Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

March 27, 2024

Contents

1 Birch and Swinnerton-Dyer Conjecture **4**

2 Algebraic number theory background **5**

2.1 Decompositions of primes in field extensions 5

2.2 Class field theory 5

2.2.1 Genus field 5

3 Norm relations **7**

3.1 Representation theory of finite groups 7

3.2 The Burnside ring and relations 7

3.3 Functions on the Burnside ring and norm relations 8

3.4 D-local functions 9

4 Forcing points of infinite order **10**

4.1 Compatibility in odd order extensions 10

4.1.1 Additive reduction 13

Introduction

Notation

We use the following notation for characters:

$R_{\mathbb{C}}(G)$	the ring of characters of representations of G over $\mathbb{C}$,
$R_{\mathbb{Q}}(G)$	the ring of characters of representations of G over $\mathbb{Q}$,
$\mathrm{Irr}_{\mathbb{C}}(G)$	the set of characters of complex irreducible representations of G,
$\mathrm{Irr}_{\mathbb{Q}}(G)$	the set of characters of $\mathbb{Q}$-irreducible representations of G,
$\mathbb{Q}(\rho)$	the field of character values of a complex character ρ,
$m(\rho)$	the Schur Index of an irreducible complex character ρ over $\mathbb{Q}(\rho)$,
$H^x = xHx^{-1}$	for $H \leq G$ a subgroup of a group G and $x \in G$,

1 Birch and Swinnerton-Dyer Conjecture

2 Algebraic number theory background

2.1 Decompositions of primes in field extensions

2.2 Class field theory

2.2.1 Genus field

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

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

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

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 unramifed 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 2.1 (Janusz 3. Extended Class group)**.** *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*

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

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 2.2. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free positive integer. Let ϵ be a fundamental unit of K. Then $[H^+\colon H] = 1$ 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 convenient to consider the maximal subfield of H that is Galois over $\mathbb{Q}$.

Definition 2.3. For any abelian extension $K/\mathbb{Q}$, the **genus field** of K over $\mathbb{Q}$ is the largest abelian extension E of $\mathbb{Q}$ contained in H. The **extended genus field** is the largest abelian extension E^+ of $\mathbb{Q}$ contained in H^+.

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

Theorem 2.4 (Janusz 3.3)**.** *1.* $\mathrm{Gal}(H/E)$ *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. $\mathrm{Gal}(H/E) \simeq (C_K)^2$.

Note that this says that every class $[\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$ is a square in C_K. This allows us to deduce the following:

Theorem 2.5. *Let p be a prime in $\mathbb{Q}$. If the inertial degree of p in $E/\mathbb{Q}$ is 1, then p is the norm of a principal ideal in K.*

Proof. It's clear by inspection that $\mathrm{Gal}(E/K) = \mathrm{Cl}_K/(\mathrm{Cl}_K)^2$ is the maximal quotient of exponent 2. Let $\mathfrak{p}$ be a prime of K lying over p. Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and $\mathfrak{p}$ splits in E, so that $[\mathfrak{p}] \in (\mathrm{Cl}_K)^2$. Thus by theorem 2.4 there is a fractional ideal $\mathfrak{U}$ of I_K such that $[\mathfrak{p}] = [\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$. Observe that $N_{K/\mathbb{Q}}(\sigma(\mathfrak{U})\mathfrak{U}^{-1}) = 1$. It follows that $[\mathfrak{p}]^n$ is represented by a fractional ideal of norm p for all n. Since Cl_K is finite, this implies there is a principal fractional ideal in K of norm p. □

The extended genus field E^+ is easier to describe than E.

Theorem 2.6. *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}.*

Theorem 2.7. *Let the discriminant of K be Δ and suppose $|\Delta| = p_1 p_2 \cdots p_t$ where $p_2, \ldots p_t$ are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is*

$$E^+ = \mathbb{Q}(\sqrt{d}, p_2^*, \ldots p_t^*) = K(p_2^*, \ldots p_t^*),$$

where

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

Corollary 2.8. *Let q be a prime in $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$ as above. If $q \equiv 1 \pmod{|\Delta|}$, then q is the norm of a principal ideal in K.*

Proof. Any prime above q in K splits in E^+, hence also in E. □

We want to understand when p is the norm of an element. Note that if $H = H^+$, then p being the norm of an ideal guarantees that it is the norm of an element. If -1 is a norm in our field then we are also fine.

Theorem 2.9. *Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$ with m odd. Suppose that K is real. Then -1 is the norm of an element from K.*

Proof. be more specific Any prime dividing d is congruent to 1 (mod 4). This implies that d is the sum of two squares, which implies that $-1 = x^2 - dy^2$ for some $x, y \in \mathbb{Q}$. □

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.

Proposition 2.10. *$\mathbb{Q}(\sqrt{p^*})$ has odd narrow class number.*

Corollary 2.11. *The prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

3 Norm relations

3.1 Representation theory of finite groups

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

Definition 3.1. Let $\chi_1, \dots \chi_h$ be the distict characters of the complex irreducible representations of G. Then the **representation ring** of G is

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

We can also view this as the Grothendieck group of the category of finitely generated $\mathbb{C}[G]$-modules.

Let K be a number field. Denote by $R_K(G)$ the group generated by characters of the reprsentations of G over K. This is a subring of $R(G)$. The characters of the distinct irreducible representations of G over K form an orthogonal basis of $R_K(G)$ (cf. Serre Proposition 32). Let m be the exponent of G. If K contains the m-th roots of unity, then $R_K(G) = R(G)$. This implies every representation of G can be realized over K. (Serre 12.3)

The rank of $R_K(G)$ is discussed in Serre 12.4. For example, the rank of $R_{\mathbb{Q}}(G)$ is equal to the number of conjugacy classes of cyclic subgroups of G.

Notation 3.2. For $\rho \in R_{\mathbb{C}}(G)$ an irreducible character let

$$\widetilde{\rho} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho) \cdot \rho^\sigma \quad \in R_{\mathbb{Q}}(G),$$

where $m(\rho) \in \mathbb{Z}$ is the Schur index of ρ.

Then $\widetilde{\rho}$ is the character of an irreducible rational representation. Every irreducible rational representation can be obtained this way. We can extend this map additively to a surjective map $R_{\mathbb{C}}(G) \to R_{\mathbb{Q}}(G)$.

3.2 The Burnside ring and relations

Let G be a finite group. Recall that there is a bijection between the isomorphism classes of transitive finite G-sets and the conjugacy classes of subgroups $H \leq G$, given by sending a transitive G-set X to $H = \mathrm{Stab}_G(x)$ for some $x \in X$. Then the action of G on X is equivalent to the action of G on G/H.

Definition 3.3. Let $[X]$ denote the isomorphism class of a G-set X. The **Burnside ring** $B(G)$ is the free abelian group on isomorphism classes of finite G-sets, modulo the relations $[S] + [T] = [S \sqcup T]$. This is a ring; multiplication is given by $[S] \cdot [T] = [S \times T]$. Using the identification of finite G-sets with subgroups of G, we write elements of $B(G)$ as $\sum_i n_i H_i$ for $n_i \in \mathbb{Z}$, $H_i \leq G$.

Notation 3.4. There is a homomorphism from the Burnside ring to the rational representation ring $R_{\mathbb{Q}}(G)$ of G given by taking the corresponding permutation representation:

$$\mathbb{C}[-]\colon B(G) \to R_{\mathbb{Q}}(G), \qquad \Theta = \sum_i n_i H_i \;\mapsto\; \mathbb{C}[\Theta] = \sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1}_{H_i}.$$

Elements in the kernel of this map are known as **Brauer relations**. These show instances of non-isomorphic G-sets giving rise to isomorphic permutation representations.

Example 3.5. S_3 example

Example 3.6. Cyclic groups have no Brauer relations.

We are interested in elements of $B(G)$ with image isomorphic to $\widetilde{\rho}$ for $\rho \in R_{\mathbb{C}}(G)$.

Definition 3.7. We call $\Theta = \sum_i n_i H_i \in B(G)$ a **ρ-relation** if $\mathbb{C}[\Theta] \simeq \widetilde{\rho}$.

There are #(Brauer relations) +1 such elements Θ. Of course, when $\rho = 0$ these are Brauer relations.

Example 3.8. Let $G = C_n$. For each $d \mid n$, let $\chi_d = \widetilde{\varphi_d}$, where φ_d is an irreducible complex character of G with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d. Then $\{\chi_d\colon d \mid n\}$ form an orthogonal basis for the irreducible rational-valued representations of G. Note that $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G contain $C_{n/d}$ in their kernel. Thus, $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain the *unqiue* φ_d-relation for each $d \mid n$:

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

Notation 3.9. For $D \leq G$, define maps $\mathrm{Res}_D\colon B(G) \to B(D)$ and $\mathrm{Ind}_D\colon B(D) \to B(G)$ by

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

These correspond to the reprsentation theory side, where $\mathrm{Res}_D \mathrm{Ind}_H^G \mathbb{1} = \sum_{x \in H\backslash G/D} \mathrm{Ind}_{D \cap H^{x^{-1}}}^D \mathbb{1}$ (Mackey's decomposition), and $\mathrm{Ind}_D^G \mathrm{Ind}_H^D \mathbb{1} = \mathrm{Ind}_H^G \mathbb{1}$.

3.3 Functions on the Burnside ring and norm relations

Consider multiplicative functions on the Burnside ring $\psi\colon B(G) \to \mathbb{Q}^\times$. Given $\rho \in R_{\mathbb{C}}(G)$ we can extend such functions from the Burnside ring to $\overline{\psi}\colon B(G) \to \mathbb{Q}^\times / N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.

Definition 3.10. If $\Theta \in \ker \overline{\psi}$, then $\psi(\Theta)$ is the norm of an element from $\mathbb{Q}(\rho)^\times$. We call an instance of this a **norm relation**.

Definition 3.11. We say two functions ψ, ψ' are **ρ-equivalent**, written $\psi \sim_\rho \psi'$, if $\overline{\psi/\psi'}$ is trivial on all ρ-relations. Equivalently, $\psi(\Theta)/\psi'(\Theta)$ is a norm relation for all ρ-relations Θ.

Remark 3.12. If $\rho = 0$ then we call functions $\psi \sim_\rho 1$ **representation theoretic**. These have been studied in cite.

Example 3.13. Take $\rho = 0$, and V a representation of G. The function $\psi(H) = \dim V^H$ satisfies $\psi \sim_\rho 1$ as $\dim V^H = \langle \mathrm{Res}_H V, \mathbb{1}_H \rangle = \langle V, \mathrm{Ind}_H^G \mathbb{1} \rangle$ by Frobenius reciprocity.

Example 3.14. Let $G = C_p$ for p a prime. Let ρ be a character of degree p. There is a unique ρ-relation given by $\Theta = C_1 - C_p$. Let $\psi(H) = [G\colon H]$. Then $\psi(\Theta) = p$, which is a norm from $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ by Corollary 2.11.

Example 3.15. Let $E/\mathbb{Q}$ be an elliptic curve, $G = \mathrm{Gal}(F/\mathbb{Q})$ for $F/\mathbb{Q}$ a Galois extension. For $H \leq G$, the function $\psi\colon H \mapsto C(E/F^H)$ extends to a multiplicative function on the Burnside ring. Given a representation ρ of G, one can ask when $\psi \sim_\rho 1$.

3.4 D-local functions

Maybe just add in definition of D-local function, and explain all this way better. Maybe also some parts of Theorem 2.36 in the reg consts paper (the parts that translate).

(This is taken from section 2.3 of Vlad and Tim's regulator constants paper.)

Consider $G = \mathrm{Gal}(F/\mathbb{Q})$ and intermediate field F^H for $H < G$. Let p be a prime with decomposition group D in G. Then the primes above p in F^H correspond to double cosets $H\backslash G/D$. If a prime w in F^H coresponds 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. In partiular, the ramification degree and residue degree over $\mathbb{Q}$ are given by $e_w = \frac{|I|}{|H \cap I^x|}$ and $f_w = \frac{[D\colon I]}{[H \cap D^x\colon H \cap I^x]}$.

Our fudge factors $C(E/F)$ are defined locally; one has $C(E/F) = \prod_v c_v(E/F) \cdot |\omega/\omega_{v,\min}|$. Here v runs over finite places of F, ω is a global minimal differential for $E/\mathbb{Q}$, and $\omega_{v,\min}$ is a minimal differential at v. Considering the function $H \mapsto C(E/F^H)$, and writing $C_p(E/F^H) = \prod_{v|p} c_v(E/F) \cdot |\omega/\omega_{v,\min}|$ one has

$$\sum_i n_i H_i \mapsto \prod_i C(E/F^{H_i})^{n_i} = \prod_p C_p(E/F^H)^{n_i}.$$

Therefore, our function is the product of local functions for each p. Since $C_p(E/F^H)$ depends on e_w, f_w for $w|p$, we are motivated to define the following:

Definition 3.16. Suppose $I \triangleleft D < G$ with D/I cyclic, and $\psi(e, f)$ is a function of $e, f \in \mathbb{N}$. Define

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

Then, this is a function on the Burnside ring.

try make thick brackets

Example 3.17. For semi-stable reduction, we're considering $\psi(e, f) = e$ (the Tamagawa number). For the d_v terms in the case of additive potentially good reduction at p (p not equal to 2 or 3), we consider $\psi(e, f) = p^{f\lfloor en/12 \rfloor}$, where $n \in \{2, 3, 4, 6, 9, 10\}$.

Example 3.18. Let $\rho = 0$. If W is a group of odd order, then $(W, W, e) \sim 1$ as functions to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. More generally if D has odd order and $I \triangleleft D$ then $(D, I, e) \sim_\rho 1$. explain and reference

4 Forcing points of infinite order

In [Dok-Wier-Ev], they establish a (dependent on some conjectures) test for forcing a point of infinite order.

Theorem 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G, ρ an irreducible representation of G and*

$$\left(\bigoplus_{g\in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^g\right)^{\oplus m(\rho)} = \left(\bigoplus_i \mathrm{Ind}_{H_i}^G \mathbb{1}\right) \ominus \left(\bigoplus_j \mathrm{Ind}_{H_j'}^G \mathbb{1}\right), \tag{1}$$

for some $m(\rho)\in\mathbb{Z}$ and subgroups $H_i, H_j' \leq G$.

If either $\prod_i C(E/F^{H_i})/\prod_j C(E/F^{H_j'})$ is not a norm from some quadratic field $\mathbb{Q}(\sqrt{D})\subset\mathbb{Q}(\rho)$, or if it is not a rational square when $m(\rho)$ is even, then E has a point of infinite order over F.

In this paper, they give two examples of applications of this theorem. Of course, another means of forcing infinite order is via root numbers. We are currently unsure as to whether this norm test is weaker/equivalent/stronger than the test of root numbers. For example, in odd order extensions, root numbers don't tell us anything. We show in the next section that this norm test doesn't either, that is, the product of Tamagawa numbers is always a norm.

As discussed in section 3.4, the function on $B(G)$ sending $H\mapsto C(E/F^H)$ is the product of local functions depending on the decomposition group D_p at a prime p. We denote each of these as (D_p, I_p, ψ_p), as in definition 3.16. Then the product of Tamagawa numbers in 4.1 is the evaluation of $\prod_p (D_p, I_p, \psi_p)$ on $\sum_i H_i - \sum_j H_j'$.

If we are interested in evaluating each (D_p, I_p, ψ_p) individually, then we have some freedom to change our field extension to make computations easier. In particular,

Lemma 4.2. *In an odd degree unramified extension, Tamagawa numbers change only up to squares. In particular, if $[D_p\colon I_p]$ is odd, then $(D_p, I_p, \psi_p) \sim_\rho (D_p, D_p, \psi_p)$ for any ρ with $[\mathbb{Q}(\rho)\colon\mathbb{Q}]$ even.*

Proof. Yadada □

4.1 Compatibility in odd order extensions

In this section we prove the following:

Theorem 4.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $F/\mathbb{Q}$ be an extension of **odd order** with Galois group G. Suppose that the primes of additive reduction of E are at worst tamely ramified in $F/\mathbb{Q}$ (and ≥ 5).*

Then for any representation ρ of G and any expression as in (1), the corresponding ratio of Tamagawa numbers is a norm from any quadratic subfield of $\mathbb{Q}(\rho)$.

If $\mathbb{Q}(\rho)=\mathbb{Q}$ there is nothing to prove. If $[\mathbb{Q}(\rho)\colon\mathbb{Q}]>1$ then this index is even. Indeed, since G has odd order, all its characters are complex, so there is an element $\sigma\in\mathrm{Aut}(\mathbb{Q}(\rho)/\mathbb{Q})$ that acts by complex conjugation (i.e. is of order 2). Therefore there is a quadratic subfield $\mathbb{Q}(\sqrt{d})\subset\mathbb{Q}(\rho)$. Choose any such quadratic subfield.

Replacing ρ by the sum of its conjugates by elements of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{d}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{d})$. Let τ be the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Let m be the smallest integer such that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$. Then m divides the exponent of G, hence is odd.

We prove that each (D_p, I_p, ψ_p) satisfies $(D_p, I_p, \psi_p) \sim_\rho 1$. Since we deal with each local factor individually, we may assume that $D_p = I_p$ by theorem 4.2.

Good reduction

If $E/\mathbb{Q}$ has good reduction at p, then it has good reduction at all primes lying above p in subfields of F. Thus $C_p(E/F_i) = 1$ for each subfield $F_i \subset F$, so that $(D_p, I_p, \psi_p) = 1$ on ρ-relations.

Multiplicative reduction

say that the dv term goes away

Non-split multiplicative reduction

Let p be a prime of muliplicative reduction. First suppose that this reduction is non-split. Since $D_p = I_p$, all primes above p have residue degree 1. Thus the reduction type remains non-split at primes above p. Therefore $\psi_p = 1$ or 2, depending on $\mathrm{ord}_p(\Delta)$ being even or odd.

We prove a more general lemma that constant functions are trivial on ρ-relations.

Lemma 4.4. *Let G, ρ be as above. If (D_p, I_p, ψ_p) is such that ψ_p is constant, then $(D_p, I_p, \psi_p) \sim_\rho 1$.*

Proof. Let $\psi_p = \alpha$. Then (D_p, I_p, ψ_p) sends $H \leq G$ to $\alpha^{|H\backslash G/D_p|}$. Thus if $\Theta = \sum_i n_i H_i$ is a ρ-relation, $(D_p, I_p, \psi_p)(\Theta) = \alpha^{\sum_i n_i \cdot |H_i\backslash G/D_p|}$. We show that $\sum_i n_i \cdot |H_i\backslash G/D_p|$ is even.

One has $\mathrm{Res}_D\Theta = \sum_i n_i \sum_{x\in H_i\backslash G/D} D \cap H^{x^{-1}}$ and the permutation representation $\mathbb{C}[\mathrm{Res}_D\Theta]$ of D is isomorphic to $\mathrm{Res}_D(\rho \oplus \tau(\rho))$. In particular the dimension of this permutation representation is even. The dimension is $\sum_i n_i \sum_{x\in H_i\backslash G/D}[D\colon D \cap H^{x^{-1}}]$. Since each $[D\colon D \cap H^{x^{-1}}]$ is odd, this implies there are an even number of terms in the summation, i.e. that $\sum_i n_i \cdot |H_i\backslash G/D_p|$ is even.

□

Split multiplicative reduction

Now suppose that p has split multiplicative reduction. Then $\psi_p(e, f) = e$. The following result shows that if $\mathbb{Q}(\mathrm{Res}_{D_p}\rho) = \mathbb{Q}$, then $(D_p, I_p, \psi_p) \sim_\rho 1$.

Lemma 4.5. *Let G, ρ be as above, $D_p \leq G$. Let the exponent of D_p be b. If $m \nmid b$, then $(D_p, I_p, \psi_p) \sim_\rho 1$.*

Proof. Note that $\mathbb{Q}(\mathrm{Res}_{D_p}\rho) \subset \mathbb{Q}(\zeta_b) \cap \mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b)$. Then $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b) \implies m \mid b$ by minimality of m. Thus, if $m \nmid b$, one has $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_b)$ and so $\mathbb{Q}(\mathrm{Res}_{D_p}\rho) = \mathbb{Q}$.

Then, $\mathrm{Res}_{D_p}\rho = \tau(\mathrm{Res}_{D_p}\rho)$. Let Θ be a ρ-relation. It follows that every rational representation that is a summand of $\mathbb{C}[\mathrm{Res}_{D_p}\Theta]$ arises with multiplicity two. Thus, there is a $(\mathrm{Res}_{D_p}\rho)$-relation Θ' such that $\mathbb{C}[\mathrm{Res}_{D_p}\Theta] \simeq \mathbb{C}[2\Theta']$. This means $\Psi = \Theta - 2\Theta'$ is a Brauer relation for D_p. Therefore, $(D_p, I_p, \psi_p)(\Theta) =$

$(D_p, I_p, \psi_p)(\Psi) \cdot (D_p, I_p, \psi_p)(2\Theta') = (D_p, I_p, e)(\Psi) \cdot (D_p, I_p, \psi_p)(\Theta')^2 = 1$ as as function to $\mathbb{Q}^\times/\mathbb{Q}^\times$. Indeed $(D_p, I_p, e) = 1$ as a function to $\mathbb{Q}^\times/\mathbb{Q}^\times$ on Brauer relations, as per example 3.18. □

We have $D_p = I_p = P_p \ltimes C_l$, 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 the previous result, it is only of interest to consider decomposition groups $D_p = P_p \ltimes C_l$, with $m \mid p^u l$ for some $u \geq 0$.

In this case, $(D_p, I_p, \psi_p)(\Theta)$ is the product of ramification indices at primes above p. We seperate 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 $\frac{|I_p|}{|H_i \cap I_p^x|} = \frac{|I_p|}{|I_p \cap H^{x^{-1}}|}$. This is the dimension of the permutation representation $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]$. Let $D_p \cap H^{x^{-1}} = P' \ltimes C_k$ where $P' \leq P$ and $k|l$. Then the ramification index is $\frac{|P|}{|P'|} \cdot \frac{l}{k}$.

Consider taking fixed points $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p} \simeq \mathbb{C}[D_p/P_p(D_p \cap H^{x^{-1}})] \simeq \mathbb{C}[D_p/P_p \ltimes C_k]$. Now this has dimension $\frac{l}{k}$, so we've killed off the p-part. Then $\mathbb{C}[\mathrm{Res}_{D_p}\Theta]^{P_p} \simeq \big(\mathrm{Res}_{D_p}\rho \oplus \tau(\rho)\big)^{P_p}$. Both sides have P_p in their kernel, so we can project this relation to the quotient $D_p/P_p \simeq C_l$. Then (C_l, C_l, e) evaluated at $P_p \cdot \mathrm{Res}_{D_p}\Theta/P_p$ equals (D_p, D_p, ψ_p) evaluated at $\mathrm{Res}_{D_p}\Theta$ modulo squares up to (possibly) a factor of p.

It turns out that this factor of p doesn't matter:

Lemma 4.6. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, contained in the minimal cyclotomic field $\mathbb{Q}(\zeta_m)$ with m odd. Let $m \mid p^u l$, for some $u \geq 0$ and l such that $p \equiv 1 \pmod{l}$. Then p is the norm of an element from $K^\times$.*

Proof. Since m is odd, it is clear that $d = \prod_{q|m} q^*$. We show that p has inertial degree 1 in the extended genus field $E^+ = K(\{\sqrt{q^*} : q|m\})$ of K. If $q \neq p$ then $q \mid l$, so $p \equiv 1 \pmod{l}$. Therefore p splits in any quadratic subfield of E^+ of disriminant not divisible by p. Else, p ramifies in any quadratic subfield with discriminant divisible by p. Thus it is clear that p has inertial degree 1 in E^+, hence also in the genus field E, and it follows from theorem 2.5 that p is the norm of a principal ideal. If K is imaginary then p is the norm of an element of K. Else, we invoke theorem 2.9. □

Thus, we only need to worry about the tame part of our ramification indices. If $m \nmid l$, then $\phi = (\mathrm{Res}_{D_p}\rho)^{P_p}$ (viewed as a representation on D_p/P_p) has rational character. Therefore by lemma 4.5, $(C_l, C_l, e) \sim_\phi 1$ as a function to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Therefore we may assume that $m \mid l$ and that ϕ has $\mathbb{Q}(\phi) = \mathbb{Q}(\rho) = K$.

Proposition 4.7. *Let $m \mid l$, then one has $(C_l, C_l, e) \sim_\phi 1$.*

Proof. Let Ψ be a ϕ-relation. One may write $\phi \oplus \tau(\phi) = \mathbb{C}[\Psi] = \sum_{k|l} a_k \chi_k$ where $a_k \in \mathbb{Z}$ and χ_k are defined in example 3.8. Writing each χ_k in terms of permutation representations as in the example, one obtains an expression for $\mathbb{C}[\Psi]$, noting this is exact since cyclic groups have no Brauer relations.

Evaluating e on χ_k is trivial unless $k = q^a$ for some q prime, $a \geq 1$. Indeed, if $k = p_1^{e_1} \cdots p_r^{e_r}$, with $r \geq 2$ and $e_i \geq 1$, then maybe expand on this

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

On the other hand,

$$\prod_{k' | q^a} (k')^{\mu(q^a/k')} = q.$$

We claim that $m \nmid k$ implies a_k is even. The irreducible representations of C_l over $\mathbb{Q}(\phi)$ are given by the orbits of the complex irreducible characters of C_l acted upon by $H = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\phi))$. One has $\chi_k = \widetilde{\varphi_k}$ where $\mathbb{Q}(\varphi_k) = \mathbb{Q}(\zeta_k)$. If $m \nmid k$ then $\mathbb{Q}(\phi) \not\subset \mathbb{Q}(\zeta_k)$, so that $B = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_k)) \not\leq H$. Then $\mathbb{Q}(\phi) = \mathbb{Q}(\zeta_k) = \mathbb{Q}$ so $BH = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. Then the orbit of φ_k under H is fixed by BH, hence is rational. It follows that $\langle \phi, \varphi_k \rangle = \langle \tau(\phi), \varphi_k \rangle$ so that a_k is even.

Thus we can only possibly get something interesting if $m = q$ is a prime. But then q is a norm from $\mathbb{Q}(\sqrt{q^*})$ by corollary 2.5. □

4.1.1 Additive reduction

Now suppose that E has additive reduction at p. In this case, assume that $p \geq 5$ is at worst tamely ramified in $F/\mathbb{Q}$. This ensures that $D_p = I_p = C_l$ is cyclic, and $l \mid p - 1$.

Potentially multiplicative reduction

TO DO

Potentially good reduction

Lemma 4.8. *Consider M/L a field extension. Let E/L be an elliptic curve, v a finite place of L and w a finite place of M with $w \mid v$. Let ω_v and ω_w be the minimal differentials for E/L_v and E/M_w respectively.*

Then, if E/K_v has potentially good reduction and the residue characteristic is not 3 or 2, one has

$$\left| \frac{\omega_v}{\omega_w} \right|_w = q^{\lfloor \frac{e_{F/K} \cdot \mathrm{ord}_v(\Delta_{E,v}^{\min})}{12} \rfloor},$$

where q is the size of the residue field at w.

We consider $F/\mathbb{Q}$ with additive potentially good reduction at p . Since $D_p = I_p$, the size of the residue field is p at all intermediate extensions. Let $n = v_p(\Delta)$. Then $n \in \{2, 3, 4, 6, 8, 9, 10\}$. Consider (D_p, I_p, ψ_p) where $\psi_p(e, f) = p^{\lfloor en/12 \rfloor}$. Then $(D_p, I_p, \psi_p) \sim_\rho 1$. Indeed, this takes values 1 or p in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. But $p \equiv 1 \pmod{l}$ implies that p is the norm of a principal ideal in $\mathbb{Q}(\rho)$, and hence the norm of an element, by corollary 2.8 and theorem 2.9.

The Tamagawa numbers take a little more work. We use the following description of Tamagawa numbers.

Lemma 4.9. *Let $K'/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let E/K be an elliptic curve with addtive reduction;*

$$E\colon y^2 = x^3 + Ax + B,$$

with discriminant $\Delta = -16(4A^3 + 27B^2)$. Let $\delta = v_K(\Delta)$, and $e = e_{K'/K}$.

If E has potentially good reduction, then

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

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

So suppose an elliptic curve $E/\mathbb{Q}$ has additive reduction at p, with $p \geq 5$. Then we can write $E\colon y^2 = x^3 + Ax + B$. Let $D = \mathrm{Gal}(F_\mathfrak{p}/\mathbb{Q}_p)$ be the local Galois group at p. Assume that p is totally tamely ramified, so that $D = I = C_n$. Since there is no wild ramification, and $f = 1$, this means that $n \mid p-1$. We consider the contribution corresponding to an irreducible rational character χ_d of D, given by

$$\prod_{d' \mid d} C(E/F_\mathfrak{p}^{D_{d'}})^{\mu(d/d')}. \tag{2}$$

Observe that in a totally ramified extension of degree coprime to 12, the Tamagawa number remains the same. If $(12, d) = 1$, then $(12, d') = 1$ for $d' \mid d$, so the Tamagawa number is consant accross subfields $F_\mathfrak{p}^{D_{d'}}$. Therefore,

$$\prod_{d' \mid d} C(E/F_\mathfrak{p}^{D_{d'}})^{\mu(d/d')} = C(E/\mathbb{Q}_p)^{\sum_{d' \mid d} \mu(d/d')} = 1,$$

assuming $d > 1$.

So we only need to worry about when $3 \mid d$. If we have type III or III^* or I_0^* then the Tamagawa number is still unchanged in any totally ramified cyclic extension of degree dividing d. We will treat the other cases seperately:

Type II and II^* reduction:

Firstly, suppose that $\delta = 2$, that is we have Type II reduction. If $3 \mid d'$ then $E/F_\mathfrak{p}^{D_{d'}}$ has type I_0^* reduction. The Tamagawa number 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 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 $p \equiv 1 \pmod{n}$, so $p \equiv 1 \pmod{3}$. Therefore the Tamagawa number will be 1 or 4, which is a square. If $3 \nmid d'$ then the reduction type over $F_\mathfrak{p}^{D_{d'}}$ is II or II^*. Then the Tamagawa number is 1. Thus in total, we get a square contribution from (2).

If $\delta = 10$, then $E/F_{\mathfrak{p}}^{D_{d'}}$ has reduction type I_0^* whenever $3 \mid d'$. Once more, $v_p(A), v_p(B) \geq 1$, and $v_p(\Delta) = 10 = \min(3v_p(A), 2v_p(B))$ maybe this is suss $\implies v_p(B) = 5$. Therefore we get $\Delta = p^{10}\alpha$ 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 our Tamagawa number product, when $\sqrt{B} \notin \mathbb{Q}_p$.

In summary,

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')} = \begin{cases} 1 & 3 \nmid d, \\ 1 & 3 \mid d, \delta \in \{0,3,6,9\}, \\ 1 \cdot \square & 3 \mid d, \delta \in \{2,10\}, \\ 3^a \cdot \square, a \in \{0,1\} & 3 \mid d, \delta \in \{4,8\}. \end{cases} \tag{3}$$

Remark 4.10. There's no reason why we can't get 3; see elliptic curve 441b1 with additive reduction at 7 of type IV and Tamagawa number equal to 3

However, it turns out we will only get 3 occuring oddly when $d = 3$. Indeed, one has that $\langle \mathrm{Ind}_{D_{d'}}^{D} \mathbb{1}, \psi_3 \rangle = 1$ if $3 \mid d'$, and 0 if $3 \nmid d'$, where ψ_3 is an irreducible character of D of order 3. Therefore one sees that the number of places with ramification degree divisible by 3 cancels unless $d = 3$. Indeed, $\langle \chi_d, \psi_3 \rangle = 0$ unless $d = 3$, in which case it is 1. Therefore (2) can only be non-square when $d = 3$. then conclude why this is fine

References

[BH06] C. J. Bushnell and G. Henniart, *The Local Langlands Conjecture for GL(2)*, Grundlehren der mathematischen Wissenschaften, Springer Berlin, 2006.