

Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

April 11, 2024

Contents

1	Norm relations	4
1.1	Rational characters and permutation representations	4
1.2	The Burnside ring and relations for permutation representations	5
1.3	Functions on the Burnside ring and norm relations	7
1.3.1	D-local functions	9
2	Elliptic Curves	11
2.1	Elliptic Curves over Local Fields and Reduction Types	12
2.2	Tamagawa Numbers	13
2.3	Elliptic Curves over Global Fields	14
3	Representations, L-functions and Artin Twists	15
3.1	Artin Representations and ℓ -adic Representations	15
3.2	Local Polynomials and L-functions	16
3.3	The Tate Module of an Elliptic Curve and their L-function	17
3.4	Artin Twists of L-functions of Elliptic Curves	19
4	Birch and Swinnerton-Dyer and Other Conjectures	20
4.1	BSD and the Arithmetic Terms	20
4.2	A BSD Analogue for Artin Twists	22
5	Predicting Positive Rank	24
5.1	Examples	25
6	Consistency cases with BSD	28
6.1	Cyclic Extensions	28
6.2	Norm relations in odd order extensions	34
A	Algebraic number theory background	39
A.1	Class field theory and genus fields	39

Introduction

In this report we study a method proposed in [DEW21] for forcing points of infinite order on elliptic curves over finite extensions F/\mathbb{Q} .

Notation

Let G be a finite group. We use the following notation for characters:

$R(G)$	the representation ring of G (Definition 1.1),
$B(G)$	the Burnside ring of G (Definition 1.7),
$R_{\mathbb{Q}}(G)$	the rational representation ring of G ,
$\text{Perm}(G)$	the ring of virtual permutations of G ,
$\text{Char}_{\mathbb{Q}}(G)$	the ring of rationally-valued characters of G ,
$\text{Irr}(G)$	the set of characters of complex irreducible representations of G ,
$\mathbb{Q}(\rho)$	the field of character values of a complex character ρ of G ,
$\hat{C}(G)$	the finite abelian group $\text{Char}_{\mathbb{Q}}(G)/\text{Perm}(G)$,
$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$	$= \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\sigma}$, where $\rho \in R(G)$ (Definition 1.2),
H^x	$= xHx^{-1}$ for $H \leq G$ a subgroup of a group G and $x \in G$,
p^*	defined for an odd prime p . If $p \equiv 1 \pmod{4}$, $p^* = p$. If $p \equiv 3 \pmod{4}$, $p^* = -p$

1 Norm relations

improve this spiel

As observed in the introduction, it can be useful to apply the theory of representations of finite groups to the study of elliptic curves over finite Galois extensions. This section introduces some representation-theoretic concepts that we will apply in later sections.

Given a Galois finite extension F/\mathbb{Q} with $G = \text{Gal}(F/\mathbb{Q})$, one may be interested in functions defined on subfields of F/\mathbb{Q} , equivalently on subgroups of G . Since subgroups up to conjugacy correspond to subfields up to isomorphism, many functions one may consider are constant on conjugacy classes of subgroups.

In the first part, we recall some rational representation theory. Then we define the Burnside ring...

In the third part we introduce... as well as D -local functions, borrowing definitions that appear in [DD09, Section 2.iii].

1.1 Rational characters and permutation representations

Let G be a finite group, K a field of characteristic zero. Recall that a **representation** of G over K is a group homomorphism $\rho: G \rightarrow \text{GL}(V)$ where V is a K -vector space. Associated to a representation ρ is a **character** $\chi: G \rightarrow K^\times$, defined by letting $\chi(g) = \text{Tr } \rho(g)$ for $g \in G$. For complex representations, ρ is determined by its character; if ρ, ρ' are representations with identical characters, then ρ and ρ' are isomorphic as representations (cf. [Ser77, Chapter 2, §2.3]).

Definition 1.1. Let χ_1, \dots, χ_h be the distinct characters of the complex irreducible representations of G , where $h = \#$ conjugacy classes of G . Then the **representation ring** of G is

$$R(G) = \mathbb{Z}\chi_1 \oplus \dots \oplus \mathbb{Z}\chi_h.$$

Since we take differences of characters in $R(G)$, we call elements of $R(G)$ **virtual representations**.

Let K be a number field. Denote by $R_K(G)$ the group generated by characters of the representations of G over K . This is a subring of $R(G)$. When $K = \mathbb{Q}$ this is called the **rational representation ring**. The characters of the distinct irreducible representations of G over K form an orthogonal basis of $R_K(G)$ with respect to the usual inner product on $R(G)$ ([Ser77, Proposition 32]). Let m be the exponent of G . If K contains the m -th roots of unity, then $R_K(G) = R(G)$ ([Ser77, Theorem 24]). This implies every representation of G can be realized over such K .

Let $\text{Perm}(G)$ be the ring of virtual permutation representations of G (i.e. the ring generated by the characters of $\mathbb{C}[G/H] = \text{Ind}_H^G \mathbb{1}$ for $H \leq G$). Let $\text{Char}_{\mathbb{Q}}(G)$ be the ring of rationally valued characters of G . Then we have inclusions

$$\text{Perm}(G) \rightarrow R_{\mathbb{Q}}(G) \rightarrow \text{Char}_{\mathbb{Q}}(G).$$

Each of these groups have equal \mathbb{Z} -rank, equal to the number of conjugacy classes of cyclic subgroups of G ([Ser77, Chapter 13, §13.1]). Moreover the cokernels of these maps are finite.

Definition 1.2. Let $\rho \in R(G)$. We define the norm of ρ , denoted $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$, by

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) := \sum_{\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^\sigma \in \text{Char}_{\mathbb{Q}}(G),$$

where $\mathbb{Q}(\rho)$ is the smallest Galois field extension that contains $\{\rho(g) : g \in G\}$, and ρ^σ is the character such that $\rho^\sigma(g) = \sigma(\rho(g))$.

It's clear that $\text{Char}_{\mathbb{Q}}(G)$ is generated by $\{\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) : \rho \in \text{Irr}(G)\}$. Indeed, if a representation has a rationally valued character, then any complex irreducible constituent must occur along with all its Galois conjugates with equal multiplicity.

Remark 1.3. This is not additive, i.e. one does not have

$$\mathfrak{N}_{\mathbb{Q}(\rho+\tau)/\mathbb{Q}}(\rho+\tau) = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) + \mathfrak{N}_{\mathbb{Q}(\tau)/\mathbb{Q}}(\tau).$$

This does hold when $\mathbb{Q}(\rho) = \mathbb{Q}(\tau)$.

Example 1.4. Let $G = C_p$ and ψ_p a character of order p . Then $\mathbb{Q}(\psi_p) = \mathbb{Q}(\zeta_p)$ and $\mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p)$ is the sum over the $p-1$ non-trivial characters of G . But $\mathfrak{N}_{\mathbb{Q}(\psi_p+1)/\mathbb{Q}}(\psi_p+1) = \mathbb{1}^{\oplus(p-1)} + \mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p) \neq \mathfrak{N}_{\mathbb{Q}(1)/\mathbb{Q}}(1) + \mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p)$.

The group

$$\hat{C}(G) := \frac{\text{Char}_{\mathbb{Q}}(G)}{\text{Perm}(G)}$$

is a finite abelian group, of exponent dividing $|G|$ (this follows from Artin's induction theorem [ref](#)). The study of this group is quite subtle, see for example [BD16]. For us, it's enough to know that there exists a minimum integer m , depending of ρ and dividing $|G|$ such that $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m} \in \text{Perm}(G)$, where m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$.

Example 1.5. If $G = C_n$ then $\hat{C}(G)$ is trivial (see Example 1.15). $\hat{C}(G)$ is also trivial for the symmetric groups $G = S_n$.

Example 1.6. $G = Q_8$, the quaternion group, has $\hat{C}(G) = \mathbb{Z}/2\mathbb{Z}$. The faithful character χ of Q_8 has rational character and

$$\chi^{\oplus 2} = \text{Ind}_{C_1}^G \mathbb{1} \ominus \text{Ind}_{C_2}^G \mathbb{1},$$

but one cannot write χ as a virtual permutation representation (χ has Schur index 2 so $\chi \notin \text{R}_{\mathbb{Q}}(G)$).

1.2 The Burnside ring and relations for permutation representations

Let G be a finite group. Recall that there is a bijection

$$\{\text{transitive finite } G\text{-sets } X \text{ up to isomorphism}\} \leftrightarrow \{\text{subgroups } H \leq G \text{ up to conjugacy}\}$$

given by sending a transitive finite G -set X to $H = \text{Stab}_G(x)$ for some $x \in X$. The action of G on X is equivalent to the action of G on G/H .

Definition 1.7. Let $[X]$ denote the isomorphism class of a G -set X . The **Burnside ring** $\text{B}(G)$ is the free abelian group on isomorphism classes of finite G -sets, modulo the relations $[S] + [T] = [S \sqcup T]$ for S, T finite G -sets. This is a ring; multiplication is given by $[S] \cdot [T] = [S \times T]$.

We only need that $\text{B}(G)$ is a group, and do not use its multiplicative structure. $\text{B}(G)$ is generated by $\{[X] : X \text{ finite transitive } G\text{-set}\}$. Using the identification of finite transitive G -sets with subgroups of G , we write elements of $\text{B}(G)$ as $\sum_i n_i H_i$ for $n_i \in \mathbb{Z}$, $H_i \leq G$.

Definition 1.8. There is a homomorphism from the Burnside ring to the rational representation ring $\text{R}_{\mathbb{Q}}(G)$ of G given by sending a G -set X to the permutation representation $\mathbb{C}[X]$. In terms of subgroups of G , we write

$$\mathbb{C}[G/-] : \text{B}(G) \rightarrow \text{Perm}(G), \quad \Theta = \sum_i n_i H_i \mapsto \mathbb{C}[G/\Theta] = \sum_i n_i \text{Ind}_{H_i}^G \mathbb{1}.$$

Definition 1.9. Elements in the kernel of $\mathbb{C}[G/-]$ are known as **Brauer relations**, that is $\sum_i n_i H_i \in B(G)$ such that $\oplus_i \mathbb{C}[G/H_i]^{\oplus n_i} = 0$ as a virtual permutation representation (so the corresponding character is 0).

Non-trivial Brauer relations are instances of non-isomorphic G -sets giving rise to isomorphic permutation representations.

Example 1.10. The irreducible representations of $G = S_3$ are the trivial representation $\mathbb{1}$, the sign representation ϵ and the 2-dimensional representation ρ . We have

$$\begin{aligned} \mathbb{C}[G/C_1] &= \mathbb{1} \oplus \epsilon \oplus \rho^{\oplus 2}, & \mathbb{C}[G/C_2] &= \mathbb{1} \oplus \rho, \\ \mathbb{C}[G/C_3] &= \mathbb{1} \oplus \epsilon, & \mathbb{C}[G/G] &= \mathbb{1}. \end{aligned}$$

Then $\Psi = C_1 - 2C_2 - C_3 + 2S_3$ is the unique Brauer relation for G .

Example 1.11. Cyclic groups have no Brauer relations. Indeed, if $G = C_n$, the \mathbb{Z} -rank of $\text{Perm}(G)$ is the number of cyclic subgroups of C_n , i.e the number of subgroups of C_n , which is the \mathbb{Z} -rank of $B(G)$. Hence the rank of the kernel of the map $B(G) \rightarrow \text{Perm}(G)$ is zero.

In the last section, we described how to obtain a character in $\text{Perm}(G)$ from a character $\rho \in R(G)$. We are interested in when this is an image of an element from the Burnside ring.

Definition 1.12. We call $\Theta = \sum_i n_i H_i \in B(G)$ a ρ -**relation** if $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, for some $m \geq 1$.

If $D \leq G$, then one can pass from $\text{Perm}(G)$ to $\text{Perm}(D)$ via restriction, and in the other direction via induction. We define analogous maps for the Burnside ring.

Definition 1.13. For $D \leq G$, define maps $\text{Res}_D: B(G) \rightarrow B(D)$ and $\text{Ind}_D: B(D) \rightarrow B(G)$ by

$$\text{Res}_D H = \sum_{x \in H \backslash G/D} D \cap H^{x^{-1}}, \quad \text{Ind}_D H = H.$$

These correspond to the representation theory side, where $\text{Res}_D \text{Ind}_H^G \mathbb{1} = \sum_{x \in H \backslash G/D} \text{Ind}_{D \cap H^{x^{-1}}}^D \mathbb{1}$ (Mackey's decomposition, cf. [Ser77, Chapter 7, §7.3]), and $\text{Ind}_D^G \text{Ind}_H^D \mathbb{1} = \text{Ind}_H^G \mathbb{1}$.

The following are some elementary properties of these relations:

Proposition 1.14. Let $\rho \in R(G)$, $\Theta \sum_i n_i H_i \in B(G)$ a ρ -relation. Then,

1. $n\Theta$ is a ρ -relation for all $n \geq 1$.
2. $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$ where m is a multiple of the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$.
3. If $\Psi \in B(G)$ is a Brauer relation, then $\Theta + \Psi$ is also a ρ -relation.
4. For a fixed $m \geq 1$, if $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m} \in \text{Perm}(G)$ then there are $\#(\text{Brauer relations of } G) + 1$ elements $\Theta \in B(G)$ with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$.
5. (Projection) If $N \trianglelefteq G$ then $(N \cdot \Theta)/N = \sum_i n_i N H_i / N$ is a ρ^N -relation, viewing this relation in $R(G/N)$.
6. (Restriction) For $D \leq G$, $\text{Res}_D \Theta$ is a $\text{Res}_D \rho$ -relation.

Proof. All but (5) are clear. For (5), observe that for $H \leq G$, $\mathbb{C}[G/H]^N \simeq \mathbb{C}[G/NH]$ as G -representations (see proof of [DD09, Theorem 2.8]). We also need to show that $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^N \simeq \mathfrak{N}_{\mathbb{Q}(\rho^N)/\mathbb{Q}}(\rho^N)^{\oplus k}$ for some $k \geq 1$. This is the case;

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^N = \left(\bigoplus_{\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^\sigma \right)^N \simeq \bigoplus_{\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} (\rho^\sigma)^N \simeq \bigoplus_{\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} (\rho^N)^\sigma = \mathfrak{N}_{\mathbb{Q}(\rho^N)/\mathbb{Q}}(\rho^N)^{\oplus k},$$

where $k = [\mathbb{Q}(\rho) : \mathbb{Q}(\rho^N)]$. □

Example 1.15. Let $G = C_n$. For each $d \mid n$, let $\chi_d = \mathfrak{N}_{\mathbb{Q}(\varphi_d)/\mathbb{Q}}(\varphi_d)$, where φ_d is an irreducible complex character of G with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d . Then $\{\chi_d : d \mid n\}$ form an orthogonal basis for the irreducible rational-valued representations of G [cite Serre exercise](#). Since $C_{n/d} \trianglelefteq G$, $\text{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G containing $C_{n/d}$ in their kernel. Thus, $\text{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain a φ_d -relation for each $d \mid n$:

$$\chi_d = \sum_{d' \mid d} \mu(d/d') \cdot \text{Ind}_{C_{n/d}}^G \mathbb{1}.$$

Note that this is the only way of writing χ_d as a sum of permutation representations, since cyclic groups have no Brauer relations (Example 1.11). Similarly, there is a unique $\Theta \in B(G)$ such that $\mathbb{C}[G/\Theta] \simeq \chi_d^m$ for all $m \geq 1$.

1.3 Functions on the Burnside ring and norm relations

Let $f: B(G) \rightarrow A$ be a multiplicative function with $f(\sum_i n_i H_i) = \prod_i f(H_i)^{n_i}$ where A is an abelian group. As in [DD09], we say that f is **representation theoretic** if f is trivial on Brauer relations. This implies that for a G -set X , f only depends on the representation $\mathbb{C}[X]$.

Example 1.16. Let $\lambda \in \mathbb{R}^\times$ and consider the function $H \mapsto \lambda^{[G:H]}$. This is trivial on Brauer relations; if $\sum_i n_i H_i$ is a Brauer relation then $\lambda^{\sum_i n_i [G:H]} = \lambda^{\dim(\oplus_i \mathbb{C}[G/H_i]^{\oplus n_i})} = 1$.

Let $\rho \in R(G)$. Let $\Theta \in B(G)$ be a ρ -relation, with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. If we have a function $f: B(G) \rightarrow \mathbb{Q}^\times$, we may then ask whether $f(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.

Definition 1.17. Let $\rho \in R(G)$, Θ a ρ -relation, and $f: B(G) \rightarrow \mathbb{Q}^\times$. If $f(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, then we call Θ a **norm relation** for f . If $f(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every ρ -relation in $B(G)$, then we say f is **trivial on ρ -relations**.

Example 1.18. Let $G = C_p$ for p a prime. Let ρ be a character of degree p , so $\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_p)$. There is a unique ρ -relation given by $\Theta = C_1 - C_p$. Let $\psi: B(G) \rightarrow \mathbb{Q}^\times$ be given by $\psi(H) = [G:H]$. Then $\psi(\Theta)$ is a norm relation, as $\psi(\Theta) = p \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ is the norm of $1 - \zeta_p$.

In general, showing that a ρ -relation Θ is a norm relation for f does not imply that this is the case for all possible ρ -relations. Under certain circumstances however, we can.

Proposition 1.19. Let $\rho \in R(G)$ and $f: B(G) \rightarrow \mathbb{Q}^\times$. Suppose that $f(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every Brauer relation $\Psi \in B(G)$. Let $\Theta \in B(G)$ be a ρ -relation, with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, where m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. If Θ is a norm relation for f , then f is trivial on ρ -relations.

Proof. Consider an arbitrary ρ -relation Θ' such that $\mathbb{C}[G/\Theta'] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus l}$ for some $l \geq 1$. Then $m \mid l$ and $\Psi = \Theta' - \frac{l}{m}\Theta$ is a Brauer relation. Thus

$$f(\Theta') = f(\Psi) \cdot f(\Theta)^{\frac{l}{m}} \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$$

and so f is trivial on all ρ -relations. \square

Example 1.20. Let $G = C_n$. Then any function $f: \mathcal{B}(G) \rightarrow \mathbb{Q}^\times$ is trivial on Brauer relations since G does not have any. Let φ_d be an irreducible complex character of G of order $d \mid n$. Thus to conclude that f is trivial on φ_d -relations, it is enough to show that the φ_d -relation constructed in Example 1.15 is a norm relation for f .

Example 1.21. Let E/\mathbb{Q} be an elliptic curve, $G = \text{Gal}(F/\mathbb{Q})$ for F/\mathbb{Q} a Galois extension. The function $C: H \mapsto C_{E/F^H}$ (defined in §4.1, (7)/ [refer to introduction](#)) for $H \leq G$ extends to a multiplicative function on the Burnside ring. In later sections we will investigate when this is trivial on ρ -relations, for $\rho \in \mathcal{R}(G)$.

It appears quite difficult in general to describe the set of ρ -relations for some finite group G and $\rho \in \mathcal{R}(G)$. Thus determining functions that are trivial on ρ -relations is even more difficult. We have a better understanding of the relations when G is cyclic, and can prove the following result.

Proposition 1.22. *Let $G = C_n$. Let $\rho \in \mathcal{R}(G)$ such that $[\mathbb{Q}(\rho): \mathbb{Q}] = 2$. Consider the function $g: \mathcal{B}(G) \rightarrow \mathbb{Q}^\times$ given by $H \mapsto [G : H]$. Then g is trivial on ρ -relations.*

Proof. Let \mathfrak{f} be the minimum positive integer such that $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_{\mathfrak{f}})$. As $\mathbb{Q}(\rho)$ is quadratic, \mathfrak{f} is described in Remark A.7 (it is the absolute value of the discriminant Δ of $\mathbb{Q}(\rho)$). Observe that $\mathfrak{f} \mid n$ since all characters of G are realized over $\mathbb{Q}(\zeta_n)$. Since $\hat{C}(G) = 1$ and G has no Brauer relations, by Proposition 1.19 it suffices to show that $\Theta \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for $\Theta \in \mathcal{B}(G)$ such that $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$.

Let $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) = \sum_{d \mid n} a_d \chi_d$ where $a_d \in \mathbb{Z}$ and χ_d are the basis of irreducible rational representations of C_n defined in Example 1.15. Let $\Psi_d = \sum_{d' \mid d} \mu(d/d') \cdot C_{n/d}$ so that $\mathbb{C}[\Psi_d] = \chi_d$, as observed in the example. Then $\mathbb{C}[G/\Theta] \simeq \mathbb{C}[\sum_{d \mid n} a_d \Psi_d]$ which implies that $\Theta = \sum_{d \mid n} a_d \Psi_d$.

Evaluating g on Ψ_d is trivial unless $d = q^a$ for some q prime, $a \geq 1$. Indeed, if $d = p_1^{e_1} \cdots p_r^{e_r}$, with $r \geq 2$ and $e_i \geq 1$, then

$$\prod_{d' \mid d} (d')^{\mu(d/d')} = \prod_{j_1, \dots, j_r \in \{0, 1\}^r} \left(p_1^{e_1 - j_1} \cdots p_r^{e_r - j_r} \right)^{\#j_i=1} = \prod_{i=1}^r \left(\frac{p_i^{e_i}}{p_i^{e_i-1}} \right)^{\sum_{j=0}^{r-1} \binom{r-1}{j} (-1)^j} = 1.$$

On the other hand,

$$\prod_{d' \mid q^a} (d')^{\mu(q^a/d')} = q.$$

The irreducible representations of C_n over $\mathbb{Q}(\rho)$ are given by the orbits of the complex irreducible characters of C_n acted upon by $H = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\rho))$. Consider $d \mid n$ with $\mathfrak{f} \nmid d$, so that $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_d)$. Recall that $\chi_d = \mathfrak{N}_{\mathbb{Q}(\varphi_d)/\mathbb{Q}}(\varphi_d)$, where $\mathbb{Q}(\varphi_d) = \mathbb{Q}(\zeta_d)$. Let $B = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d))$. Then $\mathbb{Q}(\rho) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$, so $BH = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The orbit of φ_d under H is fixed by BH , hence is rational. It follows that $\langle \rho, \varphi_d \rangle = \langle \rho^\sigma, \varphi_d \rangle$ for σ the generator of $\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$. Thus $2 = [\mathbb{Q}(\rho) : \mathbb{Q}]$ divides a_d , and so $g(a_d \Psi_d) = g(\Psi_d)^{a_d} \in \mathbb{Q}^{\times 2} \subset N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.

Thus a_d can only be odd when $\mathfrak{f} \mid d$. Therefore for $g(\Theta)$ to be non-square we require $\mathfrak{f} = p$ for some prime p . Then p must be odd ($|\Delta|$ cannot be 2) and $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{p^*})$. But p is a norm in $\mathbb{Q}(\sqrt{p^*})$ by Corollary A.13. \square

1.3.1 D-local functions

We are interested in functions on the Burnside ring that are number-theoretic in nature, where we take G to be a Galois group. Often, these functions are *local*.

Example 1.23. Let F/K be a finite Galois extension of number fields and let $G = \text{Gal}(F/K)$. Let \mathfrak{p} be a prime of K and \mathfrak{q} a prime of F above \mathfrak{p} . Let $D_{\mathfrak{q}} \leq G$ be the corresponding decomposition group. For $H \leq G$, the number of primes in $L = F^H = K(\alpha)$ above \mathfrak{p} are in one-to-one correspondence with the double cosets $H \backslash G / D_{\mathfrak{q}}$. This correspondence is given by sending a prime \mathfrak{s} in L above \mathfrak{p} to the elements of G that send \mathfrak{q} to some prime above \mathfrak{s} .

We can use the function $f: B(G) \rightarrow \mathbb{Q}^\times$ given by $H \mapsto \lambda^{|H \backslash G / D|}$ (for $\lambda \neq \pm 1$) to describe the number of places above \mathfrak{p} in any intermediate extension of F/K . But if we let $g: B(D) \rightarrow \mathbb{Q}^\times$ be defined by $H \mapsto \lambda$, then

$$f(H) = g(\text{Res}_D H) = \prod_{x \in H \backslash G / D} g(D \cap H^{x^{-1}}).$$

Therefore the value of f on any G -set X only depends on the structure of X as a D -set.

Such functions motivate the following definition:

Definition 1.24. ([DD09, Definition 2.33]) If $D \leq G$, we say a function f on $B(G)$ is **D -local** if there is a function f_D on $B(D)$ such that $f(H) = f_D(\text{Res}_D H)$ for $H \leq G$. If this is the case, we write

$$f = (D, f_D).$$

Example 1.25. For $G = \text{Gal}(F/K)$, v a place of K with decomposition group D , the function

$$H \mapsto \prod_{w|v} c_w(E/F^H)$$

is D -local, where E is an elliptic curve over K and c_w is the local Tamagawa number.

Let $I \triangleleft D$ be the inertia subgroup of the place v , so D/I is cyclic. If a prime w in F^H corresponds to the double coset HxD , then its decomposition and inertia groups in F/F^H are $H \cap D^x$ and $H \cap I^x$ respectively. The ramification degree and residue degree of w over K are given by $e_w = \frac{|I|}{|H \cap I^x|}$ and $f_w = \frac{[D:I]}{|H \cap D^x : H \cap I^x|}$. We will consider functions that depend on e and f , and so introduce the following:

Definition 1.26. [DD09, Definition 2.35] Suppose $I \triangleleft D < G$ with D/I cyclic, and $\psi(e, f)$ is a function of $e, f \in \mathbb{N}$. Define a function on $B(G)$ by

$$(D, I, \psi): H \mapsto \prod_{x \in H \backslash G / D} \psi\left(\frac{|I|}{|H \cap I^x|}, \frac{[D:I]}{|H \cap D^x : H \cap I^x|}\right).$$

This is a D -local function on $B(G)$ with

$$(D, I, \psi) = \left(D, U \mapsto \psi\left(\frac{|I|}{|U \cap I|}, \frac{|D|}{|UI|}\right)\right).$$

Example 1.27. If E/K has split multiplicative reduction at v with $c_v(E/K) = n$, then $c_w(E/F^H) = e_w n$ for a place w of F^H above v . In this case the function in Example 1.25 is (D, I, en) .

Proposition 1.28. Let $D \leq G$, $N \trianglelefteq G$. Let $\rho \in R(G)$.

1. (Restriction) Suppose that $\mathbb{Q}(\rho) = \mathbb{Q}(\text{Res}_D \rho)$. If $f = (D, f_D)$ and f_D is trivial on $(\text{Res}_D \rho)$ -relations, then f is trivial on ρ -relations.
2. (Projection) Suppose that $\mathbb{Q}(\rho) = \mathbb{Q}(\rho^N)$ (view ρ^N as a representation of G/N). Consider f a function on $B(G)$ such that $f(H) = f_{G/N}(NH/N)$ for some function $f_{G/N}$ on $B(G/N)$. If $f_{G/N}$ is trivial on ρ^N -relations (viewed in $R(G/N)$), then f is trivial on ρ -relations.

One would like to be able to say that if $f = (D, f_D)$ and f_D is trivial on $(\text{Res}_D \rho)$ -relations, then f is trivial on ρ -relations. But as defined, one cannot conclude this when $[\mathbb{Q}(\rho) : \mathbb{Q}(\text{Res}_D \rho)] > 1$. Under some conditions however, when $\mathbb{Q}(\text{Res}_D \rho) = \mathbb{Q}$, one can automatically conclude that f is trivial on ρ -relations, as in the following.

Proposition 1.29. *Let $D \leq G$. Consider $\rho \in R(G)$ with $[\mathbb{Q}(\rho) : \mathbb{Q}] = n$, where multiplication by n is injective on $\hat{C}(D)$. Consider $f = (D, f_D)$ a D -local function on $B(G)$. Suppose that $f_D(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every Brauer relation $\Psi \in B(D)$. Then, if $\mathbb{Q}(\text{Res}_D \rho) = \mathbb{Q}$, f is trivial on ρ -relations.*

Proof. Let Θ be a ρ -relation, with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. Then

$$\mathbb{C}[D/\text{Res}_D \Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\text{Res}_D \rho)/\mathbb{Q}}(\text{Res}_D \rho)^{\oplus mn} \in \text{Perm}(D).$$

The condition on n ensures that there exists $\Theta' \in B(D)$ with $\mathbb{C}[D/\Theta'] \simeq \mathfrak{N}_{\mathbb{Q}(\text{Res}_D \rho)/\mathbb{Q}}(\text{Res}_D \rho)^{\oplus m} \in \text{Perm}(D)$. Then $\Psi = \text{Res}_D \Theta - n\Theta'$ is a Brauer relation for D . Thus

$$f(\Theta) = f_D(\text{Res}_D \Theta) = f_D(\Psi) f_D(n\Theta') = f_D(\Psi) f_D(\Theta')^n \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times),$$

since $f_D(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ and $\mathbb{Q}^{\times n} \subset N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. \square

The following is an example of when constant D -local functions are squares when evaluated on ρ -relations.

Proposition 1.30. *Let $D \leq G$ with D of odd order, and $f = (D, \alpha)$ a D -local function on $B(G)$, where $\alpha \in \mathbb{Q}^\times$ is constant. Let $\rho \in R(G)$ with $[\mathbb{Q}(\rho) : \mathbb{Q}]$ even. Then for a ρ -relation Θ , $f(\Theta) \in \mathbb{Q}^{\times 2}$.*

Proof. The function (D, α) on $B(G)$ sends $H \leq G$ to $\alpha^{|H \setminus G/D|}$. Let $\Theta = \sum_i n_i H_i$ be a ρ -relation with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$ for some $m \geq 1$. One has $(D, \alpha)(\Theta) = \alpha^{\sum_i n_i \cdot |H_i \setminus G/D|}$. We show that $\sum_i n_i \cdot |H_i \setminus G/D|$ is even.

One has $\text{Res}_D \Theta = \sum_i n_i \sum_{x \in H_i \setminus G/D} D \cap H_i^{x^{-1}}$, and $\mathbb{C}[D/\text{Res}_D \Theta]$ has even dimension, since it is isomorphic to $\sum_{\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \text{Res}_D \rho^\sigma$ and $\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ has even order. The dimension is

$$\sum_i n_i \sum_{x \in H_i \setminus G/D} [D : D \cap H_i^{x^{-1}}].$$

Since each $[D : D \cap H_i^{x^{-1}}]$ is odd, this implies there are an even number of terms in the summation, i.e. that $\sum_i n_i \cdot |H_i \setminus G/D|$ is even. \square

2 Elliptic Curves

Having discussed the relevant aspects of representation theory that we will require, we now introduce elliptic curves, our main object to study. Our discussion will be rather informal and brief, and will avoid most proofs. We will spend some time discussing the reduction type of elliptic curves and how this can change over finite extensions. Nevertheless, we assume good familiarity with elliptic curves. There is great material available for elliptic curves, and [Sil09] gives a complete discussion.

An elliptic curve E over a field K is a genus one smooth projective curve with a specified K -rational point. Any such curve can be written as the locus on \mathbb{P}^2 of a **Weierstrass equation**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_2, a_4, a_6 \in K, \quad (1)$$

together with the specified K -rational point $[0 : 1 : 0]$ at infinity.

When $\text{Char}(K) \neq 2$, which will always be the case, we can further simplify the equation to

$$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6, \quad a_2, a_4, a_6 \in K, \quad (2)$$

so unless stated otherwise we will assume that E has an equation of this form. We remark that if $\text{Char}(K) = 2$, then (2) always defines a singular curve. Associated to this equation there are constants

$$c_4 = 16(a_2^2 - 3a_4) \quad \text{and} \quad \Delta = 16(a_2^2a_4^2 - 4a_2^3a_6 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6)$$

and differential

$$w = \frac{dx}{2y} = \frac{dy}{3x^2 + 2a_2x + a_4}. \quad (3)$$

One can also define these constants for the general Weierstrass equation (1), but we omit the description. A complete description is given in [Sil09, §III.1]

The curve defined by (2) is singular if and only if the polynomial $f(x)$ has repeated roots over \bar{K} . If it has a double and a simple root, then we say it has a node; if it has a triple root, then it has a cusp. The following proposition characterizes this behaviour in terms of c_4 and Δ .

Proposition 2.1. *The curve given by a Weierstrass equation satisfies:*

1. *It is nonsingular if and only if $\Delta \neq 0$.*
2. *It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.*
3. *It has a cusp if and only if $\Delta = c_4 = 0$.*

Proof. [Sil09, §III Proposition 1.4]. □

When $\Delta \neq 0$, the equation defines an elliptic curve. A fundamental property is that the set of K -rational points of an elliptic curve forms an abelian group, denoted by $(E(K), \oplus)$ ([Sil09, §III.2]). When K is a number field, the Mordell-Weil theorem shows that this group is also finitely generated, and therefore

$$E(K) = E(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $E(K)_{\text{tors}}$ is a finite abelian group and r is denoted the rank of E .

2.1 Elliptic Curves over Local Fields and Reduction Types

Now assume that K is a local field of characteristic 0 with a discrete valuation ν , ring of integers R and residue field κ . We denote by $a \mapsto \tilde{a}$ for the natural quotient map $K \rightarrow \kappa$. We say that (2) is a **minimal Weierstrass equation** if $a_2, a_4, a_6 \in R$ and $\nu(\Delta)$ is minimal among all such equations. When this is the case, we have a well-defined associated curve \tilde{E} over κ defined by the equation $y^2 = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$ and the associated **reduction map**

$$\widetilde{(\cdot)} : E(K) \longrightarrow \tilde{E}(\kappa), \quad (4)$$

obtained by reducing the coordinates of a point $P \in E(K)$ modulo κ . One needs to have some care defining the reduction map. For a detailed construction, see [Sil09, §1 VII.2]. We remark that \tilde{E} may be a singular curve, and the **reduction type** of E over K describes the behaviour of \tilde{E} as a curve over κ .

Definition 2.2. Let E/K and \tilde{E}/κ be as above. Then we say that

- (a) E/K has good (or stable) reduction if \tilde{E} is non-singular.
- (b) E/K has multiplicative (or semistable) reduction if \tilde{E} has a node.
- (c) E/K has additive (or unstable) reduction if \tilde{E} has a cusp.

In cases (b) and (c) we say that E/K has bad reduction. Moreover, if E/K has multiplicative reduction, we say that the reduction is split if the slopes of the tangent lines at the node are in K , and non-split otherwise.

By Proposition 2.1 we immediately see that E/K has good reduction if $\nu(\Delta) = 0$ and bad otherwise. In that case, E/K has multiplicative reduction if $\nu(c_4) = 0$ and additive otherwise.

An important question which will be of interest for us is to understand how the reduction type of an elliptic curve E changes over a finite field extension F/K . The following proposition gathers this information.

Proposition 2.3 (Semistable reduction Theorem). *Let E be an elliptic curve over a local field K of characteristic 0.*

- (i) *Let F/K be an unramified extension. Then the reduction type of E over K (good multiplicative or additive) is the same as the reduction type of E over F .*
- (ii) *Let F/K be a finite extension. If E has good or multiplicative reduction over K , then it has the same reduction type over F . This also applies specifically to split multiplicative reduction.*
- (iii) *If E has non-split multiplicative reduction over K and F/K is a finite extension with even residual degree, then E has split multiplicative reduction over F .*
- (iv) *There exists a finite extension F/K such that E has either good or split multiplicative over F .*

Proof. [Sil09, §VII Proposition 5.4] □

Given an unstable elliptic curve E over K , we say that it has potentially good (resp. multiplicative) reduction if it has good (resp. multiplicative) reduction over a finite field extension of K .

2.2 Tamagawa Numbers

Recall from the previous section that if E/K has bad reduction, then \tilde{E} is not a smooth curve and therefore its κ -rational points may not form a group. However, the set $\tilde{E}_{ns}(\kappa)$ of non-singular points of $\tilde{E}(\kappa)$ does indeed form a group. The reduction map (4) is in general not surjective, but it does surject onto $\tilde{E}_{ns}(\kappa)$. It is natural therefore to define $E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(\kappa)\}$, which is also a subgroup of $E(K)$. Importantly, the resulting reduction map

$$\widetilde{(\cdot)} : E_0(K) \longrightarrow \tilde{E}_{ns}(\kappa)$$

is a surjective homomorphism of abelian groups.

Definition 2.4. The **Tamagawa number** of E/K is defined as

$$c(E/K) := |E(K)/E_0(K)|. \quad (5)$$

In later sections we will be concerned in computing Tamagawa numbers. Note that if E/K has good reduction, then $E_0(K) = E(K)$ and therefore $c(E/K) = 1$. However, when E/K has bad reduction, this is a hard question to answer in general. Fortunately, this question can always be resolved using Tate's Algorithm (see [Sil94, §IV.9]), and for semistable reduction, Tamagawa numbers have a simple explicit description.

Proposition 2.5. *Let E/K have multiplicative reduction, and let $n = \nu(\Delta)$ be the valuation of the minimal discriminant. Then*

$$c(E/K) = \begin{cases} n & \text{if } E/K \text{ has split reduction,} \\ 1 & \text{if } n \text{ is odd and } E/K \text{ is non-split,} \\ 2 & \text{if } n \text{ is even and } E/K \text{ is non-split.} \end{cases}$$

The unstable case is harder, but there exists an explicit description for elliptic curves with equation $y^2 = x^3 + Ax + B$ and residual characteristic is at least 5.

Lemma 2.6. *Let $F/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let*

$$E : y^2 = x^3 + Ax + B$$

be an elliptic curve over K with additive reduction. Let $n = v_K(\Delta)$ be the valuation of the minimal discriminant, and e the ramification index of K'/K .

If E has potentially good reduction, then

$$\begin{aligned} \gcd(ne, 12) = 2 &\implies c(E/K') = 1, & (II, II^*) \\ \gcd(ne, 12) = 3 &\implies c(E/K') = 2, & (III, III^*) \\ \gcd(ne, 12) = 4 &\implies c(E/K') = \begin{cases} 1, & \sqrt{B} \notin K' \\ 3, & \sqrt{B} \in K' \end{cases}, & (IV, IV^*) \\ \gcd(ne, 12) = 6 &\implies c(E/K') = \begin{cases} 2, & \sqrt{\Delta} \notin K' \\ 1 \text{ or } 4, & \sqrt{\Delta} \in K' \end{cases}, & (I_0^*) \\ \gcd(ne, 12) = 12 &\implies c(E/K') = 1. & (I_0) \end{aligned}$$

Moreover, the extensions $K'(\sqrt{B})/K'$ and $K'(\sqrt{\Delta})/K'$ are unramified.

If E has potentially multiplicative reduction of type I_n^ over K , and e is odd, then it has Kodaira type I_{en}^* over K' . Moreover,*

$$\begin{aligned} 2 \nmid n &\implies c(E/K') = \begin{cases} 2, & \sqrt{B} \notin K' \\ 4, & \sqrt{B} \in K' \end{cases}, & (I_{ne}^*) \\ 2 \mid n &\implies c(E/K') = \begin{cases} 2 & \sqrt{\Delta} \notin K' \\ 4 & \sqrt{\Delta} \in K' \end{cases}, & (I_{ne}^*) \end{aligned}$$

Proof. [DD09, Lemma 3.22]

□

2.3 Elliptic Curves over Global Fields

The topics we have discussed so far, such as the reduction type of an elliptic curve and the Tamagawa number, are intrinsically local objects. We now briefly discuss how we can associate these objects to global fields. For simplicity, assume that E is an elliptic curve over a number field K , let \mathfrak{p} be a finite place of K and denote $K_{\mathfrak{p}}$ by the completion of K at \mathfrak{p} with residue field $\kappa_{\mathfrak{p}}$. Clearly, we have that $E(K) \subseteq E(K_{\mathfrak{p}})$ and therefore we can apply the previous description to the curve $E/K_{\mathfrak{p}}$.

In particular, the reduction type of E/K at \mathfrak{p} is the reduction type of $E/K_{\mathfrak{p}}$ and the Tamagawa number of E/K at \mathfrak{p} is defined as

$$c_{\mathfrak{p}}(E/K) := c(E/K_{\mathfrak{p}}),$$

and we also define

$$c(E/K) := \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/K).$$

Finally, we say that a Weierstrass equation (1) is a **global minimal equation** if it is a minimal equation for all finite places \mathfrak{p} of K . Even though such an equation does not always exist for any K , it does hold for \mathbb{Q} .

Proposition 2.7. *Let E/\mathbb{Q} be an elliptic curve. Then E has a global minimal Weierstrass equation.*

Throughout the document, we will work with elliptic curves over \mathbb{Q} , so unless stated otherwise we will assume the defining equation is global minimal.

3 Representations, L-functions and Artin Twists

The Birch-Swinnerton-Dyer conjecture classically provides a connection between the arithmetic of elliptic curves and their L -functions. In this preliminary section, we explore the classical definition of L -functions attached to an elliptic curve and their twists, and we explore some of the relevant properties that we will use later on. To do so, we first need to explore the notion of an Artin representation and of an ℓ -adic representation.

Throughout this section we fix a field K , which will either be a number field or a local field of characteristic 0. We always specify what K is in each context. We also fix an algebraic closure \bar{K} of K and we denote by G_K the absolute Galois group $\text{Gal}(\bar{K}/K)$ of K . We recall that G_K is a profinite group

$$G_K = \varprojlim_F \text{Gal}(F/K),$$

where F ranges over the finite Galois extensions of K and therefore has a natural topology where a basis of open sets is given by $\text{Gal}(\bar{K}/F)$ where F is a finite extension of K .

3.1 Artin Representations and ℓ -adic Representations

We begin by recalling the notion of an Artin representation.

Definition 3.1. Let K be a number field or a local field with characteristic 0. An **Artin representation** ρ over K is a complex finite-dimensional vector space V together with a homomorphism $\rho : G_K \rightarrow \text{GL}(V) = \text{GL}_n(\mathbb{C})$ such that there is some finite Galois extension F/K with $\text{Gal}(\bar{K}/F) \subseteq \ker \rho$. In other words, ρ factors through $\text{Gal}(F/K)$ for some finite extension F of K .

Hence, an Artin representation can be equivalently viewed as a finite dimensional representation of $\text{Gal}(F/K)$ where F is some finite Galois extension of K . Throughout the document, we will use both notions and refer to either of them as Artin representations. Which notion we refer to is always clear from context.

Remark 3.2. The condition above that $\text{Gal}(\bar{K}/F) \subseteq \ker \rho$ is equivalent to $\ker \rho$ being open in G_K . This condition is clearly equivalent to ρ being continuous with respect to the discrete topology on $\text{GL}_n(\mathbb{C})$. Interestingly, the profinite topology of G_K has an surprising consequence: this condition is also equivalent to continuity with respect to the usual complex topology on $\text{GL}_n(\mathbb{C})$. Necessity is clear, and the proof of sufficiency relies on the fact that under the complex topology, ‘small’ neighbourhoods of the identity in $\text{GL}(V) = \text{GL}_n(\mathbb{C})$ do not contain any non-trivial subgroups. Hence, if $\phi : G_K \rightarrow \text{GL}(V)$ is continuous with respect to the complex topology and U is such a neighbourhood in $\text{GL}(V)$, then $\phi^{-1}(U) \subseteq \ker \phi$ and $\phi^{-1}(U)$ is open, showing that $\ker \phi$ is open too. Hence, Artin representations are simply continuous group homomorphisms $\rho : G_K \rightarrow \text{GL}_n(\mathbb{C})$.

Next, we define the notion of an ℓ -adic representation, which will be needed to define the L -function of an elliptic curve. This is the local analogue of an Artin representation.

Definition 3.3. Let K be a number field or a local field of characteristic 0. A **continuous ℓ -adic representation** ρ over K is a continuous homomorphism $\rho : G_K \rightarrow \text{GL}_n(F)$ where F is a finite extension of \mathbb{Q}_ℓ and $\text{GL}_n(F)$ is equipped with the ℓ -adic topology.

Remark 3.4. The topologies on $\text{GL}_n(\mathbb{C})$ and $\text{GL}_n(\mathbb{Q}_\ell)$ are very different, and in particular an ℓ -adic representation may not have an open kernel. Instead, continuity is equivalent to the following condition: for every $m \geq 1$, there is some finite field extension F_m of K such that for all $g \in \text{Gal}(\bar{K}/F_m)$, $\rho(g) \equiv \text{Id}_n \pmod{\ell^m}$.

Given an Artin representation ρ , one can view it as homomorphism $\rho : G_K \rightarrow \mathrm{GL}_n(\bar{\mathbb{Q}})$ and since it factors through a finite quotient, we can realise it as $\rho : G_K \rightarrow \mathrm{GL}_n(F)$ for some number field F . Hence, if ℓ is any rational prime and \mathfrak{l} is a prime in F above ℓ , then one can realise ρ as an ℓ -adic representation

$$\rho : G_K \longrightarrow \mathrm{GL}_n(F_{\mathfrak{l}}),$$

which is continuous since ρ factors through a finite quotient. Furthermore, Artin and ℓ -adic representations over K have more structure; namely, one can take **direct sums** and **tensor products**.

We describe the construction for Artin representations, since the ℓ -adic case is completely analogous. Suppose we have two Artin representations ρ_1, ρ_2 over K , and by the discussion on the preceding paragraph we can realise them as maps $\rho_i : G_K \rightarrow \mathrm{GL}_{n_i}(L_i)$, $i = 1, 2$ where L_1 and L_2 are number fields. If we let $L = L_1 L_2$, then the natural maps $\rho_1 \oplus \rho_2 : G_K \rightarrow \mathrm{GL}_{n_1+n_2}(L)$ and $\rho_1 \otimes \rho_2 : G_K \rightarrow \mathrm{GL}_{n_1 n_2}(L)$ are both Artin representations. One can also show that this construction is also well-defined up to equivalence.

Finally, we discuss the notion of an induced Artin representation. Suppose L is a finite field extension of K of degree d and let $\rho : G_L \rightarrow \mathrm{GL}(V)$ be an Artin representation. Then G_L is naturally a subgroup of G_K of index d , and therefore we can construct $\mathrm{Ind}_{G_L}^{G_K} \rho$ in the usual way. This turns out to be an Artin representation of K : if F be a number field so that ρ factors through $\mathrm{Gal}(F/L)$, then $\mathrm{Ind}_{G_L}^{G_K} \rho$ will factor through $\mathrm{Gal}(F/K)$. Furthermore, the corresponding representation over $\mathrm{Gal}(F/K)$ will be equivalent to $\mathrm{Ind}_{\mathrm{Gal}(F/L)}^{\mathrm{Gal}(F/K)} \rho$ where ρ is now viewed as a representation of $\mathrm{Gal}(F/L)$. Hence, the notion of induction is naturally compatible with this process of passing through finite quotients. Therefore, and to simplify notation, we will write $\mathrm{Ind}_{L/K} \rho$ for the induced Artin representation, and it will always be clear from context the implicit field F .

3.2 Local Polynomials and L-functions

We now briefly discuss how to attach analytic objects to Artin and ℓ -adic representations. These objects are usually described for local fields of characteristic 0 first. Then, one constructs global objects attached to number fields by completing them at their finite places, obtaining the local information and then combining it appropriately.

To begin, let K be a local field with 0 characteristic and let p be the characteristic of the residue field κ . Let $\rho : G_K \rightarrow \mathrm{GL}(V)$ be an Artin or ℓ -adic representation such that $\ell \neq p$ (this is an important technical assumption that we will not discuss further). It is a fundamental result in algebraic number theory that the natural map

$$\epsilon : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(\bar{\kappa}/\kappa)$$

is surjective, and $I_K := \ker \epsilon$ is denoted as the inertia group of K . Therefore, we have a short exact sequence

$$0 \longrightarrow I_K \longrightarrow \mathrm{Gal}(\bar{K}/K) \xrightarrow{\epsilon} \mathrm{Gal}(\bar{\kappa}/\kappa) \longrightarrow 0.$$

In addition, the map $\phi \in \mathrm{Gal}(\bar{\kappa}/\kappa)$ such that $\phi(x) = x^p$ is a topological generator of $\mathrm{Gal}(\bar{\kappa}/\kappa)$ and any preimage of ϕ under ϵ is called a Frobenius element Frob_K , which is well-defined up to I_K . Furthermore, the space of inertia-invariants

$$V^{I_K} := \{v \in V : \rho(g)v = v \text{ for all } g \in I_K\}$$

is naturally a G_K/I_K representation, which we denote ρ^{I_K} . In this setting, $\rho^{I_K}(\mathrm{Frob}_K)$ is therefore well-defined. We are now ready to define the local polynomial attached to ρ .

Definition 3.5. Let K be a local field of characteristic 0 and let p the characteristic of its local field. If ρ is an Artin or ℓ -adic representation such that $\ell \neq p$, then the local polynomial attached to ρ is

$$P(\rho, T) := \det \left(I - T \cdot \rho^{I_K} (\text{Frob}_K^{-1}) \right).$$

If K is instead a number field, the idea is to consider all finite places of K and consider all the local polynomials attached to all local completions of K to build the corresponding L-function. More concretely, let $\rho : G_K \rightarrow \text{GL}(V)$ be an Artin or ℓ -adic representation, let \mathfrak{p} be a finite place of K and let $K_{\mathfrak{p}}$ be the corresponding completion. Since $G_{K_{\mathfrak{p}}} = \text{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ is naturally a subgroup of G_K , we can restrict ρ to $\text{Res}_{\mathfrak{p}} \rho : G_{K_{\mathfrak{p}}} \rightarrow \text{GL}(V)$ and then calculate the corresponding local polynomial as long as \mathfrak{p} and ℓ are coprime. If ρ is an Artin representation, this allows us to construct the associated L -function.

Definition 3.6. Let K be a number field and ρ an Artin representation over K . If \mathfrak{p} is a finite place of K , we denote the local polynomial at \mathfrak{p} as

$$P_{\mathfrak{p}}(\rho, T) := P(\text{Res}_{\mathfrak{p}} \rho, T).$$

The associated L -function to ρ is

$$L(\rho, s) := \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\rho, N(\mathfrak{p})^{-s})}.$$

However, if ρ is an ℓ -adic representation, constructing a global object is harder, since the above method does not yield information at the finite places \mathfrak{p} that divide ℓ . This motivates the following important definition.

Definition 3.7. Let $\{\rho_{\ell}\}_{\ell}$ be a family of ℓ -adic representations for each prime ℓ . We then say that $\{\rho_{\ell}\}_{\ell}$ is a **weakly compatible system of ℓ -adic representations** if for every finite place \mathfrak{p} of K and rational primes ℓ, ℓ' not divisible by \mathfrak{p} ,

$$P_{\mathfrak{p}}(\rho_{\ell}, T) = P_{\mathfrak{p}}(\rho_{\ell'}, T)$$

.

When $\{\rho_{\ell}\}_{\ell}$ is a weakly compatible system of ℓ -adic representations, the local polynomial $P_{\mathfrak{p}}(\rho_{\ell}, T)$ can be computed using any ℓ not divisible by \mathfrak{p} . This also allows us to define the L -function in this context.

Definition 3.8. Let K be a number field and let $\{\rho_{\ell}\}_{\ell}$ be a weakly compatible system of ℓ -adic representations. Then the L -function attached to the system is

$$L(\{\rho_{\ell}\}, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\{\rho_{\ell}\}, N(\mathfrak{p})^{-s})}.$$

3.3 The Tate Module of an Elliptic Curve and their L-function

For this subsection, let K be a number field and let E be an elliptic curve defined over K . To avoid notational confusion, whenever we write E we refer to all of its \bar{K} points, while $E(K)$ refers only to the K -rational points. The aim of this section is to describe a procedure to attach an L -function to a given elliptic curve over K . In order to achieve this, we will first construct a 2-dimensional ℓ -adic representation attached to E , and then construct the L -function as described in the section above.

Let ℓ be a rational prime number. For any $n \geq 1$, we denote by $E[\ell^n]$ to be the ℓ^n -torsion points; in other words, $E[\ell^n]$ is the kernel of the map $E[\ell^n] : E \rightarrow E$. We then have the diagram of compatible maps

$$\longrightarrow E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \xrightarrow{[\ell]} \cdots \xrightarrow{[\ell]} E[\ell^2] \xrightarrow{[\ell]} E[\ell] \xrightarrow{[\ell]} \mathcal{O}_E$$

and therefore we can construct the inverse limit of this diagram

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

denoted as the ℓ -adic Tate module of the elliptic curve E . By the uniformization theorem, we know that

$$E[\ell^n] \cong \frac{\mathbb{Z}}{\ell^n \mathbb{Z}} \oplus \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}$$

as groups, and therefore

$$T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$$

as \mathbb{Z}_ℓ -modules. In addition, the Tate module carries important extra structure, namely the action of the absolute Galois group G_K . Since E is defined over K , and the multiplication by m maps are determined by polynomials with coefficients in K , there is a well-defined additive action $\psi_n : G_K \rightarrow \text{Aut}_{\mathbb{Z}}(E[\ell^n])$. Furthermore, one can show that these actions are compatible with the inverse limit diagram of the Tate module. That is, for every $n \geq 1$ and $\sigma \in G_K$, the diagram

$$\begin{array}{ccc} E[\ell^{n+1}] & \xrightarrow{\ell} & E[\ell^n] \\ \downarrow \psi_{n+1}(\sigma) & & \downarrow \psi_n(\sigma) \\ E[\ell^{n+1}] & \xrightarrow{\ell} & E[\ell^n] \end{array}$$

commutes. Therefore, the actions ψ_n induce an action of G_K on $T_\ell(E)$ and since $T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$, this corresponds to a 2-dimensional ℓ -adic representations

$$\psi_{E,\ell} : G_K \longrightarrow \text{GL}_2(\mathbb{Z}_\ell) \subseteq \text{GL}_2(\mathbb{Q}_\ell).$$

We will also denote from now on $\rho_{E,\ell}$ to be the dual representation of $\psi_{E,\ell}$. For technical reasons we will not discuss, the L -function is typically constructed using the later ones.

Remark 3.9. The representation above does indeed satisfy the conditions in Remark 3.4. In particular, given any $n \geq 1$, the field $F_n := K(E[\ell^n])$ is a finite extension of K since it is obtained by attaching finitely many algebraic numbers. By construction, $\text{Gal}(\bar{K}/F_n)$ acts trivially on $E[\ell^n]$ and thus $\rho_{E,\ell}(g) \equiv \text{Id} \pmod{\ell^n}$ for all $g \in \text{Gal}(\bar{K}/F_n)$.

Of course, the above construction can be followed by any rational prime ℓ , and this gives a family $\{\rho_{E,\ell}\}_\ell$. To build an L -function as described in the section above, we would need this family to be weakly compatible. Thankfully, this and much more is true, and the next theorem collects the relevant results.

Theorem 3.10. *Let E be an elliptic curve over a number field K and $\rho_{E,\ell}$ be the dual representation on $T_\ell(E)$. For every finite place \mathfrak{p} of K , let $\kappa_{\mathfrak{p}}$ be the residue field of $K_{\mathfrak{p}}$, $q_{\mathfrak{p}} = |\kappa_{\mathfrak{p}}|$ and $a_{\mathfrak{p}} = 1 + q_{\mathfrak{p}} - |\tilde{E}(\kappa_{\mathfrak{p}})|$. Then for any \mathfrak{p} not dividing ℓ ,*

$$\begin{aligned} P_{\mathfrak{p}}(\rho_{E,\ell}, T) &= 1 - a_{\mathfrak{p}}T + q_{\mathfrak{p}}T^2, & \text{if } E/K_{\mathfrak{p}} \text{ has good reduction,} \\ &= 1 - T, & \text{if } E/K_{\mathfrak{p}} \text{ has split multiplicative reduction,} \\ &= 1 + T, & \text{if } E/K_{\mathfrak{p}} \text{ has non-split multiplicative reduction,} \\ &= 1, & \text{if } E/K_{\mathfrak{p}} \text{ has additive reduction.} \end{aligned}$$

In particular, for any ℓ, ℓ' not divisible by \mathfrak{p} ,

$$P_{\mathfrak{p}}(\rho_{E,\ell}, T) = P_{\mathfrak{p}}(\rho_{E,\ell'}, T),$$

and so $\{\rho_{E,\ell}\}$ is a weakly compatible system of ℓ -adic representations.

This allows us to define the L -function of an elliptic curve as above.

Definition 3.11. Let E be an elliptic curve over K . Then the L -function attached to E is

$$L(E/K, s) = L(\{\rho_{E,\ell}\}, s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{P_{\mathfrak{p}}(\rho_{E,\ell}, N(\mathfrak{p})^{-s})}$$

3.4 Artin Twists of L-functions of Elliptic Curves

We have already seen that given an elliptic curve over a number field K , one can construct the L -function $L(E/K, s)$. However, given an Artin representation ρ over K , it is possible to attach more analytic objects, with remarkable arithmetic properties. We outline the main results below, without proofs. **Insert here relevant reference.**

Fix some number field K , an elliptic curve E over K and an Artin representation ρ . Then, similar to the previous section, it is possible to show that $\{\rho_{E,\ell} \otimes \rho\}_{\ell}$ is also a weakly compatible system of ℓ -adic representations. The corresponding L -function

$$L(E, \rho, s) = L(\{\rho_{E,\ell} \otimes \rho\}, s)$$

is denoted as the **Artin-twist** of $L(E, s)$ by ρ . These objects have remarkable (both proven and conjectural) properties that we describe now.

Theorem 3.12 (Artin Formalism). *Let E be an elliptic curve over a number field K .*

1. *For Artin representations ρ_1, ρ_2 over K ,*

$$L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s) \quad \text{and} \quad L(E/K, \rho_1 \oplus \rho_2, s) = L(E/K, \rho_1, s)L(E/K, \rho_2, s)$$

2. *If L/K is a finite extension and ρ is an Artin representation over L , then $\text{Ind}_{L/K} \rho$ is an Artin representation over K and*

$$L(\rho, s) = L(\text{Ind}_{L/K} \rho, s) \quad \text{and} \quad L(E/L, \rho, s) = L(E/L, \text{Ind}_{L/K} \rho, s).$$

3. *If L/K is a finite extension as above and*

$$\text{Ind}_{L/K} \mathbb{1} \cong \bigoplus_i \rho_i,$$

then

$$L(E/L, s) = \prod_i L(E/K, \rho_i, s).$$

Furthermore, as mentioned after Remark 3.4, by fixing some basis of V , any Artin representation ρ can be viewed as a representation $\rho : G_K \rightarrow \text{GL}_n(F)$ for some number field F . The smallest such field is the **field of values** of ρ and denoted by $\mathbb{Q}(\rho)$. Any $\sigma \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ induces a homomorphism $\sigma : \text{GL}_n(\mathbb{Q}(\rho)) \rightarrow \text{GL}_n(\mathbb{Q}(\rho))$ and also a map which is another Artin representation, denoted as the twist of ρ by σ .

Conjecture 3.13 (Galois Equivariance of L-Twists). I need to check the precise statement of this result. This may need to come after the discussion on BSD.

4 Birch and Swinnerton-Dyer and Other Conjectures

The Birch-Swinnerton-Dyer conjecture classically provides a connection between the arithmetic of elliptic curves and their L -functions. We have already investigated the construction and main results of the ‘ L -functions side’, and now we turn our attention to statement of the conjecture and towards understanding the arithmetic terms present in the conjecture. Some arithmetic terms present in the conjecture are easier to describe if the elliptic curve has a global minimal Weierstrass equation. Since we will be mainly interested in elliptic curves over \mathbb{Q} , and in view of Proposition 2.7, we will assume throughout that E is an elliptic curve over \mathbb{Q} with **global minimal Weierstrass equation**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, and let

$$w = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

be the associated **global minimal differential**.

4.1 BSD and the Arithmetic Terms

The Birch-Swinnerton-Dyer conjecture states the following.

Conjecture 4.1 (BSD). Let E be an elliptic curve defined over a number field K . Then

BSD1. The rank of the Mordell-Weil group of E over K equals the order of vanishing of the L -function; that is,

$$\text{ord}_{s=1} L(E/K, s) = \text{rk } E/K.$$

BSD2. The leading term of the Taylor series at $s = 1$ of the L -function is given by

$$\lim_{s \rightarrow 1} \frac{L(E/K, s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_+(E)^{r_1+r_2} |\Omega_-(E)|^{r_2}} = \frac{\text{Reg}_{E/K} |\text{III}_{E/K}| C_{E/K}}{|E(K)_{\text{tors}}|^2}. \quad (6)$$

We briefly explore the arithmetic invariants that appear as part of the statement of BSD2. Some of these invariants depend only on the number field K . These are the discriminant Δ_K of K and the numbers r_1 and r_2 , corresponding to the number of real and complex embeddings of K . A basic formula states that if $n = [K : \mathbb{Q}]$, then $r_1 + 2r_2 = n$.

The other factors are arithmetic values related to the elliptic curve E . Importantly, here we assume that E has rational coefficients.

1. **Periods:** For elliptic curves E defined over \mathbb{Q} , there is a conjugation map $E \rightarrow E$, $P \mapsto \bar{P}$. We then define $E(\mathbb{C})^+ = \{P \in E : \bar{P} = P\} = E(\mathbb{R})$ and $E(\mathbb{C})^- = \{P \in E : \bar{P} = -P\}$. Then the \pm -periods of E are

$$\Omega_+(E) = \int_{E(\mathbb{C})^+} \omega \quad \text{and} \quad \Omega_-(E) = \int_{E(\mathbb{C})^-} \omega,$$

and orientation chosen so that $\Omega_+(E) \in \mathbb{R}_{>0}$ and $\Omega_-(E) \in i\mathbb{R}_{>0}$.

2. **Torsion:** $|E(K)_{\text{tors}}|$ is the size of the torsion subgroup of $E(K)$.

3. **Regulator:** To properly define the regulator one needs to carefully construct the canonical height $\hat{h} : E(\bar{K}) \rightarrow \mathbb{R}^+$, which roughly evaluates the ‘arithmetic complexity’ of a given point $P \in E(\bar{K})$. We refer the reader to [Sil09, Chapter VIII: §4, §5, §6 and §9] for a complete discussion of this topic. This map satisfies many important properties (as listed in [Sil09, Chapter VIII, Theorem 9.3]), among which is the fact that \hat{h} is a quadratic form; in particular, the pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) &\longrightarrow \mathbb{R} \\ \langle P, Q \rangle &= \hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q) \end{aligned}$$

is bilinear. Then the regulator is the volume of $E(K)/E(K)_{\text{tors}}$ computed using the quadratic form \hat{h} . In other words, let P_1, \dots, P_r be generators of the group $E(K)/E(K)_{\text{tors}}$. Then

$$\text{Reg}_{E/K} = \det(\langle P_i, P_j \rangle)_{1 \leq i, j \leq r}$$

if $r \geq 1$ and $\text{Reg}_{E/K} = 1$ if $r = 0$.

4. **Tate-Shafarevich group:** This is the most mysterious group and it is commonly defined using Galois cohomology as

$$\text{III}_{E/K} = \ker \left[H^1(K, E) \rightarrow \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E) \right],$$

where $H^1(F, E) := H^1(G_F, E(\bar{F}))$ and the implicit map is induced by the inclusions $G_{K_{\mathfrak{p}}} \hookrightarrow G_K$. One can interpret $H^1(F, E)$ as ‘homogeneous spaces’ of E over K up to equivalence. A homogeneous space over K is trivial if and only if it has a K -rational point, so a non-trivial element of $\text{III}_{E/F}$ is a homogeneous space that has points locally in every $K_{\mathfrak{p}}$ but has no K -rational point.

5. **Local data:** The term $C_{E/K}$ is defined in terms of local data as

$$C_{E/K} = \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/K) \left| \frac{\omega}{\omega_{\mathfrak{p}}^{\min}} \right|_{\mathfrak{p}} = \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/K) \left| \frac{\Delta_{E, \mathfrak{p}}^{\min}}{\Delta_E} \right|_{\mathfrak{p}}^{\frac{1}{12}}. \quad (7)$$

where $c_{\mathfrak{p}}(E/K)$ are the Tamagawa numbers of E/K at a prime \mathfrak{p} of K , as discussed in §2.2. To discuss the second term, fix some finite place \mathfrak{p} of K and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. By assumption, Δ_E is a minimal discriminant at p , but this may not be a minimal discriminant at \mathfrak{p} if $K_{\mathfrak{p}}/\mathbb{Q}_p$ is ramified, and we denote $\Delta_{E, \mathfrak{p}}^{\min}$ as the minimal discriminant of E/K at \mathfrak{p} .

We remark that if p is unramified at K , or if E has semistable reduction at p , then $\Delta_{E, \mathfrak{p}}^{\min} = \Delta_E$ and the second term vanishes.

We will spend some time computing the local terms for families of elliptic curves, so we introduce some more notation that will be used throughout.

Notation 4.2. Let E be an elliptic curve defined over \mathbb{Q} and let F/K be a finite extension of number fields. For each finite place \mathfrak{p} of K , we write

$$T_{\mathfrak{p}|K}(E/F) = \prod_{\mathfrak{P}|\mathfrak{p}} c_{\mathfrak{P}}(E/F) \quad \text{and} \quad D_{\mathfrak{p}|K}(E/F) = \prod_{\mathfrak{P}|\mathfrak{p}} \left| \frac{\Delta_{E, \mathfrak{P}}^{\min}}{\Delta_E} \right|_{\mathfrak{P}}^{\frac{1}{12}},$$

where the product ranges over primes \mathfrak{P} of F dividing p . We also write

$$C_{\mathfrak{p}|K}(E/F) = T_{\mathfrak{p}|K}(E/F) D_{\mathfrak{p}|K}(E/F).$$

An immediate consequence of this notation is the fact that $C_{E/F} = \prod_{\mathfrak{p}} C_{\mathfrak{p}|p}(E/F)$. Observe that if E has good reduction over \mathfrak{p} , then $C_{\mathfrak{p}|p}(E/F) = 1$ for any finite extension F of K .

Notation 4.3. If $G = \text{Gal}(F/\mathbb{Q})$ then we define functions $T_{\mathfrak{p}|p}$, $D_{\mathfrak{p}|p}$ and $C_{\mathfrak{p}|p}$ on $B(G)$ by

$$T_{\mathfrak{p}|p}(H) = T_{\mathfrak{p}|p}(E/F^H), \quad D_{\mathfrak{p}|p}(H) = D_{\mathfrak{p}|p}(E/F^H), \quad C_{\mathfrak{p}|p}(H) = C_{\mathfrak{p}|p}(E/F^H).$$

Note that if H, H' are conjugate then $F^H, F^{H'}$ are isomorphic, and so the values of these functions are constant on conjugate subgroups, hence they are well-defined. Let $C: B(G) \rightarrow \mathbb{Q}^\times$ be given by $C: H \mapsto C_{E/F^H}$.

Note that $C_{\mathfrak{p}|p}$ is a D_p -local function. Indeed, suppose $D_p = \text{Gal}(F_w/\mathbb{Q}_p)$, where F_w denotes the completion of F with respect to a place w lying above p . Recall the notation that for a number field K and place v , $C_v(E/K) = c_v(E/K) \cdot |\omega/\omega_v^{\min}|_v$ **put this somewhere....** We use the same notation if K is a local field (then the v subscript holds no meaning). One has

$$C_{\mathfrak{p}|p} = (D_p, C_v)$$

where C_v is a function on $B(D_p)$ sending $H \mapsto C_v(E/F_w^H)$.

We remark that the way we have organised the terms in (6) is not arbitrary, and in fact we give specific notation to both sides of the equation.

Notation 4.4. Let E/\mathbb{Q} be a number field and K a number field. We define

$$\mathcal{L}(E/F) = \lim_{s \rightarrow 1} \frac{L(E/K, s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_+(E)^{r_1+r_2} |\Omega_-(E)|^{r_2}}$$

and

$$\text{BSD}(E/F) = \frac{\text{Reg}_{E/K} |\text{III}_{E/K}| C_{E/K}}{|E(K)_{\text{tors}}|^2}.$$

4.2 A BSD Analogue for Artin Twists

A natural question to ask at this point is whether there is a conjectural analogue to the above for the Artin twists of L -functions. The analogue of BSD 1 is known in this case, which is directly compatible with Artin formalism.

Conjecture 4.5 (BSD1 for Twists). Let E/\mathbb{Q} be an elliptic curve, ρ an Artin representation and K any Galois extension over \mathbb{Q} such that ρ factors through $G = \text{Gal}(K/\mathbb{Q})$. Then

$$\text{ord}_{s=1} L(E, \rho, s) = \langle \rho, E(K)_{\mathbb{C}} \rangle_G.$$

Unfortunately, a conjectural analogue for BSD 2 is not known. The problem is the lack of an analogue for the term $\text{BSD}(E/F)$ as above. However, there is indeed an important analogue of the term $\mathcal{L}(E/F)$ in this setting.

Notation 4.6. Let E/\mathbb{Q} be an elliptic curve and ρ an Artin representation over \mathbb{Q} . We define

$$\mathcal{L}(E, \rho) = \lim_{s \rightarrow 1} \frac{L(E, \rho, s)}{(s-1)^r} \cdot \frac{\sqrt{\mathfrak{f}_\rho}}{\Omega_+(E)^{d^+(\rho)} |\Omega_-(E)|^{d^-(\rho)} \omega_\rho},$$

where $r = \text{ord}_{s=1} L(E, \rho, s)$ is the order of the zero at $s = 1$, \mathfrak{f}_ρ is the conductor of ρ , and $d^\pm(\rho)$ are the dimensions of the ± 1 -eigenspaces of complex conjugation in its action on ρ .

Even though the precise conjectural expression of the $\text{BSD}(E, \rho)$ is not known, they conjecturally satisfy many important properties. The next conjecture lists some of these properties.

Conjecture 4.7. [DEW21, Conjecture 4] Let E/\mathbb{Q} be an elliptic curve. For every Artin representation ρ over \mathbb{Q} there is an invariant $\text{BSD}(E, \rho) \in \mathbb{C}^\times$ with the following properties. Let ρ and τ be Artin representations and K a finite extension of \mathbb{Q} such that ρ and τ factor through $\text{Gal}(K/\mathbb{Q})$.

- C1.** $\text{BSD}(E/F) = \text{BSD}(E, \text{Ind}_{F/\mathbb{Q}} \mathbb{1})$ for a number field F (and $\text{III}_{E/F}$ is finite).
- C2.** $\text{BSD}(E, \rho \oplus \tau) = \text{BSD}(E, \rho) \text{BSD}(E, \tau)$.
- C3.** $\text{BSD}(E, \rho) = \text{BSD}(E, \rho^*) \cdot (-1)^r \omega_{E, \rho} \omega_\rho^{-2}$, where $r = \langle \rho, E(K)_\mathbb{C} \rangle$.
- C4.** If ρ is self-dual, then $\text{BSD}(E, \rho) \in \mathbb{R}$ and $\text{sign } \text{BSD}(E, \rho) = \text{sign } \omega_\rho$.
If $\langle \rho, E(K)_\mathbb{C} \rangle = 0$, then moreover:
- C5.** $\text{BSD}(E, \rho) \in \mathbb{Q}(\rho)^\times$ and $\text{BSD}(E, \rho^g) = \text{BSD}(E, \rho)^g$ for all $g \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.
- C6.** If ρ is a non-trivial primitive Dirichlet character of order d , and either the conductors of E and ρ are coprime or E is semistable and has no non-trivial isogenies over \mathbb{Q} , then $\text{BSD}(E, \rho) \in \mathbb{Z}[\zeta_d]$.

The great advantage of the above conjecture is that it is free of L -functions since only the ‘arithmetic’ $\text{BSD}(E/F)$ terms appear. Conditional to some well-known conjectures, Conjecture 4.7 holds.

Theorem 4.8. [DEW21, Theorem 5] *Conjecture 4 holds with $\text{BSD}(E, \rho) = \mathcal{L}(E, \rho)$ assuming the analytic continuation of L -functions $L(E, \rho, s)$, their functional equation, the Birch-Swinnerton-Dyer conjecture, Deligne’s period conjecture, Stevens’s Manin constant conjecture for E/\mathbb{Q} and the Riemann hypothesis for $L(E, \rho, s)$.*

5 Predicting Positive Rank

At this point, we aim to study the arithmetic applications of Conjecture 4.7. Some of these applications are already studied in [DEW21, §3], and it allows to predict non-trivial interplay of the primary parts of the Tate-Shafarevich group of families of elliptic curves, non-trivial Selmer groups and even positive rank. All of these results appear not to be tractable with other common current methods.

The most interesting case is the prediction of positive rank for families of elliptic curves on certain number fields. We illustrate the proof of the main result that predict positive rank conditional on Conjecture 4.7. Let F be a Galois extension over \mathbb{Q} and let $G = \text{Gal}(F/\mathbb{Q})$. Let E/\mathbb{Q} be an elliptic curve and let ρ be an irreducible representation over G , which we view as an Artin representation. Then the representation

$$\bigoplus_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}$$

has \mathbb{Q} -valued character and therefore there is some $m \geq 1$ and subfields F_i, F'_j such that

$$\left(\bigoplus_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} \right)^m \oplus \bigoplus_j \text{Ind}_{F'_j/\mathbb{Q}} \mathbb{1} = \bigoplus_i \text{Ind}_{F_i/\mathbb{Q}} \mathbb{1}.$$

Assume that $\text{rk } E/F = 0$ so that in particular $\langle \rho, E(F)_{\mathbb{C}} \rangle_G = 0$. Therefore (C1), (C2) and (C5) from Conjecture 4.7 imply that

$$\frac{\prod_i \text{BSD}(E/F_i)}{\prod_j \text{BSD}(E/F'_j)} = \frac{\prod_i \text{BSD}(E, \text{Ind}_{F_i/\mathbb{Q}} \mathbb{1})}{\prod_j \text{BSD}(E, \text{Ind}_{F'_j/\mathbb{Q}} \mathbb{1})} = \left(\prod_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \text{BSD}(E, \rho^{\mathfrak{g}}) \right)^m \quad (8)$$

and the right-hand side is clearly the m -th power of a norm of an element in $\mathbb{Q}(\rho)$.

The product of BSD terms on the LHS of (8) involve regulators, the torsion subgroups, the Tate-Shafarevich groups and the terms $C_{E/F}$ which are the product of local factors. Under the assumption that $\text{rk } E/F = 0$, the regulators vanish from the product. In general, it is very difficult to deal with the size of the Tate-Shafarevich group for families of elliptic curves, and therefore very difficult to know if the LHS is an m -th power the norm of an element in $\mathbb{Q}(\rho)$. However, not all hope is lost, since Cassel's proved the following.

Theorem 5.1. *Let E be an elliptic curve over a number field K . If $\text{III}_{E/K}$ is finite, then $|\text{III}_{E/K}|$ is a square.*

Rational squares are not necessarily the norms of general number fields, but they are always norms of quadratic number fields. Furthermore, if $\mathbb{Q}(\sqrt{D})$ is a quadratic subfield of $\mathbb{Q}(\rho)$, then the RHS of (8) is also the norm of an element of $\mathbb{Q}(\sqrt{D})$ and a rational square if m is even. Under the assumption of finiteness of III , we know that $|\text{III}_{E/F}|$ and $|E(F)_{\text{tors}}|^2$ are rational squares and therefore norms of $\mathbb{Q}(\sqrt{D})$. The only remaining terms on the LHS of (8) are the product of local factors C_{E/F_i} and C_{E/F'_j} . We have therefore proven the following.

Theorem 5.2. *[DEW21, Theorem 33] Suppose Conjecture 4.7 holds. Let E/\mathbb{Q} be an elliptic curve, F/\mathbb{Q} a finite Galois extension with Galois group G , $\rho \in \text{R}(G)$ and*

$$\left(\bigoplus_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} \right)^m = \bigoplus_i \text{Ind}_{F_i/\mathbb{Q}} \mathbb{1} \ominus \bigoplus_j \text{Ind}_{F'_j/\mathbb{Q}} \mathbb{1}$$

for some $m \geq 1$ and subfields $F_i, F'_j \subseteq F$. If either $\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$ is not a norm from some quadratic subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, or if it is not a rational square when m is even, then E has a point of infinite order over F .

This is a remarkable result, since it can predict positive rank of general families of elliptic curves based solely on local data. In later sections, we will aim to show that the product of local factors is indeed a norm in quadratic subextension of the field of values, and the following notation, which expands on Notation 4.2 will be useful.

Notation 5.3. Let F, ρ, m and the fields F_i, F'_j be as in Theorem 5.2. Let K be a subfield of F and \mathfrak{p} a prime of K . Then we define

$$\text{contr}_\rho(\mathfrak{p}) = \frac{\prod'_i C_{\mathfrak{p}|p}(F_i)}{\prod'_j C_{\mathfrak{p}|p}(F'_j)},$$

where the restricted product is taken over all F_i and F'_j containing K . We remark that

$$\frac{\prod'_i C_{E/F_i}}{\prod'_j C_{E/F'_j}} = \prod_p \text{contr}_\rho(p)$$

where the product runs over all rational primes. Our strategy is to calculate all $\text{contr}_\rho(p)$ locally first, to then multiply them together. We recall once again that if p is a prime of good reduction of the elliptic curve, then $\text{contr}_\rho(p) = 1$, so we will only care about the primes of bad reduction.

Remark 5.4. We rephrase Theorem 5.2 in the language introduced in §1.3. Replacing ρ by the sum of its conjugates by elements of $\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{D}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{D})$. Note that this does not affect the order of ρ in $\hat{C}(G)$, nor the set of ρ -relations (since $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ is unchanged).

Let Θ be a ρ -relation with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. Let $C: \text{B}(G) \rightarrow \mathbb{Q}^\times$ be the function sending $H \mapsto C_{E/F^H}$. The theorem then states that, if Θ is not a norm relation for C when m is odd, or if $C(\Theta) \notin \mathbb{Q}^{\times 2}$ for m even, then $\text{rk } E/F > 0$.

5.1 Examples

We now present some examples where we use Theorem 5.2 to force positive rank. Throughout we will consider an elliptic curve E defined over \mathbb{Q} , and a finite Galois extension F/\mathbb{Q} with Galois group $G = \text{Gal}(F/\mathbb{Q})$. As described in Remark 5.4, the strategy is to find $\rho \in \text{R}(G)$ and a ρ -relation $\Theta \in \text{B}(G)$ such that $C(\Theta)$ is either not a norm from a quadratic subfield of $\mathbb{Q}(\rho)$, or not a rational square, as appropriate.

Remark 5.5 (Taking quotients). Let E, F, G be as above. Consider $H \leq G$, and $N \triangleleft G$ such that $N \leq H$. Then $C(H) = C_{E/F^H}$ is equal to $C(NH/N) = C_{E/L^{NH/N}}$ (viewing C as a function on $\text{B}(G/N)$) as the fields F^H and $L^{NH/N}$ are isomorphic.

Consider $\rho \in \text{R}(G)$ with $N \leq \ker \rho$, so that $\mathbb{Q}(\rho) = \mathbb{Q}(\rho^N)$. Then, if $\Theta = \sum_i n_i H_i \in \text{B}(G)$ with $N \leq H_i$ for all i , it follows that $N \cdot \Theta/N = \Theta/N$ being a norm relation for $C: \text{B}(G/N) \rightarrow \mathbb{Q}^\times$ implies that Θ is a norm relation for $C: \text{B}(G) \rightarrow \mathbb{Q}^\times$.

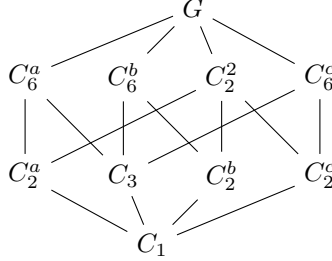
We will need to be able to count primes and compute residue degrees in intermediate extensions of F/\mathbb{Q} , which is described by the following result.

Proposition 5.6 (Counting primes and ramification degrees). *Consider a prime $p \in \mathbb{Q}$ and decomposition and inertia groups $D_p, I_p \leq G$. Let $H \leq G$.*

1. The number of primes above p in F^H is given by the number of orbits of D_p on $H \backslash G$, where D_p acts by $d(Hg) = Hgd^{-1}$ for $d \in D_p$. Equivalently it is $|H \backslash G / D_p|$.
2. The inertia degree of a prime \mathfrak{P} above p in F^H is the size of the I_p sub-orbits on $H \backslash G$.

Proof. [reference somewhere....](#) □

Example 5.7 (Brauer relation forces growth). Let $G = C_2 \times C_6$, with subgroup diagram



There is a Brauer relation coming from the $C_2 \times C_2$ -quotient, given by

$$\Psi = C_3 - C_6^a - C_6^b - C_6^c + 2G.$$

Consider an order 6 character ρ_a of G with C_2^a in its kernel. This has $\mathbb{Q}(\rho_a) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Then

$$\Theta = C_2^a - C_6^a - C_2^2 + G$$

is a ρ_a -relation, with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho_a)/\mathbb{Q}}(\rho_a)$.

Let E/\mathbb{Q} be a semistable elliptic curve and F/\mathbb{Q} an abelian extension with $G = \text{Gal}(F/\mathbb{Q})$. We claim that $C(\Theta) \in N_{\mathbb{Q}(\rho_a)/\mathbb{Q}}(\mathbb{Q}(\rho_a)^\times)$, for all such E . Since each subgroup in Θ contains C_2^a , we have that $C(\Theta)$ equals $C(\Theta/C_2^a)$ where $\Theta/C_2^a \in \text{B}(G/C_2^a) = \text{B}(C_6)$. Now Θ/C_2^a is a χ_6 -relation, where $\chi_6 = \rho_a^{C_2^a}$ is a faithful order 6 character of C_6 , with $\mathbb{Q}(\chi_6) = \mathbb{Q}(\rho_a)$. But for cyclic groups we always get norm relations; by Theorem 6.1, $C(\Theta/C_2^a) \in N_{\mathbb{Q}(\rho_a)/\mathbb{Q}}(\mathbb{Q}(\rho_a)^\times)$.

On the other hand, $C(\Theta + \Psi) = C(\Theta)C(\Psi)$ is not always a norm. Indeed suppose E/\mathbb{Q} has split multiplicative reduction at a prime p with $D_p = G$, $I_p = C_6^b$ (assuming tamely ramified, one can take a prime p such that $6 \mid p^2 - 1$, e.g. $p = 5$). Let $\text{ord}_p(\Delta_E) = n$. Then there is only one prime above p in each subfield, and the Tamagawa number at a prime \mathfrak{P} above p in F^H is given by $c_{\mathfrak{P}}(E/F^H) = e_{\mathfrak{P}/p}n$. Suppose E has good reduction at all other primes ([or be more lenient](#)). Then

$$C(\Theta) = \frac{(6n)(n)}{(2n)(3n)} = 1, \quad C(\Psi) = \frac{(2n)(n)^2}{(2n)(n)(2n)} = \frac{1}{2} \cdot \square.$$

Thus $C(\Theta + \Psi) = \frac{1}{2} \pmod{\mathbb{Q}^{\times 2}}$, but 2 is not a norm in $\mathbb{Q}(\sqrt{-3})$. Hence one must have $\text{rk } E/F > 0$.

Example 5.8 (Semi-direct product). Let q_1, q_2 be odd primes with $q_1, q_2 \equiv 1 \pmod{4}$. Consider $G = C_{q_1 q_2} \rtimes C_4$ with $C_{q_1 q_2} \triangleleft G$ and C_4 acting faithfully on $C_{q_1 q_2}$, C_{q_1} , and C_{q_2} . This is a semidirect product by an abelian group, and its irreducible representations are described in [Ser77, Chapter 8, §8.2]. There is an irreducible representation $\rho \in \text{R}(G)$, obtained by inducing a linear order $q_1 q_2$ faithful representation from $C_{q_1 q_2}$. Thus ρ is of degree 4 and $\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_{q_1 q_2})^{C_4}$. Then ρ has $\frac{(q_1-1)(q_2-1)}{4}$ Galois conjugates in $\text{R}(G)$, and so $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ is of dimension $4 \cdot \frac{(q_1-1)(q_2-1)}{4}$. There is a ρ -relation

$$\Theta = C_4 - (C_{q_1} \times C_4) - (C_{q_2} \times C_4) + G, \quad \mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho).$$

Suppose that E/\mathbb{Q} is semistable. Recall that $C(\Theta) = \prod_p T_{\mathfrak{p}|p}(\Theta)$, where $T_{\mathfrak{p}|p}$ depends on D_p , I_p , the decomposition group and inertia group at p respectively. Suppose that E/\mathbb{Q}_p has split multiplicative reduction. Ranging over all possible D_p and I_p , a case by case analysis yields that $T_{\mathfrak{p}|p}(\Theta)$ is non-square only when $D_p = C_{q_1} \rtimes C_4$ or $C_{q_2} \rtimes C_4$ (and I_p is non-trivial).

For example, let $D_p = C_{q_1} \rtimes C_4$, $I_p = C_{q_1}$.

- The action of D_p on $C_4 \backslash G$ yields 1 orbit of size C_{q_1} (the orbit of the identity) and $\frac{q_2-1}{4}$ orbits of size $4q_1$ (coming from C_4 acting faithfully on C_{q_2}). The size of the inertia sub-orbits is q_1 . Hence $T_{\mathfrak{p}|p}(C_4) = (q_1 n)^{1+\frac{q_2-1}{4}}$.
- The action of D_p on $C_{q_1} \rtimes C_4 \backslash G$ yields the same number of orbits as above, but now the action of $C_{q_1} \leq D_p$ is trivial and the size of the inertia sub-orbits are all 1, so that $T_{\mathfrak{p}|p}(C_{q_1} \times C_4) = n^{1+\frac{q_2-1}{4}}$.
- The action of D_p on $C_{q_2} \rtimes C_4 \backslash G$ yields one orbit of size q_1 , with the inertia sub-orbit also of size q_1 , hence $T_{\mathfrak{p}|p}(C_{q_2} \times C_4) = q_1 n$.

Hence

$$T_{\mathfrak{p}|p}(\Theta) = \frac{(q_1 n)^{1+\frac{q_2-1}{4}}(n)}{(n)^{1+\frac{q_2-1}{4}}(q_1 n)} = q_1^{\frac{q_2-1}{4}}.$$

By symmetry, taking $D_p = C_{q_2} \rtimes C_4$, $I_p = C_{q_2}$, one has $T_{\mathfrak{p}|p}(\Theta) = q_2^{\frac{q_1-1}{4}}$.

So let E/\mathbb{Q} have split multiplicative reduction at p with $D_p = C_{q_1} \rtimes C_4$, $I_p = C_{q_1}$, and good reduction at all other primes. Suppose that $q_2 \not\equiv 1 \pmod{8}$ and that $\left(\frac{q_1}{q_2}\right) = -1$. Then $\mathbb{Q}(\sqrt{q_1 q_2}) \subset \mathbb{Q}(\rho)$ but $T_{\mathfrak{p}|p}(\Theta) \notin N_{\mathbb{Q}(\sqrt{q_1 q_2})/\mathbb{Q}}(\mathbb{Q}(\sqrt{q_1 q_2})^\times)$. One has $T_{\mathfrak{p}|p}(\Theta) \equiv q_1 \pmod{\mathbb{Q}^{\times 2}}$, but q_1 is not the norm of an element of $\mathbb{Q}(\sqrt{q_1 q_2})$. If it were, then there would exist $x, y, z \in \mathbb{Z}$ such that $z^2 q_1 = x^2 - q_1 q_2 y^2$. Looking mod q_2 this implies that $q_1 = \square \pmod{q_2}$, a contradiction. Thus $\text{rk } E/F > 0$ by Theorem 5.2. For example, one can take $q_1 = 17$, $q_2 = 5$.

This rank growth is predicted by root number computations also, however. Assume that F/\mathbb{Q} is totally real. Then $w(E/F^H) = (-1)^{[F^H:\mathbb{Q}] + |H \backslash G/D_p|}$. Thus **I need to introduce these somewhat somewhere**

- $w(E/\mathbb{Q}) = (-1)^2 = 1$,
- $w(E/F^{C_4}) = (-1)^{q_1 q_2} (-1)^{1+\frac{q_2-1}{4}} = (-1)^{\frac{q_2-1}{4}}$,
- $w(E/F^{C_{q_1} \rtimes C_4}) = (-1)^{q_2} (-1)^{1+\frac{q_2-1}{4}} = (-1)^{\frac{q_2-1}{4}}$,
- $w(E/F^{C_{q_2} \rtimes C_4}) = (-1)^{q_1} (-1) = 1$.

Therefore if $q^2 \not\equiv 1 \pmod{8}$, we must have $\text{rk } E/F^{C_4}, \text{rk } E/F^{C_{q_1} \rtimes C_4} > 0$, so $\text{rk } E/F > 0$. Note that we needed to additionally assume that $\left(\frac{q_1}{q_2}\right) = -1$, but the root number computation doesn't need this assumption. For example, if $q_1 = 29$, $q_2 = 5$, then $5 = (\frac{15}{4})^2 - 29 * 5(\frac{1}{4})^2$ is a norm from $\mathbb{Q}(\sqrt{5 \cdot 29})$, so we can't use Theorem 5.2.

Example 5.9 (Additive reduction example).

6 Consistency cases with BSD

As we discussed in the previous section, our motivation is to use Theorem 5.2 to predict points of infinite order for families of elliptic curves. However, in this section we prove that in several cases the theorem will never make such a prediction. In other words, in such cases, the product

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$$

is always a norm for every subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$.

6.1 Cyclic Extensions

In this subsection we prove the following.

Theorem 6.1. *Let E/\mathbb{Q} be a semistable elliptic curve and let F be a finite cyclic Galois extension \mathbb{Q} so that $\text{Gal}(F/\mathbb{Q}) = C_d$ for some $d \geq 2$. Let χ be a faithful character of C_d (so that $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta_d)$), and let $F_i, F'_j \subseteq F$ be such that*

$$\bigoplus_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \chi^{\mathfrak{g}} = \bigoplus_i \text{Ind}_{F_i/\mathbb{Q}} \mathbf{1} \ominus \bigoplus_j \text{Ind}_{F'_j/\mathbb{Q}} \mathbf{1}.$$

Then for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_d)$,

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$$

is a norm of $\mathbb{Q}(\sqrt{D})$. Moreover, the contribution is always the square of rational number unless $d = 2^n, p^n, 2p^n$ for some odd prime p .

The first step in proving Theorem 6.1 is to show that the fields F_i, F'_j exist, and to give a precise description. Recall that for each $k \mid d$ the cyclic group C_d has one unique subgroup of order k , which is of course also cyclic. Therefore, for each $k \mid d$, there is one unique subfield L_k of F of degree k over \mathbb{Q} which is also cyclic. Under the Galois correspondence, this field corresponds to the subgroup $H_k = \text{Gal}(F/L_k) = C_{d/k}$.

To give the required description, we recall that the Möbius function μ is the function supported on the square-free integers, and $\mu(n) = (-1)^s$ whenever n is square free and s is the number of prime factors of n .

Lemma 6.2. *Let E/\mathbb{Q} , F and χ be as in Theorem 6.1. Writing characters of C_d additively, we have that*

$$\sum_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})} \chi^{\mathfrak{g}} = \sum_{k \mid d} \mu(d/k) \text{Ind}_{L_k/\mathbb{Q}} \mathbf{1}. \quad (9)$$

Furthermore, such an expression is unique.

Remark 6.3. This lemma has an important consequence. Given an integer $d \geq 2$, let $\text{rad}(d) = \prod_{p \mid d} p$ be the radical of d , and let $K = L_{d/\text{rad}(d)}$ be the unique subfield of F such that $[F : K] = \text{rad}(d)$. For $k \mid d$, $\mu(d/k) \neq 0$ precisely when $[K : \mathbb{Q}] = \frac{d}{\text{rad}(d)} \mid k$ and therefore the fields appearing in the right hand side of (9) are the fields L_k satisfying $K \subseteq L_k \subseteq F$.

Following this observation, we will compute the product of the local factors locally for each finite place \mathfrak{p} of K and the places above it in the other fields $L_k \supseteq K$. To that objective, the following notation will be useful.

Notation 6.4. Let E/\mathbb{Q} , F and χ be as in Theorem 6.1, and let L_k and K be as in Remark 6.3. For a finite place \mathfrak{p} of K , we write

$$\text{contr}_\chi(\mathfrak{p}) = \prod_{\frac{d}{\text{rad}(d)} | k|d} C_{\mathfrak{p}|\mathfrak{p}}(L_k/K)^{\mu(d/k)} = \prod_{k|d} C_{\mathfrak{p}|\mathfrak{p}}(L_k/K)^{\mu(d/k)}$$

where the terms in the product are defined as in Notation 4.2.

An immediate consequence of the above definition is the fact that

$$\prod_{k|d} (C_{E/L_k})^{\mu(d/k)} = \prod_{\mathfrak{p}} \text{contr}_\chi(\mathfrak{p}), \quad (10)$$

and therefore we can calculate the product of local terms **locally**, one prime \mathfrak{p} at a time.

We divide the proof of Theorem 6.1 into two cases: odd and even cyclic extensions. The main idea in both cases is to simplify the general case into smaller cases where we can directly compute $\text{contr}_\chi(\mathfrak{p})$ for each finite place \mathfrak{p} of K . We note that if E has good reduction over \mathfrak{p} , then $\text{contr}_\chi(\mathfrak{p}) = 1$ and therefore we focus our attention to bad semistable reduction.

Odd Cyclic Extensions

For the first case, we assume that d is odd. Following the observation in Remark 6.3, we need to calculate $\text{contr}_\chi(\mathfrak{p})$ for each finite place \mathfrak{p} of K . To that objective, we first calculate them for “small” cases and then we use them for the general case. The following lemmas build on this idea.

Lemma 6.5. *Let p be a rational prime, F/K a Galois extension of number fields such that $\text{Gal}(F/K) = C_p$ and E/\mathbb{Q} an elliptic curve with semistable reduction at 2 and 3. Then*

$$\frac{C_{E/F}}{C_{E/K}}$$

is a rational square up factors of p .

Proof. Fix some prime \mathfrak{p} in K . Since the extension L/K is cyclic, the splitting behaviour in L is determined by the ramification index $e_{\mathfrak{p}}$ and the residual degree $f_{\mathfrak{p}}$. Since $\text{contr}_\chi(\mathfrak{p}) = 1$ if E has good reduction at \mathfrak{p} and E is assumed to be semistable, we assume that E has split or non-split multiplicative reduction. The following table records the contribution of \mathfrak{p} depending on $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$, and the entries for split and non-split multiplicative reduction of type I_n are separated by a “;”. The proof follows immediately from (10). \square

$e_{\mathfrak{p}}$	$f_{\mathfrak{p}}$	$C_{\mathfrak{p} \mathfrak{p}}(K/K)$	$C_{\mathfrak{p} \mathfrak{p}}(F/K)$	$\text{contr}_\chi(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	\square
p	1	$n; \tilde{n}$	$pn; \tilde{n}$	$p\square; \square$
1	p	$n; \tilde{n}$	$n; \tilde{n}$	\square

Next, we prove an analogous result for C_{pq} extensions, where p and q are odd rational primes.

Lemma 6.6. *Let p, q be distinct, odd rational primes and let F/K be a Galois extension of number fields such that $\text{Gal}(F/K) = C_{pq}$. Let E/\mathbb{Q} be an elliptic curve with semistable reduction at 2 and 3 and let L_k be the fields as above. Then*

$$\frac{C_{E/F} C_{E/K}}{C_{E/L_p} C_{E/L_q}}$$

is always a rational square.

Proof. The idea of the proof is identical to Lemma 6.5 since in a C_{pq} extension L/K the splitting behaviour of a prime \mathfrak{p} of K in L and all the intermediate fields is determined by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$. The following table records the contribution of \mathfrak{p} depending on these values, and again the entries for split and non-split multiplicative reduction of type I_n are separated by “;”.

$e_{\mathfrak{p}}$	$f_{\mathfrak{p}}$	$C_{\mathfrak{p} p}(K)$	$C_{\mathfrak{p} p}(L_p)$	$C_{\mathfrak{p} p}(L_q)$	$C_{\mathfrak{p} p}(F)$	$\text{contr}_{\chi}(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n^q; \tilde{n}^q$	$n^{pq}; \tilde{n}^{pq}$	\square
1	p	$n; \tilde{n}$	$n; \tilde{n}$	$n^q; \tilde{n}^q$	$n^q; \tilde{n}^q$	\square
1	q	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n; \tilde{n}$	$n^p; \tilde{n}^p$	\square
1	pq	$n; \tilde{n}$	$n; \tilde{n}$	$n; \tilde{n}$	$n; \tilde{n}$	\square
p	1	$n; \tilde{n}$	$pn; \tilde{n}$	$n^q; \tilde{n}^q$	$p^q n^q; \tilde{n}^q$	\square
p	q	$n; \tilde{n}$	$pn; \tilde{n}$	$n; \tilde{n}$	$pn; \tilde{n}$	\square
q	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$qn; \tilde{n}$	$q^p n^p; \tilde{n}^p$	\square
q	p	$n; \tilde{n}$	$n; \tilde{n}$	$qn; \tilde{n}$	$qn; \tilde{n}$	\square
pq	1	$n; \tilde{n}$	$pn; \tilde{n}$	$qn; \tilde{n}$	$pqn; \tilde{n}$	\square

Again, the result follows immediately from the table and (10). \square

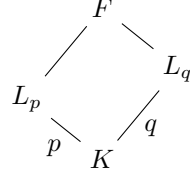


Figure 1: Subfields of a C_{pq} -extension

We are finally ready to prove the main result of this section, from which Theorem 6.1 will follow.

Lemma 6.7. *Let d be a composite, odd squarefree integer and let F/K be a Galois extension of number fields such that $\text{Gal}(F/K) = C_d$. Let E/\mathbb{Q} be an elliptic curve and let L_k be the fields as above. Then*

$$\prod_{k|d} (C_{E/L_k})^{\mu(d/k)}$$

is always a rational square.

Proof. Let n be the number of distinct prime numbers dividing d , so that $d = p_1 \dots p_n$ for some distinct odd primes p_i . We prove this result by induction. The base case for $n = 2$ is the content of Lemma 6.6. Assume that the result holds for squarefree integers with $n - 1$ prime factors and consider the two sets of fields

$$\mathcal{A} = \{L_k : p_n \nmid k\} \quad \text{and} \quad \mathcal{B} = \{L_k : p_n \mid k\},$$

which are clearly a partition of all intermediate fields of F/K . Furthermore, the fields in \mathcal{A} are precisely the intermediate fields of K and L_{d/p_n} , while the fields in \mathcal{B} are the intermediate fields of L_{p_n} and F . However, since $\text{Gal}(L_{d/p_n}/K) = \text{Gal}(F/L_{p_n}) = C_{d/p_n}$, it follows from the inductive hypothesis applied to the fields of \mathcal{A} and \mathcal{B} respectively that

$$\prod_{k|\frac{d}{p_n}} (C_{E/L_k})^{\mu(\frac{d}{kp_n})} \quad \text{and} \quad \prod_{p_n|k|d} (C_{E/L_k})^{\mu(d/k)}$$

are both rational squares. By the natural decomposition

$$\prod_{k|d} (C_{E/L_k})^{\mu(d/K)} = \prod_{k|\frac{d}{p_n}} (C_{E/L_k})^{\mu(d/k)} \prod_{p_n|k|d} (C_{E/L_k})^{\mu(d/k)} = \left(\prod_{k|\frac{d}{p_n}} (C_{E/L_k})^{\mu(\frac{d}{kp_n})} \right)^{-1} \prod_{p_n|k|d} (C_{E/L_k})^{\mu(d/k)},$$

it follows that the left hand side is also a rational square, as desired. \square

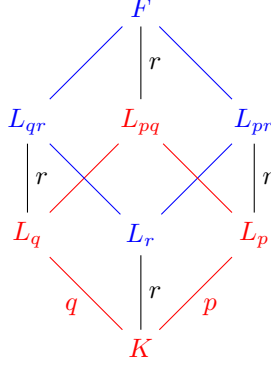


Figure 2: Partition of $n = 3$ into $n = 2$. Red fields are in \mathcal{A} while blue fields are in \mathcal{B} .

We are now ready to prove Theorem 6.1 for odd d .

Theorem 6.1 for odd d . The proof is divided into two cases depending on whether d is the power of a prime or not. Suppose first that d is not, so that $\text{rad}(d)$ is a squarefree **composite** number. However, by Remark 6.3 and Lemma 6.7 we know that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$$

is a rational square, and therefore it is the norm of an element for any quadratic extension of \mathbb{Q} .

The case when $d = p^n$ for some odd prime p and $n \geq 1$ requires some more work. Lemma 6.2 and Lemma 6.5 show that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F}}{C_{E/L_{p^{n-1}}}}$$

is a rational square up to factors of p . Therefore, it suffices to show that p is the norm of any quadratic subextension of $\mathbb{Q}(\zeta_{p^n})$. Since $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})$ is cyclic, $\mathbb{Q}(\zeta_{p^n})$ has one unique quadratic subextension. Hence, it suffices to find the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$. A simple calculation shows that

$$\left(\sum_{a=0}^{p-1} \left(\frac{a}{p} \right) \zeta_p^a \right)^2 = (-1)^{(p-1)/2} p,$$

and therefore $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$, where $p^* = (-1)^{(p-1)/2} p$. The fact that p is a norm in this field is precisely the content of Corollary A.13, and so the Theorem follows. \square

Even Cyclic Extensions

A bit more care is required to prove Theorem 6.1 for even d . This difficulty mainly lies in the case when d is only divisible by one odd prime p . Likewise to the earlier case, we first prove some relevant results.

Lemma 6.8. *Let p be an odd prime and let F/K be a Galois extension of number fields such that $\text{Gal}(F/K) = C_{2p}$ and let L_k be the fields as above. Let E/\mathbb{Q} be an elliptic curve. Then*

$$\frac{C_{E/F}C_{E/K}}{C_{E/L_2}C_{E/L_p}}$$

is a rational square up to factors of p .

Proof. The proof is identical to the proof of Lemmas 6.5 and 6.6 since the splitting behaviour of a prime \mathfrak{p} in K is again determined by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$. The following table records the contribution.

$e_{\mathfrak{p}}$	$f_{\mathfrak{p}}$	$C_{\mathfrak{p} \mathfrak{p}}(\mathbb{Q})$	$C_{\mathfrak{p} \mathfrak{p}}(L_p)$	$C_{\mathfrak{p} \mathfrak{p}}(L_2)$	$C_{\mathfrak{p} \mathfrak{p}}(F)$	$\text{contr}_{\chi}(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n^2; \tilde{n}^2$	$n^{2p}; \tilde{n}^{2p}$	\square
1	p	$n; \tilde{n}$	$n; \tilde{n}$	$n^2; \tilde{n}^2$	$n^2; \tilde{n}^2$	\square
1	2	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$n; n$	$n^p; n^p$	\square
1	$2p$	$n; \tilde{n}$	$n; \tilde{n}$	$n; n$	$n; n$	\square
p	1	$n; \tilde{n}$	$pn; \tilde{n}$	$n^2; \tilde{n}^2$	$p^2n^2; \tilde{n}^2$	$p\square; \square$
p	2	$n; \tilde{n}$	$pn; \tilde{n}$	$n; n$	$pn; n$	\square
2	1	$n; \tilde{n}$	$n^p; \tilde{n}^p$	$2n; 1$	$2^pn^p; 1^p$	\square
2	p	$n; \tilde{n}$	$n; \tilde{n}$	$2n; 1$	$2n; 1$	\square
$2p$	1	$n; \tilde{n}$	$pn; \tilde{n}$	$2n; 1$	$2pn; 1$	\square

The result follows again from (10). \square

However, as soon as d is divisible by 4, the product of local factors is a rational square even if the individual contributions might not be, as the next lemma suggests.

Lemma 6.9. *Let p be an odd prime and let F/K be a Galois extension of number fields such that $\text{Gal}(F/K) = C_{4p}$ and let L_k be the fields as above. Let E/\mathbb{Q} be an elliptic curve. Then*

$$\frac{C_{E/F}C_{E/L_2}}{C_{E/L_4}C_{E/L_{2p}}}$$

is a rational square.

Proof. All fields appearing in the product are intermediate fields of L_2 and F , and $\text{Gal}(F/L_2) = C_{2p}$. Lemma 6.8 shows that given some prime \mathfrak{p} in L_2 , $\text{contr}_{\chi}(\mathfrak{p})$ is a square unless $e_{\mathfrak{p}} = p$ and $f_{\mathfrak{p}} = 1$. That is, \mathfrak{p} ramifies in L_{2p}/L_2 and is split in L_4/L_2 . Now consider $\bar{\mathfrak{p}} = \mathfrak{p} \cap \mathcal{O}_K$. Since \mathfrak{p} splits in L_4 , this forces $\bar{\mathfrak{p}}$ to split as well in L_2/K . Hence, $\bar{\mathfrak{p}} = \mathfrak{p}\mathfrak{p}'$ for two **distinct** primes in K that have the same splitting behaviour and therefore $\text{contr}_{\chi}(\mathfrak{p})\text{contr}_{\chi}(\mathfrak{p}')$ is a rational square, as desired. \square

We are now ready to prove Theorem 6.1 for even d . We break down the proof into three cases:

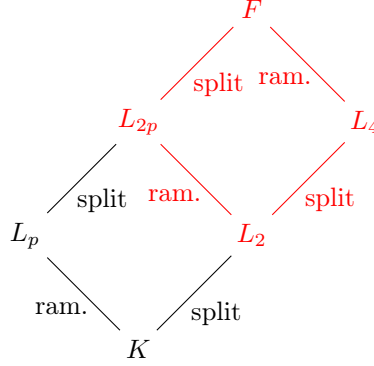


Figure 3: Field diagram for a C_{4p} extension, together with the splitting behaviour of a prime \mathfrak{p} in L_2 with $e_{\mathfrak{p}} = p$ and $f_{\mathfrak{p}} = 1$ over F .

Case 1: d is not divisible by any odd prime, so $d = 2^l$

If $l = 1$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, so there is nothing to prove, so assume that $l \geq 2$. If $\text{Gal}(F/\mathbb{Q}) = C_{2^l}$, then

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F}}{C_{E/L_{2^{l-1}}}},$$

and by Lemma 6.5, we know that this is a rational square up to factors of 2, so it suffices to show that 2 is a norm of every quadratic subfield of $\mathbb{Q}(\zeta_{2^l})$. A standard argument shows that $\text{Gal}(\mathbb{Q}(2^l)/\mathbb{Q}) = (\mathbb{Z}/2^l\mathbb{Z})^* = C_{2^{l-2}} \times C_2$ and therefore $\mathbb{Q}(\zeta_{2^l})$ has $\mathbb{Q}(i)$ as its unique quadratic subextension if $l = 2$ and has three quadratic subextensions if $l \geq 3$. Note that $\zeta_8 = (1+i)/\sqrt{2}$ and therefore $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. The three quadratic subextensions are therefore $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Then the result follows from the fact that

$$2 = \text{Norm}_{\mathbb{Q}(i)}(1+i) = \text{Norm}_{\mathbb{Q}(\sqrt{-2})}(2) = \text{Norm}_{\mathbb{Q}(\sqrt{2})}(2 + \sqrt{2}).$$

Case 1: d is divisible by at least two odd primes

Let $K = L_{d/\text{rad}(d)}$ be as in Remark 6.3 such that $\text{Gal}(F/K) = C_{\text{rad}(d)}$ and all fields appearing in the product of local factors contain K . Then using the same idea as in Lemma 6.7, let

$$\mathcal{A} = \{L_k \supseteq K : 2 \nmid [L_k : K]\} \quad \text{and} \quad \mathcal{B} = \{L_k \supseteq K : 2 \mid [L_k : K]\}.$$

Then the fields in \mathcal{A} and \mathcal{B} are the intermediate fields of (distinct!) $C_{\text{rad}(d)/2}$ extensions. These are odd cyclic extensions, and therefore by Lemma 6.7 the contribution is a rational square and therefore the norm of any quadratic extension.

Case 3: d is divisible by one odd prime

In this case, write $d = 2^l p^n$ and let L_k be the fields as above. In this case, we note that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F} C_{E/L_{d/2p}}}{C_{E/L_{d/2}} C_{E/L_{d/p}}}.$$

By Lemma 6.5, we know that this product is a square up to multiples of p . If $l = 1$, then $\text{Gal}(\mathbb{Q}(\zeta_{2p^n})/\mathbb{Q}) = (\mathbb{Z}/2p^n\mathbb{Z})^* = (\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic, and therefore the unique quadratic subfield is $\mathbb{Q}(\sqrt{p^*})$, and we already know that p is a norm of this field.

From Lemma 6.8 that the contribution of p comes from those primes \mathfrak{p} in $L_{d/2p}$ such that they ramify in $L_{d/2}$ and they split in $L_{d/p}$. However, as in the proof of Lemma 6.9, the prime $\bar{\mathfrak{p}} = \mathfrak{p} \cap L_{d/4p}$ must also split in $L_{d/2p}$ so $\bar{\mathfrak{p}} = \mathfrak{p}\mathfrak{p}'$ for $\mathfrak{p}' \neq \mathfrak{p}$ in $L_{d/2p}$. Since \mathfrak{p} and \mathfrak{p}' have the same splitting behaviour, they give the same contribution. Hence, the product of local terms is in fact a rational square and therefore the norm of any quadratic extension.

This concludes the proof of Theorem 6.1, and we have in addition shown that the contribution is always a square except when $d = 2^n, p^n$ or $2p^n$, where p is an odd rational prime. \square

6.2 Norm relations in odd order extensions

add some motivation (justification) for why I'm proving this result. The point is that the test for positive rank provided by root number computations never says anything in odd order extensions. If we expect the norm relations test to be weaker than root numbers, then nor should this test.

Theorem 6.10. *Let E/\mathbb{Q} be an elliptic curve, F/\mathbb{Q} be an extension of odd order with Galois group G .*

Assume that E has semistable reduction at 2 and 3. Take any representation $\rho \in \mathbf{R}(G)$ with quadratic subfield $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\rho)$ and relation

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m} = \left(\bigoplus_{\mathfrak{g} \in \text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} \right)^{\oplus m} = \bigoplus_i \text{Ind}_{F_i/\mathbb{Q}} \mathbf{1} \ominus \bigoplus_j \text{Ind}_{F'_j/\mathbb{Q}} \mathbf{1}$$

as in Theorem 5.2. Then

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} \in \begin{cases} N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\mathbb{Q}(\sqrt{D})^\times) & m \text{ odd,} \\ \mathbb{Q}^{\times 2} & m \text{ even.} \end{cases}$$

In other words, one cannot use Theorem 5.2 to conclude that E/F must have positive rank.

As in Remark 5.4, we may replace ρ by the sum of its conjugates by elements of $\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{D}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{D})$. We take $D \in \mathbb{Z} \setminus \{0, 1\}$ to be squarefree.

The product of terms we are computing is $C(\Theta)$, where $C: \mathbf{B}(G) \rightarrow \mathbb{Q}^\times$ is given by $C: H \mapsto C_{E/F^H}$, and Θ is any ρ -relation. We break up the function C into $C = \prod_p C_{\mathfrak{p}|p} \prod_p = T_{\mathfrak{p}|p} \cdot D_{\mathfrak{p}|p}$, ranging over primes $p \in \mathbb{Q}$, as defined in Notation 4.3. Then one has

$$T_{\mathfrak{p}|p} \cdot D_{\mathfrak{p}|p} = (D_p, C_v)$$

where C_v is a function on $\mathbf{B}(D_p)$ sending $H \mapsto C_v(E/F_w^H)$. The following result will allow us to apply some results from §1.3.

Theorem 6.11. *When D_p has odd order, $C_v(\Psi) \in \mathbb{Q}^{\times 2}$ for any Brauer relation $\Psi \in \mathbf{B}(D_p)$.*

Proof. This follows from [DD09, Theorem 2.47] and [DD09, Theorem 3.2 (Tam)]. \square

Corollary 6.12. *It is enough to prove Theorem 6.10 when m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. Thus we need to prove that, given any $\Theta \in \mathbf{B}(G)$ such that $\mathbb{C}[\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, Θ is a norm relation for the function C .*

Proof. Since $\mathbb{Q}(\rho)$ is quadratic, we have $\mathbb{Q}^{\times 2} \subset N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. As G is odd, any choice of D_p is odd. It follows from Theorem 6.11 that $C(\Psi) \in \mathbb{Q}^{\times 2}$ for all Brauer relations $\Psi \in \mathbf{B}(G)$. Therefore by Proposition 1.19, it is enough to prove Theorem 6.10 when m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. Then m divides $|G|$, hence is odd. \square

Let τ be the generator of $\text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Let \mathfrak{f} be the smallest integer such that $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_{\mathfrak{f}})$. Then $\mathfrak{f} \mid |G|$, hence is odd. By Remark A.7, $\mathfrak{f} = |D|$ and that $D \equiv 1 \pmod{4}$. The following shows that it is only of interest to consider decomposition groups of exponent divisible by \mathfrak{f} .

Corollary 6.13. *Let the exponent of D_p be b . If $\mathfrak{f} \nmid b$, then $(T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p})(\Theta) \in \mathbb{Q}^{\times 2}$.*

Proof. Note that $\mathbb{Q}(\text{Res}_{D_p} \rho) \subset \mathbb{Q}(\zeta_b) \cap \mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b)$. Then $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b) \implies \mathfrak{f} \mid b$ by minimality of \mathfrak{f} . Since $\mathfrak{f} \nmid b$, we have $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_b)$, so $\mathbb{Q}(\text{Res}_{D_p} \rho) = \mathbb{Q}$. The corollary then follows from Proposition 1.29 and Theorem 6.11, noting that since $\hat{C}(D_p)$ is odd, multiplication by 2 is injective. \square

Fix $\Theta = \sum_i n_i H_i \in \text{B}(G)$ with $\mathbb{C}[\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. We prove that at each prime p , $(T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p})(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$. As observed, this depends on D_p and I_p . As we deal with each local factor individually, we argue that one can take $D_p = I_p$.

Lemma 6.14. *Let E/K be an elliptic curve. Let K'/K be an extension of number fields odd degree, unramified at the place v of K . Then $C_w(E/K') \equiv C_v(E/K) \pmod{\mathbb{Q}^{\times 2}}$ for any place w of K' with $w \mid v$.*

Proof. This is automatic for good reduction and split multiplicative reduction. It is also clear for non-split multiplicative reduction since the residue degree cannot be even (so the reduction type remains non-split at w). For additive reduction, see [DD09, Lemma 3.12]. \square

Lemma 6.15. *At a prime p , we may assume that $D_p = I_p$ when computing $(T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p})(\Theta)$.*

Proof. Let p have residue degree f_p . Let L/\mathbb{Q} be a Galois extension of degree f_p with cyclic Galois group, such that p is inert in L . Further ensure that $F \cap L = \mathbb{Q}$. Then $\text{Gal}(FL/L) = G$. Let $F_i = F^{H_i}$ and $L_i = F_i L$.

Let v be a place over p in F_i . The extension L_i/F_i is Galois, so v is either split or inert in L_i . We claim that $C_v(E/F_i) \equiv \prod_{w|v} C_w(E/L_i) \pmod{\mathbb{Q}^{\times 2}}$. Indeed, the number of terms in the product on the right is odd, and by Lemma 6.14 $C_v(E/F_i) \equiv C_w(E/L_i) \pmod{\mathbb{Q}^{\times 2}}$. Letting $T'_{\mathfrak{P}|p}$ and $D'_{\mathfrak{P}|p}$ be functions on $\text{B}(G)$ defined as in (4.3) but with \mathbb{Q}, F replaced by L, FL , we see that $(T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p})(\Theta) \equiv (T'_{\mathfrak{P}|p} \cdot D'_{\mathfrak{P}|p})(\Theta) \pmod{\mathbb{Q}^{\times 2}}$. Thus it is equivalent to do our computation in FL/L , but here p has residue degree 1. \square

To prove Theorem 6.10, we proceed by considering separately each reduction type.

Good reduction

If E/\mathbb{Q} has good reduction at p , it has good reduction at all primes lying above p in subfields of F . Hence the Tamagawa number is always one, as well as $|\omega/\omega_{\mathfrak{P}}^{\min}|_{\mathfrak{P}} = 1$ for any finite place $\mathfrak{P} \mid p$ in an intermediate field. Therefore $T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p} = 1$ as a function on $\text{B}(G)$.

Multiplicative reduction

If E/\mathbb{Q}_p has multiplicative reduction, then as in the good reduction case one has $|\omega/\omega_{\mathfrak{P}}^{\min}|_{\mathfrak{P}} = 1$ for any place $\mathfrak{P} \mid p$ in an intermediate field. Thus $D_{\mathfrak{P}|p} = 1$. For $T_{\mathfrak{P}|p}$, we consider non-split/split reduction separately.

Non-split multiplicative reduction

Let E/\mathbb{Q}_p have non-split multiplicative reduction. Since $D_p = I_p$, all primes above p have residue degree 1. Then the reduction at places above p remains non-split in all intermediate subfields. It follows that

$$T_{\mathfrak{P}|p} = (D_p, \alpha)$$

where α is the constant function on $B(D_p)$ with $\alpha \in \{1, 2\}$, depending on $\text{ord}_p(\Delta)$ being even or odd. By Proposition 1.30, it follows that $T_{\mathfrak{P}|p}(\Theta) \in \mathbb{Q}^{\times 2}$.

Split multiplicative reduction

Now suppose E/\mathbb{Q}_p has split multiplicative reduction. The reduction type remains split at all places above p within sub-extensions of F/\mathbb{Q} . Let $\text{ord}_p(\Delta) = n$. Then

$$T_{\mathfrak{P}|p} = (D_p, D_p, en).$$

Since the n factor is constant, $(D_p, D_p, en)(\Theta) \equiv (D_p, D_p, e)(\Theta) \pmod{\mathbb{Q}^{\times 2}}$ by Proposition 1.30.

We have $D_p = I_p = P_p \rtimes C_l$, where $P_p \triangleleft I_p$ is wild inertia, and $C_l = I_p/P_p$ is the tame quotient. C_l is a cyclic group, with $l \mid p^f - 1 = p - 1$. By Corollary 6.13, we may consider such D_p with exponent $p^u l$ for some $u \geq 0$ such that $\mathfrak{f} \mid p^u l$.

Now, $(D_p, D_p, e)(\Theta)$ is the product of ramification indices at primes above p . We separate the p -part and tame part of this expression. Recall that the ramification index of a place w above p corresponding to the double coset $H_i x D_p$ has ramification degree $e_w = \frac{|I_p|}{|H_i \cap I_p^x|} = \frac{|I_p|}{|I_p \cap H^{x^{-1}}|}$. This is the dimension of the permutation representation $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]$. Let $D_p \cap H^{x^{-1}} = P' \rtimes C_a$ where $P' \leq P$ and $a \mid l$. Then the ramification index is $\frac{|P|}{|P'|} \cdot \frac{l}{a}$.

Taking fixed points under wild inertia, one has the following isomorphism of D_p -representations

$$\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p} \simeq \mathbb{C}[D_p/P_p(D_p \cap H^{x^{-1}})] \simeq \mathbb{C}[D_p/P_p \rtimes C_a].$$

This permutation representation has dimension $\frac{l}{a}$, so we've killed off the p -part. Then

$$\mathbb{C}[\text{Res}_{D_p} \Theta]^{P_p} \simeq (\text{Res}_{D_p} \rho^{\oplus m} \oplus \tau(\text{Res}_{D_p} \rho^{\oplus m}))^{P_p},$$

and we can consider these as representations of $D_p/P_p = C_l$.

Let $\Psi = P_p \cdot \text{Res}_{D_p} \Theta / P_p \in B(C_l)$. Consider the function g on $B(C_l)$ with $H \mapsto [C_l : H] = \dim \mathbb{C}[C_l/H]$. It follows from the above discussion that $(D_p, D_p, e)(\Theta)$ differs from $g(\Psi)$ up to a factor of p . Note that if $p = 2$ then $P_p = 1$ since $|P_p| \mid |G|$ which is odd. So we only need to consider this factor of p for p odd. Crucially, this factor of p doesn't matter:

Lemma 6.16. *Let $K = \mathbb{Q}(\sqrt{D})$, with \mathfrak{f} the smallest positive integer such that $K \subset \mathbb{Q}(\zeta_{\mathfrak{f}})$. Suppose that \mathfrak{f} is odd. Let $\mathfrak{f} \mid p^u l$, for some odd prime p , $u \geq 0$ and l such that $p \equiv 1 \pmod{l}$. Then p is the norm of an element from K^{\times} .*

Proof. Since \mathfrak{f} is odd, one has $D = \prod_{q \mid \mathfrak{f}} q^*$, the product being taken over primes dividing \mathfrak{f} . Note that if $q \neq p$, then since $q \mid l$, we have $p \equiv 1 \pmod{l} \implies p \equiv 1 \pmod{q}$. By Theorem A.9, p is the norm of a principal fractional ideal of K . If K is imaginary, then p is the norm of an element of K . Else, we invoke Theorem A.11 or Theorem A.12. \square

Therefore we only need to worry about the tame part of our ramification indices. Let $\phi = (\text{Res}_{D_p} \rho)^{P_p}$, viewed as a representation on $D_p/P_p = C_l$. Then Ψ is a ϕ -relation. If $\mathfrak{f} \nmid l$ then $\mathbb{Q}(\phi) = \mathbb{Q}$. Therefore $\mathbb{C}[C_l/\Psi] \simeq \phi^{\oplus 2}$, implying that $\Psi = 2\Psi'$ for some $\Psi' \in B(C_l)$ with $\mathbb{C}[C_l/\Psi'] = \phi$. Then $g(\Psi) = g(\Psi')^2 \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$. Otherwise, suppose that $\mathbb{Q}(\phi) = \mathbb{Q}(\rho)$. It follows from Proposition 1.22 that $g(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$.

Additive reduction

Now suppose that E/\mathbb{Q}_p has additive reduction. In this case, assume that $p \geq 5$. We have $D_p = P_p \rtimes C_l$ with $l \mid p - 1$. Once again we may assume that $\mathfrak{f} \mid p^k l$ where $p^k l$ is the exponent of D_p by Corollary 6.13.

Let $\delta = \text{ord}_p(\Delta_E)$. Consider a place \mathfrak{P} of F^H over p with ramification degree $e_{\mathfrak{P}}$ over \mathbb{Q} . Then Δ_E has valuation $ne_{\mathfrak{P}}$ with respect to \mathfrak{P} . Then $\left| \Delta_E / \Delta_{E, \mathfrak{P}}^{\min} \right|_{\mathfrak{P}} = p^{-(\delta \cdot e_{\mathfrak{P}} - \delta_H)}$, where $\delta_H = \text{ord}_{\mathfrak{P}}(\Delta_{E, \mathfrak{P}}^{\min})$. Recall that

$$\left| \frac{\omega}{\omega_{\mathfrak{P}}^{\min}} \right|_{\mathfrak{P}}^{-12} = \left| \frac{\Delta_E}{\Delta_{E, \mathfrak{P}}^{\min}} \right|_{\mathfrak{P}}.$$

Therefore $|\omega / \omega_{\mathfrak{P}}^{\min}|_{\mathfrak{P}} = p^{\lfloor \frac{\delta \cdot e_{\mathfrak{P}} - \delta_H}{12} \rfloor}$.

Suppose that E/\mathbb{Q}_p has Kodaira type I_n^* , so $\delta = 6 + n$. For a finite extension K'/\mathbb{Q}_p with ramification degree e , E/K' has Kodaira type I_{en}^* if e is odd, and type I_{en} if n is even. Thus in odd degree extensions the reduction type will stay potentially multiplicative. Then $\delta \cdot e_{\mathfrak{P}} - \delta_H = 6e_{\mathfrak{P}}$.

If E/\mathbb{Q}_p has potentially good reduction then $\delta \in \{2, 3, 4, 6, 8, 9, 10\}$. E also has potentially good reduction at the place \mathfrak{P} in F^H . Hence $\delta_H \leq 12$ and it follows that $\delta_H = \delta \cdot e_{\mathfrak{P}} - 12 \cdot \lfloor \delta \cdot e_{\mathfrak{P}} / 12 \rfloor$.

In conclusion,

$$D_{\mathfrak{P}|p} = \begin{cases} (D_p, D_p, p^{\lfloor e/2 \rfloor}) & \text{if } E \text{ has potentially multiplicative reduction,} \\ (D_p, D_p, p^{\lfloor \delta \cdot e / 12 \rfloor}) & \text{if } E \text{ has potentially good reduction.} \end{cases}$$

In either case, $D_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$. Indeed, this takes values 1 or p in $\mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$. But $p \equiv 1 \pmod{l}$ implies $p \equiv 1 \pmod{\mathfrak{f}}$ so that p is the norm of a principal ideal in $\mathbb{Q}(\rho)$, and hence the norm of an element, by Corollary A.9 and Theorem A.11.

For the Tamagawa number computations, since $p \geq 5$ we may write E/\mathbb{Q}_p as $E: y^2 = x^3 + Ax + B$ and use the description from [DD09] for computing Tamagawa numbers, as detailed in Lemma 2.6. The discriminant of E/\mathbb{Q}_p is $\Delta = -16(4A^3 + 27B^2)$, and we write $\delta = v_p(\Delta)$. **maybe add a small reminder**

Firstly, suppose that E/\mathbb{Q}_p has reduction type I_n^* . Write $D_p = \text{Gal}(F_w/\mathbb{Q}_p)$. Since we assume $D_p = I_p$, i.e. the residue degree is one, it follows that any subextension L' of F_w/\mathbb{Q}_p satisfies $\sqrt{B} \in L' \iff \sqrt{B} \in \mathbb{Q}_p$ and $\sqrt{\Delta} \in L' \iff \sqrt{B} \in \mathbb{Q}_p$. Therefore $T_{\mathfrak{P}|p} = (D_p, \alpha)$ where $\alpha \in \{2, 4\}$. But then $(D_p, \alpha)(\Theta) \in \mathbb{Q}^{\times 2}$ by Proposition 1.30.

Now suppose that E/\mathbb{Q}_p has potentially good reduction. Observe that in a totally ramified extension of degree coprime to 12, the Tamagawa number remains the same. Hence for D_p odd, if $3 \nmid |D_p|$ it follows that $T_{\mathfrak{P}|p} = (D_p, \alpha)$ for some constant α and so $T_{\mathfrak{P}|p}(\Theta) \in \mathbb{Q}^{\times 2}$.

Thus we assume that $3 \mid |D_p|$. Since we assumed $p \geq 5$, we have $D_p = I_p = P_p \rtimes C_l$ with $3 \mid l$ and $p \equiv 1 \pmod{l}$. If we have type III or III^* or I_0^* then the Tamagawa number is still unchanged in any totally ramified extension of odd degree extension, even when the degree is divisible by 3. We will treat the other cases separately:

Type II and II^* reduction:

Suppose $\delta = 2$, that is we have Type II reduction. If L'/\mathbb{Q}_p is an odd degree extension that is divisible by 3, then E/L' has reduction type I_0^* . By Lemma 2.6 the Tamagawa number of E/L' then depends on whether $\sqrt{\Delta} \in \mathbb{Q}_p$. Since we have additive reduction, we know that $p \mid A$, $p \mid B$. Moreover, $\delta = 2$ implies $2 = v_p(\Delta) = v_p(27B^2 + 4A^3)$, so that $v_p(B) = 1$. Then, $\Delta = p^2 \cdot \alpha$, and $\alpha \equiv -27 \cdot \square \pmod{p}$. Therefore $\sqrt{\Delta} \in \mathbb{Q}_p \iff -3$ is a square \pmod{p} . But this is the case; we assumed $p \equiv 1 \pmod{l}$, so $p \equiv 1 \pmod{3}$. Then $\left(\frac{-3}{p} \right) = \left(\frac{p}{3} \right) = 1$. Therefore the Tamagawa number will be 1 or 4, which is a square. On the other hand if L'/\mathbb{Q}_p is an extension of odd degree then the reduction type over L' is II or II^* and the Tamagawa number is 1. It follows that $T_{\mathfrak{P}|p}(\Theta)$ is a product of square terms, so is itself square.

If $\delta = 10$, then E/L' has reduction type I_0^* whenever $3 \mid [L' : \mathbb{Q}_p]$. We show again that one must have $\sqrt{\Delta} \in \mathbb{Q}_p$. Recall that E/\mathbb{Q}_p has potentially good reduction if and only if its j -invariant

is integral, i.e. $v_p(j) \geq 0$ (cf. [Sil09, §VII.5, Proposition 5.5]). One has $j = -1728(4A^3)/\Delta$ and so $3v_p(A) \geq v_p(\Delta) = 10 \implies 3v_p(A) > v_p(\Delta) \implies v_p(\Delta) = 2v_p(B)$, so $v_p(B) = 5$. Thus $\Delta = p^{10} \cdot \alpha$ with $\alpha \equiv -27 \cdot \square \pmod{p}$, and we conclude as above.

Type IV and IV reduction:*

Now, if E/\mathbb{Q}_p has additive reduction of type IV or IV*, it attains good reduction over any totally ramified cyclic extension of degree divisible by 3. This could result with 3 coming up an odd number of times in $T_{\mathfrak{P}|p}(\Theta)$, when $\sqrt{B} \notin \mathbb{Q}_p$.

Recall from the proof of Proposition 1.30 that $\text{Res}_{D_p} \Theta = \sum_i n_i \sum_{x \in H_i \setminus G/D_p} D_p \cap H^{x^{-1}}$, with $\sum_i n_i |H_i \setminus G/D_p|$ even. If $D_p = \text{Gal}(F_w/\mathbb{Q}_p)$, then the number of subextensions divisible by 3 (i.e. the number of subextensions where we obtain good reduction) corresponds to the number of subgroups with index divisible by 3 in $\text{Res}_{D_p} \Theta$. We compute this number to determine $\text{ord}_3(T_{\mathfrak{P}|p}(\Theta))$ modulo squares.

Similarly to the split multiplicative case, we may pass to the tame quotient $C_p/P_p = C_l$. Indeed

$$3 \mid [D_p : D_p \cap H^{x^{-1}}] = \dim \mathbb{C}[D_p/D_p \cap H^{x^{-1}}] \iff 3 \mid \dim \mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p},$$

since $3 \nmid |P_p|$. Therefore we may compute the number of subgroups divisible by 3 in $\Psi = P_p \cdot \text{Res}_{D_p} \Theta/P_p \in B(C_l)$. Let $h : B(C_l) \rightarrow \mathbb{Q}^\times$ be the function given by $H \mapsto \begin{cases} 3 & 3 \mid [C_l : H], \\ 1 & 3 \nmid [C_l : H]. \end{cases}$

Proposition 6.17. *Suppose that E/\mathbb{Q}_p has additive reduction of Type IV or IV*, with $c_v(E/\mathbb{Q}_p) = 3$. Then $T_{\mathfrak{P}|p}(\Theta) \equiv h(\Psi) \pmod{\mathbb{Q}^{\times 2}}$ and $T_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.*

Proof. The fact that $T_{\mathfrak{P}|p}(\Theta) \equiv h(\Psi) \pmod{\mathbb{Q}^{\times 2}}$ has been observed above. Let ψ_3 be an irreducible character of D_p of order 3. One has that $\langle \text{Ind}_{C_{l/l'}}^{C_l} \mathbb{1}, \psi_3 \rangle = 1$ when $3 \mid l'$ and is zero when $3 \nmid l'$. Thus

$$h(\Psi) = 3^{\langle \mathbb{C}[C_l/\Psi], \psi_3 \rangle}.$$

As in the proof of Proposition 1.22, write $\mathbb{C}[C_l/\Psi] = \sum_{l'|l} a_{l'} \chi_{l'}$, where $\chi_{l'}$ is an irreducible rational character, of C_l with kernel of index l' . Observe that $\langle \chi_{l'}, \psi_3 \rangle = 0$ unless $l' = 3$, in which case it is 1. Therefore $h(\Psi) \equiv 3^{a_3} \pmod{\mathbb{Q}^{\times 2}}$. In the proof of Proposition 1.22, we showed that a_3 is even unless $3 \mid f$, i.e. that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$. But then 3 is a norm in $\mathbb{Q}(\rho)$. Thus we see that in all cases $T_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. \square

We have observed that for all reduction types of E/\mathbb{Q}_p , one always has $T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, and so $C(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, completing the proof of Theorem 6.10. \square

corollary about restricting to odd order decomposition groups??

Appendix A Algebraic number theory background

A.1 Class field theory and genus fields

In this section we introduce the concept of a genus field, as well as properties that will be useful for us.

Let K be a number field. The **ideal class group** $\text{Cl}_K = I_K/P_K$ is the group of fractional ideals modulo principal fractional ideals. For an ideal \mathfrak{p} , we let $[\mathfrak{p}]$ denote its class in Cl_K .

The **extended ideal class group** is the group $\text{Cl}_K^+ = I_K/P_K^+$, where P_K^+ denotes the subgroup of principal fractional ideals with totally positive generator, i.e. ideals $\alpha\mathcal{O}_K$ where $\sigma(\alpha) > 0$ for all real embeddings $\sigma: K \hookrightarrow \mathbb{R}$.

Note that Cl_K^+ is the ray class group for the modulus \mathfrak{m} of K consisting of the product of all real places. The corresponding ray class field is known as the **extended Hilbert class field**, which we'll denote as H^+ . This is the maximal extension of K that is unramified at all finite primes. Let H be the usual Hilbert Class field of K . Then one has $H \subset H^+$. Moreover, the index can be described in terms of the structure of K :

Theorem A.1. *[Jan96, Chapter VI, Section 3, Theorem 3.1] Let r be the number of real primes of K . Let U_K, U_K^+ the group of units and totally positive units of K respectively, Then*

$$[H^+ : H] = 2^r [U_K : U_K^+]^{-1}.$$

Observe that if K has no real places, then $H^+ = H$. For quadratic fields, the index depends on the norm of a fundamental unit:

Corollary A.2. *Let $K = \mathbb{Q}(\sqrt{D})$ with D a square-free positive integer. Let ϵ be a fundamental unit of K . Then $[H^+ : H] = 1$ or 2 , according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1 .*

Fix $K = \mathbb{Q}(\sqrt{D})$ for D a squarefree integer. The (extended) Hilbert class field of K need not be abelian over \mathbb{Q} (note that it is Galois over \mathbb{Q} by uniqueness of the (extended) Hilbert class field). However it can be useful to consider the maximal subfield of H that is abelian over \mathbb{Q} .

Definition A.3. For any abelian extension K/\mathbb{Q} , the **genus field** of K/\mathbb{Q} is the largest abelian extension L/\mathbb{Q} contained in H . The **extended genus field** is the largest abelian extension L^+/\mathbb{Q} contained in H^+ .

Let $\sigma \in \text{Gal}(H^+/\mathbb{Q})$ be such that $\sigma|_K$ generates $\text{Gal}(K/\mathbb{Q})$. L has the following properties:

Theorem A.4. *[Jan96, Ch. VI, §3, Theorem 3.3] Let $K = \mathbb{Q}(\sqrt{D})$.*

1. $\text{Gal}(H/L)$ is isomorphic to the subgroup of C_K generated by the ideal classes of the form $[\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$, $\mathfrak{U} \in I_K$.
2. $\text{Gal}(H/L) \simeq (C_K)^2$.

Proof sketch of 1. Let $G = \text{Gal}(H/\mathbb{Q})$. Then $L = H^{[G,G]}$ is the fixed field of the commutator subgroup of G . The Artin map induces an isomorphism $\varphi: C_K \rightarrow C \subset G$ with $\varphi(C_K) \simeq C = \text{Gal}(H/K)$. One shows that $\varphi([\sigma(\mathfrak{U})\mathfrak{U}^{-1}]) \in [G, C]$ and conversely that every commutator element in $[G, G]$ can be expressed as $\varphi([\sigma(\mathfrak{U})\mathfrak{U}^{-1}])$ for some $\mathfrak{U} \in I_K$. \square

This allows us to deduce the following:

Theorem A.5. *Let p be a prime in \mathbb{Q} . If the residue degree of p in L/\mathbb{Q} is 1, then p is the norm of a principal fractional ideal in K .*

Proof. Let $\varphi: C_K \rightarrow \text{Gal}(H/K)$ be the isomorphism induced by the Artin map. By Theorem A.4, $\text{Gal}(L/K) = \text{Cl}_K / (\text{Cl}_K)^2$ is abelian. Let \mathfrak{p} be a prime of K lying over p . Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and \mathfrak{p} has residue degree 1 in L . It follows that $\varphi([\mathfrak{p}])|_L = \text{Id}$ so that $\varphi([\mathfrak{p}]) \in \text{Gal}(H/L)$. Thus by Theorem A.4 there is a fractional ideal \mathfrak{A} of I_K such that $[\mathfrak{p}] = [\sigma(\mathfrak{A})\mathfrak{A}^{-1}]$. Observe that $N_{K/\mathbb{Q}}(\sigma(\mathfrak{A})\mathfrak{A}^{-1}) = 1$. It follows that we can represent $[\mathfrak{p}]^n$ by a fractional ideal of norm p for all $n \geq 1$. Since Cl_K is finite, this implies there is a principal fractional ideal in K of norm p . \square

Observe that $C_K / (C_K)^2$ is an abelian group of exponent 2. The following theorem describes its order:

Theorem A.6. [Jan96, Ch VI, §3, Theorem 3.9] Suppose the discriminant of K/\mathbb{Q} has t prime divisors. Then $C_K / (C_K)^2$ has order 2^{t-1} if $D < 0$ or if $D > 0$ and a unit of K has norm -1 . Otherwise, if $D > 0$ and all units of K have norm 1, it has order 2^{t-2} .

Remark A.7. The conductor of K/\mathbb{Q} is a particular modulus for K/\mathbb{Q} (ref). We denote the finite part of it by $\mathfrak{f} \in \mathbb{Z}_{>0}$. Then \mathfrak{f} is the smallest positive integer such that $K \subset \mathbb{Q}(\zeta_{\mathfrak{f}})$. For quadratic fields, one has that $\mathfrak{f} = |\Delta|$ where Δ is the discriminant of K (ref). Thus

$$\mathfrak{f} = |\Delta| = \begin{cases} |D| & D \equiv 1 \pmod{4}, \\ 4|D| & D \not\equiv 1 \pmod{4}. \end{cases}$$

Our introduction of the extended genus field L^+ is mostly because it is easier to describe than L .

Theorem A.8. [Jan96, Ch VI, §3, Theorem 3.10] Let the discriminant of $K = \mathbb{Q}(\sqrt{D})$ be Δ and suppose $|\Delta| = p_1 p_2 \cdots p_t$ where p_2, \dots, p_t are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is

$$L^+ = \mathbb{Q}(\sqrt{D}, \sqrt{p_2^*}, \dots, \sqrt{p_t^*}) = K(\sqrt{p_2^*}, \dots, \sqrt{p_t^*}),$$

where

$$\begin{cases} p_i^* = p_i & \text{if } p_i \equiv 1 \pmod{4}, \\ p_i^* = -p_i & \text{if } p_i \equiv 3 \pmod{4} \end{cases}$$

Corollary A.9. Let p be an odd prime in \mathbb{Q} , $K = \mathbb{Q}(\sqrt{D})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$, as in Theorem A.8. If $p \equiv 1 \pmod{|\Delta|}$, then p is the norm of a principal fractional ideal in K . It is also the norm of a principal fractional ideal in $K' = \mathbb{Q}(\sqrt{p^* D})$.

Proof. Let $L^+ = \mathbb{Q}(\sqrt{D}, \sqrt{p_2^*}, \dots, \sqrt{p_t^*})$ be the extended genus field of K , and L the genus field. If p has residue degree 1 in L^+/\mathbb{Q} , then it has residue degree 1 in L/\mathbb{Q} , and the first result follows by Theorem A.5.

Note that p splits in the quadratic subfields $\mathbb{Q}(\sqrt{p_i^*})$ for $i = 2, \dots, t$, since $\left(\frac{p_i^*}{p}\right) = \left(\frac{p}{p_i}\right) = 1$, as $p \equiv 1 \pmod{\Delta} \implies p \equiv 1 \pmod{p_i}$ for $i = 2, \dots, t$. To show that p splits in L^+ we just need to show that it also splits in K .

First suppose $D \equiv 1 \pmod{4}$. Write $D = \prod_{i=1}^t p_i^*$. Then

$$\left(\frac{D}{p}\right) = \prod_{i=1}^t \left(\frac{p_i^*}{p}\right) = \prod_{i=1}^t \left(\frac{p}{p_i}\right) = 1.$$

Thus p splits in K .

Now consider that $D \not\equiv 1 \pmod{4}$. First assume $D \equiv 3 \pmod{4}$. Write $D = -\prod_{i=2}^t p_i^*$. Then

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right) \prod_{i=2}^t \left(\frac{p_i^*}{p}\right) = \left(\frac{-1}{p}\right) = 1,$$

since $p \equiv 1 \pmod{|\Delta|}$ and $4 \mid |\Delta| \implies p \equiv 1 \pmod{4}$.

Now assume that $2 \mid D$ so that $8 \mid |\Delta|$ and $p \equiv 1 \pmod{8}$. Then $D = \pm 2 \prod_{i=2}^t p_i^*$. Thus

$$\left(\frac{D}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right) \prod_{i=2}^t \left(\frac{p_i^*}{p}\right) = 1.$$

Let L'^+ be the extended genus field of K' . Now p ramifies in $K', \mathbb{Q}(\sqrt{p^*})$. Using the calculations above, it is either split or ramified in all quadratic subfields of L'^+ , and so has residue degree 1 in L'^+ , and the result follows. \square

We want to understand when $p \in N_{K/\mathbb{Q}}(K^\times)$. If p is the norm of a principal fractional ideal in K , then $\pm p \in N_{K/\mathbb{Q}}(K^\times)$. If K is imaginary, one must have $p \in N_{K/\mathbb{Q}}(K^\times)$. We can also arrive to the same conclusion when K is real and $-1 \in N_{K/\mathbb{Q}}(K^\times)$.

Theorem A.10. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ squarefree and suppose that all odd primes dividing D are congruent to 1 (mod 4). Then -1 is the norm of an element of K^\times .*

Proof. The condition on D ensures that there exists $x, y \in \mathbb{Q}$ such that $D = x^2 + y^2$. Therefore $-1 = (x/y)^2 - D(1/y)^2$ so that -1 is the norm of the element $\frac{x}{y} + \frac{1}{y}\sqrt{D}$. \square

Note that -1 being the norm of an element in K does not ensure that -1 is the norm of a unit in K . The smallest counter-example is $K = \mathbb{Q}(\sqrt{34})$. The element $\frac{5}{3} + \sqrt{34}$ has norm -1 , but there is no unit with norm -1 .

Theorem A.11. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field. If p is an odd prime such that $p \equiv 1 \pmod{|\Delta|}$, then p is the norm of an element from K .*

Proof. We know that p is the norm of a principal fractional ideal of K by Corollary A.9. Therefore there exists integers x, y, z such that $\pm pz^2 = x^2 - Dy^2$.

Suppose firstly that all odd primes dividing D are congruent to 1 (mod 4). Then there is an element of K^\times of norm -1 by Theorem A.10. Hence we can find an element of norm p .

Otherwise, there exists a prime $q \mid D$ such that $q \equiv 3 \pmod{4}$. Reducing mod q , we have $\pm p = \square$. Since $p \equiv 1 \pmod{q}$, it is a square (mod q). But -1 is not a square mod q , hence our sign must have been $+$ and so p is the norm of an element from K^\times . \square

Theorem A.12. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field. Let p be an odd prime such that $p \mid D$ and $p \equiv 1 \pmod{|\Delta|/p}$. Then p is the norm of an element from K .*

Proof. By Corollary A.9, we know that p is the norm of a principal fractional ideal of K . The rest of the argument is analogous to the previous proof. \square

Corollary A.13. *The odd prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

References

- [BD16] Alex Bartel and Tim Dokchitser, *Rational representations and permutation representations of finite groups*, Math. Ann. **364** (2016), no. 1-2, 539–558. MR 3451397
- [DD09] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71. MR 2534092
- [DEW21] V. Dokchitser, R. Evans, and H. Wiersema, *On a BSD-type formula for L -values of Artin Twists of Elliptic Curves*, Graduate Texts in Mathematics, Crelles Journal, 2021.
- [Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR 1362545
- [Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, french ed., Graduate Texts in Mathematics, vol. Vol. 42, Springer-Verlag, New York-Heidelberg, 1977. MR 450380
- [Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 1994.
- [Sil09] ———, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 2009.