University of Nottingham



School of Mathematical Sciences

Kolyvagin Derivatives of Modular Points on Elliptic Curves

Richard Hatton

A thesis submitted to the University of Nottingham for the degree of

Doctor of Philosophy

5th June 2020

Abstract

Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves. We can construct modular points derived from A via the modular parametrisation of E. With certain assumptions we can show that these points are of infinite order and are not divisible by a given prime p. We can also show that the group generated by these points is isomorphic to a representation of the projective general linear group.

We further investigate this representation, initially looking at the modular representation theory associated to it. We classify all the $\mathbb{F}_p$-submodules and look at their group cohomology with respect to subgroups of the projective general linear group. We then look at the integral representation theory associated to the representation. We look at some of the $\mathbb{Z}_p$-lattices and apply the modular representation theory to determine the size of their group cohomologies.

We finally look at applying the representation theory to the group generated by the modular points. In particular, using Kolyvagin's construction of derivative classes, we find elements in certain Shafarevich-Tate groups of prime power order.

Acknowledgements

I would first like to thank Chris Wuthrich who has provided me with invaluable advice and direction throughout my studies, which have helped me become a better mathematician. All this would not have been possible without him.

I would also like to thank all the members of the Number Theory group at the University of Nottingham, in particular Fredrik, Nikos and Sergey for their advice along this journey. It is great to know that I could turn to them if I was struggling. I would also like to thank Andreea for her continued help and support throughout my time and Michalis for being so welcoming in my first year. I am also grateful to the School of Mathematical Sciences for making all the resources available to me during this time.

Also, I am thankful to the friends I have made during this time in the department for making this journey even more enjoyable. Special mention goes to the maths football group who made Friday afternoons enjoyable even when my research wasn't going well.

I would like to thank my family and friends from home who have put up with and supported me during this time. In particular, my mum and dad who I hope will enjoy reading this thesis.

Finally, I would like to thank the EPSRC, whose funding enabled me to conduct this research.

Contents

1 INTRODUCTION 1

1.1 Notation . . . 9

1.1.1 Arithmetic Notation . . . 9

1.1.2 Algebraic Notation . . . 12

2 BACKGROUND 15

2.1 Elliptic Curves and Selmer Groups . . . 17

2.2 Heegner Points . . . 21

2.2.1 Construction of the Derivative Classes . . . 24

2.2.2 Tate Local Duality . . . 34

2.2.3 Calculation of the Selmer Group . . . 37

2.3 Self Points . . . 47

3 REPRESENTATION THEORY OF $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ 58

3.1 Group Properties of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ . . . 61

3.2 Cohomological Results . . . 68

3.3 Modular Representation Theory of $\mathcal{G}_n$ . . . 77

3.3.1 Module Structure . . . 77

3.3.2 Cohomology of $\mathbb{F}_p[\mathcal{G}_n]$-modules . . . 92

3.4 Representations of $\mathrm{PGL}_2(\mathbb{F}_p)$ . . . 115

3.5 Representations of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ . . . 117

3.6 The Cohomology of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices . . . 130

3.6.1 The $\mathcal{G}_n$-Cohomology . . . 132

3.6.2 The $\mathcal{A}_n$-Cohomology . . . 135

3.6.3 The $N(\mathcal{A}_n)$-Cohomology . . . 138

3.6.4 The $\mathcal{B}_n$-Cohomology . . . 140

3.6.5 The $\mathcal{I}_n$-Cohomology . . . 142

3.6.6 The $\mathcal{P}_n$-Cohomology . . . 144

3.6.7 The $\mathcal{H}_n$-Cohomology . . . 145

3.6.8 The $\mathcal{D}_n$-Cohomology 149
3.6.9 The $N(\mathcal{D}_n)$-Cohomology 151

4 MODULAR POINTS ON ELLIPTIC CURVES 153
4.1 Modular Points on Elliptic Curves 156
4.2 Higher Modular Points 161
4.2.1 Multiplicative Case 161
4.2.2 Good Case 166
4.3 Derivatives 168
4.3.1 Field Extensions 170
4.3.2 Construction of Derivatives 176
4.4 Examples 185

Chapter 1

Introduction

Throughout this thesis, we are interested in a specific type of curve.

Definition. *An elliptic curve E over a field K is a smooth projective curve of genus 1 defined over K together with a distinguished K-rational point O.*

Let K be a number field, a finite field extension of $\mathbb{Q}$. We are interested in the structure of $E(K)$. An important starting point for this is the following.

Theorem (Mordell-Weil Theorem)**.** *Let E/K be an elliptic curve. Then there exists an $r \geq 0$, called the rank of E/K, such that*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

where $E(K)_{\text{tors}}$ is the finite subgroup of all torsion points in $E(K)$. In particular, $E(K)$ is finitely generated.

Therefore, to understand the structure of this group, we want to calculate the rank of the elliptic curve. For an integer $m \geq 1$, the quotient $E(K)/mE(K)$ is isomorphic to a subgroup of the m-th Selmer group, denoted $\text{Sel}^m(E/K)$ and whose defintion is provided in Definition 2.1.4. In particular, for certain primes p such that $E(K)[p] = 0$, the quotient group $E(K)/pE(K)$ has dimension as an $\mathbb{F}_p$-vector space equal to its rank. Therefore, the study of Selmer groups is important in the understanding of the rank of elliptic curves.

Kolyvagin and Wuthrich have both looked at bounding the size of Selmer groups. This involved the study of modular points on elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Due to the modularity theorem there exists a surjective morphism

$$\Phi_E : X_0(N_E) \to E$$

defined over $\mathbb{Q}$, known as the modular parametrisation attached to E, where $X_0(N_E)(\mathbb{C}) = \Gamma_0(N_E)\backslash\mathbb{H}^*$ is a modular curve and ∞ on $X_0(N_E)$ maps to the point of infinity on E. We will not look at the definition of $X_0(N_E)$ in this thesis, but for details on its construction, see [14]. There exists a subvariety $Y_0(N_E)$ of $X_0(N_E)$ which can be viewed as a moduli space of pairs (A, C) where A is an elliptic curve and C is a cyclic subgroup in A of order N_E.

Definition. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and let*

$$(A, C) \in Y_0(N_E)(K)$$

for some number field K. Then we define $\Phi_E(A, C) \in E(K)$ as a modular point.

Kolyvagin was able to use a specific type of modular point known as a Heegner point to prove the following.

Theorem (Kolyvagin)**.** *Let K be an imaginary quadratic field such that all primes dividing a fixed integer N_E are split. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $P_K \in E(K)$ be the trace of a certain Heegner point and suppose that P_K is of infinite order. Then:*

1. *The rank of $E(K)$ is 1.*
2. *The Shafarevich-Tate group of E/K is finite.*

In order to prove this, Kolyvagin used Heegner points to create cohomology classes to bound Selmer groups over K. In particular, the cohomology classes he created were shown to lie outside the Selmer group, hence bounding the Selmer group from above. He then showed that the Selmer group is generated by the image of $[P_K] \in E(K)/pE(K)$ under the Kummer map, which is defined in the notation, for a certain type of prime p such that $E(K)[p] = 0$. Hence, he showed that no element in the Selmer group is a lift of a non-trivial element of the Shafarevich-Tate group and hence the rank of $E(K)$ is equal to the dimension of $\mathrm{Sel}^p(E/K)$ as an $\mathbb{F}_p$-vector space.

Wuthrich then worked on an analogue system to Kolyvagin's work where he uses a type of modular point known as self points to create derivative classes. He then linked the group generated by the self points with the representation theory associated to the projective general linear group, as seen in Theorem 2.3.8 and Theorem 2.3.9. Using this link, unlike in Kolyvagin's case, he showed that the derivative classes created lie in the Selmer groups over certain fields and hence found lower bounds for these, as seen in Theorem 2.3.10.

We would like to follow Kolyvagin's construction of derivative classes to bound Selmer groups by extending the idea of self points to a generalised construction of modular point. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Define

$x_{A,C} := (A, C)$ where A is an elliptic curve and C is a cyclic subgroup in A of order N_E. Fixing $A/\mathbb{Q}$, we will denote $P_{A,C} := \Phi_E(x_{A,C}) \in E(\mathbb{Q}(C))$ where $\mathbb{Q}(C)$ is the field of definition of C. We denote the compositum of all such $\mathbb{Q}(C)$ as K_{N_E}. This is the smallest field K such that its absolute Galois group G_K acts by scalars on $A[N_E]$. This has Galois group $G_{N_E} := \mathrm{Gal}(K_{N_E}/\mathbb{Q})$ which can be identified as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N_E\mathbb{Z})$ via the mapping

$$\overline{\tau}_{\mathbb{Q},A,N_E} : G_{\mathbb{Q}} \to \mathrm{Aut}(A[N_E]) \cong \mathrm{GL}_2(\mathbb{Z}/N_E\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/N_E\mathbb{Z}).$$

In Kolyvagin's case, $\overline{\tau}_{\mathbb{Q},A,N_E}$ is far from surjective, however in the generic case, we will take it to be surjective. As in the work of both Kolyvagin and Wuthrich, we need to look at the divisibility of the modular points in $E(\mathbb{Q}(C))$ and understand the relationships between them. This will provide us with an understanding of the rank of the group generated by these points. Initially, we want to see when the modular points are of infinite order. We obtain the following result, which is Theorem 4.1.1.

Theorem. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $A/\mathbb{Q}$ be an elliptic curve such that the j invariant of A is not in $\frac{1}{2}\mathbb{Z}$ and the degree of any isogeny of A defined over $\mathbb{Q}$ is coprime to N_E. Then the modular points $P_{A,C}$ are of infinite order for all cyclic subgroups C of order N_E in A.*

From this, we can show that if p is a prime with specific conditions related to A and E, then $P_{A,C}$ is not divisible by p in $E(\mathbb{Q}(C))$ as seen in Proposition 4.1.5. We also see that there exist linear relations between the modular points. If $d \neq N_E$ is a divisor of N_E and B is a cyclic subgroup in A of order d, then

$$\sum_{C \supset B} P_{A,C} \in E(K_d) \text{ is torsion,}$$

where K_d is the smallest number field such that its absolute Galois group acts by scalars on $A[d]$, as seen in Proposition 4.1.3. This reduces the rank of the group generated by these points.

We then take a look at a specific case of creating higher modular points for a prime p of either good ordinary or multiplicative reduction with respect to E. Here, we will look at the case where p is a prime of good ordinary reduction. Let D be a cyclic subgroup in A of order p^{n+1} for a prime p and $n \geq 0$. We look

at the higher modular point coming from $(A/D, \psi(C))$ where $\psi : A \to A/D$ is the isogeny defined by D. We define $Q_{A,D} = \Phi_E(A/D, \psi(C)) \in E(\mathbb{Q}(C, D))$. Then the higher modular points form a trace-compatible system with

$$a_p(E) \cdot Q_{A,D} = \sum_{D' \supset D} Q_{A,D'}$$

where the sum is taken over the subgroups D' of A of order p^{n+2} containing D and $a_p(E)$ is the p-th Fourier coefficient for the modular form associated to the isogeny class of E. Using this, we can show that if $P_{A,C}$ is of infinite order, then we have created a tower of points which are also of infinite order. In particular, we show that the higher modular points generate a group of rank $p^{n+1} + p^n$ as seen in Proposition 4.2.3, and so if F_n defines the compositum of all such $\mathbb{Q}(C, D)$, where C and D intersect trivially as their orders are coprime, we have $F_n = K_{p^{n+1}N_E}$ and $\text{rank}(E(F_n)) \geq p^{n+1} + p^n$ by [20, Corollary 3.7]. Hence we are able to use this information to establish a link between the group generated by the higher modular points and the representation theory associated to the projective general linear group, as seen in Proposition 4.2.3.

If we let $\mathcal{G}_n := \text{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ for $n \geq 0$, we will see that we can relate the group generated by the higher modular points to certain $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in

$$V_n = \ker\left(\mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] \to \mathbb{Q}_p\right)$$

for p prime and $\mathcal{B}_n$ a Borel subgroup of $\mathcal{G}_n$. We can view

$$V_n = \left\{ f : \mathbb{P}^1_n \to \mathbb{Q}_p : \sum_C f(C) = 0 \right\}$$

where $\mathbb{P}^1_n := \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$. This contains the standard lattice

$$T_n = \ker\left(\mathbb{Z}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] \to \mathbb{Z}_p\right),$$

whose cohomology with respect to subgroups of $\mathcal{G}_n$ is easily understood. Hence, we take a look at the integral representation theory of $\mathcal{G}_n$ in Chapter 3 in order to further understand the $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in V_n. This will require understanding the modular representation theory associated to $\mathcal{G}_n$ as seen in section 3.3. In particular, we find all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\text{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ in Theorem 3.3.8 and

link them to the $\mathbb{Z}_p[\mathcal{G}_n]$-lattices we have found in section 3.5. They also help to calculate the cohomology of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to subgroups of $\mathcal{G}_n$, as seen in section 3.6, which we can apply to the modular points. In particular, we show the following, which is Theorem 3.6.20.

Theorem. *Let W be a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice of V_n such that $W^{\mathcal{B}_n} = T_n^{\mathcal{B}_n}$. Then $W \cong T_n$.*

We then generalise Wuthrich's work in [39] using the ideas of Kolyvagin in [24] in Chapter 4. We create derivative classes coming from higher modular points of infinite order which are not divisible by p in $E(\mathbb{Q}(C))$ as shown in Proposition 4.1.5.

Suppose p is one of the following:

- A prime of split multiplicative reduction for E and $p \nmid \mathrm{ord}_p(\Delta_E)$,
- A prime of non-split multiplicative reduction for E,
- A non-anomalous prime of good ordinary reduction for E,

where Δ_E is the minimal discriminant of E. Here, a prime p of good reduction for E is said to be anomalous if p divides $|\tilde{E}(\mathbb{F}_p)|$ and is non-anomalous otherwise as defined in Definition 4.1.4. This ensures that the higher modular points are not divisible by p in $E(\mathbb{Q}(C))$. Let

$$F_n := \begin{cases} K_{p^{n+1}N_E} & \text{if } p \text{ is a prime of good reduction for } E, \\ K_{p^n N_E} & \text{if } p \text{ is a prime of multiplicative reduction for } E, \end{cases}$$

for $n \geq -1$ with $F := F_{-1}$. We assume

$$\tau_{F,A,p} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{PGL}_2(\mathbb{Z}_p)$$

is surjective giving $\mathrm{Gal}(F_n/F) \cong \mathcal{G}_n$. We let $\mathcal{A}_n$ be a non-split Cartan subgroup of $\mathcal{G}_n$. This is a cyclic subgroup of order $p^{n+1} + p^n$. Then we define L_n to be the subfield of F_n fixed by $\mathcal{A}_n$. We are able to construct a mapping

$$\delta_n : \mathrm{H}^1(\mathcal{A}_n, S_n) \to Ш(E/L_n)[p^\infty]$$

as seen in Lemma 4.3.15, where S_n denotes the saturated group generated by the higher modular points in $E(F_n)$ as defined in the notation. With the conditions

on p, we can show that the source of δ_n is a cyclic group of order p^n. This result derives from the link between the construction of the derivative classes and integral representation theory. The group S_n defined earlier is isomorphic to a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice containing T_n as seen in subsection 4.3.2. Due to the structure of S_n and the above theorem, we are able to show that $S_n \cong T_n$ under the conditions we have stated and therefore, as we understand the cohomology of T_n associated to subgroups of $\mathcal{G}_n$, we can show that the source of δ_n is a cyclic group of order p^n. We can then use this to prove the main theorem of this thesis, which is Theorem 4.3.18.

Theorem. *Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let $p > 3$ be a prime of multiplicative reduction for A such that $\mathrm{ord}_p(\Delta_A) = 1$ and let F_n be as defined above. Assume that:*

1. *A is semistable,*
2. *E has either split multiplicative reduction at p with $p \nmid \mathrm{ord}_p(\Delta_E)$, non-split multiplicative reduction at p, or good ordinary non-anomalous reduction at p,*
3. *The degree of any isogeny of A defined over $\mathbb{Q}$ is coprime to N_E,*
4. *$\overline{\rho}_{\mathbb{Q},A,p}$ is surjective,*
5. *$\overline{\rho}_{\mathbb{Q},E,p}$ is surjective,*
6. *Any prime ℓ of bad reduction for E and good reduction for A has $a_\ell(A)^2 - 4\ell$ square modulo p where $a_\ell(A)$ is the Hecke eigenvalue of the newform f attached to the isogeny class of A.*

Then there exists an element of order p^n in $\mathrm{Sel}^{p^n}(E/L_n)$.

As with the modular curve, we will not look at the definition of a newform f attached to A in this thesis, but for more details, refer to [14]. This theorem is not only a generalisation of Wuthrich's work on self points to the modular points setting, by bounding Selmer groups from below, but it shows that we can also construct specific elements of prime power order in these groups. We are able to prove that if the first and fourth conditions in the theorem are true, then $\tau_{F,A,p}$ is surjective and so $\mathrm{Gal}(F_n/F) \cong \mathcal{G}_n$ for all $n \geq 0$ as seen in Proposition 4.3.17. The fifth point is essential in order to ensure $E(F_n)[p] = 0$ for all $n \geq 0$ as

seen in Proposition 4.3.14. We know that this condition excludes only a finite number of primes if E has no complex multiplication. The final point ensures that the primes dividing N_E but not N_A split completely in F_n/L_n as seen in Theorem 4.3.2. This is fundamental when showing that the image of the derivation map δ_n lies in $Ш(E/L_n)$ in Lemma 4.3.15.

This thesis will compose of three chapters. The first chapter will look at two different constructions of modular points and how they can be used to bound Selmer groups. We initially look at the construction of Heegner points and follow the method of Kolyvagin exactly as shown in [19] to construct cohomology classes coming from Heegner points. We will see that the cohomology classes lie outside of the Selmer group, restricting its size. In particular, the Selmer groups are cyclic and generated by an element that lies in the image of the Kummer map rather then a lift of a non-trivial element in the Shafarevich-Tate group.

We then look at Wuthrich's work in [39] on the construction of a different type of modular point called a self point, and how they form an analogue system to Kolyvagin's work to produce cohomology classes. We will look at how we can relate the group generated by the points in the elliptic curve to a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice inside V_n. We will see that Wuthrich was able to use information on the integral representation theory of $\mathcal{G}_n$ to show that the derivative classes lie in the Selmer groups, increasing their size. In particular, the size of the Selmer groups are bounded below by a prime power as seen in Theorem 2.3.10.

The second chapter will focus on the representation theory of $\mathcal{G}_n$. We initially look at the group theoretical properties associated to $\mathcal{G}_n$ in section 3.1 as well as some important cohomological results that will be vital to the understanding of the representations in section 3.2. We then focus on the modular representation theory of $\mathcal{G}_n$ in section 3.3 in order to provide a further understanding of the integral representation theory. Here we find all the possible $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$, defining all in Theorem 3.3.8, and look at some cohomological results associated to them.

We then focus on the integral representation theory associated to $\mathcal{G}_n$. We initially look at the $n = 0$ case in section 3.4 and show that we are able to find all $\mathbb{Z}_p[\mathcal{G}_0]$-lattices in V_0 in Theorem 3.4.1 due to its irreducibility as a $\mathbb{Q}_p[\mathcal{G}_0]$-module. However, this is not the case when $n \geq 1$. We study the lattices

we have found in section 3.5 and their cohomological results with respect to subgroups of $\mathcal{G}_n$ in section 3.6.

The final chapter will look at generalising the construction of self points, as seen in both sections 4.1 and 4.2, to prove the above theorem in section 4.3. We will show that we are able to follow the method of Wuthrich to bound Selmer groups from below by a prime power. However, we go further to show that the Selmer groups must contain an element of prime power order as seen in both Theorem 4.3.1 and Theorem 4.3.18. This relies on the work on the representation theory in the previous chapter to further understand the structure of S_n. We finally look at some examples of the results to elliptic curves in section 4.4.

1.1 Notation

We briefly mention the notation that will be used throughout this thesis. We will split this section into two, starting with the notation for the arithmetic side, which will be required for chapters 2 and 4. Then we will look at the notation used for the algebraic side.

1.1.1 Arithmetic Notation

For a number field K, we define its absolute Galois group as G_K. If we let ν be a place of K, then we define K_ν as the completion of K at ν. We then let I_ν be the inertia subgroup of G_{K_ν}. We will also be looking at the Galois cohomology attached to a G_K-module M. We define $\mathrm{H}^i(K, M) := \mathrm{H}^i(G_K, M)$ for $i \geq 0$.

For an elliptic curve E over K and $m > 1$ an integer, let $E[m]$ be the m-torsion subgroup of $E(\overline{K})$. We have G_K acting on $E[m]$ and this leads to a Galois representation

$$\overline{\rho}_{K,E,m} : G_K \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let p be a prime number. We then define $E[p^\infty] = \cup_{n\geq 1} E[p^n]$. Also, we define $T_pE = \varprojlim_n E[p^n]$ to be the p-adic Tate module of E. This leads to the Galois representation

$$\rho_{K,E,p} : G_K \to \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$$

where $\mathbb{Z}_p$ will denote the p-adic integers. If we let

$$\overline{\pi}_m : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z}) \quad \text{and} \quad \pi_p : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}_p)$$

be the quotient mappings where $Z_m := \ker(\overline{\pi}_m)$ is the centre of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we define the mappings $\overline{\tau}_{K,E,m} = \overline{\pi}_m \circ \overline{\rho}_{K,E,m}$ and $\tau_{K,E,p} = \pi_p \circ \rho_{K,E,p}$.

We also define the Kummer map. Let E/K be an elliptic curve over a number field K and $m \geq 1$ an integer. Then there is a short exact sequence

$$0 \to E(K)/mE(K) \xrightarrow{\kappa} \mathrm{H}^1(K, E[m]) \to \mathrm{H}^1(K, E)[m] \to 0$$

as shown in section 2.1. Here, we define the mapping κ as the Kummer map, where for $P \in E(K)$, we let $Q \in E(\overline{K})$ such that $P = mQ$. Then the class $\kappa[P] \in \mathrm{H}^1(K, E[m])$ is given by

$$\kappa[P](\sigma) = \sigma(Q) - Q.$$

For p a prime, we define $a_p(E)$ to be the Hecke eigenvalue of the newform f attached to the isogeny class of E. We will not look at the definition of a newform f attached to E in this thesis, but for more details, refer to [14].

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Due to the modularity theorem, there exists a surjective morphism

$$\Phi_E : X_0(N_E) \to E$$

defined over $\mathbb{Q}$ where $X_0(N_E)(\mathbb{C}) = \Gamma_0(N_E)\backslash\mathbb{H}^*$ is a modular curve with subvariety $Y_0(N_E)(\mathbb{C}) = \Gamma_0(N_E)\backslash\mathbb{H}$, which is isomorphic to

$$\{(A,C) | A \text{ is an elliptic curve and } C \text{ is a cyclic subgroup in } A \text{ of order } N_E\}/\sim$$

where $(A, C) \sim (A', C')$ if there exists an isomorphism $\psi : A \to A'$ such that $\psi(C) = C'$. We will not look at definitions of $X_0(N_E)$ or $Y_0(N_E)$ in this thesis, but for details on their construction, see [14].

Using this, we look at the notation for the modular points we will look at in chapters 2 and 4. Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let C be a cyclic subgroup in A of order N_E and define

$$x_{A,C} := (A, C) \in X_0(N_E)(\mathbb{Q}(C))$$

where $\mathbb{Q}(C)$ is the field of definition of C. If $A = E$, then we define $x_C := x_{E,C}$. The image of this point under Φ_E will be defined as

$$P_{A,C} := \Phi_E(x_{A,C}) \in E(\mathbb{Q}(C))$$

with $P_C := P_{E,C}$ when $A = E$. The compositum of all such $\mathbb{Q}(C)$ will be denoted K_{N_E}. We then define the group $G_{N_E} := \mathrm{Gal}(K_{N_E}/\mathbb{Q})$. Via $\overline{\tau}_{\mathbb{Q},A,N_E}$, this can be viewed as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N_E\mathbb{Z})$. Let d be a divisor of N_E. Then we define the image of G_{N_E} in the projection

$$\mathrm{PGL}_2(\mathbb{Z}/N_E\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/d\mathbb{Z})$$

as G_d with K_d defined as it's fixed field in K_{N_E}. Namely, K_d is the smallest field such that its absolute Galois group acts by scalars on $A[d]$.

We then look at the notation required for higher modular points. Their construction will be explained in chapters 2 and 4, but they will be denoted $Q_{A,D}$ where D is a cyclic subgroup in A of order p^{n+1} for p prime and $n \geq 0$. Here, we let $Q_D := Q_{E,D}$ whenever $A = E$. The points $Q_{A,D}$ will be defined over

$$F_n := \begin{cases} K_{p^{n+1}N_E} & \text{if } p \nmid N_E, \\ K_{p^n N_E} & \text{if } p || N_E, \end{cases}$$

for $n \geq -1$ with $F := F_{-1}$. Here, $p||N_E$ means p strictly divides N_E and so is a prime of multiplicative reduction with respect to E. We will also let $G_n := \mathrm{Gal}(F_n/F)$. Finally, we let

$$S_n := \{P \in E(F_n) : \text{ there exists a } k \geq 0 \text{ such that } p^k P \in \mathbb{Z}_p[G_n] \cdot Q_{A,D}\}$$

be the saturated group of higher modular points.

1.1.2 Algebraic Notation

For the algebraic side, we will be looking at the representation theory associated to

$$\mathcal{G}_n := \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$$

and its action on the projective line defined over a cyclic group of prime power order, which we will denote $\mathbb{P}^1_n := \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Throughout this thesis, we let an element

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{G}_n$$

denote the coset representing this matrix in $\mathcal{G}_n$. We first look at the notation we will use with regards to subgroups of $\mathcal{G}_n$. Let $\mu_n : \mathcal{G}_n \to \mathcal{G}_0$ be the surjective reduction mapping. We now fix definitions for certain subgroups. We let:

1) $\mathcal{G}_n := \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$,
2) $\mathcal{B}_n := \{\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a Borel subgroup of order $p^{2n+1}(p-1)$,
3) $\mathcal{H}_n := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a cyclic subgroup of order p^{n+1}, generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$,
4) $\mathcal{I}_n := \{g \in \mathcal{G}_n : \mu_n(g) \in \mathcal{B}_0\}$ the standard Iwahori subgroup which has order $p^{3n+1}(p-1)$,
5) $\mathcal{P}_n := \{g \in \mathcal{G}_n : \mu_n(g) \in \mathcal{H}_0\}$ the pro-p Iwahori subgroup and a Sylow-p subgroup of $\mathcal{I}_n$,
6) $\mathcal{U}_n := \{\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \in \mathcal{G}_n : p|a\}$ a cyclic subgroup of order p^n, generated by $\left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$,
7) $\mathcal{D}_n := \{\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a split Cartan subgroup, which is cyclic of order $p^n(p-1)$ and generated by the element $\left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where c generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$,
8) $N(\mathcal{D}_n)$ the normaliser of a split Cartan subgroup, a subgroup of $\mathcal{G}_n$ which contains $\mathcal{D}_n$ of index 2,
9) $\mathcal{A}_n$ a non-split Cartan subgroup, which is cyclic of order $p^n(p+1)$ and generated by an element denoted α_n,
10) $N(\mathcal{A}_n)$ the normaliser of a non-split Cartan subgroup, a subgroup of $\mathcal{G}_n$ which contains $\mathcal{A}_n$ of index 2.

If we define the surjective reduction mapping $\mu_n^k : \mathcal{G}_n \to \mathcal{G}_k$ for $0 \leq k \leq n$, then we may define the subgroup

$$\mathcal{I}_n^k = \{g \in \mathcal{G}_n : \mu_n^k(g) \in \mathcal{B}_k\}.$$

We have $\mathcal{I}_n^n = \mathcal{B}_n$ and also, as $\mu_n = \mu_n^0$, we have $\mathcal{I}_n^0 = \mathcal{I}_n$.

We also look at the notation we will use for the representations associated to $\mathcal{G}_n$. Let $p \neq 2$ be a prime. Then for $n \geq 0$, we define the $\mathbb{Q}_p[\mathcal{G}_n]$-modules

$$V_{(n)} := \mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{Q}_p)$$

and

$$V_n := \ker\left(V_{(n)} \to \mathbb{Q}_p\right).$$

We can view

$$V_{(n)} = \mathrm{Maps}(\mathbb{P}_n^1 \to \mathbb{Q}_p)$$

and

$$V_n := \left\{f : \mathbb{P}_n^1 \to \mathbb{Q}_p : \sum_C f(C) = 0\right\}$$

We can then define the standard $\mathbb{Z}_p[\mathcal{G}_n]$-lattices

$$T_{(n)} := \mathbb{Z}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{Z}_p)$$

and

$$T_n := \ker\left(T_{(n)} \to \mathbb{Z}_p\right)$$

inside $V_{(n)}$ and V_n respectively. We will see in Theorem 2.3.4 that as a $\mathbb{Q}_p[\mathcal{G}_n]$-module, $V_{(n)}$ decomposes as

$$V_{(n)} = \bigoplus_{i=-1}^{n} W_i$$

where W_i are irreducible $\mathbb{Q}_p[\mathcal{G}_n]$-modules of dimension δ_i as a $\mathbb{Q}_p$-vector space where

$$\delta_i = \begin{cases} 1 & \text{if } i = -1, \\ p & \text{if } i = 0, \\ p^{i+1} - p^{i-1} & \text{if } i \geq 1. \end{cases}$$

These modules take the form

$$W_i = \ker\left(\mathbb{Q}_p\left[{}^{\mathcal{G}_i}/_{\mathcal{B}_i}\right] \to \mathbb{Q}_p\left[{}^{\mathcal{G}_{i-1}}/_{\mathcal{B}_{i-1}}\right]\right)$$
$$= \left\{ f : \mathbb{P}^1_i \to \mathbb{Q}_p : \sum_{C \supset D} f(C) = 0 \text{ for } D \in \mathbb{P}^1_{i-1} \right\}$$

for $i \geq 0$ and $W_{-1} = \mathbb{Q}_p$. We also define the standard $\mathbb{Z}_p[\mathcal{G}_n]$-lattice inside W_i as

$$R_i = \ker\left(\mathbb{Z}_p\left[{}^{\mathcal{G}_i}/_{\mathcal{B}_i}\right] \to \mathbb{Z}_p\left[{}^{\mathcal{G}_{i-1}}/_{\mathcal{B}_{i-1}}\right]\right)$$
$$= \left\{ f : \mathbb{P}^1_i \to \mathbb{Z}_p : \sum_{C \supset D} f(C) = 0 \text{ for } D \in \mathbb{P}^1_{i-1} \right\}$$

for $i \geq 0$ and $R_{-1} = \mathbb{Z}_p$. Finally, we can extend this construction to the standard lattice in $\bigoplus_{i=k+1}^{n} W_i$ for $0 \leq k \leq n-1$ which is

$$R_n^k := \left\{ f : \mathbb{P}^1_n \to \mathbb{Z}_p : \sum_{C \supset D} f(C) = 0 \text{ for all } D \in \mathbb{P}^1_k \right\}.$$

Finally, throughout Chapter 3, we let $M_n := \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$ and will show that M_n is uniserial as an $\mathbb{F}_p[\mathcal{I}_n]$-module for all $n \geq 1$ in Proposition 3.3.1. We then define all the $\mathbb{F}_p[\mathcal{I}_n]$-submodules of M_n as E_t where t is the dimension of E_t as an $\mathbb{F}_p$-vector space and $1 \leq t \leq p^n$. Using this, we define $K_t := \mathrm{Ind}_{\mathcal{I}_n}^{\mathcal{G}_n}(E_t)$. For the definitions of all the other $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$, see Theorem 3.3.8.

Chapter 2

Background

This chapter is split up into three sections. In section 2.1, we look at the definitions of both Selmer groups and Shafarevich-Tate groups and the motivation to study them, mainly following [12]. We initially look at the group structure of an elliptic curve in Theorem 2.1.1, the Mordell-Weil Theorem, and provide a summary of its proof. This involves looking at the Weak Mordell-Weil Theorem, Theorem 2.1.3, which requires the definitions of both the Selmer group and the Shafarevich-Tate group in Definition 2.1.4 as well as the Selmer group being finite as seen in Theorem 2.1.5. We then state a version of the Birch and Swinnerton-Dyer Conjecture, which is Conjecture 2.1.8, and state a contribution towards it in Theorem 2.1.9, the contribution of Kolyvagin to Theorem 2.1.9 being reviewed in section 2.2. The following sections will look at two different constructions of modular points and how they can be used to bound Selmer groups.

In section 2.2, we review the work of Kolyvagin on Heegner points by following the method exactly as shown in [19], with no new material. However, we do go more in-depth in some explanations to parts of the proof in [19]. We review this work in order to understand how Kolyagin was able to use a certain type of modular point to bound Selmer groups which ultimately led to his contribution to Theorem 2.1.9. We look at the construction of Heegner points and how Kolyvagin was able to use them in order to create cohomology classes. This construction of cohomology classes coming from modular points, known as derivative classes, are an important aspect not only in Kolyvagin's work, but the subsequent work of both Wuthrich with regards to self points and the work in Chapter 4 of this thesis, which will look at creating a different type of modular point in order to bound Selmer groups. We will see that the cohomology classes created by Kolyvagin do not lie in certain Selmer groups, bounding its size. In particular, the elements of these Selmer groups belong to the image of the Kummer map rather than lifted from non-trivial elements in Shafarevich-Tate groups.

We initially state the theorem of Kolyvagin, which is Theorem 2.2.3, that contributed to the proof of Theorem 2.1.9. However, we will only review the proof of Proposition 2.2.8 in this section, which is a slightly weaker result of Theorem 2.2.3. In subsection 2.2.1, we review the construction of the derivative classes. We prove Proposition 2.2.12 using Proposition 2.2.13, the trace relations associated to the Heegner points. Then using Proposition 2.2.15, we

define the classes c_n and see when they are non-trivial in Proposition 2.2.16. In subsection 2.2.2, we review some Tate local duality results that will be required in the proof of Proposition 2.2.8. In particular, we use Proposition 2.2.23 and Lemma 2.2.24 to prove Proposition 2.2.22, which will be required in subsection 2.2.3. Finally, in subsection 2.2.3, we use the previous two subsections to prove Proposition 2.2.8. In particular, we see that the classes c_n do not lie in the Selmer group when they are non-trivial unless $n = 1$ when it generates the Selmer group, as seen in Proposition 2.2.32, Proposition 2.2.33 and Proposition 2.2.34.

In section 2.3, we review the work of Wuthrich on self points in [39]. This will be important when generalising the construction of self points in Chapter 4. We will see that these points form an analogue system to the construction proposed by Kolyvagin to produce cohomology classes coming from the points. However, the classes constructed lie in the Selmer groups and hence, we can bound its size from below rather than from above as in Kolyvagin's case. We provide no new material here and skip the proofs as we can prove the results when looking at the more generalised construction in Chapter 4.

We initially review the construction of the self points, as seen in Definition 2.3.1, and the properties the points have in Theorem 2.3.2 as well as the relationships between them in Proposition 2.3.3. We then look at the construction of the higher self points, related to the self points, in Definition 2.3.6 and depending on the type of reduction of a certain prime p, we look at the group generated by the higher modular point, Theorem 2.3.8 being the multiplicative case and Theorem 2.3.9 being the good ordinary case. We end the section with the main theorem in [39], which is Theorem 2.3.10, and look at a sketch of the proof. This will again be important in chapter 4 as we will follow an identical method when generalising the construction of self points.

2.1 Elliptic Curves and Selmer Groups

Let E/K be an elliptic curve for a number field K. To understand the structure of the points in $E(K)$, we have the following.

Theorem 2.1.1 (Mordell-Weil Theorem)**.** *Let E/K be an elliptic curve. Then there exists an $r \geq 0$, called the rank of E/K, such that*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}}$$

where $E(K)_{\text{tors}}$ is the finite subgroup of all torsion points in $E(K)$. In particular, $E(K)$ is finitely generated.

This can be proved when applying the following to elliptic curves.

Theorem 2.1.2 (Descent Theorem)**.** *[34, Theorem 8.3.1] Let A be an abelian group. Suppose there exists a height function*

$$h : A \to \mathbb{R}$$

such that is satisfies the following properties:

1. *Let $P \in A$. Then there exists a constant C depending on A and P such that for all $Q \in A$,*
$$h(P+Q) \leq 2h(Q) + C.$$

2. *There exists an integer $m \geq 2$ and a constant C' depending on A such that for all $Q \in A$,*
$$h(mQ) \geq m^2 h(Q) - C'.$$

3. *For every constant C'', the set*
$$\{P \in A : h(P) \leq C''\}$$
is finite.

Suppose further that for the integer m in 2., A/mA is finite. Then A is finitely generated.

There are two steps needed in order to apply Theorem 2.1.2 in the proof of Theorem 2.1.1. The first is to define a height function $h : E(K) \to \mathbb{R}$, which we will not dwell on in this thesis, but we know that such a height function exists. The other would would be to prove the following.

Theorem 2.1.3 (Weak Mordell-Weil Theorem)**.** *Let E/K be an elliptic curve. Then for all $m \geq 1$, the group $E(K)/mE(K)$ is finite.*

To see the method of this proof, we let $m \geq 1$. Then there exists a short exact sequence

$$0 \to E(\overline{K})[m] \to E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \to 0$$

of G_K-modules. This induces a long exact sequence

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\kappa} \mathrm{H}^1(K, E[m]) \to \mathrm{H}^1(K, E) \to \mathrm{H}^1(K, E)$$

which induces

$$0 \to E(K)/mE(K) \xrightarrow{\kappa} \mathrm{H}^1(K, E[m]) \to \mathrm{H}^1(K, E)[m] \to 0$$

which is known as the descent exact sequence. The Kummer map, κ, is defined in the following way as shown on [34, pg. 216]. Let $P \in E(K)$ and choose a point $Q \in E(\overline{K})$ such that $P = mQ$. Then the class $\kappa[P] \in \mathrm{H}^1(K, E[m])$ is given by

$$\kappa[P](\sigma) = \sigma(Q) - Q.$$

Let M_K be the set of absolute values of K and take $v \in M_K$ with completion K_v. If we look at the embedding $\overline{K}$ into $\overline{K}_v$, then we have an inclusion of absolute Galois groups G_{K_v} in G_K. This leads to the local version of the descent exact sequence which fits into a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\kappa} & \mathrm{H}^1(K, E[m]) & \longrightarrow & \mathrm{H}^1(K, E)[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_v} & \searrow^{\delta_v} & \downarrow{\scriptstyle \mathrm{res}_v} & & \\
0 & \longrightarrow & E(K_v)/mE(K_v) & \xrightarrow{\kappa_v} & \mathrm{H}^1(K_v, E[m]) & \longrightarrow & \mathrm{H}^1(K_v, E)[m] & \longrightarrow & 0.
\end{array}$$

Here, the vertical maps are restriction mappings to G_{K_v}.

Definition 2.1.4. *We define the* m-Selmer group of E/K *as,*

$$\mathrm{Sel}^m(E/K) = \bigcap_{v \in M_K} \ker\left(\delta_v : \mathrm{H}^1(K, E[m]) \to \mathrm{H}^1(K_v, E)[m]\right)$$

and we define the Shafarevich-Tate group of E/K *as,*

$$Ш(E/K) = \bigcap_{v \in M_K} \ker\Big(\mathrm{res}_v : \mathrm{H}^1(K, E) \to \mathrm{H}^1(K_v, E)\Big).$$

Therefore, by the definitions of the Selmer and the Shafarevich-Tate groups, as well as using the above commutative diagram, we are able to create a short exact sequence

$$0 \to E(K)/mE(K) \xrightarrow{\kappa} \mathrm{Sel}^m(E/K) \to Ш(E/K)[m] \to 0. \tag{1}$$

Therefore, by exact sequence (1), Theorem 2.1.3 is a direct consequence of the following.

Theorem 2.1.5. *Let E/K be an elliptic curve. Then for all $m \geq 1$, the Selmer group $\mathrm{Sel}^m(E/K)$ is finite.*

Therefore, using the Weak Mordell-Weil Theorem and knowing that a height function $h : E(K) \to \mathbb{R}$ exists, then Theorem 2.1.2 is proven and hence Theorem 2.1.1 is proven also. The Mordell-Weil Theorem now poses a few questions about $E(K)$. In particular, when is the rank of $E(K)$ non-trivial? Is there a way to compute the rank or even calculate the points that generate $E(K)/E(K)_{\mathrm{tors}}$?

The relationship between $E(K)/mE(K)$ and $\mathrm{Sel}^m(E/K)$ is dependant upon $Ш(E/K)[m]$, which is reliant on m. In particular, if $Ш(E/K)[m] = 0$, we have an isomorphism $E(K)/mE(K) \cong \mathrm{Sel}^m(E/K)$. However, if the following is true, then this isomorphism exists for all but finitely many m.

Conjecture 2.1.6. *[12, Conjecture 1.9] Let E/K be an elliptic curve. Then $Ш(E/K)$ is finite.*

If this were true, we would be able to find information on $E(K)/mE(K)$ by calculating $\mathrm{Sel}^m(E/K)$. In particular, if p is a prime such that $E(K)[p] = 0$ and $p \nmid |Ш(E/K)|$, then the rank of $E(K)$ is equal to the dimension of $\mathrm{Sel}^p(E/K)$ as an $\mathbb{F}_p$-vector space. We would like to see when Conjecture 2.1.6 is true.

Definition 2.1.7. *Let E be an elliptic curve of conductor N and let $a_p := a_p(E)$ denote the Hecke eigenvalue of the newform f attached to E. Then the L-function attached to E is defined as*

$$L(E,s) := \prod_{p \nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \prod_{p|N} \left(1 - a_p p^{-s}\right)^{-1}.$$

This function only converges when $\mathrm{Re}(s) > \frac{3}{2}$. There is a link between analytic and algebraic number theory which culminates in the following.

Conjecture 2.1.8 (Birch and Swinnerton-Dyer)**.** *[12, Conjecture 1.12] Let $E/\mathbb{Q}$ be an elliptic curve. Then the L-function $L(E,s)$ extends to an entire function on $\mathbb{C}$ and the rank $r(E/\mathbb{Q})$ of $E(\mathbb{Q})$ is equal to the order of vanishing of $L(E,s)$ at $s = 1$.*

There have been contributions to this conjecture. In particular, we have the following.

Theorem 2.1.9 (Gross-Zagier, Kolyvagin)**.** *[12, Theorem 1.14] Let $E/\mathbb{Q}$ be an elliptic curve.*

1. *If $L(E,1) \neq 0$, then the rank of $E(\mathbb{Q})$ is zero.*
2. *If $L(E,1) = 0$ and $L'(E,1) \neq 0$ then the rank of $E(\mathbb{Q})$ is 1.*

In both cases, $Ш(E/\mathbb{Q})$ is finite.

This proof relies on the work of both Gross-Zagier and Kolyvagin as well as the modularity of elliptic curves. Again, the work by Gross-Zagier involves the height function associated to E, which we will not look at. However, we are interested in Kolyvagin's work on using Heegner points to bound Selmer groups.

2.2 Heegner Points

In this section, we review [19], which looks at how Kolyvagin used Heegner points to bound Selmer groups and using this, found the rank of elliptic curves over certain imaginary quadratic fields as well as showing that certain Shafarevich-Tate groups are finite.

Let K be an imaginary quadratic field of the form $\mathbb{Q}(\sqrt{d_K})$ with ring of integers O_K such that $d_K \notin \{-3, -4\}$. This is to ensure that $O_K^\times = \{\pm 1\}$.

Definition 2.2.1. *An order, O, in K is a subring of K that generates K as a $\mathbb{Q}$-vector space and is finitely generated as a $\mathbb{Z}$-module. The order of conductor $n \in \mathbb{Z}_{>0}$, denoted O_n, is the order $O_n = \mathbb{Z} \oplus nO_K$ which has index n in O_K.*

Fix an integer N. We will now require the *Heegner hypothesis* as defined in [12, Hypothesis 3.9], that all primes dividing N are split in $K/\mathbb{Q}$. This ensures that there exists a prime ideal, I, of O_K such that $O_K/I \cong \mathbb{Z}/N\mathbb{Z}$. We can define for all n coprime to N, $I_n = I \cap O_n$. This is an invertible ideal in O_n such that $O_n/I_n \cong \mathbb{Z}/N\mathbb{Z}$.

Let I_n^{-1} denote the inverse of I_n. As $\mathbb{C}/O_n$ and $\mathbb{C}/I_n^{-1}$ represent elliptic curves over $\mathbb{C}$, and $O_n \subset I_n^{-1}$, we have

$$I_n^{-1}/O_n = \ker\left(\mathbb{C}/O_n \to \mathbb{C}/I_n^{-1}\right).$$

Therefore, $I_n^{-1}/O_n \cong O_n/I_n$ is a cyclic subgroup of $\mathbb{C}/O_n$ of order N and we have a point

$$x_n := \left(\mathbb{C}/O_n, I_n^{-1}/O_n\right) \in X_0(N)(K_n)$$

where K_n is the ring class field of K of conductor n, as seen in [19, pg. 238]. In particular, $\mathbb{C}/O_n$ is an elliptic curve with complex multiplication as $\sqrt{d_K} \notin \mathbb{Q}$ by [34, Theorem 6.5.5].

Definition 2.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then a* Heegner point of conductor n *on E associated to K is $P_n = \Phi_E(x_n) \in E(K_n)$.*

Here, the definition of Φ_E is as defined in the notation. Therefore, the construction of a Heegner point comes from an elliptic curve with complex multiplication. We denote the set of Heegner points of conductor n as $HP(n)$.

Kolyvagin studied the relationship between these points and noticed that they satisfied certain trace relations which show that the Heegner points form an Euler system. He was then able to bound Selmer groups attached to E/K using the Heegner points.

Theorem 2.2.3. *(Kolyvagin) [19, Theorem 1.3] Let* $P_K := \mathrm{Tr}_{K_1/K}(P_1) \in E(K)$. *If* P_K *is non-torsion in* $E(K)$*, then:*

1. *The Mordell-Weil group* $E(K)$ *has rank 1.*
2. $Ш(E/K)$ *is finite.*

In this section, we will prove the "mod p" version of this theorem for certain primes.

Definition 2.2.4. *A prime* p *is called a* descent prime *if it satisfies the following conditions:*

1. $p \nmid 6N$,
2. $\overline{\rho}_{\mathbf{Q},E,p}$ *is surjective.*

We then have the mod p version of Kolyvagin's theorem.

Proposition 2.2.5. *[19, Proposition 2.1] Let* p *be a descent prime such that* p *doesn't divide the order of* P_K *in* $E(K)$*. Then:*

1. $E(K)$ *has rank* 1,
2. $Ш(E/K)[p]$ *is trivial.*

This theorem is not as strong as Kolyvagin's theorem, but if E has no complex multiplication then this only excludes a finite number of primes. This is due to the following theorem by Serre.

Theorem 2.2.6. *[33, Theorem 2, pg 294] Let* E/F *be an elliptic curve where* F *is a number field and* E *has no complex multiplication over* $\overline{F}$*. Then* $\overline{\rho}_{F,E,p}$ *is surjective for all but finitely many primes* p*.*

From the exact sequence

$$0 \to E(K)/pE(K) \xrightarrow{\kappa} \mathrm{Sel}^p(E/K) \to Ш(E/K)[p] \to 0,$$

we see that the rank of $E(K)$, denoted $r(E/K)$, is equal to the dimension of $E(K)/pE(K)$ as an $\mathbb{F}_p$-vector space due to the following.

Lemma 2.2.7. *Let* p *be a descent prime for* $E/\mathbf{Q}$*. Then* $E(K)[p] = 0$.

Proof. Suppose $E(K)[p] \neq 0$. Then as $K/\mathbb{Q}$ is a quadratic, $K \subseteq \mathbb{Q}(E[p])$. Hence, $\mathrm{Gal}(\mathbb{Q}(E[p])/K)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This contradicts that $\overline{\rho}_{\mathbb{Q},E,p}$ is surjective. □

This can be used in order to reduce proving Proposition 2.2.5 to proving the following.

Proposition 2.2.8. *[19, Proposition 2.3] Let p be a descent prime such that p doesn't divide the order of P_K in $E(K)$. Then $\mathrm{Sel}^p(E/K)$ is cyclic and generated by $\kappa[P_K]$.*

Therefore, if Proposition 2.2.8 is true, then $[P_K] \in E(K)/pE(K)$ is non-zero by the hypothesis of Proposition 2.2.8, so the dimension of $E(K)/pE(K)$ as an $\mathbb{F}_p$-vector space is non-zero. However, as κ is injective and $\mathrm{Sel}^p(E/K)$ has rank 1, then

$$r(E/K) = \dim_{\mathbb{F}_p}\Big(E(K)/pE(K)\Big) = 1.$$

Also, as $\mathrm{Sel}^p(E/K)$ is generated by $\kappa[P_K]$, then all elements of $\mathrm{Sel}^p(E/K)$ are sent to zero under the mapping $\mathrm{Sel}^p(E/K) \to Ш(E/K)[p]$. However, this map is surjective meaning $Ш(E/K)[p] = 0$. Therefore, for the remainder of this section, we will show an outline of the proof of Proposition 2.2.8.

2.2.1 Construction of the Derivative Classes

In this part, we will look at how Kolyvagin created derivative classes coming from the Heegner points. We also look at some properties associated to these classes and determine when they lie in $\mathrm{Sel}^p(E/K)$.

We initially provide some information on the Galois groups associated to the ring class fields K_n. By [12, Theorem 3.3], K_n/K is an abelian extension unramified outside n such that $\mathrm{Gal}(K_n/K) \cong \mathrm{Pic}(O_n)$ for all $n \geq 1$ prime to N, with $\mathrm{Gal}(K_1/K) \cong \mathrm{Pic}(O_K)$ being the Picard group. If we let τ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$, then it can be lifted to K_n and acts on $\mathrm{Gal}(K_n/K)$ by $\tau\sigma\tau^{-1} = \sigma^{-1}$. We want to look at some specific values of n. We first require the following.

Definition 2.2.9. *Let ℓ be prime. Then ℓ is a Kolyvagin prime associated to the system (E, K, p) if it satisfies the following.*

1. *ℓ does not divide $p \cdot N \cdot d_K$,*
2. *If* Frob_ℓ *denotes the conjugacy class of* $\mathrm{Gal}(K(E[p])/\mathbb{Q})$ *containing the Frobenius element,* Fr_γ*, for every prime γ above ℓ of $K(E[p])$, then if we lift τ to $K(E[p])$, then $\tau \in \mathrm{Frob}_\ell$.*

By the Chebotarev Density Theorem, there exists infinitely many such primes. We see that (1) implies ℓ is unramified in $K(E[p])/\mathbb{Q}$. Further, as $\tau \in \mathrm{Frob}_\ell$, ℓ remains inert in K. Therefore, we let λ denote the prime of K above ℓ with Frobenius element $\mathrm{Fr}_\lambda = \tau$. We now focus on the Heegner points of conductor n such that

1. n is squarefree,
2. All primes $\ell \mid n$ are Kolyvagin primes associated to (E, K, p).

We let $a_\ell := a_\ell(E)$ denote the ℓ-th Fourier coefficient for the newform associated to the isogeny class of E. As stated in the notation, we will not look at the definition here, but refer you to [14].

Lemma 2.2.10. *We have $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$.*

Proof. As τ is complex conjugation, then the characteristic polynomial of τ acting on $E[p]$ is $x^2 - 1$. Also, the characteristic polynomial of Frob_ℓ acting on $E[p]$ is $x^2 - a_\ell x + \ell$. However, as $\mathrm{Frob}_\ell = \tau$ in $\mathrm{Gal}(K/\mathbb{Q})$, we must have

$$a_l \equiv l + 1 \equiv 0 \pmod{p}. \qquad \square$$

As ℓ is inert in $K/\mathbb{Q}$, then we have $\mathbb{F}_\lambda \cong \mathbb{F}_{\ell^2}$. Also, by Definition 2.2.9 part (2), λ splits completely in $K(E[p])/K$. Therefore, if γ is a prime above λ in $K(E[p])$, then $\mathbb{F}_\lambda \cong \mathbb{F}_\gamma$ and so $\tilde{E}(\mathbb{F}_\lambda)[p] \cong \mathbb{F}_p^2$. In particular, this shows that $\tilde{E}(\mathbb{F}_\lambda)$ obtains full p-torsion and we have the following.

Proposition 2.2.11. *Let λ be as above. Then $\tilde{E}(\mathbb{F}_\lambda)[p]^\pm \cong \mathbb{F}_p$ where $\pm$ denotes the eigenspace of* $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. As $\tau \in \mathrm{Frob}_\ell$ as seen earlier, then $\mathrm{Fr}_\lambda = \tau$ on $\mathbb{F}_\lambda$. Therefore

$$\begin{aligned}\left|\tilde{E}(\mathbb{F}_\lambda)[p]^+\right| &= \left|\ker\left(\mathrm{Fr}_\lambda - 1 : \tilde{E}(\mathbb{F}_\lambda)[p] \to \tilde{E}(\mathbb{F}_\lambda)[p]\right)\right| \\ &= \left|\ker\left(\mathrm{Fr}_\lambda - 1 : \tilde{E}[p] \to \tilde{E}[p]\right)\right| \\ &= \deg(\mathrm{Fr}_\lambda - 1) \\ &= |\tilde{E}(\mathbb{F}_\ell)| = \ell + 1 - a_\ell\end{aligned}$$

as $\mathrm{Fr}_\lambda - 1$ is separable. It can be similarly shown that

$$\left|\tilde{E}(\mathbb{F}_\lambda)[p]^-\right| = \deg(\mathrm{Fr}_\lambda + 1)$$

as $\mathrm{Fr}_\lambda + 1$ is separable. We also see from the parallelogram identity on endomorphisms on E that

$$\begin{aligned}\deg(\mathrm{Fr}_\lambda + 1) &= 2\deg(\mathrm{Fr}_\lambda) + 2 - \deg(\mathrm{Fr}_\lambda - 1) \\ &= 2(\ell + 1) + a_\ell - (\ell + 1) = \ell + 1 + a_\ell.\end{aligned}$$

Therefore, by Lemma 2.2.10, both must be divisible by p which gives our result. □

We now look at the Galois groups associated to the ring class fields. We define $G_n := \mathrm{Gal}(K_n/K_1)$ and so if $n = \prod \ell$ is the prime decomposition of n, then $G_n \cong \prod G_\ell$ where $G_m := \mathrm{Gal}(K_n/K_{n/m})$ for $m \mid n$. Then

$$G_\ell \cong \mathrm{Gal}(K_\ell/K_1) \cong \frac{\mathrm{Pic}(O_\ell)}{\mathrm{Pic}(O_K)} \cong \mathbb{F}_\lambda^\times/\mathbb{F}_\ell^\times$$

which is cyclic of order $\ell + 1$. Let σ_ℓ generate G_ℓ. Then $\sigma_\ell - 1$ generates the augmentation ideal of $\mathbb{Z}[G_\ell]$. Define

$$\mathrm{Tr}_\ell := \sum_{i=0}^{\ell} \sigma_\ell^i \in \mathbb{Z}[G_\ell]$$

and $D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbb{Z}[G_\ell]$. Then we have

$$\begin{aligned}(\sigma_\ell - 1)D_\ell &= \sum_{i=1}^{\ell} i\sigma_\ell^{i+1} - \sum_{j=1}^{\ell} j\sigma_\ell^j \\ &= \sum_{i=2}^{\ell+1}(i-1)\sigma_\ell^i - \sum_{j=1}^{\ell} j\sigma_\ell^j \\ &= \sum_{i=2}^{\ell+1} i\sigma_\ell^i - \sum_{k=2}^{\ell+1}\sigma_\ell^k - \sum_{j=1}^{\ell} j\sigma_\ell^j \\ &= \ell + 1 - \sigma_\ell - 1 - \sum_{k=2}^{\ell}\sigma_\ell^k \\ &= \ell + 1 - \mathrm{Tr}_\ell\,.\end{aligned}$$

Let $D_n := \prod D_\ell$. We would like to prove the following.

Proposition 2.2.12. *[19, Proposition 3.6] We have the class*

$$[D_n P_n] \in (E(K_n)/pE(K_n))^{G_n}.$$

However, we will need the following first, which we provide a sketch of the proof.

Proposition 2.2.13. *[19, Proposition 3.7] Let $n = \ell m$ where ℓ is prime. Then:*

1. $\mathrm{Tr}_\ell\, P_n = a_\ell P_m \in E(K_m)$,
2. *Each prime factor λ_n of ℓ in K_n divides a unique prime λ_m of K_m and* $P_n \equiv \mathrm{Fr}_{\lambda_m} P_m \pmod{\lambda_n}$.

Proof. (Sketch) For the first part, it can be shown that $\mathrm{Tr}_\ell(x_n) = T_\ell(x_m)$ on $X_0(N)$ where T_ℓ is the Hecke operator on the Jacobian $J_0(N)$. As T_ℓ acts as multiplication by a_ℓ on the points of E, then we have

$$\mathrm{Tr}_\ell\, P_n = \mathrm{Tr}_\ell\, \Phi_E(x_n) = \Phi_E(\mathrm{Tr}_\ell\, x_n) = \Phi_E(T_\ell x_m) = a_\ell \Phi_E(x_m) = a_\ell P_m$$

where Φ_E is the modular parametrisation associated to E as defined in the notation. For the second part, it can be shown that λ splits completely in

K_m/K for $(m,\ell) = 1$. Also, as $O_K^\times = \{\pm 1\}$, then if λ_m and λ_n are primes above λ in K_m and K_n respectively, then it can be shown that

$$\mathbb{F}_{\lambda_m} = \mathbb{F}_{\lambda_n} = \mathbb{F}_\lambda = \mathbb{F}_{\ell^2}.$$

The points in the divisor of $T_\ell(x_m)$ are conjugates of x_n over K_m, so they are all congruent to x_n modulo λ_n. Using the Eichler-Shimura congruence relation, it can be shown that

$$\mathrm{Fr}_{\lambda_m} x_m \equiv x_n \pmod{\lambda_n}.$$

Using Φ_E, we have our result. □

In particular, Kolyvagin uses these trace relations to show that the Heegner points from an Euler system. We can now use this to prove Proposition 2.2.12.

Proof of Proposition 2.2.12. Let $n = \ell m$. By definition, we have $D_n = D_\ell D_m$ and so

$$(\sigma_\ell - 1)D_n = (\sigma_\ell - 1)D_\ell D_m = (\ell + 1 - \mathrm{Tr}_\ell)D_m = (\ell+1)D_m - \mathrm{Tr}_\ell\, D_m.$$

Therefore we have

$$(\sigma_\ell - 1)D_nP_n = (\ell+1)D_mP_n - D_m\,\mathrm{Tr}_\ell\, P_n = (\ell+1)D_mP_n - a_\ell D_mP_m$$

by the previous proposition. However, by Lemma 2.2.10, we have

$$(\sigma_\ell - 1)D_nP_n \in pE(K_n).$$

As this is true for all primes ℓ dividing n, and $G_n \cong \prod G_\ell$ is generated by the set $\{\sigma_\ell : \ell | n \text{ prime}\}$, then we are done. □

Let $H_n := \mathrm{Gal}(K_n/K)$. We then have the short exact sequence

$$0 \to G_n \to H_n \to \mathrm{Gal}(K_1/K) \to 0.$$

Let S be the set of coset representatives of ${}^{H_n}/_{G_n}$. We then define

$$Q_n := \sum_{\sigma \in S} \sigma(D_nP_n) \in E(K_n).$$

As $[D_nP_n] \in (E(K_n)/pE(K_n))^{G_n}$, then $[Q_n] \in (E(K_n)/pE(K_n))^{H_n}$. We also see for $n = 1$ that G_1 is trivial and so is D_1. Therefore

$$Q_1 = \sum_{\sigma \in S} \sigma P_1 = \mathrm{Tr}_{K_1/K}(P_1) = P_K.$$

We want to construct cohomology classes coming from the points Q_n. However, we first need the following.

Lemma 2.2.14. *[19, Lemma 4.3] For all such n, $E(K_n)[p] = 0$.*

Proof. We know that as p is a descent prime, then it is a prime of good reduction for E and $\overline{\rho}_{\mathbb{Q},E,p}$ is surjective. Therefore, the smallest Galois extension F of K such that $E(F)[p] \neq 0$ is $F = K(E[p])$, which has Galois group $\mathrm{Gal}(F/K) \cong \mathrm{GL}_2(\mathbb{F}_p)$, as seen in the proof of Lemma 2.2.7. Therefore, if $E(K_n)[p] \neq 0$, then $F \subseteq K_n$ and so H_n contains a subgroup whose quotient is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. This cannot happen as H_n is abelian. Therefore, $E(K_n)[p] = 0$. □

Using this, we can prove the following.

Proposition 2.2.15. *There exists an isomorphism*

$$\mathrm{H}^1(K, E[p]) \cong \mathrm{H}^1(K_n, E[p])^{H_n}.$$

Proof. We have the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(H_n, E(K_n)[p]) \to \mathrm{H}^1(K, E[p]) \to \mathrm{H}^1(K_n, E[p])^{H_n} \to \mathrm{H}^2(H_n, E(K_n)[p]).$$

The isomorphism occurs as $E(K_n)[p] = 0$ by Lemma 2.2.14. □

We thus have the following commutative diagram of cohomology groups.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{H}^1(H_n, E(K_n))[p] & & \\
 & & & & & & \downarrow{\scriptstyle \inf} & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\kappa} & \mathrm{H}^1(K, E[p]) & \xrightarrow{\mathrm{res}_K} & \mathrm{H}^1(K, E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \cong\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}_p} & & \\
0 & \longrightarrow & (E(K_n)/pE(K_n))^{H_n} & \xrightarrow{\kappa_n} & \mathrm{H}^1(K_n, E[p])^{H_n} & \xrightarrow{\mathrm{res}_n} & \mathrm{H}^1(K_n, E)[p]^{H_n}. & &
\end{array}$$

We have $[Q_n] \in (E(K_n)/pE(K_n))^{H_n}$. Therefore, using Proposition 2.2.15, we let $c_n \in \mathrm{H}^1(K, E[p])$ be the unique class such that $\mathrm{res}(c_n) = \kappa_n[Q_n]$. We let $d_n := \mathrm{res}_K(c_n)$. Then

$$\mathrm{res}_p(d_n) = \mathrm{res}_p \circ \mathrm{res}_K(c_n) = \mathrm{res}_n \circ \mathrm{res}(c_n) = \mathrm{res}_n \circ \kappa_n[Q_n] = 0$$

so $d_n \in \ker(\mathrm{res}_p)$. Therefore, we can define $\tilde{d}_n \in \mathrm{H}^1(H_n, E(K_n))[p]$ such that $d_n = \inf(\tilde{d}_n)$.

Proposition 2.2.16. *[19, Proposition 4.7]*

1. *c_n is trivial if and only if $Q_n \in pE(K_n)$.*
2. *d_n and $\tilde{d}_n$ are trivial if and only if $Q_n \in pE(K_n) + E(K)$.*

Proof. For the first part, $Q_n \in pE(K_n)$ if and only if

$$[Q_n] = 0 \in (E(K_n)/pE(K_n))^{H_n}.$$

However, as κ_n is injective, then this is true if and only if $\kappa_n[Q_n] = 0$. Therefore, we have $\mathrm{res}(c_n) = 0$ and as res is an isomorphism, this is true if and only if c_n is trivial.

For the second part, as inf is injective, then d_n is trivial if and only if $\tilde{d}_n$ is trivial. We also see that d_n is trivial if and only if c_n is trivial or $c_n = \kappa[T]$ for some $[T] \in E(K)/pE(K)$. Then due to the isomorphism of res, we have our result. □

We note here that $c_1 = \kappa[Q_1]$ as $Q_1 = P_K \in E(K)$. Therefore, c_1 is trivial if and only if P_K is divisible by p in $E(K)$, and the classes d_1 and $\tilde{d}_1$ are always globally trivial.

Using the Kummer pairing, we can represent the class $c_n : G_K \to E[p]$ with the 1-cocycle

$$c_n(\sigma) = \sigma\left(\tfrac{1}{p}Q_n\right) - \tfrac{1}{p}Q_n$$

and the class $\tilde{d}_n : H_n \to E[p]$ with the 1-cocycle

$$\tilde{d}_n(\sigma) = \tfrac{1}{p}Q_n - \sigma\left(\tfrac{1}{p}Q_n\right).$$

We now wish to look at some properties associated to the cohomology classes we have constructed. We know $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{H}^1(K, E[p])$ and as $p > 2$, we have a direct decomposition of eigenspaces for τ:

$$\mathrm{H}^1(K, E[p]) = \mathrm{H}^1(K, E[p])^+ \oplus \mathrm{H}^1(K, E[p])^-$$

where

$$\mathrm{H}^1(K, E[p])^\pm = \{\rho \in \mathrm{H}^1(K, E[p]) : \rho^\tau = \pm\rho\}.$$

We would like to know which eigenspace c_n lies in. Let w_N be the Fricke involution associated to $X_0(N)$. Then if $f = \sum a_n(f)q^n$ is the modular form associated to the isogeny class of E, we have

$$w_N(f) = \epsilon f$$

where $-\epsilon$ is the root number of $E/\mathbb{Q}$. We will need the following.

Proposition 2.2.17. *[19, Proposition 5.3] There exists a $\sigma \in H_n$ such that*

$$\tau P_n = \epsilon \cdot \sigma P_n + T$$

for some torsion point $T \in E(K_n)$.

We can use this to prove the following.

Proposition 2.2.18. *[19, Proposition 5.4]*

1. *The class* $[Q_n]$ *lies in the* e_n*-eigenspace for* τ *in* $(E(K_n)/pE(K_n))^{H_n}$ *where* $e_n = \epsilon \cdot (-1)^{f_n}$ *and* $f_n = |\{\ell \text{ prime } : \ell | n\}|$.
2. *We have* $c_n \in \mathrm{H}^1(K, E[p])^{e_n}$ *and* $d_n \in \mathrm{H}^1(K, E)[p]^{e_n}$.

Proof. We lift the element τ to $\mathrm{Gal}(K_n/\mathbb{Q}) = H_n \rtimes \mathrm{Gal}(K/\mathbb{Q})$. As this group is a dihedral group, then if $\sigma \in H_n$, then $\tau\sigma = \sigma^{-1}\tau$ and so we have

$$\tau Q_n = \tau \sum_{\sigma \in S} \sigma(D_n P_n) = \sum_{\sigma \in S} \sigma^{-1}\tau(D_n P_n).$$

Now, τ commutes with $\ell + 1 - \mathrm{Tr}_\ell$ for ℓ dividing n as G_ℓ is generated by σ_ℓ and $\tau\sigma_\ell = \sigma_\ell^{-1}\tau$. Therefore, as $(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell$, then

$$\begin{aligned}(\sigma_\ell - 1)D_\ell\tau &= \tau(\sigma_\ell - 1)D_l \\ &= (\tau\sigma_\ell - \tau)D_\ell \\ &= (\sigma_\ell^{-1}\tau - \tau)D_\ell \\ &= -\sigma_\ell^{-1}(\sigma_\ell - 1)\tau D_\ell,\end{aligned}$$

meaning $(\sigma_\ell - 1)(\sigma_\ell D_\ell \tau + \tau D_\ell) = 0$. However, if $t = \sum_{i=0}^{\ell} b_i \sigma_\ell^i \in \mathbb{Z}[G_\ell]$ such that $(\sigma_\ell - 1)t = 0$, then we must have $b_i = k$ for all $0 \leq i \leq \ell$. Therefore, $\sigma_\ell D_\ell \tau + \tau D_\ell$ must be a multiple of Tr_ℓ. By Proposition 2.2.13, we have $\mathrm{Tr}_\ell P_n \equiv 0 \pmod{pE(K_n)}$ as a_ℓ is divisible by p. Therefore,

$$\tau D_\ell P_n \equiv -\sigma_\ell D_\ell \tau P_n \pmod{pE(K_n)}$$

and so

$$\begin{aligned}\tau Q_n &= \sum_{\sigma \in S} \sigma^{-1} \prod_{\ell | n} \tau D_\ell P_n \\ &\equiv \sum_{\sigma \in S} \sigma^{-1} \prod_{\ell | n} (-\sigma_\ell D_\ell \tau) P_n \pmod{pE(K_n)} \\ &\equiv (-1)^{f_n} \prod_{\ell | n} \sigma_\ell \sum_{\sigma \in S} \sigma^{-1} D_n \tau P_n \pmod{pE(K_n)}\end{aligned}$$

as D_ℓ commutes with σ_ℓ by definition. However, by Proposition 2.2.17, there exists an $\alpha \in H_n$ such that $\tau P_n = \epsilon \cdot \alpha P_n + T$ for some torsion point $T \in E(K_n)$.

Therefore, as $E(K_n)[p] = 0$, then $T \in pE(K_n)$ as T is a torsion point. Therefore

$$\begin{aligned}\tau Q_n &\equiv (-1)^{f_n} \prod_{\ell|n} \sigma_\ell \sum_{\sigma \in S} \sigma^{-1} D_n(\epsilon \cdot \alpha P_n) \pmod{pE(K_n)} \\ &\equiv e_n \prod_{\ell|n} \sigma_\ell \alpha \sum_{\sigma \in S} \sigma^{-1} D_n P_n \pmod{pE(K_n)}.\end{aligned}$$

We have $\prod\limits_{\ell|n} \sigma_\ell \alpha \in H_n$ and $\sum\limits_{\sigma \in S} \sigma^{-1} D_n P_n = Q_n$ by definition. Also,

$$[Q_n] \in (E(K_n)/pE(K_n))^{H_n}$$

so we have

$$\tau Q_n \equiv e_n Q_n \pmod{pE(K_n)}$$

and so the first statement is proved. The second statement follows from the first statement and the commutative diagram earlier. □

We now want to examine whether c_n lies in $\mathrm{Sel}^p(E/K)$. As $d_n = \mathrm{res}_K(c_n)$, then this is equivalent to asking when is d_n locally trivial.

Proposition 2.2.19. *[19, Proposition 6.2]*

1. *The class*

$$d_n \in \ker\Big(\mathrm{res}_\nu : \mathrm{H}^1(K, E)[p] \to \mathrm{H}^1(K_\nu, E)[p]\Big)$$

   when $\nu = \infty$ or ν is a finite place of K such that $\nu \nmid n$.

2. *Let $n = \ell m$ where ℓ is prime and let λ be the unique prime of K dividing ℓ. Then $d_n \in \ker\Big(\mathrm{res}_\lambda : \mathrm{H}^1(K, E)[p] \to \mathrm{H}^1(K_\lambda, E)[p]\Big)$ if and only if $Q_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for all places λ_m of K_m above λ.*

We already know $c_1 \in \mathrm{Sel}^p(E/K)$ as d_1 is globally trivial. We also see for a Kolyvagin prime ℓ that for $c_\ell \in \mathrm{Sel}^p(E/K)$, we only need to check whether d_ℓ is locally trivial in $\mathrm{H}^1(K_\lambda, E)$, which is equivalent to checking whether $P_K \in pE(K_\lambda)$.

We know the conditions for $c_n \in \mathrm{Sel}^p(E/K)$. Before we start to prove Proposition 2.2.8, we require some results in Tate local duality.

2.2.2 Tate Local Duality

We now need to look at some results in Tate local duality that will be required for the proof of Proposition 2.2.8. Throughout this section, let λ be a prime of K. Let K_λ be a local field with ring of integers O_λ such that the finite residue field $\mathbb{F}_\lambda = O_\lambda/\mathfrak{m}$ has characteristic ℓ. We let K_λ^{ur} be the maximal unramified extension of K_λ. Then we have

$$G_\lambda := \mathrm{Gal}(K_\lambda^{ur}/K_\lambda) \cong G_{\mathbb{F}_\lambda}$$

where $G_{\mathbb{F}_\lambda}$ is the absolute Galois group of $\mathbb{F}_\lambda$. We let Fr_λ be the generator of G_λ, the Frobenius automorphism. Let E be an elliptic curve over K_λ with good reduction over O_λ and let $p \neq \ell$ be a prime. We have the following.

Lemma 2.2.20. *We have*

$$E(K_\lambda)/pE(K_\lambda) \cong \mathrm{H}^1(K_\lambda^{ur}/K_\lambda, E[p]).$$

Proof. We have the short exact sequence

$$0 \to E[p] \to E \xrightarrow{[p]} E \to 0$$

which induces

$$0 \to \tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \to \mathrm{H}^1(\mathbb{F}_\lambda, \tilde{E}(\overline{\mathbb{F}}_\lambda)[p]) \to \mathrm{H}^1(\mathbb{F}_\lambda, \tilde{E}(\overline{\mathbb{F}}_\lambda))[p] \to 0$$

where the last term is trivial due to Lang's Theorem. Therefore, we have

$$\tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \cong \mathrm{H}^1(\mathbb{F}_\lambda, \tilde{E}(\overline{\mathbb{F}}_\lambda)[p]).$$

As $\lambda \nmid p$, then the mapping $[p]$ on the formal group associated to E is an isomorphism. Also, as ℓ is a prime of good reduction for E, then we have the isomorphisms

$$\tilde{E}(\overline{\mathbb{F}}_\lambda)[p] \cong E(K_\lambda^{ur})[p] = E[p] \quad \text{and} \quad \tilde{E}(\mathbb{F}_\lambda)/p\tilde{E}(\mathbb{F}_\lambda) \cong E(K_\lambda)/pE(K_\lambda)$$

which gives our result. □

We now recall Tate's Local Duality Theorem.

Theorem 2.2.21 (Tate's Local Duality Theorem)**.** *There exists a symmetric, non-degenerate pairing of* $\mathbb{F}_p$*-vector spaces*

$$\langle , \rangle : \mathrm{H}^1(K_\lambda, E[p]) \times \mathrm{H}^1(K_\lambda, E[p]) \to \mathbb{F}_p.$$

Using this, we would like to prove the following.

Proposition 2.2.22. *[19, Proposition 7.5] The pairing in Theorem* 2.2.21 *induces a non-degenerate pairing of* $\mathbb{F}_p$*-vector spaces*

$$\langle , \rangle : E(K_\lambda)/pE(K_\lambda) \times \mathrm{H}^1(K_\lambda, E)[p] \to \mathbb{F}_p.$$

In order to prove this, we will require the following.

Proposition 2.2.23. *The group* $\mathrm{H}^1(K_\lambda^{ur}/K_\lambda, E[p])$ *is isotropic for the pairing* $\langle , \rangle$ *seen in Theorem* 2.2.21*.*

Proof. This is true as $\mathrm{H}^2(K_\lambda^{ur}/K_\lambda, \mu_p) = 0$ and by the construction of the pairing. □

There exists a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K_\lambda)/pE(K_\lambda) & \longrightarrow & \mathrm{H}^1(K_\lambda, E[p]) & \longrightarrow & \mathrm{H}^1(K_\lambda, E)[p] & \longrightarrow & 0 \\ & & \downarrow & & \cong\downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(K_\lambda, E)[p]^* & \longrightarrow & \mathrm{H}^1(K_\lambda, E[p])^* & \longrightarrow & \Big(E(K_\lambda)/pE(K_\lambda)\Big)^* & \longrightarrow & 0. \end{array}$$

where $*$ represents the Cartier dual. The rows are exact and by Theorem 2.2.21, the middle mapping is an isomorphism. Also, by Lemma 2.2.20 and Proposition 2.2.23, $E(K_\lambda)/pE(K_\lambda)$ is isotropic for the pairing $\langle , \rangle$. Therefore, the first vertical mapping is injective. However, we want to show that this mapping is an isomorphism, which shows that $E(K_\lambda)/pE(K_\lambda)$ is maximal isotropic. This is equivalent to proving the following.

Lemma 2.2.24. $E(K_\lambda)/pE(K_\lambda)$ *and* $\mathrm{H}^1(K_\lambda, E)[p]$ *have the same dimension as* $\mathbb{F}_p$*-vector spaces.*

Proof. As we have the exact sequence

$$0 \to \ker(\mathrm{Fr}_\lambda - 1) \to E[p] \xrightarrow{\mathrm{Fr}_\lambda - 1} E[p] \to E[p]\big/(\mathrm{Fr}_\lambda - 1)E[p] \to 0,$$

then the dimension of $\ker(\mathrm{Fr}_\lambda - 1)$ and $E[p]/(\mathrm{Fr}_\lambda - 1)E[p]$ as $\mathbb{F}_p$-vector spaces must be the same. We also have

$$\ker(\mathrm{Fr}_\lambda - 1) = E[p]^{G_{\mathbb{F}_\lambda}} \cong E[p]^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} = E(K_\lambda)[p]$$

and by [30, Lemma B.2.8],

$$\mathrm{H}^1(K_\lambda^{ur}/K_\lambda, E[p]) \cong E[p]\big/(\mathrm{Fr}_\lambda - 1)E[p].$$

Therefore, we now just need to show $E(K_\lambda)[p]$ and $\mathrm{H}^1(K_\lambda, E)[p]$ have the same dimension by Lemma 2.2.20. We have the following short exact sequence

$$0 \to \mathrm{H}^1(K_\lambda^{ur}/K_\lambda, E[p]) \to \mathrm{H}^1(K_\lambda, E[p]) \to \mathrm{H}^1(I_\lambda, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} \to 0$$

by [30, Lemma 3.2 (ii)] as $\ell \neq p$. We also have the short exact sequence

$$0 \to E(K_\lambda)/pE(K_\lambda) \to \mathrm{H}^1(K_\lambda, E[p]) \to \mathrm{H}^1(K_\lambda, E)[p] \to 0.$$

Therefore, by Lemma 2.2.20 and the two previous short exact sequences, we have

$$\mathrm{H}^1(K_\lambda, E)[p] \cong \mathrm{H}^1(I_\lambda, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)}.$$

However we have

$$\begin{aligned} \mathrm{H}^1(I_\lambda, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} &\cong \mathrm{Hom}(I_\lambda, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} \\ &\cong \mathrm{Hom}({}^{I_\lambda}\!/_{W_\lambda}, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} \\ &\cong \mathrm{Hom}(\mu_p, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)}, \end{aligned}$$

where W_λ is the wild inertia subgroup and μ_p are the p-th roots of unity. The first isomorphism comes from $\ell \neq p$ being a prime of good reduction for E. The second isomorphism comes from the fact that W_λ is a normal Sylow pro-

ℓ-subgroup of I_λ by definition, so $\mathrm{H}^i(W_\lambda, E[p]) = 0$ for all $i > 0$ as $\ell \neq p$. The third isomorphism is because

$$I_\lambda/W_\lambda \cong \prod_{q \neq \ell} \mathbb{Z}_q(1)$$

as a Fr_λ-module. We in fact have

$$\left|\mathrm{Hom}(\mu_p, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)}\right| = \left|E[p]^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)}\right| = |E(K_\lambda)[p]|$$

by the Weil pairing. Therefore, $E(K_\lambda)[p]$ and $\mathrm{H}^1(K_\lambda, E)[p]$ have the same dimension as $\mathbb{F}_p$-vector spaces, which gives the result. □

Therefore, we have

$$E(K_\lambda)/pE(K_\lambda) \cong \mathrm{H}^1(K_\lambda, E)[p]^*$$

and so we have proved Proposition 2.2.22. We have an explicit formula for this pairing when $E(K_\lambda)[p] \cong \mathbb{F}_p^2$. Let $c_1 \in E(K_\lambda)/pE(K_\lambda)$ and construct the point

$$b_1 = \left(\frac{1}{p}c_1\right)^{\mathrm{Fr}_\lambda - 1} \in E(K_\lambda)[p].$$

Take $c_2 \in \mathrm{H}^1(K_\lambda, E)[p]$ and associate the homomorphism $\phi : \mu_p \to E(K_\lambda)[p]$ as we have shown

$$\mathrm{H}^1(K_\lambda, E)[p] \cong \mathrm{Hom}(\mu[p], E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)}.$$

Fix a primitive p-th root of unity in K_λ, denoted θ, and let $b_2 = \phi(\theta)$. Then

$$\theta^{\langle c_1, c_2 \rangle} = e_p(b_1, b_2)$$

where $e_p : E[p] \times E[p] \to \mu_p$ denotes the Weil pairing. We now have the required tools from Tate local duality.

2.2.3 Calculation of the Selmer Group

We will now prove Proposition 2.2.8 by applying the knowledge in the previous part. We have seen earlier that if λ is the unique prime of K above ℓ, then

$\tilde{E}(\mathbb{F}_\lambda)[p] \cong \mathbb{F}_\ell^2$. Also, as $\ell \neq p$ is a prime of good reduction for E by definition, then $E(K_\lambda)[p] \cong \tilde{E}(\mathbb{F}_\lambda)[p]$ and

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(K_\lambda/\mathbb{Q}_l) = \{1, \tau\}$$

acts on the $\mathbb{F}_p$-vector spaces $E(K_\lambda)/pE(K_\lambda)$ and $\mathrm{H}^1(K_\lambda, E)[p]$.

In this case, the pairing in Proposition 2.2.22 is working with $\mathbb{F}_p$-vector spaces of dimension 2. We would like to work with $\mathbb{F}_p$-vector spaces of dimension 1. We have $E(K_\lambda)[p]^\pm \cong \mathbb{F}_p$ by Proposition 2.2.11. We in fact have a similar relationship associated to $E(K_\lambda)/pE(K_\lambda)$ and $\mathrm{H}^1(K_\lambda, E)[p]$.

Proposition 2.2.25. *[19, Proposition 8.1 (1)] The eigenspaces*

$$(E(K_\lambda)/pE(K_\lambda))^\pm$$

and $\mathrm{H}^1(K_\lambda, E)[p]^\pm$ *for* $\mathrm{Gal}(K_\lambda/\mathbb{Q}_l)$ *each have dimension* 1 *over* $\mathbb{F}_p$.

Proof. As seen in the proof of Lemma 2.2.24, we have the short exact sequences

$$0 \to \mathrm{H}^1(K_\lambda^{ur}/K_\lambda, E[p]) \to \mathrm{H}^1(K_\lambda, E[p]) \to \mathrm{H}^1(I_\lambda, E[p])^{\mathrm{Gal}(K_\lambda^{ur}/K_\lambda)} \to 0$$

and

$$0 \to E(K_\lambda)/pE(K_\lambda) \to \mathrm{H}^1(K_\lambda, E[p]) \to \mathrm{H}^1(K_\lambda, E)[p] \to 0.$$

Therefore, as $\mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell)$-modules and by Lemma 2.2.20, we have

$$E(K_\lambda)/pE(K_\lambda) \cong E(K_\lambda)[p] \quad \text{and} \quad \mathrm{H}^1(K_\lambda, E)[p] \cong \mathrm{Hom}(\mu_p(K_\lambda), E[p]).$$

As p divides $\ell + 1$ and p is odd, so p doesn't divide $\ell - 1$, then $\mu_p(\mathbb{Q}_\ell) = \{1\}$ and so

$$\mu(K_\lambda) = \mu(K_\lambda)^-$$

and so

$$\mathrm{H}^1(K_\lambda, E)[p]^\pm \cong \mathrm{Hom}(\mu_p(K_\lambda), E[p])^\pm \cong E(K_\lambda)[p]^\mp.$$

They both have dimension 1 by Proposition 2.2.11. □

Using this and Proposition 2.2.22, we have the following.

Proposition 2.2.26. *[19, Proposition 8.1 (2)] The pairing in Proposition* 2.2.22 *induces a non-degenerate pairing of* $\mathbb{F}_p$*-vector spaces*

$$\langle , \rangle^{\pm} : \Big(E(K_\lambda)/pE(K_\lambda)\Big)^{\pm} \times \mathrm{H}^1(K_\lambda, E)[p]^{\pm} \to \mathbb{F}_p.$$

Proof. We just need to show that the $+$ and $-$ eigenspaces for τ are orthogonal under τ. A known result is that τ acts trivially on $\mathrm{H}^2(K_\lambda, \mu_p) \cong \mathbb{F}_p$, so by Tate's pairing, we have

$$\langle a^\tau, b^\tau \rangle = \langle a, b \rangle^\tau = \langle a, b \rangle$$

which provides the result. □

Therefore, we can use this to prove the following.

Proposition 2.2.27. *[19, Proposition 8.2] Assume a class* $d \in \mathrm{H}^1(K, E)[p]^{\pm}$ *is locally trivial at all places* $\nu \neq \lambda$*, but* $d_\lambda \neq 0$ *in* $\mathrm{H}^1(K_\lambda, E)[p]^{\pm}$*. Then for any class* $s \in \mathrm{Sel}^p(E/K)^{\pm}$*, we have* $s_\lambda = 0$ *in* $\mathrm{H}^1(K_\lambda, E[p])^{\pm}$*.*

Proof. (Sketch) As $s \in \mathrm{Sel}^p(E/K)^{\pm}$, then s_λ lies in the image of the mapping

$$\Big(E(K_\lambda)/pE(K_\lambda)\Big)^{\pm} \to \mathrm{H}^1(K_\lambda, E[p])^{\pm}.$$

Let us denote this element as P_λ. Then if $\langle P_\lambda, d_\lambda \rangle = 0$, then we must have $P_\lambda = 0$ and hence $s_\lambda = 0$. This pairing can be shown to be trivial using the local components of the Brauer group. □

We now want to use the classes $d_n \in \mathrm{H}^1(K, E)[p]$ constructed earlier to bound the order of $\mathrm{Sel}^p(E/K)$. We first look at the Galois groups associated to K. We know that if we let $L := K(E[p])$, then we have

$$\mathcal{G} := \mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

as seen in the proof of Lemma 2.2.7 and as p is a descent prime.

Proposition 2.2.28. *[19, Proposition 9.1] For all* $n \geq 0$*, we have*

$$\mathrm{H}^n(\mathcal{G}, E[p]) = 0$$

and we have the isomorphism

$$\mathrm{res} : \mathrm{H}^1(K, E[p]) \xrightarrow{\sim} \mathrm{H}^1(L, E[p])^{\mathcal{G}} = \mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\overline{\mathbb{Q}}/L), E[p]).$$

Proof. We know $\mathcal{G}$ has centre $Z_p \cong \mathbb{F}_p^\times$. As p is odd and $Z_p \neq 1$, then $E[p]^{Z_p} = 0$. Also, as $p-1$ is prime to p, then $\mathrm{H}^i(Z_p, E[p]) = 0$ for all $i \geq 1$. We then use the Hochshild-Serre Spectral Sequence with

$$\mathrm{H}^m(\mathcal{G}/Z_p, \mathrm{H}^n(Z_p, E[p])) \Rightarrow \mathrm{H}^{m+n}(\mathcal{G}, E[p])$$

to see that $\mathrm{H}^n(\mathcal{G}, E[p]) = 0$ for all $n \geq 0$ by [28, Lemma 2.1.4]. Also, the isomorphism is due to the Inflation-Restriction sequence as $\mathrm{H}^n(\mathcal{G}, E[p]) = 0$ for $n \in \{1, 2\}$. Finally, the equality sign is due to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ acting trivially on $E[p]$. □

This proposition implies that there exists a pairing

$$[,] : \mathrm{H}^1(K, E[p]) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \to E[p]$$

where $[s, \rho] = s(\rho)$. If $\sigma \in \mathcal{G}$, then $[s, \rho^\sigma] = [s, \rho]^\sigma$ for all $s \in \mathrm{H}^1(K, E[p])$ and $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$. Also, if $[s, \rho] = 0$ for all $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, then s is the zero map when restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and so $s = 0$ in $\mathrm{H}^1(K, E[p])$ by the isomorphism in Proposition 2.2.28.

Now, let $S \subset \mathrm{H}^1(K, E[p])$ be a finite subgroup. Let

$$\mathrm{Gal}_S(\overline{\mathbb{Q}}/L) = \{\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) : \ [s, \rho] = 0 \text{ for all } s \in S\}$$

and let $M := L^S$ be the fixed field of $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$. Then M is a finite normal extension of L with Galois group $H := \mathrm{Gal}(M/L)$. Then it can be shown that we have the following.

Proposition 2.2.29. *[19, Proposition 9.3] There is an induced pairing*

$$[,] : S \times H \to E[p]$$

which is non-degenerate and induces an isomorphism of $\mathcal{G}$-modules

$$H \cong \mathrm{Hom}(S, E[p])$$

as well as an isomorphism of $\mathrm{Gal}(K/\mathbb{Q})$*-modules*

$$S \cong \mathrm{Hom}_{\mathcal{G}}(H, E[p]).$$

Proof. If we look at the mapping

$$H \hookrightarrow \mathrm{Hom}(S, E[p])$$

where $\rho \mapsto t_\rho$ with $t_\rho(s) = [s, \rho]$, then this is a well-defined injective $\mathcal{G}$-homomorphism by definition of M and by the isomorphism in Proposition 2.2.28. Similarly, there is an injection

$$S \hookrightarrow \mathrm{Hom}_{\mathcal{G}}(H, E[p]).$$

We just want to show that these mappings are isomorphisms. Let $r = \dim_{\mathbb{F}_p}(S)$ as an $\mathbb{F}_p$-vector space. We know $E[p]$ is a simple $\mathcal{G}$-module as if it weren't, there would exist an $\mathbb{F}_p[\mathcal{G}]$-submodule of $E[p]$ generated by the point P and such that $\sigma(P)$ is a multiple of P for all $\sigma \in \mathcal{G}$. This contradicts that $\mathcal{G} \cong \mathrm{GL}_2(\mathbb{F}_p)$.

In particular, we know that $\mathrm{Hom}(S, E[p]) \cong E[p]^r$. Therefore, as $E[p]^r$ is semisimple, then H is a semisimple $\mathcal{G}$-module and by the injective mapping, we must have $H \cong E[p]^s$ for some $s \leq r$. In particular, we have $\mathrm{Hom}_{\mathcal{G}}(S, E[p]) \cong \mathbb{F}_p^s$. However, we have shown that S injects into this group. Hence $s = r$ and we have our result. □

We would like to apply Proposition 2.2.29 to $S = \mathrm{Sel}^p(E/K)$. We assume that $P_K \in E(K)$ has infinite order and is not divisible by p in $E(K)$. Also, let $c_1 = \kappa[P_K]$ be its nonzero image in $\mathrm{Sel}^p(E/K)$. We let $I \leq H$ which fixes $L\left(\frac{1}{p}P_K\right)$. By Proposition 2.2.29, we have

$$H \cong \mathrm{Hom}(\mathrm{Sel}^p(E/K), E[p]).$$

We also see by Proposition 2.2.29 with $S = \langle c_1 \rangle$ that $L^S = L\left(\frac{1}{p}P_K\right)$ and so

$$H/I \cong \mathrm{Gal}\left(L\left(\tfrac{1}{p}P_K\right)/L\right) \cong \mathrm{Hom}(S, E[p]) \cong E[p]$$

as $\dim_{\mathbb{F}_p}(S) = 1$ in this case. Let τ be a fixed lifting of complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$ and let

$$H^+ = \{\sigma \in H : \ \sigma^\tau = \sigma\}$$

and similarly for I^+.

Proposition 2.2.30. *[19, Proposition 9.5]*

1. *We have* $H^+ = \{(\tau h)^2 : h \in H\}$, $I^+ = \{(\tau i)^2 : i \in I\}$ *and* $H^+/I^+ \cong \mathbb{F}_p$.
2. *Let* $s \in \mathrm{Sel}^p(E/K)^{\pm}$. *Then the following are equivalent:*
   - *a)* $[s, f] = 0$ *for all* $f \in H$,
   - *b)* $[s, f] = 0$ *for all* $f \in H^+$,
   - *c)* $[s, f] = 0$ *for all* $f \in H^+ \backslash I^+$,
   - *d)* $s = 0$.

Proof. We initially prove part 1. Let $H^{\tau+1} = \{h^\tau \cdot h : h \in H\}$. As $\tau^2 - 1 = 0$, then for $h \in H^{\tau+1}$, we have

$$h^{\tau-1} = g^{\tau^2-1} = \mathrm{id}$$

for some $g \in H$, meaning $H^{\tau+1} \subseteq H^+$. Also, as p is odd and H is an $\mathbb{F}_p$-vector space, then 2 is an automorphism of H. Hence, for $h \in H^+$, then $h = (h^{1/2})^{\tau+1} \in H^{\tau+1}$. Therefore, we have $H^+ = H^{\tau+1}$. However, as $\tau^{-1} = \tau$, then

$$h^{\tau+1} = \tau h \tau^{-1} h = (\tau h)^2$$

which proves the equality. It is similarly shown for I^+. Also,

$$H^+/I^+ = (H/I)^+ = E[p]^+ \cong \mathbb{F}_p.$$

For part 2, it is clear that $a \Rightarrow b \Rightarrow c$ and $a \Leftrightarrow d$ by Proposition 2.2.29. Therefore, we just need to show $c \Rightarrow a$.

Let $s \in \mathrm{Sel}^p(E/K)^{\pm}$. As we have an isomorphism

$$\mathrm{Sel}^p(E/K) \cong \mathrm{Hom}_{\mathcal{G}}(H, E[p]),$$

then we can induce a $\mathcal{G}$-homomorphism $s : H \to E[p]$ such that $s(H^+) \subseteq E[p]^{\pm}$ and $s(H^-) \subseteq E[p]^{\mp}$. We have seen that $E[p]$ is a simple $\mathcal{G}$-module, so we must have $\mathrm{im}(s) \in \{0, E[p]\}$. If we suppose c is true, then as $H^+ \backslash I^+ \neq 0$ and

$$s(H^+) \subseteq E[p]^{\pm} \cong \mathbb{F}_p,$$

we must have $s(H^+) = 0$. As $s(H^-) \subseteq E[p]^{\mp}$, $\mathrm{im}(s) \neq E[p]$ and so $\mathrm{im}(s) = 0$. Therefore, we have shown $c \Rightarrow a$. □

Now, let λ be a prime of K that doesn't divide pN. Then λ is unramified in M/K. Let λ_M be a prime above λ of M. Assume λ splits completely in L/K. Let Fr_{λ_M} denote the Frobenius element of λ_M in $\mathrm{Gal}(M/K)$. As λ splits completely in L/K, then $\mathrm{Fr}_{\lambda_M} \in H$ and its $\mathcal{G}$-orbit only depends on λ. Therefore, we denote this conjugacy class as Frob_λ.

Proposition 2.2.31. *[19, Proposition 9.6] For $s \in \mathrm{Sel}^p(E/K)$, the following are equivalent:*

1. $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$ *where* $\mathrm{Fr}_{\lambda_M/\lambda}$ *is the Frobenius element of* λ_M *in* H,
2. $[s, \rho] = 0$ *for all* $\rho \in \mathrm{Frob}_\lambda$,
3. $s_\lambda = 0$ *in* $\mathrm{H}^1(K_\lambda, E[p])$.

Proof. We have seen that $[s, \rho^\sigma] = [s, \rho]^\sigma$ for all $\sigma \in \mathcal{G}$, which implies that (1) and (2) are equivalent.

Let $P_\lambda \in E(K_\lambda)/pE(K_\lambda)$ be such that it has image $s_\lambda \in \mathrm{H}^1(K_\lambda, E[p])$. Then by definition, we have $\frac{1}{p}P_\lambda \in E(M_{\lambda_M})$. We have

$$[s, \mathrm{Fr}_{\lambda_M/\lambda}] = \mathrm{Fr}_{\lambda_M/\lambda}\left(\tfrac{1}{p}P_\lambda\right) - \tfrac{1}{p}P_\lambda \in E(M_{\lambda_M})[p] \cong E(M)[p].$$

Therefore, $[s, \mathrm{Fr}_{\lambda_M/\lambda}] = 0$ if and only if $P_\lambda \in pE(K_\lambda)$ if and only if $s_\lambda = 0$. □

We can finally look at the proof of Proposition 2.2.8. Recall that P_K lies in the $e_1 = \epsilon$ eigenspace for τ in $E(K)/pE(K)$ by Proposition 2.2.18. Therefore,

$\kappa[P_K] = c_1 \in \mathrm{Sel}^p(E/K)^\epsilon$. Therefore, in order to prove Proposition 2.2.8, we initially want to show the following.

Proposition 2.2.32. *[19, Claim 10.1] We have* $\mathrm{Sel}^p(E/K)^{-\epsilon} = 0$.

Proof. Let $s \in \mathrm{Sel}^p(E/K)^{-\epsilon}$. We want to show $s = 0$ in $\mathrm{Sel}^p(E/K)^{-\epsilon}$. To do this, by Proposition 2.2.30, we want to show for all $\rho \in H^+\backslash I^+$, we have $[s, \rho] = 0$. We have seen that every element in H^+ takes the form $(\tau h)^2$ for some $h \in H$ by Proposition 2.2.30.

Let ℓ be a prime such that it is unramified in $M/\mathbb{Q}$ and such that there exists a prime λ_M of M above ℓ such that its Frobenius element is equal to τh for some $h \in H$. We can always find such an ℓ due to Chebotarev's density theorem. Then $\lambda \mid \ell$ is inert in K and splits completely in L. Also, $\mathrm{Fr}_{\lambda_M/\lambda}$ is $(\tau h)^2$, so by Proposition 2.2.31, we just need to show $s_\lambda = 0$ in $\mathrm{H}^1(K_\lambda, E[p])$.

We know that $c_\ell \in \mathrm{H}^1(K, E[p])^{-\epsilon}$ and $d_\ell \in \mathrm{H}^1(K, E)[p]^{-\epsilon}$ by Proposition 2.2.18. By Proposition 2.2.19, d_ℓ is locally trivial at all primes except λ. By Proposition 2.2.19, we see that $(d_\ell)_\lambda$ is trivial if and only if $P_K \in pE(K_\lambda)$. This is equivalent to λ splitting completely in $L\left(\frac{1}{p}P_K\right)$. Since $\mathrm{Fr}_{\lambda_M/\lambda} = \rho$ is not in I^+ by hypothesis, then this splitting doesn't occur. Therefore, $(d_\ell)_\lambda \neq 0$ in $\mathrm{H}^1(K_\lambda, E)[p]$ and by Proposition 2.2.27, $s_\lambda = 0$ in $\mathrm{H}^1(K_\lambda, E[p])$. □

We can in fact put together some of the previous results to obtain the following.

Proposition 2.2.33. *[19, Proposition 10.2] Assume P_K is not divisible by p in $E(K)$. Let ℓ be a prime unramified in the extension $M/\mathbb{Q}$ and such that there exists a prime $\lambda_M \mid \ell$ of M whose Frobenius element equals τh in* $\mathrm{Gal}(M/\mathbb{Q})$ *for some $h \in H$. Then the prime λ of K above ℓ is inert, λ splits completely in L and the following are equivalent:*

1. $c_\ell = 0$ *in* $\mathrm{H}^1(K, E[p])$,
2. $c_\ell \in \mathrm{Sel}^p(E/K)$,
3. $Q_\ell \in pE(K_\ell)$,
4. $d_\ell = 0$ *in* $\mathrm{H}^1(K, E)[p]$,
5. d_ℓ *is locally trivial at* λ,

6. $P_K \in pE(K_\lambda)$,

7. $h^{\tau+1} \in I^+$.

Proof. By definition of $\mathrm{Sel}^p(E/K)$, we have $1 \Rightarrow 2$. For the other implication, by Proposition 2.2.18, we have $c_\ell \in \mathrm{H}^1(K, E[p])^{-\epsilon}$ and so

$$c_\ell \in \mathrm{Sel}^p(E/K)^{-\epsilon} = 0$$

by Proposition 2.2.32. Therefore, we have $1 \Leftrightarrow 2$.

We have $1 \Leftrightarrow 3$ by Proposition 2.2.16. By Proposition 2.2.32, we must have $\Big(E(K)/pE(K)\Big)^{-\epsilon} = 0$ and so $\mathrm{H}^1(K, E[p])^{-\epsilon}$ injects into $\mathrm{H}^1(K, E)[p]$. Therefore, as $d_\ell = \mathrm{res}_K(c_\ell)$, then $1 \Leftrightarrow 4$.

We have $4 \Rightarrow 5$. On the other hand, we have seen that d_ℓ is locally trivial except possibly at λ by Proposition 2.2.19. Therefore, if d_ℓ is locally trivial at λ, then $d_\ell \in Ш(E/K)[p]^{-\epsilon} = 0$ by Proposition 2.2.32. Hence, we must have $5 \Rightarrow 4$. Also, $5 \Leftrightarrow 6$ by Proposition 2.2.19 as $P_K = Q_1$.

Finally, $P_K \in pE(K_\lambda)$ is equivalent to λ splitting completely in $L\Big(\frac{1}{p}P_K\Big)/K$, which is equivalent to the Frobenius substitution of the prime λ_M above λ in M/K lying in I^+. However, $(\tau h)^2 = h^{\tau+1}$, so $6 \Leftrightarrow 7$. □

In particular, this proposition shows that for such primes, if c_ℓ is non-trivial in $\mathrm{H}^1(K, E[p])$, then it cannot lie in $\mathrm{Sel}^p(E/K)$, which reduces the size of the Selmer group. Therefore, by Proposition 2.2.32, to finish the proof of Proposition 2.2.8, we just need the following.

Proposition 2.2.34. *[19, Claim 10.3] We have*

$$\mathrm{Sel}^p(E/K)^\epsilon \cong \mathbb{F}_p \cdot \kappa[P_K].$$

Proof. We have seen that $H/I \cong E[p]$. This was shown when using Proposition 2.2.29 for $S = \langle c_1 \rangle$ where $c_1 = \kappa[P_K]$. Also by Proposition 2.2.29, this implies that

$$\langle c_1 \rangle \cong \mathrm{Hom}_{\mathcal{G}}(H/I, E[p]) \cong \mathbb{F}_p.$$

Therefore,

$$\mathrm{Hom}_{\mathcal{G}}(H/I, E[p]) \cong \mathbb{F}_p \cdot c_1.$$

Let $s \in \mathrm{Sel}^p(E/K)^\epsilon$. We will show that $[s, \rho] = 0$ for all $\rho \in I^+$ as if this is true, $s(I) = s(I^-) \subseteq E[p]^{-\epsilon} \cong \mathbb{F}_p$ and so $s(I) = 0$ as $E[p]$ is a simple $\mathcal{G}$-module. Therefore, we may restrict s to H/I and so

$$s \in \mathrm{Hom}_{\mathcal{G}}(H/I, E[p]) \cong \mathbb{F}_p \cdot c_1.$$

We have seen by Proposition 2.2.30 that all elements of I^+ have the form $(\tau i)^2$ for some $i \in I$.

Let q be a prime such that its Frobenius element lies in the conjugacy class of τh in $\mathrm{Gal}(M/\mathbb{Q})$ where $h \in H$ and $h^{\tau+1} \notin I^+$. Then $c_q \neq 0$ in $\mathrm{H}^1(K, E[p])$ and $c_q \notin \mathrm{Sel}^p(E/K)$ by Proposition 2.2.33. Therefore, we let $S' = \langle c_q \rangle$. Then by the construction as seen in Proposition 2.2.29, as $E[p]$ is a simple $\mathcal{G}$-module, we have $L' \cap M = L$ where $L' = L\left(\frac{1}{p}Q_q\right)$. A prime λ of K above a prime ℓ, which is inert in $K/\mathbb{Q}$ and splits completely in L, splits completely in L' if and only if $Q_q \in pE(L'_\gamma) = pE(K_\lambda)$ for all primes γ of L' above λ.

Let ℓ be a prime whose Frobenius element is conjugate to τi in $\mathrm{Gal}(M/\mathbb{Q})$ for some $i \in I$ and conjugate to τj in $\mathrm{Gal}(L'/\mathbb{Q})$ for some $j \in \mathrm{Gal}(L'/L)$ such that $j^{\tau+1} \neq 1$. These conditions can be satisfied due to $M \cap L' = L$. We will show $d_{\ell q} \in \mathrm{H}^1(K, E)^\epsilon$ is locally trivial for all places $\nu \neq \lambda$ but $d_{\ell q}$ is not locally trivial in $\mathrm{H}^1(K_\lambda, E)$.

We know $d_{\ell q}$ is locally trivial for places $\nu \nmid \ell q$ by Proposition 2.2.19. By Proposition 2.2.30, as $i \in I$, then $i^{\tau+1} \in I^{\tau+1} = I^+$. Therefore, $c_\ell = 0$ in $\mathrm{H}^1(K, E[p])$ by Proposition 2.2.33 and $Q_\ell \in pE(K_\ell)$. Therefore, Q_ℓ is locally divisible by p in the completion at a place dividing the prime $\mathfrak{q}$ above q in K. Hence, by Proposition 2.2.19, $d_{\ell q}$ is locally trivial in $\mathrm{H}^1(K_\mathfrak{q}, E)$. Finally, $d_{\ell q}$ is locally trivial in $\mathrm{H}^1(K_\lambda, E)$ if and only if $Q_q \in pE(K_\lambda)$. But then λ splits in L' and so $j^{\tau+1} = 1$, which is a contradiction. Therefore, by Proposition 2.2.27, we have $s_\lambda = 0$ in $\mathrm{H}^1(K_\lambda, E[p])$ and so $[s, (\tau i)^2] = 0$. As this argument works by choosing ℓ accordingly and as $I^+ = \{(\tau i)^2 : i \in I\}$, we have $s(I^+) = 0$. $\square$

Therefore, we have provided a summary of the proof of Proposition 2.2.8 and therefore Proposition 2.2.5. We have shown that Kolyvagin used Heegner points on elliptic curves to create cohomology classes. Of these classes, if ℓ is a Kolyvagin prime associated to (E, K, p) such that c_ℓ is non-trivial, then they lie outside $\mathrm{Sel}^p(E/K)$ by Proposition 2.2.33, restricting its size. The class c_1

however is non-trivial and lies in $\text{Sel}^p(E/K)$ as the class d_1 is trivial by Proposition 2.2.16. In particular, by Proposition 2.2.32 and Proposition 2.2.34, c_1 generates $\text{Sel}^p(E/K)$, which lies in the image of the Kummer map rather than a lift of a non-trivial element in the Shafarevich-Tate group.

This construction works due to the Galois groups $\text{Gal}(K_\ell/K)$ being abelian and the Chebotarev Density Theorem. Using these, we can vary the Kolyvagin prime ℓ such that we can create the cohomology class c_ℓ which are non-trivial and lie outside $\text{Sel}^p(E/K)$, hence bounding its size. We will now look at a different type of modular point and show how we can follow a similar method of creating derivative classes to bound certain Selmer groups. However, unlike the Heegner point case, the derivative classes constructed will be shown to lie inside the Selmer group, hence we bound the Selmer group from below rather than above.

2.3 Self Points

We now provide a summary of an analogue system to Kolyvagin's work devised by Wuthrich in [39]. This will be looked at in more detail in Chapter 4 when we look at a generalised construction.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. We have seen that there is a surjective morphism

$$\Phi_E : X_0(N) \to E$$

where we can view the subvariety $Y_0(N)$ of $X_0(N)$ as a moduli space of the set of pairs (A, C) where A is an elliptic curve and C is a cyclic subgroup in A of order N. We can now define a self point as defined on [39, pg. 283].

Definition 2.3.1. *Let $x_C = (E, C) \in X_0(N)$. Then the point*

$$P_C = \Phi_E(x_C) \in E(\mathbb{Q}(C))$$

is defined as a self point on E.

We see in [23, Theorem 6.6.1] that the number of such subgroups of order N is equal to

$$N \prod_{\substack{p|N \\ \text{prime}}} \left(1 + {}^1\!/_p\right),$$

which is the number of elements in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and in turn is the number of self points.

We denote the field of compositum of all such $\mathbb{Q}(C)$ as K_N. If we let $\{P, Q\}$ be a basis of $E[N]$, we see that if $\sigma \in G_{K_N}$, then $P^\sigma = aP$ and $Q^\sigma = bQ$ for some $a, b \in \mathbb{Z}$. We also see that $(P+Q)^\sigma = c(P+Q)$ for some $c \in \mathbb{Z}$, so

$$aP + bQ = P^\sigma + Q^\sigma = (P+Q)^\sigma = cP + cQ.$$

Therefore,

$$bQ = (c-a)P + cQ$$

which means $a = b = c$. Therefore, as K_N is the field of definition for all cyclic subgroups in E of order N, then it is the smallest field K such that G_K acts by scalars on $E[N]$. This has Galois group $G_N := \mathrm{Gal}(K_N/\mathbb{Q})$ which can be identified as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ via the mapping $\overline{\tau}_{\mathbb{Q},E,N}$.

For $\sigma \in G_{\mathbb{Q}}$, we have $P_C^\sigma = P_{C^\sigma}$. We refer the readers to [31, Section 2.4] to see how this is proved, but we give a very brief explanation here. We let $X(N)$ be the modular curve as defined on [14, pg. 58]. Then by [31, Definition 2.20], there exists a functor $M(N)$ from the set of schemes over $\mathbb{Q}$ such that

$$M(N)(T) = \left\{ \begin{array}{c} \text{Isomorphism classes of pairs } (E, \alpha) \text{ where } E \text{ is} \\ \text{an elliptic curve over } T \text{ and } \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N] \\ \text{is an isomorphism of group schemes} \end{array} \right\}.$$

In particular, for any morphism of schemes $f : T \to T'$ over $\mathbb{Q}$, there exists a mapping $f^* : M(N)(T') \to M(N)(T)$ such that

$$f^*[(E, \alpha)] = [(E \times_{T'} T, \alpha_T)].$$

Therefore, for $\sigma \in G_{\mathbb{Q}}$, this is precisely $[(E, \alpha)]^\sigma = [(E, \alpha^\sigma)]$. By [31, Theorem 2.21], the curve $X(N)/\mathbb{Q}$ is a fine moduli space for the functor $M(N)$. This means that there exists a corresponding mapping $X(N)(T) \to X(N)(T')$ and

all such maps together for $\sigma \in G_{\mathbb{Q}}$ define an action of $G_{\mathbb{Q}}$ on $X(N)$, which corresponds to the action on the torsion points.

However, we want to look at this for the $X_0(N)$ case, which is not a fine moduli space but a coarse moduli space defined by the quotient of $X(N)$ by a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as seen in [31, Proposition 2.23]. Therefore, [31, Lemma 2.27] says that we can follow the same procedure for $X_0(N)$ as $X(N)$ above to define an action of $G_{\mathbb{Q}}$ on $X_0(N)$, which corresponds to the action on the torsion points. In particular, as there exists the subvariety $Y_0(N)$ as seen above, this corresponds to the action $x_C^\sigma = x_{C^\sigma}$ for all $\sigma \in G_{\mathbb{Q}}$. Therefore, $P_C^\sigma = P_{C^\sigma}$.

We want to follow the methods of Kolyvagin by using self points to bound Selmer groups of elliptic curves over certain fields. As with the construction of Heegner points, we would like to know the conditions for which the self points are of infinite order.

Theorem 2.3.2. *[39, Theorem 5] Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Suppose $j(E) \notin \frac{1}{2}\mathbb{Z}$. Then there exists at least one self point P_C of infinite order in $E(K_N)$.*

We also see that there exist relationships between the self points.

Proposition 2.3.3. *[39, Proposition 7] Let $d \neq N$ be an integer such that $d|N$. Then we have the relations*

$$\sum_{C \supset B} P_C \text{ is torsion in } E(K_d)$$

where B is a cyclic subgroup of order d and the sum is taken over all cyclic subgroups C of E of order N containing B. In particular, if $d = 1$, then the sum of all self points is a torsion point in $E(\mathbb{Q})$.

We will use this result to understand the group generated by the self points by reformulating these relations using irreducible representations of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. We define

$$V_N := \mathbb{Q}_p\Big[{}^{\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})}/_B\Big].$$

This is the $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module induced from a Borel subgroup B of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. We can view

$$V_N = \bigoplus_{C \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} \mathbb{Q}_p e_C$$

where $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ by permuting the basis. Here e_C denotes the characteristic function on $C \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. We would like to understand how this module splits as a $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module.

Theorem 2.3.4. *[39, Theorem 8] The $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module V_N decomposes into a direct sum of irreducible $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-modules*

$$V_N = \bigoplus_{D|N} W_D$$

where D runs through all divisors of N and W_D has dimension $\delta(D)$ as a $\mathbb{Q}_p$-vector space. Here, if we let $D = \prod_{p|D} p^{d_p}$ be the prime decomposition of D, then $\delta(D) = \prod_{p|D} \delta(p)$ where

$$\delta(p) = \begin{cases} 1 & \text{if } d_p = 0, \\ p & \text{if } d_p = 1, \\ p^{d_p} - p^{d_p - 2} & \text{if } d_p > 1. \end{cases}$$

Proof. We shall split this proof into three cases. The first case will be when $N = p$ is prime. Then $V_p = \mathbb{Q}_p\left[{}^{\mathcal{G}_0}/_B\right]$ is a $\mathbb{Q}_p[\mathcal{G}_0]$-module of dimension $p+1$ as a $\mathbb{Q}_p$-vector space which decomposes as

$$V_p = W_1 \oplus W_p.$$

Here, W_1 is the trivial $\mathbb{Q}_p[\mathcal{G}_0]$-module and

$$W_p = \left\{ f : \mathbb{P}^1_0 \to \mathbb{Q}_p : \sum_C f(C) = 0 \right\}$$

is an irreducible $\mathbb{Q}_p[\mathcal{G}_0]$-module of dimension p as a $\mathbb{Q}_p$-vector space called the Steinberg representation, as seen in [18, Section 7.2].

The second case we look at is if N is a prime power, say $N = p^{n+1}$ for $n \geq 1$. We see in [18, Section 7.3] that we have

$$V_{p^{n+1}} \cong V_{p^n} \oplus W_{p^{n+1}}$$

where we view the summand as a representation of $\mathcal{G}_n$ via the reduction mapping $\mathcal{G}_n \to \mathcal{G}_{n-1}$. Here, $W_{p^{n+1}}$ is an irreducible $\mathbb{Q}_p[\mathcal{G}_n]$-module of dimension $p^{n+1} - p^{n-1}$ as a $\mathbb{Q}_p$-vector space and can be viewed as

$$W_{p^{n+1}} = \left\{ f : \mathbb{P}^1_n \to \mathbb{Q}_p : \sum_{C \supset C'} f(C) = 0 \text{ for all } C' \in \mathbb{P}^1_{n-1} \right\}.$$

Finally, the case for general N, we assume N is not a prime power and has prime decomposition $N = \prod_{p|N} p^{a_p}$. Then we have

$$\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathrm{PGL}_2(\mathbb{Z}/p^{a_p}\mathbb{Z})$$

by the Chinese remainder theorem. We also have

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathbb{P}^1(\mathbb{Z}/p^{a_p}\mathbb{Z})$$

similarly and so

$$V_N = \bigotimes_{p|N} V_{p^{a_p}}$$

as a $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module. Therefore, we have

$$V_N = \bigotimes_{p|N} \bigoplus_{i=0}^{a_p} W_{p^i}.$$

In particular, if D is a divisor of N with prime factorisation $D = \prod_{p|D} p^{d_p}$, then we define

$$W_D = \bigotimes_{p|D} W_{p^{d_p}}.$$

Then by the representation theory of direct products, W_D is irreducible as a $\mathbb{Q}_p[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module with dimension $\delta(D)$ as a $\mathbb{Q}_p$-vector space. This shows that

$$V_N = \bigoplus_{D|N} W_D. \qquad \square$$

Now, we are able to construct a G_N-equivariant map

$$l_N : V_N \to E(K_N) \otimes \mathbb{Q}_p$$

where $e_C \mapsto P_C$. Due to the relationship stated in Proposition 2.3.3, the kernel of l_N contains all the submodules W_d where $d|N$ and $d \neq N$. So this induces

$$W_N \to E(K_N) \otimes \mathbb{Q}_p$$

where W_N is the Steinberg representation. This leads to the following corollary.

Corollary 2.3.5. *[39, Corollary 10] The self points generate a group of rank at most $\delta(N)$ inside $E(K_N)$. If W_N is an irreducible $\mathbb{Q}_p[G_N]$-module and $j(E) \notin \frac{1}{2}\mathbb{Z}$, then the self points generate a group of rank $\delta(N)$ and the Galois group acts like the Steinberg representation W_N on it.*

We now wish to extend the construction of self points.

Definition 2.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with cyclic subgroup C of order N. Let $E'/\mathbb{Q}$ be an elliptic curve isogenous to E over $\overline{\mathbb{Q}}$ with isogeny $\psi : E \to E'$. Then $\Phi_E(E', \psi(C))$ is called a higher self point above P_C.*

In particular, if we let D be a cyclic subgroup in E with isogeny $\psi : E \to E/D$ associated to it, then for any cyclic subgroup C of order N in E, we can define a higher self point

$$\Phi_E(E/D, \psi(C)) \in E(\mathbb{Q}(C, D)).$$

We focus on two cases of construction of higher self points. Firstly, we will look at the construction when p is a prime of multiplicative reduction for E and then look at when p is a prime of good ordinary reduction for E.

For the multiplicative case, let E be an elliptic curve of conductor N which has multiplicative reduction at a prime p. Let $N = pM$ where $(p, M) = 1$. If we let $F := K_M$ and $F_n := K_{p^{n+1}M}$ for $n \geq 0$, then we define the Galois group $G_n := \mathrm{Gal}(F_n/F)$. This identifies with a subgroup of $\mathcal{G}_n$ via the mapping $\tau_{F,E,p}$.

Let D be a cyclic subgroup in E of order p^{n+1} and fix B, a cyclic subgroup in E of order M. Let $C = D[p] \oplus B$, which is a cyclic subgroup of order N and let $\psi : E \to E/D$ be the isogeny associated to D with dual $\hat{\psi}$. We define

$$C' = \ker(\hat{\psi})[p] \oplus \psi(B)$$

which is a cyclic subgroup in E' of order N. Let $y_D = (E', C') \in Y_0(N)$. Then the point

$$Q_D = \Phi_E(y_D) \in E(F_n)$$

is known as a higher self point above P_C.

When $n = 0$, we have $y_D = w_p(x_C)$ where w_p is the Atkin-Lehner involution on $X_0(N)$. Therefore, we have $Q_D = -a_p(E) \cdot P_C + T$ for some $T \in E(\mathbb{Q})[2]$ and $a_p(E) \in \{\pm 1\}$ is the Hecke eigenvalue of the newform f_E attached to E.

For $n \geq 0$, let T_p be the Hecke operator on $J_0(N)$, the Jacobian of $X_0(N)$. Then

$$T_p((y_D) - (\infty)) = \sum_{D' \supset D} ((y_{D'}) - (\infty))$$

where the sum runs over all cyclic subgroups D' of order p^{n+2}. This then leads to the trace relation

$$a_p(E) \cdot Q_D = \sum_{D' \supset D} Q_{D'}.$$

This relationship between the higher self points can be viewed as an analogue system to the Euler system of Heegner points. Using this relationship, we see by induction that if P_C is of infinite order then so is Q_D. It also leads to the following.

Lemma 2.3.7. *[39, Lemma 19] Let B be a fixed cyclic subgroup in E of order M and let $n \geq 0$. Then $\sum_D Q_D$ is a torsion point in $E(F)$ where the sum runs over all cyclic subgroups of E of order p^{n+1}.*

Now, if we let

$$V_n := \ker\left(\mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] \to \mathbb{Q}_p\right) = \frac{\oplus_D \mathbb{Q}_p e_D}{\mathbb{Q}_p(\sum_D e_D)}$$

where $\mathcal{B}_n$ is a Borel subgroup of $\mathcal{G}_n$, we can again show that there exists a G_n-equivariant map

$$l_n : V_n \to E(F_n) \otimes \mathbb{Q}_p$$

$$e_D \mapsto Q_D$$

where D runs over elements of $\mathbb{P}^1_n$. This leads to the following.

Theorem 2.3.8. *[39, Theorem 20] Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of multiplicative reduction. Suppose $\tau_{F,E,p}$ is surjective and there exists a point P_C of infinite order in $E(F_0)$. Then for all $n \geq 0$ and all cyclic subgroups D of E of order p^{n+1} such that $D[p] \subset C$, Q_D is of infinite order and they generate a $\mathbb{Q}_p[\mathcal{G}_n]$-module inside $E(F_n) \otimes \mathbb{Q}_p$ isomorphic to V_n of dimension $p^{n+1} + p^n - 1$.*

We now let p be a prime of good ordinary reduction for E. Let F be a field such that $E(F)$ contains a point P_C of infinite order where C is a fixed cyclic subgroup of order N.

Define $F_n = F \cdot K_{p^{n+1}}$ for $n \geq 0$. This ensures that F_n is the smallest Galois extension of F such that G_F acts by scalars on $E[p^{n+1}]$. We also define $G_n := \mathrm{Gal}(F_n/F)$ which can be viewed as a subgroup of $\mathcal{G}_n$ via $\tau_{F,E,p}$.

Let D be a cyclic subgroup in E of order p^{n+1}. Let $\psi : E \to E/D$ be the isogeny associated to D and define $y_D = (E/D, \psi(C)) \in Y_0(N)$. Then we define the higher self point $Q_D = \Phi_E(y_D) \in E(F_n)$ above P_C.

We can again use the Hecke operator T_p to show that for all $n \geq 0$ we obtain the trace relation

$$a_p(E) \cdot Q_D = \sum_{D' \supset D} Q_{D'}$$

where D' runs through all cyclic subgroups of E of order p^{n+2} containing D. We also have

$$a_p(E) \cdot P_C = \sum_D Q_D$$

where the sum runs through all cyclic subgroups of E of order p. Therefore, as P_C is of infinite order in $E(F)$, then for all cyclic subgroups D of order p^{n+1} and all $n \geq 0$, Q_D is of infinite order in $E(F_n)$. This shows that we cannot obtain a relationship similar to that in Lemma 2.3.7.

If we let

$$V_{(n)} := \mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] = \bigoplus_D \mathbb{Q}_p e_D$$

where $\mathcal{B}_n$ is a Borel subgroup of $\mathcal{G}_n$, we can again show that there exists a G_n-equivariant map

$$l_n : V_{(n)} \to E(F_n) \otimes \mathbb{Q}_p$$

$$e_D \mapsto Q_D$$

where D runs over elements of $\mathbb{P}^1_n$. This leads to the following.

Theorem 2.3.9. *[39, Theorem 21] Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and p a prime of good ordinary reduction. Let F be a number field such that $E(F)$ contains a self point P_C of infinite order and suppose $\tau_{F,E,p}$ is surjective. Then all Q_D above P_C are of infinite order and generate a group of rank $p^{n+1} + p^n$ in $E(F_n) \otimes \mathbb{Q}_p$.*

We want to use the higher self points to bound Selmer groups in a similar way to Kolyvagin did in the Heegner point case, which involved creating derivative classes. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and p be an odd prime of good ordinary or multiplicative reduction. We let

$$F = \begin{cases} K_N & \text{if } p \nmid N, \\ K_{\frac{N}{p}} & \text{if } p || N, \end{cases}$$

as defined in the notation. Let F_n be the smallest extension of F such that $G_n = \mathrm{Gal}(F_n/F)$ acts as scalars on $E[p^{n+1}]$ and assume that $\tau_{F,E,p}$ is surjective, which implies that $G_n \cong \mathcal{G}_n$. We let $\mathcal{A}_n$ be a non-split Cartan subgroup of G_n, which is cyclic of order $p^{n+1} + p^n$ and denote the subfield of F_n fixed by $\mathcal{A}_n$ as L_n.

Theorem 2.3.10. *[39, Theorem 24] Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E does not have potentially good supersingular reduction at any prime of additive reduction and let p be a prime of either good ordinary or multiplicative reduction.*

Assume $\tau_{F,E,p}$ is surjective and that there exists a self point of infinite order in $E(K_N)$. Then

$$\left|\text{Sel}^{p^n}(E/L_n)\right| \geq p^n.$$

Proof. (Sketch) We will show a sketch of the proof here. The full proof will be explored in Chapter 4 when generalising the modular point construction. There is an injection

$$l_n : V_n \to E(F_n) \otimes \mathbb{Q}_p$$

$$f \mapsto \sum_D f(D) \cdot Q_D.$$

Let

$$S_n = \{P \in E(F_n) \mid \text{ there exists a } k \geq 0 \text{ such that } p^k \cdot P \in \mathbb{Z}_p[G_n] \cdot Q_D\}$$

be the higher saturated group of higher self points. It can be shown using the inclusion mapping of $E(F_n)_{\text{tors}}$ in S_n that $|\,\text{H}^1(\mathcal{A}_n, S_n)| = p^n$.

Let Y_n be the free $\mathbb{Z}_p$-module that denotes the cokernel of the inclusion of S_n in $E(F_n)$. Then there exists a long exact

$$0 \to E(L_n)_{\text{tors}} \to E(L_n) \to \text{Y}_n^{\mathcal{A}_n} \to \text{H}^1(\mathcal{A}_n, S_n) \to \text{H}^1(\mathcal{A}_n, E(F_n)).$$

If we compose the last map with the inflation mapping, we obtain the derivation map

$$\delta_n : \text{H}^1(\mathcal{A}_n, S_n) \to \text{H}^1(\mathcal{A}_n, E(F_n)) \xrightarrow{\text{inf}} \text{H}^1(L_n, E).$$

In particular, as it can be shown that S_n contains no p-torsion points, then there exists an isomorphism

$$\left(\frac{S_n}{p^n S_n}\right)^{\mathcal{A}_n} \cong \text{H}^1(\mathcal{A}_n, S_n)$$

and so the image of δ_n are the derived classes coming from the higher self points.

It can be shown that the image of δ_n lies in $Ш(E/L_n)$. Therefore, using the long exact sequence, either the image of the Kummer map contributes p^n elements in $\text{Sel}^{p^n}(E/L_n)$ if δ_n is not injective, or p^n elements of $\text{Sel}^{p^n}(E/L_n)$ are lifts of elements in $Ш(E/L_n)[p^n]$ if δ_n is injective. □

Therefore, we are able to bound Selmer groups using a method akin to Kolyvagin's work. We look to extend the idea of self points to a generalised construction of modular point. In particular, we use more advanced methods in modular representation theory to show that Selmer groups over certain fields must contain points of prime power order when the higher modular points satisfy certain conditions. This will however require a more in-depth look at the representation theory associated to $\mathcal{G}_n$.

Chapter 3

Representation Theory of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$

We have seen in the higher self points situation that if $\tau_{F,E,p}$ is surjective, then the points generate a $\mathbb{Q}_p[\mathcal{G}_n]$-module in the elliptic curve which we have denoted $V_{(n)}$ or V_n depending on the reduction type of the prime p. In particular, the saturated group of higher modular points will be isomorphic to a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice contained in this module. Therefore, we require further study into the integral representation theory of $\mathcal{G}_n$ in order to understand this saturated group.

Throughout this chapter we assume $p \neq 2$. Let

$$V_{(n)} := \mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{Q}_p)$$

be a $\mathbb{Q}_p[\mathcal{G}_n]$-module of dimension $p^{n+1}+p^n$, where $\mathcal{B}_n$ is a Borel subgroup of $\mathcal{G}_n$. We can view

$$V_{(n)} = \mathrm{Maps}(\mathbb{P}_n^1 \to \mathbb{Q}_p)$$

where $\mathcal{G}_n$ acts on $\mathbb{P}_n^1$ by its usual action. This decomposes as

$$V_{(n)} = \bigoplus_{i=-1}^{n} W_i$$

where W_i are irreducible $\mathbb{Q}_p[\mathcal{G}_n]$-modules with dimension δ_i as a $\mathbb{Q}_p$-vector space where

$$\delta_i = \begin{cases} 1 & \text{if } i = -1, \\ p & \text{if } i = 0, \\ p^{i+1} - p^{i-1} & \text{if } i \geq 1 \end{cases}$$

as seen in Theorem 2.3.4. These modules take the form

$$\begin{aligned} W_i &= \ker\left(\mathbb{Q}_p\left[{}^{\mathcal{G}_i}/_{\mathcal{B}_i}\right] \to \mathbb{Q}_p\left[{}^{\mathcal{G}_{i-1}}/_{\mathcal{B}_{i-1}}\right]\right) \\ &= \left\{ f : \mathbb{P}_i^1 \to \mathbb{Q}_p : \sum_{C \supset D} f(C) = 0 \text{ for } D \in \mathbb{P}_{i-1}^1 \right\} \end{aligned}$$

for $i \geq 0$ and $W_{-1} = \mathbb{Q}_p$. We have seen in the previous chapter that the $\mathbb{Q}_p[\mathcal{G}_n]$-module $V_n := V_{(n)}/W_{-1}$ will be of interest. We will study the possible lattices contained in the $\mathbb{Q}_p[\mathcal{G}_n]$-module V_n. Throughout this chapter, the standard $\mathbb{Z}_p[\mathcal{G}_n]$-lattice in $V_{(n)}$ is defined as

$$T_{(n)} = \mathbb{Z}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{Z}_p) = \mathrm{Maps}(\mathbb{P}_n^1 \to \mathbb{Z}_p)$$

and the standard $\mathbb{Z}_p[\mathcal{G}_n]$-lattice in V_n will be defined

$$T_n = \ker\left(\mathbb{Z}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right]\to\mathbb{Z}_p\right) = \left\{f : \mathbb{P}^1_n\to\mathbb{Z}_p : \sum_C f(C) = 0\right\}.$$

We also define the standard $\mathbb{Z}_p[\mathcal{G}_n]$-lattice inside W_i as

$$\begin{aligned} R_i &= \ker\left(\mathbb{Z}_p\left[{}^{\mathcal{G}_i}/_{\mathcal{B}_i}\right]\to\mathbb{Z}_p\left[{}^{\mathcal{G}_{i-1}}/_{\mathcal{B}_{i-1}}\right]\right) \\ &= \left\{f : \mathbb{P}^1_i\to\mathbb{Z}_p : \sum_{C\supset D} f(C) = 0 \text{ for } D \in \mathbb{P}^1_{i-1}\right\} \end{aligned}$$

for $i \geq 0$ and $R_{-1} = \mathbb{Z}_p$.

Throughout this chapter, we let an element

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{G}_n$$

denote the coset representing this matrix in $\mathcal{G}_n$.

In this chapter, we will examine the $\mathbb{Z}_p[\mathcal{G}_n]$-sublattices of T_n and the cohomologies associated to them with respect to subgroups of $\mathcal{G}_n$. In section 3.1, we look at group properties associated to $\mathcal{G}_n$ and its subgroups that will be of importance throughout the chapter.

In section 3.2, we look at some cohomological results which will be of importance when calculating cohomologies associated to the $\mathbb{Z}_p[\mathcal{G}_n]$-lattices. This culminates in Theorem 3.2.7, which provides the first cohomology group of $T_{(n)}$ with respect to all subgroups of $\mathcal{G}_n$.

In section 3.3, we look at the modular representation theory associated to $\mathcal{G}_n$. This will involve classifying all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\overline{T}_{(n)} = T_{(n)} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ in subsection 3.3.1, where we use Theorem 3.3.3 and Theorem 3.3.4 to classify all the $\mathbb{F}_p[\mathcal{I}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$, as seen in Theorem 3.3.5. We can then induce the modules we have found to $\mathcal{G}_n$ and find all $\mathbb{F}_p[\mathcal{G}_n]$-submodules in $\overline{T}_{(n)}$, with the full classification in Theorem 3.3.8. We then calculate their cohomologies with respect to certain subgroups of $\mathcal{G}_n$. This will be useful when looking at the integral case. Again, in subsection 3.3.2, we initially look at the cohomologies associated to $\mathbb{F}_p[\mathcal{I}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$. For the irre-

ducible $\mathbb{F}_p[\mathcal{I}_n]$-representations, we calculate the cohomologies with respect to $\mathcal{I}_n^k$ for $0 \leq k \leq n$, as seen in Theorem 3.3.11, in order to try and understand the cohomology of the $\mathbb{F}_p[\mathcal{I}_n]$-submodules. We are able to calculate the fixed part, as seen in Lemma 3.3.14. However, we can only come up with Conjecture 3.3.16 for the first cohomology groups. Therefore, from this conjecture, we induce the modules to $\mathcal{G}_n$ to provide Lemma 3.3.17 and Conjecture 3.3.19, which is what we believe to be the first cohomology groups of all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\overline{T}_{(n)}$ with respect to $\mathcal{G}_n$. We then use Lemma 3.3.23 to find the cohomology of all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\overline{T}_{(n)}$ with respect to a non-split Cartan subgroup $\mathcal{A}_n$, the 0-th cohomology results in Lemma 3.3.24 and the first cohomology results in Theorem 3.3.26. We end this subsection with Lemma 3.3.27, which looks at the fixed part of these modules by a Borel subgroup and show that they are always non-trivial if the module is non-trivial. This result will be useful not only later in this chapter, but in the next.

We then identify all the $\mathbb{Z}_p[\mathcal{G}_0]$-lattices contained in T_0 in section 3.4, as seen in Theorem 3.4.1, and it will be shown why this scenario cannot be followed for the $n \geq 1$ case in section 3.5. In particular, we look at the construction of some $\mathbb{Z}_p[\mathcal{G}_n]$-sublattices of T_n for $n \geq 1$.

We finally use the modular representation theory of $\mathcal{G}_n$ we have found throughout this chapter to calculate the cohomologies of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in V_n associated to subgroups of $\mathcal{G}_n$ in section 3.6, with each subsection fixed on a certain subgroup.

3.1 Group Properties of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$

In this section, we will look at the subgroups of $\mathcal{G}_n$ and the properties associated to them which will be useful throughout the chapter. We quickly remind ourselves of the notation used for the groups we will look at throughout this chapter. Let $\mu_n : \mathcal{G}_n \to \mathcal{G}_0$ be the surjective reduction mapping. We now fix definitions for certain subgroups. We let:

1) $\mathcal{G}_n := \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$,

2) $\mathcal{B}_n := \{\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a Borel subgroup of order $p^{2n+1}(p-1)$,

3) $\mathcal{H}_n := \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a cyclic subgroup of order p^{n+1}, generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$,

4) $\mathcal{I}_n := \{g \in \mathcal{G}_n : \mu_n(g) \in \mathcal{B}_0\}$ the standard Iwahori subgroup which has order $p^{3n+1}(p-1)$,

5) $\mathcal{P}_n := \{g \in \mathcal{G}_n : \mu_n(g) \in \mathcal{H}_0\}$ the pro-p Iwahori subgroup and a Sylow-p subgroup of $\mathcal{I}_n$,

6) $\mathcal{U}_n := \{\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \in \mathcal{G}_n : p|a\}$ a cyclic subgroup of order p^n, generated by $\left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$,

7) $\mathcal{D}_n := \{\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}$ a split Cartan subgroup, which is cyclic of order $p^n(p-1)$ and generated by the element $\left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where c generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$,

8) $N(\mathcal{D}_n)$ the normaliser of a split Cartan subgroup, a subgroup of $\mathcal{G}_n$ which contains $\mathcal{D}_n$ of index 2,

9) $\mathcal{A}_n$ a non-split Cartan subgroup, which is cyclic of order $p^n(p+1)$ and generated by an element denoted α_n,

10) $N(\mathcal{A}_n)$ the normaliser of a non-split Cartan subgroup, a subgroup of $\mathcal{G}_n$ which contains $\mathcal{A}_n$ of index 2.

If we define the surjective reduction mapping $\mu_n^k : \mathcal{G}_n \to \mathcal{G}_k$ for $0 \leq k \leq n$, then we may define the subgroup

$$\mathcal{I}_n^k = \{g \in \mathcal{G}_n : \mu_n^k(g) \in \mathcal{B}_k\}.$$

We have $\mathcal{I}_n^n = \mathcal{B}_n$ and also, as $\mu_n = \mu_n^0$, we have $\mathcal{I}_n^0 = \mathcal{I}_n$.

We would also like to look at some key results with respect to these groups. We initially look at certain cosets that will appear in this chapter. We have seen that the modules we are looking at are induced from $\mathcal{B}_n$ to $\mathcal{G}_n$ and so we would like to see the coset decomposition of $\mathcal{B}_n\backslash\mathcal{G}_n$. This will require the following.

Lemma 3.1.1. *[39, Lemma 25] $\mathcal{A}_n$ intersects trivially with any Borel subgroup in $\mathcal{G}_n$.*

Hence, $\mathcal{G}_n = \mathcal{B}_n\mathcal{A}_n$ and therefore the coset representatives of $\mathcal{B}_n\backslash\mathcal{G}_n$ can be viewed as $\mathcal{A}_n$. We will also encounter induced modules from $\mathcal{I}_n$ to $\mathcal{G}_n$ when looking at the modular representation theory associated to $\mathcal{G}_n$. However, we first need the following.

Lemma 3.1.2. *For all $n \geq 0$, $\mathcal{I}_n = \mathcal{H}_n\mathcal{D}_n\mathcal{U}_n$.*

Proof. All elements of $\mathcal{I}_n$ can be written in the form

$$\left(\begin{smallmatrix} u & v \\ t & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & v \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} u-tv & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right) \in \mathcal{H}_n\mathcal{D}_n\mathcal{U}_n$$

and obviously $\mathcal{H}_n\mathcal{D}_n\mathcal{U}_n \subseteq \mathcal{I}_n$ which gives our result. □

We can show that $\mathcal{B}_n = \mathcal{H}_n\mathcal{D}_n$ meaning $\mathcal{I}_n = \mathcal{B}_n\mathcal{U}_n$ and so the coset representatives of $\mathcal{B}_n\backslash\mathcal{I}_n$ can be viewed as $\mathcal{U}_n$. Also, we can view $\mathcal{A}_n = \mathcal{U}_n\mathcal{N}_n$ where $\mathcal{N}_n$ is a cyclic group generated by ${\alpha_n}^{p^n}$. Using this, we see that $\mathcal{G}_n = \mathcal{I}_n\mathcal{N}_n$ and so the coset representatives of $\mathcal{I}_n\backslash\mathcal{G}_n$ can be viewed as powers of $v_n := {\alpha_n}^{p^n}$. The final set of coset representative we want to find are for $\mathcal{I}_n^k\backslash\mathcal{I}_n$ for $1 \leq k \leq n$. If we let

$$C_{n,k} = \mathcal{U}_n\backslash\Big(\mathcal{U}_n \cap \ker(\mu_n^k)\Big) = \Big\{\left(\begin{smallmatrix} 1 & 0 \\ ap & 1 \end{smallmatrix}\right) \in \mathcal{G}_n : 0 \leq a \leq p^k - 1\Big\},$$

then we have $\mathcal{I}_n = \mathcal{I}_n^k C_{n,k}$ and hence the coset representatives of $\mathcal{I}_n^k\backslash\mathcal{I}_n$ can be viewed as $C_{n,k}$.

We will also encounter the first cohomology groups of subgroups of $\mathcal{G}_n$ with respect to $\mathbb{Z}/p^m\mathbb{Z}$ for $m \geq 1$ with trivial action. Therefore, we will need to know the homomorphism groups of subgroups of $\mathcal{G}_n$ to $\mathbb{Z}/p^m\mathbb{Z}$. Calculating these for subgroups such as $\mathcal{H}_n$, $\mathcal{D}_n$ and $\mathcal{A}_n$ are obvious due to them being cyclic groups. However, for groups such as $\mathcal{B}_n$, $\mathcal{I}_n$ and $\mathcal{G}_n$ itself, we require their abelianisation. We initially look at $\mathcal{G}_0$.

Lemma 3.1.3. *We have $[\mathcal{G}_0, \mathcal{G}_0] = \mathrm{PSL}_2(\mathbb{F}_p)$.*

Proof. We know that there exists the quotient mapping $\tau : \mathrm{GL}_2(\mathbb{F}_p) \to \mathcal{G}_0$ where $\mathrm{PSL}_2(\mathbb{F}_p) = \tau(\mathrm{SL}_2(\mathbb{F}_p))$. Let $g, h \in \mathcal{G}_0$. Then as $\mathrm{SL}_2(\mathbb{F}_p)$ is the commutator subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, we have

$$[g, h] = [\tau(x), \tau(y)] = \tau([x, y]) \in \tau(\mathrm{SL}_2(\mathbb{F}_p)) = \mathrm{PSL}_2(\mathbb{F}_p)$$

for some $x, y \in \mathrm{GL}_2(\mathbb{F}_p)$. Now let $g \in \mathrm{PSL}_2(\mathbb{F}_p)$. Then there exists an $s \in \mathrm{SL}_2(\mathbb{F}_p)$ such that

$$g = \tau(s) = \tau([a,b]) = [\tau(a), \tau(b)] \in [\mathcal{G}_0, \mathcal{G}_0]$$

for some $a, b \in \mathrm{GL}_2(\mathbb{F}_p)$. □

We now look at the subgroup $\mathcal{B}_n$.

Lemma 3.1.4. *For all $n \geq 0$, we have $[\mathcal{B}_n, \mathcal{B}_n] = \mathcal{H}_n$.*

Proof. Let $t = [\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)] \in [\mathcal{B}_n, \mathcal{B}_n]$. Then

$$\begin{aligned} t &= \left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -v \\ 0 & u \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -b \\ 0 & a \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} au & bu+v \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -av-b \\ 0 & au \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} au & au(bu+v-av-b) \\ 0 & au \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & bu+v-av-b \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{H}_n. \end{aligned}$$

We know that $\mathcal{H}_n$ is generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = [\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)] \in [\mathcal{B}_n, \mathcal{B}_n]$$

which gives the equality. □

We now move on to $\mathcal{I}_n$.

Lemma 3.1.5. *For all $n \geq 0$, we have $[\mathcal{I}_n, \mathcal{I}_n] = \mathcal{P}_n$.*

Proof. Let $[a,b] \in [\mathcal{I}_n, \mathcal{I}_n]$. Then as μ_n is a homomorphism, we have

$$\mu_n([a,b]) = [\mu_n(a), \mu_n(b)] \in [\mathcal{B}_0, \mathcal{B}_0] = H_0$$

by Lemma 3.1.4. Therefore, $[a,b] \in \mathcal{P}_n$. On the other hand, if we let $t \in \mathcal{P}_n$, then $\mu_n(t) \in H_0 = [\mathcal{B}_0, \mathcal{B}_0]$ by Lemma 3.1.4. Therefore, there exists a $a, b \in \mathcal{B}_0$ such that $\mu_n(t) = [a,b]$. However, μ_n is surjective and so there exists $u, v \in \mathcal{I}_n$ such that $\mu_n(t) = [\mu_n(u), \mu_n(v)] = \mu_n([u,v])$. Therefore, $t[u,v]^{-1} \in \ker(\mu_n)$.

Therefore, we may write $t = k[u, v]$ for $k \in \ker(\mu_n)$. We know that the kernel of μ_n is generated by the matrices

$$\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

We have

$$\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right) = \left[\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1-p & 0 \\ 0 & 1 \end{smallmatrix}\right)\right], \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right) = \left[\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -2 & 0 \\ p & 1 \end{smallmatrix}\right)\right]$$

and

$$\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left[\left(\begin{smallmatrix} z & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} z^{-1} & 0 \\ z-1 & 1 \end{smallmatrix}\right)\right]$$

where $z^2 = p + 1$. We know $p + 1$ is a quadratic residue modulo p^{n+1} as it is modulo p. Therefore, $\ker(\mu_n) \leq [\mathcal{I}_n, \mathcal{I}_n]$ and so $t = k[u, v] \in [\mathcal{I}_n, \mathcal{I}_n]$. □

We can now look at the homomorphism groups. We first look at $\mathcal{G}_n$.

Proposition 3.1.6. *For all $n \geq 0$ and $m \geq 1$, we have* $\mathrm{Hom}(\mathcal{G}_n, \mathbb{Z}/p^m\mathbb{Z}) = 0$.

Proof. As $\mathbb{Z}/p^m\mathbb{Z}$ is abelian, then $\mathrm{Hom}(\mathcal{G}_n, \mathbb{Z}/p^m\mathbb{Z}) = \mathrm{Hom}({\mathcal{G}_n}^{ab}, \mathbb{Z}/p^m\mathbb{Z})$ where ${\mathcal{G}_n}^{ab}$ is the abelianisation of $\mathcal{G}_n$. We saw in the proof of Lemma 3.1.5 that $\ker(\mu_n) \subseteq [\mathcal{I}_n, \mathcal{I}_n] \subseteq [\mathcal{G}_n, \mathcal{G}_n]$. Hence

$$\begin{aligned} \mathrm{Hom}(\mathcal{G}_n, \mathbb{Z}/p^m\mathbb{Z}) &= \mathrm{Hom}({\mathcal{G}_n}^{ab}, \mathbb{Z}/p^m\mathbb{Z}) \\ &= \mathrm{Hom}({\mathcal{G}_0}^{ab}, \mathbb{Z}/p^m\mathbb{Z}) \\ &\cong \mathrm{Hom}(\mathbb{F}_2, \mathbb{Z}/p^m\mathbb{Z}) = 0. \end{aligned}$$

by Lemma 3.1.3. □

We also look at the $\mathcal{B}_n$ case.

Proposition 3.1.7. *For $n \geq 0$ and $m \geq 1$, we have*

$$\mathrm{Hom}(\mathcal{B}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathbb{Z}/p^{\min(m,n)}\mathbb{Z}.$$

Proof. As $\mathbb{Z}/p^m\mathbb{Z}$ is abelian, we have

$$\mathrm{Hom}(\mathcal{B}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathrm{Hom}({\mathcal{B}_n}^{ab}, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathrm{Hom}(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z})$$

by Lemma 3.1.4. However, $\mathcal{D}_n$ is a cyclic group of order $p^n(p-1)$, which gives our result. □

Also, we have the $\mathcal{I}_n$ case.

Proposition 3.1.8. *For all $n \geq 0$ and $m \geq 1$, we have* $\mathrm{Hom}(\mathcal{I}_n, \mathbb{Z}/p^m\mathbb{Z}) = 0$.

Proof. As $\mathbb{Z}/p^m\mathbb{Z}$ is abelian, we have

$$\mathrm{Hom}(\mathcal{I}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathrm{Hom}({\mathcal{I}_n}^{ab}, \mathbb{Z}/p^m\mathbb{Z}) = 0$$

by Lemma 3.1.5 and as $\mathcal{P}_n$ is a Sylow-p subgroup of $\mathcal{I}_n$. □

Using this, we can show the following.

Proposition 3.1.9. *We have* $\mathrm{Hom}(\mathcal{P}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathbb{F}_p^2$ *for all $n \geq 0$ and $m \geq 1$.*

Proof. We first look at $[\mathcal{P}_n, \mathcal{P}_n]$. Let $[a, b] \in [\mathcal{P}_n, \mathcal{P}_n]$. Then

$$\mu_n([a, b]) = [\mu_n(a), \mu_n(b)] \in [\mathcal{H}_0, \mathcal{H}_0] = \{I_2\}$$

as $\mathcal{H}_0$ is an abelian group. Therefore, $[\mathcal{P}_n, \mathcal{P}_n] \subseteq \ker(\mu_n)$. Now, we know $\ker(\mu_n)$ is generated by the matricies $\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$ and we have

$$\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right) \in [\mathcal{P}_n, \mathcal{P}_n]$$

as seen in the proof of Lemma 3.1.5. However, if we let $\left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) \in \mathcal{P}_n$, then

$$\left[\left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right)\right] = \left(\begin{smallmatrix} * & * \\ cu+w+bcuw+bw^2-c^2v-c-acvw-aw & * \end{smallmatrix}\right)$$

with

$$\begin{aligned} &cu + w + bcuw + bw^2 - c^2v - c - acvw - aw \\ &= c(u-1) + w(1-a) + bcuw + bw^2 - c^2v - acvw \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

Therefore, $\left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right) \notin [\mathcal{P}_n, \mathcal{P}_n]$. However, we have

$$\left(\begin{smallmatrix} 1 & 0 \\ p^2 & 1 \end{smallmatrix}\right) = \left[\left(\begin{smallmatrix} (p+1)^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)\right]$$

and so

$$[\mathcal{P}_n, \mathcal{P}_n] = \left\langle \left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ p^2 & 1 \end{smallmatrix}\right) \right\rangle.$$

Therefore, we have

$$\mathcal{P}_n/_{[\mathcal{P}_n, \mathcal{P}_n]} = \left\langle \left(\begin{smallmatrix} \overline{1} & \overline{1} \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \overline{1} & 0 \\ p & 1 \end{smallmatrix}\right) \right\rangle \cong \mathbb{F}_p^2.$$

Finally, we can use this to prove the proposition. We have

$$\begin{aligned} \mathrm{Hom}(\mathcal{P}_n, \mathbb{Z}/p^m\mathbb{Z}) &= \mathrm{Hom}(\mathcal{P}_n^{ab}, \mathbb{Z}/p^m\mathbb{Z}) \\ &\cong \mathrm{Hom}(\mathbb{F}_p^2, \mathbb{Z}/p^m\mathbb{Z}) \\ &\cong \mathbb{F}_p^2 \end{aligned}$$

which gives our result. □

We finish this section by looking at the group action of $\mathcal{G}_n$ on $\mathbb{P}_n^1$. We know that if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{G}_n$ and $[u : v] \in \mathbb{P}_n^1$, then

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot [u : v] = [au + bv : cu + dv].$$

We would like to know whether the group action is transitive and whether it is doubly transitive.

Lemma 3.1.10. *The action of $\mathcal{G}_n$ on $\mathbb{P}_n^1$ is transitive for all $n \geq 0$.*

Proof. We have

$$\left(\begin{smallmatrix} 1 & v-u \\ 0 & 1 \end{smallmatrix}\right) \cdot [u : 1] = [v : 1],$$

$$\left(\begin{smallmatrix} 1 & 0 \\ v-u & 1 \end{smallmatrix}\right) \cdot [1 : u] = [1 : v]$$

and

$$\left(\begin{smallmatrix} 0 & 1 \\ 1 & v-u \end{smallmatrix}\right) \cdot [u : 1] = [1 : v]$$

which proves the lemma. □

However, we see that the action is not always doubly transitive.

Lemma 3.1.11. *The action of $\mathcal{G}_n$ on $\mathbb{P}^1_n$ is doubly transitive if $n = 0$ whereas for all $n \geq 1$, it is not.*

Proof. If we fix a $C \in \mathbb{P}^1_n$, then the action is doubly transitive if and only if it is transitive and $\mathrm{Stab}_{\mathcal{G}_n}(C)$ acts transitively on $\mathbb{P}^1_n \backslash \{C\}$. We will fix $C = [0:1]$. Then we have

$$\mathrm{Stab}_{\mathcal{G}_n}([0:1]) = \{\left(\begin{smallmatrix} a & 0 \\ b & 1 \end{smallmatrix}\right) \in \mathcal{G}_n\}.$$

For the case $n = 0$, we know that the action is transitive and we have

$$\left(\begin{smallmatrix} vu^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot [u:1] = [v:1]$$

for all $u, v \in \mathbb{F}_p^\times$ and

$$\left(\begin{smallmatrix} u^{-1} & 0 \\ -u^{-1} & 1 \end{smallmatrix}\right) \cdot [u:1] = [1:0]$$

which proves the case for $n = 0$.

For $n \geq 1$, there is no matrix $g \in \mathrm{Stab}_{\mathcal{G}_n}([0:1])$ such that $g \cdot [1:0] = [k:1]$ where $k > 0$ and $p|k$, so it cannot be doubly transitive for $n \geq 1$. □

We now have the group theoretical results that will be required throughout this chapter. We will now look at some standard results for group cohomology.

3.2 Cohomological Results

In this section, we will look at some general cohomological results that we can use throughout this chapter. In particular, we can use Theorem 3.2.7 to find the first cohomology group of $T_{(n)}$ with respect to all subgroups of $\mathcal{G}_n$. We initially want to utilise the spectral sequences to prove both Proposition 3.2.1 and Proposition 3.2.2.

Proposition 3.2.1. *Let H be a normal subgroup of G and M a G-module such that $\mathrm{H}^i(H, M) = 0$ for $i \in \{0, 2\}$. Then*

$$\mathrm{H}^1(G, M) \cong \mathrm{H}^1(H, M)^{G/H}$$

and

$$\mathrm{H}^2(G, M) \cong \mathrm{H}^1(G/H, \mathrm{H}^1(H, M)).$$

Proof. We will look at the spectral sequence to obtain the results. We have the following stage 2 table of the Hochschild–Serre spectral sequence:

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ E_2^{0,1} & E_2^{1,1} & E_2^{2,1} & E_2^{3,1} \\ 0 & 0 & 0 & 0 \end{array}$$

where

$$E_2^{p,q} = \mathrm{H}^p(G/H, \mathrm{H}^q(H, M)).$$

Due to the hypothesis, the top and bottom lines are all zeros. If we look at the third stage, we obtain

$$\begin{array}{cccc} \ker(E_2^{0,2} \to E_2^{2,1}) & \ker(E_2^{1,2} \to E_2^{3,1}) & \frac{\ker(E_2^{2,2} \to E_2^{4,1})}{\mathrm{im}(E_2^{0,3} \to E_2^{2,2})} & \frac{\ker(E_2^{3,2} \to E_2^{5,1})}{\mathrm{im}(E_2^{1,3} \to E_2^{3,2})} \\ \ker(E_2^{0,1} \to E_2^{2,0}) & \ker(E_2^{1,1} \to E_2^{3,0}) & \frac{\ker(E_2^{2,1} \to E_2^{4,0})}{\mathrm{im}(E_2^{0,2} \to E_2^{2,1})} & \frac{\ker(E_2^{3,1} \to E_2^{5,0})}{\mathrm{im}(E_2^{1,2} \to E_2^{3,1})} \\ E_2^{0,0} & E_2^{1,0} & \frac{E_2^{2,0}}{\mathrm{im}(E_2^{0,1} \to E_2^{2,0})} & \frac{E_2^{3,0}}{\mathrm{im}(E_2^{1,1} \to E_2^{3,0})} \end{array}$$

where each section represents $E_3^{p,q}$, which leads to the table

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ E_2^{0,1} & E_2^{1,1} & E_2^{2,1} & E_2^{3,1} \\ 0 & 0 & 0 & 0 \end{array}$$

as $E_2^{a,0} = E_2^{a,2} = 0$ for all $a \geq 0$. As this is the third stage, we can deduce that

$$E_\infty^{0,0} = E_\infty^{1,0} = E_\infty^{2,0} = 0$$

and

$$E_\infty^{0,1} = E_2^{0,1}, \quad E_\infty^{1,1} = E_2^{1,1}, \quad E_\infty^{2,1} = E_2^{2,1}.$$

We can also deduce that $E_\infty^{0,2} = 0$ from this table as the next stage would remain unchanged.

We obtain the following exact sequence from the spectral sequence

$$0 \to E_\infty^{1,0} \to \mathrm{H}^1(G, M) \to E_\infty^{0,1} \to 0.$$

However, as $E_\infty^{1,0} = 0$, we have

$$\mathrm{H}^1(G, M) \cong E_\infty^{0,1} = \mathrm{H}^1(H, M)^{G/H}.$$

We also obtain the sequence

$$0 \to E_\infty^{1,1} \to \mathrm{H}^2(G, M) \to E_\infty^{0,2} \to 0,$$

as $E_\infty^{2,0} = 0$. Therefore, as $E_\infty^{0,2} = 0$, we have

$$\mathrm{H}^2(G, M) \cong E_\infty^{1,1} = \mathrm{H}^1(G/H, \mathrm{H}^1(H, M)).$$

□

We also use the spectral sequence to prove the following.

Proposition 3.2.2. *Let H be a normal subgroup of G and M a G-module such that $\mathrm{H}^1(H, M) = 0$. Then*

$$\mathrm{H}^1(G, M) \cong \mathrm{H}^1(G/H, M^H)$$

and there exists an exact sequence

$$0 \to \mathrm{H}^2(G/H, M^H) \to \mathrm{H}^2(G, M) \to \mathrm{H}^2(H, M)^{G/H} \to$$

$$\to \mathrm{H}^3(G/H, M^H) \to \mathrm{H}^3(G, M) \to 0.$$

Proof. The first part is taken from the five term exact sequence. We will look at the spectral sequence to obtain the exact sequence. We have the following stage 2 table of the Hochschild–Serre spectral sequence:

$$\begin{array}{cccc} E_2^{0,2} & E_2^{1,2} & E_2^{2,2} & E_2^{3,2} \\ 0 & 0 & 0 & 0 \\ E_2^{0,0} & E_2^{1,0} & E_2^{2,0} & E_2^{3,0} \end{array}$$

where

$$E_2^{p,q} = \mathrm{H}^p(G/H, \mathrm{H}^q(H, M)).$$

The middle row entries are all zeros due to the hypothesis. If we look at the third stage, we obtain

$$\begin{array}{cccc}
\ker(E_2^{0,2}\to E_2^{2,1}) & \ker(E_2^{1,2}\to E_2^{3,1}) & \frac{\ker(E_2^{2,2}\to E_2^{4,1})}{\operatorname{im}(E_2^{0,3}\to E_2^{2,2})} & \frac{\ker(E_2^{3,2}\to E_2^{5,1})}{\operatorname{im}(E_2^{1,3}\to E_2^{3,2})} \\
\ker(E_2^{0,1}\to E_2^{2,0}) & \ker(E_2^{1,1}\to E_2^{3,0}) & \frac{\ker(E_2^{2,1}\to E_2^{4,0})}{\operatorname{im}(E_2^{0,2}\to E_2^{2,1})} & \frac{\ker(E_2^{3,1}\to E_2^{5,0})}{\operatorname{im}(E_2^{1,2}\to E_2^{3,1})} \\
E_2^{0,0} & E_2^{1,0} & \frac{E_2^{2,0}}{\operatorname{im}(E_2^{0,1}\to E_2^{2,0})} & \frac{E_2^{3,0}}{\operatorname{im}(E_2^{1,1}\to E_2^{3,0})}
\end{array}$$

where each section represents $E_3^{p,q}$, which leads to the table

$$\begin{array}{cccc}
E_2^{0,2} & E_2^{1,2} & \frac{E_2^{2,2}}{\operatorname{im}(E_2^{0,3}\to E_2^{2,2})} & \frac{E_2^{3,2}}{\operatorname{im}(E_2^{1,3}\to E_2^{3,2})} \\
0 & 0 & 0 & 0 \\
E_2^{0,0} & E_2^{1,0} & E_2^{2,0} & E_2^{3,0}
\end{array}$$

as $E_2^{a,1} = 0$ for all $a \geq 0$. We next see the fourth stage

$$\begin{array}{cccc}
\ker(E_2^{0,2}\to E_2^{3,0}) & \ker(E_2^{1,2}\to E_2^{3,1}) & \star & \star \\
0 & 0 & 0 & 0 \\
E_2^{0,0} & E_2^{1,0} & E_2^{2,0} & \frac{E_2^{3,0}}{\operatorname{im}(E_2^{0,2}\to E_2^{3,0})}
\end{array}$$

We obtain the following exact sequence from the spectral sequence

$$0\to E_2^{2,0}\to \mathrm{H}^2(G,M)\to \ker(E_2^{0,2}\to E_2^{3,0})\to 0.$$

We also obtain the sequence

$$0\to \frac{E_2^{3,0}}{\operatorname{im}(E_2^{0,2}\to E_2^{3,0})}\to \mathrm{H}^3(G,M).$$

If we combine the two exact sequence we obtain

$$0\to E_2^{2,0}\to \mathrm{H}^2(G,M)\to E_2^{0,2}\to E_2^{3,0}\to \mathrm{H}^3(G,M)\to 0$$

which gives the result. □

We now focus on $\mathbb{Z}_p[G]$-modules for a finite group G. Let X be a $\mathbb{Z}_p[G]$-module. We define the norm map $N_G : X \to X$, an endomorphism such that

$$N_G(x) = \sum_{g \in G} g \cdot x.$$

Let

$$I_G X = \{(g-1)x : g \in G,\, x \in X\}.$$

Then we have $I_G X \subset \ker(N_G)$ and $\mathrm{im}(N_G) \subset X^G$. We can then define the Tate cohomology groups

$$\hat{\mathrm{H}}^{-1}(G, X) = {}^{\ker(N_G)}\!/_{I_G X} \quad \text{and} \quad \hat{\mathrm{H}}^{0}(G, X) = {}^{X^G}\!/_{\mathrm{im}(N_G)}.$$

If G is a cyclic group, then for $i \geq 1$ we have non-canonical isomorphisms

$$\mathrm{H}^i(G, X) \cong \hat{\mathrm{H}}^{-1}(G, X) \quad \text{for } i \equiv 1 \pmod 2,$$

$$\mathrm{H}^i(G, X) \cong \hat{\mathrm{H}}^{0}(G, X) \quad \text{for } i \equiv 0 \pmod 2$$

by [17, pg. 133]. We would like to use results on the Tate cohomology groups to look at group cohomology of certain $\mathbb{Z}_p[G]$-modules.

Proposition 3.2.3. *Let G be a finite group, X a finite set with an action by G, A an abelian group with trivial action by G and $M = \mathrm{Maps}(X \to A)$. Then*

$$\hat{\mathrm{H}}^{-1}(G, M) \cong \bigoplus_{G\cdot x \text{ orbits}} A[|\mathrm{Stab}_G(x)|]$$

where the sum is taken over all orbits of the action and $A[|\mathrm{Stab}_G(x)|]$ are the elements of A killed by $|\mathrm{Stab}_G(x)|$.

Proof. We first look at when G acts transitively on X. Then we have

$$\sum_{g \in G} g \cdot x = \frac{|G|}{|X|} \cdot \sum_{x \in X} x$$

for $x \in X$. Hence, for all $x \in X$, we have $N_G(e_x) = \frac{|G|}{|X|}e_X$ where e_x and e_X are the characteristic functions on x and X respectively. Therefore, we have

$$N_G(f) = \tfrac{|G|}{|X|}\Big(\sum_{x\in X} f(x)\Big)e_X$$

and so

$$\ker(N_G) = \left\{ f \in M \middle| \tfrac{|G|}{|X|}\sum_{x\in X} f(x) = 0 \right\}.$$

If $g \in G$, then $(g-1)e_x = e_{g\cdot x} - e_x$. Therefore, for $f \in I_G M$, there exists a $h \in M$ such that

$$f = (g-1)h = \sum_{x\in X}(h(g^{-1}\cdot x) - h(x))e_x$$

and

$$\sum_{x\in X} f(x) = \sum_{x\in X} h(g^{-1}\cdot x) - h(x) = 0$$

as the action of G on X is transitive. Also, if $f \in M$ such that $\sum\limits_{x\in X} f(x) = 0$, then fix a $z \in X$. Then

$$f(z) = -\sum_{x\in X\setminus\{z\}} f(x)$$

and so

$$f = \sum_{x\in X\setminus\{z\}} f(x)(e_x - e_z).$$

However, as the action of G on X is transitive, then for all $x, z \in X$ there exists a $g \in G$ such that $g\cdot x = z$. Therefore,

$$e_x - e_z = e_{g\cdot z} - e_z = (g-1)e_z$$

and so $f \in I_G M$ as it is a linear sum of elements of the form $(g-1)h$ for $g \in G$ and $h \in M$. Therefore, we have

$$I_G M = \left\{ f \in M \middle| \sum_{x\in X} f(x) = 0 \right\}$$

and so

$$\hat{\mathrm{H}}^{-1}(G, M) \cong \left\{ a \in A \middle| \tfrac{|G|}{|X|}a = 0 \right\} = A\big[\tfrac{|G|}{|X|}\big].$$

If the group action of G on X is not transitive, then

$$M = \bigoplus_{U \text{ orbits}} \text{Maps}(U \to A)$$

as a G-module, where the sum is taken over all orbits. Therefore, we have

$$\hat{H}^{-1}(G, M) \cong \bigoplus_{G \cdot x \text{ orbits}} A[|\text{Stab}_G(x)|]$$

□

We can also find a similar result with respect to the other Tate cohomology group we have identified.

Proposition 3.2.4. *Let G be a finite group, X a finite set with an action by G, A an abelian group with trivial action by G and $M = \text{Maps}(X \to A)$. Then*

$$\hat{\text{H}}^0(G, M) \cong \bigoplus_{G \cdot x \text{ orbits}} A \Big/ |\text{Stab}_G(x)| A$$

where the sum is taken over all orbits of the action.

Proof. We first look at when G acts transitively on X. If $f \in M^G$, then $f(g^{-1} \cdot x) = f(x)$ for all $g \in G$. However, as the action is transitive, this means that f is constant on X. Therefore, if e_X is the characteristic function on X, then

$$M^G = \{ae_X : a \in A\} \cong A.$$

We now want to show

$$N_G(M) = \left\{ \tfrac{|G|}{|X|} ae_X : a \in A \right\} \cong \tfrac{|G|}{|X|} A.$$

We saw in the proof of Proposition 3.2.3 that

$$N_G(f) = \tfrac{|G|}{|X|} \Big(\sum_{x \in X} f(x) \Big) e_X$$

for all $f \in M$. Also, as

$$\tfrac{|G|}{|X|} e_X = N_G(e_x)$$

for any $x \in X$, we have shown $N_G(M) \cong \frac{|G|}{|X|}A$ and so

$$\hat{\mathrm{H}}^0(G, M) \cong A \Big/ \tfrac{|G|}{|X|}A$$

if the group action of G on A is transitive.

If the group action of G on X is not transitive, then

$$M = \bigoplus_{U \text{ orbits}} \mathrm{Maps}(U \to A)$$

as a G-module, where the sum is taken over all orbits. Therefore, we have

$$\hat{H}^0(G, M) \cong \bigoplus_{G \cdot x \text{ orbits}} A \Big/ |\mathrm{Stab}_G(x)|A. \qquad \square$$

We will look at the Tate cohomology of $\mathbb{Z}_p[G]$-modules with trivial G-action.

Lemma 3.2.5. *Let G be a group acting trivially on torsion-free M. Then*

$$\hat{\mathrm{H}}^{-1}(G, M) = 0, \qquad \hat{\mathrm{H}}^0(G, M) \cong M/|G|M.$$

Proof. For the first case, we have

$$\hat{\mathrm{H}}^{-1}(G, M) = \frac{\ker(N_G)}{I_G M}.$$

As the action is trivial, then N_G is the multiplication-by-$|G|$ map. As M is torsion-free, we obtain our first result.

For the second case, we have

$$\hat{\mathrm{H}}^0(G, M) = \frac{M}{N_G(M)} \cong M/|G|M$$

as the action is trivial. $\square$

We will also look at extensions of $\mathbb{Z}_p[G]$-modules as well. The following result will be important when linking extensions to our cohomological results.

Proposition 3.2.6. *Let G be a group and let M and N be $\mathbb{Z}_p[G]$-modules such that M is projective as a $\mathbb{Z}_p$-module. Then for all $i \geq 1$ we have*

$$\mathrm{Ext}^i_{\mathbb{Z}_pG}(M,N) \cong \mathrm{H}^i(G, \mathrm{Hom}_{\mathbb{Z}_p}(M,N))$$

as $\mathbb{Z}_p$-modules.

Proof. By [28, Theorem 2.6.10], we have a spectral sequence with

$$E_2^{p,q} = \mathrm{H}^p(G, \mathrm{Ext}^q_{\mathbb{Z}_p}(M,N)) \implies \mathrm{Ext}^{p+q}_{\mathbb{Z}_pG}(M,N).$$

As M is projective as a $\mathbb{Z}_p$-module, then $\mathrm{Ext}^i_{\mathbb{Z}_p}(M,N) = 0$ for all $i \geq 1$ and so $E_2^{p,q} = 0$ for all $q > 0$. Then we have our result by [28, Lemma 2.1.4]. □

We can apply this in the proof of the following important result.

Theorem 3.2.7. *Let $H, H' \leq G$. Then $\mathrm{H}^1\left(H, \mathrm{Ind}^G_{H'}(\mathbb{Z}_p)\right) = 0$.*

Proof. By Proposition 3.2.6, we have

$$\begin{aligned}\mathrm{H}^1\left(H, \mathrm{Ind}^G_{H'}(\mathbb{Z}_p)\right) &\cong \mathrm{Ext}^1_{\mathbb{Z}_pH}\left(\mathbb{Z}_p, \mathrm{Ind}^G_{H'}(\mathbb{Z}_p)\right) \\ &\cong \mathrm{Ext}^1_{\mathbb{Z}_pG}\left(\mathrm{Ind}^G_H(\mathbb{Z}_p), \mathrm{Ind}^G_{H'}(\mathbb{Z}_p)\right).\end{aligned}$$

Using [6, Corollary 3.3.5 (vi)], we have

$$\begin{aligned}&\mathrm{Ext}^1_{\mathbb{Z}_pG}\left(\mathrm{Ind}^G_H(\mathbb{Z}_p), \mathrm{Ind}^G_{H'}(\mathbb{Z}_p)\right) \\ &\cong \bigoplus_{H'gH} \left(\mathrm{Ext}^1_{\mathbb{Z}_p(H'\cap gHg^{-1})}\left(\mathrm{Res}^{gHg^{-1}}_{H'\cap gHg^{-1}}(\mathbb{Z}_p), \mathrm{Res}^{H'}_{H'\cap gHg^{-1}}(\mathbb{Z}_p)\right)\right) \\ &\cong \bigoplus_{H'gH} \mathrm{Ext}^1_{\mathbb{Z}_p(H'\cap gHg^{-1})}(\mathbb{Z}_p, \mathbb{Z}_p)\end{aligned}$$

where the sum is taken over the double cosets $H'gH$. However, we know $H' \cap gHg^{-1}$ acts trivially on $\mathbb{Z}_p$. Therefore we have

$$\begin{aligned}\mathrm{Ext}^1_{\mathbb{Z}_p(H'\cap gHg^{-1})}(\mathbb{Z}_p, \mathbb{Z}_p) &\cong \mathrm{H}^1(H' \cap gHg^{-1}, \mathbb{Z}_p) \\ &= \mathrm{Hom}(H' \cap gHg^{-1}, \mathbb{Z}_p) = 0.\end{aligned}$$

As this is true for all double cosets $H'gH$, then we have our result. □

We now want use the results in this section to calculate group cohomology associated to $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in T_n . However, before we look at this, we will look at the modular representation theory associated to $\mathcal{G}_n$ in order to further understand the $\mathbb{Z}_p[\mathcal{G}_n]$-lattices and their group cohomology.

3.3 Modular Representation Theory of $\mathcal{G}_n$

In this section, we look at the modular representation theory of $\mathcal{G}_n$. We are interested in the $\mathbb{F}_p[\mathcal{G}_n]$-module

$$\overline{T}_{(n)} = T_{(n)} \otimes_{\mathbb{Z}_p} \mathbb{F}_p = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p).$$

We want to classify all its $\mathbb{F}_p[\mathcal{G}_n]$-submodules. In order to find them, we will require the study of the $\mathbb{F}_p[\mathcal{I}_n]$-module $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$. Using this, we are able to find all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ by inducing the submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$ to $\mathcal{G}_n$. We can then find the remaining $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ by looking at the irreducible $\mathbb{F}_p$-representations of $\mathcal{G}_n$.

We then look at the group cohomology results associated to these $\mathbb{F}_p[\mathcal{G}_n]$-modules. Again, this will initially require looking at the group cohomologies of the $\mathbb{F}_p[\mathcal{I}_n]$-modules we have found as well as the irreducible $\mathbb{F}_p$-representations of $\mathcal{G}_n$.

3.3.1 Module Structure

We initially want to find all the $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$. This will first require finding all the $\mathbb{F}_p[\mathcal{I}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$.

We will look at the irreducible $\mathbb{F}_p[\mathcal{I}_n]$-representations. The kernel of the surjective reduction mapping $\mathcal{I}_n \to \mathcal{B}_0$ is a normal p-group. Therefore, the irreducible $\mathbb{F}_p$-representations of $\mathcal{I}_n$ are the same as the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_0$. We know that the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_0$ are all 1-dimensional and take the form V_t for $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ with character $\beta_t : \mathcal{B}_0 \to \mathbb{F}_p^\times$ such that

$$\beta_t\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) = u^t$$

as seen in [18, Section 7.2]. Hence, the irreducible $\mathbb{F}_p$-representations of $\mathcal{I}_n$ are of the form V_t with $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ and character $\beta_t : \mathcal{I}_n \to \mathbb{F}_p^\times$ such that

$$\beta_t\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) = u^t + p\Big(\mathbb{Z}/p^{n+1}\mathbb{Z}\Big).$$

For all $0 \leq t \leq p-2$, define

$$M_n^t := \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(V_t) = \Big\{f : \mathcal{I}_n \to \mathbb{F}_p \mid f\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) = u^t f\left(\begin{smallmatrix} 1 & 0 \\ w & 1 \end{smallmatrix}\right)\Big\}.$$

Then M_n^t is an $\mathbb{F}_p[\mathcal{I}_n]$-module with dimension p^n as an $\mathbb{F}_p$-vector space. By definition, $\mathcal{I}_n$ acts on M_n^t by $(h \cdot f)(g) = f(gh)$. Now, we saw in Lemma 3.1.2 that $\mathcal{I}_n$ is generated by the matrices $x := \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$, $y := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $b := \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where c generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. Therefore, the action of $\mathcal{I}_n$ is defined by the action of these generators and we have

$$\begin{aligned}
(x \cdot f)\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) &= f\left(\begin{smallmatrix} u+vp & v \\ w+p & 1 \end{smallmatrix}\right) = u^t f\left(\begin{smallmatrix} 1 & 0 \\ w+p & 1 \end{smallmatrix}\right) \\
(y \cdot f)\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) &= f\Big(\begin{smallmatrix} u(w+1)^{-1} & (u+v)(w+1)^{-1} \\ w(w+1)^{-1} & 1 \end{smallmatrix}\Big) = u^t f\Big(\begin{smallmatrix} 1 & 0 \\ w(w+1)^{-1} & 1 \end{smallmatrix}\Big) \\
(b \cdot f)\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) &= f\left(\begin{smallmatrix} cu & v \\ cw & 1 \end{smallmatrix}\right) = (cu)^t f\left(\begin{smallmatrix} 1 & 0 \\ cw & 1 \end{smallmatrix}\right).
\end{aligned}$$

We will prove the following.

Proposition 3.3.1. *For all $n \geq 1$ and $0 \leq t \leq p-2$, M_n^t is uniserial as an $\mathbb{F}_p[\mathcal{I}_n]$-module.*

Before proving this, we require the following.

Lemma 3.3.2. *For all $n \geq 1$ and $0 \leq t \leq p-2$,*

$$M_n^t \cong \mathrm{Ind}^{\mathcal{U}_n}(\mathbb{F}_p) = \mathrm{Maps}(\mathcal{U}_n \to \mathbb{F}_p)$$

as $\mathbb{F}_p[\mathcal{U}_n]$-modules.

Proof. We let $\rho_n : M_n^t \to \mathrm{Ind}^{\mathcal{U}_n}(\mathbb{F}_p)$ take a map to its restriction to $\mathcal{U}_n$. Then it is clear that ρ_n is an $\mathbb{F}_p[\mathcal{U}_n]$-homomorphism as $x \cdot \rho_n(f) = x \cdot f = \rho_n(x \cdot f)$ for all $0 \leq t \leq p-2$. As f is determined by elements of $\mathcal{U}_n$, ρ_n is both surjective and injective which gives the result. □

Proof of Proposition 3.3.1. We know $\mathcal{U}_n \leq \mathcal{I}_n$, so any $\mathbb{F}_p[\mathcal{I}_n]$-submodule of M_n^t is an $\mathbb{F}_p[\mathcal{U}_n]$-submodule. However, $M_n^t \cong \mathrm{Ind}^{\mathcal{U}_n}(\mathbb{F}_p) \cong \mathbb{F}_p[\mathcal{U}_n]$ as $\mathbb{F}_p[\mathcal{U}_n]$-modules by Lemma 3.3.2 and as $\mathcal{U}_n$ is a cyclic p-group, $\mathbb{F}_p[\mathcal{U}_n]$ is uniserial as an $\mathbb{F}_p[\mathcal{U}_n]$-module by [37, Theorem 6.1.2]. Therefore, M_n^t is uniserial as an $\mathbb{F}_p[\mathcal{U}_n]$-module and hence as an $\mathbb{F}_p[\mathcal{I}_n]$-module for all $0 \leq t \leq p-2$. □

We also look at the induced module $\mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(V_t)$ for $1 \leq k \leq n$, which we define as the set of functions $f : \mathcal{I}_n \to \mathbb{F}_p$ such that

$$f\begin{pmatrix} u & v \\ zp^{k+1}+wp & 1 \end{pmatrix} = u^t f\begin{pmatrix} 1 & 0 \\ wp & 1 \end{pmatrix}$$

for all $0 \leq z \leq p^{n-k}-1$ and $0 \leq w \leq p^k - 1$. This is an $\mathbb{F}_p[\mathcal{I}_n]$-module which has dimension p^k as an $\mathbb{F}_p$-vector space. In particular, we have $\mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(V_t) \cong M_k^t$ as $\mathbb{F}_p[\mathcal{I}_n]$-modules. Also, $\mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(V_t)$ are $\mathbb{F}_p[\mathcal{I}_n]$-submodules of M_n^t for $1 \leq k \leq n$ and $0 \leq t \leq p-2$.

We will need this to look at the module structure of $M_n := M_n^0$. We shift our focus to the $k = 1$ case to obtain the following.

Theorem 3.3.3. *Let* $E_p^t := \mathrm{Ind}_{\mathcal{I}_n^1}^{\mathcal{I}_n}(V_t)$ *for all* $0 \leq t \leq p-2$ *and define for all* $1 \leq j \leq p-1$

$$E_j^t := \left\{ f \in E_p^t \;\middle|\; \forall\ 0 \leq m \leq p-1-j,\ \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^m = 0 \right\}.$$

Then for all such j, E_j^t *are* $\mathbb{F}_p[\mathcal{I}_n]$*-modules such that* $\dim_{\mathbb{F}_p}(E_j^t) = j$ *and there exist non-split short exact sequences of* $\mathbb{F}_p[\mathcal{I}_n]$*-modules*

$$0 \to E_j^t \xrightarrow{g_j^t} E_{j+1}^t \xrightarrow{h_j^t} V_{j+t} \to 0$$

where g_j^t *is the inclusion map and*

$$h_j^t(f) = \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j}.$$

Proof. Obviously, $\ker(h_j^t) = \mathrm{im}(g_j^t)$ and g_j^t is an injective $\mathbb{F}_p[\mathcal{I}_n]$-homomorphism. Therefore, we just need to show that h_j^t is a surjective $\mathbb{F}_p[\mathcal{I}_n]$-homomorphism. Now, x and y act trivially on V_j for all $0 \leq j \leq p-2$,

$$\begin{aligned}
h_j^t(x \cdot f) &= \sum_{i=0}^{p-1} (x \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ (i+1)p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) (i-1)^{p-1-j} \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) \sum_{m=0}^{p-1-j} \binom{p-1-j}{m} i^m (-1)^{p-1-j-m} \\
&= \sum_{m=0}^{p-1-j} \binom{p-1-j}{m} (-1)^{p-1-j-m} \left(\sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^m \right) \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= h_j^t(f)
\end{aligned}$$

as for all $0 \leq m \leq p-2-j$, we have $\sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^m = 0$. Also, we have

$$\begin{aligned}
h_j^t(y \cdot f) &= \sum_{i=0}^{p-1} (y \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} (ip+1)^{-1} & (ip+1)^{-1} \\ i(ip+1)^{-1}p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= \sum_{i=0}^{p-1} \left((ip+1)^{-1}\right)^t f\left(\begin{smallmatrix} 1 & 0 \\ i(ip+1)^{-1}p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= h_j^t(f)
\end{aligned}$$

for all $1 \leq j \leq p-1$ as $i(ip+1)^{-1}p \equiv ip \pmod{p^2}$ and as $f \in \mathrm{Ind}_{\mathcal{I}_n^1}^{\mathcal{I}_n}(V_t)$. Finally, we have

$$\begin{aligned} h_j^t(b \cdot f) &= \sum_{i=0}^{p-1} (b \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^{p-1-j} \\ &= \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} c & 0 \\ cip & 1 \end{smallmatrix}\right) i^{p-1-j} \\ &= c^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ cip & 1 \end{smallmatrix}\right) (ci)^{p-1-j} \\ &= c^{t+j} \sum_{m=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ mp & 1 \end{smallmatrix}\right) m^{p-1-j} \\ &= b \cdot h_j^t(f), \end{aligned}$$

for all $1 \leq j \leq p-1$. Therefore, h_j^t is an $\mathbb{F}_p[\mathcal{I}_n]$-homomorphism for all $1 \leq j \leq p-1$. We need to show that the h_j^t are surjective. If $a \in \mathbb{F}_p$, then define $f \in E_p^t$ such that $f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) = -i^j a$. Then

$$\sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip & 1 \end{smallmatrix}\right) i^m = -a \sum_{i=0}^{p-1} i^{m+j} = 0$$

when $0 \leq m \leq p-2-j$ as $1 \leq j \leq m+j \leq p-2$ and by [9, pg. 137]. Therefore, $f \in E_{j+1}^t$ and we have

$$h_j^t(f) = -a \sum_{i=0}^{p-1} i^{p-1} = -a(p-1) = a$$

for all $1 \leq j \leq p-1$. Therefore, h_j^t are surjective for all $1 \leq j \leq p-1$ and $0 \leq t \leq p-2$. Finally, the short exact sequences are all non-split due to M_n^t being uniserial as an $\mathbb{F}_p[\mathcal{I}_n]$-module by Proposition 3.3.1. □

We will now look at the $k \geq 2$ cases. We in fact have the following theorem, which extends the $k = 1$ case but written in a separate theorem to make the construction clearer.

Theorem 3.3.4. *Let* $E^t_{p^k} := \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(V_t)$ *for all* $0 \leq t \leq p-2$ *and* $2 \leq k \leq n$. *For all* $1 \leq j \leq p-1$, *let* $E^t_{jp^{k-1}}$ *be defined as*

$$\left\{ f \in E^t_{p^k} \;\middle|\; \forall\ 0 \leq m \leq p-1-j,\ \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip^k+zp & 1 \end{smallmatrix}\right) i^m = 0 \text{ for all } 0 \leq z \leq p^{k-1}-1 \right\}.$$

Then for all such j, $E^t_{jp^{k-1}}$ *are* $\mathbb{F}_p[\mathcal{I}_n]$*-modules such that* $\dim_{\mathbb{F}_p}(E^t_{jp^{k-1}}) = jp^{k-1}$ *and there exist non-split short exact sequences of* $\mathbb{F}_p[\mathcal{I}_n]$*-modules*

$$0 \to E^t_{jp^{k-1}} \xrightarrow{g^t_{j,k}} E^t_{(j+1)p^{k-1}} \xrightarrow{h^t_{j,k}} \mathrm{Ind}_{\mathcal{I}_n^{k-1}}^{\mathcal{I}_n}(V_{t+j}) \to 0$$

where $g^t_{j,k}$ *is the inclusion map and*

$$h^t_{j,k}(f)\left(\begin{smallmatrix} u & v \\ zp^k+wp & 1 \end{smallmatrix}\right) = u^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip^k+wp & 1 \end{smallmatrix}\right) i^{p-1-j}$$

for $0 \leq z \leq p^{n-k+1}-1$ *and* $0 \leq w \leq p^{k-1}-1$.

Proof. Again, we just need to show that $h^t_{j,k}$ is a surjective $\mathbb{F}_p[\mathcal{I}_n]$-homomorphism. For all $1 \leq j \leq p-1$, we have

$$\begin{aligned}
h^t_{j,k}(x \cdot f)\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right) &= u^{t+j} \sum_{i=0}^{p-1} (x \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip^k+wp & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= u^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip^k+(w+1)p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= (u+vp)^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip^k+(w+1)p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= h^t_{j,k}(f)\left(\begin{smallmatrix} u+vp & v \\ (w+1)p & 1 \end{smallmatrix}\right) \\
&= [x \cdot h^t_{j,k}(f)]\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right)
\end{aligned}$$

and so $h^t_{j,k}(x \cdot f) = x \cdot h^t_{j,k}(f)$ for all $1 \leq j \leq p-1$. Also, we have

$$\begin{aligned}
h^t_{j,k}(y \cdot f)\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right) &= u^{t+j} \sum_{i=0}^{p-1} (y \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip^k+wp & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= u^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} (ip^k+wp+1)^{-1} & (ip^k+wp+1)^{-1} \\ (ip^k+wp)(ip^k+wp+1)^{-1} & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= u^{t+j} \sum_{i=0}^{p-1} [(ip^k+wp+1)^{-1}]^t f\left(\begin{smallmatrix} 1 & 0 \\ (ip^k+wp)(ip^k+wp+1)^{-1} & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= (u(wp+1)^{-1})^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ ip^k+w(wp+1)^{-1}p & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= h^t_{j,k}(f)\left(\begin{smallmatrix} u(wp+1)^{-1} & (u+v)(wp+1)^{-1} \\ w(wp+1)^{-1}p & 1 \end{smallmatrix}\right) \\
&= [y \cdot h^t_{j,k}(f)]\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right)
\end{aligned}$$

and so $h^t_{j,k}(y \cdot f) = y \cdot h^t_{j,k}(f)$ for all $1 \leq j \leq p-1$. This is due to

$$ip^k + wp + 1 \equiv wp + 1 \pmod{p^k},$$

so

$$\begin{aligned}
(ip^{k-1}+w)(ip^k+wp+1)^{-1}p &\equiv (ip^{k-1}+w)(wp+1)^{-1}p \pmod{p^{k+1}} \\
&\equiv ip^k + w(wp+1)^{-1}p \pmod{p^{k+1}}
\end{aligned}$$

and as $f \in \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(V_t)$. Finally, we have

$$\begin{aligned}
h^t_{j,k}(b \cdot f)\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right) &= u^{t+j} \sum_{i=0}^{p-1} (b \cdot f)\left(\begin{smallmatrix} 1 & 0 \\ ip^k+wp & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= u^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} c & 0 \\ cip^k+cwp & 1 \end{smallmatrix}\right) i^{p-1-j} \\
&= (cu)^{t+j} \sum_{i=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ cip^k+cwp & 1 \end{smallmatrix}\right) (ci)^{p-1-j} \\
&= (cu)^{t+j} \sum_{m=0}^{p-1} f\left(\begin{smallmatrix} 1 & 0 \\ mp^k+cwp & 1 \end{smallmatrix}\right) m^{p-1-j} \\
&= h^t_{j,k}(f)\left(\begin{smallmatrix} cu & v \\ cwp & 1 \end{smallmatrix}\right) \\
&= [b \cdot h^t_{j,k}(f)]\left(\begin{smallmatrix} u & v \\ wp & 1 \end{smallmatrix}\right)
\end{aligned}$$

and so $h^t_{j,k}(b\cdot f) = b\cdot h^t_{j,k}(f)$ for all $1\leq j\leq p-1$. Therefore, $h^t_{j,k}$ is an $\mathbb{F}_p[\mathcal{I}_n]$-homomorphism for all $1\leq j\leq p-1$ and $0\leq t\leq p-2$. We need to show that the $h^t_{j,k}$ are surjective. If $g\in \mathrm{Ind}_{\mathcal{I}_n^{k-1}}^{\mathcal{I}_n}(V_{k+j})$, then define $f\in \mathrm{Ind}_{\mathcal{I}_n^{k}}^{\mathcal{I}_n}(V_t)$ such that $f\left(\begin{smallmatrix}1 & 0\\ ip^k+wp & 1\end{smallmatrix}\right) = -i^j g\left(\begin{smallmatrix}1 & 0\\ wp & 1\end{smallmatrix}\right)$ for all $0\leq i\leq p-1$ and $0\leq w\leq p^{k-1}-1$. Then

$$\sum_{i=0}^{p-1} f\left(\begin{smallmatrix}1 & 0\\ ip^k+wp & 1\end{smallmatrix}\right) i^m = -g\left(\begin{smallmatrix}1 & 0\\ wp & 1\end{smallmatrix}\right)\sum_{i=0}^{p-1} i^{m+j} = 0$$

when $0\leq m\leq p-2-j$ as $1\leq j\leq m+j\leq p-2$ and by [9, pg. 137]. Therefore, $f\in E^t_{(j+1)p^{k-1}}$ and we have

$$\begin{aligned} h^t_{j,k}(f)\left(\begin{smallmatrix}u & v\\ wp & 1\end{smallmatrix}\right) &= u^{t+j}\sum_{i=0}^{p-1} f\left(\begin{smallmatrix}1 & 0\\ ip^k+wp & 1\end{smallmatrix}\right) i^{p-1-j}\\ &= -u^{t+j} g\left(\begin{smallmatrix}1 & 0\\ wp & 1\end{smallmatrix}\right)\sum_{i=0}^{p-1} i^{p-1}\\ &= u^{t+j} g\left(\begin{smallmatrix}1 & 0\\ wp & 1\end{smallmatrix}\right)\\ &= g\left(\begin{smallmatrix}u & v\\ wp & 1\end{smallmatrix}\right)\end{aligned}$$

meaning $g = h^t_{j,k}(f)$ for all $1\leq j\leq p-1$. Therefore, $h^t_{j,k}$ is surjective for all $1\leq j\leq p-1$ and $0\leq t\leq p-2$. Finally, the short exact sequences are all non-split due to M_n^k being uniserial as an $\mathbb{F}_p[\mathcal{I}_n]$-module by Proposition 3.3.1. □

Then we have the unique Jordan-Hölder decomposition of M_n for all $n\geq 1$ by Theorem 3.3.3 and Theorem 3.3.4.

Example. *Let $p=5$ and $n=2$. We have 4 irreducible $\mathbb{F}_5[\mathcal{I}_2]$-representations of the form V_j for $0\leq j\leq 3$. Let $E_{25} := M_2$ and for all $1\leq k\leq 24$, let E_k be the unique $\mathbb{F}_5[\mathcal{I}_2]$-submodule of E_{25} such that $\dim_{\mathbb{F}_5}(E_k) = k$. Then by Theorem 3.3.4, we have the decomposition*

$$E_{25}\supseteq E_{20}\supseteq E_{15}\supseteq E_{10}\supseteq E_5\supseteq 0$$

where ${}^{E_{5(m+1)}}\!/_{E_{5m}} \cong \mathrm{Ind}_{\mathcal{I}_2^1}^{\mathcal{I}_2}(V_m)$ as $\mathbb{F}_5[\mathcal{I}_2]$-modules for all $0\leq m\leq 4$. By Theorem 3.3.3, we must have the following unique Jordan-Hölder decomposition of E_{25}

$$\begin{array}{ccccccccccccccccccc}
E_{25} & & E_{24} & & E_{23} & & E_{22} & & E_{21} & & E_{20} \\
& V_0 & & V_3 & & V_2 & & V_1 & & V_0 & \\
E_{20} & & E_{19} & & E_{18} & & E_{17} & & E_{16} & & E_{15} \\
& V_3 & & V_2 & & V_1 & & V_0 & & V_3 & \\
E_{15} & & E_{14} & & E_{13} & & E_{12} & & E_{11} & & E_{10} \\
& V_2 & & V_1 & & V_0 & & V_3 & & V_2 & \\
E_{10} & & E_9 & & E_8 & & E_7 & & E_6 & & E_5 \\
& V_1 & & V_0 & & V_3 & & V_2 & & V_1 & \\
E_5 & & E_4 & & E_3 & & E_2 & & E_1 & & E_0. \\
& V_0 & & V_3 & & V_2 & & V_1 & & V_0 &
\end{array}$$

In particular, using Theorem 3.3.3 and Theorem 3.3.4, we have shown the following.

Theorem 3.3.5. *For all $n \geq 1$, let $E_{p^n} := M_n$ and let E_i be the unique $\mathbb{F}_p[\mathcal{I}_n]$-submodule of E_{p^n} such that $\dim_{\mathbb{F}_p}(E_i) = i$ for all $1 \leq i \leq p^n$. Define $d_n := \frac{p^n-1}{p-1}$. Then we have ${}^{E_{p^n}}\!/_{E_{p^n-1}} \cong V_0$ and*

$${}^{E_{m(p-1)+k+1}}\!/_{E_{m(p-1)+k}} \cong V_k \qquad \text{for all } 0 \leq m \leq d_n - 1 \text{ and } 0 \leq k \leq p-2.$$

We now shift our focus to $\mathbb{F}_p[\mathcal{G}_n]$-modules. For all $1 \leq t \leq p^n$, we let $K_t := \mathrm{Ind}_{\mathcal{I}_n}^{\mathcal{G}_n}(E_t)$. Then we know we have the chain of $\mathbb{F}_p[\mathcal{G}_n]$-modules

$$K_{p^n} \supsetneq K_{p^n-1} \supsetneq K_{p^n-2} \supsetneq ... \supsetneq K_1 \supsetneq 0$$

where $\dim_{\mathbb{F}_p}(K_t) = t(p+1)$. We require the following.

Theorem 3.3.6. *[22, Theorem 2.2.9] Let $H \leq G$ be finite groups and R a commutative ring. Suppose there exists an exact sequence*

$$0 \to U \to V \to W \to 0$$

of $R[H]$-modules. Then we have a short exact sequence of $R[G]$-modules

$$0 \to \mathrm{Ind}_H^G(U) \to \mathrm{Ind}_H^G(V) \to \mathrm{Ind}_H^G(W) \to 0.$$

In particular, if U is an $R[H]$-submodule of V, then

$$\mathrm{Ind}_H^G\left({}^{V}\!/_{U}\right) \cong {}^{\mathrm{Ind}_H^G(V)}\!/_{\mathrm{Ind}_H^G(U)}.$$

Therefore, we define $\sigma_t := \mathrm{Ind}_{\mathcal{I}_n}^{\mathcal{G}_n}(V_t)$ for $0 \leq t \leq p-2$ in order to follow the notation as seen in [18, Chapter 7]. Then using Theorem 3.3.6, we have the short exact sequence

$$0 \to K_{p^n-1} \to K_{p^n} \to \sigma_0 \to 0$$

and for all $0 \leq m \leq d_n - 1$ and $0 \leq t \leq p-2$, we have the short exact sequences of $\mathbb{F}_p[\mathcal{G}_n]$-modules

$$0 \to K_{m(p-1)+t} \to K_{m(p-1)+t+1} \to \sigma_t \to 0.$$

We also see from [18, Chapter 7] that the irreducible $\mathbb{F}_p[\mathcal{G}_n]$-representations take the form

$$\tau_{j,1} = \mathrm{Sym}^{j-1} \otimes \det^{\frac{1-j}{2}} \quad \textit{or} \quad \tau_{j,2} = \tau_{j,1} \otimes \tau$$

for $j \in \{1, 3, ..., p\}$ where τ is the non-trivial 1-dimensional $\mathbb{F}_p[\mathcal{G}_n]$-representation. Here, Sym^{j-1} can be viewed as degree $j-1$ homogeneous polynomials over $\mathbb{F}_p$ in two variables, which is acted on by $\mathcal{G}_n$ by linear substitution, and

$$\det : \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{F}_p^\times$$

is the determinant function.

We also see from [18, Chapter 7] that $\sigma_t \cong \sigma_{p-1-t}$ as $\mathbb{F}_p[\mathcal{G}_n]$-modules for all $1 \leq t \leq \frac{p-3}{2}$. Also, $\sigma_0 = \mathbb{F}_p \oplus \mathrm{St}$ as $\mathbb{F}_p[\mathcal{G}_n]$-modules where $\mathrm{St} = \tau_{p,2}$ is the Steinberg representation and $\sigma_{\frac{p-1}{2}} = \sigma_0 \otimes \tau = \tau \oplus (\mathrm{St} \otimes \tau)$. For the remaining representations, we have $\sigma_t^{\mathrm{ss}} = \tau_{2t+1,1} \oplus \tau_{p-2t,2}$ for all $1 \leq t \leq \frac{p-3}{2}$. We in fact have the following.

Proposition 3.3.7. *Let $n \geq 1$ and $0 \leq t \leq \frac{p-1}{2}$. Then we have the short exact sequences of $\mathbb{F}_p[\mathcal{G}_n]$-modules*

$$0 \to \tau_{p-2t,2} \to \sigma_t \to \tau_{2t+1,1} \to 0$$

which splits only when $t \in \left\{0, \frac{p-1}{2}\right\}$.

Proof. Let W be an irreducible $\mathbb{F}_p[\mathcal{G}_n]$-submodule of σ_t. Then we know W must either be $\tau_{2t+1,1}$, $\tau_{p-2t,2}$ or both. Let

$$W_H = {}^{W}\!/_{\langle (h-1)W:\, h\in H\rangle}$$

for $H \leq \mathcal{G}_n$. Then as $\sigma_t = \mathrm{Ind}_{\mathcal{I}_n}^{\mathcal{G}_n}(V_t)$, we have

$$\begin{aligned}\mathrm{Hom}_{\mathbb{F}_p[\mathcal{G}_n]}(W, \sigma_t) &\cong \mathrm{Hom}_{\mathbb{F}_p[\mathcal{I}_n]}(W, V_t)\\ &\cong \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathcal{I}_n}, V_t)\\ &\cong \mathrm{Hom}_{\mathbb{F}_p[{}^{\mathcal{I}_n}\!/_{\mathcal{P}_n}]}(W_{\mathcal{P}_n}, V_t).\end{aligned}$$

We know that $\mathcal{P}_n$ is generated by $\left(\begin{smallmatrix}1 & 0\\ p & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}p+1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Therefore, we would like to view the action of W on these matrices. As W is an irreducible $\mathbb{F}_p[\mathcal{G}_n]$-representation, we can view W having an underlying representation isomorphic to either $\tau_{j,1}$ or $\tau_{j,2}$ for $j \in \{1, 3, ..., p\}$ as defined earlier. Firstly, if we let $\det : \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{F}_p^{\times}$ be the determinant map, then

$$\det\left(\begin{smallmatrix}1 & 0\\ p & 1\end{smallmatrix}\right) = \det\left(\begin{smallmatrix}p+1 & 0\\ 0 & 1\end{smallmatrix}\right) = 1.$$

Also, as Sym^{j-1} can be viewed as degree $j-1$ homogeneous polynomials over $\mathbb{F}_p$ in two variables, which we denote $\mathbb{F}_p[u, v]$, then

$$\left(\begin{smallmatrix}1 & 0\\ p & 1\end{smallmatrix}\right) \cdot u^{j-1-i}v^i = (u+pv)^{j-1-i}v^i = u^{j-1-i}v^i$$

and

$$\left(\begin{smallmatrix}p+1 & 0\\ 0 & 1\end{smallmatrix}\right) \cdot u^{j-1-i}v^i = u^{j-1-i}v^i.$$

Therefore, this shows that these matrices fix $\tau_{j,1}$ and $\tau_{j,2}$ for all $j \in \{1, 3, ..., p\}$ and so $W_{\mathcal{P}_n} = W_{\mathcal{H}_n}$ where $\mathcal{H}_n$ is cyclic. If $\overline{a}$ is a representative of a coset in ${}^{\mathcal{I}_n}\!/_{\mathcal{P}_n}$, the representation underlying $\tau_{2t+1,1}$ maps $\overline{a}$ to a^{-t} and the representation underlying $\tau_{p-2t,2}$ maps $\overline{a}$ to a^t. Hence for $W_{\mathcal{H}_n} = V_t$ where V_t maps $\overline{a}$ to a^t, then we must have $W = \tau_{p-2t,2}$ for all $0 \leq t \leq \frac{p-1}{2}$ and further, $W = \tau_{2t+1,1}$ for $t \in \left\{0, \frac{p-1}{2}\right\}$. □

We can now look for the other $\mathbb{F}_p[\mathcal{G}_n]$-submodules of K_{p^n}. Let $J_{m,t}$ be the unique $\mathbb{F}_p[\mathcal{G}_n]$-modules such that $K_{m(p-1)+t} \subsetneq J_{m,t} \subsetneq K_{m(p-1)+t+1}$ for all

$0 \leq m \leq d_n - 1$ and $1 \leq t \leq p-2$ such that $t \neq \frac{p-1}{2}$. Then we have the short exact sequences

$$0 \to K_{m(p-1)+t} \to J_{m,t} \to \tau_{p-2t,2} \to 0$$

and

$$0 \to J_{m,t} \to K_{m(p-1)+t+1} \to \tau_{2t+1,1} \to 0.$$

For $t = \frac{p-1}{2}$, there exist $\mathbb{F}_p[\mathcal{G}_n]$-submodules Γ_m, Δ_m for all $0 \leq m \leq d_n - 1$ such that we have the short exact sequences

$$0 \to K_{m(p-1)+\frac{p-1}{2}} \to \Gamma_m \to \tau \to 0$$

and

$$0 \to K_{m(p-1)+\frac{p-1}{2}} \to \Delta_m \to \mathrm{St} \otimes \tau \to 0.$$

Finally, there exists $\mathbb{F}_p[\mathcal{G}_n]$-submodules Θ_m, Λ_m for all $0 \leq m \leq d_n$ such that we have the short exact sequences

$$0 \to K_{m(p-1)} \to \Theta_m \to \mathbb{F}_p \to 0$$

and

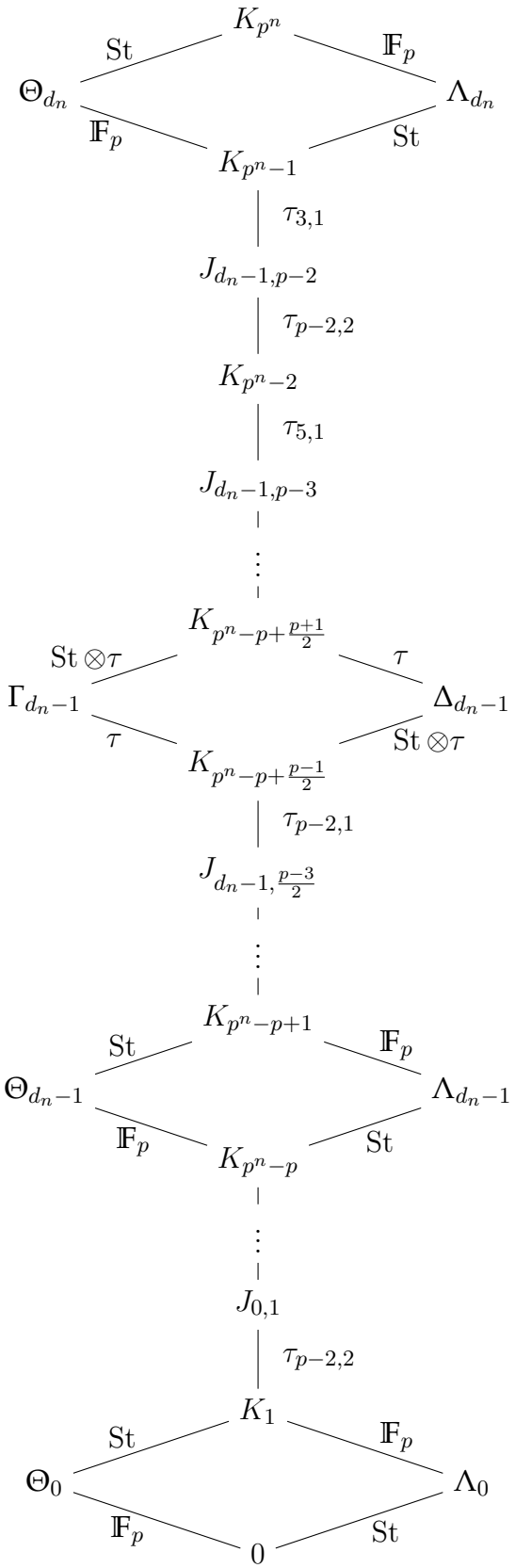
$$0 \to K_{m(p-1)} \to \Lambda_m \to \mathrm{St} \to 0$$

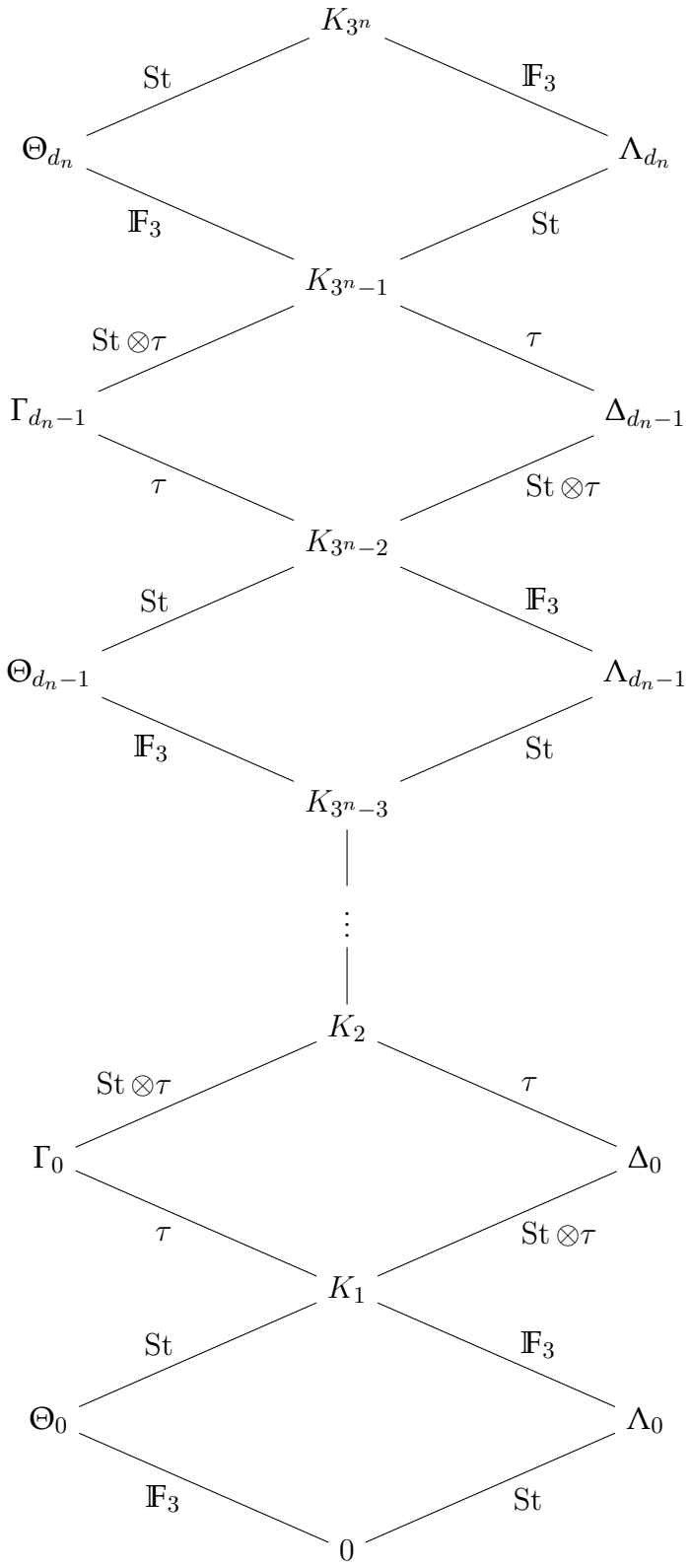
where $K_0 = 0$. In particular, we have $\Theta_0 = \mathbb{F}_p$ and $\Lambda_0 = \mathrm{St}$. Therefore, we have shown the following.

Theorem 3.3.8. *Let $n \geq 1$ and $d_n = \frac{p^n-1}{p-1}$. Then we classify all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ and their dimension as $\mathbb{F}_p$-vector spaces as the following:*

1. *K_t for $1 \leq t \leq p^n$ such that $\dim_{\mathbb{F}_p}(K_t) = t(p+1)$,*
2. *$J_{m,t}$ for $0 \leq m \leq d_n - 1$ and $1 \leq t \leq p-2$, $t \neq \frac{p-1}{2}$ such that $\dim_{\mathbb{F}_p}(J_{m,t}) = [m(p+1)+t](p-1)+p$,*
3. *Γ_m for $0 \leq m \leq d_n - 1$ and $\dim_{\mathbb{F}_p}(\Gamma_m) = m(p^2-1) + \frac{p^2+1}{2}$,*
4. *Δ_m for $0 \leq m \leq d_n - 1$ and $\dim_{\mathbb{F}_p}(\Delta_m) = m(p^2-1) + \frac{(p+1)^2}{2} - 1$,*
5. *Θ_m for $0 \leq m \leq d_n$ and $\dim_{\mathbb{F}_p}(\Theta_m) = m(p^2-1) + 1$,*
6. *Λ_m for $0 \leq m \leq d_n$ and $\dim_{\mathbb{F}_p}(\Lambda_m) = m(p^2-1) + p$.*

We show on the next couple of pages the diagrams of the decomposition series of K_{p^n} for $p \neq 3$ in the first case and $p = 3$ in the second.


K_{p^n}
St
$\mathbb{F}_p$
Θ_{d_n}
Λ_{d_n}
$\mathbb{F}_p$
St
K_{p^n-1}
$\tau_{3,1}$
$J_{d_n-1,p-2}$
$\tau_{p-2,2}$
K_{p^n-2}
$\tau_{5,1}$
$J_{d_n-1,p-3}$
$K_{p^n-p+\frac{p+1}{2}}$
$\mathrm{St}\otimes\tau$
τ
Γ_{d_n-1}
Δ_{d_n-1}
τ
$\mathrm{St}\otimes\tau$
$K_{p^n-p+\frac{p-1}{2}}$
$\tau_{p-2,1}$
$J_{d_n-1,\frac{p-3}{2}}$
K_{p^n-p+1}
St
$\mathbb{F}_p$
Θ_{d_n-1}
Λ_{d_n-1}
$\mathbb{F}_p$
St
K_{p^n-p}
$J_{0,1}$
$\tau_{p-2,2}$
K_1
St
$\mathbb{F}_p$
Θ_0
Λ_0
$\mathbb{F}_p$
St
0


K_{3^n}
St
$\mathbb{F}_3$
Θ_{d_n}
Λ_{d_n}
$\mathbb{F}_3$
St
K_{3^n-1}
St $\otimes\tau$
τ
Γ_{d_n-1}
Δ_{d_n-1}
τ
St $\otimes\tau$
K_{3^n-2}
St
$\mathbb{F}_3$
Θ_{d_n-1}
Λ_{d_n-1}
$\mathbb{F}_3$
St
K_{3^n-3}
$\vdots$
K_2
St $\otimes\tau$
τ
Γ_0
Δ_0
τ
St $\otimes\tau$
K_1
St
$\mathbb{F}_3$
Θ_0
Λ_0
$\mathbb{F}_3$
St
0

3.3.2 Cohomology of $\mathbb{F}_p[\mathcal{G}_n]$-modules

We now want to find the cohomology of the $\mathbb{F}_p[\mathcal{G}_n]$-modules with respect to subgroups of $\mathcal{G}_n$. We first look at the cohomology associated to $\mathcal{G}_n$. For this, we will require the cohomology of the $\mathbb{F}_p[\mathcal{I}_n]$-modules associated to $\mathcal{I}_n$, denoted E_t in the previous section for $1 \leq t \leq p^n$. This will require looking at the cohomology of the irreducible $\mathbb{F}_p[\mathcal{B}_n]$-representations with respect to $\mathcal{B}_n$. We look at the $n = 0$ case first. We have already seen that the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_0$ are all 1-dimensional and take the form V_t for $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ with character $\beta_t : \mathcal{B}_0 \to \mathbb{F}_p^\times$ such that

$$\beta_t\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) = u^t.$$

Lemma 3.3.9. *We have*

$$\mathrm{H}^0(\mathcal{B}_0, V_t) = V_t^{\mathcal{B}_0} = \begin{cases} \mathbb{F}_p & \text{if } t = 0, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathrm{H}^1(\mathcal{B}_0, V_t) \cong \begin{cases} \mathbb{F}_p & \text{if } t = 1, \\ 0 & \text{otherwise,} \end{cases}$$

Proof. The first part comes from the fact that $\beta_t(b) = c^t$ for all $0 \leq t \leq p-2$ and this is equal to 1 if and only if $t = 0$. Here, $b = \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as defined earlier.

For the second part, $\mathcal{H}_0 = \langle y \rangle$ is a normal subgroup of $\mathcal{B}_0$ with quotient isomorphic to $\mathcal{D}_0$ where $y = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ as defined earlier. Therefore, as $\mathcal{H}_0$ acts trivially on V_t for all $0 \leq t \leq p-2$, we have the exact sequence

$$0 \to \mathrm{H}^1(\mathcal{D}_0, V_t) \to \mathrm{H}^1(\mathcal{B}_0, V_t) \to \mathrm{Hom}(\mathcal{H}_0, V_t)^{\mathcal{D}_0} \to \mathrm{H}^2(\mathcal{D}_0, V_t).$$

As $\mathcal{D}_0$ is cyclic of order $p-1$, then for all $0 \leq t \leq p-2$, we have

$$\mathrm{H}^1(\mathcal{D}_0, V_t) = \mathrm{H}^2(\mathcal{D}_0, V_t) = 0$$

and $\mathrm{H}^1(\mathcal{B}_0, V_t) \cong \mathrm{Hom}(\mathcal{H}_0, V_t)^{\mathcal{D}_0}$.

Now, $\mathcal{H}_0$ is a cyclic group of order p, so $\mathrm{Hom}(\mathcal{H}_0, V_t) \cong \mathbb{F}_p$ generated by the mapping f such that $f(y) = 1$. $\mathcal{D}_0$ acts on f by $(b \cdot f)(h) = b \cdot f(b^{-1}hb)$ for $h \in \mathcal{H}_0$. Therefore, $b^{-1}yb = \left(\begin{smallmatrix} 1 & c^{-1} \\ 0 & 1 \end{smallmatrix}\right)$ and so

$$(b \cdot f)(y) = b \cdot f\left(\begin{smallmatrix} 1 & c^{-1} \\ 0 & 1 \end{smallmatrix}\right) = b \cdot c^{-1} = c^{t-1}.$$

As c generates $\mathbb{F}_p^\times$, then f is fixed by b only when $t = 1$. Therefore, we have

$$\mathrm{Hom}(\mathcal{H}_0, V_t)^{\mathcal{D}_0} \cong \begin{cases} \mathbb{F}_p & \text{if } t = 1, \\ 0 & \text{otherwise,} \end{cases}$$

which gives our result. □

We now look at $n \geq 1$. The kernel of the surjective reduction mapping $\mathcal{B}_n \to \mathcal{B}_0$ is a normal p-subgroup of $\mathcal{B}_n$. Therefore, the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_n$ are the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_0$. Therefore, as the irreducible $\mathbb{F}_p$-representations of $\mathcal{B}_n$, we see for V_t with $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $\beta_t : \mathcal{B}_n \to \mathbb{F}_p^\times$ we have

$$\beta_t\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) = u^t + p(\mathbb{Z}/p^{n+1}\mathbb{Z}).$$

We would like to calculate the cohomology associated to these irreducible $\mathbb{F}_p[\mathcal{B}_n]$-representations.

Proposition 3.3.10. *For all $n \geq 1$, we have*

$$\mathrm{H}^0(\mathcal{B}_n, V_t) = V_t^{\mathcal{B}_n} = \begin{cases} \mathbb{F}_p & \textit{if } t = 0, \\ 0 & \textit{otherwise,} \end{cases}$$

and

$$\mathrm{H}^1(\mathcal{B}_n, V_t) \cong \begin{cases} \mathbb{F}_p & \textit{if } t \in \{0, 1\}, \\ 0 & \textit{otherwise,} \end{cases}$$

Proof. The first part is identical to the proof of the first part of Lemma 3.3.9. For the second part, we deal with the $t = 0$ case first. We know $\mathcal{B}_n$ acts trivially on $\mathbb{F}_p$, so we have

$$\mathrm{H}^1(\mathcal{B}_n, \mathbb{F}_p) \cong \mathrm{Hom}(\mathcal{B}_n, \mathbb{F}_p) \cong \mathbb{F}_p$$

by Proposition 3.1.7. We now look at the case $1 \leq t \leq p-2$. We have that $\mathcal{H}_n = \langle y \rangle$ is a normal subgroup of $\mathcal{B}_n$ with quotient isomorphic to $\mathcal{D}_n$.

Therefore, as $\mathcal{H}_n$ acts trivially on V_t for all $1 \leq t \leq p-2$, we have the exact sequence

$$0 \to \mathrm{H}^1(\mathcal{D}_n, V_t) \to \mathrm{H}^1(\mathcal{B}_n, V_t) \to \mathrm{Hom}(\mathcal{H}_n, V_t)^{\mathcal{D}_n} \to \mathrm{H}^2(\mathcal{D}_n, V_t).$$

We first look at $\mathrm{H}^1(\mathcal{D}_n, V_t)$. There exists a surjective mapping $\mathcal{D}_n \to \mathcal{D}_0$ with kernel D_n generated by $\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Therefore, as $\mathcal{D}_0$ is cyclic of order $p-1$, then $\mathrm{H}^1(\mathcal{D}_n, V_t) \cong \mathrm{Hom}(D_n, V_t)^{\mathcal{D}_0}$ as D_n acts trivially on V_t. Now, $\mathrm{Hom}(D_n, V_t)$ is generated by f such that $f(\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = 1$. Then

$$(b \cdot f)(\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = c^t \cdot f(\left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = c^t \neq 1$$

as $1 \leq t \leq p-2$. Therefore, $\mathrm{H}^1(\mathcal{D}_n, V_t) = 0$ for all $1 \leq t \leq p-2$. Also, by the Herbrand quotient, we have $\mathrm{H}^2(\mathcal{D}_n, V_t) = 0$ for all such t and so $\mathrm{H}^1(\mathcal{B}_n, V_t) \cong \mathrm{Hom}(\mathcal{H}_n, V_t)^{\mathcal{D}_n}$.

Now, as $\mathcal{H}_n$ is a cyclic group of order p^{n+1}, then $\mathrm{Hom}(\mathcal{H}_n, V_t) \cong \mathbb{F}_p$ is generated by the mapping f such that $f(y) = 1$. Now, we know $\mathcal{D}_n$ acts on f by $(b \cdot f)(h) = b \cdot f(b^{-1}hb)$. Therefore, as $b^{-1}yb = \left(\begin{smallmatrix} 1 & c^{-1} \\ 0 & 1 \end{smallmatrix}\right)$, then

$$(b \cdot f)(y) = b \cdot f(\left(\begin{smallmatrix} 1 & c^{-1} \\ 0 & 1 \end{smallmatrix}\right)) = b \cdot c^{-1} = c^{t-1}.$$

As c generates $\mathbb{F}_p^\times$, then f is fixed by b only when $t = 1$. Therefore, we have

$$\mathrm{Hom}(\mathcal{H}_n, V_t)^{\mathcal{D}_n} \cong \begin{cases} \mathbb{F}_p & \text{if } t = 1, \\ 0 & \text{otherwise,} \end{cases}$$

which gives our result. □

We now shift our focus to $\mathcal{I}_n^k$ for $0 \leq k \leq n$. As before, the kernel of the surjective reduction mapping $\mathcal{I}_n^k \to \mathcal{B}_k$ is a p-group, so we know all the irreducible $\mathbb{F}_p[\mathcal{I}_n^k]$-representations for all $0 \leq k \leq n$ as we know the irreducible $\mathbb{F}_p[\mathcal{B}_k]$-representations. We now calculate the cohomology associated to the irreducible $\mathbb{F}_p[\mathcal{I}_n^k]$-representations.

Theorem 3.3.11. *For all $0 \leq k \leq n$, we have for $0 \leq t \leq p-2$*

$$\mathrm{H}^0(\mathcal{I}_n^k, V_t) = V_t^{\mathcal{I}_n^k} = \begin{cases} \mathbb{F}_p & \text{if } t = 0, \\ 0 & \text{otherwise,} \end{cases}$$

for $p \neq 3$, we have

$$\mathrm{H}^1(\mathcal{I}_n^k, V_t) \cong \begin{cases} \mathbb{F}_p & \text{if } t \in \{1, p-2\} \text{ or } t = 0 \text{ and } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

and for $p = 3$, we have

$$\mathrm{H}^1(\mathcal{I}_n^k, V_t) \cong \begin{cases} \mathbb{F}_3^2 & \text{if } t = 1 \text{ and } k < n, \\ \mathbb{F}_3 & \text{if } t = 1 \text{ and } k = n \text{ or } t = 0 \text{ and } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

In order to prove this, we shall require the following.

Lemma 3.3.12. *For all $n \geq 1$, we have* $\mathrm{Hom}(\ker(\mu_n), \mathbb{F}_p) \cong \mathbb{F}_p^3$.

Proof. We shall show this for the $n = 1$ case first. There exists a group isomorphism

$$\ker(\mu_1) \to \mathbb{F}_p^3$$
$$\begin{pmatrix} ap+1 & bp \\ cp & 1 \end{pmatrix} \mapsto \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

as

$$\begin{pmatrix} ap+1 & bp \\ cp & 1 \end{pmatrix}\begin{pmatrix} rp+1 & sp \\ zp & 1 \end{pmatrix} = \begin{pmatrix} (a+r)p+1 & (b+s)p \\ (c+z)p & 1 \end{pmatrix}.$$

Therefore, we have

$$\mathrm{Hom}(\ker(\mu_1), \mathbb{F}_p) \cong \mathrm{Hom}(\mathbb{F}_p^3, \mathbb{F}_p) \cong \mathbb{F}_p^3.$$

We now want to prove this for $n > 1$. We have $\mu_n = \mu_1 \circ \mu_n^1$. This is a surjective group homomorphism and we have the short exact sequence

$$0 \to \ker(\mu_n^1) \to \ker(\mu_n) \xrightarrow{\mu_n^1} \ker(\mu_1) \to 0.$$

This induces

$$0 \to \mathrm{Hom}(\ker(\mu_1), \mathbb{F}_p) \xrightarrow{\overline{\mu_n^1}} \mathrm{Hom}(\ker(\mu_n), \mathbb{F}_p) \to \mathrm{Hom}(\ker(\mu_n^1), \mathbb{F}_p)$$

where $\overline{\mu_n^1}(s) = s \circ \mu_n^1$ and the second map restricts the group homomorphism to $\ker(\mu_n^1)$. Let $s \in \mathrm{Hom}(\ker(\mu_n), \mathbb{F}_p)$. Then if we let $\left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right) \in \ker(\mu_n^1)$, we have

$$\left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a-bc & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right)$$

where

$$\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)^{\frac{c}{p}}, \qquad \left(\begin{smallmatrix} a-bc & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} p+1 & 0 \\ 0 & 1 \end{smallmatrix}\right)^{pm} \qquad \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)^{\frac{b}{p}}$$

for some $0 \leq m \leq p^{n-1} - 1$. Therefore, as s is a group homomorphism to $\mathbb{F}_p$, then

$$s\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right) = \frac{c}{p} s\left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right) = 0$$

and similarly for the others. In particular, this ensures that s restricted to $\ker(\mu_n^1)$ is trivial implying $\overline{\mu_n^1}$ is an isomorphism. □

We also require the following.

Lemma 3.3.13. *For all $1 \leq k \leq n$, we have an isomorphism*

$$\ker(\mu_n^k) \cong \ker(\mu_{n-k}).$$

Proof. The isomorphism comes from the mapping

$$\begin{pmatrix} up^{k+1}+1 & vp^{k+1} \\ wp^{k+1} & 1 \end{pmatrix} \mapsto \begin{pmatrix} up+1 & vp \\ wp & 1 \end{pmatrix}$$

for $0 \leq u, v, w \leq p^{n-k} - 1$. □

Therefore, we have the required information to prove Theorem 3.3.11.

Proof of Theorem 3.3.11. The $k = n$ case has been proven in Proposition 3.3.10 as $\mathcal{I}_n^n = \mathcal{B}_n$, so we let $0 \leq k \leq n-1$. If $\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) \in \mathcal{I}_n^k$, then the action on V_t is $\left(\begin{smallmatrix} u & v \\ w & 1 \end{smallmatrix}\right) \cdot 1 = u^t$. Therefore, we have our result for $V_t^{\mathcal{I}_n^k}$.

Now, we have $\ker(\mu_n^k) \trianglelefteq \mathcal{I}_n^k$ and ${}^{\mathcal{I}_n^k}/_{\ker(\mu_n^k)} \cong \mathcal{B}_k$. We also have

$$\ker(\mu_n^k) = \left\langle \begin{pmatrix} 1 & 0 \\ p^{k+1} & 1 \end{pmatrix}, \begin{pmatrix} p^{k+1}+1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & p^{k+1} \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Therefore, $\ker(\mu_n^k)$ acts trivially on V_t for all $0 \leq t \leq p-2$ and we have the exact sequence

$$0 \to \mathrm{H}^1(\mathcal{B}_k, V_t) \to \mathrm{H}^1(\mathcal{I}_n^k, V_t) \to \mathrm{Hom}(\ker(\mu_n^k), V_t)^{\mathcal{B}_k}.$$

We see from Lemma 3.3.9 and Proposition 3.3.10 that

$$\mathrm{H}^1(\mathcal{B}_k, V_t) \cong \begin{cases} \mathbb{F}_p & \text{if } t = 1 \text{ and } k \geq 0 \text{ or } t = 0 \text{ and } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

We now want to show

$$\mathrm{Hom}(\ker(\mu_n^k), V_t)^{\mathcal{B}_k} \cong \begin{cases} \mathbb{F}_p & \text{if } t = p-2, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 3.3.12 and Lemma 3.3.13, we have seen that any element in

$$\mathrm{Hom}(\ker(\mu_n^k), V_t) \cong \mathrm{Hom}(\ker(\mu_{n-k}), V_t)$$

factors through to an element of $\mathrm{Hom}(\ker(\mu_1), V_t)$. Therefore, we can assume $n = 1$ and $k = 0$. The action of $\mathcal{B}_1$ on $\ker(\mu_1)$ factors through the action of $\mathcal{B}_0$ on $\ker(\mu_1)$.

We have seen in Lemma 3.3.12 that there exists an isomorphism of groups

$$\ker(\mu_1) \to \mathbb{F}_p^3$$

$$\begin{pmatrix} ap+1 & bp \\ cp & 1 \end{pmatrix} \mapsto \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

In particular, as the action of an element $m = \left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{B}_0$ on

$$g = \begin{pmatrix} ap+1 & bp \\ cp & 1 \end{pmatrix} \in \ker(\mu_1)$$

is

$$\begin{aligned} m \cdot g = m^{-1}gm &= \left(\begin{smallmatrix} 1 & -s \\ 0 & r \end{smallmatrix}\right)\left(\begin{smallmatrix} ap+1 & bp \\ cp & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} (a-cs)p+1 & bp-s \\ crp & r \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} r(a-cs)p+r & (as+b-cs^2)p \\ cr^2p & r(csp+1) \end{smallmatrix}\right) \\ &= \left(\begin{smallmatrix} (a-2cs)p+1 & r^{-1}(as+b-cs^2)p \\ crp & 1 \end{smallmatrix}\right). \end{aligned}$$

Therefore, the action of $\mathcal{B}_0$ on $\ker(\mu_1)$ using the isomorphism is

$$m \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a-2cs \\ r^{-1}(as+b-cs^2) \\ cr \end{pmatrix}$$

and the matrix relative to the group action is

$$\begin{pmatrix} 1 & 0 & -2s \\ r^{-1}s & r^{-1} & -r^{-1}s^2 \\ 0 & 0 & r \end{pmatrix}.$$

This has characteristic polynomial $(1-\lambda)(r^{-1}-\lambda)(r-\lambda)$ and so the semisimplification of $\ker(\mu_1)$ as an $\mathbb{F}_p[\mathcal{B}_0]$-module is $V_0 \oplus V_1 \oplus V_{p-2}$.

The only irreducible $\mathbb{F}_p[\mathcal{B}_0]$-submodule of $\ker(\mu_1)$ is generated by the element $\left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right)$ which has $\mathcal{B}_0$-representation V_1. Hence, the matrix of the action of $\mathcal{B}_0$ on

$$\ker(\mu_1) \Big/ \left\langle \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right) \right\rangle$$

is $\left(\begin{smallmatrix} 1 & -2s \\ 0 & r \end{smallmatrix}\right)$. Therefore, the only irreducible $\mathbb{F}_p[\mathcal{B}_0]$-submodule of this quotient is generated by the element $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ which has $\mathcal{B}_0$-representation V_0. Therefore, we have the unique Jordan-Hölder decomposition of $\ker(\mu_1)$ as an $\mathbb{F}_p[\mathcal{B}_0]$-module

$$\ker(\mu_1) \xrightarrow[V_{p-2}]{} \left\langle \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right) \right\rangle \xrightarrow[V_0]{} \left\langle \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right) \right\rangle \xrightarrow[V_1]{} 0$$

Therefore, we must have

$$\mathrm{Hom}(\ker(\mu_1), V_t)^{\mathcal{B}_0} \cong \begin{cases} \mathbb{F}_p & \text{if } t = p-2, \\ 0 & \text{otherwise.} \end{cases}$$

as the kernel of an element in this group must be a 2-dimensional $\mathbb{F}_p[\mathcal{B}_0]$-submodule of $\ker(\mu_1)$ and we have shown by its unique Jordan-Hölder decomposition that the only such one has quotient isomorphic to V_{p-2}.

Now, we know from [18, Chapter 7] that $\mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{G}_n}(V_t) \cong \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{G}_n}(V_{p-1-t})$ for all $1 \leq t \leq \frac{p-3}{2}$. Therefore, we have

$$\mathrm{H}^1(\mathcal{I}_n^k, V_t) \cong \mathrm{H}^1\left(\mathcal{G}_n, \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{G}_n}(V_t)\right) \cong \mathrm{H}^1\left(\mathcal{G}_n, \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{G}_n}(V_{p-1-t})\right) \cong \mathrm{H}^1(\mathcal{I}_n^k, V_{p-1-t}).$$

Therefore, we only need to look at the cases for $0 \leq t \leq \frac{p-1}{2}$ when $p \neq 3$, where we have $\mathrm{Hom}(\ker(\mu_n^k), V_t)^{\mathcal{B}_k} = 0$ meaning $\mathrm{H}^1(\mathcal{I}_n^k, V_t) \cong \mathrm{H}^1(\mathcal{B}_k, V_t)$.

Finally, when $p = 3$, we want to show that the restriction mapping

$$\mathrm{res} : \mathrm{H}^1(\mathcal{I}_n^k, V_1) \to \mathrm{Hom}(\ker(\mu_n^k), V_1)^{\mathcal{B}_k}$$

is surjective as this would imply that we have the short exact sequence

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{I}_n^k, V_1) \to \mathbb{F}_p \to 0,$$

which would give our result. We have seen that $\mathrm{Hom}(\ker(\mu_n^k), V_1)^{\mathcal{B}_k} \cong \langle f \rangle$ where

$$f\left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right) = c.$$

Define $\rho : \mathcal{I}_n^k \to V_1$ such that

$$\rho\left(\begin{smallmatrix} a & b \\ 3^{k+1}c & 1 \end{smallmatrix}\right) = c.$$

Then as

$$\left(\begin{smallmatrix} a & b \\ 3^{k+1}c & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ 3^{k+1}u & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ar+3^{k+1}bu & as+b \\ 3^{k+1}(cr+u) & 3^{k+1}cs+1 \end{smallmatrix}\right)$$

and

$$\left(\begin{smallmatrix} r & s \\ 3^{k+1}u & 1 \end{smallmatrix}\right) \cdot \rho\left(\begin{smallmatrix} a & b \\ 3^{k+1}c & 1 \end{smallmatrix}\right) = cr,$$

then we see that $[\rho] \in \mathrm{H}^1(\mathcal{I}_n^k, V_1)$ such that $\mathrm{res}([\rho]) \cong f$. Therefore, res is surjective in this case and so we have our result. □

We now look at the cohomology of E_t for $1 \leq t \leq p^n$ with respect to $\mathcal{I}_n$. We look at the fixed module first.

Lemma 3.3.14. *For all $1 \leq t \leq p^n$, we have $E_t^{\mathcal{I}_n} \cong \mathbb{F}_p$.*

Proof. We know $\mathcal{I}_n$ acts trivially on $E_1 = \mathbb{F}_p$. Therefore, $E_1^{\mathcal{I}_n} = \mathbb{F}_p$. We also see that as $E_{p^n} = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{I}_n}(\mathbb{F}_p)$, then $E_{p^n}^{\mathcal{I}_n} \cong \mathbb{F}_p^{\mathcal{B}_n} = \mathbb{F}_p$. Therefore, as for all $1 \leq t \leq p^n$, we have $E_1 \subseteq E_t \subseteq E_{p^n}$, this gives our result. □

We can now look at the cohomology groups $\mathrm{H}^1(\mathcal{I}_n, E_t)$ for $1 \leq t \leq p^n$. As $E_1 = \mathbb{F}_p$, by Theorem 3.3.11, we have $\mathrm{H}^1(\mathcal{I}_n, E_1) = 0$. We also look at the E_{p^k} cases for $1 \leq k \leq n$.

Lemma 3.3.15. *For all $1 \leq k \leq n$, we have $\mathrm{H}^1(\mathcal{I}_n, E_{p^k}) \cong \mathbb{F}_p$.*

Proof. We have seen that $E_{p^k} = \mathrm{Ind}_{\mathcal{I}_n^k}^{\mathcal{I}_n}(\mathbb{F}_p)$ for all $1 \leq k \leq n$, so we have

$$\mathrm{H}^1(\mathcal{I}_n, E_{p^k}) \cong \mathrm{H}^1(\mathcal{I}_n^k, \mathbb{F}_p)$$

by Shapiro's Lemma. We then use Theorem 3.3.11. □

We can now start to calculate the cohomology of E_t for the other values of t. We have already seen that $\mathrm{H}^1(\mathcal{I}_n, E_1) = 0$. For all $0 \leq m \leq d_n - 1$, we have the short exact sequence

$$0 \to E_{m(p-1)+1} \to E_{m(p-1)+2} \to V_1 \to 0$$

which induces

$$0 \to \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+1}) \to \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+2}) \to \mathbb{F}_p$$

when $p \neq 3$. If $p = 3$, this induces

$$0 \to \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+1}) \to \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+2}) \to \mathbb{F}_p^2.$$

We also have the short exact sequence

$$0 \to E_{m(p-1)+k} \to E_{m(p-1)+k+1} \to V_k \to 0$$

for all $p > 3$ and $2 \leq k \leq p - 3$. Therefore, by Theorem 3.3.11, we have

$$\mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+k}) \cong \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+k+1}).$$

We then have the short exact sequence

$$0 \to E_{m(p-1)+p-2} \to E_{(m+1)(p-1)} \to V_{p-2} \to 0$$

which induces

$$0 \to \mathrm{H}^1(\mathcal{I}_n, E_{m(p-1)+p-2}) \to \mathrm{H}^1(\mathcal{I}_n, E_{(m+1)(p-1)}) \to \mathbb{F}_p.$$

Finally, $0 \leq m \leq d_n - 1$, we have the short exact sequence

$$0 \to E_{(m+1)(p-1)} \to E_{(m+1)(p-1)+1} \to \mathbb{F}_p \to 0$$

which induces

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{I}_n, E_{(m+1)(p-1)}) \to \mathrm{H}^1(\mathcal{I}_n, E_{(m+1)(p-1)+1}) \to 0.$$

We see from these exact sequences and Lemma 3.3.15 that for all $1 \leq k \leq n$, we have $\mathrm{H}^1(\mathcal{I}_n, E_{p^k-1}) \cong \mathbb{F}_p^2$. However, we cannot show precisely the exact first cohomology group for each module, but using magma [7], we can suggest the following.

Conjecture 3.3.16. *For all $n \geq 1$, we have*

$$\mathrm{H}^1(\mathcal{I}_n, E_t) \cong \begin{cases} 0 & \text{if } t = 1, \\ \mathbb{F}_p^2 & \text{if } p-1 | t, \\ \mathbb{F}_p & \text{otherwise,} \end{cases}$$

We can now look at the cohomology of the $\mathbb{F}_p[\mathcal{G}_n]$-modules with respect to $\mathcal{G}_n$. We first recall all the possible $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ as seen in Theorem 3.3.8. Let $n \geq 1$ and $d_n = \frac{p^n-1}{p-1}$. Then we classify all $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$ and their dimension as $\mathbb{F}_p$-vector spaces as the following:

1. K_t for $1 \leq t \leq p^n$ such that $\dim_{\mathbb{F}_p}(K_t) = t(p+1)$,
2. $J_{m,t}$ for $0 \leq m \leq d_n - 1$ and $1 \leq t \leq p-2$, $t \neq \frac{p-1}{2}$ such that $\dim_{\mathbb{F}_p}(J_{m,t}) = [m(p+1)+t](p-1)+p$,
3. Γ_m for $0 \leq m \leq d_n - 1$ and $\dim_{\mathbb{F}_p}(\Gamma_m) = m(p^2-1) + \frac{p^2+1}{2}$,

4. Δ_m for $0 \leq m \leq d_n - 1$ and $\dim_{\mathbb{F}_p}(\Delta_m) = m(p^2-1) + \frac{(p+1)^2}{2} - 1$,
5. Θ_m for $0 \leq m \leq d_n$ and $\dim_{\mathbb{F}_p}(\Theta_m) = m(p^2-1) + 1$,
6. Λ_m for $0 \leq m \leq d_n$ and $\dim_{\mathbb{F}_p}(\Lambda_m) = m(p^2-1) + p$.

We look at the fixed modules first.

Lemma 3.3.17. *Let $n \geq 0$ and W be an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n}. Then we have*

$$W^{\mathcal{G}_n} \cong \begin{cases} 0 & \text{if } W = \Lambda_0, \\ \mathbb{F}_p & \text{otherwise.} \end{cases}$$

Proof. As E_{p^n} is uniserial as an $\mathbb{F}_p[\mathcal{I}_n]$-module with composition series

$$E_{p^n} \supsetneq E_{p^n-1} \supsetneq ... \supsetneq E_1 \supsetneq 0,$$

then we have the series

$$K_{p^n} \supsetneq K_{p^n-1} \supsetneq ... \supsetneq K_1 \supsetneq 0$$

and all other $\mathbb{F}_p[\mathcal{G}_n]$-submodules of K_{p^n} must lie between K_{t-1} and K_t for some $1 \leq t \leq p^n$ with $K_0 = 0$. If W is an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n} such that $K_1 \subseteq W$, as $K_t^{\mathcal{G}_n} \cong E_t^{\mathcal{I}_n} \cong \mathbb{F}_p$ for all $1 \leq t \leq p^n$ by Lemma 3.3.14, then $W^{\mathcal{G}_n} \cong \mathbb{F}_p$.

If W is an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n} such that $W \subsetneq K_1$ then $W \in \{\Theta_0, \Lambda_0\}$. As $\Theta_0 = \mathbb{F}_p$, then $\Theta_0^{\mathcal{G}_n} = \mathbb{F}_p$. We have a short exact sequence

$$0 \to \mathbb{F}_p \to K_1 \to \Lambda_0 \to 0$$

which induces

$$0 \to \mathbb{F}_p \to \mathbb{F}_p \to \Lambda_0^{\mathcal{G}_n} \to 0$$

by Proposition 3.1.6. Therefore $\Lambda_0^{\mathcal{G}_n} = 0$ and we have our result. □

Now we move on to the first cohomology groups. By Shapiro's Lemma, we have

$$\mathrm{H}^1(\mathcal{G}_n, K_t) \cong \mathrm{H}^1(\mathcal{I}_n, E_t)$$

for all $1 \leq t \leq p^n$. Therefore, we want to find the cohomology of the other $\mathbb{F}_p[\mathcal{G}_n]$-submodules of K_{p^n}. We will assume Conjecture 3.3.16. To do this, we need to further understand the irreducible $\mathbb{F}_p[\mathcal{G}_n]$-representations. We have the following.

Lemma 3.3.18. *Let $i \in \{1, 3, ..., p\}$, $j \in \{1, 2\}$ and $\tau_{i,j}$ be the irreducible $\mathbb{F}_p[\mathcal{G}_n]$-representations. Then*

$$\tau_{i,j}^{\mathcal{G}_n} \cong \begin{cases} \mathbb{F}_p & \text{if } i = j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have $\tau_{i,j}^{\mathcal{G}_n} = \mathrm{Hom}_{\mathcal{G}_n}(\mathbb{F}_p, \tau_{i,j})$ by definition. Then by Schur's Lemma, we have our result. □

We start with the smaller sized modules first. As $\mathcal{G}_n$ acts trivially on $\mathbb{F}_p$, then by Proposition 3.1.6, we have $\mathrm{H}^1(\mathcal{G}_n, \mathbb{F}_p) = 0$. We know that $\sigma_0 = \mathbb{F}_p \oplus \mathrm{St}$, so we have the short exact sequence

$$0 \to \mathrm{St} \to \sigma_0 \to \mathbb{F}_p \to 0$$

which induces

$$0 \to \mathbb{F}_p \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, \mathrm{St}) \to 0$$

as $\mathrm{St}^{\mathcal{G}_n} = \mathrm{H}^1(\mathcal{G}_n, \sigma_0) = 0$. Therefore, we have $\mathrm{H}^1(\mathcal{G}_n, \mathrm{St}) = 0$.

Let $1 \leq t \leq \frac{p-3}{2}$. Then by Proposition 3.3.7, we have the short exact sequence

$$0 \to \tau_{p-2t,2} \to \sigma_t \to \tau_{2t+1,1} \to 0$$

which induces

$$0 \to \mathrm{H}^1(\mathcal{G}_n, \tau_{p-2t,2}) \to \mathrm{H}^1(\mathcal{G}_n, \sigma_t).$$

For all $2 \leq t \leq \frac{p-3}{2}$, we have $\mathrm{H}^1(\mathcal{G}_n, \tau_{p-2t,2}) = 0$ as $\mathrm{H}^1(\mathcal{G}_n, \sigma_t) = 0$.

We know that we have a short exact sequence

$$0 \to K_{m(p-1)+t} \to J_{m,t} \to \tau_{p-2t,2} \to 0$$

for all $0 \leq m \leq d_n - 1$ and $1 \leq t \leq \frac{p-3}{2}$. Therefore, this induces the exact sequence

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \to \mathrm{H}^1(\mathcal{G}_n, \tau_{p-2t,2})$$

as $\tau_{p-2t,2}^{\mathcal{G}_n} = 0$ and $\mathrm{H}^1(\mathcal{G}_n, K_{m(p-1)+t}) \cong \mathbb{F}_p$. We also have the short exact sequence

$$0 \to J_{m,t} \to K_{m(p-1)+t+1} \to \tau_{2t+1,1} \to 0$$

which induces

$$0 \to \mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, \tau_{2t+1,1})$$

as $J_{m,t}^{\mathcal{G}_n} \cong K_{m(p-1)+t+1}^{\mathcal{G}_n} \cong \mathrm{H}^1(\mathcal{G}_n, K_{m(p-1)+t+1}) \cong \mathbb{F}_p$ and $\tau_{2t+1,1}^{\mathcal{G}_n} = 0$. Therefore, we have $\mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \cong \mathbb{F}_p$.

For $t = \frac{p-1}{2}$, as $\sigma_{\frac{p-1}{2}} = \tau \oplus (\mathrm{St} \otimes \tau)$ and $\sigma_{\frac{p-1}{2}}^{\mathcal{G}_n} = \mathrm{H}^1\left(\mathcal{G}_n, \sigma_{\frac{p-1}{2}}\right) = 0$ when $p \neq 3$, then $\mathrm{H}^1(\mathcal{G}_n, \tau) = \mathrm{H}^1(\mathcal{G}_n, \mathrm{St} \otimes \tau) = 0$. Therefore, as we have the exact sequences

$$0 \to K_{m(p-1)+\frac{p-1}{2}} \to \Gamma_m \to \tau \to 0, \qquad 0 \to K_{m(p-1)+\frac{p-1}{2}} \to \Delta_m \to \mathrm{St} \otimes \tau \to 0,$$

then we have $\mathrm{H}^1(\mathcal{G}_n, \Gamma_m) \cong \mathrm{H}^1(\mathcal{G}_n, \Delta_m) \cong \mathrm{H}^1\left(\mathcal{G}_n, K_{m(p-1)+\frac{p-1}{2}}\right) \cong \mathbb{F}_p$ for all $0 \leq m \leq d_n - 1$.

If $p = 3$, then $\sigma_1^{\mathcal{G}_n} = 0$ and $\mathrm{H}^1(\mathcal{G}_n, \sigma_1) \cong \mathbb{F}_3^2$. Also, as $\sigma_1 = \tau \oplus (\mathrm{St} \otimes \tau)$, then

$$\mathrm{H}^1(\mathcal{G}_n, \sigma_1) \cong \mathrm{H}^1(\mathcal{G}_n, \tau) \oplus \mathrm{H}^1(\mathcal{G}_n, \mathrm{St} \otimes \tau).$$

Therefore, we will find $\mathrm{H}^1(\mathcal{G}_n, \tau)$. We have the exact sequence

$$0 \to \mathrm{H}^1(\mathcal{G}_0, \tau) \to \mathrm{H}^1(\mathcal{G}_n, \tau) \to \mathrm{Hom}(\ker(\mu_n), \tau)^{\mathcal{G}_0}$$

as $\ker(\mu_n)$ acts trivially on τ. As for all elements $\left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{B}_0$, we have

$$\tau\left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) = r,$$

then the action of $\mathcal{B}_0$ on $\mathrm{Hom}(\ker(\mu_n), \tau)$ is identical to the action of $\mathcal{B}_0$ on $\mathrm{Hom}(\ker(\mu_n), V_1)$ as seen in the proof of Theorem 3.3.11. Therefore, we have

$$\mathrm{Hom}(\ker(\mu_n), \tau)^{\mathcal{B}_0} \cong \langle f \rangle \cong \mathbb{F}_3$$

where

$$f\begin{pmatrix} a \\ b \\ c \end{pmatrix} = c.$$

However, we see that

$$[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot f]\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = -f\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = -1.$$

Therefore,

$$\mathrm{Hom}(\ker(\mu_n), \tau)^{\mathcal{G}_0} = 0,$$

and so $\mathrm{H}^1(\mathcal{G}_n, \tau) \cong \mathrm{H}^1(\mathcal{G}_0, \tau)$. We can verify that $\mathrm{H}^1(\mathcal{G}_0, \tau) \cong \mathbb{F}_3$ by using magma [7]. Therefore, we must also have $\mathrm{H}^1(\mathcal{G}_n, \mathrm{St} \otimes \tau) \cong \mathbb{F}_3$. As we have short exact sequences

$$0 \to K_{2m+1} \to \Gamma_m \to \tau \to 0, \qquad \text{and} \qquad 0 \to \Gamma_m \to K_{2(m+1)} \to \mathrm{St} \otimes \tau \to 0$$

which induce sequences

$$0 \to \mathbb{F}_3 \to \mathrm{H}^1(\mathcal{G}_n, \Gamma_m) \to \mathbb{F}_3 \qquad \text{and} \qquad 0 \to \mathrm{H}^1(\mathcal{G}_n, \Gamma_m) \to \mathbb{F}_3^2 \to \mathbb{F}_3.$$

Therefore, we must have $\mathrm{H}^1(\mathcal{G}_n, \Gamma_m) \in \{\mathbb{F}_3, \mathbb{F}_3^2\}$. However, we cannot determine which it is. The case is identical for $\mathrm{H}^1(\mathcal{G}_n, \Delta_m)$.

We know that for all $\frac{p+1}{2} \leq t \leq p-2$, we have $\sigma_t \cong \sigma_{p-1-t}$. Therefore, we have for $\frac{p+1}{2} \leq t \leq p-2$, $\sigma_t^{\mathrm{ss}} = \tau_{2p-2t-1,1} \oplus \tau_{2t+2-p,2}$ and the short exact sequence

$$0 \to \tau_{2t+2-p,2} \to \sigma_t \to \tau_{2p-2t-1,1} \to 0.$$

From above, we already know that $\tau_{2t+2-p,2}^{\mathcal{G}_n} = \tau_{2p-2t-1,1}^{\mathcal{G}_n} = 0$ and for $t \neq p-2$, $\mathrm{H}^1(\mathcal{G}_n, \tau_{2t+2-p,2}) = 0$. Therefore, we obtain the results similar to earlier, which are the exact sequences

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \to \mathrm{H}^1(\mathcal{G}_n, \tau_{2t+2-p,2})$$

and

$$0 \to \mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, \tau_{2p-2t-1,1})$$

showing that $\mathrm{H}^1(\mathcal{G}_n, J_{m,t}) \cong \mathbb{F}_p$. Finally, for all $1 \leq m \leq d_n$, we have the short exact sequences

$$0 \to K_{m(p-1)} \to \Lambda_m \to \mathrm{St} \to 0$$

and

$$0 \to \Theta_m \to K_{m(p-1)+1} \to \mathrm{St} \to 0.$$

Therefore, as $\mathrm{St}^{\mathcal{G}_n} = \mathrm{H}^1(\mathcal{G}_n, \mathrm{St}) = 0$, then

$$\mathrm{H}^1(\mathcal{G}_n, \Theta_m) \cong \mathrm{H}^1(\mathcal{G}_n, K_{m(p-1)+1}) \cong \mathbb{F}_p$$

and $\mathrm{H}^1(\mathcal{G}_n, \Lambda_m) \cong \mathrm{H}^1(\mathcal{G}_n, K_{m(p-1)}) \cong \mathbb{F}_p^2$ similarly. Therefore, assuming Conjecture 3.3.16 we have the following.

Conjecture 3.3.19. *Let $p > 3$ and W be an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of $\mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p)$. Then we have*

$$\mathrm{H}^1(\mathcal{G}_n, W) \cong \begin{cases} 0 & \text{if } W \in \{\Theta_0, \Lambda_0, K_1\}, \\ \mathbb{F}_p^2 & \text{if } W \in \{K_{m(p-1)}, \Lambda_m : 1 \leq m \leq d_n\} \\ \mathbb{F}_p & \text{otherwise.} \end{cases}$$

We now look at the cohomology with respect to $\mathcal{A}_n$. We look at some results for general n.

Lemma 3.3.20. *Let $n \geq 0$. Then we have $\mathbb{F}_p^{\mathcal{A}_n} = \mathbb{F}_p$ and*

$$\mathrm{H}^1(\mathcal{A}_n, \mathbb{F}_p) \cong \mathrm{H}^2(\mathcal{A}_n, \mathbb{F}_p) \cong \begin{cases} \mathbb{F}_p & \text{if } n \geq 1, \\ 0 & \text{if } n = 0. \end{cases}$$

Proof. We know $\mathcal{A}_n$ acts trivially on $\mathbb{F}_p$ so the first part is true. Therefore, we have

$$\begin{aligned} \mathrm{H}^1(\mathcal{A}_n, \mathbb{F}_p) &\cong \mathrm{Hom}(\mathcal{A}_n, \mathbb{F}_p) \\ &= \mathrm{Hom}(\mathbb{Z}/p^n(p+1)\mathbb{Z}, \mathbb{F}_p), \end{aligned}$$

which gives our the second result. Finally, the Herbrand quotient gives our result as $\mathcal{A}_n$ is cyclic. □

We want to find $\mathrm{H}^1(\mathcal{A}_n, K_{p^n})$. We know that we have an $\mathbb{F}_p[\mathcal{G}_n]$-isomorphism

$$K_{p^n} = \mathrm{Ind}_{\mathcal{B}_n}^{\mathcal{G}_n}(\mathbb{F}_p) \cong \mathrm{Maps}(\mathbb{P}_n^1 \to \mathbb{F}_p).$$

Therefore, we can prove the following.

Proposition 3.3.21. *For all $n \geq 0$, we have $K_{p^n}^{\mathcal{A}_n} \cong \mathbb{F}_p$ and*

$$\mathrm{H}^1(\mathcal{A}_n, K_{p^n}) = \mathrm{H}^2(\mathcal{A}_n, K_{p^n}) = 0.$$

Proof. As $\mathcal{A}_n$ acts transitively on $\mathbb{P}_n^1$, this gives the result for the first part. Also, this implies that there only exists one orbit and so by Proposition 3.2.3 and as $\mathcal{A}_n$ is cyclic, we have

$$\mathrm{H}^1(\mathcal{A}_n, K_{p^n}) \cong \mathbb{F}_p\Big[\Big|\mathrm{Stab}_{\mathcal{A}_n}\Big(\mathbb{P}_n^1\Big)\Big|\Big].$$

However, by the orbit-stabiliser theorem, $\mathrm{Stab}_{\mathcal{A}_n}(\mathbb{P}_n^1)$ is trivial which gives our result. The final part follows from the Herbrand quotient. □

Using this, we can show the following.

Lemma 3.3.22. *For all $n \geq 1$, we have*

$$\Lambda_{d_n}^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \Lambda_{d_n}) \cong \mathrm{H}^2(\mathcal{A}_n, \Lambda_{d_n}) \cong \mathbb{F}_p.$$

Proof. We know that we can view

$$\Lambda_{d_n} = \left\{ f : \mathbb{P}_n^1 \to \mathbb{F}_p : \sum_C f(C) = 0 \right\}.$$

We have

$$K_{p^n}^{\mathcal{A}_n} = \left\langle \sum_{C \in \mathbb{P}_n^1} e_C \right\rangle \cong \mathbb{F}_p$$

where e_C is the characteristic function for C. Hence, this generating element lies in $\Lambda_{d_n}^{\mathcal{A}_n}$ and this proves the first part. For the second, we have the short exact sequence

$$0 \to \Lambda_{d_n} \to K_{p^n} \to \mathbb{F}_p \to 0$$

which induces

$$0 \to \mathbb{F}_p \to \mathbb{F}_p \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, \Lambda_{d_n}) \to 0$$

as $\mathrm{H}^1(\mathcal{A}_n, K_{p^n}) = 0$. The final part follows from the Herbrand quotient. □

We now want to find the cohomology of the other $\mathbb{F}_p[\mathcal{G}_n]$-submodules of K_{p^n} with respect to $\mathcal{A}_n$. In order to find these, we need to find the cohomology of σ_t by $\mathcal{A}_n$ for all $0 \leq t \leq \frac{p-1}{2}$. We know that

$$\sigma_t = \{f : \mathcal{G}_n \to V_t : f(gh) = \beta_t(g)f(h) \text{ for all } g \in \mathcal{I}_n\}$$

with group action $(g \cdot f)(g') = f(g'g)$. We have also seen that elements of the quotient $\mathcal{I}_n \backslash \mathcal{G}_n$ can be represented by powers of the element $v_n := {\alpha_n}^{p^n}$ where α_n is a chosen generator for $\mathcal{A}_n$. We can now look at the cohomology on σ_t with respect to $\mathcal{A}_n$. Let $\pi_n := \sum_{i=0}^{n-1} (-p)^i$. We see for $0 \leq j \leq p$ that

$$v_n^j \alpha_n = {\alpha_n}^{jp^n+1} = {\alpha_n}^{(j+(-1)^n)p^n+\pi_n(p+1)} = {\alpha_n}^{\pi_n(p+1)} v_n^{j+(-1)^n}$$

and so if $f \in \sigma_t$, then

$$\begin{aligned}
(\alpha_n \cdot f)\left(v_n^j\right) &= f\left(v_n^j \alpha_n\right) \\
&= f\left({\alpha_n}^{\pi_n(p+1)} v_n^{j+(-1)^n}\right) \\
&= \beta_t\left({\alpha_n}^{\pi_n(p+1)}\right) f\left(v_n^{j+(-1)^n}\right) \\
&= f\left(v_n^{j+(-1)^n}\right)
\end{aligned}$$

as ${\alpha_n}^{p+1} \in \mathcal{U}_n$ and β_t is trivial on $\mathcal{U}_n$. Therefore, if $f \in \sigma_t^{\mathcal{A}_n}$, then f must constant on v_n^j for all $0 \leq j \leq p$. Hence, we have f generating $\sigma_t^{\mathcal{A}_n}$ where

$f\left(gv_n^j\right) = \beta_t(g)$ for all $g \in \mathcal{I}_n$. Now, as $\mathcal{A}_n$ is cyclic, we wish to calculate $\ker(\mathrm{Nm}_{\mathcal{A}_n} : \sigma_t \to \sigma_t)$. Let $\rho \in \sigma_t$. Then

$$\begin{aligned}
\mathrm{Nm}_{\mathcal{A}_n}(\rho)(gv_n^j) &= \sum_{m=0}^{p^n(p+1)-1} ({\alpha_n}^m \cdot \rho)\left(gv_n^j\right) \\
&= \sum_{m=0}^{p^n(p+1)-1} \rho\left(gv_n^j {\alpha_n}^m\right) \\
&= \sum_{m=0}^{p^n(p+1)-1} \rho\left(g{\alpha_n}^{jp^n+m}\right) \\
&= \sum_{m=0}^{p^n(p+1)-1} \rho\left(g{\alpha_n}^{m\pi_n(p+1)} v_n^{j+m(-1)^n}\right) \\
&= \beta_t(g) \sum_{m=0}^{p^n(p+1)p-1} \rho\left(v_n^{j+m(-1)^n}\right) \\
&= \beta_t(g) \sum_{k=0}^{p^n(p+1)-1} \rho\left(v_n^k\right) \\
&= p^n \beta_t(g) \sum_{k=0}^{p} \rho\left(v_n^k\right)
\end{aligned}$$

Therefore, we have $\ker(\mathrm{Nm}_{\mathcal{A}_n}) = \sigma_t$. In particular, we have

$$\mathrm{H}^1(\mathcal{A}_n, \sigma_t) \cong {}^{\sigma_t}\!/_{\mathrm{im}(\alpha_n - 1)}.$$

Now, as $\sigma_t^{\mathcal{A}_n} \cong \mathbb{F}_p$ for all $0 \leq t \leq \frac{p-1}{2}$, then $\mathrm{im}(\alpha_n - 1)$ is an $\mathbb{F}_p[\mathcal{A}_n]$-submodule of σ_t that has dimension p as an $\mathbb{F}_p$-vector space. Therefore, by the Herbrand quotient and that σ_t are all finite $\mathbb{F}_p[\mathcal{G}_n]$-modules, we have proved the following.

Lemma 3.3.23. *For all $n \geq 1$ and $0 \leq t \leq \frac{p-1}{2}$, we have*

$$\sigma_t^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \sigma_t) \cong \mathrm{H}^2(\mathcal{A}_n, \sigma_t) \cong \mathbb{F}_p.$$

We know that $\sigma_0 = \mathbb{F}_p \oplus \mathrm{St}$, $\sigma_{\frac{p-1}{2}} = \tau \oplus (\mathrm{St} \otimes \tau)$ and for all $1 \leq t \leq \frac{p-3}{2}$, $\sigma_t^{\mathrm{ss}} = \tau_{2t+1,1} \oplus \tau_{p-2t,2}$. For $t = 0$, we know that

$$\mathbb{F}_p^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \mathbb{F}_p) \cong \mathrm{H}^2(\mathcal{A}_n, \mathbb{F}_p) \cong \mathbb{F}_p.$$

We also see that

$$K_1 \cong \sigma_0 \cong \left\{ f : \mathbb{P}^1_n \to \mathbb{F}_p : f(C) = t_D \text{ if } C \supset D \in \mathbb{P}^1_0 \right\}$$

and

$$\Lambda_0 \cong \mathrm{St} \cong \left\{ f : \mathbb{P}^1_n \to \mathbb{F}_p : f(C) = t_D \text{ if } C \supset D \in \mathbb{P}^1_0, \sum_{D \in \mathbb{P}^1_0} t_D = 0 \right\}.$$

Now as

$$K_1^{\mathcal{A}_n} = \left\langle \sum_{C \in \mathbb{P}^1_n} e_C \right\rangle \cong \mathbb{F}_p,$$

we will show that this element does not lie in Λ_0. For this element, we see that $t_D = 1$ for all $D \in \mathbb{P}^1_0$. However, as $|\mathbb{P}^1_0| = p + 1$, we have

$$\sum_{D \in \mathbb{P}^1_0} t_D = p + 1 = 1 \neq 0.$$

Hence, $\Lambda_0^{\mathcal{A}_n} = 0$. In particular, as $\mathcal{A}_n$ is a cyclic group, then $\mathrm{H}^2(\mathcal{A}_n, \Lambda_0)$ is a quotient of $\Lambda_0^{\mathcal{A}_n}$ meaning $\mathrm{H}^2(\mathcal{A}_n, \Lambda_0) = 0$. We also see that the Herbrand quotient is trivial as Λ_0 is a finite $\mathbb{F}_p[\mathcal{G}_n]$-module and so $\mathrm{H}^1(\mathcal{A}_n, \Lambda_0) = 0$.

For $1 \leq t \leq \frac{p-3}{2}$, we have the short exact sequence

$$0 \to \tau_{p-2t,2} \to \sigma_t \to \tau_{2t+1,1} \to 0$$

which induces

$$0 \to \tau_{p-2t,2}^{\mathcal{A}_n} \to \mathbb{F}_p \to \tau_{2t+1,1}^{\mathcal{A}_n} \to \mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) \to$$

$$\to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \to \mathrm{H}^2(\mathcal{A}_n, \tau_{p-2t,2}) \to \mathbb{F}_p.$$

We will show that there are three potential outcomes. From the exact sequence, we must have $\tau_{p-2t,2}^{\mathcal{A}_n} \in \{0, \mathbb{F}_p\}$. If $\tau_{p-2t,2}^{\mathcal{A}_n} = 0$, then as $\mathcal{A}_n$ is cyclic,

$$\mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) = \mathrm{H}^2(\mathcal{A}_n, \tau_{p-2t,2}) = 0.$$

This implies that

$$\tau_{2t+1,1}^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathrm{H}^2(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathbb{F}_p.$$

If $\tau_{p-2t,2}^{\mathcal{A}_n} \cong \mathbb{F}_p$, then $\mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) \cong \mathrm{H}^2(\mathcal{A}_n, \tau_{p-2t,2}) \in \{0, \mathbb{F}_p\}$. If they are 0, then this implies $\tau_{2t+1,1}^{\mathcal{A}_n} = 0$ and $\mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathbb{F}_p$, which contradicts the Herbrand quotient. Therefore, if $\tau_{p-2t,2}^{\mathcal{A}_n} \cong \mathbb{F}_p$, then

$$\mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) \cong \mathrm{H}^2(\mathcal{A}_n, \tau_{p-2t,2}) \cong \mathbb{F}_p.$$

If this is the case, then we either have

$$\tau_{2t+1,1}^{\mathcal{A}_n} = \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) = \mathrm{H}^2(\mathcal{A}_n, \tau_{2t+1,2}) = 0$$

or

$$\tau_{2t+1,1}^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathrm{H}^2(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathbb{F}_p.$$

Therefore we have three potential outcomes, for which the first and second cohomology groups are isomorphic to the fixed modules.

1. $\tau_{p-2t,2}^{\mathcal{A}_n} = 0$ and $\tau_{2t+1,1}^{\mathcal{A}_n} \cong \mathbb{F}_p$,
2. $\tau_{p-2t,2}^{\mathcal{A}_n} \cong \mathbb{F}_p$ and $\tau_{2t+1,1}^{\mathcal{A}_n} = 0$,
3. $\tau_{p-2t,2}^{\mathcal{A}_n} \cong \mathbb{F}_p$ and $\tau_{2t+1,1}^{\mathcal{A}_n} \cong \mathbb{F}_p$.

For $t = \frac{p-1}{2}$, then we have

$$\tau(g) = \det(g)^{\frac{p-1}{2}} = \left(\frac{\det(g)}{p}\right).$$

This mapping is not trivial on $\mathcal{A}_n$, so $\tau^{\mathcal{A}_n} = 0$. As $\sigma_{\frac{p-1}{2}} = \tau \oplus (\mathrm{St} \otimes \tau)$ and $\sigma_{\frac{p-1}{2}}^{\mathcal{A}_n} \cong \mathbb{F}_p$, then we must have $(\mathrm{St} \otimes \tau)^{\mathcal{A}_n} \cong \mathbb{F}_p$. Therefore, as

$$\mathrm{H}^1(\mathcal{A}_n, \sigma_{\frac{p-1}{2}}) \cong \mathrm{H}^2(\mathcal{A}_n, \sigma_{\frac{p-1}{2}}) \cong \mathbb{F}_p$$

and $\mathcal{A}_n$ is cyclic, then by the Herbrand quotient, we have

$$\mathrm{H}^1(\mathcal{A}_n, \tau) = \mathrm{H}^2(\mathcal{A}_n, \tau) = 0$$

and

$$\mathrm{H}^1(\mathcal{A}_n, \mathrm{St} \otimes \tau) \cong \mathrm{H}^2(\mathcal{A}_n, \mathrm{St} \otimes \tau) \cong \mathbb{F}_p.$$

For $\frac{p+1}{2} \leq t \leq p-2$, we end up with the exact same outcome as the $1 \leq t \leq \frac{p-3}{2}$ case. We can now calculate the cohomology with respect to $\mathbb{F}_p[\mathcal{G}_n]$-submodules of K_{p^n}. We first look at the fixed modules.

Lemma 3.3.24. *Let $n \geq 1$ and W be an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n}. Then we have*

$$W^{\mathcal{A}_n} \cong \begin{cases} 0 & \text{if } W = \Lambda_0, \\ \mathbb{F}_p & \text{otherwise.} \end{cases}$$

Proof. We have seen that the only $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n} that doesn't contain $\Theta_0 = \mathbb{F}_p$ is Λ_0 and if W contains $\mathbb{F}_p$, then $W^{\mathcal{A}_n} \cong \mathbb{F}_p$ as $K_{p^n}^{\mathcal{A}_n} \cong \mathbb{F}_p$. We have already shown that $\Lambda_0^{\mathcal{A}_n} = 0$ which gives our result. □

We now start with the smallest modules. We have the short exact sequence

$$0 \to \mathbb{F}_p \to K_1 \to \mathrm{St} \to 0$$

which implies that $\mathrm{H}^1(\mathcal{A}_n, K_1) \cong \mathrm{H}^1(\mathcal{A}_n, \mathbb{F}_p) \cong \mathbb{F}_p$ as $\mathrm{St}^{\mathcal{A}_n} = \mathrm{H}^1(\mathcal{A}_n, \mathrm{St}) = 0$.

For all $0 \leq m \leq d_n - 1$, we have the short exact sequence

$$0 \to K_{m(p-1)+t} \to K_{m(p-1)+t+1} \to \sigma_t \to 0$$

for $0 \leq t \leq p-2$. Then this induces

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, K_{m(p-1)+t}) \to \mathrm{H}^1(\mathcal{A}_n, K_{m(p-1)+t+1}) \to \mathbb{F}_p$$

as $K_{m(p-1)+t}^{\mathcal{A}_n} \cong K_{m(p-1)+t+1}^{\mathcal{A}_n} \cong \sigma_t^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \sigma_t) \cong \mathbb{F}_p$. This shows that $\mathbb{F}_p \leq \mathrm{H}^1(\mathcal{A}_n, K_{m(p-1)+t})$. Therefore, as $\mathcal{A}_n$ is cyclic, then by the Herbrand quotient and Lemma 3.3.24, we have $\mathrm{H}^1(\mathcal{A}_n, K_{m(p-1)+t}) \cong \mathbb{F}_p$. Also, we have shown that $\mathrm{H}^2(\mathcal{A}_n, K_{m(p-1)+t}) \cong \mathbb{F}_p$.

We also have the short exact sequence

$$0 \to K_{p^n-1} \to K_{p^n} \to \sigma_0 \to 0$$

which extends to

$$0 \to \mathbb{F}_p \to \mathbb{F}_p \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, K_{p^n-1}) \to 0$$

as $\mathrm{H}^1(\mathcal{A}_n, K_{p^n}) = 0$. Therefore, this shows $\mathrm{H}^1(\mathcal{A}_n, K_{p^n-1}) \cong \mathbb{F}_p$. We also see that $\mathrm{H}^2(\mathcal{A}_n, K_{p^n-1}) \cong \mathbb{F}_p$ by the Herbrand quotient and therefore, we have shown the following.

Proposition 3.3.25. *We have*

$$\mathrm{H}^1(\mathcal{A}_n, K_t) \cong \mathrm{H}^2(\mathcal{A}_n, K_t) \cong \begin{cases} \mathbb{F}_p & \text{if } 1 \leq t \leq p^n - 1, \\ 0 & \text{if } t = p^n. \end{cases}$$

We now look at the intermediate $\mathbb{F}_p[\mathcal{G}_n]$-submodules. We already know the results for Θ_0 and Λ_0. We look at the intermediates $J_{m,t}$ for $0 \leq m \leq d_n - 1$ and $1 \leq t \leq \frac{p-3}{2}$. We have the short exact sequence

$$0 \to K_{m(p-1)+t} \to J_{m,t} \to \tau_{p-2t,2} \to 0$$

which induces

$$0 \to \tau_{p-2t,2}^{\mathcal{A}_n} \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \to \mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) \to \mathbb{F}_p.$$

We also have the short exact sequence

$$0 \to J_{m,t} \to K_{m(p-1)+t+1} \to \tau_{2t+1,1} \to 0$$

which induces

$$0 \to \tau_{2t+1,1}^{\mathcal{A}_n} \to \mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \to \mathbb{F}_p.$$

If $\tau_{p-2t,2}^{\mathcal{A}_n} = 0$, then $\mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) = 0$ and the first sequence implies that $\mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \cong \mathbb{F}_p$. Similarly, if $\tau_{2t+1,1}^{\mathcal{A}_n} = 0$, then $\mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) = 0$ and the second sequence implies that $\mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \cong \mathbb{F}_p$. Also, if

$$\tau_{2t+1,1}^{\mathcal{A}_n} \cong \tau_{p-2t,2}^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, \tau_{2t+1,1}) \cong \mathrm{H}^1(\mathcal{A}_n, \tau_{p-2t,2}) \cong \mathbb{F}_p,$$

then the first sequence induces

$$0 \to \mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \to \mathbb{F}_p$$

and the second induces

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, J_t)$$

meaning $\mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \cong \mathbb{F}_p$. Therefore, we must have $\mathrm{H}^1(\mathcal{A}_n, J_{m,t}) \cong \mathbb{F}_p$. The case for $\frac{p+1}{2} \leq t \leq p-2$ can be proved similarly.

For $t = \frac{p-1}{2}$, we have the short exact sequences

$$0 \to K_{m(p-1)+\frac{p-1}{2}} \to \Gamma_m \to \tau \to 0$$

and

$$0 \to \Delta_m \to K_{m(p-1)+\frac{p+1}{2}} \to \tau \to 0.$$

Hence, we have $\mathrm{H}^1(\mathcal{A}_n, \Gamma_m) \cong \mathrm{H}^1(\mathcal{A}_n, \Delta_m) \cong \mathbb{F}_p$ for all $0 \leq m \leq d_n - 1$.

We also have for all $1 \leq m \leq d_n - 1$

$$0 \to K_{m(p-1)} \to \Lambda_m \to \mathrm{St} \to 0$$

and

$$0 \to \Theta_m \to K_{m(p-1)+1} \to \mathrm{St} \to 0.$$

As $\mathrm{St}^{\mathcal{A}_n} = \mathrm{H}^1(\mathcal{A}_n, \mathrm{St}) = 0$, then we have $\mathrm{H}^1(\mathcal{A}_n, \Theta_m) \cong \mathrm{H}^1(\mathcal{A}_n, \Lambda_m) \cong \mathbb{F}_p$ for all $1 \leq m \leq d_n - 1$.

Finally, we have the short exact sequence

$$0 \to \Theta_{d_n} \to K_{p^n} \to \mathrm{St} \to 0$$

and as $\mathrm{St}^{\mathcal{A}_n} = \mathrm{H}^1(\mathcal{A}_n, \mathrm{St}) = 0$, then $\mathrm{H}^1(\mathcal{A}_n, \Theta_{d_n}) \cong \mathrm{H}^1(\mathcal{A}_n, K_{p^n}) = 0$. We also have $\mathrm{H}^1(\mathcal{A}_n, \Lambda_{d_n}) \cong \mathbb{F}_p$ by Lemma 3.3.22. Therefore, we have shown the following.

Theorem 3.3.26. *Let $n \geq 1$ and W be an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n}. Then we have*

$$\mathrm{H}^1(\mathcal{A}_n, W) \cong \begin{cases} 0 & \text{if } W \in \{\Lambda_0, \Theta_{d_n}, K_{p^n}\}, \\ \mathbb{F}_p & \text{otherwise.} \end{cases}$$

We end this section with a result with respect to $\mathcal{B}_n$ which will become vital later on in this chapter and the next.

Lemma 3.3.27. *Let $n \geq 0$ and W be an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of K_{p^n}. Then $W^{\mathcal{B}_n} \neq 0$.*

Proof. We know that either $W \supseteq \Theta_0 = \mathbb{F}_p$ or $W = \Lambda_0$. For the first case, as $\mathcal{B}_n$ acts trivially on $\mathbb{F}_p$, then $\mathbb{F}_p^{\mathcal{B}_n} = \mathbb{F}_p$. Hence, $W^{\mathcal{B}_n} \supseteq \mathbb{F}_p$. Secondly, as we can view

$$\Lambda_0 = \left\{ f : \mathbb{P}_n^1 \to \mathbb{F}_p : f(C) = t_D \text{ for } C \supset D \in \mathbb{P}_0^1 \text{ and } \sum_D t_D = 0 \right\},$$

then for a fixed element of $\mathbb{P}_0^1$, denoted D_0, $\mathcal{B}_n$ acts transitively on the set of $C \not\supset D_0$ for $C \in \mathbb{P}_n^1$ and on the set of elements $C \supset D_0$ for $C \in \mathbb{P}_n^1$. As the number of all elements $\mathbb{P}_0^1 \backslash \{D_0\}$ is divisible by p, then $\Lambda_0^{\mathcal{B}_n}$ contains the function f such that

$$f(C) = \begin{cases} 1 & \text{if } C \not\supset D_0, \\ 0 & \text{otherwise,} \end{cases}$$

Hence, $\Lambda_0^{\mathcal{B}_n} \neq 0$. □

We now have all the required modular representation theory associated to $\mathcal{G}_n$ when looking at the integral representation theory associated to $\mathcal{G}_n$. We first look at the $n = 0$ case in the next section.

3.4 Representations of $\mathrm{PGL}_2(\mathbb{F}_p)$

We now look at the $\mathbb{Z}_p[\mathcal{G}_0]$-lattices in V_0. We have that $V_0 = W_0$ is an irreducible $\mathbb{Q}_p[\mathcal{G}_0]$-module and we have the standard lattice

$$T_0 = \left\{ f : \mathbb{P}_0^1 \to \mathbb{Z}_p : \sum_C f(C) = 0 \right\}$$

in V_0. We want to show the following.

Theorem 3.4.1. *All $\mathbb{Z}_p[\mathcal{G}_0]$-lattices in V_0 are of the form $p^k T_0$ for some $k \geq 0$.*

Proof. Let S be a $\mathbb{Z}_p[\mathcal{G}_0]$-lattice in V_0. Then we can scale S such that

$$p^k T_0 \subseteq S \subseteq T_0$$

for some $k \geq 1$. We will show that $S = p^l T_0$ for some $0 \leq l \leq k$. We do this by induction. If $k = 1$, we let $\overline{T}_0 := T_0 \otimes \mathbb{F}_p$. Then we have seen in the previous section that $\overline{T}_0 = \Lambda_0$ is an irreducible $\mathbb{F}_p[\mathcal{G}_0]$-module meaning $\overline{S} \to \overline{T}_0$ is surjective as if it were the zero map then $S = pT_0$. Therefore, by the surjective mapping before, we must have ${}^{T_0}/_{S} = 0$ meaning $S = T_0$.

Now assume this is true for k. We have a short exact sequence

$$0 \to \overline{T}_0 \to {}^{T_0}/_{p^{k+1}T_0} \to {}^{T_0}/_{p^k T_0} \to 0$$

so we can view $\overline{T}_0$ as a $\mathbb{Z}/p^{k+1}\mathbb{Z}[\mathcal{G}_0]$-submodule of ${}^{T_0}/_{p^{k+1}T_0}$. If

$${}^{S}/_{p^{k+1}T_0} \cap \overline{T}_0 \neq 0,$$

then as $\overline{T}_0$ is an irreducible $\mathbb{F}_p[\mathcal{G}_0]$-module, then $\overline{T}_0 \subseteq {}^{S}/_{p^{k+1}T_0}$ meaning $p^k T_0 \subseteq S$. Therefore, by induction, $S = p^t T_0$ for some $0 \leq t \leq k$. Hence we can assume ${}^{S}/_{p^{k+1}T_0} \cap \overline{T}_0 = 0$. Then by the second isomorphism theorem, we have

$$\frac{{}^{S}/_{p^{k+1}T_0} + \overline{T}_0}{\overline{T}_0} \cong \frac{{}^{S}/_{p^{k+1}T_0}}{{}^{S}/_{p^{k+1}T_0} \cap \overline{T}_0} \cong {}^{S}/_{p^{k+1}T_0}.$$

Hence

$${}^{S}/_{p^{k+1}T_0} \cong \frac{{}^{S}/_{p^{k+1}T_0} + \overline{T}_0}{\overline{T}_0} \leq \frac{{}^{T_0}/_{p^{k+1}T_0}}{\overline{T}_0} \cong {}^{T_0}/_{p^k T_0}.$$

Therefore, we have $S \subseteq pT_0$. However, by induction, this implies that $S = p^{l+1}T_0$ for some $0 \leq l \leq k$. □

The standard lattice in $V_{(0)}$ takes the form

$$T_{(0)} = \mathbb{Z}_p\left[{}^{\mathcal{G}_0}/_{\mathcal{B}_0}\right] = \mathrm{Maps}(\mathbb{P}^1_0 \to \mathbb{Z}_p).$$

Using this we can view all isomorphism classes of $\mathbb{Z}_p[\mathcal{G}_0]$-lattices in $V_{(0)}$.

Proposition 3.4.2. *Any $\mathbb{Z}_p[\mathcal{G}_0]$-lattice in $V_{(0)}$ is isomorphic to $\mathbb{Z}_p \oplus T_0$.*

Proof. Let $M \subset V_{(0)}$ be any lattice and assume $M \subset T_{(0)}$. We define

$$M_0 = M \cap T_0 \cong T_0$$

and $\pi_0(M) \cong \mathbb{Z}_p$ where $\pi_0 : T_{(0)} \to \mathbb{Z}_p$. So we have a short exact sequence

$$0 \to T_0 \to M \to \mathbb{Z}_p \to 0.$$

We want to show this sequence splits. We have the short exact sequence

$$0 \to T_0 \to T_{(0)} \xrightarrow{\pi_0} \mathbb{Z}_p \to 0.$$

This sequence induces

$$0 \to T_0^{\mathcal{G}_0} \to T_{(0)}^{\mathcal{G}_0} \xrightarrow{\pi_0} \mathbb{Z}_p \to \mathrm{H}^1(\mathcal{G}_0, T_0) \to \mathrm{H}^1(\mathcal{G}_0, T_{(0)}).$$

As $\mathcal{G}_0$ acts transitively on $\mathbb{P}_0^1$, we have $T_0^{\mathcal{G}_0} = 0$ and $T_{(0)}^{\mathcal{G}_0} \cong \mathbb{Z}_p$. Thus π_0 in this sequence represents the multiplication-by-$|\mathbb{P}_0^1|$ map and so π_0 is an isomorphism as $|\mathbb{P}_0^1| = p + 1$. However, we have $\mathrm{H}^1(\mathcal{G}_0, T_{(0)}) \cong \mathrm{H}^1(\mathcal{B}_0, \mathbb{Z}_p) = 0$ by Shapiro's Lemma and as the action of $\mathcal{B}_0$ on $\mathbb{Z}_p$ is trivial. Therefore, we have $\mathrm{H}^1(\mathcal{G}_0, T_0) = 0$. We have

$$\mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_0}(\mathbb{Z}_p, T_0) \cong \mathrm{H}^1(\mathcal{G}_0, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p, T_0)) \cong \mathrm{H}^1(\mathcal{G}_0, T_0) = 0$$

by Proposition 3.2.6. Hence $M \cong \mathbb{Z}_p \oplus T_0$. □

So in the $n = 0$ case, we see that any $\mathbb{Z}_p[\mathcal{G}_0]$-lattice in V_0 is isomorphic to T_0. This is not so though for $n \geq 1$.

3.5 Representations of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$

In this section, we will look at $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in T_n for $n \geq 1$ and the relationships between them. We have seen in Theorem 2.3.4 that

$$V_n = \bigoplus_{i=0}^{n} W_i$$

where each W_i contains the standard lattice R_i. We can extend this construction to the standard lattice in $\bigoplus_{i=k+1}^{n} W_i$ for $0 \leq k \leq n-1$ which is

$$R_n^k := \left\{ f : \mathbb{P}_n^1 \to \mathbb{Z}_p : \sum_{C \supset D} f(C) = 0 \text{ for all } D \in \mathbb{P}_k^1 \right\}.$$

There exist a short exact sequence

$$0 \to R_n^k \to T_n \xrightarrow{\pi} T_k \to 0$$

where the first mapping is the inclusion mapping and

$$\pi(f)(D) = \sum_{C \supset D} f(C).$$

We note that the sequence is still exact if we replace T_k and T_n with $T_{(k)}$ and $T_{(n)}$ respectively.

We now look at $\mathbb{Z}_p[\mathcal{G}_n]$-lattices contained in R_n^k. Naturally defined lattices in R_n^k include

$$O_n^{m,k} = \{ f \in R_n^k : f(C) \equiv s_D \pmod{p^m} \text{ for } C \supset D \in \mathbb{P}_k^1 \}$$

and

$$Z_n^{m,k} = \{ f \in R_n^k : f \text{ is constant mod } p^m \}$$

for $m \geq 0$. Here, the condition that $f \in O_n^{m,k}$ is to say that f is constant on discs. The first fits into the short exact sequence

$$0 \to R_n^k \to O_n^{m,k} \to \mathbb{Z}/p^m\mathbb{Z}\left[{}^{\mathcal{G}_k}/_{\mathcal{B}_k}\right] \to 0,$$

and the second fits into

$$0 \to R_n^k \to Z_n^{m,k} \to \mathbb{Z}/p^m\mathbb{Z} \to 0.$$

We can also define $F_n^{m,k}$ for $m \geq 0$ as

$$\left\{ f \in O_n^{m,k} : \sum_D s_D = 0 \text{ where } f(C) \equiv s_D \pmod{p^m} \text{ for } C \supset D \in \mathbb{P}_k^1 \right\}.$$

This fits into the short exact sequence

$$0 \to R_n^k \to F_n^{m,k} \to \ker\left(\mathbb{Z}/p^m\mathbb{Z}\left[{}^{\mathcal{G}_k}/_{\mathcal{B}_k}\right] \to \mathbb{Z}/p^m\mathbb{Z}\right) \to 0.$$

In particular, we have the short exact sequence

$$0 \to F_n^{m,k} \to O_n^{m,k} \to \mathbb{Z}/p^m\mathbb{Z} \to 0.$$

We can now create a bound on m.

Lemma 3.5.1. *For all $m \geq n-k$, we have $O_n^{m,k} = p^{m-n+k}O_n^{n-k,k}$ and similarly, $Z_n^{m,k} = p^{m-n+k}Z_n^{n-k,k}$ and $F_n^{m,k} = p^{m-n+k}F_n^{n-k,k}$*

Proof. Any element of $p^{m-n+k}O_n^{n-k,k}$ must be constant modulo p^m on discs and its sum must be 0 on discs by definition of $O_n^{n-k,k}$. Hence we have one inclusion.

We also see that if $g \in O_n^{m,k}$ then $g(C) = p^m t_C + s_D$ where $C \supset D \in \mathbb{P}_k^1$. Then as $\sum_{C \supset D} g(C) = 0$ for all $D \in \mathbb{P}_k^1$, we have $p^m \sum_{C \supset D} t_C + p^{n-k}s_D = 0$ and so $s_D \equiv 0 \pmod{p^{m-n+k}}$. Therefore, $g \in p^{m-n+k}R_n^k$. But, we also see that as $g = p^{m-n+k}f$ for $f \in R_n^k$, then $f(C) = p^{n-k}t_C + u_D$ where $s_D = p^{m-n+k}u_D$. Hence, $f \in O_n^{n-k,k}$. The $Z_n^{m,k}$ and $F_n^{m,k}$ cases follow similarly. □

Therefore, we only need to consider $0 \leq k \leq n-1$ and $1 \leq m \leq n-k$. Let $j : T_{(k)} \to T_{(n)}$ be the mapping that sends f to $f \circ s$, with $s : \mathbb{P}_n^1 \to \mathbb{P}_k^1$ the reduction mapping. Then $T_{(n)}$ contains $j(T_{(k)}) \oplus R_n^k \cong T_{(k)} \oplus R_n^k$. We obtain an exact sequence

$$0 \to T_{(k)} \xrightarrow{j} T_{(n)} \xrightarrow{\phi} R_n^k$$

as $\ker(\phi)$ is precisely the functions that are constant on each disc. Here

$$\phi(f)(C) = p^{n-k} \cdot f(C) - \sum_{C' \supset D} f(C')$$

with $C \supset D \in \mathbb{P}_k^1$.

We now want to show that $\mathrm{im}(\phi) = O_n^{n-k,k}$. Let $f \in \mathrm{im}(\phi)$. Then

$$f(C) = p^{n-k} \cdot t_C - \sum_{C' \supset D} t_{C'} \equiv - \sum_{C' \supset D} t_{C'} \pmod{p^{n-k}}.$$

Therefore, $f \in O_n^{n-k,k}$.

Conversely let $g \in O_n^{n-k,k}$. Then we can write $g(C) = p^{n-k}t_C + s_D$ where $C \supset D \in \mathbb{P}_k^1$ and

$$0 = \sum_{C \supset D} g(C) = p^{n-k} \sum_{C \supset D} t_C + p^{n-k} s_D.$$

Therefore,

$$g(C) = p^{n-k}t_C - \sum_{C' \supset D} t_{C'} = \phi(h)(C)$$

where $h : \mathbb{P}_n^1 \to \mathbb{Z}_p$ such that $h(C) = t_C$. Hence, $g = \phi(h) \in \mathrm{im}(\phi)$. Therefore we have the short exact sequence

$$0 \to T_{(k)} \xrightarrow{j} T_{(n)} \xrightarrow{\phi} O_n^{n-k,k} \to 0. \tag{2}$$

In particular, if we restrict ϕ to T_n, then we have the following exact sequence

$$0 \to T_k \xrightarrow{j} T_n \xrightarrow{\phi} F_n^{n-k,k} \to 0.$$

Hence, the short exact sequence (2) hints as to the possible dual of R_n^k.

Proposition 3.5.2. *Let $(R_n^k)^* := \mathrm{Hom}_{\mathbb{Z}_p}(R_n^k, \mathbb{Z}_p)$ denote the $\mathbb{Z}_p$-dual of R_n^k. Then $(R_n^k)^* \cong O_n^{n-k,k}$.*

Proof. We have the exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. This induces

$$0 \to T_{(k)}^* \to T_{(n)}^* \to (R_n^k)^* \to \mathrm{Ext}^1_{\mathbb{Z}_p}(T_{(k)}, \mathbb{Z}_p).$$

As $T_{(k)}$ is a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice, then it is a projective $\mathbb{Z}_p$-module and therefore, we have $\mathrm{Ext}^1_{\mathbb{Z}_p}(T_{(k)}, \mathbb{Z}_p) = 0$. Also, as $T_{(i)} = \mathbb{Z}_p\left[{}^{\mathcal{G}_i}/_{B_i}\right]$ then $T_{(i)}^* = T_{(i)}$ by [22, Corollary 2.5.10]. We see that the mapping $T_{(k)} \to T_{(n)}$ is j as defined earlier.

From these two exact sequences, we define $x : R_n^k \overset{f}{\hookrightarrow} T_{(n)} \overset{g}{\twoheadrightarrow} (R_n^k)^*$ and we have the multiplication-by-p^{n-k} map $T_{(k)} \overset{j}{\hookrightarrow} T_{(n)} \overset{\pi}{\twoheadrightarrow} T_{(k)}$. We have that $\ker(x) = R_n^k \cap j(T_{(k)}) = 0$ and so

$$\begin{aligned}
\operatorname{coker}(x) &= {}^{\operatorname{im}(g)}\!/_{\operatorname{im}(x)} \\
&\cong \left({}^{T_{(n)}}\!/_{\ker(g)}\right)\!/_{\operatorname{im}(f)} \\
&= \left({}^{T_{(n)}}\!/_{\operatorname{im}(j)}\right)\!/_{\ker(\pi)} \\
&\cong \left({}^{T_{(n)}}\!/_{\ker(\pi)}\right)\!/_{\operatorname{im}(j)} \\
&\cong {}^{\operatorname{im}(\pi)}\!/_{\operatorname{im}(j)} \\
&= \operatorname{coker}\left([p^{n-k}] : T_{(k)} \to T_{(k)}\right) \\
&= \mathbb{Z}/p^{n-k}\mathbb{Z}\left[{}^{\mathcal{G}_k}\!/_{\mathcal{B}_k}\right]
\end{aligned}$$

However, we have $\operatorname{im}(x) \cong R_n^k$ meaning we have an exact sequence

$$0 \to R_n^k \to (R_n^k)^* \to \mathbb{Z}/p^{n-k}\mathbb{Z}\left[{}^{\mathcal{G}_k}\!/_{\mathcal{B}_k}\right] \to 0$$

which shows $O_n^{n-k,k} \cong (R_n^k)^*$ by the exact sequence that defines $O_n^{n-k,k}$. □

We now introduce some of the sublattices of T_n we are able to define. The first lattice we look at is

$$T_n^m = \{f \in T_n : f \text{ is constant mod } p^m\}$$

for $m \geq 1$. We do not need $m > n$ due to the following.

Lemma 3.5.3. *For $m > n$, we have $T_n^m = p^{m-n}T_n^n$.*

Proof. If we let $f \in T_n^m$, then we have $f(C) \equiv 0 \pmod{p^{m-n}}$ for all $C \in \mathbb{P}_n^1$ as $m > n$ and $\sum_C f(C) = 0$, so $f \in p^{m-n}T_n^n$. It is clear that if $f \in p^{m-n}T_n^n$ then $f \in T_n^m$. □

As this is the case, then for all $m \geq n$, we have $T_n^m \cong T_n^n$. If we let $0 \leq i < m \leq n$, then the third isomorphism theorem gives

$${}^{T_n^m}\!/_{p^{m-i}T_n^i} \cong \left({}^{T_n^m}\!/_{p^mT_n}\right)\Big/\left({}^{p^{m-i}T_n^i}\!/_{p^mT_n}\right) \cong \left({}^{T_n^m}\!/_{p^mT_n}\right)\Big/\left({}^{T_n^i}\!/_{p^iT_n}\right) \cong \mathbb{Z}/p^{m-i}\mathbb{Z}.$$

In particular, this leads to the short exact sequence

$$0 \to pT_n^{m-1} \to T_n^m \to \mathbb{F}_p \to 0$$

for $m \geq 1$. We now define $\overline{T_n^m} := T_n^m \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Then we have the following.

Proposition 3.5.4. *We have the following exact sequences of $\mathbb{Z}_p[\mathcal{G}_n]$-modules*

$$0 \to \mathbb{F}_p \to \overline{T_n^m} \to {}^{T_n^m}\!/_{T_n^{m+1}} \to 0$$

for $0 \leq m \leq n-1$ and the exact sequence

$$0 \to {}^{T_n^{n-1}}\!/_{T_n^n} \to \overline{T_n^n} \to \mathbb{F}_p \to 0.$$

The first exact sequence splits for $1 \leq m \leq n-1$ and the other sequences are non-split.

Proof. These sequences are exact due to the third isomorphism theorem. We want to show for $1 \leq m \leq n-1$ that the first set of sequences split. We define the mapping $e : \overline{T_n^m} \to \mathbb{F}_p$ by $e(f) = f(C) \pmod p$. This is well defined as $f(C)$ are congruent modulo p^m. It is also $\mathcal{G}_n$-equivariant and so we have shown the sequence splits.

For the first sequence with $m = 0$, we have seen that $\overline{T}_n = \Lambda_{d_n}$. Hence, by the work on the $\mathbb{F}_p[\mathcal{G}_n]$-submodules of $\overline{T}_{(n)}$ in section 3.3, we have seen that this sequence cannot split.

For the last sequence, let $f \in T_n^n$ be a lift of $1 \in \mathbb{F}_p$ under a section of $e : \overline{T_n^n} \to \mathbb{F}_p$. Then we have $f(C) \equiv 1 \pmod p$ and $(h-1) \cdot f \in pT_n^n$ for every $h \in \mathcal{G}_n$. Now, $\mathcal{G}_n$ acts transitively on $\mathbb{P}_n^1$ by Lemma 3.1.10, so for all $C, D \in \mathbb{P}_n^1$, $(f(C) - f(D))/p$ is constant modulo p^n and so $f(C)$ is constant modulo p^{n+1}.

But

$$0 = \sum_C f(C) \equiv (p^{n+1} + p^n) f(C) \pmod{p^{n+1}}.$$

Hence, $f(C) \equiv 0 \pmod p$, which is a contradiction. □

Using these lattices, we can find the dual of T_n.

Proposition 3.5.5. *Let* $T_n^* := \mathrm{Hom}_{\mathbb{Z}_p}(T_n, \mathbb{Z}_p)$ *denote the* $\mathbb{Z}_p$*-dual of* T_n*. Then* $T_n^* \cong T_n^n$.

Proof. We have the short exact sequence

$$0 \to T_n \to T_{(n)} \to \mathbb{Z}_p \to 0$$

which induces

$$0 \to \mathbb{Z}_p \xrightarrow{m} T_{(n)} \to T_n^* \to 0$$

via $\mathrm{Hom}_{\mathbb{Z}_p}(_, \mathbb{Z}_p)$, where $m(1)$ is the function that maps all of $\mathbb{P}_n^1$ to 1. If we let $x : T_n \hookrightarrow T_{(n)} \twoheadrightarrow T_n^*$ then x has cokernel equal to the cokernel of the multiplication-by-$|\mathbb{P}_n^1|$ map $\mathbb{Z}_p \hookrightarrow T_{(n)} \twoheadrightarrow \mathbb{Z}_p$ as $\ker(x) \subset T_n \cap m(\mathbb{Z}_p) = 0$. Hence we have the exact sequence

$$0 \to T_n \to T_n^* \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

which shows the result. □

We also have for $0 \leq k \leq n-1$ and $m \geq 0$

$$Y_n^{m,k} = \left\{ f \in T_n : \sum_{C \supset D} f(C) \text{ is constant mod } p^m \text{ for all } D \in \mathbb{P}_k^1 \right\}.$$

But, if $0 \leq k < m$, then all the terms are congruent to $a \pmod{p^m}$ and so $p^k(p+1)a \equiv 0 \pmod{p^m}$ and so $p^{m-k} | a$. Therefore we have

$$Y_n^{m,k} = \left\{ f \in T_n : \sum_{C \supset D} f(C) \equiv 0 \pmod{p^{m-k}} \text{ for all } D \in \mathbb{P}_k^1 \right\}.$$

Also, for $0 \leq k \leq n-1$ and $m \geq 0$, we have

$$X_n^{m,k} = \{ f \in T_n : f(C) \text{ is constant mod } p^m \text{ for all } C \supset D \in \mathbb{P}_k^1 \}.$$

These will be of importance later on.

We now compare the sublattices of R_n^k and T_n. We have the exact sequence

$$0 \to R_n^k \to T_n \xrightarrow{\pi} T_k \to 0$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. We have $Z_n^{m,k} = T_n^m \cap R_n^k$ and as $\pi(T_n^m) = p^m T_k$, we have the exact sequence

$$0 \to Z_n^{m,k} \to T_n^m \xrightarrow{\pi} p^m T_k \to 0.$$

However this sequence is non-split.

Proposition 3.5.6. *We have* $p^m T_k \oplus Z_n^{m,k} \subsetneq T_n^m$

Proof. Let $f \in p^m T_k \oplus Z_n^{m,k}$. Then f is constant mod p^m and $\sum_C f(C) = 0$, so $f \in T_n^m$. However, if we let $A, B \in \mathbb{P}_n^1$ lie in different discs and define $f : \mathbb{P}_n^1 \to \mathbb{Z}_p$ such that

$$f(C) = \begin{cases} p^m & \text{if } C = A, \\ -p^m & \text{if } C = B, \\ 0 & \text{otherwise,} \end{cases}$$

then $f \in T_n^m$. But if $f = p^m a + b$ for $a \in T_k$, $b \in Z_n^{m,k}$, then we would have

$$\begin{aligned} p^m &= p^m a(A) + b(A), \\ -p^m &= p^m a(B) + b(B), \\ 0 &= p^m a(C) + b(C), \end{aligned}$$

for $C \in \mathbb{P}_n^1 \backslash \{A, B\}$. In particular, if we have $U \in \mathbb{P}_n^1$ different from A lying in the same disc as $A \supset D \in \mathbb{P}_k^1$, then $b(A) = p^m + b(U)$ and so we have

$$0 = \sum_{C \supset D} b(C) = p^{n-k} b(U) + p^m.$$

We have two cases. If $m < n - k$, then $p^m \equiv 0 \pmod{p^{n-k}}$, which cannot happen.

If $m \geq n - k$ then $b(U) = -p^{m-n+k}$ and so $p^m a(U) = p^{m-n+k}$ meaning $p^{n-k} a(U) = 1$, which cannot happen. Therefore, $f \notin p^m T_k \oplus Z_n^{m,k}$. □

We can also use the comparison when looking at $Y_n^{m,k}$ for $m \geq n$.

Proposition 3.5.7. *For all* $0 \leq k < n \leq m$, *we have* $Y_n^{m,k} = p^{m-n} T_k \oplus R_n^k$.

Proof. Let $f \in Y_n^{m,k}$. Then $\sum_C f(C) = 0$ and $\sum_{C \supset D} f(C) = p^{m-k} t_D$ for all $D \in \mathbb{P}_k^1$. Define $a : \mathbb{P}_n^1 \to \mathbb{Z}_p$ such that $a(C) = t_D$ if $C \supset D$ and define $b : \mathbb{P}_n^1 \to \mathbb{Z}_p$ such that $b = f - p^{m-n} a$. We now need to show $a \in T_k$ and $b \in R_n^k$. We have

$$\begin{aligned}\sum_{C \supset D} b(C) &= \sum_{C \supset D} (f(C) - p^{m-n} a(C)) \\ &= \left(\sum_{C \supset D} f(C) \right) - p^{m-k} t_D \\ &= p^{m-k} t_D - p^{m-k} t_D \\ &= 0.\end{aligned}$$

Hence $b \in R_n^k$. We have $\sum_C a(C) = 0$ as $\sum_C f(C) = \sum_C b(C) = 0$. Also, a is constant on discs by definition, so $a \in T_k$. Therefore, $f = p^{m-n} a + b \in p^{m-n} T_k \oplus R_n^k$.

Let $g = p^{m-n} e + h \in p^{m-n} T_k \oplus R_n^k$. Then $\sum_C g(C) = 0$ and

$$\sum_{C \supset D} g(C) = p^{m-n} \sum_{C \supset D} e(C) = p^{m-k} e(C) \equiv 0 \pmod{p^{m-k}}$$

and so $g \in Y_n^{m,k}$. □

Now, we have $p^t T_k \cong T_k$ for all $t \geq 0$ and so we have $Y_n^{m,k} \cong Y_n^{n,k} = T_k \oplus R_n^k$ for all $m \geq n$.

In general, if $M \subset T_n$ is a lattice then $M_n = M \cap R_n^0$ is a lattice in R_n^0. The image of M in R_0 is a lattice isomorphic to R_0. So we have a short exact sequence

$$0 \to M_n \to M \xrightarrow{\pi} R_0 \to 0.$$

Therefore, we are interested in $\mathrm{Ext}^1_{\mathbb{Z}_p \mathcal{G}_n}(R_0, M_n)$ for all lattices $M_n \subset R_n^0$.

Proposition 3.5.8. *We have* $\mathrm{Ext}^1_{\mathbb{Z}_p \mathcal{G}_n}(R_0, R_n^0) \cong \mathbb{Z}/p^n\mathbb{Z}$.

In order to prove this, we will require the following.

Lemma 3.5.9. *We have* $\mathrm{Ext}^1_{\mathbb{Z}_p \mathcal{G}_n}(T_{(0)}, T_{(n)}) = 0$.

Proof. Using Shapiro's Lemma and Proposition 3.2.6 we have

$$\mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(T_{(0)}, T_{(n)}) \cong \mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{I}_n}(\mathbb{Z}_p, T_{(n)}) \cong \mathrm{H}^1(\mathcal{I}_n, T_{(n)}) = 0$$

by Theorem 3.2.7. □

Proof of Proposition 3.5.8. We have the exact sequence

$$0 \to R_n^0 \to T_{(n)} \xrightarrow{\pi} T_{(0)} \to 0$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. This induces

$$0 \to \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, R_n^0) \to \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)}) \xrightarrow{\rho} \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(0)}) \to$$

$$\to \mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_0, R_n^0) \to \mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)})$$

by applying $\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, _)$. We have $\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, R_n^0) = 0$ as they intersect trivially and

$$\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)}) \subset \mathrm{Hom}_{\mathbb{Q}_p\mathcal{G}_n}\left(W_0, \bigoplus_{i=-1}^{n} W_i\right) \cong \mathbb{Q}_p$$

by Schur's Lemma and so must be a rank 1 $\mathbb{Z}_p$-module. Similarly

$$\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(0)}) \subset \mathrm{Hom}_{\mathbb{Q}_p\mathcal{G}_n}(W_0, \mathbb{Q}_p \oplus W_0) \cong \mathbb{Q}_p.$$

We have

$$\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)}) = < j >$$

where $j(f) = f \circ s$ and $s : \mathbb{P}^1_n \to \mathbb{P}^1_0$ is the reduction mapping. Also,

$$\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(0)}) = < k >$$

where k is the inclusion mapping. We have $\rho(j) = \pi \circ j$ which is the multiplication-by-p^n map. As k is the inclusion mapping, then $\rho(j) = p^n \cdot k$. Therefore we have $\mathrm{coker}(\rho) \cong \mathbb{Z}/p^n\mathbb{Z}$. If we show $\mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)}) = 0$ then we are done.

We have the short exact sequence $0\to\mathbb{Z}_p \xrightarrow{w_0} R_{(0)}\to R_0\to 0$ where $w_0(b)(C) = b$ for all $C \in \mathbb{P}^1_0$. This induces

$$0\to \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)})\to \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(R_{(0)}, T_{(n)}) \xrightarrow{\chi} \mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(\mathbb{Z}_p, T_{(n)})\to$$

$$\to \mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_0, T_{(n)})\to \mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_{(0)}, T_{(n)})$$

via applying $\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(_, T_{(n)})$. However, we have seen in Lemma 3.5.9 that $\mathrm{Ext}^1_{\mathbb{Z}_p\mathcal{G}_n}(R_{(0)}, T_{(n)}) = 0$, so we will show χ is surjective.

We have

$$\mathrm{Hom}_{\mathbb{Z}_p\mathcal{G}_n}(\mathbb{Z}_p, T_{(n)}) \subset \mathrm{Hom}_{\mathbb{Q}_p\mathcal{G}_n}(\mathbb{Q}_p, V_{(n)}) \cong \mathbb{Q}_p$$

so it must be generated by the map w_n where $w_n(a)(C) = a$ for all $C \in \mathbb{P}^1_n$. Then $w_n(a) = a \cdot w_n(1)$ for all $a \in \mathbb{Z}_p$. Define $\alpha = w_n \circ \gamma$ where $\gamma : R_{(0)}\to\mathbb{Z}_p$ such that $\gamma(f) = \sum\limits_C f(C)$. Then we have

$$\chi(\alpha)(1) = (w_n \circ \gamma \circ w_0)(1) = w_n(p+1) = (p+1)\cdot w_n(1).$$

Therefore $\chi(\alpha) = (p+1)\cdot w_n$ and so χ is surjective, giving our result. □

We now look to apply the work on the modular representation theory of $\mathcal{G}_n$ in section 3.3 to the sublattices of R^k_n and T_n containing pR^k_n and pT_n respectively. Throughout, if X is a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice, we define the $\mathbb{F}_p[\mathcal{G}_n]$-module $\overline{X} := X \otimes \mathbb{F}_p$ and use the notation for such modules as in section Theorem 3.3.8.

We have $\overline{R^k_n} \cong K_{p^k d_{n-k}(p-1)}$ as an $\mathbb{F}_p[\mathcal{G}_n]$-module, where $d_i = \frac{p^i-1}{p-1}$ for $i \geq 1$. Also, as $\dim_{\mathbb{F}_p}(\overline{R}_0) = p-1$, then we must have $\overline{R}_0 \cong \Lambda_0 = \mathrm{St}$. Therefore, we have $\overline{R}_{(0)} \cong K_1$. Also, if we view $T_{(k)}$ and T_k as $\mathbb{Z}_p[\mathcal{G}_n]$-lattices for $0 \leq k < n$, then we have $\overline{T}_{(k)} = K_{p^k}$ and $\overline{T}_k = \Lambda_{d_k}$.

We initially look at the sublattices of R^k_n. We let $O^k_n := O^{1,k}_n$ and similarly define Z^k_n and F^k_n, then we have the exact sequences

$$0\to R^k_n \xrightarrow{[p]} Z^k_n\to\mathbb{F}_p\to 0, \quad 0\to R^k_n \xrightarrow{[p]} O^k_n\to K_{p^k}\to 0, \quad 0\to R^k_n \xrightarrow{[p]} F^k_n\to\Lambda_{d_k}\to 0.$$

Hence, we can define F_n^k as

$$\left\{ f \in O_n^k : \sum_{D \in \mathbb{P}_k^1} t_D \equiv 0 \pmod{p} \text{ where } f(C) \equiv t_D \pmod{p} \text{ when } C \supset D \right\}.$$

We would like to see if ${}^{R_n^0}\!/_{O_n^0}$ is an indecomposable $\mathbb{F}_p[\mathcal{G}_n]$-module. To do this, we want to show $({}^{R_n^0}\!/_{O_n^0})^{\mathcal{G}_n} = 0$.

Lemma 3.5.10. *We have* $({}^{R_n^0}\!/_{O_n^0})^{\mathcal{G}_n} = 0$.

Proof. We have the short exact sequence

$$0 \to K_1 \to K_{p^n-1} \to {}^{R_n^0}\!/_{O_n^0} \to 0$$

which induces

$$0 \to K_1^{\mathcal{G}_n} \to K_{p^n-1}^{\mathcal{G}_n} \to ({}^{R_n^0}\!/_{O_n^0})^{\mathcal{G}_n} \to \mathrm{H}^1(\mathcal{G}_n, K_1).$$

We then have our result as $K_1^{\mathcal{G}_n} \cong K_{p^n-1}^{\mathcal{G}_n} \cong \mathbb{F}_p$ by Lemma 3.3.17 and by Theorem 3.3.11, we have $\mathrm{H}^1(\mathcal{G}_n, K_1) = 0$. □

We want to check whether Z_n^k is a lattice isomorphic to R_n^k. However, we first need the following result.

Lemma 3.5.11. *We have* $\mathrm{H}^1(\mathcal{G}_n, R_n^k) = \mathbb{Z}/p^{n-k}\mathbb{Z}$.

Proof. We have a short exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0.$$

This induces

$$0 \to (R_n^k)^{\mathcal{G}_n} \to T_{(n)}^{\mathcal{G}_n} \xrightarrow{\pi} T_{(k)}^{\mathcal{G}_n} \to \mathrm{H}^1(\mathcal{G}_n, R_n^k) \to \mathrm{H}^1(\mathcal{G}_n, T_{(n)}).$$

Now we have $(R_n^k)^{\mathcal{G}_n} = 0$ and $\mathrm{H}^1(\mathcal{G}_n, T_{(n)}) = \mathrm{H}^1(\mathcal{B}_n, \mathbb{Z}_p) = 0$ by Shapiro's Lemma. We also see that as $T_{(n)}^{\mathcal{G}_n} \cong T_{(k)}^{\mathcal{G}_n} \cong \mathbb{Z}_p$, π must be the multiplication-by-p^{n-k} map as ${}^{|\mathbb{P}_n^1|}\!/_{|\mathbb{P}_k^1|} = p^{n-k}$. Therefore we have our result. □

We can compare this result to the following.

Lemma 3.5.12. *We have* $\mathrm{H}^1(\mathcal{G}_n, Z_n^k) = \mathbb{Z}/p^{n-k-1}\mathbb{Z}$.

Proof. We have the short exact sequence $0 \to R_n^k \to Z_n^k \to \mathbb{F}_p \to 0$ which induces

$$0 \to \mathbb{F}_p \to \mathbb{Z}/p^{n-k}\mathbb{Z} \to \mathrm{H}^1(\mathcal{G}_n, Z_n^k) \to 0$$

as $(Z_n^k)^{\mathcal{G}_n} = \mathrm{H}^1(\mathcal{G}_n, \mathbb{F}_p) = 0$ and by Lemma 3.5.11. Therefore, we have our result. □

Therefore, as the cohomology groups are not equal, $Z_n^k \ncong R_n^k$ as $\mathbb{Z}_p[\mathcal{G}_n]$-modules.

If we look at the sublattices of T_n, we define $X_n^k := X_n^{1,k}$ and similarly with Y_n^k. Then there exists a short exact sequence

$$0 \to T_n \to X_n^k \to K_{p^k} \to 0.$$

For Y_n^k, we have the following.

Lemma 3.5.13. *For $k = 0$, there exists a short exact sequence*

$$0 \to T_n \to Y_n^0 \to K_{p^n-1} \to 0$$

and for $k \geq 1$, there exists a short exact sequence

$$0 \to T_n \to Y_n^k \to \Theta_{p^k d_{n-k}} \to 0.$$

Proof. We have

$$\overline{Y_n^k} = \left\{ f : \mathbb{P}_n^1 \to \mathbb{F}_p : \sum_C f(C) = 0, \sum_{C \supset D} f(C) \text{ is constant for all } D \in \mathbb{P}_k^1 \right\}.$$

For the $k = 0$ case, as $|\mathbb{P}_0^1|$ is coprime to p, then if $\sum_{C \supset D} f(C)$ is constant, it must be constantly 0. Therefore, we have $\overline{Y_n^0} \cong \overline{R_n^0} \cong K_{p^n-1}$.

For $k \geq 1$, we have the short exact sequence

$$0 \to \overline{R_n^k} \to \overline{Y_n^k} \xrightarrow{\pi} \mathbb{F}_p \to 0$$

where $\pi(f) = \sum_{C \supset D} f(C)$. As $\overline{R_n^k} \cong K_{p^k d_{n-k}(p-1)}$, then $\overline{Y_n^k} \cong \Theta_{p^k d_{n-k}}$. □

We have already seen that there exists the short exact sequence

$$0 \to T_n \to T_n^1 \to \mathbb{F}_p \to 0.$$

We would now like to find the cohomology associated to these lattices.

3.6 The Cohomology of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices

We now want to look at the cohomology of the lattices we have found with respect to subgroups of $\mathcal{G}_n$. We will study the group cohomology with respect to $T_{(n)}$ which will help to calculate the group cohomology with respect $\mathbb{Z}_p[\mathcal{G}_n]$-sublattices of T_n.

We want to use section 3.2 to find the cohomologies on $\mathbb{Z}_p$ and $T_{(n)}$. We have the short exact sequence

$$0 \to T_n \to T_{(n)} \xrightarrow{\gamma} \mathbb{Z}_p \to 0$$

where $\gamma(f) = \sum_C f(C)$. By Theorem 3.2.7, if $H \leq \mathcal{G}_n$ then $\mathrm{H}^1(H, T_{(n)}) = 0$. Therefore, we have the exact sequence

$$0 \to T_n^H \to T_{(n)}^H \xrightarrow{\gamma} \mathbb{Z}_p \to \mathrm{H}^1(H, T_n) \to 0$$

as H acts trivially on $\mathbb{Z}_p$. Therefore, we have

$$\mathrm{H}^1(H, T_n) \cong \mathbb{Z}_p \big/ \gamma\big(T_{(n)}^H\big).$$

In particular, we obtain the following.

Lemma 3.6.1. *Let $H \leq \mathcal{G}_n$ such that $\mathbb{P}_n^1$ contains a fixed point of H. Then $\mathrm{H}^1(H, T_n) = 0$.*

Proof. Let $C \in \mathbb{P}_n^1$ be a point fixed by H. Then $1 = \gamma(e_C)$ where e_C is the characteristic function on C, with $e_C \in T_{(n)}^H$. Therefore, γ is surjective and so $\mathrm{H}^1(H, T_n) = 0$. □

We also have the following, which will enable us to find $\mathrm{H}^2(H, T_n)$ for all $H \leq \mathcal{G}_n$ cyclic.

Lemma 3.6.2. *Let $H \leq \mathcal{G}_n$. Then*

$$\hat{\mathrm{H}}^0(H, T_{(n)}) = \bigoplus_{\textit{Orbits } H\cdot x \textit{ of } H \textit{ on } \mathbb{P}^1_n} \mathbb{Z}_p/|\mathrm{Stab}_H(x)|\mathbb{Z}_p.$$

Proof. Follows directly from Proposition 3.2.4. □

We now want to look at the cohomology of $\mathbb{Z}_p$ with respect to subgroups of $\mathcal{G}_n$. If $H \leq \mathcal{G}_n$, then H acts trivially on $\mathbb{Z}_p$ and so

$$\mathrm{H}^1(H, \mathbb{Z}_p) = \mathrm{Hom}(H, \mathbb{Z}_p) = 0$$

as H is finite. We can also look at the 2nd cohomology group with respect to $\mathbb{Z}_p$.

Proposition 3.6.3. *Let $H \leq \mathcal{G}_n$. Then $\mathrm{H}^2(H, \mathbb{Z}_p) \cong H^{ab}[p^\infty]$.*

In order to prove this, we require the following.

Theorem 3.6.4. *[10, Integral Duality Theorem, pg 250] Let G be a finite group and $n \geq 1$. Then*

$$\mathrm{H}^{n+1}(G, \mathbb{Z}) \cong \mathrm{H}_n(G, \mathbb{Z}).$$

We thus need to understand $\mathrm{H}_1(G, \mathbb{Z})$. However, we can identify this group with the following.

Theorem 3.6.5. *[38, Theorem 6.1.11] For any group G, $\mathrm{H}_1(G, \mathbb{Z}) \cong G^{ab}$.*

We can therefore prove the proposition.

Proof of Proposition 3.6.3. We see that

$$\mathrm{H}^2(H, \mathbb{Z}_p) \cong \mathrm{H}^2(H, \mathbb{Z})[p^\infty] \cong \mathrm{H}_1(G, \mathbb{Z})[p^\infty] \cong H^{\mathrm{ab}}[p^\infty]$$

by the Integral Duality Theorem and Theorem 3.6.5. □

We also have the short exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0$$

where $\pi(f)(D) = \sum_{C \supset D} f(D)$. Similarly to the T_n case, as $\mathrm{H}^1(H, T_{(n)}) = 0$ for all $H \leq \mathcal{G}_n$, we have

$$\mathrm{H}^1(H, R_n^k) \cong T_{(k)}^H \big/ \pi\big(T_{(n)}^H\big)$$

which will be a useful result throughout this section. We now want to find the cohomology of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to subgroups of $\mathcal{G}_n$. We initially look at the whole group.

3.6.1 The $\mathcal{G}_n$-Cohomology

We will start with looking at the cohomology of the whole group. We have already seen that $\mathrm{H}^1(\mathcal{G}_n, T_{(n)}) = 0$. This can be used for the following.

Proposition 3.6.6. *For all $n \geq 0$,*

$$\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. We have

$$\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}_p \big/ \gamma\big(T_{(n)}^{\mathcal{G}_n}\big)$$

where $\gamma(f) = \sum_C f(C)$ as seen in the previous section. As $\mathcal{G}_n$ acts transitively on $\mathbb{P}_n^1$, then $T_{(n)}^{\mathcal{G}_n} \cong \mathbb{Z}_p$ and is generated by the function that maps all of $\mathbb{P}_n^1$ to 1. Therefore, we have $\mathrm{im}(\gamma) = |\mathbb{P}_n^1|\mathbb{Z}_p$ and so

$$\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}_p/|\mathbb{P}_n^1|\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \qquad \square$$

We would also like to calculate the second cohomology group with respect to T_n.

Proposition 3.6.7. *For all $n \geq 0$, we have $\mathrm{H}^2(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We have the short exact sequence

$$0 \to T_n \to T_{(n)} \to \mathbb{Z}_p \to 0.$$

We know $\mathrm{H}^1(\mathcal{G}_n, \mathbb{Z}_p) = 0$ as $\mathcal{G}_n$ acts trivially on $\mathbb{Z}_p$ and is finite. We also see that as $\mathcal{P}_n = [\mathcal{I}_n, \mathcal{I}_n] \leq [\mathcal{G}_n, \mathcal{G}_n]$ by Lemma 3.1.5, then as $\mathcal{P}_n$ is a Sylow-p subgroup of $\mathcal{G}_n$, ${\mathcal{G}_n}^{\mathrm{ab}}$ has order coprime to p and so $\mathrm{H}^2(\mathcal{G}_n, \mathbb{Z}_p) = 0$ by Proposition 3.6.3. Therefore, we have

$$\mathrm{H}^2(\mathcal{G}_n, T_n) \cong \mathrm{H}^2(\mathcal{G}_n, T_{(n)}) \cong \mathrm{H}^2(\mathcal{B}_n, \mathbb{Z}_p) \cong \mathcal{D}_n[p^\infty] \cong \mathbb{Z}/p^n\mathbb{Z}$$

by Proposition 3.6.3 and as ${\mathcal{B}_n}^{\mathrm{ab}} \cong \mathcal{D}_n$ by Lemma 3.1.4. □

We can thus calculate the cohomology with respect to T_n^m.

Proposition 3.6.8. *For all $1 \leq m \leq n$ we have*

$$\mathrm{H}^1(\mathcal{G}_n, T_n^m) \cong \mathbb{Z}/p^{n-m}\mathbb{Z}.$$

Proof. We have the short exact sequence $0 \to T_n \to T_n^m \to \mathbb{Z}/p^m\mathbb{Z} \to 0$ which induces

$$(T_n^m)^{\mathcal{G}_n} \to \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{H}^1(\mathcal{G}_n, T_n) \to \mathrm{H}^1(\mathcal{G}_n, T_n^m) \to \mathrm{Hom}(\mathcal{G}_n, \mathbb{Z}/p^m\mathbb{Z})$$

as $\mathcal{G}_n$ acts trivially on $\mathbb{Z}/p^m\mathbb{Z}$. Now, $(T_n^m)^{\mathcal{G}_n} = 0$ and $\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$ by Proposition 3.6.6. We also know that $\mathrm{Hom}(\mathcal{G}_n, \mathbb{Z}/p^m\mathbb{Z}) = 0$ by Proposition 3.1.6. Hence we have our result. □

We have also shown for $0 \leq k \leq n-1$ that $\mathrm{H}^1(\mathcal{G}_n, R_n^k) \cong \mathbb{Z}/p^{n-k}\mathbb{Z}$ in Lemma 3.5.11. We now focus on $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in V_n, denoted W, such that they may be scaled so that $pT_n \subseteq W \subseteq T_n$. Then we have a short exact sequence

$$0 \to T_n \xrightarrow{[p]} W \to M \to 0$$

for some $\mathbb{F}_p[\mathcal{G}_n]$-submodule M of Λ_{d_n}. We have shown that $\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$. Then we know that

$$M^{\mathcal{G}_n} \cong \begin{cases} 0 & \text{if } M = \Lambda_0, \\ \mathbb{F}_p & \text{otherwise,} \end{cases}$$

by Lemma 3.3.17 and it is conjectured that

$$\mathrm{H}^1(\mathcal{G}_n, M) \cong \begin{cases} 0 & \text{if } M \in \{\Theta_0, \Lambda_0, K_1\}, \\ \mathbb{F}_p^2 & \text{if } M \in \{K_{m(p-1)}, \Lambda_m : 1 \leq m \leq d_n\}, \\ \mathbb{F}_p & \text{otherwise,} \end{cases}$$

in Conjecture 3.3.19, where $d_i := \frac{p^i-1}{p-1}$ for $i \geq 1$. We point out that the trivial cases in the conjecture have been proven. For the case when $M = \Lambda_0$, we have $\mathrm{H}^1(\mathcal{G}_n, W) \cong \mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.

For the case when $M \in \{\Theta_0, K_1\}$, then we induce the sequence

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, T_n) \to \mathrm{H}^1(\mathcal{G}_n, W) \to 0$$

which implies that $\mathrm{H}^1(\mathcal{G}_n, W) \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$.

If $M = K_{p^n-1}$, then we have the short exact sequence

$$0 \to M \to \Lambda_{d_n} \to \Lambda_0 \to 0.$$

We thus have the short exact sequence

$$0 \to W \to T_n \to \Lambda_0 \to 0$$

which implies that $\mathrm{H}^1(\mathcal{G}_n, W) \cong \mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$. The case $M = \Lambda_{d_n}$ is obvious as this would mean $W = T_n$.

Finally, for the other cases we have the exact sequence

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{G}_n, T_n) \to \mathrm{H}^1(\mathcal{G}_n, W) \to \mathrm{H}^1(\mathcal{G}_n, M) \to \mathrm{H}^2(\mathcal{G}_n, T_n).$$

Therefore, we have

$$0 \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \mathrm{H}^1(\mathcal{G}_n, W) \to \mathrm{H}^1(\mathcal{G}_n, M) \to \mathbb{Z}/p^n\mathbb{Z}$$

as $\mathrm{H}^1(\mathcal{G}_n, T_n) \cong \mathrm{H}^2(\mathcal{G}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$. In particular, we have shown the following.

Theorem 3.6.9. *Let W be a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice such that it can be scaled so that $pT_n \subseteq W \subseteq T_n$. Then there exists an element of order p^{n-1} in $\mathrm{H}^1(\mathcal{G}_n, W)$.*

We now look at proper subgroups of $\mathcal{G}_n$.

3.6.2 The $\mathcal{A}_n$-Cohomology

We would like to look at the cohomology of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to $\mathcal{A}_n$. We already know that $\mathrm{H}^1(\mathcal{A}_n, T_{(n)}) = 0$ by Theorem 3.2.7. This will be useful for the following.

Lemma 3.6.10. *For all $n \geq 0$, we have $\mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We know that

$$\mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}_p \big/ \gamma\Big(T_{(n)}^{\mathcal{A}_n}\Big)$$

where $\gamma(f) = \sum_C f(C)$. As $\mathcal{A}_n$ acts transitively on $\mathbb{P}_n^1$, then $T_{(n)}^{\mathcal{A}_n} \cong \mathbb{Z}_p$ and $\mathrm{im}(\gamma) = |\mathbb{P}_n^1|\mathbb{Z}_p$, so

$$\mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}_p/|\mathbb{P}_n^1|\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \qquad \square$$

We also look at the cohomology with respect to R_n^k.

Lemma 3.6.11. *For all $0 \leq k \leq n-1$, we have $\mathrm{H}^1(\mathcal{A}_n, R_n^k) \cong \mathbb{Z}/p^{n-k}\mathbb{Z}$.*

Proof. We have seen that

$$\mathrm{H}^1(\mathcal{A}_n, R_n^k) \cong T_{(k)}^{\mathcal{A}_n} \big/ \pi\Big(T_{(n)}^{\mathcal{A}_n}\Big)$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. As $\mathcal{A}_n$ acts transitively on $\mathbb{P}_n^1$, then

$$T_{(n)}^{\mathcal{A}_n} \cong T_{(k)}^{\mathcal{A}_n} \cong \mathbb{Z}_p.$$

Then the image of π is the multiplication-by-p^{n-k} mapping and so

$$\mathrm{H}^1(\mathcal{A}_n, R_n^k) \cong \mathbb{Z}/p^{n-k}\mathbb{Z}. \qquad \square$$

We can use Lemma 3.6.10 to calculate the size of the $\mathcal{A}_n$-cohomologies for all $\mathbb{Z}_p[\mathcal{G}_n]$-lattices. In particular, we know the size of these groups for all $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in V_n.

Proposition 3.6.12. *[39, Proposition 29] Let W be any $\mathbb{Z}_p[\mathcal{G}_n]$-lattice in V_n. Then*

$$|\,\mathrm{H}^1(\mathcal{A}_n, W)| = p^n.$$

Proof. All such lattices are contained in a scaled version of T_n with finite index. Hence we have a short exact sequence

$$0 \to W \to T_n \to M \to 0$$

where M is a finite $\mathbb{Z}_p[\mathcal{G}_n]$-module. As the Herbrand quotient of $\mathcal{A}_n$ with respect to M, denoted $h(\mathcal{A}_n, M)$, is trivial, and $W^{\mathcal{A}_n} = T_n^{\mathcal{A}_n} = 0$ then

$$|\,\mathrm{H}^1(\mathcal{A}_n, W)| = h(\mathcal{A}_n, W) = h(\mathcal{A}_n, T_n) = |\,\mathrm{H}^1(\mathcal{A}_n, T_n)| = p^n. \qquad \square$$

We will specifically look at the cohomology for T_n^m.

Theorem 3.6.13. *For all $0 \leq m \leq n$ we have*

$$\mathrm{H}^1(\mathcal{A}_n, T_n^m) \cong \mathbb{Z}/p^{n-m}\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}.$$

Proof. We have $0 \to T_n \to T_n^m \to \mathbb{Z}/p^m\mathbb{Z} \to 0$ which induces

$$0 \to \mathbb{Z}/p^m\mathbb{Z} \to \hat{\mathrm{H}}^{-1}(\mathcal{A}_n, T_n) \to \hat{\mathrm{H}}^{-1}(\mathcal{A}_n, T_n^m) \to \mathbb{Z}/p^m\mathbb{Z} \to 0$$

as $\hat{\mathrm{H}}^0(\mathcal{A}_n, T_n) = 0$ due to $\mathcal{A}_n$ being cyclic. This leads to the exact sequence

$$0 \to \mathbb{Z}/p^{n-m}\mathbb{Z} \to \hat{\mathrm{H}}^{-1}(\mathcal{A}_n, T_n^m) \to \mathbb{Z}/p^m\mathbb{Z} \to 0$$

by Lemma 3.6.10. We now want to show that this sequence splits. Fix a $D \in \mathbb{P}_n^1$ and define

$$h\big(\alpha_n^i \cdot D\big) = \begin{cases} p^m h_0 & \text{if } i = 0, \\ -ip^m & \text{if } 1 \leq i \leq p^n(p+1) - 1, \end{cases}$$

where $h_0 = \frac{|\mathbb{P}^1_n|^2 - |\mathbb{P}^1_n|}{2}$. Then we have

$$(\alpha_n - 1)h(C) = \begin{cases} p^m(1 - |\mathbb{P}^1_n| - h_0) & \text{if } C = D, \\ p^m(1 + h_0) & \text{if } C = \alpha_n \cdot D, \\ p^m & \text{otherwise.} \end{cases}$$

If we define

$$f(C) = \begin{cases} 1 - |\mathbb{P}^1_n| - h_0 & \text{if } C = D, \\ 1 + h_0 & \text{if } C = \alpha_n \cdot D, \\ 1 & \text{otherwise,} \end{cases}$$

then we have $p^m f = (\alpha_n - 1)h$, so $[f]$ is an element of order p^m in $\hat{\mathrm{H}}^{-1}(\mathcal{A}_n, T_n^m)$ that maps to 1 under $s : \hat{\mathrm{H}}^{-1}(\mathcal{A}_n, T_n^m) \to \mathbb{Z}/p^m\mathbb{Z}$. Therefore, s splits and we have our result as $\mathcal{A}_n$ is cyclic. □

We now look at the cohomology with respect to $\mathbb{Z}_p[\mathcal{G}_n]$-lattices in V_n, denoted W, that can be scaled such that $pT_n \subseteq W \subseteq T_n$. Then we have a short exact sequence

$$0 \to T_n \to W \to M \to 0$$

where M is an $\mathbb{F}_p[\mathcal{G}_n]$-submodule of Λ_{d_n} as defined in the previous section. We have seen that

$$M^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, M) \cong \begin{cases} 0 & \text{if } M = \Lambda_0, \\ \mathbb{F}_p & \text{otherwise,} \end{cases}$$

by Lemma 3.3.24 and Theorem 3.3.26. For the $M = \Lambda_0$ case, the short exact sequence implies $\mathrm{H}^1(\mathcal{A}_n, W) \cong \mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.

If $M = K_{p^n - 1}$, then we have the short exact sequence

$$0 \to M \to \Lambda_{d_n} \to \Lambda_0 \to 0.$$

Therefore, we have the short exact sequence

$$0 \to W \to T_n \to \Lambda_0 \to 0$$

which implies that $\mathrm{H}^1(\mathcal{A}_n, W) \cong \mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$. The case $M = \Lambda_{d_n}$ is obvious as that would mean $W = T_n$.

For the other cases, we have the exact sequence

$$0 \to \mathbb{F}_p \to \mathrm{H}^1(\mathcal{A}_n, T_n) \to \mathrm{H}^1(\mathcal{A}_n, W) \to \mathbb{F}_p \to 0$$

which leads to the exact sequence

$$0 \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \mathrm{H}^1(\mathcal{A}_n, W) \to \mathbb{F}_p \to 0.$$

Therefore, we have shown the following.

Theorem 3.6.14. *Let W be a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice that can be scaled such that $pT_n \subseteq W \subseteq T_n$. Then*

$$\mathrm{H}^1(\mathcal{A}_n, W) \in \{\mathbb{Z}/p^n\mathbb{Z}, \quad \mathbb{Z}/p^{n-1}\mathbb{Z} \oplus \mathbb{F}_p\}.$$

In particular, $\mathrm{H}^1(\mathcal{A}_n, W)$ must contain an element of order p^{n-1}.

We now want to look at the cohomology with respect to the normaliser of $\mathcal{A}_n$.

3.6.3 The $N(\mathcal{A}_n)$-Cohomology

We now want to look at cohomologies of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to $N(\mathcal{A}_n)$. We have

$$N(\mathcal{A}_n) = \mathcal{A}_n \cup \mathcal{A}_n k$$

where k is a matrix of order 2 and with eigenvalues ± 1. We know that $\mathrm{H}^1(N(\mathcal{A}_n), T_{(n)}) = 0$ for all $n \geq 0$ by Theorem 3.2.7. We can use this for the following.

Proposition 3.6.15. *For all $n \geq 0$, we have $\mathrm{H}^1(N(\mathcal{A}_n), T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We know that

$$\mathrm{H}^1(N(\mathcal{A}_n), T_n) \cong \mathbb{Z}_p \Big/ \gamma\Big(T_{(n)}^{N(\mathcal{A}_n)}\Big)$$

where $\gamma(f) = \sum_C f(C)$. As $N(\mathcal{A}_n)$ acts transitively on $\mathbb{P}^1_n$, then $T_{(n)}^{N(\mathcal{A}_n)} \cong \mathbb{Z}_p$ and $\mathrm{im}(\gamma) = |\mathbb{P}^1_n|\mathbb{Z}_p$, so

$$\mathrm{H}^1(N(\mathcal{A}_n), T_n) \cong \mathbb{Z}_p/|\mathbb{P}^1_n|\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \qquad \square$$

We also look at the cohomology with respect to R_n^k.

Proposition 3.6.16. *For all $0 \leq k \leq n-1$, we have*

$$\mathrm{H}^1(N(\mathcal{A}_n), R_n^k) \cong \mathbb{Z}/p^{n-k}\mathbb{Z}.$$

Proof. We have seen that

$$\mathrm{H}^1(N(\mathcal{A}_n), R_n^k) \cong T_{(k)}^{N(\mathcal{A}_n)} \Big/ \pi\Big(T_{(n)}^{N(\mathcal{A}_n)}\Big)$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. As $N(\mathcal{A}_n)$ acts transitively on $\mathbb{P}^1_n$, then

$$T_{(n)}^{N(\mathcal{A}_n)} \cong T_{(k)}^{N(\mathcal{A}_n)} \cong \mathbb{Z}_p.$$

Then the image of π is the multiplication-by-p^{n-k} mapping and so

$$\mathrm{H}^1(N(\mathcal{A}_n), R_n^k) \cong \mathbb{Z}/p^{n-k}\mathbb{Z}. \qquad \square$$

We again look at the cohomology associated to T_n^m.

Corollary 3.6.17. *We have $\mathrm{H}^2(N(\mathcal{A}_n), T_n^m) = 0$ for all $0 \leq m \leq n$.*

Proof. As $(T_n^m)^{\mathcal{A}_n} = \mathrm{H}^2(\mathcal{A}_n, T_n^m) = 0$, then by Proposition 3.2.1, we have

$$\mathrm{H}^2(N(\mathcal{A}_n), T_n^m) \cong \mathrm{H}^1(N(\mathcal{A}_n)/\mathcal{A}_n, \mathrm{H}^1(\mathcal{A}_n, T_n^m)) = 0$$

as 2 is coprime to $|\,\mathrm{H}^1(\mathcal{A}_n, T_n^m)|$. $\square$

We can now use this to find the first cohomology group of T_n^m with respect to $N(\mathcal{A}_n)$.

Theorem 3.6.18. *For all $0 \leq m \leq n$, we have*

$$\mathrm{H}^1(N(\mathcal{A}_n), T_n^m) \cong \mathbb{Z}/p^{n-m}\mathbb{Z}.$$

Proof. We have already seen that we have a short exact sequence

$$0 \to T_n \to T_n^m \to \mathbb{Z}/p^m\mathbb{Z} \to 0$$

which induces

$$0 \to \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{H}^1(N(\mathcal{A}_n), T_n) \to \mathrm{H}^1(N(\mathcal{A}_n), T_n^m) \to \mathrm{Hom}(N(\mathcal{A}_n), \mathbb{Z}/p^m\mathbb{Z}) \to 0$$

as $(T_n^m)^{N(\mathcal{A}_n)} = \mathrm{H}^2(N(\mathcal{A}_n), T_n) = 0$ and $N(\mathcal{A}_n)$ acts trivially on $\mathbb{Z}/p^m\mathbb{Z}$.

We now show that $\mathrm{Hom}(N(\mathcal{A}_n), \mathbb{Z}/p^m\mathbb{Z})$ is trivial. We know

$$N(\mathcal{A}_n) = \langle r, s | r^{t_0} = s^2 = (sr)^2 = 1 \rangle$$

is a dihedral group. So, let $f \in \mathrm{Hom}(N(\mathcal{A}_n), \mathbb{Z}/p^m\mathbb{Z})$. Then $|f(s)| \Big| 2$ and $|f(s)| \Big| p^m$. But as p is odd, then this means that $f(s) = 1$ and

$$f(r) = f(s)f(r) = f(sr).$$

But then we follow the same idea to show that $f(r) = 1$ and so f must be trivial. Hence, using the exact sequence and Proposition 3.6.15, we have our result. □

We now move on to look at the cohomology with respect to a Borel subgroup.

3.6.4 The $\mathcal{B}_n$-Cohomology

We have $\mathrm{H}^1(\mathcal{B}_n, T_{(n)}) = 0$ by Theorem 3.2.7. We also know that there exists a point of $\mathbb{P}_n^1$ that is fixed by $\mathcal{B}_n$. Therefore, by Lemma 3.6.1, $\mathrm{H}^1(\mathcal{B}_n, T_n) = 0$ also.

We have an exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. This leads to the following.

Proposition 3.6.19. *For all $0 \leq k \leq n-1$, we have*

$$\mathrm{H}^1(\mathcal{B}_n, R_n^k) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^{k+1}.$$

Proof. From the short exact sequence above and as $\mathrm{H}^1(\mathcal{B}_n, T_{(n)}) = 0$, we have

$$\mathrm{H}^1(\mathcal{B}_n, R_n^k) \cong T_{(k)}^{\mathcal{B}_n} \big/ \pi\big(T_{(n)}^{\mathcal{B}_n}\big).$$

We look at the action of $\mathcal{B}_n$ on $\mathbb{P}_n^1$. If we fix $D_0 \in \mathbb{P}_0^1$, then $\mathcal{B}_n$ acts transitively on the set $C \not\supset D_0$. Also, if we fix $D_i \in \mathbb{P}_i^1$ for $0 \leq i \leq n$, where

$$D_n \supset D_{n-1} \supset \ldots \supset D_1 \supset D_0,$$

and define

$$\Pi_i = \Big\{C \in \mathbb{P}_n^1 : \ C \supset D_i \text{ but } C \not\supset D_{i+1}\Big\},$$

then $\mathcal{B}_n$ acts transitively on Π_i for all $0 \leq i \leq n$. Therefore, $T_{(n)}^{\mathcal{B}_n} \cong \mathbb{Z}_p^{n+2}$ and $T_{(k)}^{\mathcal{B}_n} \cong \mathbb{Z}_p^{k+2}$. However, the image of π is $\mathbb{Z}_p \oplus (p^{n-k}\mathbb{Z}_p)^{k+1}$ and so $\mathrm{H}^1(\mathcal{B}_n, R_n) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^{k+1}$. □

We now want to look generally at $\mathbb{Z}_p[\mathcal{G}_n]$-lattices. Let W be a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice. Then we can scale W such that $T_n \subseteq W \subseteq \frac{1}{p^k} T_n$ for some $k \geq 1$. We would like to show the following.

Theorem 3.6.20. *Let W be a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice of V_n such that $W^{\mathcal{B}_n} = T_n^{\mathcal{B}_n}$. Then $W \cong T_n$.*

We have the short exact sequence

$$0 \to T_n \to W \to {}^{W}\!/_{T_n} \to 0.$$

Therefore, if $W^{\mathcal{B}_n} = T_n^{\mathcal{B}_n}$ then $({}^{W}\!/_{T_n})^{\mathcal{B}_n} = 0$ as $\mathrm{H}^1(\mathcal{B}_n, T_n) = 0$. We have the following.

Proposition 3.6.21. *Let Z be a non-trivial $\mathbb{Z}/p^k\mathbb{Z}[\mathcal{G}_n]$-module contained in ${}^{T_{(n)}}\!/_{p^k T_{(n)}}$ for $k \geq 1$. Then $Z^{\mathcal{B}_n} \neq 0$.*

Proof. We do this by induction. The $k = 1$ case is true by Lemma 3.3.27 so assume this is true for k. Let $\overline{T}_{(n)} = \mathbb{F}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right]$. We have a short exact sequence

$$0 \to \overline{T}_{(n)} \to {}^{T_{(n)}}/_{p^{k+1}T_{(n)}} \to {}^{T_{(n)}}/_{p^k T_{(n)}} \to 0$$

so we can view $\overline{T}_{(n)}$ as a $\mathbb{Z}/p^{k+1}\mathbb{Z}[\mathcal{G}_n]$-submodule of ${}^{T_{(n)}}/_{p^{k+1}T_{(n)}}$. Let Z be a non-trivial $\mathbb{Z}/p^{k+1}\mathbb{Z}[\mathcal{G}_n]$-module contained in ${}^{T_{(n)}}/_{p^{k+1}T_{(n)}}$. If $Z \cap \overline{T}_{(n)} \neq 0$, then Z contains an irreducible $\mathbb{F}_p[\mathcal{G}_n]$-module U such that $U^{\mathcal{B}_n} \neq 0$ as shown in Lemma 3.3.27. Hence we can assume $Z \cap \overline{T}_{(n)} = 0$. Then by the second isomorphism theorem, we have

$$\frac{Z + \overline{T}_{(n)}}{\overline{T}_{(n)}} \cong \frac{Z}{Z \cap \overline{T}_{(n)}} \cong Z.$$

Hence

$$Z \cong \frac{Z + \overline{T}_{(n)}}{\overline{T}_{(n)}} \leq \frac{{}^{T_{(n)}}/_{p^{k+1}T_{(n)}}}{\overline{T}_{(n)}} \cong {}^{T_{(n)}}/_{p^k T_{(n)}}.$$

As $Z \neq 0$, then by induction, $Z^{\mathcal{B}_n} \neq 0$. □

We finish this section by proving the theorem.

Proof of Theorem 3.6.20. We can scale W such that $T_n \subseteq W \subseteq \frac{1}{p^k}T_n$ for some $k \geq 1$. As $W^{\mathcal{B}_n} = T_n^{\mathcal{B}_n}$, then we have seen that $({}^{W}/_{T_n})^{\mathcal{B}_n} = 0$. Therefore by Proposition 3.6.21, $W \cong T_n$. □

We now move onto the standard Iwahori subgroup.

3.6.5 The $\mathcal{I}_n$-Cohomology

Define an element $D \in \mathbb{P}^1_0$ to be the fixed point of $\mathcal{I}_n$. Then $\mathcal{I}_n$ acts transitively on the sets $\{C \in \mathbb{P}^1_n : C \supset D\}$ and $\{C \in \mathbb{P}^1_n : C \not\supset D\}$. We have $\mathrm{H}^1(\mathcal{I}_n, T_{(n)}) = 0$ by Theorem 3.2.7. We use this for the following.

Lemma 3.6.22. *For all $n \geq 0$, we have $\mathrm{H}^1(\mathcal{I}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We have seen that if we have the short exact sequence

$$0 \to T_n \to T_{(n)} \xrightarrow{\gamma} \mathbb{Z}_p \to 0$$

then

$$\mathrm{H}^1(\mathcal{I}_n, T_n) \cong \mathbb{Z}_p \big/ \gamma\big(T_{(n)}^{\mathcal{I}_n}\big)$$

where $\gamma(f) = \sum_C f(C)$. We see that $T_{(n)}^{\mathcal{I}_n}$ is generated by the elements

$$f(C) = \begin{cases} 1 & \text{if } C \supset D, \\ 0 & \text{otherwise.} \end{cases}$$

and

$$h(C) = \begin{cases} 1 & \text{if } C \not\supset D, \\ 0 & \text{otherwise.} \end{cases}$$

with $\gamma(f) = p^n$ and $\gamma(h) = p^{n+1}$. Therefore, $\mathrm{im}(\gamma) = p^n\mathbb{Z}_p$ which gives our result. □

We also look at the cohomology with respect to T_n^m.

Lemma 3.6.23. *For all $n \geq 0$, we have $\mathrm{H}^1(\mathcal{I}_n, T_n^m) \cong \mathbb{Z}/p^{n-m}\mathbb{Z}$.*

Proof. We have the short exact sequence $0 \to T_n \to T_n^m \xrightarrow{\overline{g}} \mathbb{Z}/p^m\mathbb{Z} \to 0$ which induces

$$0 \to T_n^{\mathcal{I}_n} \to (T_n^m)^{\mathcal{I}_n} \xrightarrow{\overline{g}} \mathbb{Z}/p^m\mathbb{Z} \to \mathrm{H}^1(\mathcal{I}_n, T_n) \to \mathrm{H}^1(\mathcal{I}_n, T_n^m) \to 0$$

as $\mathcal{I}_n$ acts trivially on $\mathbb{Z}/p^m\mathbb{Z}$, so $\mathrm{H}^1(\mathcal{I}_n, \mathbb{Z}/p^m\mathbb{Z}) = \mathrm{Hom}(\mathcal{I}_n, \mathbb{Z}/p^m\mathbb{Z}) = 0$ by Proposition 3.1.8. We see that $T_n^{\mathcal{I}_n}$ is generated by the element

$$f(C) = \begin{cases} 1 & \text{if } C \not\supset D, \\ -p & \text{otherwise.} \end{cases}$$

Using this, as $T_n^m \subseteq T_n$, then $(T_n^m)^{\mathcal{I}_n} \subseteq T_n^{\mathcal{I}_n}$ and so $(T_n^m)^{\mathcal{I}_n}$ is generated by a multiple of f. Therefore, $(T_n^m)^{\mathcal{I}_n}$ is generated by $p^m f$ as this is the smallest multiple of f in T_n^m and so the mapping $\overline{g}$ is the zero map. Therefore, as $\mathrm{H}^1(\mathcal{I}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$, this gives our result. □

We also look at the cohomology with respect to R_n^k.

Lemma 3.6.24. *For all $n \geq 1$ and $0 \leq k \leq n-1$, we have*

$$\mathrm{H}^1(\mathcal{I}_n, R_n^k) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^2.$$

Proof. We know that as we have the short exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0$$

where $\pi(f)(C') = \sum_{C \supset C'} f(C)$, then

$$\mathrm{H}^1(\mathcal{I}_n, R_n^k) \cong T_{(k)}^{\mathcal{I}_n} \big/ \pi\big(T_{(n)}^{\mathcal{I}_n}\big).$$

We have seen that $T_{(n)}^{\mathcal{I}_n}$ is generated by the elements f and h where

$$f(C) = \begin{cases} 1 & \text{if } C \supset D, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$h(C) = \begin{cases} 1 & \text{if } C \not\supset D, \\ 0 & \text{otherwise,} \end{cases}$$

and the generators of $T_{(k)}^{\mathcal{I}_n}$ are similarly defined. Therefore, $\mathrm{im}(\pi) = p^{n-k} T_{(k)}^{\mathcal{I}_n}$ and so

$$\mathrm{H}^1(\mathcal{I}_n, R_n^k) \cong T_{(k)}^{\mathcal{I}_n} / p^{n-k} T_{(k)}^{\mathcal{I}_n} \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^2. \qquad \square$$

We are able to use these results in the next part where we look at the cohomologies associated to $\mathcal{P}_n$.

3.6.6 The $\mathcal{P}_n$-Cohomology

Again, define an element $D \in \mathbb{P}_0^1$ to be the fixed point of $\mathcal{P}_n$. Then $\mathcal{P}_n$ acts transitively on the sets $\{C \in \mathbb{P}_n^1 : C \supset D\}$ and $\{C \in \mathbb{P}_n^1 : C \not\supset D\}$. Also, by Theorem 3.2.7, we have $\mathrm{H}^1(\mathcal{P}_n, T_{(n)}) = 0$. We use these pieces of information for the following.

Lemma 3.6.25. *For all $n \geq 0$, we have $\mathrm{H}^1(\mathcal{P}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We have seen that if we have the short exact sequence

$$0 \to T_n \to T_{(n)} \xrightarrow{\gamma} \mathbb{Z}_p \to 0$$

then

$$\mathrm{H}^1(\mathcal{P}_n, T_n) \cong \mathbb{Z}_p \big/ \gamma\left(T_{(n)}^{\mathcal{P}_n}\right)$$

where $\gamma(f) = \sum_C f(C)$. As $\mathrm{im}(\gamma) = p^n\mathbb{Z}_p$, this gives our result. □

We also look at the cohomology with respect to R_n^k.

Lemma 3.6.26. *For all $n \geq 1$ and $0 \leq k \leq n-1$, we have*

$$\mathrm{H}^1(\mathcal{P}_n, R_n^k) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^2.$$

Proof. We know that as we have the short exact sequence

$$0 \to R_n^k \to T_{(n)} \xrightarrow{\pi} T_{(k)} \to 0$$

where $\pi(f)(C') = \sum_{C \supset C'} f(C)$, then

$$\mathrm{H}^1(\mathcal{P}_n, R_n^k) \cong T_{(k)}^{\mathcal{P}_n} / \pi\left(T_{(n)}^{\mathcal{P}_n}\right).$$

We have $\mathrm{im}(\pi) = p^{n-k}T_{(k)}^{\mathcal{P}_n}$ and so

$$\mathrm{H}^1(\mathcal{P}_n, R_n^k) \cong T_{(k)}^{\mathcal{P}_n} / p^{n-k}T_{(k)}^{\mathcal{P}_n} \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^2.$$ □

We now move on to the cohomology with respect to $\mathcal{H}_n$.

3.6.7 The $\mathcal{H}_n$-Cohomology

We know that

$$\mathrm{H}^1(\mathcal{H}_n, T_{(n)}) = \mathrm{H}^1(\mathcal{H}_n, T_n) = 0$$

by Theorem 3.2.7 and Lemma 3.6.1. We would like to calculate the second cohomology groups with respect to these $\mathbb{Z}_p[\mathcal{G}_n]$-lattices.

Proposition 3.6.27. *For all $n \geq 0$,*

$$\mathrm{H}^2(\mathcal{H}_n, T_{(n)}) \cong \begin{cases} (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{n/2}} \oplus \bigoplus_{k=1}^{\frac{n}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is even,} \\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{(n+1)/2}} \oplus \bigoplus_{k=1}^{\frac{n-1}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. We know that

$$\mathrm{H}^2(\mathcal{H}_n, T_{(n)}) \cong \bigoplus_{\text{Orbits } \mathcal{H}_n \cdot C \text{ of } \mathcal{H}_n \text{ on } \mathbb{P}^1_n} \mathbb{Z}_p/|\mathrm{Stab}_{\mathcal{H}_n}(C)|\mathbb{Z}_p$$

by Lemma 3.6.2 as $\mathcal{H}_n$ is cyclic.

Now, we know $y = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generates $\mathcal{H}_n$. Then y acts transitively on the set

$$A = \{[u : 1] : u \in \mathbb{Z}/p^{n+1}\mathbb{Z}\},$$

which has size p^{n+1}, so for this orbit, the stabiliser is trivial.

We will have a look at the fixed elements. We have $y \cdot [1 : 0] = [1 : 0]$ and

$$y \cdot [1 : p^k u] = [1 + p^k u : p^k u]$$

for $1 \leq k \leq n$. But, if $k \geq \lfloor \frac{n+2}{2} \rfloor$, then $(1 + p^k u)^{-1} = 1 - p^k u$ and so

$$[1 + p^k u : p^k u] = [1 : p^k u(1 - p^k u)] = [1 : p^k u]$$

as $2k \geq n + 1$. Here $\lfloor \cdot \rfloor$ is the floor function. Hence the fixed points are either $[1 : 0]$ or of the form $[1 : p^k u]$ for $\lfloor \frac{n+2}{2} \rfloor \leq k \leq n$ and so we have the following number of fixed points:

$$\begin{cases} 1 + \sum\limits_{j=\frac{n+2}{2}}^{n} p^{n-j}(p-1) = p^{\frac{n}{2}} & \text{if } n \text{ is even,} \\ 1 + \sum\limits_{j=\frac{n+1}{2}}^{n} p^{n-j}(p-1) = p^{\frac{n+1}{2}} & \text{if } n \text{ is odd.} \end{cases}$$

where $p^{n-i}(p-1)$ comes from the size of $C_i = \{[1 : a] : \mathrm{ord}_p(a) = i\}$ for $1 \leq i \leq n$.

We just need to have a look at the elements in C_i for $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$. We see that $y \cdot [1 : p^i u] = \left[1 : \frac{p^i u}{1 + p^i u}\right]$. As $1 + p^i u$ is a unit, then $y \cdot [1 : p^i u] \in C_i$ for all i.

We will look at the stabilisers for each element. Let $\overline{a} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{H}_n$. Then if $\overline{a} \in \mathrm{Stab}_{\mathcal{H}_n}([1 : p^i u])$, we have $\left[1 : \frac{p^i u}{1+ap^i u}\right] = [1 : p^i u]$ and so

$$p^i u(1 + ap^i u) \equiv p^i u \pmod{p^{n+1}}.$$

Hence, $ap^{2i}u^2 \equiv 0 \pmod{p^{n+1}}$ and so $p^{n+1-2i} | a$ as $p \nmid u$. Therefore

$$\mathrm{Stab}_{\mathcal{H}_n}([1 : p^i u]) = \left\langle \left(\begin{smallmatrix} 1 & p^{n+1-2i} \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$$

which has size p^{2i} for all $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$.

We now just need to see how many orbits are contained in each C_i. This is just

$$\frac{|C_i| \cdot |\mathrm{Stab}_{\mathcal{H}_n}([1 : p^i u])|}{|\mathcal{H}_n|} = \frac{p^{n-i}(p-1)p^{2i}}{p^{n+1}} = p^{i-1}(p-1)$$

as each orbit contained in C_i has the same size due to them all having the same stabiliser group. Then we obtain our answer. □

We can use this to show the following.

Proposition 3.6.28. *For all $n \geq 0$,*

$$\mathrm{H}^2(\mathcal{H}_n, T_n) \cong \begin{cases} (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{n/2}-1} \oplus \bigoplus_{k=1}^{\frac{n}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is even,} \\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{(n+1)/2}-1} \oplus \bigoplus_{k=1}^{\frac{n-1}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. We have the short exact sequence $0 \to T_n \to T_{(n)} \xrightarrow{\gamma} \mathbb{Z}_p \to 0$ which induces

$$0 \to \hat{\mathrm{H}}^0(\mathcal{H}_n, T_n) \to \hat{\mathrm{H}}^0(\mathcal{H}_n, T_{(n)}) \to \hat{\mathrm{H}}^0(\mathcal{H}_n, \mathbb{Z}_p) \to 0$$

where $\hat{\mathrm{H}}^{-1}(\mathcal{H}_n, T_n) \cong \mathrm{H}^1(\mathcal{H}_n, T_n) = 0$ as $\mathcal{H}_n$ is cyclic and $\hat{\mathrm{H}}^{-1}(\mathcal{H}_n, \mathbb{Z}_p) = 0$. Also, by Proposition 3.6.27, we have

$$\hat{\mathrm{H}}^0(\mathcal{H}_n, T_{(n)}) \cong \begin{cases} (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{n/2}} \oplus \bigoplus_{k=1}^{\frac{n}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is even,} \\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{(n+1)/2}} \oplus \bigoplus_{k=1}^{\frac{n-1}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is odd.} \end{cases}$$

As Proposition 3.6.3 shows that $\hat{\mathrm{H}}^0(\mathcal{H}_n, \mathbb{Z}_p) \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$, then

$$\hat{\mathrm{H}}^0(\mathcal{H}_n, T_n) \cong \begin{cases} (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{n/2}-1} \oplus \bigoplus_{k=1}^{\frac{n}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is even,} \\ (\mathbb{Z}/p^{n+1}\mathbb{Z})^{p^{(n+1)/2}-1} \oplus \bigoplus_{k=1}^{\frac{n-1}{2}} (\mathbb{Z}/p^{2k}\mathbb{Z})^{p^{k-1}(p-1)} & \text{if } n \text{ is odd.} \end{cases}$$

We then have our result as H is cyclic. □

This can then be used to prove the following.

Theorem 3.6.29. *We have for all $1 \leq m \leq n$, we have*

$$\mathrm{H}^1(\mathcal{H}_n, T_n^m) = 0$$

and $|\mathrm{H}^2(\mathcal{H}_n, T_n^m)| = |\mathrm{H}^2(\mathcal{H}_n, T_n)|$.

Proof. We have the short exact sequence $0 \to T_n \to T_n^m \xrightarrow{\overline{g}} \mathbb{Z}/p^m\mathbb{Z} \to 0$ which induces

$$0 \to \hat{\mathrm{H}}^{-1}(\mathcal{H}_n, T_n^m) \to \hat{\mathrm{H}}^{-1}(\mathcal{H}_n, \mathbb{Z}/p^m\mathbb{Z}) \to \hat{\mathrm{H}}^0(\mathcal{H}_n, T_n) \to$$
$$\to \hat{\mathrm{H}}^0(\mathcal{H}_n, T_n^m) \to \hat{\mathrm{H}}^0(\mathcal{H}_n, \mathbb{Z}/p^m\mathbb{Z}) \to 0.$$

As $\mathcal{H}_n$ acts trivially on $\mathbb{Z}/p^m\mathbb{Z}$, then

$$\hat{\mathrm{H}}^{-1}(\mathcal{H}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \hat{\mathrm{H}}^0(\mathcal{H}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathbb{Z}/p^m\mathbb{Z}.$$

Let $\delta : \hat{\mathrm{H}}^{-1}(\mathcal{H}_n, \mathbb{Z}/p^m\mathbb{Z}) \to \hat{\mathrm{H}}^0(\mathcal{H}_n, T_n)$ and $C_0 \in \mathbb{P}_n^1$ be fixed by $\mathcal{H}_n$. Let $t \in \mathbb{Z}/p^m\mathbb{Z}$ and $f_t \in T_n^m$ be defined as

$$f_t(C) = \begin{cases} t(1 - |\mathbb{P}_n^1|) & \text{if } C = C_0, \\ t & \text{otherwise.} \end{cases}$$

Then we have $\overline{g}(f_t) = t$ and

$$\mathrm{Nm}_{\mathcal{H}_n}(f_t)(C) = \begin{cases} tp^{n+1}(1 - |\mathbb{P}_n^1|) & \text{if } C = C_0, \\ tp^{n+1} & \text{otherwise.} \end{cases}$$

Hence, $\delta(t) \in T_n$ is represented by the map

$$\delta(t)(C) = \begin{cases} tp^{n+1-m}(1 - |\mathbb{P}_n^1|) & \text{if } C = C_0, \\ tp^{n+1-m} & \text{otherwise.} \end{cases}$$

To show δ is injective, we want to show that the only value of t such that $\delta(t) = \mathrm{Nm}_{\mathcal{H}_n}(h)$ for some $h \in T_n$ is 0. As C_0 is fixed by $\mathcal{H}_n$, then $\mathrm{Nm}_{\mathcal{H}_n}(h)(C_0)$ is a multiple of $|\mathcal{H}_n| = p^{n+1}$. Therefore, we must have t divisible by p^m. Hence, δ is injective and $\hat{\mathrm{H}}^{-1}(\mathcal{H}_n, T_n^m) = 0$. This also shows that

$$|\hat{\mathrm{H}}^0(\mathcal{H}_n, T_n^m)| = |\hat{\mathrm{H}}^0(\mathcal{H}_n, T_n)|$$

and we have our result as $\mathcal{H}_n$ is cyclic. □

We next look at the cohomology with respect to a split Cartan subgroup.

3.6.8 The $\mathcal{D}_n$-Cohomology

We know that

$$\mathrm{H}^1(\mathcal{D}_n, T_{(n)}) = \mathrm{H}^1(\mathcal{D}_n, T_n) = 0$$

by Theorem 3.2.7 and Lemma 3.6.1. We would like to calculate the second cohomology groups with respect to these $\mathbb{Z}_p[\mathcal{G}_n]$-lattices.

Lemma 3.6.30. *For all $n \geq 0$, we have*

$$\mathrm{H}^2(\mathcal{D}_n, T_{(n)}) \cong \left(\mathbb{Z}/p^n\mathbb{Z} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/p^i\mathbb{Z}\right)^2.$$

Proof. If we let $C_0, C_1 \in \mathbb{P}_n^1$ be the points fixed by $\mathcal{D}_n$, then as the $\mathcal{D}_n$-orbits are the points with the same distance from C_i, by Lemma 3.6.2, we have our result as $\mathcal{D}_n$ is cyclic. □

We use this result to show the following.

Lemma 3.6.31. *For all $n \geq 0$, we have*

$$\mathrm{H}^2(\mathcal{D}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z} \oplus \left(\bigoplus_{i=1}^{n} \mathbb{Z}/p^i\mathbb{Z}\right)^2.$$

Proof. We have already seen that we have the short exact sequence

$$0 \to T_n \to T_{(n)} \xrightarrow{\gamma} \mathbb{Z}_p \to 0$$

which induces

$$0 \to \mathrm{H}^2(\mathcal{D}_n, T_n) \to \mathrm{H}^2(\mathcal{D}_n, T_{(n)}) \to \mathrm{H}^2(\mathcal{D}_n, \mathbb{Z}_p) \to 0,$$

as $\mathrm{H}^1(\mathcal{D}_n, \mathbb{Z}_p) = \mathrm{H}^1(\mathcal{D}_n, T_n) = 0$ and $\mathcal{D}_n$ is cyclic. As Proposition 3.6.3 shows that $\mathrm{H}^2(\mathcal{D}_n, \mathbb{Z}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$, we have our result using Lemma 3.6.30. □

We can then use this result in order to prove the following.

Proposition 3.6.32. *We have for all* $0 \leq m \leq n$,

$$\mathrm{H}^1(\mathcal{D}_n, T_n^m) = 0$$

and $|\mathrm{H}^2(\mathcal{D}_n, T_n^m)| = |\mathrm{H}^2(\mathcal{D}_n, T_n)| = p^{n^2+2n}$.

Proof. We have seen that we have the short exact sequence

$$0 \to T_n \to T_n^m \xrightarrow{\overline{g}} \mathbb{Z}/p^m\mathbb{Z} \to 0$$

which induces

$$0 \to \hat{\mathrm{H}}^{-1}(\mathcal{D}_n, T_n^m) \to \hat{\mathrm{H}}^{-1}(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z}) \to \hat{\mathrm{H}}^0(\mathcal{D}_n, T_n) \to$$

$$\to \hat{\mathrm{H}}^0(\mathcal{D}_n, T_n^m) \to \hat{\mathrm{H}}^0(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z}) \to 0$$

as $\hat{\mathrm{H}}^{-1}(\mathcal{D}_n, T_n) = 0$. The action of $\mathcal{D}_n$ on $\mathbb{Z}/p^m\mathbb{Z}$ is trivial, so

$$\hat{\mathrm{H}}^{-1}(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \hat{\mathrm{H}}^0(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z}) \cong \mathbb{Z}/p^m\mathbb{Z}.$$

Let $\delta : \hat{\mathrm{H}}^{-1}(\mathcal{D}_n, \mathbb{Z}/p^m\mathbb{Z}) \to \hat{\mathrm{H}}^0(\mathcal{D}_n, T_n)$ and $C_0 \in \mathbb{P}_n^1$ be fixed by $\mathcal{D}_n$. Let $t \in \mathbb{Z}/p^m\mathbb{Z}$ and $f_t \in T_n^m$ be defined as

$$f_t(C) = \begin{cases} t(1 - |\mathbb{P}_n^1|) & \text{if } C = C_0, \\ t & \text{otherwise.} \end{cases}$$

Then we have $\overline{g}(f_t) = t$ and

$$\mathrm{Nm}_{\mathcal{D}_n}(f_t)(C) = \begin{cases} t|\mathcal{D}_n|(1 - |\mathbb{P}_n^1|) & \text{if } C = C_0, \\ t|\mathcal{D}_n| & \text{otherwise.} \end{cases}$$

Hence, $\delta(t) \in T_n$ is represented by the map

$$\delta(t)(C) = \begin{cases} t\frac{|\mathcal{D}_n|}{p^m}(1 - |\mathbb{P}^1_n|) & \text{if } C = C_0, \\ t\frac{|\mathcal{D}_n|}{p^m} & \text{otherwise.} \end{cases}$$

To show δ is injective, we want to show that the only value of t such that $\delta(t) = \mathrm{Nm}_{\mathcal{D}_n}(h)$ for some $h \in T_n$ is 0. As C_0 is fixed by $\mathcal{D}_n$, then $\mathrm{Nm}_{\mathcal{D}_n}(h)(C_0)$ is a multiple of $|\mathcal{D}_n|$. Therefore, we must have t divisible by p^m. Hence, δ is injective and $\hat{\mathrm{H}}^{-1}(\mathcal{D}_n, T_n^m) = 0$. This also shows that

$$|\hat{\mathrm{H}}^0(\mathcal{D}_n, T_n^m)| = |\hat{\mathrm{H}}^0(\mathcal{D}_n, T_n)|$$

and we have our result as $\mathcal{D}_n$ is cyclic. □

We also look at the cohomology with respect to R_n^k.

Lemma 3.6.33. *For all $n \geq 1$ and $0 \leq k \leq n-1$, we have*

$$\mathrm{H}^1(\mathcal{D}_n, R_n^k) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^{2k+1}.$$

Proof. We have seen that as $\mathrm{H}^1(\mathcal{D}_n, T_{(n)}) = 0$,

$$\mathrm{H}^1(\mathcal{D}_n, R_n^k) \cong T_{(k)}^{\mathcal{D}_n} \big/ \pi\left(T_{(n)}^{\mathcal{D}_n}\right)$$

where $\pi(f)(D) = \sum_{C \supset D} f(C)$. If we let $C_0, C_1 \in \mathbb{P}^1_n$ be the points fixed by $\mathcal{D}_n$, then as the $\mathcal{D}_n$-orbits are the points with the same distance from C_i, we have $T_{(n)}^{\mathcal{D}_n} \cong \mathbb{Z}_p^{2n+3}$ and similarly $T_{(k)}^{\mathcal{D}_n} \cong \mathbb{Z}_p^{2k+3}$. However, the image of π is $\mathbb{Z}_p^2 \oplus (p^{n-k}\mathbb{Z}_p)^{2k+1}$ and so $\mathrm{H}^1(\mathcal{D}_n, R_n) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^{2k+1}$. □

We are able to use the results in this section when calculating the cohomology with respect to the normaliser of a split Cartan subgroup.

3.6.9 The $N(\mathcal{D}_n)$-Cohomology

We briefly mention the cohomologies of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to $N(\mathcal{D}_n)$. We have

$$N(\mathcal{D}_n) = \mathcal{D}_n \cup \mathcal{D}_n h$$

where $h = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which is a matrix of order 2. We will use the results from the previous section to prove the following.

Proposition 3.6.34. *For all $n \geq 0$, we have*

$$\mathrm{H}^1(N(\mathcal{D}_n), T_{(n)}) = 0.$$

Proof. We know $\mathrm{H}^1(\mathcal{D}_n, T_{(n)}) = 0$. We also see that $T_{(n)}^{\mathcal{D}_n}$ is the set of functions constant on the orbits of $\mathcal{D}_n$. If we look at these orbits under the action of $N(\mathcal{D}_n)/\mathcal{D}_n$, then none are fixed. So as a $N(\mathcal{D}_n)/\mathcal{D}_n$-module, $T_{(n)}^{\mathcal{D}_n}$ is an induced module, which gives our result by Shapiro's Lemma. □

We also have the following.

Proposition 3.6.35. *For all $0 \leq m \leq n$, we have $\mathrm{H}^1(N(\mathcal{D}_n), T_n^m) = 0$*

Proof. As $\mathrm{H}^1(\mathcal{D}_n, T_n^m) = 0$ by Proposition 3.6.32, then

$$\mathrm{H}^1(N(\mathcal{D}_n), T_n^m) \cong \mathrm{H}^1(N(\mathcal{D}_n)/\mathcal{D}_n, (T_n^m)^{\mathcal{D}_n})$$

by Proposition 3.2.2. The cyclic quotient group has order prime to p, so we have

$$\mathrm{H}^1(N(\mathcal{D}_n)/\mathcal{D}_n, (T_n^m)^{\mathcal{D}_n}) = 0$$

which gives our result. □

This concludes our look at the cohomologies of $\mathbb{Z}_p[\mathcal{G}_n]$-lattices with respect to subgroups of $\mathcal{G}_n$. We now wish to apply some of the results to the higher modular points.

Chapter 4

Modular Points on Elliptic Curves

In this chapter, we look to extend the idea of self points to a generalised construction of modular point. In particular, we use more advanced methods in modular representation theory to show that Selmer groups over certain fields must contain non-trivial elements when the higher modular points satisfy certain conditions.

We will show that some of the properties associated to the self points carry to the generalised setting and further, we look at the divisibility of these points in the Mordell-Weil group. We then show that, as in the self point case, a link can be established between the modular points and certain $\mathbb{Q}_p[\mathcal{G}_n]$-modules. We can then use the results in the previous chapter to understand the saturated groups attached to the modular points.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. We know that there exists a subvariety $Y_0(N_E)$ of $X_0(N_E)$, which is a moduli space of points $x_{A,C} := (A, C)$, where A is an elliptic curve and C is a cyclic subgroup in A of order N_E as shown in the notation. Fixing $A/\mathbb{Q}$ an elliptic curve, the image of $x_{A,C}$ under

$$\Phi_E : X_0(N_E) \to E$$

will be denoted $P_{A,C} \in E(\mathbb{Q}(C))$. We denote the compositum of all such $\mathbb{Q}(C)$ as K_{N_E}. This is the smallest field K such that its absolute Galois group G_K acts by scalars on $A[N_E]$. This has Galois group $G_{N_E} := \mathrm{Gal}(K_{N_E}/\mathbb{Q})$ which can be identified as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N_E\mathbb{Z})$ via the mapping $\overline{\tau}_{\mathbb{Q},A,N_E}$. In particular, as in the self point case as seen on pg. 48, for all $\sigma \in G_{\mathbb{Q}}$, we have $P_{A,C}^{\sigma} = P_{A,C^{\sigma}}$. For a more in depth explanation, see [31, Section 2.4].

We initially look at the divisibility of the modular points in $E(\mathbb{Q}(C))$ and understand the relationships between them in section 4.1. This will provide us with an understanding of the rank of the group generated by these points. As in the self points case, we want to see when the modular points are of infinite order. We obtain the following result, which is Theorem 4.1.1 in this chapter.

Theorem. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $A/\mathbb{Q}$ be an elliptic curve such that the j invariant of A is not in $\frac{1}{2}\mathbb{Z}$ and the degree of any isogeny of A defined over $\mathbb{Q}$ is coprime to N_E. Then the modular points $P_{A,C}$ are of infinite order for all cyclic subgroups C of order N_E in A.*

From this, we can show that if p is a prime with specific conditions related to E, then $P_{A,C}$ is not divisible by p in $E(\mathbb{Q}(C))$ as seen in Proposition 4.1.5. We also see that there exist linear relations between the modular points similar to Proposition 2.3.3, as seen in Proposition 4.1.3. This reduces the rank of the group generated by these points.

We then follow an identical construction as in the higher self point case to create higher modular points for a prime p of good ordinary or multiplicative reduction in subsections 4.2.2 and 4.2.1 respectively. We will show that the trace relations will still exist in the general construction of the higher self points and will form analogue results to both Theorem 2.3.8 and Theorem 2.3.9, as seen in Proposition 4.2.2 and Proposition 4.2.3.

We then look at the proof of Theorem 4.3.1 in section 4.3. This involves following the method of the proof of Theorem 2.3.10 to construct a mapping

$$\delta_n : \mathrm{H}^1(\mathcal{A}_n, S_n) \rightarrow Ш(E/L_n)[p^\infty]$$

as seen in Lemma 4.3.15. Here, S_n denotes the saturated group generated by the higher modular points in $E(F_n)$ as seen in the notation and L_n is the fixed field of F_n by $\mathcal{A}_n$, where F_n and $\mathcal{A}_n$ are as defined in the notation also. This will require looking at the splitting of primes in the field extension F_n/L_n in subsection 4.3.1. This subsection will culminate in using Lemma 4.3.3 and Proposition 4.3.9 to prove Theorem 4.3.2.

With the conditions on p together with Theorem 3.6.20 and Proposition 4.3.16, we can show that the source of δ_n is a cyclic group of order p^n. This result derives from the link between the group generated by the higher modular points and the integral representation theory of $\mathcal{G}_n$. We can then modify Theorem 4.3.1 to look at the case when $A/\mathbb{Q}$ is semistable to show that we only require $p > 3$ and $\overline{\rho}_{\mathbb{Q},A,p}$ to be surjective in order for $\tau_{F,A,p}$ to be surjective, as seen in Proposition 4.3.17. This leads to Theorem 4.3.18

We finally look at some examples of applying Theorem 4.3.18 in section 4.4.

4.1 Modular Points on Elliptic Curves

In this section, we will see when the points $P_{A,C}$ are of infinite order. Further, when the prime p satisfies certain conditions with respect to E, we will show that the points $P_{A,C}$ are not divisible by p in $E(\mathbb{Q}(C))$. We prove the following.

Theorem 4.1.1. *Let $A/\mathbb{Q}$ and $E/\mathbb{Q}$ be elliptic curves of conductor N_A and N_E respectively. Suppose the j invariant of A is not in $\frac{1}{2}\mathbb{Z}$. Then there exists a cyclic subgroup of order N_E in A, denoted C, such that $P_{A,C} \in E(\overline{\mathbb{Q}_p})$ is non-torsion.*

Proof. The following has been adapted from the proof of [39, Theorem 5] for the more general setting. Let p be a prime which divides the denominator of the j-invariant of A. If $p^2 \mid N_A$, we know A acquires multiplicative reduction at p over some extension of $\mathbb{Q}$. Fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_p}$. We consider the modular parametrisation over $\overline{\mathbb{Z}_p}$. The modular curve $X_0(N_E)$ over $\overline{\mathbb{Z}_p}$ has a neighbourhood of the cusp ∞ consisting of couples (J, C) of the Tate curve of the form $J(\overline{\mathbb{Q}_p}) = \overline{\mathbb{Q}_p}^{\times}/q^{\mathbb{Z}}$ together with a cyclic subgroup C of order N_E generated by a N_E^{th} root of unity. The parameter q is a p-adic analytic uniformiser at ∞, so that the Spf $\overline{\mathbb{Z}_p}[[q]]$ is the formal completion of $X_0(N_E)/\overline{\mathbb{Z}_p}$ at the cusp ∞, as seen in [23, Chapter 8].

Since A has multiplicative reduction over $\overline{\mathbb{Z}_p}$, there is exactly one point $x_{A,C}$ in the neighbourhood of ∞ on $X_0(N_E)$ which is represented by the p-adic Tate parameter q_A associated to A and C is isomorphic to $\mu[N_E]$, the N_E^{th} roots of unity. Let $f_E = \sum a_n(E)q^n$ be the normalised newform associated to E and let ω_E be the invariant differential on E. If we let Φ_E^* be the pullback map, then by [12, Equation 2.16, pg. 19], we have $\Phi_E^*(\omega_E) = c_E \cdot f_E/q \cdot dq$ where c_E is the Manin constant of E. We see on [34, pg. 127] that

$$\log_E(\Phi_E(x_{A,C})) = \int_O^{\Phi_E(x_{A,C})} \omega_E$$

where $\log_E$ is the formal logarithm associated to E from the formal group $\hat{E}(\mathfrak{m})$ to the maximal ideal $\mathfrak{m}$ of $\overline{\mathbb{Z}_p}$. However, as $x_{A,C}$ is defined by q_A and by the change of variables formula, we have

$$\begin{aligned}\int_O^{\Phi_E(x_{A,C})} \omega_E &= \int_O^{\Phi_E(q_A)} \omega_E \\ &= \int_O^{q_A} \Phi_E^*(\omega_E) \\ &= c_E \cdot \int_0^{q_A} f_E \frac{dq}{q} \\ &= c_E \cdot \sum_{n=1}^{\infty} \frac{a_n(E)}{n} \cdot q_A^n.\end{aligned}$$

We let $|\cdot|_p$ be the normalised absolute value such that $|p|_p = p^{-1}$. We then require the following.

Lemma 4.1.2. *[39, Lemma 6] Let $x_{J,C}$ be a point on $Y_0(N_E)(\overline{\mathbb{Q}_p})$ such that J is isomorphic to the Tate curve with parameter $q_0 \neq 0$ and C is isomorphic to $\mu[N_E]$. If $|q_0|_p < p^{-\frac{1}{p-1}}$ then $\Phi_E(x_{J,C})$ is a point of infinite order on $E(\overline{\mathbb{Q}_p})$.*

Hence, we have for $p \neq 2$ that

$$|q_A|_p = |j(A)|_p^{-1} \leq p^{-1} < p^{-\frac{1}{p-1}}$$

and if $p = 2$ then

$$|q_A|_2 = |j(A)|_2^{-1} \leq p^{-2} < p^{-\frac{1}{p-1}}.$$

Therefore, by the lemma, we have that $P_{A,C} = \Phi_E(x_{A,C})$ is a point of infinite order in $E(\overline{\mathbb{Q}_p})$. □

We assume for all primes ℓ of bad reduction for E, there exists no ℓ-isogeny on A rational over $\mathbb{Q}$. Hence the set of modular points $\{P_{A,C}\}_C$ form a single orbit under the action of G_{N_E}. This shows that the points $P_{A,C}$ are not equal and have the same order for all C. Hence, $P_{A,C}$ is of infinite order in $E(K_{N_E})$ for all C.

We can also show that there exist relationships between these points. These are in fact identical to the relations for the self point case as in Proposition 2.3.3.

Proposition 4.1.3. *The sum of the modular points $P_{A,C}$ as C varies through all cyclic subgroups in A of order N_E is a torsion point defined over $\mathbb{Q}$. Let $d \neq N_E$ be an integer dividing N_E. Then*

$$\sum_{C \supset B} P_{A,C} \in E(K_d)$$

is a torsion point where B is a cyclic subgroup in A of order d and the sum is taken over all cyclic subgroups in A of order N_E containing B. In particular, the sum of all the modular points is a torsion point defined over $\mathbb{Q}$.

Proof. We adapt the proof of [39, Proposition 7] to the general construction. As seen in [27, Section 2], for every triple (M, d, N_E) where $M \cdot d$ divides N_E, there exists a morphism

$$\pi_M : X_0(N_E) \to X_0(d)$$

defined over $\mathbb{Q}$ and defined in the following way. Let $x_{A,C} \in X_0(N_E)$ and let C_M be the unique cyclic subgroup of C of order M. Let $\psi : A \to A/C_M$ be the isogeny associated to C_M and let D_d be the unique cyclic subgroup of $\psi(C)$ of order d. We then define

$$\pi_M(x_{A,C}) = (A/C_M, D_d).$$

In particular, if $M = 1$, then $\pi_1(x_{A,C}) = (A, C[d])$. These maps induce pullback mappings $\pi_M^* : J_0(d) \to J_0(N_E)$ on Jacobians.

We define $J_0(N_E)^{\text{old}}$, the old part of $J_0(N_E)$, as the abelian subvariety over $\mathbb{Q}$ generated by the images of π_M^* for all triples (M, d, N_E) such that $d \neq N_E$. We then define $J_0(N_E)^{\text{new}}$, the new part of $J_0(N_E)$, as the quotient abelian variety of $J_0(N_E)$ by $J_0(N_E)^{\text{old}}$ and so we can view the Jacobian as

$$J_0(N_E) = J_0(N_E)^{\text{old}} \oplus J_0(N_E)^{\text{new}}.$$

Now, let B be a cyclic subgroup in A of order d and let $x_{A,B} = (A, B) \in X_0(d)$. Then if we define $\pi := \pi_1$, by [14, Definition 6.2.5], we have

$$\begin{aligned}\pi^*\Big((x_{A,B}) - (\infty)\Big) &= \sum_{y \in \pi^{-1}(x_{A,B})} y - \pi^*[(\infty)] \\ &= \sum_{C \supset B} (x_{A,C}) - \pi^*[(\infty)].\end{aligned}$$

As N_E is the conductor of E, we have the mapping $\Phi_E : J_0(N_E) \to E$ where $J_0(N_E)^{\text{new}} \twoheadrightarrow E$ by [14, Theorem 8.8.4] and $\text{im}(\pi^*) \subseteq J_0(N_E)^{\text{old}}$ as $d \neq N_E$. Therefore, we have $\text{im}(\pi^*) \subseteq \ker(\Phi_E)$. This gives the relation. In particular, if $d = 1$ then this shows that

$$\sum_C P_{A,C} \in E(\mathbb{Q})$$

is a torsion point. □

Hence, we have provided the terms in which the points are of infinite order and have found the relationships between them in order to understand the group generated by these points. We can in fact further show that the points are not divisible by p in $E(\mathbb{Q}(C))$ when the prime p satisfies certain conditions. One of the conditions we will require is the following.

Definition 4.1.4. *Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime of good reduction for E. Then p is an anomalous prime for E if p divides $|\tilde{E}(\mathbb{F}_p)|$ and is a non-anomalous prime otherwise.*

Using this, we have the following.

Proposition 4.1.5. *Suppose $j(A) \notin \frac{1}{2}\mathbb{Z}$ and $p > 2$ is a prime of multiplicative reduction for A such that it is one of the following:*

- *A prime of split multiplicative reduction for E and $p \nmid \text{ord}_p(\Delta_E)$,*
- *A prime of non-split multiplicative reduction for E,*
- *A non-anomalous prime of good reduction for E.*

Let Δ_A be the minimal discriminant for A. Then $P_{A,C} \notin p^{\text{ord}_p(\Delta_A)} \cdot E(\mathbb{Q}(C))$.

Proof. We saw in the proof of Theorem 4.1.1 that as $j(A) \notin \frac{1}{2}\mathbb{Z}$, then there exists a point $x_{A,C}$ in the neighbourhood of ∞ on $X_0(N_E)$ which is represented by the p-adic Tate parameter q_A associated to A and C is isomorphic to $\mu[N_E]$, the N_E^{th} roots of unity. Therefore, we saw that the point $P_{A,C}$ is of infinite order. Let $\mathfrak{p}$ be the place of $\mathbb{Q}(C)$ corresponding to the chosen embedding $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}_p}$. Now, as $C \cong \mu[N_E]$, we have $\mathbb{Q}_p(C) = \mathbb{Q}_p$. Therefore, as $\mathfrak{p}$ is the place corresponding to C, we must have $\mathbb{Q}(C)_{\mathfrak{p}} = \mathbb{Q}_p$. As p is one of the primes in the proposition with respect to E, then the order of the group of components of E over $\mathbb{Q}_p$ and the number of non-singular points in the reduction $\tilde{E}(\mathbb{F}_p)$ are both prime to p. Hence, if $P_{A,C}$ is divisible by $p^{\text{ord}_p(\Delta_A)}$ in $E(\mathbb{Q}_p)$ then it is divisible by $p^{\text{ord}_p(\Delta_A)}$ in $\hat{E}(p\mathbb{Z}_p)$. But the valuation of $\log_E(P_{A,C})$ shows this cannot happen. Let $z = \log_E(P_{A,C})$. As $\mathbb{Q}(C)_{\mathfrak{p}} = \mathbb{Q}_p$, then we have $\text{ord}_p(q_A) = \text{ord}_p(\Delta_A)$. We then see that

$$\begin{aligned}\text{ord}_p(z) &= \min\{\text{ord}_p(q_A), \text{ord}_p(a_p(E)) + p \cdot \text{ord}_p(q_A) - \text{ord}_p(p)\} \\ &= \min\{\text{ord}_p(\Delta_A), \text{ord}_p(a_p(E)) + p \cdot \text{ord}_p(\Delta_A) - 1\} = \text{ord}_p(\Delta_A)\end{aligned}$$

as $a_p(E)$ is an integer. Therefore $P_{A,C} \in \hat{E}(p^{\text{ord}_p(\Delta_A)}\mathbb{Z}_p)$. If $p \neq 2$, then for all $n \geq 2$, we have $n - \text{ord}_p(n) \geq 2$. This is obviously true for $(n, p) = 1$. If $\text{ord}_p(n) = k \geq 1$, then $n - k \geq p^k - k \geq 2$ by induction. Therefore, we have

$$\begin{aligned}\text{ord}_p(z - q_A) &\geq \min_{n \geq 2} \Big[\text{ord}_p(a_n(E)) - \text{ord}_p(n) + n \cdot \text{ord}_p(q_A) \Big] \\ &\geq \min_{n \geq 2} \Big[n \cdot \text{ord}_p(\Delta_A) - \text{ord}_p(n) \Big] \\ &\geq \min_{n \geq 2} \Big[(n - \text{ord}_p(n)) \cdot \text{ord}_p(\Delta_A) \Big] \\ &\geq 2\,\text{ord}_p(\Delta_A).\end{aligned}$$

Hence, z is congruent to q_A modulo $p^{2\,\text{ord}_p(\Delta_A)}$. So the value z is non zero and hence $P_{A,C} \notin p^{\text{ord}_p(\Delta_A)} \cdot E(\mathbb{Q}(C))$. □

We have now seen the divisibility of the modular points in $E(\mathbb{Q}(C))$. This will become important when we study the application of the representation theory in the previous chapter to the modular points on E.

4.2 Higher Modular Points

We now extend the construction of modular points to higher modular points by following the construction of higher self points in the more generalised setting. We will create a tower of number fields in which the higher modular points will be defined and will show that they satisfy certain trace relations similar to that in Kolyvagin's construction of Heegner points. In particular, the relations between the points show that a link can be established with representations of $\mathcal{G}_n$.

Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively and let D be a cyclic subgroup in A. We then take the isogenous curve A/D and a cyclic subgroup of order N_E in this isogenous curve and look at the image of the point under Φ_E. We will focus on two cases of construction of higher modular points that are an analogue to the construction of the higher self points. The first will be the multiplicative reduction case and the second the good reduction case.

4.2.1 Multiplicative Case

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E and let p be a prime of multiplicative reduction. We let $N_E = pM$ and define $F_n := K_{p^{n+1}M}$ for all $n \geq -1$ with $F := F_{-1}$. We can view $G_n = \mathrm{Gal}(F_n/F)$ as a subgroup of $\mathcal{G}_n$.

Let B be a cyclic subgroup in A of order M. Let $n \geq 0$ and D be a cyclic subgroup in A of order p^{n+1}. Let $C = D[p] \oplus B$ which is a cyclic subgroup of order N_E and let $\psi : A \to A/D$ be the isogeny associated with D with dual $\hat{\psi}$. We define

$$C' = \ker(\hat{\psi})[p] \oplus \psi(B).$$

This is a cyclic subgroup in A/D of order N_E. We then define

$$y_{A,D} = (A/D, C') \in Y_0(N_E)$$

and define a higher modular point above $P_{A,C}$ as the point

$$Q_{A,D} = \Phi_E(y_{A,D}) \in E(F_n).$$

When $n = 0$, we have $C = D \oplus B$ and if we let w_p be the Atkin-Lehner involution on $X_0(N_E)$, then

$$\begin{aligned} w_p(x_{A,C}) &= (A/C[p], (A[p] + C)/C[p]) \\ &= (A/D, (A[p] \oplus B)/D) \\ &= (A/D, \psi(A[p] \oplus B)). \end{aligned}$$

We know that $\psi(A[p] \oplus B)$ is a cyclic subgroup of order N_E. Therefore, we can write

$$\psi(A[p] \oplus B) = U \oplus V$$

where $|U| = p$ and $|V| = M$. We then have

$$\hat{\psi}(U \oplus V) = (\hat{\psi} \circ \psi)(A[p] \oplus B) = [p](A[p] \oplus B) = [p]B = B$$

as $(M, p) = 1$. Therefore,

$$V = [p]V = [p](U \oplus V) = (\psi \circ \hat{\psi})(U \oplus V) = \psi(B).$$

We then see that

$$\hat{\psi}(U \oplus \psi(B)) = B = [p]B = (\hat{\psi} \circ \psi)(B)$$

meaning $U \subseteq \ker(\hat{\psi})$. However, as both have order p, then $U = \ker(\hat{\psi})$ and therefore

$$\begin{aligned} w_p(x_{A,C}) &= (A/D, \psi(A[p] \oplus B)) \\ &= (A/D, \ker(\hat{\psi}) \oplus \psi(B)) \\ &= (A/D, C') \\ &= y_{A,D}. \end{aligned}$$

Therefore, if $a_p(E) \in \{\pm 1\}$ is the Hecke eigenvalue of the newform f attached to E, then we have

$$w_p(f) = -a_p(E) \cdot f$$

by [3, Theorem 5]. Hence, we have

$$\begin{aligned} Q_{A,D} &= \Phi_E(y_{A,D}) \\ &= (\Phi_E \circ w_p)(x_{A,C}) \\ &= -a_p(E) \cdot \Phi_E(x_{A,C}) + T \\ &= -a_p(E) \cdot P_{A,C} + T \end{aligned}$$

for some $T \in E(\mathbb{Q})[2]$.

Let D be a cyclic subgroup in A of order p^{n+1}. Let T_p be the Hecke operator T_p on $J_0(N_E)$. Then

$$T_p((y_{A,D}) - (\infty)) = \sum_H (((A/D)/H, (C' + H)/H) - (\infty))$$

where the sum runs through all cyclic subgroups in A/D, denoted H, of order p that intersect trivially with C'. However, as H is a cyclic subgroup in A/D of order p, then there exists a cyclic subrgroup D' in A of order p^{n+2} such that $H = D'/D$. Therefore, $D' \supset D$. Also, we must have

$$H \cap C' = H \cap \ker(\hat{\psi}) \in \{0, H\}$$

as H is of order p. However, we know $H = D'/D = \psi(D')$ and so

$$\hat{\psi}(H) = (\hat{\psi} \circ \psi)(D') = [p^{n+1}]D' \neq 0$$

as D' is cyclic of order p^{n+2}. Therefore, $H \cap C' = 0$. Therefore, we have

$$\sum_H (((A/D)/H, (C' + H)/H) - (\infty)) = \sum_{D' \supset D} ((A/D', (C' + H)/H) - (\infty))$$

where the sum runs through all cyclic subgroups of order p^{n+2} containing D and $H = D'/D = \psi(D')$.

Let $\psi_{D'} : A \to A/D'$ be the isogeny associated to D' and let $\psi_H : A/D \to A/D'$ be the isogeny associated to $H = D'/D = \psi(D')$, so $\psi_{D'} = \psi_H \circ \psi$. We want to show

$$(C' + H)/H = \ker(\hat{\psi}_{D'})[p] \oplus \psi_{D'}(B).$$

We have that $(C' + H)/H = \psi_H(C' + H)$ is a cyclic group of order N_E, so we can write

$$\psi_H(C' + H) = U \oplus V$$

where $|U| = p$ and $|V| = M$. We then have

$$\hat{\psi}_H(U \oplus V) = (\hat{\psi}_H \circ \psi_H)(C' + H) = [p](C' + H) = [p]\psi(B) = \psi(B).$$

Therefore, we have

$$V = [p]V = [p](U \oplus V) = (\psi_H \circ \hat{\psi}_H)(U \oplus V) = (\psi_H \circ \psi)(B) = \psi_{D'}(B).$$

We then see that

$$\begin{aligned}
\hat{\psi}_{D'}(U \oplus \psi_{D'}(B)) &= (\hat{\psi} \circ \hat{\psi}_H)(U \oplus \psi_{D'}(B)) \\
&= (\hat{\psi} \circ \psi)(B) \\
&= [p^{n+1}]B \\
&= [p^{n+2}]B \\
&= (\hat{\psi}_{D'} \circ \psi_{D'})(B)
\end{aligned}$$

as the order of B is coprime with p. Therefore, we have $U \subset \ker(\hat{\psi}_{D'})$ and so $U = \ker(\hat{\psi}_{D'})[p]$. Hence, we have

$$(C' + H)/H = \ker(\hat{\psi}_{D'})[p] \oplus \psi_{D'}(B)$$

which shows that

$$\sum_{D' \supset D} ((A/D', (C' + H)/H) - (\infty)) = \sum_{D' \supset D} ((y_{A,D'}) - (\infty))$$

and therefore, we have shown

$$T_p((y_{A,D}) - (\infty)) = \sum_{D' \supset D} ((y_{A,D'}) - (\infty))$$

where the sum runs over all cyclic subgroups D' of order p^{n+2} in A containing D. This then leads to the trace relation

$$a_p(E) \cdot Q_{A,D} = \sum_{D' \supset D} Q_{A,D'}.$$

We know that if $J, J' \supset D$ where J and J' are cyclic subgroups of order p^{n+2}, then the points $Q_{A,J}$ and $Q_{A,J'}$ lie in the same Galois orbit with trivial stabiliser. In particular, this ensures that these points are not equal and have the same order. Hence, by induction, if $P_{A,C}$ is of infinite order then so is $Q_{A,D}$. Also, if $P_{A,C}$ is not divisible by p in $E(F_0)$ then $Q_{A,D}$ is not divisible by p in $E(F_n)$.

We are able to obtain the following lemma, which is a generalised version of Lemma 2.3.7.

Lemma 4.2.1. *Fix a cyclic subgroup B in A of order M and let $n \geq 0$. Then $\sum_D Q_{A,D}$ is a torsion point in $E(F)$ where the sum is over all cyclic subgroups D in A of order p^{n+1}.*

Proof. We adapt the proof of [39, Lemma 19] to the general construction. We will do this by induction. For $n = 0$, we have

$$\sum_D Q_{A,D} = \sum_{C \supset B} (-a_p(E) \cdot P_{A,C} + T) = (p+1)T - a_p(E) \sum_{C \supset B} P_{A,C}.$$

By Proposition 4.1.3, we know that the summation on the right hand side is a torsion point in $E(F)$ and so it is true for the $n = 0$ case. We assume the statement is true for n. Then we have

$$\sum_{D'} Q_{A,D'} = a_p(E) \sum_D Q_{A,D}$$

where the first sum runs over all cyclic subgroups D' of order p^{n+2} and the second sum runs over all cyclic subgroups D of order p^{n+1}. Hence this point is torsion by induction. □

If we fix a cyclic subgroup B of order M in A, then we have a G_n-morphism

$$l_n : V_n \to E(F_n) \otimes \mathbb{Q}_p$$

where $e_D \mapsto Q_{A,D}$ and e_D is the characteristic function on D. Here, we have

$$V_n := \ker\left(\mathbb{Q}_p\left[{}^{\mathcal{G}_n}/_{\mathcal{B}_n}\right] \to \mathbb{Q}_p\right) = \left\{f : \mathbb{P}^1_n \to \mathbb{Q}_p : \sum_C f(C) = 0\right\}$$

is a $\mathbb{Q}_p[G_n]$-module of dimension $p^{n+1} + p^n - 1$. If we then assume that $\tau_{F,A,p}$ is surjective, then we have $G_n \cong \mathcal{G}_n$. We thus have the following, a generalised version of Theorem 2.3.8.

Proposition 4.2.2. *Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let p be a prime of multiplicative reduction with respect to E and let $P_{A,C} \in E(F_0)$ be of infinite order. Suppose $\tau_{F,A,p}$ is surjective. Then all higher modular points $Q_{A,D}$ above $P_{A,C}$ are of infinite order and generate a group of $\mathbb{Q}_p$-dimension $p^{n+1} + p^n - 1$ in $E(F_n) \otimes \mathbb{Q}_p$.*

Proof. We adapt the proof of [39, Theorem 20] to the general construction. We will show that l_n is injective by induction. For the $n = 0$ case, we have $V_0 = W_0$ which is an irreducible $\mathbb{Q}_p[\mathcal{G}_n]$-module. Therefore $\ker(l_0) \in \{0, W_0\}$. If $\ker(l_0) = W_0$, then l_0 is the zero map which contradicts the fact that $Q_{A,D}$ is of infinite order in $E(F_0)$.

Let $n \geq 1$ be the smallest value such that l_n is not injective. We have the following decomposition of V_n as a $\mathbb{Q}_p[\mathcal{G}_n]$-module

$$V_n = \bigoplus_{i=0}^{n} W_i$$

where W_i are irreducible $\mathbb{Q}_p[\mathcal{G}_n]$-modules. Then $V_n \cong W_n \oplus V_{n-1}$ as $\mathbb{Q}_p[\mathcal{G}_n]$-modules for $n \geq 1$. Therefore, by induction, l_n restricted to W_n is not injective. However, this means that l_n is trivial on W_n as it is irreducible meaning $\mathrm{im}(l_n) \cong V_{n-1}$ which contradicts the fact that all $Q_{A,D}$ above $P_{A,C}$ have infinite order in $E(F_n)$. □

4.2.2 Good Case

Let p be a prime of good reduction for E. We define $F_n := K_{p^{n+1}N_E}$ where $F := F_{-1}$ is a number field such that $P_{A,C}$ is of infinite order in $E(F)$. Hence, we can view $G_n = \mathrm{Gal}(F_n/F)$ as a subgroup of $\mathcal{G}_n$.

For $n \geq 0$, we let D be a cyclic subgroup in A of order p^{n+1} and let $\psi : A \to A/D$ be the isogeny associated to D. Then we have $y_{A,D} = (A/D, \psi(C)) \in Y_0(N_E)$. We then define the higher modular point above $P_{A,C}$ as

$$Q_{A,D} = \Phi_E(y_{A,D}) \in E(F_n).$$

As before, if we use the Hecke operator T_p, we obtain the trace relation

$$a_p(E) \cdot Q_{A,D} = \sum_{D' \supset D} Q_{A,D'}$$

for all $n \geq 0$ and D as defined before. Here, the sum runs over all cyclic subgroups D' of order p^{n+2} containing D. Hence, we have

$$a_p(E) \cdot P_{A,C} = \sum_{D} Q_{A,D}$$

where the sum runs over all cyclic subgroups of order p. Therefore, as in the multiplicative case, if $J, J' \supset D$ where J and J' are cyclic subgroups of order p^{n+2}, then the points $Q_{A,J}$ and $Q_{A,J'}$ are not equal and have the same order. Therefore, if $P_{A,C}$ is of infinite order in $E(F)$, then $Q_{A,D}$ is of infinite order in $E(F_n)$. Also, if $P_{A,C}$ is not divisible by p in $E(F)$ then $Q_{A,D}$ is not divisible by p in $E(F_n)$.

Therefore, as we have

$$V_{(n)} = \mathbb{Q}_p\left[\mathcal{G}_n/\mathcal{B}_n\right] = \mathrm{Maps}(\mathbb{P}^1_n \to \mathbb{Q}_p),$$

a $\mathbb{Q}_p[G_n]$-module of dimension $p^{n+1} + p^n$, then we can define a G_n-morphism

$$V_{(n)} \to E(F_n) \otimes \mathbb{Q}_p$$

$$e_D \mapsto Q_{A,D}.$$

If we then assume that $\tau_{F,A,p}$ is surjective, then we have $G_n \cong \mathcal{G}_n$. Again, we are able to obtain the following lemma, which is a generalised version of Theorem 2.3.9.

Proposition 4.2.3. *Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let p be a prime of good ordinary reduction of E ensuring*

$a_p(E) \neq 0$ and let $P_{A,C} \in E(F)$ have infinite order. Suppose $\tau_{F,A,p}$ is surjective. Then all higher modular points $Q_{A,D}$ above $P_{A,C}$ are of infinite order and generate a group of $\mathbb{Q}_p$-dimension $p^{n+1} + p^n$ in $E(F_n) \otimes \mathbb{Q}_p$.

Proof. This follows along similar lines as to the proof of Proposition 4.2.2, taking into account that $a_p(E) \neq 0$, so the trace relations aren't trivial. □

Therefore, we have established a link between the higher modular points and the representation theory of $\mathcal{G}_n$.

4.3 Derivatives

We now look at creating derivative classes associated to the higher modular points with the method proposed by Wuthrich in [39] in order to create points of prime power order in certain Selmer groups. To do this, we will use the link created between the higher modular points and representations of $\mathcal{G}_n$ in Proposition 4.2.2 and Proposition 4.2.3 as well as applying Theorem 3.6.20. We will show that under the conditions of the prime p with respect to E as outlined in Proposition 4.1.5, we understand the type of $\mathbb{Z}_p[\mathcal{G}_n]$-lattice the saturated group generated by the higher modular points must be isomorphic to. Further, we can use this to not only show that the order of certain Selmer groups must be divisible by a certain prime power, but also contain an element of that prime power order.

Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductors N_E and N_A respectively. Let p be a prime of good ordinary or multiplicative reduction with respect to E and let

$$F := \begin{cases} K_{N_E} & \text{if } p \nmid N_E, \\ K_{\frac{N_E}{p}} & \text{if } p || N_E. \end{cases}$$

as defined in the notation. We assume that $\tau_{F,A,p}$ is surjective. Hence, if we let F_n be the smallest field extension of F such that $G_n := \mathrm{Gal}(F_n/F)$ acts as scalars on $A[p^{n+1}]$, then we have $G_n \cong \mathcal{G}_n$. We let L_n be the subfield of F_n fixed by $\mathcal{A}_n$. We also remind ourselves of the definition of a prime of good non-anomalous reduction with respect to E as defined in Definition 4.1.4.

Theorem 4.3.1. *Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let $p > 2$ be a prime of multiplicative reduction for A such that $\mathrm{ord}_p(\Delta_A) = 1$ and let F be as defined above. Assume that:*

1. *A does not have potentially good supersingular reduction for any prime of additive reduction,*
2. *E has either split multiplicative reduction at p with $p \nmid \mathrm{ord}_p(\Delta_E)$, non-split multiplicative reduction at p, or good ordinary non-anomalous reduction at p,*
3. *The degree of any isogeny of A defined over $\mathbb{Q}$ is coprime to N_E,*
4. *$\tau_{F,A,p}$ is surjective,*
5. *$\overline{\rho}_{\mathbb{Q},E,p}$ is surjective,*
6. *Any prime ℓ of bad reduction for E and good reduction for A has $a_\ell(A)^2 - 4\ell$ square modulo p where $a_\ell(A)$ is the Hecke eigenvalue of the newform f attached to the isogeny class of A.*

Then there exists an element of order p^n in $\mathrm{Sel}^{p^n}(E/L_n)$.

Remark. *We explain here the restriction imposed by each condition in the theorem. The first point is important in order for all places above these primes to be unramified in the extension F_n/L_n.*

We require the second point so the modular points $P_{A,C}$ are not divisible by p in $E(\mathbb{Q}(C))$ by Proposition 4.1.5. *Here, we remind ourselves that a prime p is non-anomalous for E if E has good reduction at p and p doesn't divide $|\tilde{E}(\mathbb{F}_p)|$.*

The third point is to ensure all the modular points lie in a single orbit under the action of G_{N_E}. This shows that the points $P_{A,C}$ are not equal and are of infinite order in $E(K_{N_E})$ for all C.

The fourth point guarantees that $G_n \cong \mathcal{G}_n$ for all $n \geq 0$. Hence we are able to apply the representation theory of chapter 3 *to the modular points. The fifth point is essential in order to ensure $E(F_n)[p] = 0$ for all $n \geq 0$. We know that this condition excludes only a finite number of primes if E has no complex multiplication by Theorem* 2.2.6.

The final point ensures that the primes dividing N_E but not $p \cdot N_A$ split completely in F_n/L_n. This is fundamental when showing that the image of the derivation map δ_n lies in $Ш(E/L_n)$.

In order to prove this theorem, we need to look at the splitting of primes in the field extension F_n/L_n.

4.3.1 Field Extensions

In this section, we will examine the splitting of primes in the field extension F_n/L_n. The main aim is to prove the following.

Theorem 4.3.2. *Suppose none of the primes of additive reduction for A are potentially good supersingular. Then the extension F_n/L_n is nowhere ramified. Furthermore, all places of above ∞, p and N_A and all places above a prime ℓ dividing N_E but not ∞, p or N_A such that $a_\ell(A)^2 - 4\ell$ is a square modulo p split completely in the extension.*

We will first need the following lemma.

Lemma 4.3.3. *[39, Lemma 26] Let ν be either a place of ordinary reduction above p, an infinite place or a place of potentially multiplicative reduction all with respect to A. Then the image of $\overline{\tau}_{F_\nu,A,p^{n+1}}$ lies in a Borel subgroup of $\mathcal{G}_n$.*

Proof. We first deal the case when ν is a place of ordinary reduction above p. In this case, there exists an exact sequence

$$0 \to M_{p^{n+1}} \to A[p^{n+1}] \to \tilde{A}[p^{n+1}] \to 0$$

where the second mapping is the reduction mapping and $M_{p^{n+1}} \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$. As $M_{p^{n+1}}$ is fixed by G_{F_ν}, then we have that the image is contained in a Borel subgroup.

If ν is a place of split multiplicative reduction for A, then we know that we can describe A as a Tate curve with

$$A[p^{n+1}] \cong \left\langle \zeta_{p^{n+1}}, q_A^{1/p^{n+1}} \right\rangle$$

where $\zeta_{p^{n+1}}$ is a primitive p^{n+1}-th root of unity and $q_A \in F_\nu^\times$. Then the image of $\sigma \in G_{F_\nu}$ takes the form

$$\begin{pmatrix} \chi_{\mathrm{cyc}}(\sigma) & \star \\ 0 & 1 \end{pmatrix}$$

where $\chi_{\mathrm{cyc}} : G_{F_\nu} \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. Hence, the image of G_{F_ν} is contained in a Borel subgroup.

If ν is a place of non-split multiplicative or additive potentially multiplicative reduction, then we know that there exists a quadratic extension, K, of F_ν such that it is unramified in the first case and ramified in the second such that A has split multiplicative reduction over K. If we let $t : G_{F_\nu} \twoheadrightarrow \mathrm{Gal}(K/F_\nu) \xrightarrow{\sim} \{\pm 1\}$ be the associated quadratic character, then

$$\sigma\left(\zeta_{p^{n+1}}^i\right) = \chi_{\mathrm{cyc}}(\sigma) \cdot t(\sigma) \cdot \zeta_{p^{n+1}}^i$$

for all $0 \leq i < p^{n+1}$ and $\sigma \in G_{F_\nu}$. Hence, the image is contained in a Borel subgroup.

If ν is an infinite real place, then there is a cyclic subgroup of order p^{n+1} in $A(\mathbb{R})$ and so the image is contained in a Borel subgroup. □

Therefore, we now need to look at the places of F of bad reduction with respect to E such that they are not above $p \cdot N_A$. Let ν be such a place with norm $\mathrm{Nm}(\nu) = q_\nu$. Let $a_\nu(A)$ be the integer such that

$$a_\nu(A) = q_\nu + 1 - |A_\nu(k)|$$

where A_ν is the reduced elliptic curve at ν and k is the residue field of ν. Let R_ν be the subring of $\mathrm{End}(A_\nu)$ generated by the Frobenius endomorphism Fr_{A_ν}. Then either $\mathrm{Fr}_{A_\nu} \in \mathbb{Z}$ and so $R_\nu = \mathbb{Z}$, or R_ν is an order in an imaginary quadratic field by [16, pg. 556]. We define

$$\Delta_\nu := \mathrm{disc}(R_\nu), \qquad \delta_\nu := 0, 1 \text{ depending on when } \Delta_\nu \equiv 0, 1 \pmod 4,$$

and b_ν such that $\Delta_\nu b_\nu^2 = a_\nu(A)^2 - 4q_\nu$. We have that $b_\nu = 0$ if $R_\nu = \mathbb{Z}$, otherwise b_ν is the index of $\mathbb{Z}[\mathrm{Fr}_{A_\nu}]$ in R_ν by [35, pg. 38]. Therefore, b_ν must be an integer. We then associate to ν the integral matrix

$$M_\nu = \begin{pmatrix} \frac{a_\nu(A)+b_\nu\delta_\nu}{2} & b_\nu \\ \frac{b_\nu(\Delta_\nu-\delta_\nu)}{4} & \frac{a_\nu(A)-b_\nu\delta_\nu}{2} \end{pmatrix}.$$

Theorem 4.3.4. *[16, Theorem 2.1] Let A be an elliptic curve over F. Let ν be a place of F of good reduction for A such that $\nu \nmid p$. Then ν is unramified in $F(A[p^{n+1}])$ and the integral matrix M_ν, when reduced modulo p^{n+1}, represents the class of the Frobenius of ν in* $\mathrm{Gal}(F(A[p^{n+1}])/F)$.

Therefore, the Frobenius element Fr_ν of G_n generates the decomposition group as F_n is a field extension of F contained in $F(A[p^{n+1}])$ by construction of F_n. We want to see when M_ν reduced modulo p^{n+1} lies in a Borel subgroup. To do this, we look at the conjugacy classes of M_ν in $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Definition 4.3.5. *A matrix $X \in \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ is* cyclic *if X is not a scalar matrix modulo any power of p.*

Using this we are able to write each matrix of $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ in a specific form.

Lemma 4.3.6. *[4, Lemma 2.1] Let $X \in \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Then either X is cyclic or can be written in the form $dI_2 + p^j\beta$ for some $1 \leq j \leq n+1$ such that $d \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ and $\beta \in \mathrm{M}_2(\mathbb{Z}/p^{n+1-j}\mathbb{Z})$ is cyclic.*

Hence, we can then find a representative of the conjugacy class each matrix in $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ lies in.

Theorem 4.3.7. *[4, Theorem 2.2] Let $X \in \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ be as in Lemma* 4.3.6. *If X is cyclic, then it is conjugate to*

$$\begin{pmatrix} 0 & 1 \\ -\det(X) & \mathrm{tr}(X) \end{pmatrix},$$

otherwise X is conjugate to

$$\begin{pmatrix} d & p^j \\ -p^j\cdot\det(\beta) & d+p^j\cdot\mathrm{tr}(\beta) \end{pmatrix}.$$

We can use this form on M_ν to prove the following.

Lemma 4.3.8. *If $a_\nu(A)^2 - 4q_\nu$ is a square modulo p then M_ν reduced modulo p^{n+1} lies in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.*

Proof. First assume $(b_\nu, p) = 1$. Then M_ν is a cyclic matrix and we have

$$M_\nu \sim \left(\begin{smallmatrix} 0 & 1 \\ -q_\nu & a_\nu(A) \end{smallmatrix}\right).$$

Any conjugate to this matrix must take the form

$$\tfrac{1}{xt-yz}\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -q_\nu & a_\nu(A) \end{smallmatrix}\right)\left(\begin{smallmatrix} t & -y \\ -z & x \end{smallmatrix}\right)$$

$$= \tfrac{1}{xt-yz}\left(\begin{smallmatrix} -xz-q_\nu yt-a_\nu(A)yz & x^2+a_\nu(A)xy+q_\nu y^2 \\ -z^2-a_\nu(A)tz-q_\nu t^2 & xz+q_\nu yt+a_\nu(A)xt \end{smallmatrix}\right)$$

where $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Hence, for M_ν to be in a Borel subgroup, then we need

$$z^2 + a_\nu(A)tz + q_\nu t^2 \equiv 0 \pmod{p^{n+1}}.$$

As the discriminant of this polynomial is a square modulo p^{n+1} with respect to z, this equation has at least one solution and so M_ν lies in a Borel subgroup.

Let $b_\nu = p^j u$ such that $(u, p) = 1$. If $j \geq n+1$ then M_ν is $\frac{a_\nu(A)}{2} I_2$ and so lies in a Borel subgroup, so suppose $1 \leq j \leq n$. Then, as $\det(M_\nu) = q_\nu$ is not divisible by p, then $a_\nu(A)$ cannot be divisible by p. Hence, we have $\frac{a_\nu(A)}{2} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ for all $n \geq 0$ and so

$$M_\nu = \tfrac{a_\nu(A)}{2} I_2 + p^j \begin{pmatrix} \frac{u\delta_\nu}{2} & u \\ u\left(\frac{\Delta_\nu - \delta_\nu}{4}\right) & -\frac{u\delta_\nu}{2} \end{pmatrix} \sim \begin{pmatrix} \frac{a_\nu(A)}{2} & p^j \\ \frac{p^j u^2 \Delta_\nu}{4} & \frac{a_\nu(A)}{2} \end{pmatrix}.$$

Any conjugate to this matrix must take the form

$$\tfrac{1}{xt-yz}\begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} \frac{a_\nu(A)}{2} & p^j \\ \frac{p^j u^2 \Delta_\nu}{4} & \frac{a_\nu(A)}{2} \end{pmatrix}\begin{pmatrix} t & -y \\ -z & x \end{pmatrix}$$

$$= \tfrac{1}{xt-yz}\begin{pmatrix} \frac{a_\nu(A)}{2}(xt-yz)+p^j\left(\frac{u^2\Delta_\nu}{4}yt-xz\right) & p^j\left(x^2-\frac{u^2\Delta_\nu}{4}y^2\right) \\ -p^j\left(z^2-\frac{u^2\Delta_\nu}{4}t^2\right) & \frac{a_\nu(A)}{2}(xt-yz)-p^j\left(\frac{u^2\Delta_\nu}{4}yt-xz\right) \end{pmatrix}$$

where $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Hence, for M_ν to be in a Borel subgroup, then we need

$$p^j\left(z^2 - \tfrac{u^2\Delta_\nu}{4}t^2\right) \equiv 0 \pmod{p^{n+1}}.$$

Therefore this matrix lies in a Borel subgroup if Δ_ν is a square modulo p. However, as $\Delta_\nu b_\nu^2 = a_\nu(A)^2 - 4q_\nu$, then this is true if $a_\nu(A)^2 - 4q_\nu$ is a square mod p. □

Therefore, we need to find conditions for $a_\nu(A)^2 - 4q_\nu$ to be a square modulo p. Let ℓ be a prime of good reduction with respect to A. Then the arithmetic Frobenius Fr_ℓ has characteristic polynomial $x^2 - a_\ell(A)x + \ell$ with roots α and β. Then we let $t_n := \mathrm{tr}(\mathrm{Fr}_\ell^n)$ for $n \geq 1$ and we have $\ell^n = \det(\mathrm{Fr}_\ell^n)$.

Proposition 4.3.9. *Let $A/\mathbb{Q}$ be an elliptic curve and p a prime. Let ℓ be a prime of good reduction with respect to A such that $\ell \neq p$. Then for all $n \geq 1$*

$$a_\ell(A) - 4\ell \text{ is a square mod } p \text{ if and only if } t_n - 4\ell^n \text{ is a square mod } p.$$

We will first look at the cases where n is odd.

Lemma 4.3.10. *For all $n \geq 0$*

$$t_{2n+1}^2 - 4\ell^{2n+1} = (t_1^2 - 4\ell)\left((1-2n)\ell^n + \sum_{j=1}^{n} \ell^{n-j}t_j^2\right)^2.$$

Proof. Let α and β be as before. Then we have

$$t_{2n+1}^2 - 4\ell^{2n+1} = (\alpha^{2n+1} - \beta^{2n+1})^2.$$

Therefore we have

$$\begin{aligned}
&\alpha^{2n+1} - \beta^{2n+1} \\
&= (\alpha - \beta)\left(\sum_{j=0}^{2n} \alpha^j \beta^{2n-j}\right) \\
&= (\alpha - \beta)\left(\alpha^n \beta^n + \sum_{j=1}^{n} \alpha^{n+j}\beta^{n-j} + \alpha^{n-j}\beta^{n+j}\right) \\
&= (\alpha - \beta)\left((1-2n)\alpha^n\beta^n + \sum_{j=1}^{n}(\alpha^{n+j}\beta^{n-j} + 2\alpha^n\beta^n + \alpha^{n-j}\beta^{n+j})\right) \\
&= (\alpha - \beta)\left((1-2n)\alpha^n\beta^n + \sum_{j=1}^{n}\alpha^{n-j}\beta^{n-j}(\alpha^j + \beta^j)^2\right) \\
&= (\alpha - \beta)\left((1-2n)\ell^n + \sum_{j=1}^{n}\ell^{n-j}t_j^2\right)
\end{aligned}$$

Squaring both sides gives the result. □

We then just need to check the case for n even. We first need the following lemma.

Lemma 4.3.11. *For all $n \geq 1$, we have $t_{2n} = t_n^2 - 2\ell^n$.*

Proof. Let α and β be as above. Then we have

$$t_{2n} = \alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2\alpha^n\beta^n = t_n^2 - 2\ell^n. \qquad \square$$

Using this, we can prove the proposition.

Proof of Proposition 4.3.9. It is true for the case when n is odd by Lemma 4.3.10. If n is even, then we can show by induction and Lemma 4.3.11 that if $n = 2^i m$ with m odd and $i \geq 1$, then

$$t_n^2 - 4\ell^n = (t_m^2 - 4\ell^m)\left(\prod_{j=0}^{i-1} t_{2^j m}\right)^2.$$

It is true for the case $i = 1$ as

$$\begin{aligned} t_{2m}^2 - 4\ell^{2m} &= (t_m^2 - 2\ell^m)^2 - 4\ell^{2m} \\ &= t_m^4 - 4\ell^m t_m^2 \\ &= t_m^2(t_m^2 - 4\ell^m) \end{aligned}$$

by Lemma 4.3.11, so assume it is true for i. Then we have

$$\begin{aligned} t_{2^{i+1}m}^2 - 4\ell^{2^{i+1}m} &= (t_{2^i m}^2 - 2\ell^{2^i m})^2 - 4\ell^{2^{i+1}m} \\ &= t_{2^i m}^4 - 4\ell^{2^i m} t_{2^i m}^2 \\ &= t_{2^i m}^2 (t_{2^i m}^2 - 4\ell^{2^i m}) \\ &= (t_m^2 - 4\ell^m) \left(\prod_{j=0}^{i} t_{2^j m} \right)^2 \end{aligned}$$

by induction. □

We now have the tools to prove Theorem 4.3.2.

Proof of Theorem 4.3.2. As $F_n \subset F(A[p^{n+1}])$, then by Theorem 4.3.4, the extension F_n/F is unramified outside ∞, p and N_A and hence so is F_n/L_n. We see by Lemma 4.3.3 that the decomposition group of a place in F dividing $\infty \cdot p \cdot N_A$ inside G_n is contained in a Borel. Furthermore, by Lemma 4.3.8, the decomposition group of a place ν in F dividing N_E but not p or N_A such that $a_\nu(A)^2 - 4q_\nu$ is a square modulo p inside $\mathcal{G}_n$ is contained in a Borel. Since any Borel intersects trivially with $\mathcal{A}_n$ by Lemma 3.1.1, then these places must split completely in F_n/L_n. We then have our result by Proposition 4.3.9. □

4.3.2 Construction of Derivatives

We are now able to prove Theorem 4.3.1, which requires the construction of derivative classes coming from the higher modular points.

Proof of Theorem 4.3.1. There is an injection

$$l_n : V_n \to E(F_n) \otimes \mathbb{Q}_p$$

$$f \mapsto \sum_D f(D) \cdot Q_{A,D}$$

where $Q_{A,D}$ are the higher modular points. Let

$$S_n = \{P \in E(F_n) : \text{ there exists a } k \geq 0 \text{ such that } p^k P \in \mathbb{Z}_p[G_n] \cdot Q_{A,D}\}$$

be the saturated group generated by the higher modular points in $E(F_n)$. We can show the following.

Lemma 4.3.12. *If $(S_n)_{\text{tors}}$ denotes the torsion subgroup of S_n, then*

$$(S_n)_{\text{tors}} = E(F_n)[p^\infty].$$

We remark that the definition of $E[p^\infty]$ is as defined in the notation.

Proof. If $P \in E(F_n)[p^\infty]$, then there exists a $k \geq 0$ such that

$$p^k P = 0 \in \mathbb{Z}_p[G_n] \cdot Q_{A,D}.$$

Therefore $P \in (S_n)_{\text{tors}}$. On the other hand, let $Q \in (S_n)_{\text{tors}}$. Then there exists an $m \geq 1$ such that $mQ = 0$. We can write $m = p^r s$ for some $r \geq 0$ and $(s, p) = 1$. Also, as $Q \in S_n$, there exists a $k \geq 0$ such that

$$p^k Q \in \mathbb{Z}_p[G_n] \cdot Q_{A,D}.$$

If $k \geq r$, then $s(p^k Q) = 0$ and so $p^k Q$ is a torsion point. However, $\mathbb{Z}_p[G_n] \cdot Q_{A,D}$ contains no non-trivial torsion points, so we must have $p^k Q = 0$ and so $Q \in E(F_n)[p^\infty]$.

Similarly, if $k < r$, then $p^{r-k} s(p^k Q) = 0$ and so $Q \in E(F_n)[p^\infty]$ which gives our result. □

Therefore, there exists a short exact sequence

$$0 \to E(F_n)[p^\infty] \to S_n \to W_n \to 0$$

where W_n can be viewed as the quotient of S_n by its torsion points. Therefore, the representatives of the points in W_n are all the points of infinite order in S_n and so can be identified as a G_n-stable lattice in the image of l_n.

Lemma 4.3.13. *We have $W_n^{\mathcal{A}_n} = 0$ and $S_n^{\mathcal{A}_n} = E(L_n)[p^\infty]$.*

Proof. As W_n can be identified as a G_n-lattice in the image of l_n, then we can view W_n as a $\mathbb{Z}_p[\mathcal{G}_n]$-lattice in V_n and therefore, as seen in the proof of Proposition 3.6.12, we must have $W_n^{\mathcal{A}_n} = 0$. Therefore, using the short exact sequence that precedes this lemma, we have

$$S_n^{\mathcal{A}_n} = (E(F_n)[p^\infty])^{\mathcal{A}_n} = E(L_n)[p^\infty]. \qquad \square$$

We would like to determine the size of $\mathrm{H}^1(\mathcal{A}_n, S_n)$. We will require the following.

Proposition 4.3.14. *If $\overline{\rho}_{\mathbb{Q},E,p}$ and $\tau_{F,A,p}$ are surjective then for all $n \geq 0$, $E(F_n)[p] = 0$.*

Proof. We first look at the $n = 0$ case. As $\overline{\rho}_{\mathbb{Q},E,p}$ is surjective, then the smallest Galois extension, K of $\mathbb{Q}$ such that $E(K)[p] \neq 0$ is $K = \mathbb{Q}(E[p])$. Suppose $E(F_0)[p] \neq 0$. As $F_0/\mathbb{Q}$ is Galois, then we must have $\mathbb{Q}(E[p]) \subseteq F_0$. Therefore we have an inclusion of fields $F \subseteq F(E[p]) \subseteq F_0$. As $F(E[p])/F$ and F_0/F are Galois extensions, then $\mathrm{Gal}(F_0/F(E[p])) \trianglelefteq \mathrm{Gal}(F_0/F) \cong \mathcal{G}_0$ as $\tau_{F,A,p}$ is surjective. Therefore, $\mathrm{Gal}(F_0/F(E[p]))$ must either be trivial, isomorphic to $\mathcal{G}_0$ or isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$.

If $\mathrm{Gal}(F_0/F(E[p]))$ is trivial, then $F(E[p]) = F_0$ and so $\mathrm{Gal}(F(E[p])/F) \cong \mathcal{G}_0$. However, this means that $\mathcal{G}_0$ is isomorphic to a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which cannot happen by [2, Theorem 4.9], as this would imply a group of that size must be isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$.

If $\mathrm{Gal}(F_0/F(E[p])) \cong \mathcal{G}_0$, then $F(E[p]) = F$. As $F/\mathbb{Q}$ is a Galois extension, then $\mathbb{Q}(E[p]) \subseteq F$ and so $\mu_p \subseteq F$ where μ_p are the p-th roots of unity. Therefore, we must have $\mathrm{Gal}(F(A[p])/F) \leq \mathrm{SL}_2(\mathbb{F}_p)$ and so $\mathrm{Gal}(F_0/F) \leq \mathrm{PSL}_2(\mathbb{F}_p)$, which is a contradiction.

Therefore, $\mathrm{Gal}(F_0/F(E[p])) \cong \mathrm{PSL}_2(\mathbb{F}_p)$. Hence, $F(E[p])/F$ must be a quadratic extension such that $\mathrm{Gal}(F(E[p])/F) \cong \mathrm{im}(\chi)$. Here, χ is the only non-trivial 1-dimensional representation over $\mathbb{C}$ admitted by $\mathcal{G}_0$, which is defined as

$$\chi : \mathcal{G}_0 \xrightarrow{\det} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \to \{\pm 1\}$$

with kernel $\mathrm{PSL}_2(\mathbb{F}_p)$. However, we know $\mathrm{Gal}(F(E[p])/F)$ is isomorphic to a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and therefore, by [2, Theorem 4.9], we must have

$$\mathrm{Gal}(F(E[p])/F) \cong \{\pm I_2\},$$

which is a contradiction. Therefore, $E(F_0)[p] = 0$.

For the $n \geq 1$ case, we let $H_n = \mathrm{Gal}(F_n/F_0)$ and $M_n = E(F_n)[p]$. Then we know H_n acts on M_n and we have already shown $M_n^{H_n} = 0$. However, as H_n is a p-group and all H_n-orbits have size greater than 1 except the orbit representing the trivial element, then $|M_n| \equiv 1 \pmod{p}$. Therefore, as M_n either has size divisible by p or is trivial, then we must have $M_n = 0$ and therefore, $E(F_n)[p] = 0$. □

As $E(F_n)[p] = 0$, then $E(F_n)[p^\infty] = 0$ and therefore, we have

$$S_n \cong W_n.$$

In particular, $\mathrm{H}^1(\mathcal{A}_n, S_n)$ contains p^n elements by Proposition 3.6.12. If we consider the natural inclusion of S_n in $E(F_n) \otimes \mathbb{Z}_p$, then the cokernel Y_n is a free $\mathbb{Z}_p$-module and we obtain a long exact sequence

$$0 \to E(L_n) \otimes \mathbb{Z}_p \to \mathrm{Y}_n^{\mathcal{A}_n} \to \mathrm{H}^1(\mathcal{A}_n, S_n) \to \mathrm{H}^1(\mathcal{A}_n, E(F_n))[p^\infty] \tag{3}$$

as $S_n^{\mathcal{A}_n} = 0$ by Lemma 4.3.13. Here, $\mathrm{Y}_n^{\mathcal{A}_n}$ has the same rank as $E(L_n) \otimes \mathbb{Z}_p$. If we compose the last map with the inflation map we obtain

$$\delta_n : \mathrm{H}^1(\mathcal{A}_n, S_n) \to \mathrm{H}^1(\mathcal{A}_n, E(F_n))[p^\infty] \hookrightarrow \mathrm{H}^1(L_n, E)[p^\infty]$$

known as the derivation map. We have the short exact sequence

$$0 \to S_n \xrightarrow{[p^n]} S_n \to {}^{S_n}/_{p^n S_n} \to 0$$

which induces

$$0 \to \left({}^{S_n}/_{p^n S_n}\right)^{\mathcal{A}_n} \to \mathrm{H}^1(\mathcal{A}_n, S_n) \xrightarrow{[p^n]} \mathrm{H}^1(\mathcal{A}_n, S_n)$$

as $S_n^{\mathcal{A}_n} = 0$. As $|\mathrm{H}^1(\mathcal{A}_n, S_n)| = p^n$ by Proposition 3.6.12, then the final mapping is the zero mapping. Hence, we have

$$\left({}^{S_n}/_{p^n S_n}\right)^{\mathcal{A}_n} \cong \mathrm{H}^1(\mathcal{A}_n, S_n).$$

We thus call the image of δ_n the derived classes of higher modular points.

Lemma 4.3.15. *The image of δ_n is contained in $Ш(E/L_n)[p^\infty]$.*

Proof. We adapt the proof of [39, Lemma 30] to the general construction. Let η be a lift of an element in the image of δ_n in the map

$$\mathrm{H}^1(L_n, E[p^m]) \to \mathrm{H}^1(L_n, E)[p^m]$$

for a sufficiently large m. Let $\Sigma := \{\nu \text{ place in } L_n : \nu \mid N_E \cdot p \cdot \infty\}$. We will look at the two cases for a place ν of L_n, when $\nu \notin \Sigma$ and $\nu \in \Sigma$.

Firstly, if $\nu \notin \Sigma$, then the extension F_n/L_n is unramified by Theorem 4.3.2. Therefore, the restriction of η to $\mathrm{H}^1((L_n)_\nu, E[p^m])$ will lie in

$$\mathrm{H}^1_f((L_n)_\nu, E[p^m]) := \mathrm{im}\left(E((L_n)_\nu)/p^m E((L_n)_\nu) \to \mathrm{H}^1((L_n)_\nu, E[p^m])\right)$$

as seen in [12, pg. 115].

If $\nu \in \Sigma$, then ν must satisfy one of the following:

- $\nu \mid \infty \cdot p$,
- $\nu \mid N_E$ and $\nu \mid \infty \cdot N_A$,
- $\nu \mid N_E$ but $\nu \nmid \infty \cdot N_A$,

as p is a prime of multiplicative reduction with respect to A. Then by Theorem 4.3.2, ν splits completely in F_n/L_n for all options. Therefore, for all $\nu \in \mathbf{\Sigma}$, ν splits completely in F_n/L_n. We have the commutative diagram

$$\begin{array}{ccccc} \mathrm{H}^1(\mathcal{A}_n, S_n) & \longrightarrow & \mathrm{H}^1(F_n/L_n, E(F_n))[p^\infty] & \xrightarrow{\inf} & \mathrm{H}^1(L_n, E)[p^\infty] \\ & & \downarrow{\scriptstyle \mathrm{res}_{w/\nu}} & & \downarrow{\scriptstyle \mathrm{res}_\nu} \\ & & \mathrm{H}^1((F_n)_w/(L_n)_\nu, E((F_n)_w))[p^\infty] & \xrightarrow{\inf_{w/\nu}} & \mathrm{H}^1((L_n)_\nu, E)[p^\infty]. \end{array}$$

where w is a place of F_n above ν and $\mathrm{im}(\delta_n) \subseteq \mathrm{im}(\inf)$. As ν splits completely in the extension F_n/L_n, then $(F_n)_w = (L_n)_\nu$ and so $\mathrm{res}_{w/\nu}(c)$ is trivial for any $c \in \mathrm{H}^1(F_n/L_n, E(F_n))[p^\infty]$. Therefore

$$(\mathrm{res}_\nu \circ \inf)(c) = (\inf_{w/\nu} \circ \mathrm{res}_{w/\nu})(c) = 0$$

and so the restriction of any element in the image of inf is trivial. Therefore, as η is a lift of any element in the image of δ_n, which is contained in the image of inf, then the restriction of η to $\mathrm{H}^1((L_n)_\nu, E)[p^m]$ is trivial. Hence, η belongs to $\mathrm{Sel}^{p^m}(E/L_n)$. □

We therefore have the map

$$\delta_n : \mathrm{H}^1(\mathcal{A}_n, S_n) \to Ш(E/L_n)[p^\infty].$$

We now want to determine the source of this mapping. With the conditions that we have on the higher modular points, we have the following.

Proposition 4.3.16. *For all $n \geq 0$, we have $S_n^{\mathcal{B}_n} = T_n^{\mathcal{B}_n}$.*

Proof. We show this by induction. For the $n = 0$ case, we have $T_0^{\mathcal{B}_0} \cong \mathbb{Z}_p$, generated by a fixed higher modular point Q_{A,D_0}. As Q_{A,D_0} is not divisible by p in $E(F_0)$, then $S_0^{\mathcal{B}_0} = T_0^{\mathcal{B}_0}$.

Now suppose $n \geq 1$. Let $P \in S_n^{\mathcal{B}_n}$ and $k \geq 0$ be minimal such that $p^k \cdot P \in T_n^{\mathcal{B}_n}$. Assume that $k > 0$. We can show that $T_n^{\mathcal{B}_n}$ is generated by the higher modular points $\{Q_{A,D_0}, ..., Q_{A,D_n}\}$ such that D_i is a cyclic group of order p^{i+1} and

$\mathrm{Nm}(Q_{A,D_i}) = a_p(E) \cdot Q_{A,D_{i-1}}$ for all $1 \leq i \leq n$, where Nm denotes the norm map from $F_i^{\mathcal{B}_i}$ to $F_{i-1}^{\mathcal{B}_{i-1}}$. In particular,

$$T_n^{\mathcal{B}_n} \Big/ T_{n-1}^{\mathcal{B}_{n-1}} = \langle \overline{Q}_{A,D_n} \rangle \cong \mathbb{Z}_p.$$

Therefore, we have $p^k \cdot P = b \cdot Q_{A,D_n} + R$ for some $b \in \mathbb{Z}_p$ and $R \in T_{n-1}^{\mathcal{B}_{n-1}}$. We then apply Nm from $F_n^{\mathcal{B}_n}$ to $F_{n-1}^{\mathcal{B}_{n-1}}$ to obtain $\mathrm{Nm}(Q_{A,D_n}) = a_p(E) \cdot Q_{A,D_{n-1}}$ and $\mathrm{Nm}(R) = pR$. Therefore, we have

$$p^k \cdot \mathrm{Nm}(P) = b a_p(E) \cdot Q_{A,D_{n-1}} + pR \in T_{n-1}^{\mathcal{B}_{n-1}}$$

and $\mathrm{Nm}(P) \in S_{n-1}^{\mathcal{B}_{n-1}} = T_{n-1}^{\mathcal{B}_{n-1}}$ by induction. As $Q_{A,D_{n-1}}$ is not divisible by p in $E(F_{n-1})$, then $b a_p(E)$ is divisible by p. However, as the reduction type of p with respect to E is either multiplicative or good ordinary, then $p \nmid a_p(E)$ and so $p \mid b$. Therefore,

$$R = p\Big(p^{k-1} \cdot P - \tfrac{b}{p} \cdot Q_{A,D_n}\Big) \in p \cdot E\Big(F_n^{\mathcal{B}_n}\Big).$$

We have seen that $E(F_n)[p] = 0$, so R must already be divisible by p in $E\Big(F_{n-1}^{\mathcal{B}_{n-1}}\Big)$ and so $R = pR'$ for some $R' \in E\Big(F_{n-1}^{\mathcal{B}_{n-1}}\Big)$. In particular, we have $R' \in S_{n-1}^{\mathcal{B}_{n-1}} = T_{n-1}^{\mathcal{B}_{n-1}}$. Therefore, as $p^k \cdot P = b \cdot Q_{A,D_n} + R$, then

$$p^{k-1} \cdot P = \tfrac{b}{p} \cdot Q_{A,D_n} + R' \in T_n^{\mathcal{B}_n}$$

which contradicts the minimality of k. Therefore, $k = 0$ and $P \in T_n^{\mathcal{B}_n}$. □

As S_n is isomorphic to a $\mathbb{Z}_p[\mathcal{G}_n]$-sublattice in V_n, then by Proposition 4.3.16 and Theorem 3.6.20, we have $S_n \cong T_n$. Therefore, as $\mathrm{H}^1(\mathcal{A}_n, T_n) \cong \mathbb{Z}/p^n\mathbb{Z}$ by Lemma 3.6.10, then the source of δ_n is a cyclic group of order p^n.

We thus have two outcomes. Firstly, if δ_n is not injective, then as we have the short exact sequence

$$0 \to E(L_n) \otimes \mathbb{Z}_p \to \Upsilon_n^{\mathcal{A}_n} \xrightarrow{\gamma} \ker(\delta_n) \to 0$$

induced from (3), then let $P \in E(F_n) \otimes \mathbb{Z}_p$ such that $\gamma(\overline{P}) = s$ where s generates $\ker(\delta_n)$. If P were a torsion point, say $mP = 0$ for some $m \geq 1$, then as $E(F_n)[p] = 0$, we must have $(m, p) = 1$. Therefore, P is trivial in

$E(F_n) \otimes \mathbb{Z}_p$ and so $\overline{P} = 0$ in $\text{Y}_n^{\mathcal{A}_n}$, which cannot happen. Therefore, the rank of $\text{Y}_n^{\mathcal{A}_n}$ must be positive and so must the rank of $E(L_n) \otimes \mathbb{Z}_p$. Hence, $E(L_n)$ will contribute a copy of $\mathbb{Z}/p^n\mathbb{Z}$ in $\text{Sel}^{p^n}(E/L_n)$ as $E(L_n)[p^n] = 0$.

If δ_n is injective, then $Ш(E/L_n)[p^\infty]$ must contain a cyclic subgroup of order p^n. Therefore, $\text{Sel}^{p^n}(E/L_n)$ must contain an element of order p^n by lifting the image of δ_n from $Ш(E/L_n)[p^n]$. □

We can look further at Theorem 4.3.1 by taking semistable $A/\mathbb{Q}$ and letting $p > 3$ be a prime such that $\overline{\rho}_{\mathbb{Q},A,p}$ is surjective. We will require the following.

Proposition 4.3.17. *Let $A/\mathbb{Q}$ be semistable and $p > 3$ be a prime such that $\overline{\rho}_{\mathbb{Q},A,p}$ is surjective. Then $\tau_{F,A,p}$ is surjective.*

Proof. If $\overline{\rho}_{F,A,p}$ is surjective, then as A is semistable, $\rho_{F,A,p}$ must be surjective and hence $\tau_{F,A,p}$ is also. Therefore, we need to show that for all primes $p > 3$, $\overline{\rho}_{F,A,p}$ is surjective.

We initially look at the case when p is a prime of split multiplicative reduction with respect to A. We have seen by construction that $F \subseteq \mathbb{Q}(A[M])$ where

$$M = \begin{cases} N_E & \text{if } p \nmid N_E, \\ \frac{N_E}{p} & \text{if } p || N_E, \end{cases}$$

so $(M, p) = 1$. Let $K = \mathbb{Q}(A[p]) \cap \mathbb{Q}(A[M])$ and ν be a place of K above p. Then

$$\begin{aligned} K_\nu &\cong \mathbb{Q}_p(A[p]) \cap \mathbb{Q}_p(A[M]) \\ &= \mathbb{Q}_p(\mu[p], \sqrt[p]{q_A}) \cap \mathbb{Q}_p(\mu[M], \sqrt[M]{q_A}) \end{aligned}$$

as p is a prime of split multiplicative reduction. Here, $\mu[n]$ denotes the group of n^{th} roots of unity and $q_A \in \mathbb{Q}_p^\times$ is a p-adic analytic uniformiser at ∞ such that $\text{ord}_p(q_A) = -\text{ord}_p(j(A)) > 0$. We want to show $K_\nu = \mathbb{Q}_p$. As $(M, p) = 1$, then $\mathbb{Q}_p(\mu[p]) \cap \mathbb{Q}_p(\mu[M]) = \mathbb{Q}_p$. Therefore,

$$\text{Gal}(\mathbb{Q}_p(\mu[pM])/\mathbb{Q}_p) \cong G \leq (\mathbb{Z}/M\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times.$$

Let $L = \mathbb{Q}_p(\mu[pM])$. Then, by Kummer theory, we have that $\mathrm{Gal}(L(\sqrt[p]{q_A})/L)$ is a subgroup of $\mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(L(\sqrt[M]{q_A})/L)$ is a subgroup of $\mathbb{Z}/M\mathbb{Z}$. As $(M,p) = 1$, then we must have $L(\sqrt[p]{q_A}) \cap L(\sqrt[M]{q_A}) = L$ and so the Galois group of $L(\sqrt[pM]{q_A}) = L(\sqrt[p]{q_A}, \sqrt[M]{q_A})$ over L is the direct product of these Galois groups. Also

$$L \cap \mathbb{Q}_p(\mu[M], \sqrt[M]{q_A}) = \mathbb{Q}_p(\mu[M])$$

and

$$L \cap \mathbb{Q}_p(\mu[p], \sqrt[p]{q_A}) = \mathbb{Q}_p(\mu[p]).$$

Therefore, looking at the Galois groups, we have

$$\mathrm{Gal}(L(\sqrt[pM]{q_A})/\mathbb{Q}_p(\mu[p], \sqrt[p]{q_A})) \cong \mathrm{Gal}(\mathbb{Q}_p(\mu[M], \sqrt[M]{q_A})/\mathbb{Q}_p).$$

As $L(\sqrt[pM]{q_A})$ is the compositum of $\mathbb{Q}_p(\mu[M], \sqrt[M]{q_A})$ and $\mathbb{Q}_p(\mu[p], \sqrt[p]{q_A})$, then this implies

$$\mathbb{Q}_p(\mu[p], \sqrt[p]{q_A}) \cap \mathbb{Q}_p(\mu[M], \sqrt[M]{q_A}) = \mathbb{Q}_p.$$

Therefore, $K_\nu = \mathbb{Q}_p$. Now, let $H = \mathrm{Gal}(\mathbb{Q}(A[p])/K)$. Then as $K_\nu = \mathbb{Q}_p$, the inertia group, I_ν of H must contain the set of matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ under the image of $\overline{\rho}_{\mathbb{Q},A,p}$ by [33, pg. 277, Corollaire]. As $K/\mathbb{Q}$ is Galois, then $H \trianglelefteq \mathrm{GL}_2(\mathbb{F}_p)$ and so as $p \geq 5$, then either $H \supseteq \mathrm{SL}_2(\mathbb{F}_p)$ or $H \subseteq Z_p$ by [2, Theorem 4.9]. Therefore, as I_ν contains the set of matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then $H \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. But then the mapping $\det : H \to \mathbb{F}_p^\times$ is surjective and has kernel $\mathrm{SL}_2(\mathbb{F}_p)$ meaning $H = \mathrm{GL}_2(\mathbb{F}_p)$. Therefore, we have $\mathbb{Q}(A[p]) \cap \mathbb{Q}(A[M]) = \mathbb{Q}$. However, as $F \subseteq \mathbb{Q}(A[M])$, then $\mathbb{Q}(A[p]) \cap F = \mathbb{Q}$ and as $\overline{\rho}_{\mathbb{Q},A,p}$ is surjective, then so is $\overline{\rho}_{F,A,p}$.

Now suppose p is a prime of non-split multiplicative reduction for A. Let $K = \mathbb{Q}(A[p]) \cap \mathbb{Q}(A[M])$ and let ν be a place of K above p. As p is a prime of non-split multiplicative reduction for A, there exists an unramified quadratic extension $L'/\mathbb{Q}_p$ such that A acquires split multiplicative reduction over L'. In particular, we can follow the same procedure as in the split case with L' to show that $L'(A[p]) \cap L'(A[M]) = L'$. This now ensures that $K_\nu \in \{\mathbb{Q}_p, L'\}$ and so $K_\nu/\mathbb{Q}_p$ is an unramified extension. Therefore, if $H = \mathrm{Gal}(\mathbb{Q}(A[p])/K)$, then the image of the inertia subgroup, I_ν of H under $\overline{\rho}_{\mathbb{Q},A,p}$ must contain the set of matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ by [33, pg. 277, Corollaire]. Therefore, we again see that as $H \trianglelefteq \mathrm{GL}_2(\mathbb{F}_p)$, then $H = \mathrm{GL}_2(\mathbb{F}_p)$ and so $\mathbb{Q}(A[p]) \cap \mathbb{Q}(A[M]) = \mathbb{Q}$.

Therefore, identically to the split case, this means that $\overline{\rho}_{F,A,p}$ is surjective and this completes the proof. □

Therefore, we can reduce Theorem 4.3.1 to the following.

Theorem 4.3.18. *Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor N_E and N_A respectively. Let $p > 3$ be a prime of multiplicative reduction for A such that $\mathrm{ord}_p(\Delta_A) = 1$ and let*

$$F := \begin{cases} K_{N_E} & \text{if } p \nmid N_E, \\ K_{\frac{N_E}{p}} & \text{if } p || N_E. \end{cases}$$

Assume that:

1. *A is semistable,*
2. *E has either split multiplicative reduction at p with $p \nmid \mathrm{ord}_p(\Delta_E)$, non-split multiplicative reduction at p, or good ordinary non-anomalous reduction at p,*
3. *The degree of any isogeny of A defined over $\mathbb{Q}$ is coprime to N_E,*
4. *$\overline{\rho}_{\mathbb{Q},A,p}$ is surjective,*
5. *$\overline{\rho}_{\mathbb{Q},E,p}$ is surjective,*
6. *Any prime ℓ of bad reduction for E and good reduction for A has $a_\ell(A)^2 - 4\ell$ square modulo p where $a_\ell(A)$ is the Hecke eigenvalue of the newform f attached to the isogeny class of A.*

Then there exists an element of order p^n in $\mathrm{Sel}^{p^n}(E/L_n)$.

In particular, if we have a look at Theorem 2.3.10 then we have extended the theorem to state that if further p satisfies certain conditions with respect to E, then we have an element of order p^n in $\mathrm{Sel}^{p^n}(E/L_n)$.

4.4 Examples

We now look at applying Theorem 4.3.18 to a few examples. For information on specific elliptic curves, we obtained our data from the LMFDB [36].

Example. *Let*

$$E : y^2 + y = x^3 - x^2 - x - 2$$

be the elliptic curve with Cremona label 143*a*1 *and*

$$A : y^2 + y = x^3 + x^2 - x$$

be the elliptic curve with Cremona label 35*a*3*. Then if we let* $p = 7$*, this is a prime of good ordinary non-anomalous reduction for* E*. As* $\Delta_A = -35$*, then* 7 *is a prime of multiplicative reduction for* A *such that* $\mathrm{ord}_7(\Delta_A) = 1$*. The only* $\mathbb{Q}$*-isogenies on* A *are of degree* 3 *or* 9*, which are coprime to* N_E *and both* $\overline{\rho}_{\mathbb{Q},A,7}$ *and* $\overline{\rho}_{\mathbb{Q},E,7}$ *are surjective. Also,*

$$\begin{aligned} a_{11}(A)^2 - 4 \cdot 11 &= -35 \equiv 0 \pmod 7 \\ a_{13}(A)^2 - 4 \cdot 13 &= -27 \equiv 1 \pmod 7 \end{aligned}$$

which are both squares modulo 7*. Therefore by Theorem* 4.3.18*, there exists an element of order* 7^n *in* $\mathrm{Sel}^{7^n}(E/L_n)$ *for all* $n \geq 1$*.*

We also see that E doesn't necessarily have to be a semistable elliptic curve.

Example. *Let*

$$E : y^2 + xy = x^3 - x^2 - 5$$

be the elliptic curve with Cremona label 45*a*1 *and*

$$A : y^2 + xy + y = x^3 + x^2$$

be the elliptic curve with Cremona label 15*a*8*. Then if we let* $p = 5$*, then this is a prime of non-split multiplicative reduction for* E *and a prime of multiplicative reduction for* A *such that* $\mathrm{ord}_5(\Delta_A) = 1$*. The only* $\mathbb{Q}$*-isogenies on* A *are of degree* 2*,* 4*,* 8 *or* 16*, which are coprime to* N_E *and both* $\overline{\rho}_{\mathbb{Q},A,5}$ *and* $\overline{\rho}_{\mathbb{Q},E,5}$ *are surjective. Therefore by Theorem* 4.3.18*, there exists an element of order* 5^n *in* $\mathrm{Sel}^{5^n}(E/L_n)$ *for all* $n \geq 1$*.*

We can even vary the curves E and A if they both have prime conductor. However, we first require the following.

Proposition 4.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p. Then there exists an elliptic curve, $A/\mathbb{Q}$, in its isogeny class such that* $\mathrm{ord}_p(\Delta_A) = 1$.

Proof. Let E_0 be the strong Weil curve in the isogeny class of E. Then by [13, Proposition 2], there are three cases. Either

- $\#E_0(\mathbb{Q}) = 1$,
- $\#E_0(\mathbb{Q}) = 2$,
- $\#E_0(\mathbb{Q}) > 2$.

For the first case, $E = E_0$ and as p is a prime of multiplicative reduction for E, then $\mathrm{ord}_p(\Delta_E) = c_p = 1$ by [13, Proposition 2], where c_p is the Tamagawa number of E. For the second case, p is of the form $u^2 + 64$ for some integer $u \equiv 3 \pmod 4$ by [13, Proposition 2]. The elliptic curve E is one of the following two isogenous curves

$$E_0 : y^2 + xy = x^3 - \frac{u+1}{4}x^2 + 4x - u$$
$$E_1 : y^2 + xy = x^3 - \frac{u+1}{4}x^2 - x$$

where $\Delta_{E_1} = p$. Finally, if $\#E_0(\mathbb{Q}) > 2$, then the conductor of E_0 will be either $11, 17, 19$ or 37. But then E_0 and hence E will be isogenous to one of the curves with Cremona label $11a2$, $17a3$, $19a3$ or $37b2$, which all have p strictly dividing their discriminant. □

Example. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor p and let $A/\mathbb{Q}$ be an elliptic curve of conductor p such that* $\mathrm{ord}_p(\Delta_A) = 1$, *which exists by Proposition* 4.4.1. *We see in [13, Proposition 2] that if p is a prime of split multiplicative reduction for E then $p \nmid \mathrm{ord}_p(\Delta_E)$ and $\overline{\rho}_{\mathbb{Q},E,p}$ is surjective for all p. We also have that $\overline{\rho}_{\mathbb{Q},A,p}$ is surjective as $p \geq 11$. In particular, A has no p-isogeny defined over $\mathbb{Q}$. Hence, by Theorem* 4.3.18, $\mathrm{Sel}^{p^n}(E/L_n)$ *contains an element of order p^n for all p prime and $n \geq 1$.*

We also show a specific example for E with conductor q when there exists an A of conductor pq for p, q prime such that $p \neq q$.

Example. *Let $a, b \in \mathbb{Z}$ such that at least one of a or b is not divisible by 3 and*

$$a^{12} - 9a^8b + 27a^4b^2 - 27b^3$$

is not a square. Then by [21, Theorem 3.10] there exists infinitely many $m \in \mathbb{Z}$ such that

$$A_m : y^2 + y = x^3 + ax^2 + bx + m$$

is an elliptic curve where $|\Delta_{A_m}| = pq$. Here, p is an odd prime and q is either 1 or an odd prime different from p. Pick m such that $p, q \geq 11$ and there exists an elliptic curve $E/\mathbb{Q}$ of conductor q such that p is a prime of good ordinary non-anomalous reduction. Then as A_m is semistable, $\overline{\rho}_{\mathbb{Q},A_m,p}$ and $\overline{\rho}_{\mathbb{Q},A_m,q}$ are surjective, which ensures that there doesn't exist a $\mathbb{Q}$-isogeny of A_m of degree q. In particular, p is a prime of multiplicative reduction such that $\mathrm{ord}_p(\Delta_{A_m}) = 1$. Also, $\overline{\rho}_{\mathbb{Q},E,p}$ is surjective as $p \geq 11$. Therefore, by Theorem 4.3.18, $\mathrm{Sel}^{p^n}(E/L_n)$ contains an element of order p^n for all $n \geq 1$.

Bibliography

[1] K. Ardakov and K. A. Brown. Ring-theoretic properties of Iwasawa algebras: a survey. *Doc. Math.*, (Extra Vol.):7–33, 2006.

[2] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[3] A. O. L. Atkin and J. W. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.

[4] N. Avni, U. Onn, A. Prasad, and L. Vaserstein. Similarity classes of 3×3 matrices over a local principal ideal ring. *Comm. Algebra*, 37(8):2601–2615, 2009.

[5] B. Baran. Normalizers of non-split cartan subgroups, modular curves, and the class number one problem. *Journal of Number Theory*, 130(12):2753 – 2772, 2010.

[6] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991. Basic representation theory of finite groups and associative algebras.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] A. Brumer. Pseudocompact algebras, profinite groups and class formations. *Journal of Algebra*, 4(3):442 – 470, 1966.

[9] L. Carlitz. The Staudt-Clausen theorem. *Mathematics Magazine*, 34(3):131–146, 1961.

[10] H. Cartan and S. Eilenberg. *Homological algebra*, volume 41. Princeton University Press, 1999.

[11] L. Clozel. Globally analytic p-adic representations of the pro-p-Iwahori subgroup of $GL(2)$ and base change, I: Iwasawa algebras and a base change map. *Bull. Iranian Math. Soc.*, 43(4):55–76, 2017.

[12] H. Darmon, B. Sturmfels, C. B. of the Mathematical Sciences, F. Conference on Modular Elliptic Curves. 2001, Orlando, and N. S. F. (U.S.). *Rational Points on Modular Elliptic Curves*. Regional conference series in mathematics. American Mathematical Society, 2004.

[13] C. Delaunay and C. Wuthrich. Self-points on elliptic curves of prime conductor. *Int. J. Number Theory*, 5(5):911–932, 2009.

[14] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer New York, 2006.

[15] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.

[16] W. Duke and A. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565 (2003), 2002.

[17] M. Greenberg and J. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 2013.

[18] R. Greenberg. Iwasawa theory, projective modules, and modular representations. *Mem. Amer. Math. Soc.*, 211(992):vi+185, 2011.

[19] B. H. Gross. *Kolyvagin's work for modular elliptic curves*, page 235–256. London Mathematical Society Lecture Note Series. Cambridge University Press, 1991.

[20] M. Harris. Systematic growth of mordell-weil groups of abelian varieties in towers of number fields. *Inventiones mathematicae*, 51:123–142, 1979.

[21] S. Howe and K. Joshi. Asymptotics of conductors of elliptic curves over $\mathbb{Q}$. preprint: see `https://arxiv.org/abs/1201.4566v2`, 2012.

[22] G. Karpilovsky. *Induced Modules over Group Algebras*. ISSN. Elsevier Science, 1990.

[23] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[24] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[25] S. Mac Lane. *Homology*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the 1975 edition.

[26] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[27] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.

[28] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[29] N. J. Newsome, M. Nogin, and A. H. Sabuwala. Congruences of power sums. 2017.

[30] K. Rubin. *Euler Systems*. Annals of mathematics studies. Princeton University Press, 2000.

[31] T. Saitō. *Fermat's last theorem : basic tools / Takeshi Saito ; translated from the Japanese by Masato Kuwata.* Translations of mathematical monographs ; v. 243. American Mathematical Society, Providence, R.I., english language ed. edition, 2013.

[32] P. Schneider. *p-adic Lie groups*, volume 344 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2011.

[33] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[34] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[35] A. V. Sutherland. Computing images of galois representations attached to elliptic curves. *Forum of Mathematics, Sigma*, 4, 2016.

[36] The LMFDB Collaboration. The L-functions and Modular Forms Database. `http://www.lmfdb.org`, 2019. [Online; accessed 14 October 2019].

[37] P. Webb. *A Course in Finite Group Representation Theory.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2016.

[38] C. A. Weibel. *An introduction to homological algebra / Charles A. Weibel.* Cambridge studies in advanced mathematics ; 38. Cambridge University Press, Cambridge, 1994.

[39] C. Wuthrich. Self-points on elliptic curves. *Algebra Number Theory*, 3(3):283–315, 2009.