Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

March 21, 2024

Contents

1 Birch and Swinnerton-Dyer Conjecture 4

2 Algebraic number theory and representation theory background 5

2.1 Representation theory of finite groups . . . 5

2.1.1 Permutation representations and the Burnside ring . . . 5

2.2 Decompositions of primes in field extensions . . . 5

2.3 Class field theory . . . 5

3 Proving things... 6

3.1 Norm relations . . . 6

3.1.1 D-local functions . . . 6

3.2 Compatibility in odd order extensions . . . 6

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 $\mathbb{Q}(\rho)$,

1 Birch and Swinnerton-Dyer Conjecture

2 Algebraic number theory and representation theory background

2.1 Representation theory of finite groups

Let G be a finite group. Recall that a **representation** of G is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$ where V is a complex vector space. Associated to a representation ρ is a **character** $\chi\colon G \to \mathbb{C}^\times$, 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.

Given an irreducible $\mathbb{Q}G$-representation with character ψ, we have that

$$\psi = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho) \cdot \rho^\sigma$$

for ρ the character of an irreducible $\mathbb{C}G$-representation, and $m(\rho)$ the Schur index.

In particular, the map $R_{\mathbb{C}}(G) \to R_{\mathbb{Q}}(G)$ given by sending an irreducible complex character ρ to $\tilde{\rho} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho) \cdot \rho^\sigma$ is surjective.

Induction, Restriction...

Theorem 2.1 (Mackey Decomposition)**.**

2.1.1 Permutation representations and the Burnside ring

Let G be a finite group. The **Burnside ring** $B(G)$ is the ring of formal sums of isomorphism classes of finite G-sets. We have addition by disjoint union: $[S] + [T] = [S \sqcup T]$, and multiplication by Cartesian product: $[S] \times [T] = [S \times T]$ for S, T finite G-sets.

There exists a bijection between the isomorphism classes of transitive G-sets and the conjugacy classes of subgroups $H \leq G$, where H is the stabilizer of a point on which G acts. Then any transitive G-set X is isomorphic to the action of G on G/H for $H \leq G$, so that we can consider $B(G)$ to be a $\mathbb{Z}$-module generated by the orbits of the action of G on the elements $\{G/H \colon H \leq G\}$, where we consider H up to conjugacy. For notational purposes, we then write elements $\Theta \in B(G)$ as $\Theta = \sum_i n_i H_i$ with $n_i \in \mathbb{Z}$, $H_i \leq G$.

Given a transitive G-set G/H for $H \leq G$, we can look at the permutation representation $\mathbb{C}[G/H]$. This defines a homomorphism from the Burnside ring to the rational representation ring $R_{\mathbb{Q}}(G)$ of G:

$$a\colon B(G) \to R_{\mathbb{Q}}(G), \qquad \sum_i n_i H_i \mapsto \sum_i n_i \mathrm{Ind}_{H_i}^G \mathbb{1}_{H_i}.$$

Elements in the kernel of this map are known as **Brauer relations**

2.2 Decompositions of primes in field extensions

2.3 Class field theory

3 Proving things...

3.1 Norm relations

Recall that in Section 2.1, we associated to $\rho \in R_{\mathbb{C}}(G)$ the character

$$\tilde{\rho} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} m(\rho)\rho^{\sigma}.$$

We call $\sum_i n_i H_i \in B(G)$ a **ρ-relation** if

$$\sum_i n_i \mathrm{Ind}_{H_i}^{G} \mathbb{1} \simeq \tilde{\rho}.$$

Given such a ρ, consider functions $\psi \colon B(G) \to \mathbb{Q}^{\times}/N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$ (written multiplicatively). We say two functions ψ, ψ' are equivalent, written $\psi \sim_{\rho} \psi'$, if ψ/ψ' is trivial on all ρ-relations.

Remark 3.1. If $\rho = 0$ then we call functions $\psi \sim_{\rho} 1$ **representation theoretic**. These have been studied in cite.

Example 3.2. Consider $G = C_2 \times C_2$.

3.1.1 D-local functions

3.2 Compatibility in odd order extensions

In this section we work towards proving the following:

Theorem 3.3. *Let $F/\mathbb{Q}$ be a Galois extension of odd degree, with $G = \mathrm{Gal}(F/\mathbb{Q})$. Consider a semistable elliptic curve $E/\mathbb{Q}$ with good reduction at primes that are wildly ramified in $F/\mathbb{Q}$.*

Then, for any $\rho \in R_{\mathbb{C}}(G)$ with $[\mathbb{Q}(\rho) \colon \mathbb{Q}] > 1$, the function $f \colon B(G) \to \mathbb{Q}^{\times}/N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^{\times})$ sending $H \mapsto C(E/F^H)$ satisfies $f \sim_{\rho} 1$.

We look at a relation of the form

$$\sum_i n_i \mathrm{Ind}_{H_i}^{G} \mathbb{1} \simeq \rho \oplus \tau(\rho), \tag{1}$$

where ρ is a character of G with $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = \langle \tau \rangle$ of size 2. In particular we let m denote the minimal positive integer such that $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_m)$. The sum on the left is over subgroups $H_i \subseteq G$.

If I consider $\mathrm{Res}_D(\rho)$ where D is a decomposition group of exponent k, then for $\mathrm{Res}_D(\rho)$ to be non-rationally valued, one needs $m|k$. Note that in the context of norm relations, if $\mathrm{Res}_D(\rho) = \mathrm{Res}_D(\tau(\rho))$, then we always get squares.

So now suppose that $D = I = C_n$ with $m|n$. Applying Res_D to (1), we get

$$\sum_i n_i \sum_{x \in H_i \ G/D} \mathrm{Ind}_{D \cap x^{-1} H_i x}^{D} \mathbb{1} \simeq \mathrm{Res}_D \rho \oplus \tau(\mathrm{Res}_D \rho). \tag{2}$$

Since both sides are now rationally valued, we can write this as $\sum_{d|n} a_d \cdot \chi_d$ where $a_d \in \mathbb{Z}$ and $\{\chi_d \colon d|n\}$ form a basis for the irreducible rational-valued representations of D. Explicitly, χ_d is the sum of the Galois conjugates of an irreducible complex character of D with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d (which we'll write as D_d).

We can write each χ_d in terms of permutation modules:

$$\chi_d = \sum_{d'|d} \mu(d'/d) \mathrm{Ind}_{D'_d}^{D} \mathbb{1}. \tag{3}$$

Substituting this into $\sum_{d|n} a_d \cdot \chi_d$ gives an expression for the LHS of (1). In particular, if we have a D-local function, we can evaluate it on each χ_d-relation as in (3). Then the total expression is the product of these, raised to a_d.

References

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