# Mordell-Weil groups as Galois modules

Thomas Vavasour and Christian Wuthrich

21st June 2023

**Abstract**

We study the action of the Galois group $G$ of a finite extension $K/k$ of number fields on the points on an elliptic curve $E$. For an odd prime $p$, we aim to determine the structure of the $p$-adic completion of the Mordell-Weil group $E(K)$ as a $\mathbb{Z}_p[G]$-module only using information of $E$ over $k$ and the completions of $K$.

## Contents



## 1 Introduction

Let $E$ be an elliptic curve defined over a number field $k$ and let $G$ be the Galois group of a finite Galois extension $K/k$. The main aim is to study the action of $G$ on the group $E(K)$. In this investigation we wish to go deeper than to decompose $E(K) \otimes \mathbb{C}$ into irreducible representations of $G$, instead we are interested in the integral representation theory of $E(K)$. Since $\mathbb{Z}[G]$-modules can be very complicated even for small groups $G$, we will $p$-adically complete $E(K)$ to get a $\mathbb{Z}_p[G]$-module for a prime $p$. If $p$ does not divide the group order of $G$, we would recover only the structure of $E(K) \otimes \mathbb{Q}$ and so we will focus on the case when $p$ divides the degree $[K : k]$.

Throughout the paper we will assume that $p$ is an **odd** prime, that $E(K)$ contains no $p$-torsion elements (Assumption 2 in Section 6) and that the $p$-primary parts of the Tate-Shafarevich groups $Ш(E/L)$ are finite (Assumption 1 in Section 6) for all elliptic curves $E$ and number fields $L$. The main object of study is the $p$-adic completion $M = E(K) \otimes \mathbb{Z}_p$ of $E(K)$ viewed as a $\mathbb{Z}_p[G]$-module.

Here is an example of the type of theorem obtained from our methods.

**Theorem 1.** Assume that $G$ is isomorphic to the dihedral group $D_p$ with $2p$ elements. Let $F$ be the intermediate field with $[F : k] = 2$ and let $\breve{E}$ be the quadratic twist of $E$ with respect to $F$. Assume that $Ш(E/k)$ and $Ш(\breve{E}/k)$ contain no elements of order $p$, that $K/F$ is everywhere unramified and that all places $v$ such that $p$ divides the Tamagawa number $c_v$ of $E$ or $\breve{E}$ split in $K/F$. If $\operatorname{rk} E(k) + \operatorname{rk} \breve{E}(k) \leqslant 1$, then the $\mathbb{Z}_p[G]$-isomorphism class of $M = E(K) \otimes \mathbb{Z}_p$ is completely determined by $\operatorname{rk} E(k)$, $\operatorname{rk} \breve{E}(k)$ and local information for $E/K$. Furthermore, in all cases $\operatorname{rk} E(K) \leqslant p$.

By "local information for $E/K$", we mean knowledge of $E$ that can be computed over the completions $K_w$ of $K$ at all places $w$ in $K$. In practice, one only needs to know the type of reduction, Tamagawa numbers and the number of points in the reduction at a finite number of finite places. For $k = \mathbb{Q}$, the above gives a fast way to determine $M$ for most curves (see Theorem 45). It is often much harder to calculate explicitly the group $E(K)$: Searching for points over large degree fields $K$ can be very costly as well as bounding the rank by an infinite descent because the class groups involved may be hard to determine.

Theorem 1 is stated for the dihedral group $D_p$ since for this group we know the 6 distinct isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-modules. Even when the conditions of the theorem do not hold, we can very often determine the decomposition of $M$ into a direct sum of these indecomposable modules using only easily accessible information. See Sections 7.1.1 and 7.3 for examples illustrating this, and Example I for which we cannot determine $E$ without having to search for points.

For certain groups, including $D_p$, a theorem by Torzewski [44] lists the invariants we need to know to determine $M$. (See Proposition 43.) Our task is to express them in terms of arithmetic invariants of $E$. At least conjecturally, we could gain the knowledge of $E(K) \otimes \mathbb{Q}$ from the order of vanishing of $L$-functions of $E$ twisted by the irreducible representations of $G$. Instead the so-called Dokchitser regulator constants (see (3) for a definition) and the group cohomology $H^1(G, M)$ are not as easy to access. This is the main reason that we focus our attention on the dihedral and cyclic case here.

As expected the $\mathbb{Z}_p[G]$-structure of $M$ is linked to the $p$-primary part $Ш(E/K)[p^\infty]$ of the Tate-Shafarevich group. Here is another simplified statement that can be deduced from our methods.

**Theorem 2.** Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a cyclic extension of degree $p$. Write $u_1$ for the number of primes $\ell$ such that $p$ divides the Tamagawa number $c_\ell$ and $\ell$ is inert in $K/\mathbb{Q}$. Denote by $u_2$ the number of primes $\ell$ that ramify in $K/\mathbb{Q}$ such that the number of points in the reduction of $E$ over $\ell$ is divisible by $p$. If $L(E, \chi, 1) \neq 0$ where $\chi$ is a primitive character of $K/\mathbb{Q}$ and $u_1 + u_2 > \operatorname{rk} E(\mathbb{Q})$, then the $\mathbb{F}_p$-dimension of $Ш(E/K)[p]$ is at least $u_1 + u_2 - \operatorname{rk} E(\mathbb{Q})$.

We produce this bound by studying the control theorem which links the $p$-primary Selmer group of $E/k$ with the $G$-invariant subspace of the $p$-primary Selmer group of $E/K$. The cokernel of the restriction map $\alpha$ between them can be determined completely and we can effectively calculate it using only local information and information of $E$ over $k$. See Proposition 29 for a precise statement.

One important ingredient for this calculation is to understand the cokernel of the norm map $E(K_w) \to E(k_v)$ where $w$ is a place in $K$ and $v$ the place below $w$. This is analogous to the main question in local class field theory and it has been studied before. In Proposition 13, we will see that in the case that the ramification index $e_v$ is not divisible by $p$, the cokernel is cyclic determined by the Tamagawa number $c_v$ and the residue class degree $f_v$.

This leads to the local question. The $p$-adic completion $E(K_w) \hat{\otimes} \mathbb{Z}_p$ of $E(K_w)$ is finite unless $K_w$ is a $p$-adic field. If $K_w$ is a $p$-adic field, then $E(K_w) \otimes \mathbb{Q}_p$ is isomorphic to $\mathbb{Q}_p[G_w]$ where $G_w$ is the Galois group of $K_w/k_v$. We determine the $\mathbb{Z}_p[G_w]$-structure explicitly for all reduction types, when $K_w$ is the unramified cyclic extension of $k_v = \mathbb{Q}_p$ in Theorem 26. Here is a simplified statement not covering all cases.

**Theorem 3.** Let $E$ be an elliptic curve over $\mathbb{Q}_p$ with $p \geqslant 5$ and let $K_w/\mathbb{Q}_p$ be the unramified extension of degree $p$. Suppose that the reduction is anything but split multiplicative. Then we are in one of the following three cases:

- If $E(\mathbb{Q}_p)$ contains no element of order $p$, then $E(K_w) \hat{\otimes} \mathbb{Z}_p \cong \mathbb{Z}_p[G_w]$.
- If $E(\mathbb{Q}_p)$ contains an element of order $p$, but $E(K_w)$ contains no element of order $p^2$, then $E(K_w) \hat{\otimes} \mathbb{Z}_p$ is a non-split extension of $\mathbb{Z}_p \oplus \ker\big(\mathbb{Z}_p[G_w] \to \mathbb{Z}_p\big)$ by the finite group $\mathbb{Z}/p\mathbb{Z}$ with trivial $G_w$-action.
- Otherwise $E(K_w)$ is the direct sum of $\mathbb{Z}_p[G_w]$ and a finite group of order $p^2$ with a non-trivial $G_w$-action.

Underlying to this theorem is the complete classification of all $\mathbb{Z}_p[G]$-modules $M$ in the case $G$ is cyclic of order $p$ and $M$ is a finitely generated $\mathbb{Z}_p$-module with a cyclic torsion part. See Theorem 19 for the complete list.

This investigation here grew out of [12, 13] where the $\mathbb{Z}_p[G]$-structure of Selmer groups plays an important role in trying to understand the explicit reformulation of the equivariant Birch and Swinnerton-Dyer conjecture under restrictions on the elliptic curve. One of the motivations of our work is to understand how to remove some of these restrictions; however the present paper does not link to algebraic $L$-values yet. See [8, 11, 22].

Similar methods to the ones used here have been successful in obtaining results on the change of Mordell-Weil groups, Selmer groups and Tate Shafarevich groups under finite extensions. For instance, [10, 31, 46] use versions of the control theorem. Bartel in [1, 3] used regulator constants to predict growth of the $p$-Selmer group in dihedral extensions. Our work can be seen as a continuation and generalisation of these methods.

Ouyang and Xie [36] prove that the size of $Ш(E/K)$ is unbounded as $K$ varies through the cyclic extensions $K/k$ for a fixed curve $E$ using further methods initiated by Mazur and Rubin as in [32] and [33]. In [34], the latter show the following for any elliptic curve $E$ over a number field $k$: For a positive proportion of primes $p$, for all $n \geqslant 1$ and all finite set $S$ of places in $k$, there are infinitely many cyclic extensions $K/k$ of degree $p^n$ such that all places in $S$ split and $E(K) = E(k)$. Their emphasis is on constructing extensions $K/k$ given a curve $E/k$, while we fix both and try to determine as much as we can on $E(K)$.

Representation theory, viewing $E(K) \otimes \mathbb{C}$ as a $\mathbb{C}[G]$-module, has produced lots of surprising results already. Much of the work of Tim and Vladimir Dokchitser [20, 21] is centred around these questions, especially in connection with parity phenomena. See [14] for a nice overview with plenty of examples.

In [7], the authors use $E(K) \otimes \mathbb{Q}$ as a $\mathbb{Q}[G]$-module to make prediction about high order vanishing of certain $L$-functions. Greenberg has used modular representation theory for Selmer groups in [26] to obtain results about the growth of the rank in extensions $K/k$, however there $k$ is an infinite extension of $\mathbb{Q}$. Finally, [9, 30] and other work by Macias Castillo and Bley contain the study of $E(K) \otimes \mathbb{Z}_p$ as $\mathbb{Z}_p[G]$-modules. Instead the question to determine what $E(K)$ is as a $\mathbb{Z}[G]$-module has attracted less attention, likely because it is much harder to say much about it. However, Theorem 6 in [22] shows that the arithmetic of $L$-values should predict interesting results in this direction.

The structure of this article is as follows. In Section 3 we will investigate the cokernel of the norm map for a local extension. Part of these results are well-known, but we try to be as general as possible. Then Section 4 is devoted to gathering results on the integral representation theory for a cyclic group of order $p$, where we allow non-trivial torsion, and certain groups that are extensions of cyclic groups by cyclic groups of order $p$. This is then used in Section 5 where we determine the local group of points as a $\mathbb{Z}_p[G_w]$-module in the case of the unramified extension of degree $p$. General results on the control theorem in a general global extension are presented in Section 6. Finally they are applied to global extensions with cyclic or dihedral Galois groups in Section 7. This section also includes a list of examples, which illustrate how to use the general method to determine the $\mathbb{Z}_p[G]$-module structure.

## 2 Notations

Throughout, $p$ is an odd prime and $\mathbb{Z}_p$ denotes the ring of $p$-adic integers.

In general, for an abelian group $Z$, we denote the projective limit of $Z/p^nZ$ by $Z \hat{\otimes} \mathbb{Z}_p$, which we call the $p$-adic completion of $Z$. If $Z$ is finitely generated this coincides with $Z \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and, if $Z$ is finite, it is isomorphic to the $p$-primary torsion subgroup $Z[p^\infty]$. If $Z$ is an discrete abelian $p$-primary group, or a compact $\mathbb{Z}_p$-module, then $Z^\vee$ denotes the Pontryagin dual $\mathrm{Hom}(Z, \mathbb{Q}_p/\mathbb{Z}_p)$.

Throughout the paper $G$ will stand for a finite group. For a $\mathbb{Z}_p[G]$-module $M$, we will write $M_t$ for the torsion subgroup of $M$ and $M_f$ to be the quotient of $M$ by $M_t$. The action is always from the left, even if we tend to write $M \otimes \mathbb{Q}_p$ for the $\mathbb{Q}_p[G]$-module obtained by extending the scalars. In Section 4.3, we will define the saturation index $\iota(M)$. The Dokchitser regulator constants $\mathcal{C}_\Theta(M)$

and their valuation $s_\Theta(M)$ are defined in Section 4.2. The groups $H^i(G,M)$ refer to the usual group cohomology with $M^G = H^0(G,M)$ and $\hat{H}^i(G,M)$ is the modified version by Tate.

The symbols $\mathbb{Z}_p$, $\breve{\mathbb{Z}}_p$, $\mathbb{Z}_p\{i\}$, $A$, $\breve{A}$, $A\{i\}$, $B$, $\breve{B}$ and $B\{i\}$ denote indecomposable $\mathbb{Z}_p[G]$-modules for the case when $G$ is a cyclic group of order $p$ as in Section 4.1, a dihedral group $D_p$ or one of the metacyclic groups as in Section 4.2. Furthermore by $\left\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\middle|\; \mathbb{Z}_p\right\}$, $\left\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\middle|\; A\right\}$ and, $\left\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\middle|\; \mathbb{Z}_p \oplus A\right\}$ we denote certain non-split extensions in the case of cyclic groups as explained in Theorem 19. Proposition 17 and Lemma 18 contain the definitions of the finite modules $J_i$ and $F_i$.

The symbols $k$ and $K$ will stand for fields such that $K/k$ is an extension of group $G$. In Sections 3 and 5 they are local fields, while they are number fields in the Sections 6 and 7. For a place $v$ in $k$, the completion is $k_v$ and $\mathbb{F}_v$ is the residue field. The discriminant is $\Delta_k$. The letters $e = e_v$ and $f = f_v$ are the ramification index and residue class degree at a place $v$.

The letter $E$ will stand for an elliptic curve defined over $k$, while $\mathcal{E}$, $\mathcal{E}_v^0$, and $\Phi_v$ relate to the Néron model as explained at the start of Section 3. If the reduction is good, we will use $\tilde{E}(\mathbb{F}_v)$ for the group of points in the reduction. The Tamagawa number of $E$ at the finite place $v$ is denoted by $c_v$. The modified product $C(E/k)$ of the Tamagawa number is defined in Section 7.

For a finite place $v$, the group $D = D_v = \hat{H}^0\big(G, E(K_w) \mathbin{\hat{\otimes}} \mathbb{Z}_p\big)$ is investigated in Section 3. The $p$-primary Selmer group $\mathcal{S}_k$ of $E$ appears first in Section 6. To shorten the notation, we will write $Ш_k = Ш(E/k)[p^\infty]$ for the $p$-primary part of the Tate-Shafarevich group. In Section 6, we will encounter the maps $\alpha$, $\beta$, $\gamma$, $\delta$, $\varepsilon$ and $\eta$. The capitulation is the kernel $C_{K/k} = \ker\eta$ and $D_{K/k}$ stands for the sum of $D_v$ over all places in the set $S$ containing all places of bad reduction for $E$, all places ramified in $K/k$ and all infinite places.

In Section 7, $\breve{E}$ denotes a quadratic twist of $E$. While $r_F$ is the rank of $E(F)$ for a field $F$, the rank of $\breve{E}(F)$ is $\breve{r}_F$.

# 3 The local norm

The aim of this section is to study the cokernel of the norm map on an elliptic curve under a finite extension of local fields. The analogous question, which is central in local class field theory, concerns the cokernel of the norm map on units. However the situation is more complicated here and it will leads us to treat different cases apart. While this has been studied partially in many situations, we try to be as general as possible.

Let $k$ be a local field with valuation $v$ and let $K$ be a finite Galois extension with valuation $w$. By $\mathbb{F}_v$ and $\mathbb{F}_w$ we will denote their residue fields, by $\mathcal{O}_v$ and $\mathcal{O}_w$ their rings of integers and by $\mathfrak{m}_w$ and $\mathfrak{m}_w$ their maximal ideals. Let $G$ be the Galois group of $K/k$. The ramification index is $e$ and $f$ stands for the residue class degree of the extension $K/k$. The degree $[K:k] = e \cdot f$ is denoted by $n$. When we write $v \mid p$, we mean that $k$ is a finite extension of $\mathbb{Q}_p$. The group we wish to determine is

$$D = \hat{H}^0\big(G, E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p\big) = \operatorname{coker}\big(\mathrm{N}\colon E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p \to E(k) \mathbin{\hat{\otimes}} \mathbb{Z}_p\big)$$

where $\hat{H}$ denotes Tate's modification of group cohomology and $E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p$ is the $p$-adic completion $\varprojlim E(K)/p^iE(K)$ of $E(K)$.

Let $\mathcal{E}_v$ be the Néron model of $E$ over the ring of integers $\mathcal{O}_v$ of $k$. Write $\mathcal{E}_v^0/\mathcal{O}_v$ for the connected component of the identity, $\tilde{\mathcal{E}}_v^0/\mathbb{F}_v$ for its special fibre, and let $\Phi_v/\mathbb{F}_v$ be the group of components of the special fibre. If we have good reduction, we will simply write $\tilde{E}$ for $\mathcal{E}_v^0$ as there is no danger of confusion. The Tamagawa number of $E$ over $k$ is denoted by $c_v = |\Phi_v(\mathbb{F}_v)|$. We use similar notation for $E/K$ with $v$ replaced by $w$.

**Lemma 4.** If $v \nmid p$, then we have an exact sequence of finite $\mathbb{Z}_p[G]$-module

$$0 \longrightarrow \tilde{\mathcal{E}}_w^0(\mathbb{F}_w)[p^\infty] \longrightarrow E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p \longrightarrow \Phi_w(\mathbb{F}_w)[p^\infty] \longrightarrow 0.$$

Note this does not necessarily mean that the $G$-fixed part of the outer terms of this sequence are the corresponding groups for $k$ as the Néron model may change in the extension.

*Proof.* We claim that, even if the Néron model changes, we may choose the model over $\mathcal{O}_w$ such that the subgroup $\mathcal{E}^0_w(\mathcal{O}_w)$ is a $G$-submodule. To prove this claim, we may assume that $E$ has bad reduction over $K$ and hence over $k$, too. We may translate a chosen equation over $\mathcal{O}_v$ to obtain a first Weierstrass model whose singular point over $\mathbb{F}_v$ is $(0,0)$. The Néron model over $\mathcal{O}_w$ constructed starting from this equation satisfies the claim.

Since the kernel of $\mathcal{E}^0_w(\mathcal{O}_w) \to \tilde{\mathcal{E}}^0_w(\mathbb{F}_w)$ is divisible by $p$, we have $\mathcal{E}^0_w(\mathcal{O}_w) \mathbin{\hat{\otimes}} \mathbb{Z}_p \cong \tilde{\mathcal{E}}^0_w(\mathbb{F}_w) \mathbin{\hat{\otimes}} \mathbb{Z}_p = \tilde{\mathcal{E}}^0_w(\mathbb{F}_w)[p^\infty]$. The projective limit over $m$ of the exact sequence

$$\Phi_w(\mathbb{F}_w)[p^m] \longrightarrow \mathcal{E}^0_w(\mathcal{O}_w)/p^m \longrightarrow E(K_w)/p^m \longrightarrow \Phi_w(\mathbb{F}_w)/p^m \longrightarrow 0$$

stays exact and the first term will vanish as $\Phi_w$ is finite. □

**Lemma 5.** Suppose $E$ has split multiplicative reduction over $k$. Let $q \in \mathcal{O}_v$ be the Tate parameter such that $E(k) \cong k^\times/q^{\mathbb{Z}}$. Then $D$ is the quotient of the $p$-primary part of $k^\times/\operatorname{N}(K^\times)$ by the group generated by $q$.

Write $G^{p\text{-ab}}$ for the Galois group of the maximal abelian $p$-extension within $K/k$. If $\operatorname{rec}\colon k^\times \to G^{p\text{-ab}}$ is the reciprocity map, then $D$ is isomorphic to $G^{p\text{-ab}}/\langle \operatorname{rec}(q)\rangle$.

*Proof.* First recall that the reduction type of $E$ is still split multiplicative over $K$ with the same parameter $q$. Since the torsion subgroup of $E(K)$ is finite, we get a diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & q^{\mathbb{Z}_p} & \longrightarrow & K^\times \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \\ 0 & \longrightarrow & q^{\mathbb{Z}_p} & \longrightarrow & k^\times \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & E(k) \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & 0. \end{array}$$

This shows that $D$, the cokernel on the right, is the quotient of the cokernel in the middle by the subgroup generated by $q$. □

**Proposition 6.** Suppose $E$ has split multiplicative reduction over $k$ and that $v \nmid p$.

- If $p \mid c_v$ and $p \mid f$, then $D$ is non-trivial.
- If $p \nmid \gcd(f, c_v)$ and $p \nmid \gcd\bigl(e, |\mathbb{F}_v^\times|\bigr)$, then $D$ is trivial.

Note this leaves the case when $p$ divides $e$ and $|\mathbb{F}_v^\times|$, but does not divide $c_v$ and $f$. In that last case, it could be trivial or non-trivial, which can only be determined by a finer analysis.

*Proof.* Note that the reduction is still split multiplicative over $K$. Inserting our knowledge about the curve with split multiplicative reduction into Lemma 4 shows that we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F}_w^\times[p^\infty] & \longrightarrow & E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & {}^{\mathbb{Z}}\!/_{ec_v\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [e]\cdot \mathrm{N}_{\mathbb{F}_w/\mathbb{F}_v}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{F}_v^\times[p^\infty] & \longrightarrow & E(k) \mathbin{\hat{\otimes}} \mathbb{Z}_p & \longrightarrow & {}^{\mathbb{Z}}\!/_{c_v\mathbb{Z}} & \longrightarrow & 0. \end{array}$$

The vertical map on the right sends $1 + ec_v\mathbb{Z}$ to $f + c_v\mathbb{Z}$. We deduce the exact sequence

$${}^{\mathbb{Z}}\!/_{e\,(c_v,f)\mathbb{Z}} \longrightarrow \mathbb{F}_v^\times[p^\infty]/e \longrightarrow D \longrightarrow {}^{\mathbb{Z}}\!/_{(c_v,f)\mathbb{Z}} \longrightarrow 0$$

where the second term is the quotient of the $p$-primary component of $\mathbb{F}_v^\times$ by its $e$-th powers. If $p \mid \gcd(c_v, f)$, then $D$ is non-trivial. If both terms next to $D$ are trivial, i.e., when $p \nmid \gcd(c_v, f)$ and $p \nmid \gcd(e, |\mathbb{F}_v^\times|)$, then $D$ is trivial. □

## 3.1 Unramified places

**Lemma 7.** Suppose $K/k$ is unramified. Then $D \cong \hat{H}^0\big(G, \Phi_v(\mathbb{F}_w)[p^\infty]\big)$.

*Proof.* Since we assume that the extension is unramified, the Néron model does not change: $\mathcal{E}_w = \mathcal{E}_v \times \mathcal{O}_w$ and in particular $\Phi_w = \Phi_v \times \mathbb{F}_w$. It is shown in Section 4 of [23] that for an unramified extension $\mathcal{E}_w^0(\mathcal{O}_w)$ is a cohomologically trivial $G$-module. From the fact that $\Phi_v(\mathbb{F}_w)$ is finite, we obtain the exact sequence

$$0 \longrightarrow \mathcal{E}_w^0(\mathcal{O}_w) \mathbin{\hat{\otimes}} \mathbb{Z}_p \longrightarrow E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p \longrightarrow \Phi_v(\mathbb{F}_w)[p^\infty] \longrightarrow 0.$$

Since the first term is cohomologically trivial, we get $D \cong \hat{H}^0\big(G, E(K) \mathbin{\hat{\otimes}} \mathbb{Z}_p\big)$ is isomorphic to $\hat{H}^0\big(G, \Phi_v(\mathbb{F}_w)[p^\infty]\big)$. □

For any integer $m$, we will denote the highest power of $p$ dividing $m$ by $\gcd(m, p^\infty)$.

**Lemma 8.** Assume that $K/k$ is unramified. Then $D$ is a cyclic group of order $c' = \gcd\big(c_v, n, p^\infty\big)$.

In particular, $D$ is trivial except possibly if either $E$ has split multiplicative reduction over $k$ of Kodaira type $\mathrm{I}_n$ with $p \mid n$ or if $p = 3$ and the special fibre of $\mathcal{E}_v$ is of Kodaira type IV or IV$^*$.

*Proof.* Since $K/k$ is unramified $\Phi_w = \Phi_v \times \mathbb{F}_w$ and $D$ is a quotient of $\big(\Phi_w(\mathbb{F}_w)[p^\infty]\big)^G = \Phi_v(\mathbb{F}_v)[p^\infty]$ by Lemma 7. Therefore if $p$ does not divide $c_v$ then $D$ is trivial. From the assumptions that $p \neq 2$, the classification of bad fibres of elliptic curves implies that $\Phi_v(\mathbb{F}_w)$ may contain a $p$-torsion element only if the reduction is split multiplicative or if $p = 3$ and the type is IV or IV$^*$.

Assume that $E$ has split multiplicative reduction in which case we may use Lemma 5. Since the extension is unramified, the valuation $v$ induces an isomorphism $k^\times / \mathrm{N}(K^\times)$ to $\mathbb{Z}/n\mathbb{Z} = {}^{\mathbb{Z}}\!/_{f\mathbb{Z}}$. As the valuation of the Tate parameter $q$ is equal to the Tamagawa number $c_v$, we find that $D$ is indeed cyclic of order $c'$.

If $p = 3$ and the fibre is of type IV or IV$^*$ with $p = c_v$ then $\Phi_v$ is the constant group scheme ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$. Therefore $D \cong \hat{H}^0\big(G, {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\big)$ is the cokernel of multiplication by $n$ on ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$. So once again $D$ is cyclic of order $\gcd\big(c_v, n, p^\infty\big)$. □

If $p$ were allowed to be 2, then we could in the same fashion go through all Kodaira types in Tate's algorithm and determine explicitly the group $D$ from the type and the degree $n$.

## 3.2 Totally ramified places

In this subsection we assume $K/k$ is totally ramified. We begin by considering the case where $v$ does not divide $p$.

**Proposition 9.** Suppose that $v \nmid p$.

- If the reduction of $E$ is good then, then $D \cong Z/nZ$ where $Z$ is the group $\tilde{E}(\mathbb{F}_v)[p^\infty]$.
- Suppose $E$ has split multiplicative reduction with Tamagawa number $c_v$ and write $q = u \cdot \mathrm{N}(\pi_w)^{c_v}$ for a choice of a uniformiser $\pi_w$ of $K$ and a unit $u \in \mathcal{O}_v^\times$. Then $D$ is isomorphic to the quotient of the $p$-primary part of $\mathbb{F}_v^\times$ by its subgroup generated by $u$ and by all $n$-th powers.
- If $E$ has non-split multiplicative reduction over $k$, then $D$ is cyclic of order $\gcd\big(n, |\mathbb{F}_v|+1, p^\infty\big)$.
- If $E$ has additive reduction, then $D$ is cyclic of order $\gcd\big(c_v, n, p^\infty\big)$.

*Proof.* Suppose first that the reduction is good over $k$. Then the reduction is also good over $\mathcal{O}_w$ and Lemma 4 tells us that $D \cong \hat{H}^0\big(G, \tilde{E}(\mathbb{F}_w)[p^\infty]\big)$. As the extension is totally ramified the action of $G$ is trivial on $Z = \tilde{E}(\mathbb{F}_w)[p^\infty]$. We conclude that $D$ is isomorphic to $Z/n\,Z$.

If the reduction is split multiplicative over $k$ we use Lemma 5. Since the extension is totally ramified and $v \nmid p$, the group $k^\times / \mathrm{N}(K)^\times$ identifies with the quotient of $\mathbb{F}_v^\times$ by its $n$-th powers. The group generated by $q$ under this identification is the one generated by $u$.

Next, we treat the case when the reduction is additive with $p \nmid c_v$. Then $E(k) \hat{\otimes} \mathbb{Z}_p \cong \tilde{\mathcal{E}}_v^0(\mathbb{F}_v)[p^\infty]$ by Lemma 4; this group is trivial as $v \nmid p$ and therefore $D$ is also trivial.

The same argument also works for non-split multiplicative reduction as the reduction will still be non-split over $K$, except that $\tilde{\mathcal{E}}_v^0(\mathbb{F}_v)$ is now a cyclic group of order $|\mathbb{F}_v| + 1$ with the trivial action by $G$ on it.

Finally, we are left with the case of reduction of type IV or IV$^*$ and $c_v = p = 3$. If the reduction is still of the same type over $K$, then $E(K) \hat{\otimes} \mathbb{Z}_p$ is isomorphic to $\Phi_w(\mathbb{F}_w) \cong \mathbb{Z}/3\mathbb{Z}$ with trivial action by $G$. Hence in this case $D$ is trivial unless $3 \mid n$ in which case it is cyclic of order $3 = c_v$.

Instead if the reduction type changes, the Tamagawa number $c_w$ must be coprime to 3. Then $E(K) \hat{\otimes} \mathbb{Z}_p$ is isomorphic to $\tilde{\mathcal{E}}_w^0(\mathbb{F}_w)[p^\infty]$ and has trivial action by $G$. But the $G$-fixed part is $E(k) \hat{\otimes} \mathbb{Z}_p$ which is cyclic of order 3. Yet again we can draw the same conclusion as before. □

Now we consider one case when $v$ divides $p$.

**Proposition 10.** Suppose $v \mid p$. Assume that $K/k$ is totally ramified and that $E$ has good ordinary reduction over $k$. Let $Z = \tilde{E}(\mathbb{F}_v)[p^\infty]$ and let $Y = G^{p-\mathrm{ab}}$ be the maximal abelian $p$-primary quotient of $G$. Then there is an exact sequence

$$Z\big[n\big] \longrightarrow Y/(1-\alpha)Y \longrightarrow D \longrightarrow Z/n\,Z \longrightarrow 0,$$

where $\alpha \in \mathbb{Z}_p^\times$ is the unit root of the characteristic polynomial $X^2 - a\,X + \#\mathbb{F}_v = 0$ of Frobenius with $a = \#\mathbb{F}_v + 1 - \#\tilde{E}(\mathbb{F}_v)$.

*Proof.* Write $\hat{E}$ for the formal group associated to a minimal Weierstrass equation of $E$. Consider the exact sequence

$$\hat{H}^{-1}\big(G, \tilde{E}(\mathbb{F}_w)[p^\infty]\big) \longrightarrow \hat{H}^0\big(G, \hat{E}(\mathfrak{m}_w)\big) \longrightarrow \hat{H}^0\big(G, E(K) \hat{\otimes} \mathbb{Z}_p\big) \longrightarrow \hat{H}^0\big(G, \tilde{E}(\mathbb{F}_w)[p^\infty]\big)$$

where the very last map is surjective since the map $E(k) \hat{\otimes} \mathbb{Z}_p \to \tilde{E}(\mathbb{F}_v)[p^\infty]$ is surjective. As the extension is totally ramified, the two extremal non-trivial terms in the sequence are isomorphic to the kernel and cokernel of multiplication by $n$ on the group $Z$.

Let $L$ be the maximal tame extension of $k$ inside $K$. The wild ramification group $G_1$ is the $p$-Sylow subgroup of $G$ and therefore $\hat{H}^0\big(G, \hat{E}(\mathfrak{m}_w)\big) \cong \hat{H}^0\big(G_1, \hat{E}(\mathfrak{m}_w)\big)$. Now we use Theorem 1 in [29] by Lubin and Rosen, which applies as we assumed good ordinary reduction. This shows that $\hat{H}^0\big(G_1, \hat{E}(\mathfrak{m}_w)\big) \cong G_1^{\mathrm{ab}}/(1-\alpha)G_1^{\mathrm{ab}}$. □

Recall that we say that $E$ has anomalous reduction at a place of good reduction over $k$ if $p$ divides $\#\tilde{E}(\mathbb{F}_v)$.

**Corollary 11.** Suppose $v \mid p$. Assume that $K/k$ is wildly ramified and that $E$ has good ordinary reduction over $k$. Then $D$ is non-trivial if and only if $E$ has anomalous reduction.

*Proof.* The group $A$ in Proposition 10 is non-trivial if and only if $E$ has anomalous reduction. In that case $D$ is non-trivial as $n$ is divisible by $p$.

Instead assume that the reduction is not anomalous. Then $1 - \alpha$ divides the evaluation of the characteristic polynomial at $X = 1$, which equals $\#\tilde{\mathcal{E}}_v(\mathbb{F}_v)$. Therefore $1 - \alpha \in \mathbb{Z}_p^\times$ and therefore $D$ is trivial. □

### 3.3 The general case

We drop any assumption on the local extension $K/k$. Recall that $e$ is the ramification index, which is the order of the inertia subgroup $I$.

**Lemma 12.** Let $X$ be a $G$-module and let $I \leqslant G$ be a normal subgroup. Then the following is an exact sequence:

$$\hat{H}^{-1}(G,X)\longrightarrow\hat{H}^{-1}(G/I,X^I)\longrightarrow\hat{H}^0(I,X)_{G/I}\longrightarrow\hat{H}^0(G,X)\longrightarrow\hat{H}^0(G/I,X^I)\longrightarrow 0.$$

In particular, if $X^I$ is cohomologically trivial as a $G/I$-module, then $\hat{H}^0(G,X)$ is isomorphic to $\hat{H}^0(I,X)_{G/I}$.

*Proof.* The norm map with respect to $G$ is equal to the composition $X_G = (X_I)_{G/I} \to (X^I)_{G/I} \to (X^I)^{G/I} = X^G$ where the first map $\rho$ is induced by the norm map for $I$ and the second is the norm map for $G/I$. The result can now be deduced from the kernel-cokernel sequence, which gives the desired exact sequence except that the term $\hat{H}^0(I,X)_{G/I}$ is replaced by $\operatorname{coker}\rho$. But these two groups are equal as taking $G/I$-coinvariants is right exact. □

**Proposition 13.** If $p \nmid e$, then $D$ is cyclic of order $c' = \gcd(c_v, n, p^\infty)$.

*Proof.* Apply the lemma with $A = E(K)\hat{\otimes}\mathbb{Z}_p$. The assumption that $p \nmid e$ implies that $\hat{H}^0(I,A) = 0$. Therefore $D$ is reduced to the computation of the same group for the unramified extension $K^I/k$ and that was done in Lemma 8. □

More generally, this proof shows that $D$ has a cyclic quotient of order $c' = \gcd(c_v, f, p^\infty)$ where $f$ is the residue class degree, for all local extensions.

**Proposition 14.** Suppose that $p \nmid c_v$. If $p = 3$, assume further that $f$ is odd or that the reduction type is not IV or IV*. If the reduction is non-split multiplicative of type $I_n$, assume that $f$ is odd or $p \nmid n$. Then $D \cong \hat{H}^0\big(I, E(K)\hat{\otimes}\mathbb{Z}_p\big)_{G/I}$ where $I$ is the inertia subgroup of $G$.

*Proof.* Let $L$ be the subextension fixed by $I$ with valuation $w'$. The assumption are made to assure that the Tamagawa number of $E$ over $L$ is still not divisible by $p$: If the Tamagawa number $c_{w'}$ over $L$ is divisible by $p$, but not $c_v$, then we must either be in the case IV or IV* and $p = 3$ or in the case $\mathrm{I}_n$ with $p \mid n$. Further the group $\Phi_v$ acquires new points of order $p$ in either cases, only if $L/k$ is of even degree.

Since $L/k$ is unramified, the Néron model $\mathcal{E}_v$ does not change under the extension. Therefore $A^I = E(L)\hat{\otimes}\mathbb{Z}_p = \mathcal{E}_v^0(\mathcal{O}_{w'})\hat{\otimes}\mathbb{Z}_p$ is a $G/I$-module that is cohomologically trivial, again by [23]. It follows that $D \cong \hat{H}^0\big(I, E(K)\hat{\otimes}\mathbb{Z}_p\big)_{G/I}$ by Lemma 12 with $A = E(K)\hat{\otimes}\mathbb{Z}_p$. □

In practice this means that in these cases the calculation of $D$ reduces to the totally ramified case treated in Section 3.2. Here is one important example.

**Proposition 15.** Suppose $E$ has good reduction and $v \nmid p$. Then $D \cong Z/eZ$ where $Z = \tilde{E}(\mathbb{F}_v)[p^\infty]$ and $e$ is the ramification index.

*Proof.* From the proof of Proposition 9, we see that $\hat{H}^0\big(I, E(K)\hat{\otimes}\mathbb{Z}_p\big)$ is isomorphic to the group $\tilde{E}(\mathbb{F}_w)[p^\infty]/e\tilde{E}(\mathbb{F}_w)[p^\infty]$ as a $G/I$-module. Since the norm $\tilde{E}(\mathbb{F}_w) \to \tilde{E}(\mathbb{F}_v)$ is surjective, the $G/I$-coinvariant space of $E(\mathbb{F}_w)[p^\infty]$ is $E(\mathbb{F}_v)[p^\infty]$. □

While the results in this section do not cover all cases, they do cover a lot and in the remaining ones one can often use the same methods to reduce it to a simple calculation. There is one major exception to this, that is when we have wild ramification, but the reduction is not good ordinary.

# 4 Representation theory

In his section, we will gather the representation theoretic results used later in the case that the Galois group is either cyclic or dihedral. We should emphasis that this is integral representation theory, in that we deal with $\mathbb{Z}_p[G]$-modules.

For a finite group $G$, we will say that $M$ is a $\mathbb{Z}_p[G]$-lattice, or simply $G$-lattice, if it is a finitely generated $\mathbb{Z}_p[G]$-module that is free as a $\mathbb{Z}_p$-module. As all modules will be finitely generated, we say $M$ is a finite module if it has finitely many elements, and no confusion should arise.

## 4.1 Cyclic group of order $p$

Let $G$ be the cyclic group of order $p$. We will write $\tau$ for a generator of $G$.

This is of course the easiest group of interest and, not surprisingly, we can give clear classification results for $\mathbb{Z}_p[G]$-modules. First, there are only two irreducible $\mathbb{Q}_p[G]$-modules, namely $\mathbb{Q}_p$ and the kernel of $\mathrm{N}\colon \mathbb{Q}_p[G] \to \mathbb{Q}_p$. The classification of indecomposable $\mathbb{Z}_p[G]$-lattices is also well-known (see Section 34B of [16], though this goes back to [19] and [40]).

**Proposition 16.** There are exactly three isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices, namely the trivial lattice $\mathbb{Z}_p$, the free module $\mathbb{Z}_p[G]$ and the augmentation kernel $A$ of $\mathrm{N}\colon \mathbb{Z}_p[G] \to \mathbb{Z}_p$.

We may view $A = (\tau - 1)\mathbb{Z}_p[G]$ also as the ring $\mathbb{Z}_p[\zeta]$ with $\zeta$ a primitive $p$-th root of unity and the action of $\tau \in G$ given by multiplication with $\zeta$. It is important to note that $\mathbb{Z}_p[G]$ and $\mathbb{Z}_p \oplus A$ are the only $G$-lattices of rank $p$ over $\mathbb{Z}_p$. In this simple case the concepts of free and projective coincide.

**Proposition 17.** For $1 \leqslant i \leqslant p$, let $J_i$ be the $i$-dimensional $\mathbb{F}_p$-vector spaces and the action by $\tau$ written as a unique Jordan block with 1 on the diagonal. Then these $J_i$ are the only indecomposable finitely generated $\mathbb{F}_p[G]$-modules.

*Proof.* The action of $G$ on a finite dimensional $\mathbb{F}_p$-vector space is described by the matrix of the action by the generator $\tau$. This matrix can be put into Jordan normal form. The eigenvalues of a matrix of order $p$ must be 1 and the module is indecomposable if there is only one block. Such a single Jordan block has order $p$ if and only if its dimension is at most $p$. □

For any $i \geqslant 1$, by $\mathbb{Z}/p^i\mathbb{Z}$ we will mean the cyclic group of order $p^i$ with trivial action by $G$. For $i \geqslant 2$, taking any other homomorphism $G \to \left(\mathbb{Z}/p^i\mathbb{Z}\right)^\times$, which means picking an image $w \neq 1$ in $1 + p^{i-1}\mathbb{Z}/p^i\mathbb{Z}$ for $\tau$, defines a $G$-module $F_i$, which is a cyclic group of order $p^i$ but with a non-trivial action by $G$. We may view $w$ as a non-zero parameter in $\mathbb{Z}/p\mathbb{Z}$. There are really $p-1$ different non-trivial $\mathbb{Z}/p^i\mathbb{Z}[G]$-modules whose underlying group is cyclic of order $p^i$, but we omit $w$ from the notation $F_i$.

**Lemma 18.** Let $i \geqslant j \geqslant 0$, If $M$ is a finite $\mathbb{Z}_p[G]$-module, which is cyclic of order $p^i$ such that $M^G$ is cyclic of order $p^j$, then $M$ is either $\mathbb{Z}/p^i\mathbb{Z}$ and $i = j$ or $M$ is one of the $F_i$ and $i = j + 1 \geqslant 2$.

*Proof.* If $j < i$, the action is non-trivial and we must have $M \cong F_i$. Then $M^G = pM$ shows that $i = j + 1$. □

We are now interested in $\mathbb{Z}_p[G]$-modules $M$ whose torsion part $M_t$ is cyclic. We will use the notation $\{X|Y\}$ representing a non-split extension $0 \longrightarrow X \longrightarrow M \longrightarrow Y \longrightarrow 0$. The ones appearing in the following proposition will be constructed explicitly in its proof.

**Theorem 19.** Let $M$ be a finitely generated $\mathbb{Z}_p[G]$-module and suppose that its $\mathbb{Z}_p$-torsion subgroup $M_t$ is cyclic. Then $M$ is a direct sum of some of the following modules:

| $M$ | $\hat{H}^0(G,M)$ | $H^1(G,M)$ | Conditions |
|---|---|---|---|
| $\mathbb{Z}/p^i\mathbb{Z}$ | $\mathbb{F}_p$ | $\mathbb{F}_p$ | $i \geqslant 1$ |
| $F_i$ | $0$ | $0$ | $i \geqslant 1$ and $w \in \mathbb{F}_p^\times$ |
| $\mathbb{Z}_p$ | $\mathbb{F}_p$ | $0$ | |
| $A$ | $0$ | $\mathbb{F}_p$ | |
| $\mathbb{Z}_p[G]$ | $0$ | $0$ | |
| $\{\mathbb{Z}/p^i\mathbb{Z} \mid \mathbb{Z}_p\}$ | $\mathbb{F}_p$ | $0$ | $i \geqslant 1$ |
| $\{\mathbb{Z}/p^i\mathbb{Z} \mid A\}$ | $0$ | $\mathbb{F}_p$ | $i \geqslant 1$ |
| $\{\mathbb{Z}/p^i\mathbb{Z} \mid \mathbb{Z}_p \oplus A\}$ | $0$ | $0$ | $i \geqslant 1$ |

The decomposition is unique up to reordering the summands.

*Proof.* Let $M$ be a finitely generated $\mathbb{Z}_p[G]$-module. There is an exact sequence

$$0 \longrightarrow M_t \longrightarrow M \longrightarrow M_f \longrightarrow 0 \tag{1}$$

where $M_f = M/M_t$ is a free, finitely generated $\mathbb{Z}_p$-module with an action by $G$. We assume that $M_t$ is a cyclic group, which implies by Lemma 18 that $M_t$ is either $\mathbb{Z}/p^i\mathbb{Z}$ or $F_i$ for some $i \geqslant 0$. Further by Proposition 16, the lattice $M_f$ is a sum of $\mathbb{Z}_p$, $A$ and $\mathbb{Z}_p[G]$.

We are now going to prove the following three statements:

$$\operatorname{Ext}^1_G(M_f, F_i) = 0, \quad \operatorname{Ext}^1_G(\mathbb{Z}_p, \mathbb{Z}/p^i\mathbb{Z}) \cong \mathbb{F}_p, \quad \text{and } \operatorname{Ext}^1_G(A, \mathbb{Z}/p^i\mathbb{Z}) \cong \mathbb{F}_p. \tag{2}$$

It is clear that $\operatorname{Ext}^1_G(\mathbb{Z}_p[G], F_i) = 0$ as $\mathbb{Z}_p[G]$ is free and hence projective. The norm map on $F_i$ with $w = 1 + p^{i-1}z$ is the multiplication by

$$1 + w + w^2 + \cdots + w^{p-1} \equiv p + p^{i-1}\frac{p(p-1)}{2}\, z \equiv p \pmod{p^i}$$

as $p$ is odd. Therefore $\hat{H}^0(G, F_i) = F_i^G/\operatorname{N}(F_i) \cong pF_i/pF_i = 0$. By the Herbrand quotient on finite modules $H^1(G, F_i) = 0$ and hence $\operatorname{Ext}^1_G(\mathbb{Z}_p, F_i)$ vanishes, too.

Consider the short exact sequence $0 \longrightarrow \mathbb{Z}_p \xrightarrow{N} \mathbb{Z}_p[G] \longrightarrow A \longrightarrow 0$ which yields

$$0 \longleftarrow \operatorname{Ext}^1_G(A, F_i) \longleftarrow \operatorname{Hom}_G(\mathbb{Z}_p, F_i) \longleftarrow \operatorname{Hom}_G(\mathbb{Z}_p[G], F_i).$$

By evaluation at 1 the right hand side identifies with $pF_i \xleftarrow{[p]} F_i$ and hence $\operatorname{Ext}^1_G(A, F_i) = 0$. This concludes the proof for the first statement in (2)

Next, we see that $\operatorname{Ext}^1_G(\mathbb{Z}_p, \mathbb{Z}/p^i\mathbb{Z}) \cong H^1(G, \mathbb{Z}/p^i\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$. Also with the same method as above, we find $\operatorname{Ext}^1_G(A, \mathbb{Z}/p^i\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ as it is the cokernel of the map $[p]$ on $\mathbb{Z}/p^i\mathbb{Z}$. This concludes all statements in (2).

We conclude that the only direct summands appearing in $M$ are $\mathbb{Z}/p^i\mathbb{Z}$, $F_i$, $\mathbb{Z}_p$, $A$, $\mathbb{Z}_p[G]$ as well as any non-split exact sequence

$$0 \longrightarrow \mathbb{Z}/p^i\mathbb{Z} \longrightarrow M \longrightarrow \mathbb{Z}_p^a \oplus A^b \longrightarrow 0$$

with $a, b \geqslant 0$. By the above such short exact sequences are parametrised by $\operatorname{Ext}^1_G(\mathbb{Z}_p^a \oplus A^b, \mathbb{Z}/p^i\mathbb{Z}) \cong \mathbb{F}_p^{a+b}$. We are now going to show that there are only three distinct $\mathbb{Z}_p[G]$-modules among these non-split exact sequences.

First, we proceed to construct the extensions explicitly. First, for any $u \in \operatorname{Hom}(\mathbb{Z}_p^a, \mathbb{F}_p)$, we set $M_u$ to be $\mathbb{Z}/p^i\mathbb{Z} \times \mathbb{Z}_p^a$ as a $\mathbb{Z}_p$-module, but with the action by a generator $\tau \in G$ defined by

$$\tau \cdot (t, x) = (t + u(x)\, p^{i-1}, x) \text{ for } t \in \mathbb{Z}/p^i\mathbb{Z} \text{ and } x \in \mathbb{Z}_p^a.$$

Then

$$0 \longrightarrow {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \longrightarrow M_u \longrightarrow \mathbb{Z}_p^a \longrightarrow 0$$

is an non-split extension of $\mathbb{Z}_p[G]$-modules.

The connecting homomorphism $\mathbb{Z}_p^a \to H^1\big(G, {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}\big) \approx {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ is equal to $u$, which shows that these are distinct extensions and they are non-split when $u \neq 0$. Assume $u \neq 0$, we find $M_u^G$ consists of all $(t, x)$ with $x \in \ker u$. The norm map on $M_u$ sends $(t, x)$ to

$$\mathrm{N}(t,x) = \sum_{j=0}^{p-1} \big(t + j \cdot u(x)\, p^{i-1}, x\big) = \big(pt + p\tfrac{p-1}{2} u(x) p^{i-1}, px\big) = \big(pt, px\big)$$

as $p$ is odd. Therefore $\hat{H}^0(G, M) \cong \mathbb{F}_p^a$ and $H^1(G, M) = 0$.

Next, for any $\mathbb{Z}_p$-linear $v : \big(A/(\tau - 1)A\big)^b \to {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, we will build an extension

$$0 \longrightarrow {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \longrightarrow M'_v \longrightarrow A^b \longrightarrow 0$$

as follows. We identify $A$ with $\mathbb{Z}_p[\zeta]$ where $\zeta^p = 1$ and the action by $\tau$ is by multiplication with $\zeta$. We define $M'_v$ as the $\mathbb{Z}_p$-module ${}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \times \mathbb{Z}_p[\zeta]^b$ together with the action by $\tau$ given by $\tau(t, y) = (t + f_v(y), \zeta \cdot y)$ where $f_v$ is a $\mathbb{Z}_p$-linear map $A^b \to {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}$ such that $f_v\big(\frac{p}{1-\zeta} y\big)$ reduces to $v(y)$ modulo $p$ for all $y$. This $f_v$ exists as the condition only imposes the values on a $b$ dimensional $\mathbb{F}_p$-subspace of the $b(p-1)$ dimensional space $(A/pA)^b$. We find for $0 \leqslant j < p$

$$\tau^j\,(t, y) = \big(t + f_v(y) + f_v(\zeta\, y) + \cdots + f_v(\zeta^{j-1} y), \zeta^j y\big) = \big(t + f_v(\tfrac{1-\zeta^j}{1-\zeta} y), \zeta^j y\big).$$

and therefore

$$\begin{aligned} N(t, y) &= \Big(pt + \sum_{j=0}^{p-1} f_v\Big(\tfrac{1-\zeta^j}{1-\zeta} y\Big),\ \sum_{j=0}^{p-1} \zeta^j y\Big) \\ &= \Big(pt + f_v\Big(\sum_{j=0}^{p-1} (1-\zeta^j) \tfrac{y}{1-\zeta}\Big),\ 0\Big) = \Big(pt + f_v(\tfrac{p}{1-\zeta} y),\ 0\Big) \end{aligned}$$

The connecting homomorphism $\hat{H}^{-1}(G, A^b) \to \hat{H}^0\big(G, {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}\big)$ identifies with $v$. When $v \neq 0$, then $\hat{H}^0(G, M_v) = 0$ and $H^1(G, M_v) \cong \mathbb{F}_p^b$.

Finally the extension $M_{u,v}$ is defined as the group ${}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \times \mathbb{Z}_p^a \times A^b$ with $\tau$ acting on $(t, x, y)$ by $(t + u(x)p^{i-1} + f_v(y), x, \zeta\, y)$ with $u$, $v$ and $f_v$ as above. It is not hard to calculate that $\dim_{\mathbb{F}_p} \hat{H}^0\big(G, M_{u,v}\big) = a - 1$ and $\dim_{\mathbb{F}_p} H^1\big(G, M_{u,v}\big) = b - 1$.

With the above, we have explicitly constructed all extensions in

$$\mathrm{Ext}^1\big(\mathbb{Z}_p^a \oplus A^b, {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}\big) \cong \mathrm{Hom}\big(\mathbb{Z}_p, \mathbb{F}_p\big) \oplus \mathrm{Hom}_{\mathbb{Z}_p[\zeta]}\big(\mathbb{Z}_p[\zeta], \mathbb{F}_p\big) \cong \mathbb{F}_p^a \oplus \mathbb{F}_p^b.$$

The group $\mathrm{Aut}_G\big(\mathbb{Z}_p^a \oplus A^b\big)$ acts from the left on this extension group and this action does not change the isomorphism class of $M_{u,v}$ as a $\mathbb{Z}_p[G]$-module. The group acting is isomorphic to $\mathrm{GL}_a(\mathbb{Z}_p) \times \mathrm{GL}_b(\mathbb{Z}_p[\zeta])$ and, for $\alpha \in \mathrm{GL}_a(\mathbb{Z}_p)$and $\beta \in \mathrm{GL}_b(\mathbb{Z}_p[\zeta])$, the action on $(u, v)$ gives $\big(u \circ \alpha^{-1}, v \circ \beta^{-1}\big)$. It follows that there are four orbits on $\mathbb{F}_p^a \oplus \mathbb{F}_p^b$ corresponding to $u$ and $v$ being zero or non-zero. We set $\big\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\big|\; \mathbb{Z}_p\big\} := M_u$, $\big\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\big|\; A\big\} := M_v$ and $\big\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}} \;\big|\; \mathbb{Z}_p \oplus A\big\} := M_{u,v}$ for any choice of non-zero $u$ and $v$ with $a = b = 1$. For larger $a$ or $b$, we can split off $a - 1$ direct summands of $\mathbb{Z}_p$ and $b - 1$ direct summands of $A$.

The last statement, that the direct sum is unique, is a consequence of the Krull-Schmidt-Azumaya Theorem (See Theorem 6.12 in [16]). □

**Lemma 20.** There are non-trivial extensions $0 \longrightarrow \mathbb{Z}_p[G] \longrightarrow M \longrightarrow F \longrightarrow 0$ where $F$ is one of the following finite $G$-module: $F = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, $F = \mathbb{F}_p G$ or $F \cong F_2$. Moreover

1. If $F = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ then $M \cong \mathbb{Z}_p \oplus A$ as a $\mathbb{Z}_p[G]$-module.
2. If $F \cong F_2$ or if $F = \mathbb{F}_p G$ and $M_t$ is cyclic, then either $M \cong \mathbb{Z}_p[G]$ or $M = \left\{ {}^{\mathbb{Z}}/_{p\mathbb{Z}} \;\middle|\; \mathbb{Z}_p \oplus A \right\}$.

*Proof.* For the first statement, we need to compute $\mathrm{Ext}^1\big(F, \mathbb{Z}_p[G]\big)$. Let $p^k$ be the exponent of $F$ as an abelian group and consider the multiplication by $p^k$ on $\mathbb{Z}_p[G]$. From

$$\mathrm{Hom}_G\big(F, \mathbb{Z}_p[G]\big) = 0 \longrightarrow \mathrm{Hom}_G\big(F, {}^{\mathbb{Z}}/_{p^k\mathbb{Z}}[G]\big) \longrightarrow \mathrm{Ext}^1\big(F, \mathbb{Z}_p[G]\big) \xrightarrow{[p^k]=0} \mathrm{Ext}^1\big(F, \mathbb{Z}_p[G]\big)$$

we see that $\mathrm{Ext}^1\big(F, \mathbb{Z}_p[G]\big) \cong \mathrm{Hom}_G\big(F, {}^{\mathbb{Z}}/_{p^k\mathbb{Z}}[G]\big)$. First the map from $F_2$ with parameter $w \in 1 + p\,{}^{\mathbb{Z}}/_{p^2\mathbb{Z}}$ to ${}^{\mathbb{Z}}/_{p^2\mathbb{Z}}[G]$ sending 1 to $\sum_{i=0}^{p-1} w^{-i}\tau^i$ is a $G$-equivariant map; therefore $\mathrm{Ext}^1\big(F_2, \mathbb{Z}_p[G]\big) \neq 0$. Since $\mathrm{Hom}_G\big({}^{\mathbb{Z}}/_{p\mathbb{Z}}, \mathbb{F}_p[G]\big) = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ and $\mathrm{Hom}_G\big(\mathbb{F}_p[G], \mathbb{F}_p[G]\big) \neq 0$ we also have the non-trivial extensions in the other cases.

Assume now $M$ is such a non-trivial extension. Since $\mathbb{Z}_p[G]$ is cohomologically trivial, we have $H^i(G, M) = H^i(G, F)$. Note also that $M_t$ injects into $F$, but it cannot surject otherwise the extension would be split.

For $F = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ the non-trivial extensions must then be torsion-free. Since $H^1\big(G, {}^{\mathbb{Z}}/_{p\mathbb{Z}}\big) = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$, the table in Theorem 19 tells us that $M$ must be isomorphic to $\mathbb{Z}_p \oplus A$.

If $F \cong F_2$, then $M_t$ is either trivial or ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Since $H^1(G, F_2) = 0$, this only leaves $\mathbb{Z}_p[G]$ or $\left\{ {}^{\mathbb{Z}}/_{p\mathbb{Z}} \;\middle|\; \mathbb{Z}_p \oplus A \right\}$; in the first case $1 \in \mathbb{Z}_p[G]$ is sent to $\tau - \tilde{w}$, where $\tilde{w} \in \mathbb{Z}_p^\times$ is a lift of $w$, in the second case it is sent to $(0, p, 1) \in M_{u,v}$.

If $F = \mathbb{F}_p[G]$ and $M_t$ is cyclic then $M_t$ has at most $p$ elements. We reach the same conclusion as above given that $H^1\big(G, \mathbb{F}_p[G]\big)$ also vanishes. Also here it is possible to write down an explicit extension. □

## 4.2 Metacyclic groups

Despite being interested mainly in the dihedral case, we present the results in a slightly more general setting. Let $m$ be a positive divisor of $p-1$. Let $\xi$ be a choice of a primitive $m$-th root of unity in $\mathbb{Z}_p$. Let $r \in \mathbb{Z}$ such that $r \equiv \xi \pmod{p}$ so that $r^m \equiv 1 \pmod{p}$. In this section we treat the case of the metacyclic group

$$G = \left\langle \tau, \sigma \;\middle|\; \tau^p = \sigma^m = 1 \text{ and } \sigma\tau = \tau^r\sigma \right\rangle$$

of order $pm$. We write $N$ for the normal subgroup generated by $\tau$ and $H$ for the subgroup generated by $\sigma$; so $G = N \rtimes H$. This includes the case $G$ is the dihedral group $D_p$ when $m = 2$ and $r = -1$.

For $i \in {}^{\mathbb{Z}}/_{m\mathbb{Z}}$, we define the $G$-lattice $\mathbb{Z}_p\{i\}$ which, as a group, is just $\mathbb{Z}_p$, the action by $\tau$ is trivial and by $\sigma$ is the multiplication with $\xi^i$. We have $\mathbb{Z}_p\big[G/N\big] \cong \bigoplus_{i=0}^{m-1} \mathbb{Z}_p\{i\}$ as the index of $N$ in $G$ is coprime to $p$.

Next, we define $A$ as the group $\mathbb{Z}_p[\zeta]$ where $\zeta$ is a primitive $p$-th root of unity. The group action is defined by letting $\tau$ act as multiplication by $\zeta$ and $\sigma(\zeta^j) = \zeta^{rj}$ for all $0 \leqslant j < p$. For any $0 \leqslant i < m$, we set $A\{i\} = A \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\{i\}$. It follows that $\mathrm{Ind}_N^G(A) \cong \bigoplus_{i=0}^{m-1} A\{i\}$. The complete list of simple $\mathbb{Q}_p[G]$-modules is given by $\mathbb{Z}_p\{i\} \otimes \mathbb{Q}_p$ and $A\{i\} \otimes \mathbb{Q}_p$.

Finally, let $B = \mathbb{Z}_p\big[G/H\big]$ and set $B\{i\} = B \otimes_{\mathbb{Z}_p} \mathbb{Z}_p\{i\}$. Then $\mathbb{Z}_p[G] \cong \bigoplus_{i=0}^{m-1} B\{i\}$. We have a non-split exact sequence

$$0 \longrightarrow A\{i\} \longrightarrow B\{i\} \longrightarrow \mathbb{Z}_p\{i\} \longrightarrow 0$$

for all $0 \leqslant i < m$.

The following was found by Pu in [38]. See [27] for the case of dihedral groups.

**Proposition 21.** The lattices $\mathbb{Z}_p\{i\}$, $A\{i\}$ and $B\{i\}$ for $0 \leqslant i < m$ represent all isomorphism classes of indecomposable finitely generated $\mathbb{Z}_p[G]$-lattices.

*Proof.* Since $[G:N]$ is coprime to $p$, the proof of Proposition 33.4 in [16] shows that all indecomposable modules are summands of $\mathrm{Ind}_N^G(X)$ as $X$ runs through all indecomposable $N$-lattices. The proposition follows now from Proposition 16 and $\mathrm{Ind}_N^G(\mathbb{Z}_p) = \bigoplus_{i=0}^{m-1} \mathbb{Z}_p\{i\}$, $\mathrm{Ind}_N^G(A) = \bigoplus_{i=0}^{m-1} A\{i\}$ and $\mathrm{Ind}_N^G(\mathbb{Z}_p[N]) = \bigoplus_{i=0}^{m-1} B\{i\}$. □

As all $B\{i\}$ are direct summands of the free $\mathbb{Z}_p[G]$, they are projective $G$-lattices. Therefore they are cohomologically trivial. Write $\mathbb{F}_p\{i\}$ for the $G$-module $\mathbb{Z}_p\{i\}/p\mathbb{Z}_p\{i\}$. Then we have that $\hat{H}^0\big(N, \mathbb{Z}_p\{i\}\big) \cong \mathbb{F}_p\{i\}$ and $H^1\big(N, A\{i\}\big) \cong \mathbb{F}_p\{i\}$ as $G/N$-modules.

Unlike for the cyclic group, the decomposition of a $\mathbb{Z}_p[G]$-lattice $M$ into indecomposable lattices cannot be determined by knowing the $\mathbb{Q}_p[G]$-module $M \otimes \mathbb{Q}_p$ and the cohomology groups $\hat{H}^i\big(N, M\big)$ only. In [44], Torzewski considered an additional invariant, which we are going to introduce next.

For a general finite group $\mathcal{G}$, we say that a $\mathbb{Z}_p[\mathcal{G}]$-lattice $M$ is rationally self-dual if $\mathrm{Hom}_{\mathbb{Q}_p}\big(M \otimes \mathbb{Q}_p, \mathbb{Q}_p\big) \cong M \otimes \mathbb{Q}_p$ as $\mathbb{Q}_p[\mathcal{G}]$-modules; equivalently there is a non-degenerate $\mathcal{G}$-equivariant symmetric bilinear pairing $\beta\colon M \times M \to \mathbb{Q}_p$. If $M \cong \tilde{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for some $\mathbb{Z}[\mathcal{G}]$-lattice $\tilde{M}$ then it is automatically rationally self-dual. All $\mathbb{Z}_p[\mathcal{G}]$-lattices are rationally self-dual if $\mathcal{G}$ is the cyclic group of order $p$ or the dihedral group of order $2p$. Instead for our group $G$, any rationally self-dual lattice is a (not necessarily unique) direct sum of

$$\mathbb{Z}_p,\ A,\ B,\ A\{i\},\ \mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\},\ B\{i\} \oplus \mathbb{Z}_p\{-i\},\ B\{i\} \oplus B\{-i\} \text{ for } 0 < i < \tfrac{m}{2}$$
$$\text{as well as } B\{\tfrac{m}{2}\},\ \mathbb{Z}_p\{\tfrac{m}{2}\} \text{ when } m \text{ is even.}$$

A Brauer relation for $G$ is a formal sum $\Theta = \sum_H a_H\, H$ of subgroups $H \leqslant G$ with coefficients $a_H \in \mathbb{Z}$ such that $\bigoplus_H \mathbb{Q}\big[G/H\big]^{a_H}$ is zero as a virtual representation of $G$. For our group $G$, all Brauer relations can be obtained from Artin's induction theorem, see Theorem 2.10 in [44]: For each divisor $1 < d \mid m$, let

$$\Theta_d = 1 - d \cdot H_d - N + d \cdot G_d$$

where $H_d$ is the subgroup of $H$ of order $d$ and $G_d = N \rtimes H_d$.

To every Brauer relation $\Theta = \sum_H a_H\, H$ and every rationally self-dual $\mathbb{Z}_p[G]$-lattice $M$ one associates a Dokchitser regulator constant $\mathcal{C}_\Theta(M) \in \mathbb{Q}_p^\times/\square$ where $\square = \big\{z^2 \;\big|\; z \in \mathbb{Z}_p^\times\big\}$ by

$$\mathcal{C}_\Theta(M) = \prod_H \det\Big(\frac{1}{|H|}\beta \;\Big|\; M^H\Big)^{a_H} \cdot \square \tag{3}$$

where $\beta$ is the $G$-equivariant pairing on $M$. See [20] for the basic properties, including the fact that the definition is independent of the choice of $\beta$. The special case of dihedral groups was already worked out by Bartel in Theorem 4.4 in [2].

We are interested in the integer $s_d(M)$ defined to be the $p$-adic valuation of $\mathcal{C}_{\Theta_d}(M)$. As proved in [44, Theorem 1.1], the kernel of the map $s = \oplus s_d$ from the $\mathbb{Q}$-vector space with basis $\mathbb{Z}_p[G/U]$ as $U$ runs through all subgroups $U \leqslant G$ to $\mathbb{Q}$ is equal to the subspace generated by all cyclic $U$.

**Proposition 22.** Let $1 < d$ be a divisor of $m$ and $0 < i < m$. We have $s_d\big(\mathbb{Z}_p\big) = 1 - d$ and $s_d\big(\mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = 2$. Also $s_d(A) = d - 1$ and $s_d\big(A\{i\}\big) = 2i - 1 - d$ and $s_d\big(B\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = 2i + 1 - d$ and $s_d\big(B\big) = r_d\big(B\{i\} \oplus B\{-i\}\big) = 0$. Further, if $m$ is even, $s_d\big(\mathbb{Z}_p\{\frac{m}{2}\}\big) = 1$ and $s_d\big(B\{\frac{m}{2}\}\big) = 0$.

Note that $s_d$ can not be extended to an additive function on all lattices. The result in the proposition can be deduced from the explicit and more general calculation by Torzewski in [44, Proof of Theorem 4.1] where he found that $s_d\big(\mathbb{Z}_p[G/G_e]\big) = (1 - \gcd(d,e)) \cdot m/e/d$ for any $d$ and $e$ dividing $m$. We proceed here to calculate it directly on all the minimal rationally self-dual lattices.

*Proof.* By Proposition 2.45.(3) in [20], the regulator constants satisfy $\mathcal{C}_{\Theta_d}(M) = \mathcal{C}_{\Theta_d}\big(M|_{G_d}\big)$, which implies that we may restrict to the case when $d = m$. We will write $\mathcal{C}$ for $\mathcal{C}_{\Theta_m}$. To show that $\mathcal{C}\big(\mathbb{Z}_p\big) = p^{1-m}$ is a direct calculation on the definition. The same goes for $\mathcal{C}\big(\mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = p^2$ using the bilinear form $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for all $0 < i < m$. From the additivity of the regulator constant, see Corollary 2.18 in [20], we may conclude that $\mathcal{C}\big(\mathbb{Z}_p\{\frac{m}{2}\}\big) = \pm p$ for even $m$.

Let $w = \sum_{j=0}^{m-1} \xi^{-j}\zeta^{r^j} \in A$. It satisfies $\sigma(w) = \xi \cdot w$. Using that $\xi \equiv r \pmod{p}$, we find

$$w \equiv \Big(\sum_{j=0}^{m-1} \xi^{-j}\Big) + \Big(\sum_{j=0}^{m-1} \xi^{-j} r^j\Big) \cdot (\zeta - 1) \equiv 0 + m \cdot (\zeta - 1) \not\equiv 0 \pmod{(\zeta-1)^2}.$$

Consider the map $A \otimes \mathbb{Z}_p\{i+1\} \to A \otimes \mathbb{Z}_p\{i\}$ sending $a \otimes z$ to $aw \otimes z$. Its image is $(\zeta - 1)A \otimes \mathbb{Z}_p\{i\}$, which is of index $p$. Therefore we have the short exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \longrightarrow A\{i+1\} \longrightarrow A\{i\} \longrightarrow \mathbb{F}_p\{i\} \longrightarrow 0. \tag{4}$$

We conclude that $A\{i+1\}$ has index $p$ in $A\{i\}$ and that $A\{i+1\}^H = A\{i\}^H$ for all $0 < i < m$. Using $A\{i\}^N = A\{i\}^G = 0$, for all $0 < i < m$, we have

$$\mathcal{C}\big(A\{i+1\}\big) = \frac{\det\big(\beta \;\big|\; A\{i+1\}\big)}{\det\big(\frac{1}{m}\beta \;\big|\; A\{i+1\}^H\big)^m} = \frac{p^2 \det\big(\beta \;\big|\; A\{i\}\big)}{\det\big(\frac{1}{m}\beta \;\big|\; A\{i\}^H\big)^m} = p^2 \cdot \mathcal{C}\big(A\{i\}\big).$$

Thus $\mathcal{C}\big(A\{i\}\big) = p^{2(i-1)} \cdot A\{1\}$ for all $1 \leqslant i \leqslant m$. Since $\bigoplus_{i=1}^m A\{i\} \cong \mathrm{Ind}_N^G(A)$, we find

$$\mathcal{C}\big(\mathrm{Ind}_N^G(A)\big) = \prod_{i=1}^m \mathcal{C}\big(A\{i\}\big) = \mathcal{C}\big(A\{1\}\big)^m \cdot p^{m(m-1)}.$$

But since $\mathcal{C}_{\Theta_m}\big(\mathrm{Ind}_N^G(A)\big) = \mathcal{C}_{\mathrm{Res}_N(\Theta_m)}\big(A\big)$ by Proposition 2.45 in [20] and the restriction of $\Theta_m$ to $N$ is trivial, we get $\mathcal{C}\big(A\{1\}\big)^m = p^{-m(m-1)}$. Hence $s_m\big(A\{1\}\big) = 1 - m$ and by the above recursion formula $s_m\big(A\{i\}\big) = 2\,i - 2 + 1 - m = 2\,i - 1 - m$ for all $1 \leqslant i \leqslant m$. In particular $s_m(A) = s_m\big(A\{m\}\big) = m - 1$.

Just as before $\mathcal{C}\big(B\big) = \mathcal{C}\big(\mathbb{Z}_p[G/H]\big) = 1$ because the restriction of $\Theta_m$ to $H$ is trivial; that is Lemma 2.46 in [20].

Consider the map

$$\begin{aligned} \Phi\colon \mathbb{Z}_p\big[G/H\big] &\to \mathbb{Z}_p \oplus A \\ \sum_{i=0}^{p-1} a_i\, \tau^i H &\mapsto \Big(\sum_{i=0}^{p-1} a_i,\ \sum_{i=0}^{p-1} a_i \zeta^i\Big) \end{aligned}$$

It is an injective $G$-equivariant map whose image is $\big\{(x,a) \in \mathbb{Z}_p \oplus A \;\big|\; x \equiv a \pmod{\zeta - 1}\big\}$ of index $p$. We deduce the exact sequence

$$0 \longrightarrow B\{i\} \oplus \mathbb{Z}_p\{-i\} \longrightarrow A\{i\} \oplus \mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\} \longrightarrow \mathbb{F}_p\{i\} \longrightarrow 0$$

for all $i$. When $0 < i < m$, then the $G$ and $H$-invariant parts of the first two terms are equal, while the $N$-invariant parts are of index $p$. The same reasoning as above concludes now that

$$\mathcal{C}\big(B\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = \mathcal{C}\big(A\{i\} \oplus \mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = \mathcal{C}\big(A\{i\}\big) \cdot \mathcal{C}\big(\mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big)$$

and hence $s_m\big(B\{i\} \oplus \mathbb{Z}_p\{-i\}\big) = 2\,i - 1 + m + 2 = 2\,i + 1 - m$.

Finally

$$\begin{aligned} \mathcal{C}\big(B\{i\} \oplus B\{-i\}\big) \cdot \mathcal{C}\big(\mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big) &= \mathcal{C}\big(B\{i\} \oplus B\{-i\} \oplus \mathbb{Z}_p\{i\} \oplus \mathbb{Z}_p\{-i\}\big) \\ &= \mathcal{C}\big(B\{i\} \oplus \mathbb{Z}_p\{-i\}\big) \cdot \mathcal{C}\big(\mathbb{Z}_p\{i\} \oplus B\{-i\}\big) \end{aligned}$$

shows that, for $0 < i < m$, we have $s_d\big(B\{i\} \oplus B\{-i\}\big) = 2\,i + 1 - m + 2(m-i) + 1 - m - 2 = 0$. □

In the special case $m = 2$, when the group is dihedral, all $G$-lattices are rationally self-dual.

**Theorem 23.** Let $p > 2$ be a prime and let $G = D_p$. Then a $\mathbb{Z}_p[G]$-lattice is determined up to isomorphism by the knowledge of

- $M \otimes \mathbb{Q}_p$ as a $\mathbb{Q}_p[G]$-module,
- $H^1(N, M)$ as a $\mathbb{F}_p[G/N]$-module, and
- the regulator constant $s(M) = \operatorname{ord}_p\big(\mathcal{C}_{\Theta_2}(M)\big)$.

This is explained in [44, Section 7.1], but can also be read off the Table 1 below. This theorem does not extend to the more general meta-cyclic groups even if one restricts to rationally self-dual $G$-lattices.

### 4.3 Saturation index

Given a finite group $G$ and a $\mathbb{Z}_p[G]$-module $M$, we define the saturation index $\iota(M)$ to be the quotient of $M$ by the subgroup generated by all $M^H$ where $H$ runs through all non-trivial cyclic subgroups of $G$. Alternatively, it is the quotient of $M$ by the sub-$\mathbb{Z}_p[G]$-module generated by all $M^H$ where $H$ runs through a set of representatives of all conjugacy classes of non-trivial cyclic subgroups of $G$.

$$\iota(M) = \frac{M}{\sum_{\text{cyclic } H \leqslant G} M^H}.$$

This index and its generalisations appear dominantly in the work of Bartel and de Smit [4, 2]. By Artin's induction theorem $\iota(M)$ is a finite $\mathbb{Z}_p[G]$-module for all non-cyclic groups $G$.

We call $\iota(M)$ the saturation index because of the following observation in the case of $M$ being the $p$-adic completion of $E(K)$ for some elliptic curve. If we need to determine $E(K)$ explicitly, then we would start by a search for points in $E(K^H)$ for proper subgroups $H$ as this is quicker than searching in $E(K)$ directly. These points then generate a submodule of $E(K)$ of finite index and there is an effective algorithm [37], called a $p$-saturation, to calculate the full $M$. This algorithm effectively calculates $\iota(M)$, though usually only it size is of interest. Unfortunately, at this stage, we have no means to relate the invariant $\iota(M)$ directly to arithmetic information of $E$ that is easier to calculate than $M$ itself. We may use it to determine $M$ once we have $E(K^H)$ for all non-trivial cyclic $H$, without having to calculate the matrices representing the action of $G$ on the generators of $E(K)$.

Note also that the functor $\iota$ is additive $\iota(M \oplus M') = \iota(M) \oplus \iota(M')$ but it does not behave well in short exact sequences.

**Proposition 24.** Let $G$ be a meta-cyclic group of order $pm$ as in (4.2). Then $\iota(M)$ is trivial for $M$ isomorphic to $A$, $B$ or $\mathbb{Z}_p\{i\}$ for any $i$ and

$$\iota\big(A\{i\}\big) \cong \iota\big(B\{i\}\big) \cong \bigoplus_{k=1}^{m-i} \mathbb{F}_p\{k\}$$

for any $0 < i < m$.

This extends the calculation by Bartel in [2] to more general meta-cyclic groups.

*Proof.* If $M = \mathbb{Z}_p\{i\}$ for any $i$ then $M^N = M$ and therefore $\iota(M) = 0$. Similarly $\iota(A) = 0$ as $A^H = A$. Also $\iota(B) = 0$ because the element $1\,H \in \mathbb{Z}_p\big[G/H\big]$ generates $B$ and it is fixed by the action of the cyclic group $H$.

Let now $m > i > 0$ and $M = A\{i\}$. Since $M^N = 0$, we only need to find $M^H$. From sequence (4) we find that $A\{i+1\}^H$ is isomorphic to $A\{i\}^H$. Hence by induction $A\{i\}^H = (\zeta - 1)^{m-i} A\{i\}$ and $\iota\big(A\{i\}\big) = \bigoplus_{k=1}^{m-i} \mathbb{F}_p\{k\}$.

If we identify $B\{i\}$ with the subset of $(a, z) \in A\{i\} \oplus \mathbb{Z}_p\{i\}$ such that $a \equiv z \pmod{\zeta - 1}$, then we find $\big(B\{i\}\big)^N = \big\{(0, z) \;\big|\; z \in p\mathbb{Z}_p\big\}$ and $\big(B\{i\}\big)^H = \big\{(a, 0) \;\big|\; a \in (\zeta - 1)^{m-i}\big\}$. It follows that $\iota\big(B\{i\}\big) \cong \iota\big(A\{i\}\big)$. □

The following can be read out directly from Table 1 below.

**Proposition 25.** The last entry in the list in Theorem 23 can be replaced by

- $\dim_{\mathbb{F}_p} \iota(M)$.

### 4.4 Summary

In Table 1 we summarise the information gathered about $\mathbb{Z}_p[G]$-lattices, in case $G = D_p$. We write $\breve{\mathbb{Z}}_p$ for $\mathbb{Z}_p\{1\}$, as well as $\breve{A} = A\{1\}$, and $\breve{B} = B\{1\}$, and $\breve{\mathbb{F}}_p = \mathbb{F}_p\{1\}$.

Table 1: Invariants of lattices for the dihedral group $D_p$

| $M$ | $\mathbb{Z}_p$ | $\breve{\mathbb{Z}}_p$ | $A$ | $\breve{A}$ | $B$ | $\breve{B}$ |
|---|---|---|---|---|---|---|
| $\operatorname{rk} M$ | 1 | 1 | $p-1$ | $p-1$ | $p$ | $p$ |
| $\operatorname{rk} M^H$ | 1 | 0 | $\frac{p-1}{2}$ | $\frac{p-1}{2}$ | $\frac{p+1}{2}$ | $\frac{p-1}{2}$ |
| $\operatorname{rk} M^N$ | 1 | 1 | 0 | 0 | 1 | 1 |
| $\operatorname{rk} M^G$ | 1 | 0 | 0 | 0 | 1 | 0 |
| $\hat{H}^0(N, M)$ | $\mathbb{F}_p$ | $\breve{\mathbb{F}}_p$ | 0 | 0 | 0 | 0 |
| $H^1(N, M)$ | 0 | 0 | $\mathbb{F}_p$ | $\breve{\mathbb{F}}_p$ | 0 | 0 |
| $s(M)$ | $-1$ | 1 | 1 | $-1$ | 0 | 0 |
| $\dim_{\mathbb{F}_p} \iota(M)$ | 0 | 0 | 0 | 1 | 0 | 1 |

## 5 The group of local points in a cyclic extension

In this section, we determine the $\mathbb{Z}_p[G]$-structure of the group of points on an elliptic curve for some local extension. The method in this section could be applied to an arbitrary extension whose group is one we understand the $\mathbb{Z}_p[G]$-modules that could arise. However we will concentrate on the simplest extension and it turns out that the answer is already quite involved.

**Theorem 26.** Let $p > 2$ be a prime and let $K/\mathbb{Q}_p$ be the unramified extension of degree $p$. Let $E/\mathbb{Q}_p$ be an elliptic curve. Suppose that, if $p = 3$, the curve has not additive reduction of type IV or IV$^*$. Unless the reduction is split multiplicative and the Tamagawa number $c_v$ is divisible by $p$, we are in one of the following three cases:

| | | | |
|---|---|---|---|
| $\lvert E(\mathbb{Q}_p)[p]\rvert$ | 1 | $p$ | $p$ |
| $\lvert E(K)[p]\rvert$ | 1 | $p$ | $p^2$ |
| $E(K) \hat{\otimes} \mathbb{Z}_p$ | $\mathbb{Z}_p[G]$ | $\{\mathbb{Z}/p\mathbb{Z} \mid \mathbb{Z}_p \oplus A\}$ | $F_2 \oplus \mathbb{Z}_p[G]$ |

If the reduction is split multiplicative and $p \mid c_v$, then set $j = \operatorname{ord}_p(c_v)$ and $\lvert E(\mathbb{Q}_p)[p^\infty]\rvert = p^i$. Then we are in one of the following cases:

| | $i = 0$ | $j = i > 0$ | $j > i > 0$ |
|---|---|---|---|
| $E(K) \hat{\otimes} \mathbb{Z}_p$ | $\mathbb{Z}_p \oplus A$ | $\mathbb{Z}/p^i\mathbb{Z} \oplus \mathbb{Z}_p[G]$ | $\{\mathbb{Z}/p^i\mathbb{Z} \mid A\} \oplus \mathbb{Z}_p$ |

*Proof.* Let $M \cong E(K)\hat{\otimes}\mathbb{Z}_p$. Since the formal logarithm induces a $\mathbb{Q}_p[G]$-isomorphism $M \otimes \mathbb{Q}_p \to K$, we have $M \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[G]$. Since $K$ is unramified, the $p$-th roots of 1 cannot be contained in $K$ and therefore $M_t = E(K)[p^\infty]$ is cyclic. Hence the classification in Theorem 19 applies.

From Lemma 7, we know that $D = \hat{H}^0(G, M)$ is cyclic of order $p$ if the reduction is split multiplicative and $p \mid c_v$ and otherwise it is trivial.

Assume $D$ is trivial. If the reduction is split multiplicative then $p \nmid c_v$ and as the Tate parameter $q$ of $E$ has a valuation that is not a multiple of $p$, there cannot be any points of order $p$ on $E(\mathbb{Q}_p)$. For other types of reduction, we know that both the formal group $\hat{E}(p\mathbb{Z}_p)$ and the group of components $\Phi(\mathbb{F}_p)$ have no elements of order $p$, which means that $E(\mathbb{Q}_p)[p^\infty]$ injects into $\tilde{\mathcal{E}}_v^0(\mathbb{F}_p)$.

By the Hasse-Weil bound in the case of good reduction and by direct considerations in the case of bad reduction, we deduce that $E(\mathbb{Q}_p)[p^\infty]$ is either trivial or cyclic of order $p$. In the first case $M_t = E(K)[p^\infty]$ is also trivial and the only option for $M$ is then $\mathbb{Z}_p[G]$. In the second case, $M_t$ is either $\mathbb{Z}/p\mathbb{Z}$ or $F_2$, which explains the other two entries in the first table.

We can now assume that the reduction is split multiplicative and $p$ divides $c_v$. So $D$ is cyclic of order $p$. Set $j = \mathrm{ord}_p(c_v) > 0$ and $i$ such that $p^i$ is the order of $E(\mathbb{Q}_p)[p^\infty]$.

Since $M_t$ injects into $\Phi(\mathbb{F}_w)[p^\infty] \cong \mathbb{Z}/p^j\mathbb{Z}$, we must have $M_t \cong \mathbb{Z}/p^i\mathbb{Z}$ as a $\mathbb{Z}_p[G]$-module. Therefore, we must have $j \geqslant i$. If $i = 0$, then the classification limits us to only one option, namely $M \cong \mathbb{Z}_p \oplus A$. If $i > 0$, then let $P$ be a point of exact order $p^i$ on $E(\mathbb{Q}_p)$ and consider the isogeny from $E$ to $E'$ whose kernel is generated by $P$. In terms of the Tate curve, this map $K^\times/q^{\mathbb{Z}} \to K^\times/q'^{\mathbb{Z}}$ is induced from the identity map and $(q')^{p^i} = q$. Now the order of the torsion subgroup of $E'$ is no longer divisible by $p$ as $q'$ is not a $p$-power in $\mathbb{Q}_p$. This implies that $E'(K) \hat{\otimes} \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p \oplus A$ or $\mathbb{Z}_p[G]$ depending on whether the Tamagawa number $c'_v$ of $E'$ is divisible by $p$ or not. If $p \nmid c'_v$, then $j = i$ and the extension between $\mathbb{Z}/p^i\mathbb{Z}$ and $\mathbb{Z}_p[G]$ must split.

Instead if $p \mid c'_v$, then $j > i$. The only extensions of $\mathbb{Z}/p^i\mathbb{Z}$ and $\mathbb{Z}_p \oplus A$ with $D \cong \mathbb{Z}/p\mathbb{Z}$ are $\left\{\mathbb{Z}/p^i\mathbb{Z} \;\middle|\; \mathbb{Z}_p\right\} \oplus A$ or $\left\{\mathbb{Z}/p^i\mathbb{Z} \;\middle|\; A\right\} \oplus \mathbb{Z}_p$. We can exclude the first case because the map from $M^G = E(\mathbb{Q}_p) \hat{\otimes} \mathbb{Z}_p$ to $E'(\mathbb{Q}_p) \hat{\otimes} \mathbb{Z}_p$ must be surjective. □

The same proof should work if $k = \mathbb{Q}_p$ is replaced by a finite extension of $\mathbb{Q}_p$ with ramification index less than $p - 1$. The case of reduction IV and IV$^*$ when $p = 3$ can be treated as well but they are more complicated as illustrated by the last example in this section.

## 5.1 Examples

To cover all possible cases with split multiplicative reduction it is enough to look at Tate curves whose parameters are, say,

$$q = p^{p^j} \cdot (1+p)^{p^i} = \left(p^{p^{j-i}} \cdot (1+p)\right)^{p^i}$$

with integers $j \geqslant i \geqslant 0$. This $q$ is a $p^i$-th power so there are $p^i$-torsion points in $E(\mathbb{Q}_p)$. Since $1+p$ is not a $p$-th power, we get $E(\mathbb{Q}_p)[p^\infty] = \mathbb{Z}/p^i\mathbb{Z}$. Also $v_p(c) = v_p(v_p(q)) = j$.

For the two additive cases, we can take the following two examples. First $E : y^2 + y = x^3$ over $\mathbb{Q}_3$ has additive reduction of type II. There is a 3-torsion point $(0, 0)$ in $E(\mathbb{Q}_3)$. Hence $E(K) \hat{\otimes} \mathbb{Z}_p$ must be $\left\{\mathbb{Z}/p\mathbb{Z} \;\middle|\; \mathbb{Z}_p \oplus A\right\}$.

Secondly, $E : y^2 + y = x^3 - 270\,x - 1708$ has additive reduction of type II$^*$ over $\mathbb{Q}_3$. This time one can show that $E(\mathbb{Q}_3)$ does not contain a point of order 3 directly by checking the roots of the 3-division polynomial. Alternatively on can use the map $\partial$ in the exact sequence

$$0 \longrightarrow E(\mathbb{Q}_p)[p] \longrightarrow \tilde{E}^0(\mathbb{F}_p)[p] \xrightarrow{\partial} \hat{E}(p\mathbb{Z}_p)/p\hat{E}(p\mathbb{Z}_p)$$

For instance the point $P = (1, 3 + 3^2 + 2 \cdot 3^3 + \cdots)$ has non-trivial non-singular reduction. Then $Q = 3P = (3^{-2} + 2{\cdot}3^2 + \cdots, 2{\cdot}3^{-3} + 2{\cdot}3^{-2} + \cdots)$ belongs to $\hat{E}(p\mathbb{Z}_p)$ but not to $p\hat{E}(p\mathbb{Z}_p) = \hat{E}(p^2\mathbb{Z}_p)$. Therefore $\partial(\tilde{P}) = Q + p\hat{E}(p\mathbb{Z}_p)$ is non-trivial. It follows that $E(\mathbb{Q}_p)[p]$ is trivial and $E(K) \hat{\otimes} \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p[G]$.

Now to curves with good reduction. The curve $y^2 + x\,y + y = x^3 - 171\,x - 874$ has good ordinary, anomalous reduction $\tilde{P} = (1, 0)$ over $\mathbb{Q}_3$. With the methods from the previous case one can show that $E(\mathbb{Q}_p)[p]$ is trivial in this case. Thus $E(K) \hat{\otimes} \mathbb{Z}_p$ is a free.

Instead the curve $E : y^2 + x\,y + y = x^3 + 4\,x - 6$ has also good ordinary, anomalous reduction over $\mathbb{Q}_3$, but it contains a 3-torsion point $(2, 2)$. It can be shown that this point does not become divisible by 3 in $K$. Therefore $E(K) \hat{\otimes} \mathbb{Z}_p$ must be isomorphic to $\left\{\mathbb{Z}/p\mathbb{Z} \;\middle|\; \mathbb{Z}_p \oplus A\right\}$.

Finally, here an example when $E(K) \hat{\otimes} \mathbb{Z}_p$ must be $F_2 \oplus \mathbb{Z}_p[G]$. The curve $E : y^2 + y = x^3 + x^2 + x$ has a 3-torsion point $T = (0, 0)$ and it has good reduction over $\mathbb{Q}_3$. The extension $K$ can be obtained

by adjoining $t$ to $\mathbb{Q}_3$ with $t^3+2\,t+1=0$. Then the point

$$S=\big((t^2+2\,t+2)+(2\,t^2+t+1)\cdot 3+(t^2+t+2)\cdot 3^2+(2\,t+2)\cdot 3^3+\cdots,\\ (t^2+t+1)+(t+2)\cdot 3+t^2\cdot 3^2+(2\,t^2+2\,t+1)\cdot 3^3+\cdots\big)$$

is such that $3\,S=T$.

Therefore we have found explicit examples for all possible $\mathbb{Z}_pG$-modules in Theorem 26. Instead the modules $\left\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}\;\middle|\;\mathbb{Z}_p\oplus A\right\}$ with $i>1$ and the modules $\left\{{}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}\;\middle|\;\mathbb{Z}_p\right\}\oplus A$ for $i\geqslant 1$ cannot occur, neither can $F_2\oplus\mathbb{Z}_p\oplus A$ or ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\oplus\mathbb{Z}_p\oplus A$.

To illustrate that the situation is more complicated in the one cases not treated in Theorem 26, we add one example. The curve

$$y^2+xy+9\,y=x^3-x^2+9\,x+9$$

over $\mathbb{Q}_3$ has additive reduction of type IV with Tamagawa number $c_v=3$. This curve has a rational 9-torsion point $T$ with $x$-coordinate $3+2\,3^2+2\,3^4+3^5+3^6+2\,3^7+3^8+2\,3^9+\mathbf{O}(3^{10}$. It has bad reduction, but $3T$ is a 3-torsion point with good reduction. It seems that $E(K)\,\hat{\otimes}\,\mathbb{Z}_p$ is isomorphic to $\left\{{}^{\mathbb{Z}}\!/_{9\mathbb{Z}}\;\middle|\;\mathbb{Z}_3\right\}\oplus A$.

# 6 Descent for Mordell-Weil and Selmer groups

We now pass to studying global extensions and gather the tools to study how the Galois group of a finite extension acts on the Mordell-Weil group and on the Selmer group.

Let $k$ now be a number field and let $K/k$ be a finite extension with Galois group $G$. Let $E/k$ be an elliptic curve and let $p$ be an odd prime.

We write $M=E(K)\,\hat{\otimes}\,\mathbb{Z}_p=E(K)\otimes\mathbb{Z}_p$, which we are going to study as a $\mathbb{Z}_p[G]$-module. Recall that $M_t$ is the torsion subgroup of $M$ and $M_f=M/M_t$. We have $M^G=E(k)\otimes\mathbb{Z}_p$. Similarly the $G$-fixed part of $M\otimes\mathbb{Q}_p=E(K)\otimes\mathbb{Q}_p$ is $E(k)\otimes\mathbb{Q}_p$. Consider instead the limit $\varinjlim E(K)/p^nE(K)$ which naturally identifies with $E(K)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$. The map comparing $\left(M\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\right)^G$ with $E(k)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$ measures if any points $P\in E(k)$ become divisible by $p$ in $E(K)$ when they were not in $E(k)$:

**Lemma 27.** We have an exact sequence

$$0\longrightarrow\ker\Big(H^1(G,M_t)\to H^1(G,M)\Big)\longrightarrow E(k)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\longrightarrow\Big(E(K)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\Big)^G\longrightarrow H^1(G,M_f)\longrightarrow 0.$$

*Proof.* First the definition of $M_f$ yields the long exact sequence

$$0\longrightarrow E(k)[p^\infty]\longrightarrow E(k)\otimes\mathbb{Z}_p\longrightarrow {M_f}^G\longrightarrow H^1(G,M_t)\longrightarrow H^1(G,M).$$

Further we have an exact sequence

$$0\longrightarrow M_f^G\longrightarrow E(k)\otimes\mathbb{Q}_p\longrightarrow\Big(E(K)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\Big)^G\longrightarrow H^1(G,M_f)\longrightarrow 0$$

deduced from the short exact sequence

$$0\longrightarrow M_f\longrightarrow E(K)\otimes\mathbb{Q}_p\longrightarrow E(K)\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\longrightarrow 0.$$

and an isomorphism

$$H^1\big(G,M\otimes{}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big)\cong H^2(G,M_f)\tag{5}$$

which will be useful later. The kernel-cokernel sequence for the composition $E(k)\hat{\otimes}\mathbb{Z}_p\to E(k)\otimes\mathbb{Q}_p$ via $M_f^G$ produces the exact sequence in the lemma. □

In particular if $M$ is torsion-free, then $H^1(G,M)$ is the cokernel of the injective map $E(k)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \to \big(E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big)^G$.

We can compare $M$ to the local group of points. Let $v$ be a finite place of $k$ and let $w$ be a place of $K$ above $v$. Let $M_w = E(K_w)\,\hat{\otimes}\,\mathbb{Z}_p$. If $v\nmid p$ then $M_w$ is finite; otherwise it is a $\mathbb{Z}_p$-module of rank $[K_w:\mathbb{Q}_p]$. In Section 5 we have investigated $M_w$ as a $\mathbb{Z}_p\big[\mathrm{Gal}(K_w/k_v)\big]$-module. Setting $M_v = \bigoplus_{w|v} M_w$ we get a $\mathbb{Z}_p[G]$-module.

By $S$ we will denote a fixed choice of a finite set of places in $k$ containing all places above $p$ and $\infty$, such that $E$ has good reduction outside $S$ and such that $K/k$ is unramified outside $S$. The Galois group of the maximal extension of $k$ which is unramified outside $S$ is denoted by $G_S(k)$.

We define the $p$-primary Selmer group $\mathcal{S}_k$ as the subgroup of $H^1\big(G_S(k),E[p^\infty]\big)$ consisting of elements whose restrictions at all places $v\in S$ lie in the image of the local Kummer map $\kappa_v\colon E(k_v)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \to H^1\big(k_v,E[p^\infty]\big)$. The compact $p$-adic Selmer group $\mathfrak{S}_k$ is the subgroup of $H^1\big(G_S(k),T_pE\big)$ defined in the same way with respect to the local Kummer maps $E(k_v)\,\hat{\otimes}\,\mathbb{Z}_p \to H^1\big(k_v,T_pE\big)$. The cokernel of the global Kummer map $E(k)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} \to \mathcal{S}_k$ is the $p$-primary part of the Tate-Shafarevich group $Ш(E/k)$. We will simply denote it by $Ш_k$.

**Assumption 1.** Throughout this article we assume that the $p$-primary subgroup $Ш_k$ of the Tate-Shafarevich group is a finite group for all number fields $k$ and all elliptic curves.

One can drop this assumption and work with the quotient of $Ш_k$ by its maximal divisible subgroup instead. It follows from this assumption that $\mathfrak{S}_K$ is simply $M = E(K)\otimes\mathbb{Z}_p$ and $\mathfrak{S}_k$ is $M^G$.

Using the isomorphism (5), we obtain a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Big(E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\Big)^G & \longrightarrow & \mathcal{S}_K^G & \longrightarrow & Ш_K^G & \longrightarrow & H^2\big(G,M_f\big) \\
 & & \uparrow & & \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\eta} & & \\
0 & \longrightarrow & E(k)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p} & \longrightarrow & \mathcal{S}_k & \longrightarrow & Ш_k & \longrightarrow & 0
\end{array}$$

which describes the link of the exact sequence in Lemma 27 to the natural restriction maps $\alpha$ on the Selmer group and $\eta$ on the Tate-Shafarevich groups. Below we will determine the kernel and cokernel of $\alpha$. We denote the kernel of $\eta$ by $C_{K/k}$ and call it the capitulation subgroup of $Ш(E/k)[p^\infty]$ with respect to the extension $K/k$. The snake lemma applied to this diagram provides us with an exact sequence

$$\begin{array}{ccccccc}
\ker(\alpha) & \longrightarrow & C_{K/k} & \longrightarrow & H^1(G,M_f) & \rightarrowtail & \\
 & & & & & & \\
\twoheadrightarrow \mathrm{coker}(\alpha) & \longrightarrow & \mathrm{coker}(\eta) & \longrightarrow & H^2(G,M_f). & &
\end{array} \tag{6}$$

**Assumption 2.** We assume that $E(K)$ does not contain any non-trivial $p$-torsion elements.

**Lemma 28.** Under Assumption 2, we have the exact sequence

$$0\longrightarrow C_{K/k}\longrightarrow H^1(G,M)\longrightarrow \mathrm{coker}(\alpha)\longrightarrow \mathrm{coker}(\eta)\longrightarrow H^2(G,M).$$

*Proof.* The kernel of the first map in the sequence (6) is in fact the kernel of $H^1(G,M_t)\to H^1(G,M)$ as we have seen in Lemma 27. By the assumption $M$ is $\mathbb{Z}_p$-free, hence $M_t$ is trivial and $M_f = M$. □

Our next aim is to determine the cokernel of the restriction map $\alpha$ between $\mathcal{S}_k$ and $\mathcal{S}_K^G$.

Global duality, in form of the exact sequence due to Cassels, see Section 1.7 in [41], allows us to compare $M$ with the local terms $M_v$. It yields the exact sequence

$$M\longrightarrow \bigoplus\nolimits_{v\in S} M_v \longrightarrow H^1\big(G_S(K),E[p^\infty]\big)^\vee \longrightarrow \mathcal{S}_K^\vee \longrightarrow 0$$

of $\mathbb{Z}_p[G]$-modules. The kernel on the left is the fine (or strict) Mordell-Weil group $\mathfrak{R}_{S,K}$. In many circumstances this group is trivial; see for instance [47]. By global duality, as in Theorem 8.6.8 in [35], $\mathfrak{R}_{S,K}$ is dual to $H^2\big(G_S(K), E[p^\infty]\big)$. We compare the $G$-fixed part of the dual of the above exact sequence with the corresponding sequence over $k$ to make the map $\alpha$ appear in the following large commutative diagram. The top sequence is only a complex; at the terms where the complex is not necessarily exact we use the symbol $\circ\!\!\longrightarrow$.

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathcal{S}_K^G & \longrightarrow & H^1\big(G_S(K), E[p^\infty]\big)^G & \longrightarrow & \bigoplus_{v|S}\big(M_v^\vee\big)^G & \circ\!\!\longrightarrow & \big(M^\vee\big)^G & \circ\!\!\longrightarrow & \big(\mathfrak{R}_{S,K}^\vee\big)^G \circ\!\!\longrightarrow 0 \\
 & & \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\gamma} & & \uparrow{\scriptstyle\delta} & & \uparrow{\scriptstyle\varepsilon} \\
0 & \longrightarrow & \mathcal{S}_k & \longrightarrow & H^1\big(G_S(k), E[p^\infty]\big) & \longrightarrow & \bigoplus_{v\in S}\big(M_v^G\big)^\vee & \longrightarrow & \big(M^G\big)^\vee & \longrightarrow & \mathfrak{R}_{S,k}^\vee \longrightarrow 0
\end{array}$$

The map $\gamma$ is then $\oplus_{v\in S}\gamma_v$ where $\gamma_v$ is the dual of the natural norm map; its kernel is dual to

$$\begin{aligned} D_v &= \operatorname{coker}\Big(\mathrm{N}\colon \bigoplus_{w|v} E(K_w)\mathbin{\hat\otimes}\mathbb{Z}_p \to E(k_v)\mathbin{\hat\otimes}\mathbb{Z}_p\Big) \\ &= \hat H^0\Big(G, \bigoplus_{w|v} E(K_w)\mathbin{\hat\otimes}\mathbb{Z}_p\Big) \cong \hat H^0\big(G_w, M_w\big). \end{aligned} \tag{7}$$

for any chosen $w$ above $v$. Here $G_w = \operatorname{Gal}(K_w/k_v)$ is the decomposition group. The groups $D_v$ was studies in detail in the section 3.

The maps $\delta$ and $\varepsilon$ are the dual of the norm maps

$$\hat\delta\colon \big(E(K)\otimes\mathbb{Z}_p\big)_G \to E(k)\otimes\mathbb{Z}_p$$

and its restriction to the fine Mordell-Weil group. Therefore $\ker\delta$ is dual to $\hat H^0(G,M)$ and $\operatorname{coker}\delta$ is dual to $\hat H^{-1}(G,M)$. The commutativity of the diagram follows from the functoriality of global duality and the local duality of restriction and corestriction.

Our assumption 2, that $E(K)$ has no non-trivial $p$-torsion points, implies that $\beta$ is an isomorphism by the inflation-restriction-transgression exact sequence, see Proposition 1.6.6 in [35].

We are in a situation where we have a morphism of complexes $A^\bullet \to B^\bullet$ with $A^\bullet$ exact. Let $\bar A^\bullet$ be the complex of kernels and $\bar B^\bullet$ the complex of cokernels. As a consequence of the long exact sequences of cohomology of complexes in short exact sequences, we can deduce that there is a long exact sequence

$$\cdots\longrightarrow H^{i+1}(\bar A^\bullet)\longrightarrow H^i(B^\bullet)\longrightarrow H^i(\bar B^\bullet)\longrightarrow H^{i+2}(\bar A^\bullet)\longrightarrow\cdots$$

In our case, since the first two terms of $B^\bullet$ have trivial cohomology, we deduce that $\ker(\alpha)=0$ and that

$$0\longrightarrow\operatorname{coker}(\alpha)\longrightarrow\ker\gamma\longrightarrow\ker\Big(\ker\delta\to\ker\varepsilon\Big)\longrightarrow\cdots$$

is exact. The image at the end is a subquotient of $\bigoplus_{w\in S_K}\big(E(K_v)\mathbin{\hat\otimes}\mathbb{Z}_p\big)^\vee$. In particular we conclude the following.

**Proposition 29.** Under our assumptions, we have $\ker(\alpha)=0$ and $\operatorname{coker}(\alpha)$ is dual to the cokernel of $E(k)\otimes\mathbb{Z}_p\to D_{K/k}$ where $D_{K/k}=\bigoplus_{v\in S}D_v=\bigoplus_{v\in S}\hat H^0\big(G_w,E(K_w)\mathbin{\hat\otimes}\mathbb{Z}_p\big)$.

We have calculated $D_v$ in many circumstance in Section 3. In most situations, the above proposition can be used to determine $\operatorname{coker}(\alpha)$ explicitly using only local information and information about $E$ over $k$.

**Proposition 30.** Suppose that no place above $p$ is wildly ramified in $K/k$ and suppose that the ramification index $e_v$ is not divisible by $p$ at all places where $E$ has bad reduction. Then

$$D_{K/k}\cong\bigoplus_{v\in S_{\mathrm{b}}}\mathbb{Z}/(c_v,f_v,p^\infty)\oplus\bigoplus_{v\in S_{\mathrm{r}}}\tilde E(\mathbb{F}_v)[p^\infty]/e_v\tilde E(\mathbb{F}_v)[p^\infty]$$

where $S_{\mathrm{b}}$ is the set of all places where $E$ has bad reduction and $S_{\mathrm{r}}$ is the set of all places where $p$ divides the ramification index $e_v$.

*Proof.* For all places with $p \nmid e_v$, Proposition 13 shows that $D_v$ is cyclic of order equal to $\gcd(c_v, f_v, p^\infty)$. This is non-trivial only for places of bad reduction and they appear in the first sum above.

If $v$ is a place in $S_{\mathrm{r}}$, then, by assumption, $E$ has good reduction and $v \nmid p$. Therefore Proposition 15 applies and gives the second term. □

Note also that the map $E(k) \to E(k_v) \to D_v$ is explicit and easy to calculate. As a consequence, we can effectively determine the cokernel of $\alpha$ in most examples.

# 7 The Galois module structure of Mordell-Weil groups

Let $E/k$ be an elliptic curve and let $K/k$ be a Galois extension of number fields with group $G$. Let $p$ be an odd prime. Throughout this section, we continue to assume the Assumptions 1 and 2.

Recall that the aim is to understand in what cases we can determine the structure of $M = E(K)\hat{\otimes}\mathbb{Z}_p$ as a $\mathbb{Z}_p[G]$-module, preferably with information that is easier to access than computing $M$ itself.

We first recall the results of [12], which can be extended to all situations when we have "perfect control", i.e., when

$$\alpha\colon \mathcal{S}_k \to \mathcal{S}_K^G$$

is an isomorphism. Recall that $\operatorname{coker}(\alpha)$ is dual to the cokernel of $E(k)\otimes\mathbb{Z}_p \to D_{K/k}$, which is effectively computable by Proposition 29.

**Theorem 31** (Theorem 2.2 in [12])**.** Assume also that $\operatorname{coker}\alpha$ is trivial. Fix a $p$-Sylow subgroup $\mathcal{H}$ of $G$. Then $M$ is a projective $\mathbb{Z}_p[G]$-module if and only if $M\otimes\mathbb{Q}_p$ is a free $\mathbb{Q}_p[G/\mathcal{H}]$-module and $C_{K/K^H}$ is trivial for all subgroups $H$ in $\mathcal{H}$.

When the $p$-Sylow subgroup $\mathcal{H}$ is cyclic, we can use the results of Yakovlev [51] to determine $M$ as follows. Since $\mathcal{H}$ is cyclic, say of order $p^n$, we have a tower of fields $F_i$ such that $[K : F_i] = p^{n-i}$ and $F_0 = K^{\mathcal{H}}$.

**Theorem 32** (Theorem 2.6 in [12])**.** Suppose that the $p$-Sylow subgroup $\mathcal{H}$ of $G$ is cyclic. Assume that $\operatorname{coker}(\alpha)$ is trivial. Then $M$ is determined up to isomorphism by the the ranks of $E(F_i)$ and the knowledge of the capitulation kernels as $\mathbb{Z}_p\big[N_G(\mathcal{H})\big]$ together with the restriction and corestriction maps between them:

$$C_{K/F_0} \rightleftarrows C_{K/F_1} \rightleftarrows \cdots \rightleftarrows C_{K/F_{s-1}}.$$

Since $C_{K/F_i} \cong \hat{H}^{-1}\big(K/F_i, M\big) \approx H^1\big(K/F_i, M\big)$ the diagram of restrictions and corestrictions above is an example of a Yakovlev diagram. Specialising to the situation when the $p$-Sylow $\mathcal{H}$ of $G$ is cyclic of order $p$, the Yakovlev diagram simplifies then to a single group $H^1\big(\mathcal{H}, M\big)$ viewed as a $\mathbb{F}_p\big[N_G(\mathcal{H})/\mathcal{H}\big]$-module. It is well possible that the results in [30] also hold under the weaker hypothesis that $\alpha$ is surjective.

Torzewski [44] generalises this to the case when $\alpha$ is not necessarily surjective (as in Theorem 23 for the dihedral case) but involving the regulator constants $s_\Theta(M)$, too. This new ingredient can be linked to arithmetic information as follows. Fix an invariant differential $\omega$ on $E$ and write $u_v = |\omega/\omega_{\text{Néron}}|_v$ for when it differs from the Néron differential $\omega_{\text{Néron}}$ of $E$ at the finite place $v$. For any field $F/k$, we define $C(E/F) = \prod_v c_v(E/F)\cdot u_v$ to be the modified product over all finite places $v$ of $F$ of the Tamagawa numbers $c_v$. This quantity together with the real and complex periods with respect $\omega$ should appear in the leading term of the Birch and Swinnerton-Dyer conjecture for $E/F$. The following is a consequence of Theorem 2.3 in [21].

**Theorem 33.** Assume that no place of additive reduction ramifies in $K/k$. Let $\Theta = \sum m_i H_i$ be a Brauer relation for $G$. For $F = K^{H_i}$ write $s_i = \operatorname{ord}_p(|Ш_F|) + \operatorname{ord}_p\big(C(E/F)\big)$. Then $s_\Theta(M) = -\sum_i m_i s_i$.

Under our assumption, we can determine the parity of $s_\Theta(M)$ from the Tamagawa numbers only as the Tate-Shafarevich groups are of square order.

**Corollary 34.** Under our assumptions, $s_\Theta(M) \equiv \sum_i m_i \operatorname{ord}_p\big(C(E/F^{H_i})\big) \pmod 2$ for any Brauer relation $\Theta = \sum_i m_i H_i$.

The parity here will link directly to global root numbers. However in general case, we often need the ranks rather than just their parity. In the particular cases that we turn our attention to, the valuation of $s_\Theta(M)$ and the rank over $k$ will provide more information than the root numbers.

## 7.1 Cyclic extensions

Suppose first that $G$ is a cyclic group of order $p$. Recall that we write $D_{K/k}$ for $\bigoplus_{v\in S} D_v$, which is a $\mathbb{F}_p$-vector space in our situation.

**Corollary 35.** Let $S_{\mathrm{r}}^0$ be the set of all ramified places in $k$ not lying above $p$ and at which $E$ has good reduction.

$$\dim_{\mathbb{F}_p} D_{K/k} \geqslant \#\big\{v \;\big|\; v \text{ inert and } p \mid c_v\big\} + \sum_{v\in S_{\mathrm{r}}^0} \dim_{\mathbb{F}_p} \tilde{E}(\mathbb{F}_v)[p].$$

If no place of bad reduction and no place above $p$ ramifies, then we have equality.

Though the calculations extend easily to all cases such that $E$ has good ordinary reduction at all places above $p$ that are ramified in $K/k$.

*Proof.* First the dimension of $D_{K/k}$ is larger than the sum of the dimensions of $D_v$ for all places excluding the ramified places above $p$ and the ramified places at which $E$ has bad reduction. For the remaining $v$, we calculated $D_v$ in Proposition 30 and we can simplify it a bit because $G$ is cyclic of order $p$. □

Recall that, by Proposition 16, there are only 3 indecomposable $\mathbb{Z}_p[G]$-lattices $\mathbb{Z}_p$, $A$ and $\mathbb{Z}_p[G]$ in this case. We note that $M$ cannot be determined by $\operatorname{rk} E(K)$ and $\operatorname{rk} E(k)$ only, but they will determine it together with the order of $H^1(G, M)$.

Here are a few statements that one can deduce easily from the fact that

**Proposition 36.** Let $E/k$ be an elliptic curve and $K/k$ a cyclic extension of degree $p$ satisfying Assumptions 1 and 2.

(i) If $Ш_k$ and $D_{K/k}$ are trivial, then $\operatorname{rk} E(K)$ and $\operatorname{rk} E(k)$ determine $M$.
(ii) If $\operatorname{rk} E(k) = 0$ and $Ш_k$ is trivial, then $\operatorname{rk} E(K) \leqslant (p-1)\dim_{\mathbb{F}_p} D_{K/k}$.
(iii) If $\operatorname{rk} E(k) = 0$ and $Ш_k$ is trivial, but $\operatorname{rk} E(K) < (p-1)\dim_{\mathbb{F}_p} D_{K/k}$, then $Ш_K$ is not trivial.
(iv) If $\alpha$ is surjective, $\operatorname{rk} E(K) > \operatorname{rk} E(k) = 1$, and $Ш_k$ trivial, then $M \cong \mathbb{Z}_p[G]$ and $Ш_K = 0$.

*Proof.* For the first point, the hypothesis imply that $\operatorname{coker}(\alpha)$ and $C_{K/k}$ are trivial. By Lemma 28, this implies that $H^1(G, M) = 0$ and hence $M$ is a direct sum of copies of $\mathbb{Z}_p$ and $\mathbb{Z}_p[G]$, which can be determined by the ranks alone.

In part (ii) and (iii), $\operatorname{rk} E(k) = 0$ implies that $M$ is a power of $A$. The power is equal to $\dim H^1(G, M)$ which is the dimension of $\ker\big(\operatorname{coker}(\alpha) \to \operatorname{coker}(\eta)\big)$. As the rank is zero over $k$, the cokernel of $\alpha$ is dual to $D_{K/k}$. If the resulting inequality is strict, then $\operatorname{coker}(\eta)$ is non-trivial and hence so is $Ш_K$.

For the final item, the surjectivity of $\alpha$ and the triviality of $Ш_k$ imply again that $H^1(G, M) = 0$. As the rank grows but is equal to 1 over $k$, we must have $M = \mathbb{Z}_p[G]$. This now also implies that $H^2(G, M) = 0$. From Lemma 28 we learn that $\eta$ is surjective. Since $G$ is a $p$-group, the triviality of $Ш_K^G$ implies that $Ш_K$ is trivial. □

*Proof of Theorem 2.* The assumption that $L(E,\chi,1)\neq 0$ implies by Kato's result that $\operatorname{rk} E(K) = \operatorname{rk} E(k)$. Therefore $M=\mathbb{Z}_p^r$ with $r=r_{\mathbb{Q}}$. By Corollary 35, the dimension of $D_{K/\mathbb{Q}}$ is greater or equal to $u_1+u_2$. Therefore, Proposition 29 tells us that $\operatorname{coker}(\alpha)$ has dimension at least equal to $u_1+u_2-r$. Since $H^1(G,M)=0$, $\operatorname{coker}(\alpha)$ injects into $\operatorname{coker}(\eta)$ by Lemma 28. Hence $\dim Ш_K \geqslant \dim Ш_K^G \geqslant \dim \operatorname{coker}(\eta) \geqslant u_1+u_2-r$. (By the way, we also get $\dim Ш_K^G \leqslant u_1+u_2+r+\dim Ш_k$.) □

The exact sequence relating the Mordell-Weil group $M$ and the Tate-Shafarevich group $Ш_K$ to the Selmer group $\mathcal{S}_K$ is split as a sequence of abelian groups [25], but not necessarily as $G$-modules. There is one important exception.

**Lemma 37.** Suppose $M\cong\mathbb{Z}_p[G]$. Then

$$\mathcal{S}_K \cong \big(E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big)\oplus Ш_K$$

as $G$-modules and we have an exact sequence

$$0\longrightarrow Ш_k\longrightarrow Ш_K^G\longrightarrow D_{K/k}^\vee\longrightarrow 0.$$

*Proof.* Note that there is an isomorphism $\operatorname{Hom}\big(E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}, {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}\big)=\operatorname{Hom}\big(M,\mathbb{Z}_p\big)$ by the assumption that $E(K)[p]$ is trivial. If $M$ is free, then so is the Pontryagin dual of $E(K)\otimes {}^{\mathbb{Q}_p}\!/_{\mathbb{Z}_p}$. Since the quotient of $\mathcal{S}_K^\vee$ by $Ш_K^\vee$ is now a projective $\mathbb{Z}_p[G]$-module, we must have $\mathcal{S}_K^\vee\cong\operatorname{Hom}\big(M,\mathbb{Z}_p\big)\oplus Ш_K^\vee$ whose Pontryagin dual is the initial statement. The exact sequence (6), together with $H^1(G,M)=0$ and $H^2(G,M)=0$, shows $C_{K/k}=0$ and that $\operatorname{coker}\eta=\operatorname{coker}\alpha$. As the norm map $M_G\to M^G$ is an isomorphism, the cokernel of $\alpha$ is dual to $D_{K/k}$. □

**Theorem 38.** Let $E/k$ be an elliptic curve and $p$ an odd prime. Suppose that $\operatorname{rk} E(k)=0$, that $Ш_k=0$ and that the image of the Galois representation $\operatorname{Gal}(\bar{k}/k)\to\operatorname{GL}\big(E[p]\big)$ contains $\operatorname{SL}_2\big(E[p]\big)$. Then there is a positive proportion of cyclic extensions $K/k$ of degree $p$, ordered by the norm of the conductor, such that $M=0$.

Note that we expect that a positive proportion of elliptic curves $E/k$ should satisfy the hypothesis in the theorem. It is important to emphasis that this results is weaker than Theorem 9.21 in [34] in the sense that we restrict to curves of rank 0 and prime degree, but more general in other aspects.

*Proof.* By Proposition 36 (ii), we only need to show that $D_{K/k}$ is trivial for a positive proportion of $K$. To avoid the conductor of $K$ being divisible by bad primes is no problem for this. A positive proportion of $K$ have the property that all primes $v$ with $p\mid c_v$ split in $K/k$. Since the Galois group of $K\big(E[p]\big)/k$ contains $\operatorname{SL}_2(\mathbb{F}_p)$ there is a positive proportion of places $v$ of good reduction such that $|\tilde{E}(\mathbb{F}_v)|$ is not divisible by $p$ by Chebotarev's density theorem. Therefore for a positive proportion of extensions $K/k$, we can avoid that it is ramified at places with $p\mid\#\tilde{E}(\mathbb{F}_v)$. □

**Proposition 39.** Let $E/k$ be an elliptic curve and $p$ and odd prime. Suppose that there are more than $\operatorname{rk} E(k)$ primes $v$ such that $p\mid c_v$. Then there is a positive proportion of cyclic extensions $K/k$ of degree $p$ for which we have $\operatorname{rk} E(K)>\operatorname{rk} E(k)$ or $Ш_K\neq 0$.

*Proof.* We will show that there is a positive proportion of $K$ such that $\operatorname{coker}(\alpha)$ is non-trivial. For that matter we only need to make sure that all places $v$ with $p\mid c_v$ are inert in $K/k$ as then the dimension of $D_{K/k}$ is larger than the rank of $E(k)$ and hence $\operatorname{coker}(\alpha)$ is non-trivial. This holds for a positive proportion of $K/k$. Now, we have $H^1(G,M)\neq 0$ or $\operatorname{coker}(\eta)\neq 0$. In the first case $M$ contains copies of $A$ and hence the rank of $E(K)$ is larger than the rank of $E(k)$. In the second case, $Ш_K^G$ and hence $Ш_K$ is non-trivial. □

Let us specialise to the case when $k = \mathbb{Q}$. Since the $L$-function $L(E, \chi, s)$ admits an analytic continuation for all $\chi$, it is easy to determine when the rank grows, that is when $\operatorname{rk} E(K) > \operatorname{rk} E(k)$. Note that we can calculate the value $L(E, \chi, 1)$ very quickly using modular symbols and if that value is non-zero, then the rank does not grow. Under our assumption that $Ш_K$ is finite, $L(E, \chi, 1) = 0$ implies that the rank grows. Rank growth is relatively rare, especially for $p > 5$, as expected by the conjectures made in [17, 24]. Cases where the rank grows by more than $p - 1$ are hard to find, but see Example G below for such a case.

**Corollary 40.** If $p = 3$ or $p = 5$, then a positive proportion of $(E, K)$ where $E/\mathbb{Q}$ is an elliptic curve, ordered by height, and $K$ is a cyclic extension of degree $p$, ordered by conductor, satisfy $E(K) = 0$.

*Proof.* This is a consequence of Theorem 38 and the results by Bhargawa and Shankar in [6, 5] which show that a positive proportion of $E/\mathbb{Q}$ have trivial $p$-Selmer group over $\mathbb{Q}$ when $p = 3$ or 5. The restriction on the Galois representation is negligible. □

For all practical purposes, we can consider the calculation of $\operatorname{ord}_{s=1} L(E, \chi, s)$, which leads to a proven upper bound for $r_K = \operatorname{rk} E(K)$, the calculation of $r_{\mathbb{Q}}$ and $Ш_{\mathbb{Q}}$ as easy. So is the determination of $D_{K/\mathbb{Q}}$. As a consequence, in most cases we can calculate $M$ effectively from our methods without having to do any point search of descent for $E$ over $K$.

### 7.1.1 Examples

All elliptic curves in this list of examples are given by their Cremona label as in [15] and provided with a link to the lmfdb [28]. The computational results are obtained using SageMath [43]. The $p$-primary parts of Tate-Shafarevich groups over $\mathbb{Q}$ are proven correct by the methods used in [42].

The conductor of a cyclic extensions $K/\mathbb{Q}$ of degree $p$ is the smallest $m$ such that $K \subset \mathbb{Q}(\zeta_m)$. If $m$ is prime, then there is a unique such $K$ in $\mathbb{Q}(\zeta_m)$, and hence we only need to specify $m$ to give $K$.

For a character $\chi$ of $K/\mathbb{Q}$, seen as a Dirichlet character modulo $m$, we define the algebraic $L$-value

$$\mathcal{L}(E, \chi) = \sum_{a \bmod m} \bar{\chi}(a) \left[\tfrac{a}{m}\right]^{\chi(-1)} \in \mathbb{Q}(\chi) = \mathbb{Q}(\zeta_p)$$

where $[\cdot]^{\pm}$ is the modular symbol attached to $E$, normalised as in [48] and computed as in [50]. Since $\mathcal{L}(E, \chi)$ is a non-zero multiple of $L(E, \chi, 1)$, the vanishing of $\mathcal{L}(E, \chi)$ indicates that the rank of $E(K)$ is larger than the rank of $E(\mathbb{Q})$. Conversely, if $\mathcal{L}(E, \chi) \neq 0$, then $E(K) = E(\mathbb{Q})$ under our assumption that $E(\mathbb{Q})[p] = 0$.

**Example A)** Let $E$ be the elliptic curve with Cremona label 67a1 and let $K$ be the cyclic field of degree $p = 7$ and conductor 29. The curve has rank 0 over $\mathbb{Q}$ and $\operatorname{coker} \alpha = D^{\vee}_{K/\mathbb{Q}}$ has dimension 1 as the number of points in $\tilde{E}(\mathbb{F}_{29})$ is divisible by 7. Calculating $\mathcal{L}(E, \chi) \neq 0$ for a non-trivial character of $K$, proves that the rank over $K$ is still 0. Therefore $M = 0$ in this case. However, since $H^1(G, M) = 0$, but $\operatorname{coker} \alpha \neq 0$, we have shown that $Ш_K$ is non-trivial. In fact, the BSD conjecture over $K$ is equivalent to $Ш(E/K)$ having $7^2 \cdot 13^2$ elements. In our example, the space of $Ш_K$ fixed by $G$ is 1-dimensional.

**Example B)** Similar to the previous example, we have a case with $M = \mathbb{Z}_p$, yet $Ш_K \neq 0$. Take $E$ to be the curve 37a1 of rank 1 over $\mathbb{Q}$ and $K$ to be the quintic field of conductor 211 and $p = 5$. Again $D^{\vee}_{K/\mathbb{Q}}$ is of dimension 1 as $E(\mathbb{F}_{211})$ is cyclic of order $5^2 \cdot 3^2$ However, the generator $P$ of $E(\mathbb{Q})$ reduces to a point of order 45 modulo 211. This shows that $\operatorname{coker} \alpha \neq 0$. This together with $\mathcal{L}(E, \chi) \neq 0$ allows us to conclude that $\operatorname{coker} \eta = Ш^G_K$ has dimension at least 1. BSD says that $Ш(E/K)$ is of order $5^4$.

**Example C)** The curve 681b3 has rank 0 over $\mathbb{Q}$, but $Ш_{\mathbb{Q}} \neq 0$ for $p = 3$. Consider the cubic extension $K$ of conductor 19. Since $\mathcal{L}(E, \chi) = 0$, the rank grows in this extension, which means that $M$ is a power of $A$. However $\operatorname{coker} \alpha$ is trivial. This implies that the capitulation kernel $C_{K/\mathbb{Q}}$

is non-trivial. A 2-descent reveals that $E(K)$ has rank 2, which shows that $M \cong A$. Therefore only a 1-dimensional subspace of $Ш_{\mathbb{Q}}$ capitulates in $K/\mathbb{Q}$. Hence $Ш_K$ is still non-trivial; it is of order 9 according to BSD.

**Example D)** Consider $p = 5$, the curve 21a1 over the quintic extension $K$ of conductor 41. The rank is 0 over $\mathbb{Q}$, but $\mathcal{L}(E, \chi) = 0$ proves that the rank is positive over $K$. Since $Ш_{\mathbb{Q}}$ is trivial, but $\operatorname{coker} \alpha$ has dimension 1, we see that $M$ cannot contain more than one copy of $A$. Therefore $\operatorname{rk} E(K) = 2$. Since the cokernel of $\eta$ must be trivial, we find that $Ш_K^G = 0$ and hence that $Ш_K = 0$ as $G$ is a $p$-group. Conjecturally $Ш(E/K)$ is trivial.

A similar argument works for $p = 7$, the curve 38b1 over the extension of conductor 71.

**Example E)** The curve 89a1 has rank 1 over $\mathbb{Q}$. As the algebraic $L$-value $\mathcal{L}(E, \chi) = 0$ for the degree 11 extension of conductor 23, i.e., $K = \mathbb{Q}(\zeta_{23})^+$, the rank must grow. However $\alpha$ is surjective and $Ш_{\mathbb{Q}} = 0$. Therefore $H^1(G, M) = 0$, which implies that $M = \mathbb{Z}_p[G]$ is free. We can also conclude that $Ш_K = 0$.

For rank 1 curves with rank growth, it is very frequent that $M$ is free.

**Example F)** The curve 130a3 has rank 1 over $\mathbb{Q}$ and $\mathcal{L}(E, \chi) = 0$ for the cubic field $K = \mathbb{Q}(\alpha)$ of conductor 43 with $\alpha^3 + \alpha^2 - 14\,\alpha + 8 = 0$. The analytic rank tells us that $r_K = 3$ and we know that $Ш_{\mathbb{Q}}$ is trivial. However, $\operatorname{coker} \alpha$ has $p = 3$ elements. Hence $M$ contains at most one copy of $A$, but we cannot decide at this point whether $M$ is $\mathbb{Z}_p \oplus A$ or $\mathbb{Z}_p[G]$. In this case, we actually calculate the points in $E(K)$. One finds that there is a point $P \in E(K)$ with $x$-coordinate $\frac{1}{16}\,(-48 - 132\,\alpha + 33\,\alpha^2)$. The usual saturation shows that $\mathbb{Z}_p[G]\,P$ has index $p$ in $M$, which already tells us that $M \cong \mathbb{Z}_p \oplus A$. Alternatively, one can calculate the matrix of how a non-trivial element $\sigma \in G$ acts on the saturated group and calculate the cohomology group $H^1(G, M)$ directly.

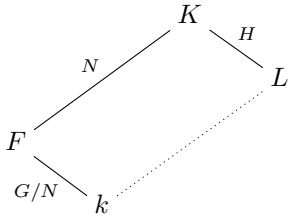
**Example G)** The most interesting example is the curve 5692a1 with $K$ the cubic extension of conductor 9, which already appears in [49]. The curve has rank 2 over $\mathbb{Q}$, generated by $P_1 = (0, 5)$ and $(2, -1)$. The group $D_2$ is cyclic of order 3 and the image of the norm map identifies with the points of good reduction as the reduction type is IV. As the Tamagawa number at the only other bad prime is coprime to 3, the only other non-trivial $D_v$ is for $v = 3$. Here the reduction is good ordinary with 6 elements in the reduction $\tilde{E}(\mathbb{F}_3)$. We are in the situation of Proposition 10. The map $\tilde{E}(\mathbb{F}_3)[3] \to \hat{E}(3\mathbb{Z}_3)/\hat{E}(9\mathbb{Z}_3)$ can shown to be surjective, which implies that $D_3$ is cyclic of order 3 as it identifies with $\check{E}(\mathbb{F}_3)/3\tilde{E}(\mathbb{F}_3)$.

Since $P_1 - P_2$ has good reduction at 2 and the reduction at 3 is of order 2, the map $E(\mathbb{Q})\hat{\otimes}\mathbb{Z}_3 \to D_{K/\mathbb{Q}}$ is not surjective. We conclude that $\operatorname{coker} \alpha$ is of dimension 1. This only reveals that $M$ contains at most one copy of $A$. Since the rank of $M$ can be determined to be 6, we can already conclude that $M$ must contain at least one factor of $\mathbb{Z}_3[G]$.

To complete the calculation and prove that $M \cong \mathbb{Z}_3 \oplus A \oplus \mathbb{Z}_3[G]$ seems to require once more to the calculation of $M$ and the action of $G$ explicitly on it. With the explicit basis in [49], this is not difficult to do.

## 7.2 Dihedral group

We suppose now that $G \cong D_p$ is the dihedral group of order $2p$. The $p$-Sylow subgroup is $N$ and pick one subgroup $H$ of order 2. There is a unique non-trivial Brauer relation $\Theta = \Theta_2 = 1 - 2 \cdot H - N + 2 \cdot G$. Write $F$ for the field fixed by $N$ and $L$ for the field fixed by our chosen $H$.




Recall the classification of indecomposable $\mathbb{Z}_p[G]$-lattices: $\mathbb{Z}_p$, $\breve{\mathbb{Z}}_p := \mathbb{Z}_p\{1\}$, $A$, $\breve{A} := A\{1\}$, $B$ and $\breve{B} := B\{1\}$. From Theorem 23 we know that the following will determine $M = E(K)\,\hat{\otimes}\,\mathbb{Z}_p$

completely:

- $M \otimes \mathbb{Q}$ as a $\mathbb{Q}[G]$-module;
- $H^1(N, M)$ as a $\mathbb{F}_p[G/N]$-module;
- $s(M) = \operatorname{ord}_p(\mathcal{C}_\Theta(M))$.

The last entry in the list above can be replaced by $\dim_{\mathbb{F}_p} \iota(M)$. However, note that these invariants are not all easy to determine. The ranks could, at least conjecturally, be determined using the order of vanishing of twisted $L$-functions. The cohomological term $H^1(N, M)$ appears in the exact sequence (6). Finally, both $s(M)$ and $\iota(M)$ seem hard to evaluate without actually calculating $M$, except for the parity of $s(M)$ by Corollary 34.

In the (frequent) case that the rank is small, we need less information to determine $M$.

**Proposition 41.**

- If $\operatorname{rk} E(F) = 0$, then $M$ is determined by $H^1(N, M)$ as a $\mathbb{F}_p[G/N]$-module.
- If $\operatorname{rk} E(F) = 1$, then $M$ is determined by $H^1(N, M)$ as a $\mathbb{F}_p[G/N]$-module, $\operatorname{rk} E(k)$ and the parity of $s(M)$.

*Proof.* We use Table 1. If $r_F = 0$, then $M$ is a direct sum of copies of $A$ and $\check{A}$. Since they have distinct $H^1(N, M)$, that group is enough to determine $M$.

If $r_F = 1$, then $M$ is a direct sum of copies of $A$, $\check{A}$ and one copy of either $\mathbb{Z}_p$, $\check{\mathbb{Z}}_p$, $B$ or $\check{B}$. Again $H^1(N, M)$ determines the number of $A$ and $\check{A}$ that appear. If $r_k = 1$, then there is an extra copy of either $\mathbb{Z}_p$ or $B$. Since $s(\mathbb{Z}_p) \equiv 1$ and $s(B) \equiv 0 \pmod 2$, the parity of $s(M)$ suffices to determine $M$, If $r_k = 0$, the same argument works with $\check{\mathbb{Z}}_p$ and $\check{B}$. □

As $F/k$ is a quadratic extension, there is a quadratic twist $\check{E}/k$ of $E$ associated to $F/k$. Since $p$ is odd, $\check{E}$ also satisfies Assumption 2. Many invariants that we might have to calculate over $F$ can be calculated over $k$ instead using $\check{E}$. First of all $r_F = \operatorname{rk} E(F) = \operatorname{rk} E(k) + \operatorname{rk} \check{E}(k)$. Since $p$ is odd, we also have $Ш_F = Ш_k \oplus \check{Ш}_k$, where $\check{Ш}_k = Ш(\check{E}/k)[p^\infty]$. Therefore, we also have $C_{K/F} = C_{K/k} \oplus \check{C}_{K/k}$ with $\check{C}_{K/k}$ the capitulation kernel for $\check{E}$.

**Lemma 42.** *$H^1(N, M)$ as a $G/N$-module is determined by the abelian groups $H^1(G, M)$ and $H^1(G, \check{M})$ where $\check{M}$ is $\check{E}(K) \hat{\otimes} \mathbb{Z}_p = M \otimes \check{\mathbb{Z}}_p$.*

*Proof.* The $\mathbb{F}_p$-vector space $H^1(N, M)$ splits into a $+1$ eigenspace and a $-1$ eigenspace with respect to the action by $G/N$. The $+1$ eigenspace is isomorphic to the $G/N$-invariants of $H^1(N, M)$, which is isomorphic to $H^1(G, M)$ by the restriction map. Twisting by $\check{\mathbb{Z}}_p$, we obtain that the $-1$ eigenspace is $H^1(G, \check{M})$. □

**Proposition 43.** *$M = E(K) \hat{\otimes} \mathbb{Z}_p$ is completely determined by*

- *$r_k = \operatorname{rk} E(k)$, $\check{r}_k = \operatorname{rk} \check{E}(k)$ and $\operatorname{rk} E(L)$;*
- *$H^1(G, M)$ and $H^1(G, \check{M})$*
- *$s(M) = \operatorname{ord}_p(\mathcal{C}_\Theta(M))$.*

*Proof.* The structure of $M \otimes \mathbb{Q}$ as a $\mathbb{Q}_p[G]$ is determined by $r_k$, $\operatorname{rk} E(F) = r_k + \check{r}_k$ and $\operatorname{rk} E(L)$. Together with the previous lemma, this theorem is now a reformulation of Theorem 23. □

*Proof of Theorem 1.* The assumptions in Theorem 1, imply that $H^1(G, M)$ is trivial as $Ш_k$ and $D_{K/k}$ are trivial as there are no places with $p \mid e_v$ and all places with $p \mid f_v$ have $p \nmid c_v$. Also $H^1(G, \check{M})$ is trivial for the same reasoning applied to $\check{E}$. This implies that neither $A$ nor $\check{A}$ can appear in $M$. Then $r_k + \check{r}_k \leqslant 1$, implies that $M$ is isomorphic to a single copy of of $\mathbb{Z}_p$, $\check{\mathbb{Z}}_p$, $B$ or $\check{B}$, unless $r_k = \check{r}_k = 0$, in which case $M = 0$. If $r_k = 1$, it is either $\mathbb{Z}_p$ or $B$, and if $\check{r}_k = 1$, it is $\check{\mathbb{Z}}_p$ or $\check{B}$. The parity of $s(M)$ distinguishes the two possibilities in both cases, and that parity can be calculated using only local information for $E$ over $K$. □

**Lemma 44.** Suppose that $p > 3$ and that no place of additive reduction ramifies in $K/k$. Let $v_1$ be the number of places in $k$ such that $E$ has split multiplicative reduction and such that $K$ contains a single ramified place above $v$. Let $v_2$ be the number of places in $k$ such that $E$ has non-split multiplicative reduction and there is a unique place above $v$ with ramification index $p$. Then $s(M) \equiv v_1 + v_2 \pmod 2$. In particular, $s(M)$ is even if there is no place of bad reduction that ramifies in $K/F$.

*Proof.* By Corollary 34, we need to calculate the contribution at each bad place $v$ in $k$ to the $p$-adic valuation of $C(E/K)/C(E/F)$.

For additive places the contribution is an even power of $p$: Since $p > 3$, the Tamagawa number is not divisible by $p$, and since $K/k$ is unramified at this place the quantity $u_v$ does no change. Hence local term is $u_v^{p-1}$ or 1 depending whether there are $p$ places above each place in $F$ or only 1.

For multiplicative places, this is calculated in the table in Section 3.1 in [3]. □

An interesting application connects our investigation to the discussion of the "minimalistic conjecture" in [14]. Recall that we are still assuming that all Tate-Shafarevich groups have finite $p$-primary parts.

**Theorem 45.** Let $K/\mathbb{Q}$ be a dihedral extension with $G = D_p$ for a prime $p > 3$ such that $p \nmid e_p$. Suppose that a proportion of at least 66.25% of elliptic curves $E/\mathbb{Q}$ (when ordered by height) satisfy $Ш(E/F)[p] = 0$. Then there is a positive proportion of elliptic curves $E/\mathbb{Q}$, when ordered by height, such that $E(K) \hat{\otimes} \mathbb{Z}_p$ is one of the following five $\mathbb{Z}_p[G]$-lattice:

$$0, \qquad B, \qquad \breve{B}, \qquad \mathbb{Z}_p \oplus \breve{\mathbb{Z}}_p, \qquad \text{and} \qquad B \oplus \breve{B} \cong \mathbb{Z}_p[G].$$

The rank of $E(\mathbb{Q})$ and of the quadratic twist $\breve{E}(\mathbb{Q})$ determines the case, except for the last two cases.

There are conjectures about the proportion of elliptic curves with $p \nmid Ш(E/\mathbb{Q})$ and $p \nmid Ш(E/F)$ going back to Delaunay [18] and [39]. It is believed that this is a large majority of curves for all $p$, but that a small positive proportion has non-trivial $Ш_F$. We cannot conclude that the most frequent $\mathbb{Z}_p[G]$-module structures among the curves with non-trivial $Ш_{\mathbb{Q}}$ are the same as in the above theorem, but this could be true. One would have to understand the frequency with which non-trivial elements in Tate-Shafarevich groups capitulate in $K$.

When tensoring the displayed formula in the theorem by $\mathbb{C}_p$, one falls onto the "minimalistic conjecture", except in the case that $M \cong B \oplus \breve{B} = \mathbb{Z}_p[G]$. With our methods we cannot determine that the case $\mathbb{Z}_p \oplus \breve{\mathbb{Z}}_p$ is more frequent than $\mathbb{Z}_p[G]$. Apart from that, the theorem is good evidence for the minimalistic conjecture.

*Proof.* By [5] a positive proportion of elliptic curve have rank 0 or 1. More precisely, consider the set of $(I, J)$ corresponding to elliptic curve in

$$\left\{ E/\mathbb{Q} \;\middle|\; (N, \Delta_K) = 1,\ \ell^p \nmid \Delta_E \text{ for all primes } \ell, p \nmid \#\tilde{E}(\mathbb{F}_v) \text{ for all prime } v \in S_{\mathrm{r}} \right\}$$

where $S_{\mathrm{r}}$ is the set of all places $v$ such that $p \mid e_v$. This is a "large family" in the sense of [5]. Therefore more than 83.75% of such elliptic curves have rank either 0 or 1. Hence at least 67.5% of all curves in the set have rank smaller than 2 and their twist corresponding to the quadratic extension in $K/\mathbb{Q}$ also have rank smaller than 2. A positive proportion of curves in the above set will now have rank either 0 or 1 for $E$ and its twist and trivial $Ш_{\mathbb{Q}}$ and $\breve{Ш}_{\mathbb{Q}}$ because $67.5+2\cdot 66.25 = 200$. We may exclude the elliptic curves with a rational $p$-torsion points without harming this.

Let $E$ be a curve in that set. Since $\ell^p \nmid \Delta$, we see that $c_\ell$ cannot be divisible by $p$. Together with the condition that no bad prime ramifies, that $p \nmid e_p$ and the condition $p \nmid \#\tilde{E}(\mathbb{F}_v)$ for all $v \in S_{\mathrm{r}}$, we deduce that $D_{K/\mathbb{Q}} = 0$ by Proposition 30. Together with $Ш_{\mathbb{Q}} = \breve{Ш}_{\mathbb{Q}} = 0$, we know now

that $H^1(G,M)=0$. Therefore $M$ is a direct sum $\mathbb{Z}_p^a \oplus \breve{\mathbb{Z}}_p^b \oplus B^e \oplus \breve{B}^f$ with $r=\operatorname{rk} E(\mathbb{Q})=a+e\leqslant 1$ and $\breve{r}=\operatorname{rk}\breve{E}(\mathbb{Q})=b+f\leqslant 1$.

By Lemma 44, the quantity $a+b$ must be even as we are in the case that no prime of bad reduction ramified in $K/\mathbb{Q}$.

If $r=\breve{r}=0$, then $M$ must be 0. If $r=1$, but $\breve{r}=0$, then $b=f=0$, which implies that $a=0$ since $a+b$ must be even, and hence $e=1$. Similar if $r=0$ and $\breve{r}=1$, we get $a=b=e=0$ and $f=1$.

Finally, if $r=1$ and $\breve{r}=1$, then $a+e=1$ and $b+f=1$ and $a+b$ is even. This leads to two possibilities, namely $M\cong\mathbb{Z}_p\oplus\breve{\mathbb{Z}}_p$ or $M\cong B\oplus\breve{B}\cong\mathbb{Z}_p[G]$. □

The four cases can also be determined by root numbers if one admits the parity conjectures. These root numbers can be calculated under our assumption (Theorem 2.15 in [14] as done in their Example 4.11): If $\Delta_F$ is the fundamental discriminant of $F$, then the root number of $E$ twisted by any of the irreducible 2-dimensional $\mathbb{C}[G]$-modules is $z=\operatorname{sign}(\Delta_F)\cdot\left(\Delta_F/N\right)$ where the second factor is the Jacobi symbol. The root number for $E$ twisted by the non-trivial quadratic character is $z$ times the root number of $E/\mathbb{Q}$. The fact that the product of the three root numbers is 1 is now equivalent to the result in Lemma 44 under the parity conjecture.

## 7.3 Examples

For the following examples, we will always take the same $D_3$-extension. Let $L$ be the field generated by $\alpha$ with $\alpha^3+2\alpha-2=0$ and let $K$ be its Galois closure. The quadratic field inside $K$ is $F=\mathbb{Q}\left(\sqrt{-35}\right)$.

There is a unique ramified prime above 2 in $K$ has ramification index 3. Above 5 and 7 there are three primes with ramification index 2. The prime 3 is unramified with residue degree 3.

Let

$$M=\mathbb{Z}_p{}^a\oplus\breve{\mathbb{Z}}_p^b\oplus A^c\oplus\breve{A}^d\oplus B^e\oplus\breve{B}^f$$

and we try to determine the unknown $a,b,c,d,e,f$ from $r_{\mathbb{Q}}=a+e$, $r_F=a+e+b+f$, $r_L=a+e+\frac{p-1}{2}(c+d+e+f)$, $a+b-c-d\equiv\operatorname{ord}_p(C(E/K)/C(E/F))\pmod 2$, $H^1(N,M)=\mathbb{F}_p^c\oplus\breve{\mathbb{F}}_p^d$.

**Example H)** We take the curve 82a1 whose rank over $\mathbb{Q}$ is 1 and it is also 1 over $F$ as the twist $\breve{E}$ has rank 0. Therefore $b=f=0$. For all places $v\neq 2$, Proposition 13 implies that $D_v=0$. Let $\mathfrak{p}=(2)$ be the prime above 2 in $F$. We can determine $D_{\mathfrak{p}}$ for the extension $K/F$ using Proposition 9 as $K/F$ is totally ramified at $\mathfrak{p}$ and $E$ has split multiplicative reduction at this place. The quantity $u$ turns out to be odd and hence $D_{\mathfrak{p}}$ is cyclic of order 3. However the rational point $P=(0,0)\in E(F)$ reduces to a non-singular point that is not in the formal group. Therefore $\operatorname{coker}(\alpha_{K/F})$ is trivial. It follows that $\alpha$ for $K/\mathbb{Q}$ is also surjective.

Since $Ш_{\mathbb{Q}}$ and $\breve{Ш}_{\mathbb{Q}}$ are trivial, we conclude that $c=d=0$. We are left with two possibilities, either $\mathbb{Z}_p$ or $B$. However Corollary 34 can be used now to show that $a$ is odd, since $C(E/K)/C(E/F)=3$.

Therefore $M\cong\mathbb{Z}_p$ and we obtained this information with local information and information about $E$ and $\breve{E}$ over $\mathbb{Q}$ only. For this particular curve it is not much effort to verify that $r_L=1$ with a 2-descent, which confirms this result.

**Example I)** The next curve, we take is 14a3 which has rank 0 over $\mathbb{Q}$, but rank 1 over $F$. Again $D_{K/\mathbb{Q}}$ is reduced to $D_2$. Over $F$, the curve has split multiplicative reduction with Tamagawa number 18. As in the above example $D_{\mathfrak{p}}$ is cyclic of order 3, but this time the rational points map trivially to $D_{\mathfrak{p}}$. Therefore $\operatorname{coker}(\alpha_{K/F})$ is cyclic of order 3. The same argument works for the twisted curve $\breve{E}$ over $\mathbb{Q}$, showing that $\operatorname{coker}(\alpha_{K/F})$ is isomorphic to $\breve{\mathbb{F}}_3$ as a $G/N$-module. Since the Tate-Shafarevich groups are trivial again, we know that $H^1(N,M)$ is either trivial or equal to $\breve{F}_3$.

This implies that $c=0$ and $d\leqslant 1$. The regulator constant yields $b\not\equiv d\pmod 2$. We now have two possibilities left $d=1$ (and then $a=c=e=f=0$ and $f=1$) or $d=0$ (and then $b=1$ and $a=c=e=f=0$); so either $M\cong\breve{A}\oplus\breve{B}$ or $M\cong\breve{\mathbb{Z}}_p$. The fact that the $L$-function of $E$

twisted with the irreducible representation $\rho$ does not vanish at $s = 1$ or, directly, a 2-descent over $L$ confirms that $M \cong \breve{\mathbb{Z}}_p$.

As a consequence, $\mathrm{coker}(\alpha_{K/F})$ having dimension 1 now implies that $Ш_K \neq 0$. We expect $Ш(E/K)$ to have 9 elements.

**Example J)** The curve 322b1 has rank 0 over $F$ and hence $a = b = e = f = 0$. The regulator constant tells us that $c \not\equiv d \pmod 2$. Once again $\mathrm{coker}(\alpha_{K/F}) = D_{K/F} = \breve{\mathbb{F}}_p$ as a $G/N$-module very much like in the previous example as the reduction at 2 is once more non-split multiplicative. Therefore $d \leqslant 1$ and $c = 0$. We conclude that $M \cong \breve{A}$ without having to use any $L$-values or 2-descents.

**Example K)** The situation is very similar for the curve 158e1 has also rank 0 over $F$, but this time $\mathrm{coker}(\alpha_{K/F}) \cong \mathbb{F}_p$ as a $G/N$-module since the reduction at 2 is split multiplicative. The argument as above will show that $M \cong A$. The difference between the two cases is that here $E(L) \oplus \tau E(L)$ will be equal to $E(K)$ while in the previous example it has index $p$. This can be checked by calculating the groups directly.

**Example L)** Finally, let us consider the curves 37a1 and the curve 57a1. Both have rank 1 over $\mathbb{Q}$ and rank 2 over $F$ and all Tate-Shafarevich groups in sight are trivial. For both curves the map $\alpha$ is surjective, which means that $H^1(N, M)$ is trivial, and all bad places are unramified, which implies that $s(M)$ is even. Therefore we are in the situation in Theorem 45 where we had two options that we could not distinguish. However determining the group $E(L)$ in both cases, reveals that for the curve 37a1, we have $M = \mathbb{Z}_p \oplus \breve{\mathbb{Z}}_p$, while for the curve 57a1 it is $M = B \oplus \breve{B}$.

Examples of $M \cong B$ or $M \cong \breve{B}$ can be found by Theorem 45 or explicitly in [13]. More details for the above an verifications using explicit points on $E(K)$ are done in [45].

# References


[1] Alex Bartel, *Large Selmer groups over number fields*, Math. Proc. Cambridge Philos. Soc. **148** (2010), no. 1, 73–86.

[2] ———, *On Brauer-Kuroda type relations of S-class numbers in dihedral extensions*, J. Reine Angew. Math. **668** (2012), 211–244.

[3] ———, *Elliptic curves with p-Selmer growth for all p*, Q. J. Math. **64** (2013), no. 4, 947–954.

[4] Alex Bartel and Bart de Smit, *Index formulae for integral Galois modules*, J. Lond. Math. Soc. (2) **88** (2013), no. 3, 845–859.

[5] Manjul Bhargava and Arul Shankar, *The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1*, 2013, `https://arxiv.org/abs/1312.7859`.

[6] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[7] Matthew Bisatt and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer conjecture and Schur indices*, Bull. Lond. Math. Soc. **50** (2018), no. 6, 1027–1034.

[8] Werner Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, Exp. Math. **20** (2011), no. 4, 426–456. MR 2859900

[9] Werner Bley and Daniel Macias Castillo, *Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions, III*, Math. Proc. Cambridge Philos. Soc. **173** (2022), no. 2, 431–456.

[10] Julio Brau, *Selmer groups of elliptic curves in degree p extensions*, 2014, `https://arxiv.org/abs/1401.3304`.

[11] David Burns and Daniel Macias Castillo, *On refined conjectures of Birch and Swinnerton-Dyer type for Hasse-Weil-Artin L-series*, 2021, `https://arxiv.org/abs/1909.03959`.

[12] David Burns, Daniel Macias Castillo, and Christian Wuthrich, *On the Galois structure of Selmer groups*, Int. Math. Res. Not. IMRN (2015), no. 22, 11909–11933.

[13] ———, *On Mordell-Weil groups and congruences between derivatives of twisted Hasse-Weil L-functions*, J. Reine Angew. Math. **734** (2017), 187–228.

[14] Lilybelle Cowland Kellock and Vladimir Dokchitser, *Root numbers and parity phenomena*, 2023, `https://arxiv.org/abs/2303.07883`.

[15] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[16] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc., New York, 1981, With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[17] Chantal David, Jack Fearnley, and Hershy Kisilevsky, *Vanishing of L-functions of elliptic curves over number fields*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 247–259.

[18] Christophe Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196.

[19] Fritz-Erdmann Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Hansischen Univ. **13** (1940), 357–412.

[20] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71.

[21] ———, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596.

[22] Vladimir Dokchitser, Robert Evans, and Hanneke Wiersema, *On a BSD-type formula for L-values of Artin twists of elliptic curves*, J. Reine Angew. Math. **773** (2021), 199–230.

[23] Nils Ellerbrock and Andreas Nickel, *On formal groups and Tate cohomology in local fields*, Acta Arith. **182** (2018), no. 3, 285–299.

[24] Jack Fearnley, Hershy Kisilevsky, and Masato Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, J. Lond. Math. Soc. (2) **86** (2012), no. 2, 539–557.

[25] Jean Gillibert and Pierre Gillibert, *On the splitting of the Kummer exact sequence*, Publications mathématiques de Besançon. Algèbre et théorie des nombres (2019), no. 2, 19–27.

[26] Ralph Greenberg, *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **211** (2011), no. 992, vi+185.

[27] Myrna Pike Lee, *Integral representations of dihedral groups of order* $2p$, Trans. Amer. Math. Soc. **110** (1964), 213–231.

[28] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2023.

[29] Jonathan Lubin and Michael I. Rosen, *The norm map for ordinary abelian varieties*, J. Algebra **52** (1978), no. 1, 236–240.

[30] Daniel Macias Castillo, *On the Krull-Schmidt decomposition of Mordell-Weil groups*, Tokyo J. Math. **40** (2017), no. 2, 353–378.

[31] Kazuo Matsuno, *Elliptic curves with large Tate-Shafarevich groups over a number field*, Math. Res. Lett. **16** (2009), no. 3, 449–461.

[32] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.

[33] ———, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. J. **143** (2008), no. 3, 437–461.

[34] ———, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616, With an appendix by Michael Larsen.

[35] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.

[36] Yi Ouyang and Jianfeng Xie, *The growth of Tate-Shafarevich groups in cyclic extensions*, Compos. Math. **158** (2022), no. 10, 2014–2032.

[37] Martin Prickett, *Saturation of Mordell-Weil Groups of Elliptic Curves over Number Fields*, Ph.D. thesis, University of Nottingham, 2004, `https://eprints.nottingham.ac.uk/10052/`.

[38] Lena Chang Pu, *Integral representations of non-abelian groups of order pq*, Michigan Math. J. **12** (1965), 231–246.

[39] Patricia L. Quattrini, *On the distribution of analytic $\sqrt{|Ш|}$ values on quadratic twists of elliptic curves*, Experiment. Math. **15** (2006), no. 3, 355–365.

[40] Irving Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. **8** (1957), 142–146.

[41] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[42] William Stein and Christian Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. **82** (2013), no. 283, 1757–1792.

[43] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.8)*, 2023, `https://www.sagemath.org`.

[44] Alex Torzewski, *Regulator constants of integral representations of finite groups*, Math. Proc. Cambridge Philos. Soc. **168** (2020), no. 1, 75–117.

[45] Thomas Vavasour, *Galois Theory of Mordell–Weil Groups*, Ph.D. thesis, University of Nottingham, 2018.

[46] Kęstutis Česnavičius, *p-Selmer growth in extensions of degree p*, J. Lond. Math. Soc. (2) **95** (2017), no. 3, 833–852.

[47] Michel Waldschmidt, *On the p-adic closure of a subgroup of rational points on an Abelian variety*, Afr. Mat. **22** (2011), no. 1, 79–89.

[48] Hanneke Wiersema and Christian Wuthrich, *Integrality of twisted L-values of elliptic curves*, `https://arxiv.org/abs/2004.05492`, 2020.

[49] Christian Wuthrich, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (2007), no. 1, 83–108.

[50] ———, *Numerical modular symbols for elliptic curves*, Math. Comp. **87** (2018), no. 313, 2393–2423.

[51] A. V. Yakovlev, *Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup*, An. Ştiinţ. Univ. Ovidius Constanţa Ser. Mat. **4** (1996), no. 2, 206–221, Representation theory of groups, algebras, and orders (Constanţa, 1995).