma)$ has the same parity as the multiplicity of $\sigma$ in $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Therefore, we indeed have

$$\lambda_E(\sigma) \;\equiv\; s_E(\sigma) \qquad (\text{mod } 2)$$

which implies the stated congruence.

For the final statement, the representation $\rho$ is isomorphic to a direct sum of irreducible representations. Symplectic irreducible representations of $D$ must occur with even multiplicity as constituents in $\rho$ by remark 9.3.2. Their contributions to both invariants will therefore be even. The contributions of each orthogonal irreducible constituent to $\lambda_E(\rho)$ and to $s_E(\rho)$ will have the same parity. Any other irreducible constituent $\theta$ in $\rho$ which is not self-dual occurs with the same multiplicity as $\check{\theta}$. According to corollary 10.1.3 and (10.0.a), their total contribution to both $\lambda_E(\rho)$ and to $s_E(\rho)$ will also be even. □

**Remark 10.2.2.** Suppose that $L$ is a finite Galois extension of $F$ of odd degree. Let $\rho$ be a self-dual Artin representation of $G_F$ and let $\rho|_L$ denote its restriction to $G_L$. Then we have the following useful congruences:

$$r_E(\rho|_L) \equiv r_E(\rho) \pmod 2, \qquad s_E(\rho|_L) \equiv s_E(\rho) \pmod 2, \qquad \lambda_E(\rho|_L) \equiv \lambda_E(\rho) \pmod 2 \ .$$

The last congruence makes sense only when the $\lambda$-invariants are defined. Remark 10.2.5 below extends the definition to all cases. For the proofs of the first two congruences, one just uses proposition 9.3.5, taking $\rho'$ to be the self-dual representation space $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. One must take $K$ large enough so that $\rho$ factors through $\mathrm{Gal}(K/F)$ and also so that $L \subseteq K$. One takes $G = \mathrm{Gal}(K/F)$ and $N = \mathrm{Gal}(K/L)$. For the third congruence, one takes $\rho'$ to be the $V$ occurring in proposition 10.1.1 (or in remark 10.2.5), $G = \mathrm{Gal}(K_\infty/F_\infty)$, and $N = \mathrm{Gal}(K_\infty/L_\infty)$ in proposition 9.3.5. ◊

The situation if $\rho$ is symplectic is interesting. The Schur index over $\mathbf{Q}$ for any such $\rho$ is 2. Consequently, it follows that $r_E(\rho)$ is even. Alternatively, if one regards $\rho$ as a representation over $\mathbf{C}$ instead of $\mathcal{F}$, one could use the fact that the canonical height pairing on $E(K) \otimes_{\mathbf{Z}} \mathbf{R}$ is symmetric, nondegenerate and $D$-invariant. One can then apply the analogue of remark 9.3.2 to that representation space, replacing $\mathbf{Q}_p$ by $\mathbf{R}$ and $\mathcal{F}$ by $\mathbf{C}$. Since one expects that

$s_E(\rho) = r_E(\rho)$, it should also be true that $s_E(\rho)$ is even whenever $\rho$ is symplectic. However, this is not known in general. There is a $p$-adic height pairing on the Pontryagin dual $X_E(K)$ of $\mathrm{Sel}_E(K)_p$. It is symmetric and $D$-invariant. It is conjectured to be nondegenerate (modulo the torsion subgroup). If that is so, then we can extend that pairing to a $\mathbf{Q}_p$-bilinear, symmetric, $D$-invariant, nondegenerate pairing on the vector space $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Remark 9.3.2 would then imply that $s_E(\rho)$ is indeed even for every symplectic $\rho \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$. The next proposition shows the same thing for the $\lambda_E(\rho)$'s.

**Proposition 10.2.3.** *Assume that $p$ is odd, that $\mathrm{Sel}_E(K_\infty)_p$ is $\mathbf{Z}_p[[\Gamma_K]]$-cotorsion, and that the $p$-adic height pairing on $\widehat{\mathrm{Sel}_E(K)}_p \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is non-degenerate. Suppose that $\rho$ is a self-dual, irreducible representation of $D$ and that $\sigma$ is an irreducible constituent in $\rho|_\Delta$. Then*

$$s_E(\rho) \;\equiv\; \lambda_E(\rho) \equiv \lambda_E(\sigma) \pmod 2 \quad .$$

*for all $\rho \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$. In particular, if $\rho$ is assumed to be symplectic, then $\lambda_E(\rho)$ is even.*

*Proof.* If we replace the base field $F$ by $F_m = K \cap F_\infty$ and $\rho$ by $\rho|_{F_m}$, then the congruences to be proved are replaced by equivalent congruences. This follows from remark 10.2.2. Thus we can assume at the start that $K \cap F_\infty = F$. Hence, we can write $\Gamma$ instead of $\Gamma_K$ and assume that $G = \Delta \times \Gamma,\ D = \Delta$. Let $X = X_E(K_\infty)$ and let $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, as in proposition 10.1.1. There is a non-degenerate, $\mathbf{Q}_p$-bilinear, $G$-equivariant pairing $V \times V \to \mathbf{Q}_p$. For any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, let $W_\sigma$ denote the underlying $\mathcal{F}$-representation space for $\sigma$. We regard $W_\sigma$ as a representation space for $G$ by letting $\Gamma$ act trivially. Let $V \otimes \sigma$ denote $V \otimes_{\mathbf{Q}_p} W_\sigma$, regarded as an $\mathcal{F}$-representation space for $G$. We will also let $X \otimes \sigma$ denote $X \otimes_{\mathbf{Z}_p} L_\sigma$, where $L_\sigma$ is a $\Delta$-invariant, and hence $G$-invariant, $\mathcal{O}$-lattice in $W_\sigma$. We have a non-degenerate, $\mathcal{F}$-bilinear, $\Delta$-equivariant pairing $W_\sigma \times W_{\check\sigma} \to \mathcal{F}$. The pairing is $G$-equivariant too. Therefore, we get a non-degenerate, $\mathcal{F}$-bilinear, $G$-equivariant pairing $(V \otimes \sigma) \times (V \otimes \check\sigma) \to \mathcal{F}$. We then get a non-degenerate, $\mathcal{F}$-bilinear, $\Gamma$-equivariant pairing on the $\sigma_0$-components:

$$(V \otimes \sigma)^\Delta \;\times\; (V \otimes \check\sigma)^\Delta \;\to\; \mathcal{F} \quad .$$

Note that $(V \otimes \sigma)^\Delta \cong (V \otimes \sigma)_\Delta \cong (X \otimes \sigma)_\Delta \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where the first isomorphism holds because $\Delta$ is finite and acts semisimply on any $\mathcal{F}$-representation space.

Now $(X \otimes \sigma)_\Delta$ is the Pontryagin dual of $\big(\mathrm{Sel}_E(K_\infty)_p \otimes \check\sigma\big)^\Delta$. Let $X_{\check\sigma}$ denote the Pontryagin dual of $\mathrm{Sel}_{E[p^\infty]\otimes\check\sigma}(F_\infty)$ and let $V_{\check\sigma} = X_{\check\sigma} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Using (4.3.b) for $\check\sigma$, we see that

$$(V \otimes \sigma)^\Delta \;\cong\; V_{\check\sigma}$$

as $\mathcal{F}$-representation spaces for $\Gamma$. Proposition 4.3.1 asserts that $\dim_{\mathcal{F}}(V_{\check\sigma}) = \lambda_E(\check\sigma)$. If $\sigma$ and $\check\sigma$ are interchanged, we have a similar isomorphism and so we get a pairing

$$V_{\check\sigma} \;\times\; V_\sigma \;\to\; \mathcal{F} \quad . \tag{10.2.a}$$

which is non-degenerate, $\mathcal{F}$-bilinear, and $\Gamma$-equivariant. If one picks a $\Gamma$-invariant $\mathcal{O}$-lattice in $V_\sigma$, one can regard that lattice as a finitely-generated torsion $\Lambda_\mathcal{O}$-module, where $\Lambda_\mathcal{O} = \mathcal{O}[[\Gamma]]$, and one can define the corresponding characteristic ideal $I_\sigma$. Now let $\iota$ be the involution of $\Gamma$ defined by $\iota(\gamma) = \gamma^{-1}$. This extends to an involution of the ring $\Lambda_\mathcal{O}$, which we also will denote by $\iota$. It is a continuous, $\mathcal{O}$-algebra automorphism of that ring. If $\theta \in \Lambda_\mathcal{O}$, its image under $\iota$ will be denoted by $\theta^\iota$. The pairing (10.2.a) implies that $I_{\check{\sigma}} = I_\sigma^\iota$.

Suppose now that $\sigma \in \mathrm{Irr}_\mathcal{F}^{(sd)}(\Delta)$. Then $V_\sigma$ is self-dual as a representation space for $\Gamma$. Also, the ideal $I_\sigma$ is fixed by $\iota$. A rather easy argument (found in [Gr91], proposition 1) shows that a generator $\theta_{E,\sigma}$ for $I_\sigma$ can be chosen so that

$$\theta_{E,\sigma}/\theta_{E,\sigma}^\iota \ \in \ \{\pm 1\}$$

This requires the assumption that $p$ is odd. The ratio is uniquely determined by $I_\sigma$. We temporarily denote it by $W(E,\sigma)$. Choose a topological generator $\gamma$ for $\Gamma$ and let $T = \gamma - \gamma^{-1}$, a generator for the augmentation ideal in $\Lambda_\mathcal{O}$ satisfying $T^\iota = -T$. Then $\Lambda_\mathcal{O}$ can be identified with the formal power series ring $\mathcal{O}[[T]]$. It then follows that the expansion of $\theta_{E,\sigma}$ requires only even powers of $T$ if $W(E,\sigma) = 1$ and only odd powers of $T$ if $W(E,\sigma) = -1$. In particular, if $T^{m_E(\sigma)}$ is the highest power of $T$ dividing $\theta_{E,\sigma}$ in $\Lambda_\mathcal{O}$, then $W(E,\sigma) = (-1)^{m_E(\sigma)}$. Furthermore, the value of $\lambda_E(\sigma)$ is determined by the first term where the coefficient is a unit in $\mathcal{O}$. Therefore, it follows that $m_E(\sigma) \equiv \lambda_E(\sigma) \pmod 2$. Hence $W(E,\sigma) = W_{Iw_p}(E,\sigma)$ and we have the "functional equation"

$$\theta_{E,\sigma}^\iota \ = \ W_{Iw_p}(E,\sigma) \cdot \theta_{E,\sigma}$$

for each $\sigma \in \mathrm{Irr}_\mathcal{F}^{(sd)}(\Delta)$.

Now it is believed that $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_\infty)[T]\big) = \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_\infty)[T^k]\big)$ for any $k \geq 1$, a kind of semisimplicity statement for the $\Lambda$-module $X_E(K_\infty)$. In fact, Schneider proves in [Sch] that this conjecture is equivalent to the nondegeneracy of the $p$-adic height pairing on $\widehat{\mathrm{Sel}_E(K)}_p$, which he also defined. Thus, we may assume that this is the case. This means that if we view $T$ as an operator on $V$, then $\ker(T) = \ker(T^k)$ for any $k \geq 1$. The same statement will be true when viewing $T$ as an operator on $V_\sigma$. Therefore,

$$m_E(\sigma) \ = \ \dim_\mathcal{F}\big(V_\sigma^\Gamma\big) = \ \dim_\mathcal{F}\big((V_\sigma)_\Gamma\big) \ .$$

The action of $\Delta$ and $\Gamma$ on $V$ commute. Thus, $(V_\sigma)_\Gamma \cong (V_\Gamma \otimes \sigma)^\Delta$. Furthermore, Mazur's control theorem implies that the restriction map $\mathrm{Sel}_E(K)_p \longrightarrow \mathrm{Sel}_E(K_\infty)_p^\Gamma$ has finite kernel and cokernel. This implies that $V_\Gamma \cong X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. It follows that the multiplicities of $\sigma$ in the $\Delta$-representation spaces $V_\Gamma$ and $X_E(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ are equal. That is, $m_E(\sigma) = s_E(\sigma)$. Since we also have $m_E(\sigma) \equiv \lambda_E(\sigma) \pmod 2$, the stated congruence follows. $\square$

**Remark 10.2.4.** A functional equation for a generator of the characteristic ideal of a Selmer group like the one in the above proof first occurs in Mazur's paper [Ma72]. The object of study in [Ma72] is a $\mathbf{Z}_p$-extension $F_\infty/F$ and a $\Lambda$-module closely related to $\mathrm{Sel}_E(F_\infty)_p$. If the $p$-adic height pairing for $E/F$ is non-degenerate, then Mazur's functional equation implies the congruence $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(F)_p\big) \equiv \lambda_E(F_\infty) \pmod 2$. It turns out that one can prove that congruence just under the assumption that $\mathrm{Sel}_E(F_\infty)_p$ is $\Lambda$-cotorsion. Such a proof is given in [Guo]. See also proposition 3.10 in [Gr99]. $\Diamond$

**Remark 10.2.5.** It is not essential to assume that $\mathrm{Sel}_E(K_\infty)_p$ is $\mathbf{Z}_p[[\Gamma_K]]$-cotorsion in proposition 10.1.1 and the parity results. Without that assumption, one has a pseudo-isomorphism

$$X_E(K_\infty) \ \sim \ \mathbf{Z}_p[[\Gamma_K]]^r \ \oplus \ Y_E(K_\infty)$$

as $\mathbf{Z}_p[[\Gamma_K]]$-modules, where $r \geq 0$ and $Y_E(K_\infty)$ denotes the torsion submodule of $X_E(K_\infty)$. We will consider the $\mathbf{Q}_p$-representation space $V = Y_E(K_\infty) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$, which of course coincides with the $V$ in the proposition if $r = 0$. We want to show that $V$ is self-dual. It will be helpful to consider $\mathcal{V} = X_E(K_\infty) \otimes_{\mathbf{Z}_p[[\Gamma_K]]} \mathfrak{L}$, where $\mathfrak{L}$ denotes the fraction field of $\mathbf{Z}_p[[\Gamma_K]]$. Thus, $\mathcal{V}$ is an $\mathfrak{L}$-representation space for $\Delta$ and its dimension is $r$. We will also prove that $\mathcal{V}$ is self-dual. Let $\chi_\mathcal{V}$ denote the character for $\mathcal{V}$. Thus, $\chi_\mathcal{V}$ is a function on $\Delta$. Its values are in $\mathfrak{L}$, but must be algebraic over $\mathbf{Q}_p$, and hence are actually in $\mathbf{Q}_p$ too. This will be clear for a different reason in the next paragraph. A representation space for $\Delta$ over any field of characteristic zero is self-dual if and only if its character $\chi$ has the following property: $\chi(\delta) = \chi(\delta^{-1})$ *for all* $\delta \in \Delta$.

Let $Z_E(K_\infty) = X_E(K_\infty)/Y_E(K_\infty)$, which is a torsion-free $\mathbf{Z}_p[[\Gamma_K]]$-module. It is pseudo-isomorphic to a free $\mathbf{Z}_p[[\Gamma_K]]$-module of rank $r$. We obviously have $\mathcal{V} \cong Z_E(K_\infty) \otimes_{\mathbf{Z}_p[[\Gamma_K]]} \mathfrak{L}$ as $\mathfrak{L}$-representation spaces for $\Delta$. Now $Z_E(K_\infty)_{\Gamma_K}$ is a finitely-generated $\mathbf{Z}_p$-module of rank $r$. The character $\chi_\mathcal{V}$ is precisely the same as the character for the $\mathbf{Q}_p$-representation space $Z_E(K_\infty)_{\Gamma_K} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Thus, we again see that its values are in $\mathbf{Q}_p$. For any $n \geq 0$, let $\phi_n : \Gamma_K \to \mathbf{Q}_p(\mu_{p^n})^\times$ be a homomorphism whose kernel is $\Gamma_{K_n}$. Then $\phi_n$ can be extended to a unique, continuous $\mathbf{Z}_p$-algebra homomorphism $\mathbf{Z}[[\Gamma_K]] \to \mathbf{Z}_p[\mu_{p^n}]$, which we also denote by $\phi_n$. Let $I_n = \ker(\phi_n)$, an ideal in $\mathbf{Z}[[\Gamma_K]]$. We then obtain a representation space $\big(Z_E(K_\infty)/I_n Z_E(K_\infty)\big) \otimes_{\mathbf{Z}_p[\mu_{p^n}]} \mathbf{Q}_p(\mu_{p^n})$ for $\Delta$ of dimension $r$ over $\mathbf{Q}_p(\mu_{p^n})$. If $n = 0$, then this representation space is the same as $Z_E(K_\infty)_{\Gamma_K} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ mentioned above. For any $n \geq 0$, its character is again $\chi_\mathcal{V}$. But viewing it as a $\mathbf{Q}_p$-representation space, the character is $a_n \cdot \chi_\mathcal{V}$, where $a_n = [\mathbf{Q}_p(\mu_{p^n}) : \mathbf{Q}_p]$.

Let $M_n$ be exactly as in the proof of proposition 10.1.1. If $r \geq 1$, then the $\mathbf{Z}_p$-corank of $M_n$ will be unbounded. Define $M_\infty$ to be $\bigcup_n s_n(M_n)$. For any $n \geq 0$, the control theorem

implies that the map

$$s_n : M_n \longrightarrow M_\infty^{\Gamma_n}$$

has finite kernel and that $s_n(M_n)$ is precisely the maximal divisible subgroup of $M_\infty^{\Gamma_n}$. It then follows that the $\mathbf{Z}_p$-corank of $M_n$ is equal to $rp^n + \lambda_0$ for all $n \geq t$, where $t$ is chosen so that $\dim_{\mathbf{Q}_p}(V_{\Gamma_{K_t}})$ is maximal and $\lambda_0$ is that dimension. It also follows that the $\mathbf{Q}_p$-representation spaces

$$X_E(K_n) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \qquad \textit{and} \qquad \big(Z_E(K_\infty)_{\Gamma_{K_n}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p\big) \oplus V_{\Gamma_{K_n}}$$

for $\Delta$ are isomorphic for all $n \geq 0$. Note that $V_{\Gamma_{K_n}}$ stabilizes when $n \geq t$ and its dimension is $\lambda_0$. Also, note that $Z_E(K_\infty)_{\Gamma_{K_n}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is isomorphic to the direct sum of the $\mathbf{Q}_p$-representation spaces $\big(Z_E(K_\infty)/I_m Z_E(K_\infty)\big) \otimes_{\mathbf{Z}_p[\mu_{p^m}]} \mathbf{Q}_p(\mu_{p^m})$ for $\Delta$, where $m$ varies in the range $0 \leq m \leq n$. Thus, the corresponding character is $p^n \chi_{\mathcal{V}}$.

If we use the fact that both $X_E(K_t) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $X_E(K_{t+1}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ are self-dual $\Delta$-representation spaces (using the result in [Dok4]), then we see that $(p^{t+1} - p^t)\chi_{\mathcal{V}}$ is the character of a self-dual representation for $\Delta$, and hence so is $\chi_{\mathcal{V}}$ itself. Thus, $\mathcal{V}$ is indeed a self-dual $\mathfrak{L}$-representation space for $\Delta$. It then follows that $V_{\Gamma_{K_t}}$ is self-dual.

Now define $A_n$ exactly as in the proof of proposition 10.1.1 and let $A_\infty = \mathrm{Sel}_E(K_\infty)_p/M_\infty$. As we've already said, the control theorem implies that $s_n(M_n)$ is the maximal divisible subgroup of $M_\infty^{\Gamma_n}$. It follows that the quotient $M_\infty^{\Gamma_n}/s_n(M_n)$ is finite and has bounded order. This suffices to deduce that the maps $a_n : A_n \to A_\infty$ induced by the $s_n$'s have finite kernel of bounded order. Choose $n$ sufficiently large so that $V_{\Gamma_n}$ stabilizes. The proof that $W = \ker(V \to V_{\Gamma_t})$ has a non-degenerate, skew-symmetric, $G$-invariant pairing is now just as before. We conclude again that $V$ is self-dual.

For any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, we define $\lambda_E(\sigma)$ to be the multiplicity of $\sigma$ in the $\mathbf{Q}_p$-representation space $V$ and $\varpi_E(\sigma)$ to be the multiplicity of $\sigma$ in the $\mathfrak{L}$-representation space $\mathcal{V}$. Of course, in both cases, one may have to extend scalars suitably to define the multiplicity. Since $V$ and $\mathcal{V}$ are both self-dual, we have

$$\lambda_E(\check{\sigma}) = \lambda_E(\sigma), \qquad \textit{and} \qquad \varpi_E(\check{\sigma}) = \varpi_E(\sigma)$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Also, if $\rho$ is an irreducible representation of $\mathrm{Gal}(K/F)$, then one can also define $\lambda_E(\rho)$ and $\varpi_E(\rho)$ in terms of $\rho|_\Delta$. As in corollary 10.1.3, one finds the same equalities.

The above argument is valid even if $p = 2$. We will now assume that $p$ is odd. One can prove a congruence like the one in proposition 10.2.1 even if one omits the assumption that $\mathrm{Sel}_E(K_\infty)_p$ is $\mathbf{Z}_p[[\Gamma_K]]$-cotorsion, namely that

$$s_E(\sigma) \equiv \lambda_E(\sigma) + \varpi_E(\sigma) \pmod 2 \tag{10.2.b}$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ which are orthogonal. This follows easily from the earlier comments in this remark. One uses the fact that the multiplicity of $\sigma$ in $Z_E(K_\infty)_{\Gamma_{K_n}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is $p^n \varpi_E(\sigma)$, which has the same parity as $\varpi_E(\sigma)$. Furthermore, if $\rho$ is a self-dual, orthogonal, irreducible representation of $\mathrm{Gal}(K/F)$, then we obtain the same congruence. $\Diamond$

# 11 $p$-modular functions.

Suppose that $f : \mathcal{R}_{\mathcal{F}}(\Delta) \longrightarrow A$ is a group homomorphism, where $A$ is an abelian group. Such a homomorphism is determined by specifying $a_\sigma = f(\sigma) \in A$ for each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$. Since $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ is a basis for $\mathcal{R}_{\mathcal{F}}(\Delta)$, the $a_\sigma$'s in $A$ can be specified arbitrarily. If $\rho$ is an arbitrary representation of $\Delta$ over $\mathcal{F}$, then

$$f(\rho) \;=\; \prod_{\sigma} a_\sigma^{m_\rho(\sigma)}$$

where $m_\rho(\sigma)$ denotes the multiplicity of $\sigma$ in $\rho$, the product varies over $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, and we are using a multiplicative notation for $A$. As previously, we let $\mathrm{Rep}_{\mathcal{F}}(\Delta)$ denote the set of representations for $\Delta$ over $\mathcal{F}$.

**Definition.** We will say that $f$ is *$p$-modular* if the following statement is true: *If* $\rho_1,\ \rho_2 \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$ *and* $\widetilde{\rho_1}^{ss} \cong \widetilde{\rho_2}^{ss}$, *then* $f(\rho_1) = f(\rho_2)$ .

Equivalently, $f$ is $p$-modular means that $f$ factors through the decomposition homomorphism $d : \mathcal{R}_{\mathcal{F}}(\Delta) \to \mathcal{R}_{\mathfrak{f}}(\Delta)$. This means that one can define a homomorphism $g : \mathcal{R}_{\mathfrak{f}}(\Delta) \to A$ such that $f = g \circ d$. One then has the formula

$$f(\sigma) \;=\; \prod_{\tau} g(\tau)^{d(\sigma,\tau)}$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, where the product varies over all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

One type of example is the following. Suppose that $X$ is a finitely generated $\mathbf{Z}_p[\Delta]$-module. We can define a homomorphism $f = \lambda_X$ as in the introduction and chapter 2. Proposition 2.1.5 is just the assertion that $f$ is $p$-modular if and only if $X$ is quasi-projective.

## 11.1 Basic examples of $p$-modular functions.

We now describe some very simple examples of $p$-modular functions which will turn out to be useful in chapter 12. In addition to defining $f$, we will also give the corresponding $g$. We

specify $f$ by giving $f(\rho)$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$ and $g$ by just giving the values $g(\tau)$ for all $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

**11.1.1.** Suppose that $a \in A$. Define $f$ by $f(\rho) = a^{n(\rho)}$. Define $g$ by $g(\tau) = a^{n(\tau)}$.

**11.1.2.** For any representation $\rho$ of $\Delta$ over $\mathcal{F}$, $det(\rho)$ is a 1-dimensional representation of $\Delta$ over $\mathcal{F}$. If $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$, then $det(\tau)$ is a 1-dimensional representation of $\Delta$ over $\mathfrak{f}$. Suppose that $A$ is a group of roots of unity in $\mathcal{F}$ of order prime to $p$ and that $det(\rho)$ has values in $A$ for all $\rho$. Suppose that $\delta \in \Delta$. Define $f$ by $f(\rho) = det(\rho)(\delta)$. To define the corresponding function $g$, note that the reduction modulo $\mathfrak{m}$ defines an isomorphism $\iota : A \longrightarrow \widetilde{A}$, where $\widetilde{A}$ is a subgroup of $\mathfrak{f}^{\times}$. Also, one can show that $det(\tau)$ has values in $\widetilde{A}$. This can be proved by using the fact that the decomposition map $d : \mathcal{R}_{\mathcal{F}}(\Delta) \longrightarrow \mathcal{R}_{\mathfrak{f}}(\Delta)$ is surjective. We can define $g$ by $g(\tau) = \iota^{-1}\big(det(\tau)(\delta)\big)$. This works because $\widetilde{det(\rho)} = det(\widetilde{\rho}^{ss})$.

**11.1.3.** Suppose that $\Delta_*$ is any subgroup of $\Delta$ and that $\vartheta$ is some fixed element of $\mathrm{Irr}_{\mathfrak{f}}(\Delta_*)$. If $\rho \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$, let $\rho_*$ denote $\rho|_{\Delta_*}$. Then we obtain a semisimple representation $\widetilde{\rho_*}^{ss}$ of $\Delta_*$ over $\mathfrak{f}$ by reduction modulo $\mathfrak{m}$. Let $A$ be the additive group $\mathbf{Z}$. Define $f$ by letting $f(\rho)$ be the multiplicity of $\vartheta$ in $\widetilde{\rho_*}^{ss}$. Define $g$ by letting $g(\tau)$ be the multiplicity of $\vartheta$ in $\tau_* = \tau|_{\Delta_*}$.

**11.1.4.** Suppose that $\Delta_*$ is a subgroup of $\Delta$ of order prime to $p$. Let $A$ be any group and let $f_* : \mathcal{R}_{\mathcal{F}}(\Delta_*) \longrightarrow A$ be any homomorphism whatsoever. We again let $\rho_*$ denote $\rho|_{\Delta_*}$ for any $\rho \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$. Define $f$ by $f(\rho) = f_*(\rho_*)$. Then $f$ is $p$-modular and one can take $g$ to be defined by $g(\tau) = f_*\big(d_*^{-1}(\tau_*)\big)$. Here we use the fact that the decomposition map $d_* : \mathcal{R}_{\mathcal{F}}(\Delta_*) \longrightarrow \mathcal{R}_{\mathfrak{f}}(\Delta_*)$ is an isomorphism because $p \nmid |\Delta_*|$. The map $d_*^{-1}$ is the inverse map to $d_*$ and $\tau_*$ denotes $\tau|_{\Delta_*}$ for any $\tau \in \mathrm{Irr}_{\mathfrak{f}}(\Delta)$.

The term $p$-modular will also be used in the following context. As in the introduction, we let $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ denote the set of irreducible, self-dual representations of $\Delta$ over $\mathcal{F}$. Let $\mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta)$ denote the subgroup of $\mathcal{R}_{\mathcal{F}}(\Delta)$ generated by self-dual representations. Thus, $\mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta)$ is a free $\mathbf{Z}$-module with basis consisting of *(i)* all $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ together with *(ii)* all elements of the form $\sigma \oplus \check{\sigma}$, where $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, but $\sigma$ is not self-dual. One makes similar definitions for representations over $\mathfrak{f}$: a subset $\mathrm{Irr}_{\mathfrak{f}}^{(sd)}(\Delta)$ of $\mathrm{Irr}_{\mathfrak{f}}(\Delta)$ and a subgroup $\mathcal{R}_{\mathfrak{f}}^{(sd)}(\Delta)$ of $\mathcal{R}_{\mathfrak{f}}(\Delta)$. We let $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$ denote the set of self-dual elements of $\mathrm{Rep}_{\mathcal{F}}(\Delta)$.

Now suppose that $f : \mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta) \longrightarrow A$ is a group homomorphism, where $A$ is an abelian group. Such a homomorphism is determined by specifying $f(\sigma) \in A$ for each $\sigma$ in $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(\Delta)$ and $f(\sigma \oplus \check{\sigma})$ for all other $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}(\Delta)$. Often, one simply defines $f(\sigma \oplus \check{\sigma}) = id_A$ for the non-self-dual $\sigma$'s. We can restrict the decomposition homomorphism $d$ to the subgroup $\mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta)$ obtaining a homomorphism $d^{(sd)}$ from that group to $\mathcal{R}_{\mathfrak{f}}^{(sd)}(\Delta)$. We will say that $f$ is $p$-modular if it factors through $d^{(sd)}$. This means that there is a homomorphism $g : \mathcal{R}_{\mathfrak{f}}^{(sd)}(\Delta) \longrightarrow A$

such that $f = g \circ d^{(sd)}$. An equivalent characterization is just as in the definition given above, but restricting $\rho_1$ and $\rho_2$ to be self-dual representations.

## 11.2 Some $p$-modular functions involving multiplicities.

The above group-theoretic observations will be useful in chapter 12. However, the arguments in that chapter will require a more subtle ingredient which involves the parities of certain multiplicities. We now consider the following arithmetic situation. As in chapter 5, let $\mathcal{G}_v = G_{F_{\infty,v}}$, where $v$ is a non-archimedean prime of $F$ not lying over $p$. Let $\varphi$ be an absolutely irreducible representation of $\mathcal{G}_v$. We are primarily interested in the $\varphi$'s for which $\langle \rho_{E,v}, \varphi \rangle > 0$. Depending on the reduction type, such a $\varphi$ is usually one-dimensional and of order relatively prime to $p$. We will first study that case. The decomposition subgroup $\Delta_v$ of $\Delta$ is a quotient of $\mathcal{G}_v$. If $\rho \in \mathrm{Rep}_{\mathcal{F}}(\Delta)$, we let $\rho_v$ denote the restriction $\rho|_{\Delta_v}$, regarded also as a representation of $\mathcal{G}_v$. The multiplicity $\langle \rho_v, \varphi \rangle$ will play an important role and our approach to studying it is to relate it to the multiplicity $\langle \widetilde{\rho}_v^{ss}, \widetilde{\varphi} \rangle$. We assume throughout this chapter and the next that $p \geq 3$. Here is one result that we will need.

**Proposition 11.2.1.** *Suppose that $\varphi$ and $\psi$ are characters of $\mathcal{G}_v$ of order prime to $p$ and that $\varphi\psi = \omega_v^j$ for some integer $j$. Define a homomorphism*

$$f : \mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta) \longrightarrow \{\pm 1\}$$

*by $f(\rho) = (-1)^{\langle \rho_v, \varphi \rangle + \langle \rho_v, \psi \rangle}$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$. Then $f$ is $p$-modular.*

If $\Delta_v$ has order prime to $p$, then this result is quite obvious. For if $\chi$ is any irreducible constituent in $\rho_v$, then $\langle \chi, \varphi \rangle \leq 1$ and equality simply means that $\chi \cong \varphi$, and that is equivalent to $\widetilde{\chi} = \widetilde{\varphi}$. However, if $|\Delta_v|$ is divisible by $p$ (i.e., if $v \in \Phi_{K/F}$), then it is possible to have $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle \geq 1$ even if $\chi \not\cong \varphi$. The proof of the proposition requires studying the difference $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle - \langle \chi, \varphi \rangle$. A crucial role in the proof is played by the set

$$\Xi = \{ \xi \mid \langle \widetilde{\xi}^{ss}, \widetilde{\xi}_0 \rangle \geq 1 \} ,$$

where the $\xi$'s are assumed to be absolutely irreducible representations of $\mathcal{G}_v$ and $\xi_0$ is the trivial representation.

The next lemma shows that $\Xi$ is an infinite set which can be described completely. We use the notation from the beginning of section 8.2. Thus, $\mathcal{M}_v$ is a normal subgroup of $\mathcal{G}_v$, the kernel of $\omega_v$. We have $w_v = [\mathcal{G}_v : \mathcal{M}_v]$. We also consider the unique subgroup $\mathcal{J}_v$ of $\mathcal{M}_v$ characterized by the isomorphism $\mathcal{M}_v/\mathcal{J}_v \cong \mathbf{Z}_p$. Then $\mathcal{J}_v$ is also a normal subgroup of $\mathcal{G}_v$ and

has profinite order prime to $p$. Furthermore, the natural action (by inner automorphisms) of $\mathcal{G}_v/\mathcal{M}_v$ on $\mathcal{M}_v/\mathcal{J}_v$ is given by the character $\omega_v$. Thus, we will write $\mathcal{M}_v/\mathcal{J}_v \cong \mathbf{Z}_p(1)$. This action is faithful. The group $\mathcal{G}_v/\mathcal{M}_v$ also acts faithfully on the Pontryagin dual of $\mathcal{M}_v/\mathcal{J}_v$. Consequently, one sees easily that if $\pi$ is any nontrivial character of $\mathcal{M}_v/\mathcal{J}_v$, then the orbit of $\pi$ under the action of $\mathcal{G}_v/\mathcal{M}_v$ will have length $w_v$. For any such $\pi$, it turns out that $\xi = \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$ is in $\Xi$. We include the easy verification of that fact in the proof of the following lemma. The trivial character $\xi_0$ of $\mathcal{G}_v$ is clearly in $\Xi$. The following lemma is valid for any prime $p$.

**Lemma 11.2.2.** *The nontrivial elements of $\Xi$ are of the form $\xi = \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$ for some nontrivial character $\pi$ of $\mathcal{M}_v$ factoring through $\mathcal{M}_v/\mathcal{J}_v$. The isomorphism class of $\xi$ depends just on the orbit of $\pi$ under the action of $\mathcal{G}_v/\mathcal{M}_v$. We have $\xi \otimes \omega_v \cong \xi$ for any nontrivial element of $\Xi$. Furthermore, we have $\langle \widetilde{\xi}^{ss}, \widetilde{\xi}_0 \rangle = 1$ for all $\xi \in \Xi$.*

*Proof.* We recall an easily proved result about induced representations. Suppose that $\mathcal{M}$ is a normal subgroup of a group $\mathcal{G}$ and has finite index. Let $w = [\mathcal{G} : \mathcal{M}]$. Suppose that $\psi$ is an absolutely irreducible representation of $\mathcal{M}$. If $g \in \mathcal{G}$, then the inner automorphism of $\mathcal{G}$ defined by $g$, restricted to $\mathcal{M}$, is an automorphism of $\mathcal{M}$. Composing $\psi$ with that automorphism of $\mathcal{M}$ gives another absolutely irreducible representation of $\mathcal{M}$ which depends (up to isomorphism) only on the coset $g\mathcal{M}$. Thus, one obtains absolutely irreducible representations $\psi_1, ..., \psi_w$ of $\mathcal{M}$. Then

$\mathrm{Ind}_{\mathcal{M}}^{\mathcal{G}}(\psi)$ *is an absolutely irreducible representation of $\mathcal{G}$ if and only if $\psi_1, ..., \psi_w$ are mutually non-isomorphic representations of $\mathcal{M}$.*

It follows that $\xi = \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$ is an absolutely irreducible representation of $\mathcal{G}_v$ if $\pi$ is a nontrivial character of $\mathcal{M}_v$ factoring through $\mathcal{M}_v/\mathcal{J}_v$. The dimension of this representation is $w_v$. If $\pi_0$ denotes the trivial representation of $\mathcal{M}_v$, then $\mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi_0)$ also has dimension $w_v$, but is isomorphic to the regular representation of $\mathcal{G}_v/\mathcal{M}_v$, a direct sum of the 1-dimensional representations $\omega_v^j$, $0 \le j \le w_v$-1. This is reducible if $w_v > 1$. Since $\widetilde{\pi} \cong \widetilde{\pi}_0$, the trivial representation of $\mathcal{M}_v/\mathcal{J}_v$ over $\mathfrak{f}$, it follows that $\widetilde{\xi}^{ss}$ is just the regular representation of $\mathcal{G}_v/\mathcal{M}_v$ over $\mathfrak{f}$, which is semisimple. That is, we have

$$\widetilde{\xi}^{ss} \cong \bigoplus_{j=0}^{w_v\text{-}1} \widetilde{\omega_v}^j \tag{11.2.a}$$

and so $\langle \widetilde{\xi}^{ss}, \widetilde{\xi}_0 \rangle = 1$ since the characters $\widetilde{\omega_v}^j$ for $0 \le j < w_v$ are all distinct. Hence, $\xi \in \Xi$. For $\xi = \xi_0$, it is obvious that $\langle \widetilde{\xi}^{ss}, \widetilde{\xi}_0 \rangle = 1$, and so $\xi_0 \in \Xi$.

We next prove that each nontrivial $\xi \in \Xi$ is induced from some $\pi$. First we show that if $\xi \in \Xi$, then $\mathcal{J}_v \subseteq ker(\xi)$. Now $\mathcal{J}_v$ is a normal subgroup of $\mathcal{G}_v$ and has profinite order relatively prime to $p$. Therefore the restriction $\xi|_{\mathcal{J}_v}$ factors through a finite quotient group of $\mathcal{J}_v$ of order prime to $p$. Since $\xi$ is absolutely irreducible, that restriction is isomorphic to a direct sum of irreducible representations of $\mathcal{J}_v$ over $\mathcal{F}$, all of which are conjugate under the action of $\mathcal{G}_v/\mathcal{J}_v$. Their reductions modulo $\mathfrak{m}$ remain irreducible. Since $\widetilde{\xi}$ is assumed to have $\widetilde{\xi_0}$ as a composition factor, $\widetilde{\xi}|_{\mathcal{J}_v}$ must have $\widetilde{\xi_0}|_{\mathcal{J}_v}$ as a direct summand. It follows that one and hence all of the irreducible constituents of $\xi|_{\mathcal{J}_v}$ are trivial and therefore $ker(\xi)$ indeed contains $\mathcal{J}_v$. Thus, $\xi$ factors through $\mathcal{G}_v/\mathcal{J}_v$.

Since $\mathcal{M}_v/\mathcal{J}_v$ is abelian, $\xi|_{\mathcal{M}_v}$ is a direct sum of 1-dimensional characters, all conjugate under the action of $\mathcal{G}_v/\mathcal{M}_v$. If $\pi$ is one of them, then $\xi$ is a direct summand of $\mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$. If $\pi \neq \pi_0$, then that induced representation is absolutely irreducible and therefore we have $\xi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$. If $\pi = \pi_0$, then the induced representation is isomorphic to the direct sum of all of the distinct 1-dimensional representations of $\mathcal{G}_v/\mathcal{M}_v$, only one of which is in $\Xi$, namely $\xi_0$. Thus, $\xi = \xi_0$ in that case. The first assertion in the lemma is proved. The second assertion is clear. For the third assertion, note that $\xi \otimes \omega_v \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi \otimes \omega_v|_{\mathcal{M}_v})$. Since $\omega_v|_{\mathcal{M}_v}$ is trivial and 1-dimensional, we have $\xi \otimes \omega_v \cong \xi$. The final statement is a consequence of (11.2.a). $\square$

The next three lemmas follow from Lemma 11.2.2 and are needed to prove proposition 11.2.1. The first two are almost immediate. Note that if $\xi$ is an absolutely irreducible representation of $\mathcal{G}_v$ and $\chi = \xi \otimes \varphi$, where $\varphi$ is a character of $\mathcal{G}_v$ of order prime to $p$, then $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = \langle \widetilde{\xi}^{ss}, \widetilde{\xi}_0^{ss} \rangle$. Hence $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle$ is positive if and only if $\xi \in \Xi$.

**Lemma 11.2.3.** *Assume that $\varphi$ is a character of $\mathcal{G}_v$ which has order prime to $p$. Assume that $\chi$ is an irreducible representation of $\mathcal{G}_v$. Then $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = 1$ if $\chi \cong \xi \otimes \varphi$ for some $\xi \in \Xi$. If $\chi$ doesn't have that form, then $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = 0$.*

**Lemma 11.2.4.** *Assume that $\varphi$ is a character of $\mathcal{G}_v$ which has order prime to $p$. Assume that $\chi \cong \xi \otimes \varphi$ for some nontrivial $\xi \in \Xi$. Then $\chi \otimes \omega_v \cong \chi$. Furthermore, $\langle \widetilde{\chi}^{ss}, \widetilde{\omega_v}^j \widetilde{\varphi} \rangle = 1$ for all integers $j$.*

**Lemma 11.2.5.** *Suppose that $\varphi$ and $\psi$ are as in the proposition and that $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$. Then $\langle \widetilde{\rho_v}^{ss}, \widetilde{\varphi} \rangle - \langle \rho_v, \varphi \rangle = \langle \widetilde{\rho_v}^{ss}, \widetilde{\psi} \rangle - \langle \rho_v, \psi \rangle$.*

*Proof of lemma 11.2.5.* The restriction $\rho_v$ is still self-dual. We write

$$\rho_v \ \cong \ \bigoplus_{\chi} \chi^{m(\chi)}$$

where $\chi$ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ and $m(\chi) = \langle \rho_v, \chi \rangle$. Since $\rho$ is assumed to be self-dual, we have $m(\check{\chi}) = m(\chi)$, where $\check{\chi}$ denotes the contragredient of $\chi$. For any character $\varphi$ of order prime to $p$, we have

$$\langle \widetilde{\rho_v}^{ss}, \widetilde{\varphi} \rangle - \langle \rho_v, \varphi \rangle = \sum_{\chi \neq \varphi} m(\chi) \langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle \quad .$$

A similar formula is valid for $\psi$. If $\chi$ factors through a quotient group of $\Delta_v$ of order prime to $p$, then $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle \neq 0$ if and only if $\chi = \varphi$. Thus, we can consider the above sum as a sum over all $\chi$'s which do not factor through such a quotient group. We denote that subset of $\mathrm{Irr}_{\mathcal{F}}(\Delta_v)$ by $J_v$ in this proof. The only nonzero contribution comes from $\chi$'s of the form $\chi = \xi \otimes \varphi$, where $\xi$ is a nontrivial element of $\Xi$. For each such term, we have $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = 1$.

As $\chi$ varies over $J_v$, so does $\check{\chi}$. Note that if $\chi = \xi \otimes \varphi$ as above, then $\check{\xi}$ is also a nontrivial element of $\Xi$ and $\check{\chi} \cong \check{\xi} \otimes \varphi^{-1}$. One then has $\langle \widetilde{\check{\chi}}, \widetilde{\varphi^{-1}} \rangle = 1$. By lemma 11.2.4, we have $\langle \widetilde{\check{\chi}}^{ss}, \widetilde{\omega_v^j \varphi^{-1}} \rangle = 1$. Since $\psi = \omega_v^j \varphi^{-1}$, it follows that $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = \langle \widetilde{\check{\chi}}^{ss}, \widetilde{\psi} \rangle$ for all $\chi \in J_v$. The equality stated in the lemma follows from these observations. $\square$

*Proof of proposition 11.2.1.* We use lemma 11.2.5 in the weaker form of a congruence

$$\langle \rho_v, \varphi \rangle + \langle \rho_v, \psi \rangle \equiv \langle \widetilde{\rho_v}^{ss}, \widetilde{\varphi} \rangle + \langle \widetilde{\rho_v}^{ss}, \widetilde{\psi} \rangle \pmod 2. \tag{11.2.b}$$

under the assumptions in the proposition. Consequently, we have

$$f(\rho) \;=\; (-1)^{\langle \widetilde{\rho_v}, \widetilde{\varphi} \rangle + \langle \widetilde{\rho_v}, \widetilde{\psi} \rangle} \quad .$$

To finish the proof, it is sufficient to note that the function $f_\vartheta : \mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta) \to \mathbf{Z}$ defined by $f(\rho) = \langle \widetilde{\rho_v}, \widetilde{\vartheta} \rangle$ is $p$-modular for $\vartheta = \widetilde{\varphi}$ or $\vartheta = \widetilde{\psi}$. This follows immediately from 11.1.3, where we take $\Delta_* = \Delta_v$. $\square$

As one example where the hypotheses in proposition 11.2.1 are satisfied, suppose that $E$ has good reduction at $v$. One can then take $\varphi = \phi_v$ and $\psi = \psi_v$. We have $\varphi_v \psi_v = \omega_v$. More generally, one can just assume that $E$ has potentially good reduction at $v$, that $\rho_{E,v}(\mathcal{G}_v)$ is abelian, and that $\varphi_v$ and $\psi_v$ are the 1-dimensional constituents in $\rho_{E,v}$.

**Remark 11.2.6.** The assumption that $\varphi$ and $\psi$ have order prime to $p$ is not needed in the above proposition and lemmas. The proposition is trivial if $\varphi$, and therefore $\psi$, have order divisible by $p$. In that case, $F_{\infty,v}$ would have a cyclic extension with ramification index divisible by $p$. By local class field theory (or ramification theory), this is only possible if $F_{\infty,v}$ contains $\mu_p$. This means that $\omega_v$ is trivial. Hence $\psi = \varphi^{-1}$ and any self-dual representation $\rho_v$ contains both $\varphi$ and $\psi$ with equal multiplicity, and therefore $f(\rho) = 1$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$.

Also, the multiplicities of $\widetilde{\varphi}$ and $\widetilde{\psi}$ in $\widetilde{\rho}_v$ are equal and hence lemma 11.2.5 is still valid. One also sees easily that lemmas 11.2.3 and 11.2.4 still hold. $\Diamond$

We will use some additional properties of the representations in $\Xi$. First note that if $\xi \in \Xi$, then $\xi|_{\mathcal{M}_v}$ is a direct sum of distinct characters of $\mathcal{M}_v/\mathcal{J}_v$, the characters in one orbit under the action of $\mathcal{G}_v/\mathcal{M}_v$. If $\xi \neq \xi_0$, then the orbit has cardinality $w_v$. If $\pi$ is in that orbit, then $\pi \neq \pi_0$ and $\xi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$. If we assume that $p$ is odd, then that orbit contains $\pi^{-1}$ if and only if $w_v$ is even. Hence if $\xi$ is a nontrivial element of $\Xi$, and $p$ is odd, then $\xi$ is self-dual if and only if $w_v$ is even. We can now prove the following proposition concerning two-dimensional $\varphi$'s.

**Proposition 11.2.7.** *Suppose that $\varphi$ is an irreducible representation of $\mathcal{G}_v$ of dimension 2, that $im(\varphi)$ is finite and of order prime to $p$, and that $p$ is odd. Define a homomorphism*

$$f_\varphi : \mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta) \longrightarrow \{\pm 1\}$$

*by $f_\varphi(\rho) = (-1)^{\langle \rho_v, \varphi \rangle}$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$. Then:*

*(i) If $w_v$ is odd and $\check{\varphi} \cong \varphi \otimes \omega_v^j$ for some integer $j$, then $f_\varphi$ is $p$-modular. This is also valid if $\varphi$ is 1-dimensional.*

*(ii) If $w_v$ is divisible by 4, $\varphi|_{\mathcal{M}_v}$ is reducible, and $det(\varphi) = \omega_v^j$ for some integer $j$, then $f_\varphi$ is $p$-modular.*

*(iii) If $\psi = \varphi \otimes \omega_v^j$ for some integer $j$, then $f_\varphi f_\psi$ is $p$-modular.*

*Proof.* For *(i)* and *(ii)*, we will prove the congruence

$$\langle \rho_v, \varphi \rangle \equiv \langle \widetilde{\rho}_v, \widetilde{\varphi} \rangle \pmod 2$$

which together with 11.1.3 implies that $f_\varphi$ is $p$-modular. Note that $\widetilde{\varphi}$ is an irreducible representation of $\mathcal{G}_v$. To establish the congruence, it suffices to show that if $\chi$ is an irreducible constituent in $\rho_v$ and $\chi \ncong \varphi$, then: *(a)* $\check{\chi} \ncong \chi$ and *(b)* the multiplicities of $\widetilde{\varphi}$ in $\widetilde{\chi}^{ss}$ and in $\widetilde{\check{\chi}}^{ss}$ are the same. The contributions of those multiplicities to $\langle \widetilde{\rho}_v, \widetilde{\varphi} \rangle - \langle \rho_v, \varphi \rangle$ will then be even. We will need the following lemma which will play the same role as lemma 11.2.3.

**Lemma 11.2.8.** *Assume that $\varphi$ is as in proposition 11.2.7, that $\chi$ is an irreducible representation of $\mathcal{G}_v$, that $\chi \ncong \varphi$, and that $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle \geq 1$. If $\varphi|_{\mathcal{M}_v}$ is irreducible, then $\chi \cong \xi \otimes \varphi$ for some nontrivial $\xi \in \Xi$. If $\varphi|_{\mathcal{M}_v}$ is reducible, then $\chi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi\alpha)$ where $\alpha$ is a character of $\mathcal{M}_v$ which occurs as a constituent in $\varphi|_{\mathcal{M}_v}$ and $\pi$ is a nontrivial character of $\mathcal{M}_v$ of $p$-power order.*

We remark that one can have $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = 2$. One has $\widetilde{\omega_v}^j \widetilde{\varphi} \cong \widetilde{\varphi}$ if and only if $\omega_v^j \varphi \cong \varphi$. Such an isomorphism can happen for one or two values of $j$.

*Proof of lemma 11.2.8.* If $\varphi|_{\mathcal{M}_v}$ is irreducible, then so is $\varphi|_{\mathcal{J}_v}$. This is so because $im(\varphi)$ has order prime to $p$ and hence $\varphi(\mathcal{J}_v) = \varphi(\mathcal{M}_v)$. Assume that $\chi$ is an irreducible representation of $\mathcal{G}_v$ such that $\widetilde{\chi}^{ss}$ has $\widetilde{\varphi}$ as a summand. The same thing is true for their restrictions to $\mathcal{J}_v$, which has profinite order prime to $p$. It follows that $\varphi|_{\mathcal{J}_v}$ is a constituent in $\chi|_{\mathcal{J}_v}$. Consequently, there exists a subgroup $\mathcal{N}_v$ of $\mathcal{M}_v$ such that $\mathcal{J}_v \subset \mathcal{N}_v$, $[\mathcal{M}_v : \mathcal{N}_v]$ is finite, and $\varphi|_{\mathcal{N}_v}$ is a constituent in $\chi|_{\mathcal{N}_v}$. Frobenius reciprocity implies that $\chi|_{\mathcal{M}_v}$ and $\mathrm{Ind}_{\mathcal{N}_v}^{\mathcal{M}_v}(\varphi|_{\mathcal{N}_v})$ have an irreducible constituent in common. Now $\mathcal{M}_v/\mathcal{N}_v$ is cyclic of $p$-power order. Therefore, $\mathrm{Ind}_{\mathcal{N}_v}^{\mathcal{M}_v}(\varphi|_{\mathcal{N}_v})$ is a direct sum of the representations $\varphi|_{\mathcal{M}_v} \otimes \pi$, where $\pi$ varies over the characters of $\mathcal{M}_v/\mathcal{N}_v$, and one of those representations is a constituent in $\chi|_{\mathcal{M}_v}$. Frobenius reciprocity then implies that $\chi$ is a direct summand in $\mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi \otimes \varphi|_{\mathcal{M}_v}) = \xi \otimes \varphi$, where $\xi = \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi)$. If $\pi$ is nontrivial, then $\xi$ is irreducible, and so we then indeed have $\chi \cong \xi \otimes \varphi$ for some $\xi \in \Xi$. To see that $\pi \neq \pi_0$, note that $\mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi_0) \otimes \varphi$ is isomorphic to the direct sum of the representations $\omega_v \otimes \varphi$. If $\chi$ is one of the direct summands, then $|im(\chi)|$ is prime to $p$. Hence $\chi \ncong \varphi$ implies that $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle = 0$.

The argument when $\varphi|_{\mathcal{M}_v}$ is reducible is quite similar. One sees that for one of the irreducible constituents $\alpha$ in $\varphi|_{\mathcal{M}_v}$, and for some character $\pi$ of $\mathcal{M}_v/\mathcal{J}_v$, the character $\pi\alpha$ of $\mathcal{M}_v$ is a constituent in $\chi|_{\mathcal{M}_v}$. Therefore, $\chi$ is a constituent in $\mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi\alpha)$ for some character $\pi$ of $\mathcal{M}_v/\mathcal{J}_v$. Again, $\pi \neq \pi_0$ since $\chi \ncong \varphi$. □

For the proof of part *(i)* of proposition 11.2.7, we first note that since $\varphi$ has dimension 2 and $[\mathcal{G}_v : \mathcal{M}_v]$ is odd, it follows that $\varphi|_{\mathcal{M}_v}$ is irreducible. Hence, if $\langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle \geq 1$, then $\chi \cong \xi \otimes \varphi$ for some $\xi \in \Xi$. If $\xi \neq \xi_0$, we then have

$$\check{\chi} \;\cong\; \check{\xi} \otimes \check{\varphi} \;\cong\; \check{\xi} \otimes \omega_v^j \otimes \varphi \;\cong\; \check{\xi} \otimes \varphi \quad ,$$

where the last isomorphism follows from lemma 11.2.2 since $\check{\xi} \in \Xi$. Assuming $\xi \neq \xi_0$, the irreducible constituents of both $\widetilde{\chi}^{ss}$ and $\widetilde{\check{\chi}}^{ss}$ will be the irreducible representations $\widetilde{\varphi} \otimes \widetilde{\omega_v}^i$, where $0 \leq i < w_v$. Hence, we have $\langle \widetilde{\check{\chi}}^{ss}, \widetilde{\varphi} \rangle = \langle \widetilde{\chi}^{ss}, \widetilde{\varphi} \rangle$. This proves assertion *(b)*. To prove *(a)*, note that $\chi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi \otimes \varphi|_{\mathcal{M}_v})$ and $\check{\chi} \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi^{-1} \otimes \varphi|_{\mathcal{M}_v})$ for some nontrivial character $\pi$ of $\mathcal{M}_v/\mathcal{J}_v$. Also, since $im(\varphi)$ has order prime to $p$, the isomorphism class of $\pi \otimes \varphi|_{\mathcal{M}_v}$ determines $\pi$. Since conjugation by elements of $\mathcal{G}_v/\mathcal{M}_v$ obviously fixes $\varphi|_{\mathcal{M}_v}$ and the orbit of $\pi$ doesn't contain $\pi^{-1}$, it follows that indeed $\check{\chi} \ncong \chi$.

For part *(ii)*, lemma 11.2.8 implies that if $\langle \widetilde{\chi}, \widetilde{\varphi} \rangle \geq 1$ and $\chi \ncong \varphi$, then $\chi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi\alpha)$, where $\alpha$ is one of the two constituents in $\varphi_{\mathcal{M}_v}$. Since $det(\varphi)|_{\mathcal{M}_v}$ is trivial, the other constituent is $\alpha^{-1}$. One sees easily that $\alpha^{-1} \neq \alpha$. Now $\check{\chi} \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi^{-1}\alpha^{-1})$. To show that $\check{\chi} \ncong \chi$, it is enough to show that $\pi\alpha$ and $\pi^{-1}\alpha^{-1}$ are not in the same orbit under the action (by conjugation)

of $\mathcal{G}_v/\mathcal{M}_v$. It is the assumption that $4|w_v$ which implies this. The isomorphism class of $\pi\alpha$, or of $\pi^{-1}\alpha^{-1}$, determines both $\pi$ and $\alpha$ since the order of $\alpha$ is prime to $p$. Now $\mathcal{G}_v/\mathcal{M}_v$ is cyclic and the action on the orbit $\{\alpha, \alpha^{-1}\}$ is through the unique quotient group of $\mathcal{G}_v/\mathcal{M}_v$ of order 2. Suppose that conjugation by $g \in \mathcal{G}_v$ sends $\pi\alpha$ to $\pi^{-1}\alpha^{-1}$. Then conjugation by $g$ must send $\pi$ to $\pi^{-1}$ and $\alpha$ to $\alpha^{-1}$. The first property implies that $g\mathcal{M}_v$ has order 2 in $\mathcal{G}_v/\mathcal{M}_v$. Hence $g\mathcal{M}_v$ is in the unique subgroup of index 2 and hence conjugation by $g$ fixes $\alpha$. But $\alpha \neq \alpha^{-1}$. This establishes *(a)*. As for *(b)*, that assertion follows by essentially the same argument as in part *(i)*. One can note that the orbit of $\pi^{-1}\alpha^{-1}$ contains a character of $\mathcal{M}_v$ of the form $\pi'\alpha$ for some character $\pi$ of $\mathcal{M}_v/\mathcal{J}_v$ and hence $\check{\chi} \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi' \otimes \alpha)$. It is then clear that the multiplicities of $\widetilde{\varphi}$ in $\widetilde{\chi}^s s$ and $\widetilde{\check{\chi}}^s s$ both are equal to the multiplicity of $\widetilde{\varphi}$ in $\widetilde{\beta}^{ss}$, where $\beta = \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\alpha)$, which establishes *(b)*.

Finally, to prove part *(iii)*, it suffices to prove the congruence

$$\langle \chi, \varphi \rangle + \langle \chi, \psi \rangle \ \equiv \ \langle \widetilde{\chi}, \widetilde{\varphi} \rangle + \langle \widetilde{\chi}, \widetilde{\psi} \rangle \pmod 2$$

for all $\chi \in \mathrm{Irr}_{\mathcal{F}}(\Delta_v)$. We may assume that $\varphi \ncong \psi$, since the congruence is obvious otherwise. If the right side is 0, then so is the left. Hence we may assume that at least one of the irreducible representations $\widetilde{\varphi}$ or $\widetilde{\psi}$ is a constituent in $\widetilde{\chi}$, say $\widetilde{\varphi}$. If $\chi$ is isomorphic to $\varphi$ or $\psi$, then $im(\chi)$ has order prime to $p$, $\widetilde{\chi}$ is irreducible, and the two sides of the congruence are clearly equal. Thus, we assume that $\chi$ is not isomorphic to $\varphi$ or $\psi$, but $\langle \widetilde{\chi}, \widetilde{\varphi} \rangle \geq 1$. The left side of the congruence is then zero. By lemma 11.2.8, either $\chi \cong \varphi \otimes \xi$ for a nontrivial $\xi \in \Xi$ or $\chi \cong \mathrm{Ind}_{\mathcal{M}_v}^{\mathcal{G}_v}(\pi\alpha)$ for a suitable $\alpha$. In either case, $\chi \otimes \omega_v^j \cong \chi$. Therefore,

$$\langle \widetilde{\chi}, \widetilde{\psi} \rangle \ = \ \langle \widetilde{\chi} \otimes \widetilde{\omega}_v^j, \ \widetilde{\varphi} \otimes \widetilde{\omega}_v^j \rangle \ = \ \langle \widetilde{\chi}, \widetilde{\varphi} \rangle$$

and so the right side of the congruence is also even. □

**Remark 11.2.9.** The special case of proposition 11.2.7*(i)* where $\varphi = \omega_v$ will come up in remark 12.2.2 which in turn is used in part **C** of section 13.3. The argument can be made almost transparent in this case. We assume that $w_v$ is odd. It suffices to show that $\langle \rho_v, \omega_v \rangle$ and $\langle \widetilde{\rho}_v, \widetilde{\omega}_v \rangle$ have the same parity. One can assume that $\langle \widetilde{\rho}_v, \widetilde{\omega}_v \rangle$ is positive. The irreducible constituents of $\rho_v$ which make a nontrivial contribution to $\langle \widetilde{\rho}_v, \widetilde{\omega}_v \rangle$ must be of the form $\xi \otimes \omega_v$, where $\xi \in \Xi$. According to lemma 11.2.2, if $\xi \neq \xi_0$, then $\xi \otimes \omega_v \cong \xi$. Also, $\xi$ cannot be self-dual. For $\xi$ is induced from some character $\pi$ of $\mathcal{M}_v$, $\check{\xi}$ is induced from $\pi^{-1}$, and the assumption that $w_v$ is odd easily implies that the orbit of $\pi$ under the action of $\mathcal{G}_v/\mathcal{M}_v$ cannot contain $\pi^{-1}$.

Now since $\rho$ is assumed to be self-dual, so is $\rho_v$. Thus, if $\xi$ occurs as a constituent in $\rho_v$, then so does $\check{\xi}$, and the multiplicities will be equal. If $\xi \neq \xi_0$, then $\check{\xi} \ncong \xi$. The contributions

to $\langle \widetilde{\rho}_v, \widetilde{\omega}_v \rangle$ coming from $\xi$ and $\check{\xi}$ will both be 1. The total contribution coming from all such pairs $\xi$ and $\check{\xi}$ will be even and hence the parity of $\langle \widetilde{\rho}_v, \widetilde{\omega}_v \rangle$ is determined by the one remaining contribution, which is from $\xi_0 \otimes \omega_v$. That contribution is exactly $\langle \rho_v, \omega_v \rangle$. $\diamondsuit$

# 12 Parity.

This chapter will include results concerning the parity of $\lambda_E(\rho)$ and $s_E(\rho)$ under the hypothesis that $\rho$ is a self-dual Artin representation of $G_F$. The results are conditional in that our approach requires the assumption that $\mathrm{Sel}_E(K_\infty)[p]$ is finite, where $K$ is chosen so that the representations being considered factor through $\mathrm{Gal}(K/F)$. Roughly speaking, our main result is that the standard parity conjectures are compatible with congruence relations. We assume that $p$ is odd throughout this chapter. We also assume that $E$ has good, ordinary reduction at the primes of $F$ lying above $p$.

For brevity, we let $\mathrm{Art}^{(sd)}(F)$ denote the set of self-dual Artin representations of $G_F$. We first introduce four functions from $\mathrm{Art}^{(sd)}(F)$ to $\{\pm 1\}$. Our results will primarily concern three of them. One function is the so-called *"root number"* associated with the $L$-function $L(E/F, \rho, s)$ for $E$ and $\rho$ over $F$. The analytic continuation and functional equation for such $L$-functions is still conjectural in most cases, but the corresponding root number has a precise definition given by Deligne in [Del]. Our discussion will be based on formulas due to Rohrlich which are derived from that definition. We denote the value of that function at $\rho$ by $W_{Del}(E, \rho)$.

One should note that the definition of $W_{Del}(E, \rho)$ is really for a self-dual representation $\rho$ of $G_F$ over the field $\mathbf{C}$ of complex numbers. For our arguments, and also for the statements of the conjectures and propositions, the representations $\rho$ which we consider are defined over a field $\mathcal{F}$ which is a finite extension of $\mathbf{Q}_p$. We will arbitrarily fix an embedding of $\mathcal{F}$ into $\mathbf{C}$. Thus, if $\rho$ is a self-dual representations over $\mathcal{F}$, then we can also view $\rho$ as a representation over $\mathbf{C}$. Rohrlich [Ro08] has proven that the value of $W_{Del}(E, \rho)$ is independent of the choice of embedding.

The other three functions are defined as follows:

$$W_{MW}(E, \rho) = (-1)^{r_E(\rho)}, \qquad W_{Sel_p}(E, \rho) = (-1)^{s_E(\rho)}, \qquad W_{Iw_p}(E, \rho) = (-1)^{\lambda_E(\rho)}$$

for an arbitrary Artin representation $\rho$. The definitions of $r_E(\rho)$ and $s_E(\rho)$ can be found at the beginning of chapter 10. The definition of $\lambda_E(\rho)$ is in section 3.5, extending the definition in section 1.2. These definitions don't assume that $\rho$ is self-dual, but our propositions will require that assumption.

We will almost always require that $\rho$ be orthogonal. Now $\rho$ may be reducible, and we say that $\rho$ is orthogonal if the underlying representation space $W_\rho$ has a nondegenerate, $G_F$-invariant $\mathcal{F}$-bilinear form which is symmetric. Equivalently, this means that if $\theta$ is any irreducible constituent in $\rho$, then either *(i)* $\theta$ is self-dual and orthogonal, or *(ii)* $\theta$ is self-dual, symplectic, and occurs with even multiplicity, or *(iii)* $\theta$ is not self-dual and both $\theta$ and $\check{\theta}$ have the same multiplicity in $\rho$.

Assuming just that $\rho$ is self-dual, the following equalities should be true:

$$W_{MW}(E,\rho) = W_{Sel_p}(E,\rho), \quad W_{Sel_p}(E,\rho) = W_{Iw_p}(E,\rho), \quad W_{Iw_p}(E,\rho) = W_{Del}(E,\rho) \ .$$

Actually, the first equality should hold for any $\rho$ and is certainly true if $Ш_E(K)_p$ is finite, where we choose $K$ so that $\rho$ factors through $\mathrm{Gal}(K/F)$. We will say nothing more about that equality. Concerning the second equality, what we can say is covered by proposition 10.2.1 for orthogonal representations and 10.2.3 for symplectic representations. The assumption in those results that $\rho$ be irreducible is not important. One can easily reduce to that case. We will study the third equality in this chapter. Our main result states that, under certain hypotheses, the ratio $W_{Iw_p}(E,\cdot)/W_{Del}(E,\cdot)$ defines a $p$-modular function.

If $D$ is a finite group, we use the notation $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$ to denote the set of all finite-dimensional, self-dual representations of $D$ over $\mathcal{F}$. We let $\mathcal{R}_{\mathcal{F}}^{(sd)}(D)$ denote the subgroup of $\mathcal{R}_{\mathcal{F}}(D)$ generated by $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. Thus, $\mathcal{R}_{\mathcal{F}}^{(sd)}(D)$ is a free $\mathbf{Z}$-module with a basis consisting of *(i)* all $\rho$'s in $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ together with *(ii)* all elements of the form $\rho \oplus \check{\rho}$, where $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$, but $\rho$ is not self-dual. If we have a function $f$ with values in the group $\{\pm 1\}$ defined on the set $\mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$, then we will automatically extend it to a group homomorphism $f$ from $\mathcal{R}_{\mathcal{F}}^{(sd)}(D)$ to $\{\pm 1\}$ by defining $f(\rho \oplus \check{\rho}) = 1$ for all the non-self-dual $\rho \in \mathrm{Irr}_{\mathcal{F}}(D)$. This is already built into the definitions of $W_{MW}(E,\cdot)$, $W_{Sel_p}(E,\cdot)$ and $W_{Iw_p}(E,\cdot)$, as one can see from (10.0.a) and corollary 10.1.3, and is also a known property of $W_{Del}(E,\cdot)$. In that case, it follows from proposition 8, part *(iii)*, in [Ro96].

## 12.1 The proof of theorem 3.

Fix a finite Galois extension $K/F$. The following hypothesis will be needed in the proof of proposition 12.1.1 for the primes $v$ of $F$ lying over 2 or 3. It should be unnecessary, but the formulas for the local root numbers that we use don't cover all cases for such $v$'s. Only *(i)* involves the field $K$.

$\mathrm{Hyp}_v$: *Either (i)* $v \notin \Phi_{K/F}$, *or (ii)* $E$ *is semistable at* $v$, *or (iii)* $E$ *has potentially multiplicative reduction at* $v$, *or (iv)* $\mathrm{Gal}(F_v(E[p])/F_v)$ *is abelian.*

The proof is rather long and uses results from chapters 9, 10, and 11 as well as the earlier chapters. As before, we let $D = \mathrm{Gal}(K/F)$ and identify $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$ with a subgroup of $D$ by the restriction map.

**Proposition 12.1.1.** *Assume that $p$ is odd and that $\mathrm{Hyp}_v$ is satisfied for all primes $v$ of $F$ lying over 2 or 3. Assume that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Suppose that $\rho_1,\ \rho_2 \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$ and that $\widetilde{\rho}_1^{\,ss} \cong \widetilde{\rho}_2^{\,ss}$. Then $W_{Iw_p}(E,\rho_1) = W_{Del}(E,\rho_1)$ if and only if $W_{Iw_p}(E,\rho_2) = W_{Del}(E,\rho_2)$.*

The following lemma will be used and may be of independent interest. We state it for $W_{Del}(E,\cdot)$, but the analogous results for $W_{MW}(E,\cdot)$, $W_{Sel_p}(E,\cdot)$, and $W_{Iw_p}(E,\cdot)$ follow immediately from remark 10.2.2. The proof reduces to a local argument which uses formulas of Rohrlich for some of the primes $v$ of $F$. For the primes $v$ where $E$ has potentially good reduction, but not good reduction, we are grateful to Rohrlich for providing us with most of the rather long argument, and an outline of the rest. In fact, his argument works for all primes $v$, but requires some additional steps when $E$ has multiplicative or potentially multiplicative reduction at $v$. For those primes, we decided to directly use Rohrlich's formulas instead. The statement of the lemma is more general than we need. We will apply it to the case where $L = F_n$, a cyclic extension of degree $p^n$, where $n$ will be chosen to be sufficiently large.

**Lemma 12.1.2.** *Suppose that $L$ is a finite Galois extension of $F$ and that $[L:F]$ is odd. Let $\rho \in \mathrm{Art}^{(sd)}(F)$ and let $\rho|_L$ denote the restriction of $\rho$ to $G_L$. Then $\rho|_L \in \mathrm{Art}^{(sd)}(L)$ and we have*

$$W_{Del}(E,\rho|_L) \;=\; W_{Del}(E,\rho) \quad .$$

*Proof.* The proof uses the factorization

$$W_{Del}(E,\rho) \;=\; \prod_v W_v(E,\rho) \tag{12.1.a}$$

over all the primes $v$ of $F$. The factors $W_v(E,\rho)$ are in $\{\pm 1\}$, the so-called *local root numbers*, which we denote below by $W_{F_v}(E,\rho)$. Those factors are only defined when $\rho$ is self-dual. We also use the analogous factorization for $W_{Del}(E,\rho|_L)$ over the primes of $L$. Suppose that $v$ is any prime of $F$. We let $L_v$ denote the completion of $L$ at any prime lying over $v$. Then $[L_v : F_v]$ is also odd. We will show that

$$W_{L_v}(E,\rho|_L) \;=\; W_{F_v}(E,\rho) \tag{12.1.b}$$

for all self-dual $\rho$. Here we are using subscripts $L_v$ and $F_v$ to avoid confusion. These local root numbers depend only on the restrictions of $\rho$ to $G_{L_v}$ and $G_{F_v}$, respectively. Establishing

(12.1.b) for all primes $v$ of $F$ will suffice because the quantities are $\pm 1$ and there are an odd number of primes of $L$ lying over each such $v$. Hence the corresponding contributions to the product formulas for $W_{Del}(E,\rho)$ and $W_{Del}(E,\rho|_L)$ will indeed be equal.

The results that we will need about local root numbers come mostly from [Ro96], theorem 2 and proposition 8. We need the formulas for both $F_v$ and $L_v$, but state them just for $F_v$. If $v$ is archimedean, then one has $W_{F_v}(E,\rho) = (-1)^{n(\rho)}$ (from [Ro96], theorem 2). It is obvious that $W_{L_v}(E,\rho|_L) = W_{F_v}(E,\rho)$. If we now assume that $v$ is a nonarchimedean prime of $F$ where $E$ has good reduction, then one has $W_{F_v}(E,\rho) = \vartheta(-1)$, where $\vartheta = det(\rho)$. Here $\vartheta$ is regarded as a character of $G_{F_v}$ and also identified with the character of $F_v^\times$ corresponding to it by local class field theory. (See [Ro96], proposition 2.) A similar formula is valid if we restrict $\rho$ to $G_{L_v}$. By local class field theory, the corresponding character of $L_v^\times$ is $\vartheta \circ N_{L_v/F_v}$, where $N_{L_v/F_v}$ is the norm map. Hence, $W_{L_v}(E,\rho|_L) = \vartheta\big(N_{L_v/F_v}(-1)\big)$. Since $[L_v : F_v]$ is odd, $N_{L_v/F_v}(-1) = -1$, and so (12.1.b) is verified.

Now assume that $\mathrm{ord}_v(j_E) < 0$. We then use the following formula from theorem 2 of [Ro96]:

$$W_{F_v}(E,\rho) \;=\; det(\rho_{F_v})(-1)\cdot\varphi(-1)^{n(\rho)}\cdot(-1)^{\langle\varphi,\ \rho_{F_v}\rangle} \quad .$$

Our notation differs from that in [Ro96]. Here we let $\rho_{F_v}$ denote the restriction of $\rho$ to $G_{F_v}$, and the character $\varphi$ occurring in this formula is of order 1 or 2. Although it is not important now, the character $\varphi$ is determined by its restriction to $\mathcal{G}_v$ and that restriction is precisely the character $\varphi_v\omega_v^{-1}$ occurring in section 5.2. We view $\varphi$ as a character of $G_{F_v}$ or of $F_v^\times$. A similar formula is valid for $W_{L_v}(E,\rho|_L)$. The roles of $\rho_{F_v}$ and $\varphi$ are then played by their restrictions to $G_{L_v}$, which we denote by $\rho_{L_v}$ and $\varphi_{L_v}$, respectively. Since $\rho_{F_v}$ and $\varphi$ are both self-dual, we can use proposition 9.3.5, obtaining

$$\langle\rho_{L_v},\varphi_{L_v}\rangle \;\equiv\; \langle\rho_{F_v},\varphi\rangle \qquad (\mathrm{mod}\ 2) \quad .$$

The equality $W_{L_v}(E,\rho) = W_{F_v}(E,\rho)$ follows from this congruence and the previous arguments given for the case of good reduction at $v$.

Assume now that $\mathrm{ord}_v(j_E) \geq 0$. Thus, $E$ has potentially good reduction at $v$. Let $n = n(\rho)$. The trivial representations of $G_{F_v}$ and $G_{L_v}$ will be denoted by $\mathbf{1}_{F_v}$ and $\mathbf{1}_{L_v}$, respectively. Let $n = [L_v : F_v]$. Consider the virtual representations

$$\alpha_{F_v} = \rho_{F_v} - n\cdot\mathbf{1}_{F_v}, \qquad \alpha_{L_v} = \rho_{L_v} - n\cdot\mathbf{1}_{L_v} \quad .$$

They have degree 0. The local root numbers behave well with respect to induction for virtual representations of degree 0. The justification for this can be found in [Ro94], property $\epsilon 2$ on page 142. One should use that property in conjunction with equation (3.1) in [Ro96], noting

that since we are assuming that $E$ has potentially good reduction at $v$, one can write $\sigma_{E/F_v}$ in place of $\sigma'_{E/F_v}$. This justifies the second equality below.

$$W_{L_v}(E,\rho|_L)W_{L_v}(E)^{-n} \;=\; W_{L_v}(E,\alpha_{L_v}) \;=\; W_{F_v}\big(E,\mathrm{Ind}_{L_v}^{F_v}(\alpha_{L_v})\big)$$

Here we write $W_{L_v}(E)$ for $W_{L_v}(E,\mathbf{1}_{L_v})$, which is just the local root number for $E$ over $L_v$. We can simplify the rest of the argument by using the fact that $\mathrm{Gal}(L_v/F_v)$ is a solvable group. This is true because it is a local Galois group, (or, alternatively, because it has odd order). Therefore, for the proof of the (12.1.b), it is enough to consider the case where the extension $L_v/F_v$ is cyclic of odd degree. We then have

$$W_{L_v}(E,\rho|_L)W_{L_v}(E)^{-n} \;=\; \prod_{\varepsilon} W_{F_v}\big(E,\alpha_{F_v}\otimes\varepsilon\big)\ , \tag{12.1.c}$$

where the product varies over the characters $\varepsilon$ of $\mathrm{Gal}(L_v/F_v)$. There are $[L_v : F_v]$ such characters. The factor for $\varepsilon=\varepsilon_0$ is $W_{F_v}\big(E,\alpha_v\big)=W_{F_v}(E,\rho)W_{F_v}(E)^{-n}$.

For any $\varepsilon$, the definition of the corresponding local root number is

$$W_{F_v}(E,\alpha_{F_v}\otimes\varepsilon) \;=\; W\big(\sigma_E\otimes\alpha_{F_v}\otimes\varepsilon\big)\quad ,$$

where $\sigma_E$ is the canonical 2-dimensional representation of the Weil-Deligne group associated to $E$, as defined on page 329 in [Ro96]. (It is denoted by $\sigma_{E/F_v}$ there.) The function $W(\cdot)$ is defined in [Ro94], chapter 12. The representation $\sigma_E$ is self-dual and has trivial determinant. For brevity, let $\gamma_{v,\varepsilon}=\sigma_E\otimes\alpha_{F_v}\otimes\varepsilon$, whose contragredient is $\gamma_{v,\varepsilon^{-1}}$. This is a virtual representation of the Weil-Deligne group and has degree 0. Its determinant can be defined. Since $\alpha_{F_v}$ has degree 0, one sees easily that $det(\alpha_{F_v}\otimes\varepsilon)=det(\alpha_{F_v})$. The values of $det(\alpha_{F_v})$ are in $\{\pm1\}$ and since $\sigma_E$ has degree 2, we have $det(\gamma_{v,\varepsilon})=det(\sigma_E)=\mathbf{1}_{F_v}$. One also has

$$W\big(\gamma_{v,\varepsilon}\big)W\big(\gamma_{v,\varepsilon^{-1}}\big) \;=\; det\big(\gamma_{v,\varepsilon}\big)(-1)=1\quad .$$

This follows from part *(i)* in the lemma on page 144 in [Ro94], taking into account the fact that $\gamma_{v,\varepsilon}$ has virtual degree 0. If $\varepsilon$ is nontrivial, then $\varepsilon\neq\varepsilon^{-1}$ since $[L_v : F_v]$ is odd. Therefore, grouping the factors for $\varepsilon$ and for $\varepsilon^{-1}$ together on the left side of (12.1.c), we have

$$W_{L_v}(E,\rho|_L)W_{L_v}(E)^{-n} \;=\; W_{F_v}(E,\rho)W_{F_v}(E)^{-n}\quad ,$$

and so (12.1.b) is equivalent to the assertion that $W_{L_v}(E)^n=W_{F_v}(E)^n$.

We will prove that $W_{L_v}(E)=W_{F_v}(E)$, which will then complete the proof of (12.1.b) and hence of lemma 12.1.2. If $E$ has good reduction over $F_v$, then $E$ has good reduction over $L_v$, and this implies that $W_{L_v}(E)=1,\ W_{F_v}(E)=1$. (See the proposition in chapter 19

of [Ro94].) Thus, no further argument is needed. We assume now that $E$ has bad reduction over $F_v$. We will use a global argument (suggested by Rohrlich) to complete the proof. Suppose that $S = \Psi_E$, the set of primes of $F$ where $E$ has bad reduction. The Grunwald-Wang theorem ([NSW], 9.2.3) implies that there exists a cyclic extension $L$ of $F$ with the following properties: *(i)* there exists just one prime of $L$ lying over $v$ and the corresponding completion of $L$ is $L_v$, *(ii)* all other primes in $S$ split completely in $L/F$. It follows that $[L : F] = [L_v : F_v]$, which is odd. Denoting the global root numbers for $E$ over $L$ and over $F$ by $W_{Del}(E/L)$ and $W_{Del}(E/F)$, respectively, we have

$$W_{Del}(E/L) \;=\; \prod_{\varepsilon} W_{Del}(E,\varepsilon) \;=\; W_{Del}(E/F) \quad ,$$

where $\varepsilon$ now runs over all the characters of $\mathrm{Gal}(L/F)$. The first equality is a consequence of the fact that the global root number is unchanged by induction from a subgroup. (A proof of this can be found in [Ro09].) The first term is the root number for $E$ and the trivial representation $\mathbf{1}_L$ of $G_L$. The second term is the root number for $E$ and for the regular representation of $\mathrm{Gal}(L/F)$, which can be regarded as $\mathrm{Ind}_{G_L}^{G_F}(\mathbf{1}_L)$. The second equality follows by grouping the factors for $\varepsilon$ and $\varepsilon^{-1}$ when $\varepsilon$ is nontrivial. One can then use part *(iii)* in proposition 8 of [Ro96] together with the fact that $\varepsilon \oplus \varepsilon^{-1}$ is a symplectic representation.

On the other hand, $W_{Del}(E/L)$ and $W_{Del}(E/F)$ can both be expressed as products of local root numbers over all the primes of $L$ or of $F$. The contributions from the unique prime of $L$ lying above $v$, and from $v$ itself, are $W_{L_v}(E)$ and $W_{F_v}(E)$, respectively. We prove that $W_{L_v}(E) = W_{F_v}(E)$, by showing that the contributions to the products from all other primes $w$ of $F$, and the primes of $L$ lying above such a $w$, are equal. The contributions for any $w$ where $E$ has good reduction, and for primes of $L$ lying over $w$, are all 1's. If $w$ is an archimedean prime of $F$ or a prime in $S$ other than $v$, then $w$ splits completely in $L/F$. For any such $w$, the contribution to the product for $W_{Del}(E/L)$ is $W_{F_w}(E)^{[L:F]}$. Since $[L : F]$ is odd, this contribution is equal to $W_{F_w}(E)$, which is the corresponding contribution to the product formula for $W_{Del}(E/F)$. This completes the proof of lemma 12.1.2. $\square$

*Proof of proposition 12.1.1.* By lemma 12.1.2 and remark 10.2.2, we are free to replace the ground field $F$ by $F_n$ for any $n \geq 0$. We make that replacement so that the restriction map from $\Delta$ to $D$ is an isomorphism. Thus, we can identify $\Delta$ with $D$. We will assume that the primes in $\Phi_{K/F}$ are inert in $F_\infty/F$. Letting $\Delta_v = \mathrm{Gal}(K_{\infty,v}/F_{\infty,v})$ and $D_v = \mathrm{Gal}(K_v/F_v)$, we will furthermore assume that the restriction map defines an isomorphism from $\Delta_v$ to $D_v$ for all $v \in \Phi_{K/F}$. Such a replacement is clearly possible. We make these simplifying assumptions from here on. Thus, we can now identify representations of $D$ with representations of $\Delta$. Similarly, we can identify the restrictions of those representations to $D_v$ and to $\Delta_v$ for any $v \in \Phi_{K/F}$.

Consider the homomorphism $f : \mathcal{R}_{\mathcal{F}}^{(sd)}(D) \longrightarrow \{\pm 1\}$ which is defined as follows: For a self-dual representation $\rho$, let $f(\rho) = W_{Iw_p}(E,\rho)\big/W_{Del}(E,\rho)$. Under the stated assumptions, we must show that $f(\rho_1) = 1$ if and only if $f(\rho_2) = 1$. This is equivalent to showing that $f$ is $p$-modular.

Let $\Sigma_0 = \Phi_{K/F}$. We define $\lambda_E(\rho)$, $\lambda_E^{\Sigma_0}(\rho)$, $\delta_E^{\Sigma_0}(\rho)$, and $\delta_{E,v}(\rho)$ for any $\rho \in \mathrm{Rep}_{\mathcal{F}}(D)$ by making them additive for direct sums. They all have values in $\mathbf{Z}$. We then have

$$(12.1.\mathrm{d}) \quad W_{Iw_p}(E,\rho) \;=\; (-1)^{\lambda_E(\rho)} = (-1)^{\lambda_E^{\Sigma_0}(\rho)}(-1)^{\delta_E^{\Sigma_0}(\rho)} \;=\; (-1)^{\lambda_E^{\Sigma_0}(\rho)} \prod_{v\in\Sigma_0} (-1)^{\delta_{E,v}(\rho)} \quad .$$

We have used (5.0.b) from chapter 5 together with the fact that the $g_v$'s are odd. As mentioned before, we have $W_{Iw_p}(E,\rho) = 1$ if $\rho \cong \theta \oplus \check{\theta}$ for some $\theta \in \mathrm{Irr}_{\mathcal{F}}(D)$. Note however that the other factors occurring above are not necessarily all 1's for such a $\rho$. For example, it is not always true that $\delta_{E,v}(\check{\theta}) = \delta_{E,v}(\theta)$, or even that they have the same parity.

Using (12.1.d) and the product formula for $W_{Del}(E,\rho)$, we have

$$(12.1.\mathrm{e}) \qquad f(\rho) \;=\; (-1)^{\lambda_E^{\Sigma_0}(\rho)} \prod_{v\notin\Sigma_0} W_v(E,\rho) \prod_{v\in\Sigma_0} \left( W_v(E,\rho)(-1)^{\delta_{E,v}(\rho)} \right) \quad .$$

We will show that each individual factor in the above product is $p$-modular. The quantity within each large parenthesis in the last product must be taken together as one factor. For the first factor, we only need to recall that the function $f_1$ defined by $f_1(\rho) = \lambda_E^{\Sigma_0}(\rho)$ is $p$-modular. This follows from proposition 3.2.1.

*The p-Modularity for $v \notin \Sigma_0$.* We first consider the primes $v$ lying over $p$ or $\infty$. For an archimedean prime $v$, one has $W_v(E,\rho) = (-1)^{n(\rho)}$ (from [Ro96], theorem 2), which certainly defines a $p$-modular function (by 11.1.1). If $v|p$, then $E$ has good reduction at $v$ and one has $W_v(E,\rho) = det(\rho)(-1)$ for all $v|p$, as stated in the proof of lemma 12.1.2. Thus, applying 11.1.2 with $A = \{\pm 1\}$ and using the assumption that $p$ is odd, we see that the function $W_v(E,\cdot)$ is $p$-modular for all $v|p$.

Now assume that $v$ doesn't lie above $p$ or $\infty$, but still that $v \notin \Sigma_0$. The index of the inertia subgroup of $\Delta_v$ (in $\Delta_v$) is not divisible by $p$. Therefore, since $v \notin \Sigma_0$, the order of $\Delta_v$ is also not divisible by $p$. Now $W_v(E,\rho)$ is determined by the restriction of $\rho$ to $D_v$, but $[D_v : \Delta_v]$ is odd and so by applying (12.1.b) to $v$, it follows that $W_v(E,\rho)$ is determined by the restriction of $\rho$ to $\Delta_v$. We can then use 11.1.4 for $\Delta_* = \Delta_v$ to conclude that the function $W_v(E,\cdot)$ is $p$-modular. Thus, the subproduct in (12.1.e) over all $v \notin \Sigma_0$ defines a $p$-modular function on $\mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta)$.

*The p-Modularity for $v \in \Sigma_0$.* The formulas found in [Ro96] are expressed in terms of the restriction of $\rho$ to $D_v$. Some of the formulas only involve the degree or determinant

of $\rho$, and the $p$-modularity then follows quite easily. For the primes $v \in \Sigma_0$, our initial reduction at the beginning of this proof allows us to identify $\Delta_v$ with $D_v$. Hence we can state Rohrlich's formulas in terms of $\rho|_{\Delta_v}$, which we will denote by $\rho_v$ in the rest of this proof. This identification is useful simply because various other representations which intervene in the argument are only defined over $F_{\infty,v}$. It will also be convenient sometimes to regard $\rho_v$ as a self-dual representation of $\mathcal{G}_v$.

For brevity, we use the notation

$$A_v(\rho) \;=\; W_v(E,\rho)\cdot(-1)^{\delta_{E,v}(\rho)} \quad .$$

We will also use the notation from section 5.2. Recall that we have defined an irreducible representation $\varphi_v$ there, and also $\psi_v$ in some cases. Those representation(s) of $\mathcal{G}_v$ occur as subrepresentations of $\rho_{E,v}$, usually with multiplicity 1. The multiplicity will be 2 in the case where $E$ has good or potentially good reduction, $\varphi_v$ is 1-dimensional, and $\psi_v = \varphi_v$.

If $E$ has good reduction at $v$, then we have $W_v(E,\rho) = det(\rho)(-1)$. The function $W_v(E,\cdot)$ is therefore $p$-modular by 11.1.2. On the other hand, in this case, we have

$$\delta_{E,v}(\rho) \equiv \langle \rho_v, \varphi_v\rangle + \langle \rho_v, \psi_v\rangle \pmod 2 \quad . \tag{12.1.f}$$

Since $\varphi_v$ and $\psi_v$ have order prime to $p$, and $\varphi_v\psi_v = \omega_v$, we can apply proposition 11.2.1 to conclude that the function $f$ defined by $f(\rho) = (-1)^{\delta_{E,v}(\rho)}$ is $p$-modular. It follows that the function $A_v(\cdot)$ is $p$-modular.

If $E$ has multiplicative or potentially multiplicative reduction at $v$, then Rohrlich's formula (from theorem 2 of [Ro96]) is

$$W_v(E,\rho) \;=\; det(\rho_v)(-1)\cdot\big(\varphi_v\omega_v^{-1}(-1)\big)^{n(\rho)}\cdot(-1)^{\langle\varphi_v\omega_v^{-1},\ \rho_v\rangle} \quad .$$

The first two factors define $p$-modular functions by 11.1.2 and 11.1.1, but the third factor might actually fail to be $p$-modular. However, we have $\delta_{E,v}(\rho) \equiv \langle \rho_v, \varphi_v\rangle \pmod 2$ and so

$$(-1)^{\langle\varphi_v\omega_v^{-1},\ \rho_v\rangle}(-1)^{\delta_{E,v}(\rho)} \;=\; (-1)^{\langle\rho_v,\varphi_v\omega_v^{-1}\rangle+\langle\rho_v,\varphi_v\rangle} \ ,$$

which defines a $p$-modular function according to proposition 11.2.1. The hypothesis in that proposition is satisfied because $\varphi_v\omega_v^{-1}$ is a character of order 1 or 2. It follows that the function $A_v(\cdot)$ is $p$-modular, as we wanted to show. Note that our arguments so far work even if $v$ divides 2 or 3.

Now we come to the case where $E$ has potentially good reduction at $v$, but not good reduction. Assume first that the image of $\mathcal{G}_v$ under $\rho_{E,v}$ is abelian. In that case, there are

two (non necessarily distinct) characters $\varphi_v$ and $\psi_v$ which are constituents in $\rho_{E,v}$. We have $\varphi_v\psi_v = \omega_v$. Rohrlich proves the formula $W_v(E,\rho) = det(\rho_v)(-1)\cdot\chi_v(-1)^{n(\rho)}$ in this case, where $\chi_v$ is a certain character of $G_{F_v}$. This is proved in [Ro07]. If $v$ doesn't lie above 2 or 3, this was already proved in [Ro96], but the proof in [Ro07] includes all $v$'s if $im(\rho_{E,v})$ is abelian. (See the proof of proposition 3, especially equation (1.6).) Such a formula defines a $p$-modular function of $\rho$. The proof that $A_v(\cdot)$ is $p$-modular is now just like the case where $E$ has good reduction at $v$, again just using proposition 11.2.1 and (12.1.f). This argument works for $p \geq 5$. But if $p = 3$, it is possible that $\varphi_v$ and $\psi_v$ will have order divisible by $p$. In that case, one can apply remark 11.2.6.

It remains to discuss the case where $v \in \Sigma_0$ and $E$ has potentially good reduction at $v$, but where the image of $\rho_{E,v}$ is non-abelian. The assumption in proposition 12.1.1 concerning $\mathrm{Hyp}_v$ implies that $v$ doesn't lie over 2 or 3. The inertia subgroup $\Theta_v$ of $\mathrm{Gal}(F_{\infty,v}(E[p])/F_{\infty,v})$ is then a cyclic group of order $e$, where $e \in \{3,4,6\}$. The value of $e$ is determined by $ord_v\big(disc(E)\big)$. We then have the following formula from [Ro96]:

$$W_v(E,\rho) \;=\; det(\rho_v)(-1)\cdot(-\epsilon)^{n(\rho)}\cdot(-1)^{\langle\rho_v,\chi_0\rangle+\langle\rho_v,\eta\rangle+\langle\rho_v,\hat\sigma_e\rangle}\quad, \tag{12.1.g}$$

where $\epsilon \in \{\pm 1\}$, $\eta$ is the unramified character of $\mathcal{G}_v$ of order 2, and $\hat\sigma_e$ is a certain 2-dimensional representation of $\mathcal{G}_v$. Rohrlich defines this on page 329 of [Ro96] as a representation of $G_{F_v}$ which factors through a certain extension with Galois group isomorphic to the dihedral group $D_{2e}$. That extension is tamely ramified, the inertia subgroup is cyclic of order $e$, and $\hat\sigma_e$ is the unique irreducible 2-dimensional representation of the Galois group. Also, $det(\hat\sigma_e) = \eta$. We can consider $\hat\sigma_e$ as a representation of $\mathcal{G}_v$.

As before, 11.1.1 and 11.1.2 imply that the first two factors in (12.1.g) define $p$-modular functions. We don't need the definition of $\epsilon$ for this. We will consider the functions $a$ and $b$ on $\mathcal{R}_{\mathcal{F}}^{(sd)}(\Delta)$ defined by

$$a(\rho) = (-1)^{\langle\rho_v,\chi_0\rangle+\langle\rho_v,\eta\rangle}, \qquad b(\rho) = (-1)^{\langle\rho_v,\hat\sigma_e\rangle}$$

separately. If $w_v$ is even, then $\eta$ is a power of $\omega_v$, and so one can apply proposition 11.2.1 to see that the function $a$ is $p$-modular. If $w_v$ is odd, then one can apply part *(i)* of proposition 11.2.7 to both $\varphi = \chi_0$ and $\varphi = \eta$ to conclude that $a$ is $p$-modular function. The function $b$ is not necessarily $p$-modular. However, it is the function $c$ defined by

$$c(\rho) \;=\; (-1)^{\langle\rho_v,\hat\sigma_e\rangle+\delta_{E,v}(\rho)}\quad,$$

which we must show is $p$-modular. The $p$-modularity of $A_v(\cdot)$ follows from that.

Note that $\delta_{E,v}(\rho) \equiv \langle\rho_v,\varphi_v\rangle \pmod 2$, where now $\varphi_v$ coincides with $\rho_{E,v}$ in the notation of chapter 5. Thus, using the notation of proposition 11.2.7, we have $c = f_{\hat\sigma_e}f_{\varphi_v}$. Assume

first that $p \geq 5$. We consider $p = 3$ later. The assumptions in the first sentence of that proposition are then satisfied for both $\varphi = \hat{\sigma}_e$ and for $\varphi = \varphi_v$. Now $\hat{\sigma}_e$ is self-dual and has determinant $\eta$. Also, $det(\varphi_v) = \omega_v$ and hence $\check{\varphi}_v \cong \varphi_v \otimes \omega_v^{-1}$. If $w_v$ is even, then the restriction of $\hat{\sigma}_e$ to $\mathcal{M}_v$ is clearly reducible. The same is true for $\varphi_v$ since the action of $\mathrm{Gal}(F_{\infty,v}(E[p])/F_{\infty,v})/\Theta_v$ on $\Theta_v$ is through a quotient group of order 2. It follows that if $w_v$ is odd or if $4 \mid w_v$, then both $f_{\hat{\sigma}_e}$ and $f_{\varphi_v}$ are $p$-modular.

We now consider the case where $w_v$ is even, but $w_v/2$ is odd. Thus $\eta = \omega_v^{w_v/2}$. It is clear that $\varphi_v \otimes \omega_v^j$ has determinant $\eta$ for some $j$. We will show that $\varphi_v \otimes \omega_v^j \cong \hat{\sigma}_e$ for that $j$. The $p$-modularity of $c$ then follows from part *(iii)* of proposition 11.2.7. To see this, let $F_{v,\infty}^{unr}$ and $F_{v,\infty}^{tr}$ denote the maximal unramified and tamely ramified extensions of $F_{\infty,v}$, respectively. Both $\varphi_v \otimes \omega_v^j$ and $\hat{\sigma}_e$ factor through $\mathrm{Gal}(F_{v,\infty}^{tr}/F_{v,\infty})$. Their restrictions to the inertia subgroup $\mathrm{Gal}(F_{v,\infty}^{tr}/F_{v,\infty}^{unr})$ are direct sums of the two characters of order $e$ and hence are isomorphic. It follows that $\varphi_v \otimes \omega_v^j \cong \hat{\sigma}_e \otimes \varepsilon$ for an unramified character $\varepsilon$. Comparing the determinants, it follows that $\varepsilon$ has order 1 or 2. In that latter case, $\varepsilon = \eta$. But $\hat{\sigma}_e \otimes \eta \cong \hat{\sigma}_e$. Thus, in either case, $\varphi_v \otimes \omega_v^j$ is indeed isomorphic to $\hat{\sigma}_e$.

Now suppose that $p = 3$. The above argument applies if $e = 4$. Assume that $e \in \{3, 6\}$. Note that $w_v = 1$ or 2. If $w_v = 1$, then $\rho_{E,v}(\mathcal{G}_v)$ is abelian, a case already settled. If $w_v = 2$, then both $\varphi_v$ and $\hat{\sigma}_e$ have determinant $\eta$. Then we have $\varphi_v \cong \hat{\sigma}_e$. Thus $c(\rho) = 1$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(\Delta)$, and so $c$ is obviously $p$-modular. □

Theorem 3 is now proved. The consequence that we mentioned (in section 1.5) is a special case of the following corollary. We assume that $\Delta$ contains a normal subgroup $\Pi$ which is a $p$-group. We might as well assume that $\Pi$ is the maximal such subgroup. Since we are identifying $\Delta$ with a normal subgroup of $D$, $\Pi$ is identified with a normal subgroup of $D$. The subfield $K^{\Pi}$ of $K$ will be denoted by $K_0$. Then $\mathrm{Gal}(K_0/F)$ can be identified with $D_0 = D/\Pi$. As previously, we let $K_{0,\infty} = K_0 F_\infty$, which coincides with $K_\infty^{\Pi}$.

**Corollary 12.1.3.** *Suppose that $p$ is odd, that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, and that $\mathrm{Hyp}_v$ is satisfied for all primes $v$ of $F$ lying over 2 or 3. If the equality $W_{Iw_p}(E,\rho) = W_{Del}(E,\rho)$ is true for all $\rho \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D_0)$, then that equality is also true for all $\rho \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$.*

*Proof.* First of all, we have $\mathrm{Irr}_{\mathfrak{f}}(D_0) = \mathrm{Irr}_{\mathfrak{f}}(D)$. The assumption that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite together with proposition 4.2.5 implies that all of the Selmer atoms $\mathrm{Sel}_{E[p]\otimes\tau}(F_\infty)$ are finite for $\tau \in \mathrm{Irr}_{\mathfrak{f}}(D)$. That same proposition then implies that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Thus, all the hypotheses in proposition 12.1.1 are satisfied.

Assume that $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. Then the class $[\widetilde{\rho}^{ss}]$ is in $\mathcal{R}_{\mathfrak{f}}^{(sd)}(D) = \mathcal{R}_{\mathfrak{f}}^{(sd)}(D_0)$. Therefore, as shown in section 9.4, there exist $\rho_a$ and $\rho_b$ in $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D_0)$ such that

$$\widetilde{\rho}^{(ss)} \oplus \widetilde{\rho}_a^{(ss)} \;\cong\; \widetilde{\rho}_b^{(ss)}$$

as representations of $D$. Assuming the equality in question for all the self-dual, irreducible constituents of $\rho_a$ and $\rho_b$, it then follows that $W_{Iw_p}(E,\rho_c) = W_{Del}(E,\rho_c)$ for $c = a$ and for $c = b$. We see that $W_{Iw_p}(E,\rho) = W_{Del}(E,\rho)$ by applying proposition 12.1.1 to $\rho_1 = \rho \oplus \rho_a$ and $\rho_2 = \rho_b$. This equality holds for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. $\square$

## 12.2 Consequences concerning $W_{Del}(E,\rho)$ and $W_{Sel_p}(E,\rho)$.

We continue to assume that $K_\infty = KF_\infty$, where $K$ is a finite Galois extension of $F$, and we let $D$ denote $\mathrm{Gal}(K/F)$. Consider the following functions $f_{Del}$, $f_{Iw_p}$, and $f_{Sel_p}$ defined by

$$f_{Del}(\rho) = W_{Del}(E,\rho), \qquad f_{Iw_p}(\rho) = W_{Iw_p}(E,\rho), \qquad f_{Sel_p}(\rho) = W_{Sel_p}(E,\rho)$$

for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. One can ask whether those functions are $p$-modular. This is not always so. However, the proof of proposition 12.1.1 gives the following result for the first two functions. Note that the assumption that $\Psi_E \bigcap \Phi_{K/F}$ is empty implies $\mathrm{Hyp}_v$ and also that $E$ has good reduction at any $v \in \Sigma_0 = \Phi_{K/F}$. With the additional assumption about $D$, the $p$-modularity for the third function follows by using proposition 10.2.1.

**Proposition 12.2.1.** *Assume that $p$ is odd and that $\Psi_E \bigcap \Phi_{K/F}$ is empty. Then the function $f_{Del}$ is $p$-modular. Furthermore, if one assumes that $\mathrm{Sel}_E(K_\infty)[p]$ is finite, then $f_{Iw_p}$ is $p$-modular. If one assumes in addition that $D$ satisfies property* **(O)**, *then $f_{Sel_p}$ is also $p$-modular.*

**Remark 12.2.2.** The proof of proposition 12.1.1 gives results about $p$-modularity for the local root numbers. We continue to assume that $p$ is odd. We need only assume that $E$ has good reduction at primes of $F$ lying above $p$. For any prime $v$ of $F$, define $f_{W_v}$ by $f_{W_v}(\rho) = W_v(E,\rho)$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. First of all, the proof shows that $f_{W_v}$ is $p$-modular if $v \notin \Psi_E \bigcap \Phi_{K/F}$. In addition, if $E$ has potentially good reduction at $v$ and $\mathrm{im}(\rho_{E,v})$ is abelian, then $f_{W_v}$ has also been shown to be $p$-modular.

Suppose that $E$ has potentially good reduction at $v$ and that $\mathrm{im}(\rho_{E,v})$ is non-abelian. We let $\varphi_v = \rho_{E,v}$ in this case. Assume that $v$ does not divide 2 or 3. Define a function $f_{\varphi_v}$ exactly as in proposition 11.2.7. We have $\delta_{E,v}(\rho) \equiv \langle \rho_v, \varphi_v \rangle \pmod 2$ and therefore $A_v(\rho) = f_{W_v}(\rho) f_{\varphi_v}(\rho)$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$, where $A_v(\rho)$ is as defined in the proof of proposition 12.1.1. Since $A_v(\cdot)$ has been proved to be $p$-modular, it follows that $f_{W_v}$ is $p$-modular if and only if $f_{\varphi_v}$ is $p$-modular. In general, $f_{\varphi_v}$ will not be $p$-modular. However, if $f_{\varphi_v}(\rho) \neq 1$, then $\langle \rho_v, \varphi_v \rangle \neq 0$. This would imply that $\varphi_v$ factors through $\Delta_v$ and therefore that $\Delta_v$ has a non-abelian quotient. If $p \geq 5$, then $\Delta_v$ would have a non-abelian quotient

of order prime to $p$. Consequently, if $\Delta_v$ has no non-abelian quotient of order prime to $p$, $p \geq 5$, and $v$ does not lie over 2 or 3, then $f_{\varphi_v}(\rho) = 1$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$ and hence $f_{\varphi_v}$ is $p$-modular. Under those assumptions, it follows that $f_{W_v}$ is also $p$-modular.

Now assume that $E$ has multiplicative or potentially multiplicative reduction at $v$. Just as in the previous paragraph, the proof of proposition 12.1.1 shows that $f_{W_v}$ is $p$-modular if and only if $f_{\varphi_v}$ is $p$-modular, where $\varphi_v$ is either $\omega_v$ or $\omega_v\varepsilon_v$ for a certain character $\varepsilon_v$ of order 2. Again, if it turns out that $\varphi_v$ does not factor through the quotient $\Delta_v$ of $\mathcal{G}_v$, then $f_{\varphi_v}(\rho) = 1$ for all $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. In that situation, $f_{W_v}$ will be $p$-modular. Furthermore, if $E$ has split, multiplicative reduction and $\omega_v$ has odd order, then $f_{W_v}$ will be $p$-modular. This follows from remark 11.2.9 which shows that $f_{\omega_v}$ is $p$-modular when $\omega_v$ has odd order. $\Diamond$

Now we will consider $W_{Sel_p}(E, \rho)$ for $\rho \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. Assume that $p$ is odd. The final conclusion in proposition 10.2.1 asserts that $W_{Sel_p}(E, \rho) = W_{Iw_p}(E, \rho)$ if $\rho$ is assumed to be orthogonal and $\mathrm{Sel}_E(K_\infty)_p$ is assumed to be $\mathbf{Z}_p[[\Gamma_K]]$-cotorsion. Applying proposition 12.1.1 and corollary 12.1.3 gives us the following results.

**Proposition 12.2.3.** *Suppose that $p$ is odd, that $\mathrm{Hyp}_v$ is satisfied for all primes $v$ of $F$ lying over 2 or 3, and that $\mathrm{Sel}_E(K_\infty)[p]$ is finite. Assume that $\rho_1$ and $\rho_2$ are self-dual, orthogonal representations of $D = \mathrm{Gal}(K/F)$ and that $\widetilde{\rho}_1^{\,ss} \cong \widetilde{\rho}_2^{\,ss}$. Then $W_{Sel_p}(E, \rho_1) = W_{Del}(E, \rho_1)$ if and only if $W_{Sel_p}(E, \rho_2) = W_{Del}(E, \rho_2)$.*

**Corollary 12.2.4.** *Suppose that we are in the setting of corollary 12.1.3. In addition to the hypotheses stated there, assume that $D_0$ satisfies property* **(O)**. *If $W_{Sel_p}(E, \rho) = W_{Del}(E, \rho)$ for all $\rho \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D_0)$, then $W_{Sel_p}(E, \rho) = W_{Del}(E, \rho)$ for all self-dual, orthogonal representations of $D$.*

**Remark 12.2.5.** A result proved in [Dok5] has a similar flavor to corollary 12.2.4, but requires no Iwasawa-theoretic hypothesis such as the vanishing of a $\mu$-invariant. We will use the same notation as in corollary 12.1.3. It is assumed that $p$ is odd, but no assumption about the reduction type of $E$ at primes over $p$ is needed. For primes $v$ over 2 or 3 where $E$ has additive reduction, it is assumed that $v$ is unramified in $K/F$. No other assumptions are needed. Theorem 1.4 in [Dok5] then asserts that if the parity conjecture for the $\mathbf{Z}_p$-corank of the Selmer group for $E$ over all extensions of $F$ contained in $K_0$ is valid, then the same statement is true for all extensions of $F$ contained in $K$. One can restate their result as follows:

*If $W_{Sel_p}(E, \rho) = W_{Del}(E, \rho)$ for all permutation representations $\rho$ of $D_0$, then $W_{Sel_p}(E, \rho) = W_{Del}(E, \rho)$ for all permutation representations of $D$.*

By definition, a permutation representation $\rho$ of a finite group $G$ is isomorphic to a direct sum of representations of the form $\mathrm{Ind}_H^G\big(\mathbf{1}_H\big)$, where $H$ is a subgroup of $G$. Such representations are obviously realizable over $\mathbf{Q}$ and therefore are orthogonal. More directly, these representations can be realized by permutation matrices, and such matrices are already orthogonal. $\Diamond$

# 13 More arithmetic illustrations.

We end this paper with a number of illustrations concerning the growth of the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K)_p$ as $K$ varies over some collection of fields. We will not strive for generality. We always take the base field $F$ to be $\mathbf{Q}$. It is in this case that we have the best chance to verify the hypotheses in the propositions and corollaries from chapters 3 and 12. We will also discuss results of J. Nekovář, of Mazur and Rubin, of Coates, Fukaya, Kato, and Sujatha, and of T. and V. Dokchitser. The illustrations that we consider are situations where one can calculate $W_{Del}(E,\sigma)$ for some interesting family of irreducible, self-dual Artin representations $\sigma$. One certainly expects that

$$W_{Sel_p}(E,\sigma) \;=\; W_{Del}(E,\sigma) \tag{13.0.a}$$

as we already mentioned in the introduction. This is especially interesting when it turns out that $W_{Del}(E,\sigma) = -1$. For it then would follow that $s_E(\sigma)$ is odd and hence nonzero, contributing at least $n(\sigma)$ to the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(K)_p$. The Galois groups that occur in our illustrations will at least satisfy property **(O)**. Most often, we will refer to corollary 12.2.4. It will be clear in each illustration that $\mathrm{Hyp}_v$ is satisfied for all $v$ lying over 2 or 3. We always assume that $p$ is an odd prime and that $E$ has good, ordinary reduction at $p$. We will describe the predictions arising from (13.0.a), the unconditional results that can be proven, and then the conditional results which one can obtain from sets of hypotheses which seem significantly weaker than (13.0.a).

The simplest case for such root number calculations is when the conductor of $E$, which we will denote by $\mathfrak{n}_E$, and the discriminant of the extension $K/F$, which we denote by $\mathfrak{d}_{K/F}$, are relatively prime. One then has the formula

$$W_{Del}(E,\sigma) \;=\; W_{Del}(E/F)^{n(\sigma)} \cdot det(\sigma)\big(\mathfrak{n}_E\big) \cdot \prod_{v\in\Sigma_\infty} det(\sigma_v)\big(\delta_v\big) \tag{13.0.b}$$

for all $\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$, where $D = \mathrm{Gal}(K/F)$. This is proposition 10 in [Ro96]. Here $W_{Del}(E/F)$ denotes the root number for the Hasse-Weil $L$-series for $E$ over $F$ and $\delta_v$ denotes

the generator of $D_v$ for each $v \mid \infty$. The factor $det(\sigma)\big(\mathfrak{n}_E\big)$ is interpreted as follows. Let $D^{ab}$ denote the maximal abelian quotient of $D$ and let $\delta_E \in D^{ab}$ denote the image of $\mathfrak{n}_E$ under the Artin map. Then $det(\sigma)$ factors through $D^{ab}$ and $det(\sigma)\big(\mathfrak{n}_E\big)$ is defined to be $det(\sigma)\big(\delta_E\big)$. Note that it isn't necessary to assume that $\sigma$ is irreducible to apply (13.0.b). We do need to assume that $\sigma$ is self-dual.

It is worth pointing out that formula (13.0.b) implies that the function $f_{_{Del}}$ is $p$-modular. This follows immediately from 11.1.1 and 11.1.2. However, proposition 12.2.1 asserts this in somewhat greater generality. Also, for the special case where $F = \mathbf{Q}$, formula (13.0.b) takes the following simpler form:

$$W_{_{Del}}(E, \sigma) = W_{_{Del}}(E/\mathbf{Q})^{n(\sigma)} \cdot det(\sigma)(-N_E) \tag{13.0.c}$$

where $N_E$ is the conductor of $E$.

In the rest of this chapter, we will assume that $E$ is an elliptic curve defined over $\mathbf{Q}$, that $p$ is an odd prime where $E$ has good, ordinary reduction, and that $F = \mathbf{Q}$. In sections 13.1 and 13.2, the extensions $K$ of $\mathbf{Q}$ to be considered will satisfy $K \cap \mathbf{Q}_\infty = \mathbf{Q}$. Hence there will be no real need to distinguish between $D = \mathrm{Gal}(K/\mathbf{Q})$ and $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$. We will simply write $\Delta$. However, the illustrations in section 13.1 will require distinguishing between the two Galois groups. The situation will be the one discussed in section 3.5..

## 13.1 An illustration where $\Psi_E \bigcap \Phi_{K/F}$ is empty.

We will consider a situation where we can apply formula (13.0.c). As one favorite illustration, we take $F = \mathbf{Q}$ and consider a tower of number fields $K_r$ such that $\Delta_r = \mathrm{Gal}(K_r/\mathbf{Q})$ is isomorphic to $PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for all $r \geq 0$. We continue to assume that $p$ is odd. In order to use formula (13.0.c), we further assume that the elliptic curve $E$ has good reduction at all the primes of $\mathbf{Q}$ which are ramified in $K_r/\mathbf{Q}$. According to proposition 9.1.1, $\Delta_r$ satisfies property (**SDO**). Also, $\Delta_r^{ab}$ is of order 2. Hence, for every $\rho \in \mathrm{Rep}_{\mathcal{F}_r}(\Delta_r)$, $det(\rho) = \sigma_0$ or $\sigma_{\mathbf{1}}$ in the notation of sections 7.2 and 7.3. Note that $\sigma_{\mathbf{1}}$ corresponds to a certain quadratic Dirichlet character for $\mathbf{Q}$ whose conductor involves only primes which are ramified in $K_0/\mathbf{Q}$. We denote that Dirichlet character by $\varepsilon_{\mathbf{1}}$. If the $K_r$'s arise as subfields of $\mathbf{Q}(A[p^\infty])$ for some elliptic curve $A$, as in the illustrations of sections 8.1 and 8.2, then $\varepsilon_{\mathbf{1}}$ is the unique quadratic Dirichlet character of conductor $p$.

Now $n(\rho)$ is even for all $\rho \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ and for all $r \geq 0$, with the exception of the four representations $\sigma_0, \sigma_{\mathbf{1}}, \sigma_{\mathbf{p},1}, \sigma_{\mathbf{p},2}$. When $n(\sigma)$ is even, the value of $W_{_{Del}}(E, \sigma)$ is determined

completely by $det(\sigma)$ and $N_E$ according to (13.0.c). This is not true for the odd-dimensional $\sigma$'s, but we do have

$$W_{Del}(E,\sigma_0)W_{Del}(E,\sigma_{\mathbf{p},2}) \;=\; W_{Del}(E,\sigma_{\mathbf{1}})W_{Del}(E,\sigma_{\mathbf{p},1}) \;=\; \varepsilon_{\mathbf{1}}(-N_E) \quad . \tag{13.1.a}$$

Howe [How] determines the set $\{\sigma \mid det(\sigma) = \sigma_{\mathbf{1}},\ n(\sigma)\ even\ \}$ precisely. It is an infinite set and the subset of primitive elements of level $r$ is precisely $\mathcal{A}_r \cup \mathcal{B}_r$ for any $r \geq 1$. (See remarks 7.3.4 and 7.4.8 for an argument using modular representations.) We will use the notation $\mathcal{A}_0$ to denote the subset of $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$ consisting of $\sigma$'s of degree $p+1$ and $\mathcal{B}_0$ for the subset consisting of $\sigma$'s of degree $p-1$. For those $\sigma$'s, we also have $det(\sigma) = \sigma_{\mathbf{1}}$.

**A.** *Predictions.* First we note one prediction from (13.0.a) that doesn't depend on the value of $\varepsilon_{\mathbf{1}}(-N_E)$ or on $W_{Del}(E/\mathbf{Q})$. It should be true that $W_{Sel_p}(E,\sigma) = 1$, and hence that $s_E(\sigma)$ is even, for all $\sigma \in \mathcal{C}_r$ and $r \geq 1$. This is because those $\sigma$'s have even degree and $det(\sigma) = \sigma_0$. (See remark 7.3.4.) In particular, $W_{Sel_p}(E,\sigma_{st}^{(r)}) = 1$ for all $r \geq 1$.

If $\varepsilon_{\mathbf{1}}(-N_E) = 1$, then $W_{Del}(E,\sigma) = 1$ for all the even-dimensional $\sigma$'s. Thus, (13.0.a) predicts that $s_E(\sigma)$ is even for all $\sigma$'s except possibly the four odd-dimensional $\sigma$'s, for which we will have $W_{Del}(E,\sigma) = W_{Del}(E/\mathbf{Q})$.

Assume now that $\varepsilon_{\mathbf{1}}(-N_E) = -1$. For the four odd-dimensional irreducible representations of $\Delta_0$, it follows that $W_{Del}(E,\sigma) = -1$ for two of them, one of dimension 1 and one of dimension $p$. For each $\sigma \in \mathcal{A}_r \cup \mathcal{B}_r$ for $r \geq 0$, one has $W_{Del}(E,\sigma) = -1$. The sum of the degrees, where $\sigma$ varies over $\mathcal{A}_r \cup \mathcal{B}_r$ and $r$ varies from 0 to $n \geq 1$, turns out to be $p^{2n+2} - p^{2n+1} - p - 1$. Thus, assuming (13.0.a) for all the relevant $\sigma$'s, one gets the lower bound

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; p^{2n+2} - p^{2n+1} \quad . \tag{13.1.b}$$

under the assumption that $\varepsilon_{\mathbf{1}}(-N_E) = -1$. Equality in (13.1.b) is equivalent to the assertion that $s_E(\sigma) = 1$ if $det(\sigma) = \sigma_{\mathbf{1}}$, $s_E(\sigma) = 0$ if $det(\sigma) = \sigma_0$.

**B.** *Unconditional results.* There are hardly any. Nekovář proved the parity conjecture for $E$ over $\mathbf{Q}$. Thus, (13.0.a) is true for $\sigma = \sigma_0$. This has been extended in [Dok1] to all quadratic twists of $E$, and so (13.0.a) holds for $\sigma = \sigma_{\mathbf{1}}$ too. For $p = 3$, one has $\Delta_0 \cong S_4$ which has a unique quotient isomorphic to $S_3$. The irreducible, 2-dimensional representation of that quotient is $\sigma = \sigma_{\mathbf{p\text{-}1},1}$ and (13.0.a) follows for that $\sigma$ from theorem 7.1 in [MR07] or theorem 1.4 in [Dok5].

One very specific result concerns the following especially interesting example where one can show that $r_E(\sigma_{st}^{(r)}) \geq 1$ for $r \geq 1$. This example is discussed in [Gr01], pages 419-421, and was first mentioned by L. Howe. Let $A$ be either one of the two elliptic curves

of conductor 1225 which have an isogeny of degree 37 defined over $\mathbf{Q}$. One can verify that $\rho_A : G_{\mathbf{Q}} \to \mathrm{Aut}\big(T_p(A)\big)$ is surjective for all $p \geq 5$, except for $p = 37$. Let $E$ be any one of the elliptic curves of conductor 37. We assume that $p \geq 5$ and that $E$ has good, ordinary reduction (which excludes $p = 37$). Since $\rho_A$ is surjective, $\mathbf{Q}(A[p^\infty])$ contains a tower of fields $K_r$ with $\mathrm{Gal}(K_r/\mathbf{Q}) \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$. The modular parametrization $X_0(37) \to E$ then provides a construction of points on $E(K_r)$ (due originally to M. Harris [Har]). Examining that construction, one can show that $\sigma_{st}^{(r)}$ has positive multiplicity in $E(K_r) \otimes_{\mathbf{Z}} \mathbf{Q}_p$ for all $r \geq 1$. Thus, it follows that $r_E(\sigma_{st}^{(r)})$ is positive, and hence so is $s_E(\sigma_{st}^{(r)})$.

**C.** *Conditional results.* In the situation we are now considering, $\Phi_{K_r/\mathbf{Q}} \cap \Psi_E$ is empty and therefore $\mathrm{Hyp}_v$ is certainly satisfied for $K = K_r$ and all primes $v$. To apply corollary 12.2.4, it would suffice to assume that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite and that (13.0.a) holds for the $p+2$ elements of $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$. As mentioned above, it is known that (13.0.a) is valid for $\sigma = \sigma_0$ and $\sigma_{\mathbf{1}}$. If one could verify (13.0.a) for the remaining $\sigma$'s in $\mathrm{Irr}_{\mathcal{F}}(\Delta_0)$, and also verify the finiteness of $\mathrm{Sel}_E(K_{0,\infty})[p]$, then (13.0.a) would actually hold for all $\sigma \in \mathrm{Irr}_{\mathcal{F}_r}(\Delta_r)$ and for all $r \geq 0$. The lower bound (13.1.b) would follow. Unfortunately, both of these verifications seem quite inaccessible at present.

Now assume that $r \geq 1$. For certain $\sigma$'s, one can establish (13.0.a) with much less information. In addition to assuming that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, we will make the following assumption in the rest of this illustration:

$$\text{(13.1.c)} \qquad W_{Sel_p}(E, \sigma_{\boldsymbol{p},1}) \;=\; W_{Del}(E, \sigma_{\boldsymbol{p},1}), \qquad W_{Sel_p}(E, \sigma_{\boldsymbol{p},2}) \;=\; W_{Del}(E, \sigma_{\boldsymbol{p},2}) \quad .$$

As mentioned above, (13.0.a) also holds for $\sigma_0$ and $\sigma_{\mathbf{1}}$. For the representation $\kappa$ of $\Delta_0$ defined in part **D** of section 7.2, we have

$$W_{Sel_p}(E, \kappa) \;=\; W_{Del}(E, \kappa) \;=\; 1 \quad .$$

The first equality follows immediately from the definition of $\kappa$ and assumption (13.1.c). For the second, one can use (13.0.c) together with the facts that $n(\kappa)$ is even and that $det(\kappa) = \sigma_0$. Propositions 7.3.1 and 12.2.3 therefore imply the first of the following equalities:

$$W_{Sel_p}(E, \sigma) \;=\; W_{Del}(E, \sigma) \;=\; 1$$

for all $\sigma \in \mathcal{C}_r$ and $r \geq 1$. The second equality was pointed out before. Furthermore, one can apply those same propositions to the irreducible representations $\sigma = \sigma_\theta^{(r)}$ and $\sigma = \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}}$, where $\theta$ is a character of $B_r$ of order $p^r$. These are elements of $\mathcal{A}_r$ which were defined in remark 7.3.5. The present assumptions again suffice to establish (13.0.a) for those $\sigma$'s.

Assuming that $\varepsilon_{\mathbf{1}}(-N_E) = -1$, and continuing to make the assumptions in the previous paragraph, (13.1.a) and (13.1.c) imply that

$$W_{Sel_p}(E,\sigma_0)W_{Sel_p}(E,\sigma_{\boldsymbol{p},2}) \;=\; W_{Sel_p}(E,\sigma_{\mathbf{1}})W_{Sel_p}(E,\sigma_{\boldsymbol{p},1}) \;=\; -1 \quad . \tag{13.1.d}$$

For any character $\theta$ of $B_r$ of order $p^r$, it follows that $W_{Sel_p}(E,\sigma) = -1$ for $\sigma = \sigma_\theta^{(r)}$ and $\sigma = \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}}$. Letting $\theta$ vary, one gets the following lower bound from those two families of $\sigma$'s and the four irreducible representations of odd dimension:

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; p^{2n+1} + 1 \tag{13.1.e}$$

for $n \geq 1$. Following the notation in section 8.1, consider the field $J_0 \subset K_0$, the fixed subfield for the Borel subgroup $B_0 \subset \Delta_0$, and let $J_0^\sharp$ denote the fixed field for the subgroup of $B_0$ of index 2. Then (13.1.d) is equivalent to the equations $W_{Sel_p}(E/J_0) = -1$, $W_{Sel_p}(E/J_0^\sharp) = +1$. Those equations simply mean that $\mathrm{corank}_{\mathbf{Z}_p}(\mathrm{Sel}_E(J_0)_p)$ is odd and $\mathrm{corank}_{\mathbf{Z}_p}(\mathrm{Sel}_E(J_0^\sharp)_p)$ is even. If one could somehow verifies those two parity statements, then one can obtain (13.1.e) just by using the last part of proposition 12.2.1, and without even considering root numbers. Alternatively, since $X_E(K_\infty)$ is quasi-projective under the present assumptions, one can simply use remark 7.3.5 together with proposition 10.2.1.

As we've indicated, the above considerations show that under the assumptions that we are now making, $s_E(\sigma_{st}^{(r)})$ will be even for $r \geq 1$. In particular, for the specific example mentioned previously (where $E$ has conductor 37, $p \geq 5$ is a prime where $E$ has good, ordinary reduction, and the fields $K_r$ are constructed by adjoining $p$-power torsion points on a certain elliptic curve $A/\mathbf{Q}$ of conductor 1225), one gets the interesting (but conditional) statement that $s_E(\sigma_{st}^{(r)})$ is even and positive for all $r \geq 1$. This behavior seems quite remarkable.

## 13.2 An illustration where $K \subset \mathbf{Q}(E[p^\infty])$.

We again take $F = \mathbf{Q}$ and assume that $p$ is odd. We also make the following assumptions throughout this illustration:

*(i)* The conductor $N_E$ is squarefree. Thus, $E$ has multiplicative reduction at all $l|N_E$ and so $E$ is a semistable curve over $\mathbf{Q}$.

*(ii)* We have $\mathrm{Gal}(\mathbf{Q}(E[p^\infty])/\mathbf{Q}) \cong GL_2(\mathbf{Z}_p)$. Thus, $\mathbf{Q}(E[p^\infty])$ contains a tower of subfields $K_r$ such that $\Delta_r = \mathrm{Gal}(K_r/\mathbf{Q}) \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$.

*(iii)* We have $ord_l(j_E) \not\equiv 0 \pmod{p}$ for all $l|N_E$.

We then have $\Phi_{K_r/\mathbf{Q}} = \Psi_E$ for all $r \geq 0$. Actually, *(i)* and *(iii)* imply *(ii)* for $p \geq 7$. (See proposition 21 in [Se72].) Although formula (13.0.c) cannot be applied, root numbers for

all self-dual representations have been calculated by Rohrlich under the above assumptions. Rohrlich actually does those calculations in [Ro06] when $F$ is arbitrary.

We will mention just part of Rohrlich's calculations. First of all,

$$W_{Del}(E, \sigma_{st}^{(r)}) \;=\; \left(\frac{N_E}{p}\right)$$

for all $r \geq 1$. Rohrlich's formulas for the four odd-dimensional irreducible representations imply that

$$W_{Del}(E, \sigma_0) W_{Del}(E, \sigma_{\mathbf{p},2}) \;=\; W_{Del}(E, \sigma_{\mathbf{1}}) W_{Del}(E, \sigma_{\mathbf{p},1}) \;=\; (-1)^{\frac{p-1}{2}} \quad . \tag{13.2.a}$$

As in section 13.1, we let $\varepsilon_{\mathbf{1}}$ be the Dirichlet character corresponding to $\sigma_{\mathbf{1}}$. But now the conductor of $\varepsilon_{\mathbf{1}}$ is $p$, which is prime to $N_E$, and so we have

$$W_{Del}(E, \sigma_{\mathbf{1}}) = \left(\frac{-N_E}{p}\right) W_{Del}(E, \sigma_0) \;=\; \left(\frac{-N_E}{p}\right)(-1)^{s+1}$$

where $s$ denotes the number of primes where $E$ has split multiplicative reduction. This follows from (13.0.c) and a well-known formula for the root number $W_{Del}(E/\mathbf{Q}) = W_{Del}(E, \sigma_0)$ for semistable elliptic curves over $\mathbf{Q}$. Furthermore, Rohrlich gives the following formula for $\sigma \in \mathcal{A}_r \cup \mathcal{B}_r$, where $r \geq 0$:

$$W_{Del}(E, \sigma) \;=\; (-1)^{\frac{p-1}{2}} \quad .$$

For $\sigma \in \mathcal{C}_r$, excluding the Steinberg representations, Rohrlich shows that $W_{Del}(E, \sigma) = 1$.

**A.** *Predictions.* Assuming that (13.0.a) holds, the above formulas give infinite families of irreducible representations $\sigma$ of the $\Delta_r$'s for which $s_E(\sigma)$ should be odd when $N_E$ is a quadratic nonresidue modulo $p$ or when $p \equiv 3 \pmod 4$. In the first case, the infinite family consists of the Steinberg representations $\sigma_{st}^{(r)}$ for $r \geq 1$. In the second case, the family is $\mathcal{A}_r \cup \mathcal{B}_r$ for $r \geq 0$. These families are disjoint.

**B.** *Unconditional results.* As mentioned before, it is known that (13.0.a) holds for $\sigma = \sigma_0$ and $\sigma = \sigma_{\mathbf{1}}$. However, (13.0.a) is also known to hold for the two $\sigma$'s such that $n(\sigma) = p$. This follows easily from one of the main results in [CFKS], their corollary 2.2, as we will now explain. Those authors prove that if $E$ has a cyclic isogeny of degree $p$ over a number field $J$, then the parity conjecture for the $\mathbf{Z}_p$-corank of $\mathrm{Sel}_E(J)_p$ is true. The result is proved under very broad assumptions on the reduction type for $E$ at primes over $p$.

We will again use the notation from section 8.1, where fields $J_r$ and $J_r^\sharp$ were defined for $r \geq 0$. In particular, $J_0 = K_0^{B_0}$ is indeed the field of rationality for a cyclic isogeny of $E$ of degree $p$. Now $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(J_0)_p\big)$ is equal to the multiplicity of $\mathbf{1}_{B_0}$ in $X_E(K_0) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$,

viewed as a representation space for $B_0$. Frobenius Reciprocity implies that this multiplicity is in turn equal to $s_E(\sigma_0) + s_E(\sigma_{\boldsymbol{p},2})$. This is because $\mathrm{Ind}_{B_0}^{\Delta_0}\big(\mathbf{1}_{B_0}\big)$ is isomorphic to $\sigma_0 \oplus \sigma_{\boldsymbol{p},2}$. (See the second part of remark 2.1.8.) Thus, corollary 2.2 in [CFKS] implies that (13.0.a) holds for that reducible representation. Since (13.0.a) holds for $\sigma_0$, it holds for $\sigma_{\boldsymbol{p},2}$ too. Now, $E$ also has an isogeny of degree $p$ over any field $J$ containing $J_0$. Taking $J = J_0^\sharp$, one can again use Frobenius Reciprocity, the parity result in [CFKS] mentioned above, and the fact that (13.0.a) holds for $\sigma = \sigma_0, \sigma_{\mathbf{1}}$, and $\sigma_{\boldsymbol{p},2}$, to conclude that (13.0.a) holds for $\sigma = \sigma_{\boldsymbol{p},1}$.

Furthermore, applying corollary 2.2 in [CFKS] to the fields $J = J_r$, one deduces (13.0.a) inductively for $\sigma = \sigma_{st}^{(r)}$ and all $r \geq 1$. As a consequence, it follows that if $N_E$ is a quadratic nonresidue modulo $p$, then $W_{Sel_p}\big(E, \sigma_{st}^{(r)}\big) = -1$. One obtains the lower bound

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; p^{n+1} + p^n - p - 1 \tag{13.2.b}$$

for $n \geq 1$. This is unconditional. One gets a better lower bound by including the odd-dimensional representations. Indeed, one can augment the above lower bound by $p+1$ when $p \equiv 1 \pmod 4$ or by either 2 or $2p$ when $p \equiv 3 \pmod 4$, assuming still that $N_E$ is a quadratic nonresidue modulo $p$.

**C.** *Conditional results.* Let us now assume that $p \equiv 3 \pmod 4$. We make no assumption about $N_E$ except for *(i)*. Conjecturally, $s_E(\sigma)$ should then be odd for all $\sigma \in \mathcal{A}_r \cup \mathcal{B}_r$. We make the assumption that $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite. We can then use propositions 7.3.1 and 12.2.3 to prove that $s_E(\sigma)$ is odd for a certain subset of $\mathcal{A}_r$, namely for all $\sigma$'s of the form $\sigma = \sigma_\theta^{(r)}$ or $\sigma = \sigma_\theta^{(r)} \otimes \sigma_{\mathbf{1}}$, where $\theta$ is of order $p^r$ and $r \geq 1$. (See remark 7.3.5 too.) One thereby obtains the lower bound (13.1.e), which is considerably stronger than the unconditional inequality (13.2.b). We can make a further improvement in the lower bound if we also assume that (13.0.a) holds for $\sigma = \sigma_{\boldsymbol{p}+1,j}$ for some $j$. If we make that assumption for all $j$'s, $1 \leq j \leq \frac{p-3}{2}$, then it would follow that $s_E(\sigma)$ is odd for all $\sigma \in \mathcal{A}_r$ and $r \geq 1$.

## 13.3 An illustration where $\mathrm{Gal}(K/\mathbf{Q})$ is isomorphic to $B_n$ or $H_n$.

This section will continue the discussion of the illustrations in sections 8.3 and 8.4. We assume as before that $p$ is an odd prime and that $E$ has good, ordinary reduction at $p$. Suppose that $L = \mathbf{Q}(\mu_p)$ and that $K$ is a finite, Galois extension of $\mathbf{Q}$ containing $L$. We will assume that $[K : L]$ is a power of $p$. Let $\Omega = \mathrm{Gal}(L/\mathbf{Q})$, $D = \mathrm{Gal}(K/\mathbf{Q})$, $P = \mathrm{Gal}(K/L)$, which is the Sylow $p$-subgroup of $D$. It will also be useful to consider the Galois groups $\Omega' = \mathrm{Gal}(L/F)$ and $D' = \mathrm{Gal}(K/F)$, where $F$ is the maximal real subfield of $L$. Thus, $\Omega'$ is the unique subgroup of $\Omega$ of order 2, $D'$ is the unique subgroup of $D$ of index $\frac{p-1}{2}$, the Sylow $p$-subgroup of $D'$ is also $P$, and $D'/P \cong \Omega'$.

The two irreducible, self-dual representations of $\Omega$ are $\sigma_0 = \omega^0$ and $\sigma_{\mathbf{1}} = \omega^{\frac{p-1}{2}}$, the quadratic character of conductor $p$. We denote the two characters of $\Omega'$ by $\rho_0$ and $\rho_{\mathbf{1}}$. The fact that $X_E(L) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a self-dual representation space for $\Omega$ implies the congruence below. The equality is obvious.

$$(13.3.a) \qquad s_E(\rho_0) \ + \ s_E(\rho_{\mathbf{1}}) \ = \ \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \ \equiv \ s_E(\sigma_0) \ + \ s_E(\sigma_{\mathbf{1}}) \qquad (\mathrm{mod}\ 2) \ .$$

Since $E$ has good reduction at $p$, one can apply (13.0.c) to $\sigma_0$ and $\sigma_{\mathbf{1}}$, obtaining

$$(13.3.b) \qquad W_{\mathit{Del}}(E, \sigma_0) W_{\mathit{Del}}(E, \sigma_{\mathbf{1}}) \ = \ \left(\frac{-N_E}{p}\right) \ .$$

Nekovář's parity theorem for $E/\mathbf{Q}$ and the generalization for quadratic fields proved by T. and V. Dokchitser show that (13.0.a) holds when $\sigma$ is $\sigma_0$ or $\sigma_{\mathbf{1}}$. Therefore, $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big)$ is odd if and only if $-N_E$ is a quadratic nonresidue modulo $p$. These remarks are the starting point for most of the results that we will now discuss.

Assume that $E$ has semistable reduction at the primes 2 and 3. Theorem 1.3 in [Dok5] then implies that (13.0.a) holds if $\sigma$ is any irreducible orthogonal representation of $D$. Their theorem is actually valid if $L$ is any finite, abelian extension of $\mathbf{Q}$, $K$ is a Galois extension of $\mathbf{Q}$ containing $L$, and $K/L$ is a $p$-extension. No additional assumption (such as ordinariness) on the reduction type of $E$ at $p$ is needed. It is valid even if $p = 2$.

Corollary 12.2.4 also implies (13.0.a) for all orthogonal $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$, but only under the following assumptions: One assumes that $E$ has good ordinary reduction at $p$ and that $p$ is odd (which will be assumed throughout this section anyway), one assumes that $\mathrm{Hyp}_2$ and $\mathrm{Hyp}_3$ are satisfied, and one assumes that $\mathrm{Sel}_E(L_\infty)[p]$ is finite. That last assumption is crucial for the approach in this paper. Note that $L_\infty = \mathbf{Q}(\mu_{p^\infty})$. We also remark that $\mathrm{Hyp}_2$ and $\mathrm{Hyp}_3$ are certainly satisfied if $E$ is assumed to have semistable reduction at the primes 2 and 3.

**A.** *Lower bounds.* Suppose that we are in a situation where $W_{\mathit{Del}}(E, \sigma) = -1$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ which are orthogonal and have degree $> 1$ (which excludes just $\sigma_0$ and $\sigma_{\mathbf{1}}$). Assuming that $E$ is semistable at 2 and 3, one can then apply the theorem from [Dok5] just cited to obtain the following inequality:

$$(13.3.c) \qquad \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K)_p\big) \ \geq \ \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \ + \ \theta_{\mathit{orth}}(D) - 2 \ ,$$

where $\theta_{\mathit{orth}}(D)$ is as defined in chapter 9. Furthermore, one can get the following lower bound for $\theta_{\mathit{orth}}(D)$ by using the Frobenius-Schur identity and the last part of remark 9.2.2:

$$(13.3.d) \qquad \theta_{\mathit{orth}}(D) \ \geq \ \theta_{D'\text{-}\mathit{orth}}(D) \ = \ \theta_{\mathit{orth}}(D') \ = \ [P : P^+] \ + \ 1 \ .$$

To explain the last equality, note that all of the elements of order 2 in $D'$ are conjugate under the action of $P$. If $\delta'$ is one of them, then the number of elements of order 2 in $D'$ is the index $[P : P^+]$, where $P^+$ denotes the centralizer of $\delta'$ in $P$. The last equality in (13.3.d) follows by applying the Frobenius-Schur identity for $D'$ and using the fact that $\theta_{symp}(D') = 0$, as pointed out in remark 9.2.1. We remark that a self-contained proof of an equivalent equality is given in [MR08]. It is part of their proposition 4.4. They also study the value of $[P : P^+]$ in a variety of cases.

The inequality in (13.3.d) is an equality if and only if $D$ satisfies property **(O)** in chapter 9. This equivalence was pointed out at the end of remark 9.2.2. In particular, we have equality if $D$ is one of the groups $B_n$ or $H_n$. Those groups have the stronger property that all irreducible, self-dual representations have degree divisible by $p-1$, apart from the two one-dimensional representations $\sigma_0$ and $\sigma_{\mathbf{1}}$. Recall also that if $\sigma \in \mathrm{Irr}_{\mathcal{F}}(D)$, then $n(\sigma)$ is divisible by $p-1$ if and only if $\sigma$ is $P$-induced. (See part **A** of section 7.4.)

To illustrate the lower bounds that one can obtain, consider a tower of Galois extensions $K_n$ of $\mathbf{Q}$ such that $\mathrm{Gal}(K_n/\mathbf{Q})$ is isomorphic to either $H_n$ or $B_n$ for all $r \geq 0$. Propositions 8.3.3 and 8.3.7 show the existence of $H_n$-towers for certain primes $p$. The Kummer extensions discussed in section 8.4 provide many $B_n$-towers for any odd prime $p$. Those towers correspond to false Tate extensions of $\mathbf{Q}$. The representation theory for $H_n$ and $B_n$ is described rather precisely in parts **D1**, **D2**, and **D3** of section 7.4. Both those groups satisfy property **(O)** and hence (13.3.d) will be an equality. . One can use the Frobenius-Schur identity to calculate $\theta_{orth}(D)$ when $D = H_n$ or $D = B_n$. The calculation of $[P : P^+]$ for $D = H_n$ is contained in the proof of proposition 9.1.1. It is easy for $D = B_n$. Alternatively, one can use the results in part **D** of section 7.4 to calculate $\theta_{orth}(D)$ directly. In particular, if $D = H_n$, proposition 7.4.4 makes that calculation easy. One finds that

$$\text{(13.3.e)} \qquad \theta_{orth}(H_n) - 2 \;=\; p^{2n+1} - 1 \;, \qquad \theta_{orth}(B_n) - 2 \;=\; p^{n+1} - 1 \;\;.$$

We then get an explicit lower bound for $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big)$ from (13.3.c) if we are in the situation where all of the relevant root numbers are equal to $-1$. The rest of this section discusses some situations where those root numbers can be determined.

**B.** *First situation.* One situation to consider is the following. Suppose that $-N_E$ is a quadratic nonresidue modulo $p$. Suppose also that the function $f_{Del}$ turns out to be $p$-modular. (That function is defined just before proposition 12.2.1. Recall that its domain of definition is $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$.) Furthermore, suppose that all self-dual irreducible representations of $D$, except for $\sigma_0$ and $\sigma_{\mathbf{1}}$, have degree divisible by $p-1$. This last assumption is satisfied when $D \cong H_n$ or $D \cong B_n$. It means that if $\sigma$ is a self-dual, irreducible representation of $D$

and $n(\sigma) > 1$, then $\sigma$ is $P$-induced and therefore

$$\widetilde{\sigma}^{ss} \ \cong \ \left( \bigoplus_{i=0}^{p-2} \widetilde{\omega}^i \right)^{p^a} \quad , \tag{13.3.f}$$

where $p^a = \frac{n(\sigma)}{p-1}$. The assumption that $f_{Del}$ is $p$-modular then implies that

$$W_{Del}(E,\sigma) \ = \ \left( W_{Del}(E,\sigma_0) W_{Del}(E,\sigma_{\mathbf{1}}) \right)^{p^a} \ = \ \left( \frac{-N_E}{p} \right)^{p^a} \ = \ -1$$

for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ with $n(\sigma) > 1$. For the first equality, we are using the fact that $W_{Del}(E, \chi \oplus \check{\chi}) = 1$ for any irreducible representation $\chi$ of $D$. One applies this when $\chi$ is a power of $\omega$ which is not self-dual. The other equalities follow from (13.3.b).

**C.** *$p$-modularity.* It is not always the case that $f_{Del}$ is $p$-modular. This will soon be quite clear. We will study this question by making use of remark 12.2.2. In the notation of that remark, we have

$$f_{Del}(\sigma) \ = \ \prod_{\ell} \ f_{W_\ell}(\sigma)$$

for all $\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$. The product is over all primes $\ell$ of $\mathbf{Q}$, including $\ell = \infty$. We will now discuss various sufficient conditions for $f_{W_\ell}$ to be $p$-modular. We refer the reader to remark 12.2.2 for their justifications. Assume that $p \geq 5$ and that $E$ is semistable at 2 and 3. First of all, if $\ell \notin \Psi_E \bigcap \Phi_{K/\mathbf{Q}}$, then $f_{W_\ell}$ is $p$-modular. Now $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$ is isomorphic to a subgroup of $D$ and hence so is the decomposition subgroup $\Delta_\ell$ for any prime $\ell$. It follows that $\Delta_\ell$ has a normal Sylow $p$-subgroup and that the corresponding quotient group is cyclic of order dividing $p-1$. Thus, $\Delta_\ell$ cannot have a nonabelian quotient of order prime to $p$. Therefore, $f_{W_\ell}$ is $p$-modular for any prime $\ell$ where $E$ has potentially good reduction.

If $\ell$ has potentially multiplicative reduction at $\ell$, but not multiplicative reduction, then the character $\varphi_\ell$ is ramified at $\ell$ and of order prime to $p$. It certainly cannot be a power of $\omega_\ell$ and hence cannot factor through $\Delta_\ell$. Therefore, $f_{W_\ell}$ is $p$-modular for any such $\ell$. Only the primes $\ell \in \Phi_{K/\mathbf{Q}}$ where $E$ has multiplicative reduction remain to be considered.

Assume that $\ell$ has odd order modulo $p$. That means that the order of $\omega_\ell$ is odd. If $E$ has split, multiplicative reduction, then $f_{W_\ell}$ is $p$-modular, as explained in remark 12.2.2. If $E$ has nonsplit, multiplicative reduction at $\ell$, then $\varphi_\ell$ has even order and therefore cannot factor through $\Delta_\ell$. It follows that $f_{W_\ell}$ is $p$-modular in that case too.

Let $\Psi_E^{(st)}$ denote the subset of $\Psi_E$ consisting of the primes where $E$ has semistable reduction. Thus, $\ell \in \Psi_E^{(st)}$ if and only if $E$ has either split or nonsplit multiplicative reduction at

$\ell$. For brevity, we denote $\Phi_{K/\mathbf{Q}} \bigcap \Psi_E^{(st)}$ by $S_{E,K}$ in this illustration. Let $\Psi_E^{(ev)}$ consist of the primes $\ell \in \Psi_E$ which have even order modulo $p$. Let $\Psi_E^{(nr)}$ denote the subset of $\Psi_E$ consisting of primes $\ell$ which are quadratic nonresidues modulo $p$. Thus, we have $\Psi_E^{(nr)} \subseteq \Psi_E^{(ev)}$. Note that $\ell \in \Psi_E^{(nr)}$ if and only if $\frac{p-1}{w_\ell}$ is odd, where $w_\ell$ denotes the order of $\ell$ modulo $p$. Hence the sets $\Psi_E^{(nr)}$ and $\Psi_E^{(ev)}$ are different when $p \equiv 1 \pmod 4$. We let $S_{E,K}^{(ev)}$ and $S_{E,K}^{(nr)}$ denote $S_{E,K} \bigcap \Psi_E^{(ev)}$ and $S_{E,K} \bigcap \Psi_E^{(nr)}$, respectively. Obviously, we have $S_{E,K}^{(nr)} \subseteq S_{E,K}^{(ev)}$. The two sets are equal if $p \equiv 3 \pmod 4$.

The above discussion shows that $f_{W_\ell}$ is $p$-modular if $\ell \notin S_{E,K}^{(ev)}$. Now $f_{Del}$ is clearly $p$-modular if $f_{W_\ell}$ is $p$-modular for all $\ell$. Thus, we have the following result.

**Proposition 13.3.1.** *Assume that $p \geq 5$, that $E$ has semistable reduction at 2 and 3, and that the set $S_{E,K}^{(ev)}$ is empty. Then $f_{Del}$ is $p$-modular.*

Note that $S_{E,K}^{(ev)} \subseteq \Phi_{K/\mathbf{Q}} \bigcap \Psi_E^{(ev)}$. The hypothesis that $S_{E,K}^{(ev)}$ be empty is therefore very closely related to the following hypothesis occurring in theorem 1.1 in [MR08]:

*If $l \in \Psi_E$, then either $l$ is unramified in the $p$-extension $K/L$ or $l$ is split in the quadratic extension $L/F$.*

This means that $\Phi_{K/\mathbf{Q}} \bigcap \Psi_E^{(ev)}$ is empty, and hence implies that $S_{E,K}^{(ev)}$ is also empty. The conclusion in that theorem of Mazur and Rubin is that

$$s_E(\rho) \ \equiv \ \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \pmod 2 \quad . \tag{13.3.g}$$

for every irreducible, self-dual representation $\rho$ of $D'$, excluding $\rho_0$ and $\rho_{\mathbf{1}}$. This is a certain congruence relation for $D'$. Their result is equivalent to saying that the function $f_{Sel}$ on $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D')$ is $p$-modular. If one also assumes that $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big)$ is odd, then their result implies the following lower bound.

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K)_p\big) \ \geq \ \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \ + \ \theta_{orth}(D') - 2 \quad ,$$

One should compare this with (13.3.c). Mazur and Rubin also prove the formula for $\theta_{orth}(D')$ in (13.3.d) and study its value in a variety of cases. Note that their results don't actually involve root numbers. Also, just as with theorem 1.3 in [Dok5], theorem 1.1 in [MR08] is far more general than the special case under consideration here.

It is worth pointing out that if $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$, if $\sigma$ is $D'$-orthogonal, and if $\rho$ is an irreducible constituent in $\sigma|_{D'}$, then

$$s_E(\sigma) \ \equiv \ s_E(\rho) \pmod 2 \quad .$$

This congruence follows from Frobenius Reciprocity by using the facts that $X_E(K)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$ is a self-dual representation space for $D$, that $\sigma$ is the only irreducible constituent in $\mathrm{Ind}_{D'}^{D}(\rho)$ which is self-dual, and that the multiplicity of $\sigma$ in $\mathrm{Ind}_{D'}^{D}(\rho)$ is 1.

**D.** *Towers with Galois groups $H_n$ and $B_n$.* In the rest of this illustration, we will consider a tower of extensions $K_n$ such that $\mathrm{Gal}(K_n/\mathbf{Q})$ is isomorphic to $H_n$ or $B_n$ for $n \geq 0$. We continue to assume that $p \geq 5$ and that $E$ has semistable reduction at 2 and 3. Furthermore, we will make the following restrictive assumption concerning ramification:

$$\Phi_{K_n/\mathbf{Q}} \;=\; \Phi_{K_0/\mathbf{Q}} \tag{13.3.h}$$

for all $n \geq 0$. Thus, the sets $S_{E,K_n}^{(ev)}$ and $S_{E,K_n}^{(nr)}$ will also be independent of $n$. To simplify notation in the discussion, we will just write $K$ for any one of the fields in the tower and identify $D = \mathrm{Gal}(K/\mathbf{Q})$ with either $H_n$ or $B_n$. In particular, $U_n$ will be regarded as a specific subgroup of $D$. The above ramification assumption then implies that the inertia subgroup $I_\ell(K/\mathbf{Q})$ of $D$ for any prime $\ell \in \Phi_{K/\mathbf{Q}}$ is conjugate to $U_n$. Thus we can simply assume that $I_\ell(K/\mathbf{Q}) = U_n$. Under these assumptions, we can weaken the hypothesis in proposition 13.3.1 by restricting $f_{Del}$ to the following subset of $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$:

$$\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp \;=\; \{\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D) \;\mid\; \sigma\otimes\sigma_{\mathbf{1}} \cong \sigma\;\} \quad .$$

Note that if $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ and $n(\sigma) > 1$, then $\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$. In fact, $\sigma\otimes\chi \cong \sigma$ for all $\chi \in \widehat{\Omega}$ since $\sigma$ is $P$-induced. In addition, $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$ contains the regular representation of $\Omega$, which we will denote by $\sigma_\Omega$ and consider as a representation of $D$. We have $n(\sigma_\Omega) = p-1$. The representation $\sigma_0 \oplus \sigma_{\mathbf{1}}$ is also in $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$.

**Proposition 13.3.2.** *In addition to the above assumptions, assume that $S_{E,K}^{(nr)}$ is empty. Then the restriction of $f_{Del}$ to $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$ is $p$-modular. Furthermore, assume also that $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ and that $n(\sigma) > 1$. Then*

$$W_{Del}(E,\sigma) \;=\; W_{Del}(E,\sigma_0)W_{Del}(E,\sigma_{\mathbf{1}}) \;=\; \left(\frac{-N_E}{p}\right) \quad .$$

*In particular, if $-N_E$ is a quadratic nonresidue modulo $p$, then $W_{Del}(E,\sigma) = -1$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ such that $n(\sigma) > 1$. As a consequence, $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big)$ is odd and the lower bounds for $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big)$ given by* (13.3.c) *and* (13.3.e) *hold.*

*Proof.* As discussed above, if $\ell \notin S_{E,K}$, then $f_{W_\ell}$ is $p$-modular on $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)$, and hence on the subset $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$. We are now assuming that if $\ell \in S_{E,K}$, then $\ell$ is a quadratic residue

modulo $p$. This means that $w_\ell$ divides $\frac{p-1}{2}$. We can also assume that $w_\ell$ is even since we already know that $f_{W_\ell}$ is $p$-modular otherwise. As before, we let $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$. Then $\omega_\ell = \omega|_{\Delta_\ell}$ has order $w_\ell$, where $\Delta_\ell$ is a decomposition subgroup of $\Delta$ for a prime above $\ell$. To show that $f_{W_\ell}$ is $p$-modular, we refer to the discussion in remark 12.2.2. It suffices to show that the function $f_{\varphi_\ell}$ defined in proposition 11.2.7, where $\varphi_\ell$ is a certain power of $\omega_\ell$, is $p$-modular when restricted to the set $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$. We will simply prove that $f_{\varphi_\ell}(\sigma) = 1$ for all $\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$. Equivalently, we will show that $\langle \sigma_\ell, \varphi_\ell \rangle$ is even for such $\sigma$, where $\sigma_\ell$ denotes the restriction of $\sigma$ to $\Delta_\ell$.

The assumption about $\ell$ means that $\omega_\ell^{\frac{p-1}{2}}$ is trivial. Recall that we are also assuming that $I_\ell(K/\mathbf{Q}) = U_n$. Thus, $U_n$ is a normal subgroup of $\Delta_\ell$. The normalizer of $U_n$ in $D$ is $B_n$ and so $\Delta_\ell$ is a subgroup of $B_n$. As in part **D1** of section 7.4, we let $\Omega_n$ denote the subgroup of $B_n$ consisting of elements represented by diagonal matrices of order $p-1$. Thus, $\Omega_n$ can be identified with $\Omega$ by the projection map $D \to \Omega$. Then $\Delta_\ell$ is a subgroup of $\Omega_n U_n$, the unique subgroup of $B_n$ containing $U_n$ as a subgroup of index $p-1$.

Suppose that $\sigma \in \mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$. Consider the restriction of $\sigma$ to $\Omega_n U_n$. The 1-dimensional constituents of $\sigma|_{\Omega_n U_n}$ are trivial on $U_n$. They are of the form $\omega^j|_{\Omega_n U_n}$ and can be identified with the corresponding character $\chi = \omega^j$ of $\Omega$. Since $\sigma \otimes \sigma_{\mathbf{1}} \cong \sigma$, where $\sigma_{\mathbf{1}} = \omega^{\frac{p-1}{2}}$, it follows that if $\chi$ is a constituent in $\sigma|_{\Omega_n U_n}$, then so is $\chi\omega^{\frac{p-1}{2}}$. Also, the multiplicities are equal. The characters $\chi$ and $\chi\omega^{\frac{p-1}{2}}$ have the same restriction to $\Delta_\ell$. Therefore, each power of $\omega_\ell$ occurs with even multiplicity in $\sigma_\ell$. In particular, $\langle \sigma_\ell, \varphi_\ell \rangle$ is indeed even. This proves the $p$-modularity of $f_{W_\ell}$ on the set $\mathrm{Rep}_{\mathcal{F}}^{(sd)}(D)^\sharp$ for $\ell \in S_{E,K}$, and hence for all $\ell$. The stated assertion about $f_{Del}$ is a consequence.

Now suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ and that $n(\sigma) > 1$. Then $\sigma$ is $P$-induced. The isomorphism (13.3.f) and the remarks after it then imply the following equalities.

$$f_{Del}(\sigma) \;=\; f_{Del}(\sigma_\Omega) \;=\; f_{Del}(\sigma_0 \oplus \sigma_{\mathbf{1}}) \quad .$$

This gives the assertion concerning the root numbers. The final statement concerning coranks of Selmer groups then follows from the results of J. Nekovář and of T. and V. Dokchitser discussed at the beginning of this illustration. □

We continue making all the assumptions in proposition 13.3.2, except for the assumption that $S_{E,K}^{(nr)}$ be empty. Suppose that $\ell \in S_{E,K}^{(nr)}$. In particular, $\ell$ has even order modulo $p$. Suppose that $\sigma \in \mathrm{Irr}_{\mathcal{F}}^{(sd)}(D)$ and $n(\sigma) > 1$. Recall that $f_{\varphi_\ell}(\sigma) = (-1)^{\delta_{E,\ell}(\sigma)}$. Applying proposition 8.3.8 to $\sigma$, we obtain

$$\delta_{E,\ell}(\sigma) \;=\; \frac{\dim_{\mathcal{F}}\bigl(W_\sigma^{U_n}\bigr)}{w_\ell} \quad ,$$

where we have used the fact that $\alpha(E,\ell)=1$. The fact that $\sigma\otimes\chi\cong\sigma$ for all $\chi\in\widehat{\Omega}$ implies that $\dim_{\mathcal{F}}\bigl(W_\sigma^{U_n}\bigr)$ is divisible by $p-1$. We will write this dimension as $(p-1)b(\sigma)$, where $b(\sigma)$ is a nonnegative integer. Applying proposition 8.3.8 to $\sigma_\Omega$ gives

$$\delta_{E,\ell}(\sigma_\Omega) \;=\; \frac{p-1}{w_\ell} \quad .$$

Referring to remark 12.2.2, we know that $f_{W_\ell}f_{\varphi_\ell}$ is $p$-modular. Using that fact together with (13.3.f), we obtain

$$f_{W_\ell}(\sigma)/f_{W_\ell}(\sigma_\Omega) \;=\; f_{\varphi_\ell}(\sigma)/f_{\varphi_\ell}(\sigma_\Omega) \;=\; (-1)^{\left(\delta_{E,\ell}(\sigma)-\delta_{E,\ell}(\sigma_\Omega)\right)} \quad .$$

Thus, we have $W_{Del}(E,\sigma) \;=\; W_{Del}(E,\sigma_0)W_{Del}(E,\sigma_{\mathbf{1}})(-1)^{a(\sigma)} \;=\; \left(\frac{-N_E}{p}\right)(-1)^{a(\sigma)}$, where

$$a(\sigma) \;=\; \sum_\ell \left(\frac{\dim_{\mathcal{F}}\bigl(W_\sigma^{U_n}\bigr)}{w_\ell} \;-\; \frac{p-1}{w_\ell}\right) \;=\; \bigl(b(\sigma)-1\bigr)\cdot\sum_\ell \frac{p-1}{w_\ell} \quad .$$

In the sums, $\ell$ varies over the set $S_{E,K}^{(nr)}$. However, note that if a prime $\ell$ is a quadratic residue modulo $p$, then $\frac{p-1}{w_\ell}$ is even. Therefore, if one wishes, one can allow the above sums to be over all primes $\ell\in S_{E,K}$ instead. The extra terms are even.

Thus, we have the congruence $a(\sigma)\equiv\bigl(b(\sigma)-1\bigr)\cdot|S_{E,K}^{(nr)}| \pmod 2$ and therefore the value of $W_{Del}(E,\sigma)$ is determined by $\left(\frac{-N_E}{p}\right)$ and the parities of $b(\sigma)$ and $|S_{E,K}^{(nr)}|$. The results of Nekovář and T. and V. Dokchitser then imply the following congruence:

$$s_E(\sigma) \;\equiv\; \mathrm{corank}_{\mathbf{Z}_p}\bigl(\mathrm{Sel}_E(L)_p\bigr) \;+\; \bigl(b(\sigma)-1\bigr)\cdot|S_{E,K}^{(nr)}| \pmod 2 \quad . \tag{13.3.i}$$

We now reintroduce the subscripts on the $K$'s. If the right hand side in (13.3.i) is odd for all $\sigma\in\mathrm{Irr}_{\mathcal{F}}^{(sd)}\bigl(\mathrm{Gal}(K_n/\mathbf{Q})\bigr)$, then the lower bounds on $\mathrm{corank}_{\mathbf{Z}_p}\bigl(\mathrm{Sel}_E(K_n)_p\bigr)$ discussed earlier will hold. These remarks are valid under the assumptions that we are now making. In particular, assumption (13.3.h) is needed.

Suppose that $D=B_n$. The self-dual irreducible representations of $D$ of degree $>1$ are the $\gamma_r$'s defined in **D1** of section 7.4, where $0\le r\le n$. The irreducible constituents of $\gamma_r|_{U_n}$ are the characters of $U_n$ of order $p^{r+1}$ and hence are all nontrivial. Hence $\dim_{\mathcal{F}}\bigl(W_{\gamma_r}^{U_n}\bigr)=0$. Thus, $b(\gamma_r)=0$. The above discussion leads us to the following formulas for root numbers:

$$W_{Del}(E,\gamma_r) \;=\; \left(\frac{-N_E}{p}\right)\prod_{l\in S_{E,K_0}}\left(\frac{l}{p}\right) \;=\; (-1)^{\mathrm{corank}_{\mathbf{Z}_p}\left(\mathrm{Sel}_E(L)_p\right)}\cdot\prod_{l\in S_{E,K_0}}\left(\frac{l}{p}\right) \quad .$$

We write $K_0$ here because we continue to assume (13.3.h). If one also makes the assumption that $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) + |S^{(nr)}_{E,K_0}|$ is odd, then the above formula and theorem 1.3 in [Dok5] give the following inequality:

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \;+\; p^{n+1} \;-\; 1 \quad .$$

For example, we might have $K_n = \mathbf{Q}\big(\mu_{p^{n+1}},\ \sqrt[p^{n+1}]{m}\ \big)$, where $m$ is an integer. The ramification assumption (13.3.h) means that if $\ell | m$ and $\ell \neq p$, then $p \nmid ord_\ell(m)$. If that assumption is satisfied, then

$$S_{E,K_n} \;=\; S_{E,K_0} \;=\; \{\ell \;\mid\; \ell \textit{ divides } m, \textit{ and } \ell \in \Psi^{(st)}_E \;\} \quad .$$

The above formula for the root numbers $W_{Del}(E,\gamma_r)$ was proved in this case by V. Dokchitser and is mentioned in (A.33) in the appendix to [Dok6]. If one allows $ord_\ell(m)$ to be divisible by $p$ for some $\ell$'s dividing $m$, then the formula for $W_{Del}(E,\gamma_r)$ is still valid if $r$ is sufficiently large if one replaces $K_0$ by $K_n$, where $n \geq r$. This is so because the index of $I_\ell(K_n/\mathbf{Q})$ in $U_n$ will become constant as $n$ increases. Consequently, one still gets a lower bound for $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big)$ of the form $p^{n+1} - c$, where $c$ is a constant.

Suppose now that $D = H_n$. Suppose that $0 \leq r \leq n$. According to proposition 7.4.4, $H_r$ has certain self-dual irreducible representations $\sigma$ of degree $(p-1)p^r$. They are the faithful irreducible representations of $H_r$. Up to isomorphism, there are $p^r$ such representations. Regarding any such representation $\sigma$ as a representation of $H_n$, we have $\sigma|_{B_n} \cong \gamma_r$. Therefore, $\dim_{\mathcal{F}}\big(W_\sigma^{U_n}\big) = 0$ and hence $b(\sigma) = 0$. As a consequence, the corresponding root number is given by the same formula as the one given above for $W_{Del}(E,\gamma_r)$. That is, assuming that (13.3.h) is satisfied and that $\sigma$ is $r$-primitive and has degree $p^r(p-1)$, the value of $W_{Del}(E,\sigma)$ is determined by the parity of the quantity $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) + |S^{(nr)}_{E,K_0}|$. If that quantity is odd, then we get the following inequality:

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \;+\; \frac{p^{2n+2}-1}{p+1} \quad .$$

This bound is not as good as (13.3.c). It only includes some of the terms in $\theta_{orth}(H_n) - 2$.

In contrast, consider the non-faithful irreducible representation $\sigma$ of $H_r$ which occurs as a constituent in $\sigma_r^{(st)}|_{H_r}$ according to proposition 7.4.4. Then $n(\sigma) = (p-1)p^{r\text{-}1}$. For $1 \leq r \leq n$, we can regard $\sigma$ as a representation of $D = H_n$. For such $\sigma$, we have

$$\dim_{\mathcal{F}}\big(W_\sigma^{U_n}\big) \;=\; \langle \sigma_r^{(st)}|_{U_r}, \mathbf{1}_{U_r}\rangle \;=\; (p-1)p^{[(r\text{-}1)/2]} \quad ,$$

as mentioned in section 8.2. Therefore, $b(\sigma)$ is odd, $a(\sigma)$ is even, and we have the formula

$$W_{Del}(E,\sigma) \;=\; \left(\frac{-N_E}{p}\right) \quad .$$

If $-N_E$ is a quadratic nonresidue modulo $p$, or equivalently if $\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big)$ is odd, then all of these root numbers are $-1$ and one gets the inequality

$$\mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(K_n)_p\big) \;\geq\; \mathrm{corank}_{\mathbf{Z}_p}\big(\mathrm{Sel}_E(L)_p\big) \;+\; p^n - 1$$

even if $|S^{(nr)}_{E,K_0}|$ happens to be odd. Of course, if $|S^{(nr)}_{E,K_0}|$ is even, one obtains a much better inequality because of the contribution from the $r$-primitive representations considered in the previous paragraph.

# References


[Alp] J. L. Alperin, Local representation theory, Cambridge Studies in Advanced Math. **11** (1986), Cambridge University Press.

[BiSt] B. J. Birch, N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295-299.

[CFKS] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, to appear in J. Alg. Geom. (2009).

[CoGr] J. Coates, R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), 129-174.

[CS00] J. Coates, R. Sujatha, Galois Cohomology of Elliptic Curves, (2000), Tata Institute of Fundamental Research, Narosa Publishing House.

[CS05] J. Coates, R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), 809-839.

[Cre] J. Cremona, Algorithms for modular elliptic curves, (1992) Cambridge University Press.

[CuRe] C. W. Curtis, I. Reiner, Methods of representation theory with applications to finite groups and orders, (1981), John Wiley and Sons.

[Del] P. Deligne, *Les constantes des équations fonctionelles des fonctions L*, Lecture Notes in Math. **349** (1973), 501-595.

[Dok1] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) **91** (2005), 300-324.

[Dok2] T. Dokchitser, V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662-679.

[Dok3] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, to appear in Annals of Math.

[Dok4] T. Dokchitser, V. Dokchitser, *Self-duality of Selmer groups*, Proc. Cam. Phil. Soc. **146** (2009), 257-267.

[Dok5] T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*, preprint.

[Dok6] T. Dokchitser, V. Dokchitser, *Computations in non-commutative Iwasawa theory*, with an appendix by J. Coates and R. Sujatha, Proc. London Math. Soc. **94** (2006), 211-272.

[Dri] M. Drinen, *Iwasawa $\mu$-invariants of elliptic curves and their symmetric powers*, J. of Number Theory **102** (2003), 191-213.

[Fei] W. Feit, Characters of finite groups, (1967), Benjamin.

[FeWa] B. Ferrero, L. Washington, *The Iwasawa invariant $\mu_p$ vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377-395.

[Fis] T. Fisher, *Descent calculations for the elliptic curves of conductor 11*, Proc. London Math. Soc. **86** (2003), 583-606.

[Gre] C. Greither, *Some cases of Brumer's conjecture for abelian CM extensions of totally real fields*, Math. Zeit. **233** (2000), 515-534.

[Gr89] R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Math. **17** (1989), 97-137.

[Gr91] R. Greenberg, *Iwasawa theory for motives*, LMS Lecture Note Series **153** (1991), 211-234.

[Gr94a] R. Greenberg, *Trivial zeros of p-adic L-functions*, Contemporary Math. **165** (1994), 149-173.

[Gr94b] R. Greenberg, *Iwasawa theory and p-adic deformations of motives*, Proceedings of Symposia in Pure Math. **55** II (1994), 193-223.

[Gr99] R. Greenberg, *Iwasawa theory for elliptic curves*, Lecture Notes in Math. **1716** (1999), 51-144.

[Gr01] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, IAS/Park City Mathematics Series **9** (2001), 409-464.

[Gr09a] R. Greenberg, *Galois representations with open image*, in preparation.

[Gr09b] R. Greenberg, *Selmer groups for elliptic curves over p-adic Lie extensions*, in preparation.

[GrVa] R. Greenberg, V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), 17-63.

[Guo] L. Guo, *General Selmer groups and critical values of Hecke L-functions*, Math. Ann. **297** (1993), 221-233.

[HaMa] Y. Hachimori, K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. **8** (1999), 581-601.

[HaSh] Y. Hachimori, R. Sharifi, *On the failure of pseudo-nullity of Iwasawa modules*, J. Algebraic Geom. **14** (2005), 567-591.

[HaVe] Y. Hachimori, O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Documenta Math. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 443-478.

[Har] M. Harris, *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Invent. Math. **51** (1979), 123-141.

[How] L. Howe, *Twisted Hasse-Weil L-functions and the rank of Mordell-Weil groups*, Can. J. of Math. **49** (1997), 749-771.

[Iwa] K. Iwasawa, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. **33** (1981), 263-288.

[JaKe] G. James, A. Kerber, The representation theory of the symmetric group, Encyclopedia of Mathematics and its Applications **16** (1981), Addison-Wesley.

[Kat] K. Kato, *p-adic Hodge theory and values of zeta functions of modular curves*, Astérisque **295** (2004), 117-290.

[Kid] Y. Kida, *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory **12** (1980), 519-528.

[Kim1] B. D. Kim, *The parity theorem of elliptic curves at primes with supersingular reduction*, Comp. Math. **143** (2007), 47-72.

[Kim2] B. D. Kim, *The parity conjecture over totally real fields for elliptic curves at supersingular reduction primes*, to appear in J. Number Theory.

[KrTu] K. Kramer, J. Tunnell, *Elliptic curves and local $\epsilon$-factors*, Comp. Math. **46** (1982), 307-352.

[Ma72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183-266.

[Ma78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129-162.

[MR07] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Math. **166** (2007) 581-614.

[MR08] B. Mazur, K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. Jour. **143** (2008) 437-461.

[MaSw] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1-61.

[MoNg] A. Movahhedi, T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Prog. Math. **81**, Birkhauser (1990), 155-200.

[Mon] P. Monsky, *Generalizing the Birch-Stephens theorem*, Math. Zeit. **221** (1996), 415-420.

[Nek1] J. Nekovář, *On the parity of ranks of Selmer groups II*, Comptes Rendus de l'Acad. Sci. Paris, Serie I, **332** (2001), No. 2, 99 - 104

[Nek2] J. Nekovář, Selmer complexes, Astérisque **310** (2006).

[Nek3] J. Nekovář, *On the parity of ranks of Selmer groups III*, Documenta Math. **12** (2007), 243-274.

[Nek4] J. Nekovář, *On the parity of ranks of Selmer groups IV*, to appear in Comp. Math.

[Nek5] J. Nekovář, *Growth of Selmer groups of Hilbert modular forms over ring class fields*, Ann. E. N. S. **41** (2008), 1003 - 1022.

[Nic] A. Nichifor, *Iwasawa theory for elliptic curves with cyclic isogenies,* University of Washington Ph. D. thesis, 2004,

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundlehren der Math. Wissenschaften **323** (2000), Springer.

[Rei] I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. **8** (1957), 142-146.

[Ro94] D. Rohrlich, *Elliptic curves and the Weil-Deligne group*, in *Elliptic Curves and Related Topics*, CRM Proceedings and Lecture Notes **4** (1994), 125-157.

[Ro96] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Comp. Math. **100** (1996), 311-349.

[Ro06] D. Rohrlich, *Root numbers of semistable elliptic curves in division towers*, Math. Research Letters **13** (2006), 359-376.

[Ro07] D. Rohrlich, *Scarcity and abundance of trivial zeros in division towers*, J. Alg. Geom. **17** (2008), 643-675.

[Ro08] D. Rohrlich, *Galois invariance of local root numbers*, preprint.

[Ro09] D. Rohrlich, *Root numbers*, in preparation.

[RuSi] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representations*, in Elliptic curves, modular forms, and Fermat's last theorem, Hong Kong, International Press, (1995), 148-161.

[Sch] P. Schneider, *p-Adic height pairings II*, Invent. Math. **79** (1985), 329-374.

[Se68] J. P. Serre, Corps locaux, Actualités scientifiques et industrialles **1296**, (1968), Hermann.

[Se72] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Se77] J. P. Serre, Linear representations of finite groups, Graduate Texts in Math. (1977), Springer.

[SeTa] J. P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492-517.

[Shu] M. Shuter, *Descent on division fields of elliptic curves*, University of Cambridge Ph. D. thesis (2006).

[Sil] A. Silberger, $PGL_2$ over the $p$-adics, its representations, spherical functions, and Fourier series, Lecture Notes in Math. **166** (1970), Springer.

[Tri] M. Trifkovic, *On the vanishing of $\mu$-invariants of elliptic curves over* $\mathbf{Q}$, Canadian Jour. of Math. **57** (2005), 812-843.

[Za1] G. Zábrádi, *Characteristic elements, pairings, and functional equations over the false Tate curve extension*, Math. Proc. Camb. Phil. Soc. **144** (2008), 535-557.

[Za2] G. Zábrádi, *Pairings and functional equations over the $GL_2$-extension*, preprint.