On certain invariants of rational and integral representations and their number-theoretic applications

Alex Bartel
Supervisor: Dr. Tim Dokchitser

Abstract

In this essay, we study certain invariants that can be attached to rational and integral representations of a finite group. These invariants arise naturally in a number theoretic context, more specifically in the theory of elliptic curves. We will investigate the behaviour of these invariants and then apply our representation theoretic results to the theory of elliptic curves. Our main number theoretic result says that p-Selmer groups of elliptic curves which are defined over $\mathbb{Q}$ can be arbitrarily large in Galois extensions of degree $2p$.

Extent of originality. Section 1 is introductory, none of this material is original, but was developed in [5] and [7]. The content of section 2 is original. It was inspired by the proof of [6, Lemma 3.2]. All the results of section 3 are original work except for the statement of Theorem 3.4. In section 3.2, everything following the statement of Conjecture 3.8 is original. Conjecture 3.8 itself was proposed to me by Tim and Vladimir Dokchitser in oral communication. In section 4 everything is original work except for the classification of indecomposable integral representations of D_{2p} which was done in [9]. All of the last section is original work, except for theorems 5.7 and 5.14, which are quoted with citations.

In summary, all results which are given with proof are original. For all results which are not due to me, citations are provided.

No part of this work was done in collaboration. But to formulate conjectures and to test approaches, I have made extensive use of MAGMA programs written by Tim Dokchitser.

Contents

Introduction

Suppose that E/K is an elliptic curve over a number field and let F/K be a finite Galois extension with Galois group G. Let H_i and H'_j be subgroups of G such that we have an isomorphism of permutation representations $\bigoplus_i \mathbb{C}[G/H_i] \cong \bigoplus_j \mathbb{C}[G/H'_j]$. Then Artin formalism for L-functions implies that we have an equality of L-functions $\prod_i L(E/L_i, s) = \prod_j L(E/L'_j, s)$, where $L_i = F^{H_i}$, $L'_j = F^{H'_j}$ are the corresponding intermediate subfields of F. In such a case, the products of the leading coefficients of the L-functions at $s = 1$ are equal and so the famous conjecture of Birch, Swinnerton-Dyer and Tate as formulated in [17] predicts that we should have an equality of the corresponding quotients

$$\prod_i \frac{\#Ш(E/L_i)\mathrm{Reg}(E/L_i)C(E/L_i)}{|E(L_i)_{\mathrm{tors}}|^2} = \prod_j \frac{\#Ш(E/L'_j)\mathrm{Reg}(E/L'_j)C(E/L'_j)}{|E(L'_j)_{\mathrm{tors}}|^2}. \tag{1}$$

where $C(E/L)$ is the product of the Tamagawa numbers at the finite places of L, Ш is the Tate-Shaffarevich group and $\mathrm{Reg}(E/L)$ is the regulator, i.e. the determinant of the Néron-Tate height pairing evaluated on a basis of $E(L)/E(L)_{\mathrm{tors}}$. Other quantities featuring in the conjectural expression for the leading coefficients of the L-functions at $s = 1$ cancel in a relation such as that above. In particular, we see that $\frac{\prod_i \mathrm{Reg}(E/L_i)}{\prod_j \mathrm{Reg}(E/L'_j)}$ is predicted to be a rational number, while, for all we know, each regulator itself might be transcendental. In fact, equation (1) really holds, provided all Tate-Shaffarevich groups are finite ([5, Theorem 2.3]), and so then the regulator quotient really is a rational number. This is explained by the fact that this regulator quotient is independent

of the pairing that is used to evaluate it and only depends on the Galois representation $E(F)/E(F)_{\mathrm{tors}}$ ([7, Theorem 2.17]). In particular, the value is the same as if the regulators were computed with respect to a $\mathbb{Q}$-valued pairing, rather than the height pairing. Since this is a purely representation theoretic quantity, it is important to understand the connections between the representation and the associated regulator quotient. Such an understanding should lead to connections between the Galois module structure of $E(F)/E(F)_{\mathrm{tors}}$ and other invariants of E such as the Tamagawa numbers, the size of the Tate-Shaffarevich group and the size of the torsion subgroup.

In [5] and [7] Tim and Vladimir Dokchitser have considered the rational representations $E(F)/E(F)_{\mathrm{tors}} \otimes \mathbb{Q}$ instead of the integral representations $E(F)/E(F)_{\mathrm{tors}}$. The corresponding regulator quotient is then only well-defined up to rational squares. But considering equation (1) up to rational squares gets rid of the Tate-Shaffarevich groups and the torsion subgroups. Thus, understanding some of the relationships between rational representations and their associated regulator quotients, Tim and Vladimir Dokchitser have been able to make statements about connections between parities of certain ranks and certain local data. In this essay we will further our understanding of such regulator quotients for rational representations and initiate the study of regulator quotients for integral representations. The two theories present very different features. We will then apply the representation theoretic result to the arithmetic of elliptic curves.

In section 1 we recall the definition of regulator constants from [5], the central object of our investigation, and quote some of its properties from [5] and [7].

In section 2 we give an alternative definition of regulator constants. It will enhance our understanding of the nature of regulator constants, as well as being more satisfactory in a certain sense, on which we remark at the beginning of the section.

We then proceed to derive several general results on the behaviour of regulator constants in section 3. The theory of regulator constants of integral representations differs widely from the theory of regulator constants of rational representations. Our main result on the former is a bound on the growth of regulator constants as a function of the $\mathbb{Z}$-rank of the representation. The main result on the latter is the proof of a very general conjecture of Tim and Vladimir Dokchitser in a special case. This part is very much work in progress, since we hope that the technique used in the special case should, with more work, yield much more general results.

As the content of section 3.2 will show, a very important family of groups for the understanding of regulator constants is that of the dihedral groups D_{2p} for p a prime number. In section 4 we compute all regulator constants of all integral representations of D_{2p}. As we remark at the beginning of that section, it is not clear a priori that this can be done at all or at least, that it is not extremely difficult.

Finally, in the last section we apply our representation theoretic results to study the growth of Selmer groups of elliptic curves in extensions of number fields. Our first main result is that p-Selmer groups of elliptic curves over $\mathbb{Q}$ can become arbitrarily large over Galois extensions of $\mathbb{Q}$ with Galois group D_{2p}. The second result is a lower bound on the growth as a function of the number of primes with certain ramification behaviour and certain type of reduction of the elliptic curve. This section can be read independently of sections 2-4 provided the reader is prepared to take the representation theoretic results on trust.

Acknowledgements. We would like to thank Arno Fehm for useful stylistic remarks on this manuscript, Antonio Lei for many helpful discussions, Vladimir Dokchitser for his keen interest in this work and Tim Dokchitser for his invaluable guidance, without which this work would not have been possible.

1 Relations and regulator constants

In this section we will introduce regulator constants, following [5] but using a slightly more flexible language. We will then quote some of the properties of regulator constants that we will need later.

1.1 Definitions

Let G be any finite group. We recall the following standard definitions (see e.g. [4]):

Definition 1.1. The Burnside ring of G is defined as the ring of formal $\mathbb{Z}$-linear combinations of isomorphism classes $[S]$ of finite G-sets modulo the relations

$$[S] + [T] = [S \sqcup T], \quad [S][T] = [S \times T],$$

where $S \sqcup T$ denotes the disjoint union and $S \times T$ denotes the cartesian product.

The set of isomorphism classes of transitive G-sets is in bijection with the set of conjugacy classes of subgroups of G via the map which assigns to the subgroup H the set of cosets G/H.

Definition 1.2. Let A be either $\mathbb{Q}$ or $\mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at a prime p. The representation ring of G over A is the ring of formal $\mathbb{Z}$-linear combinations of isomorphism classes $[M]$ of A-free finite dimensional AG-modules[1] modulo the relations

$$[M] + [N] = [M \oplus N], \quad [M][N] = [M \otimes N].$$

We have a natural map from the Burnside ring to the representation ring that sends a G-set S to the AG-module $A[S]$ with A-basis indexed by the elements of S and the natural G-action. If we take A to be $\mathbb{Q}$ then the image of the Burnside ring in the representation ring has finite index (called the Artin index of the group G).

Definition 1.3. We will call an element Θ of the kernel of the above map from the Burnside ring of G to the representation ring over A an AG-relation. If $A = \mathbb{Q}$ then we will drop A from the notation and just say that Θ is a G-relation.

Example 1.4. The symmetric group on 3 letters, S_3 has three irreducible representations over $\mathbb{C}$, the trivial representation 1, the 1-dimensional sign representation ϵ and a 2-dimensional representation ρ, all of which are already defined over $\mathbb{Q}$. Since there are four conjugacy classes of subgroups in S_3, comparing the $\mathbb{Z}$-ranks of the Burnside ring and the representation ring we see that the kernel of the natural map must have at least rank 1. Since this map has finite cokernel, the rank of the kernel is in fact exactly 1. We have the decompositions

$$\begin{aligned} \mathbb{Q}[S_3/1] &\cong 1 \oplus \epsilon \oplus \rho^{\oplus 2}, \\ \mathbb{Q}[S_3/C_2] &\cong 1 \oplus \rho, \\ \mathbb{Q}[S_3/C_3] &\cong 1 \oplus \epsilon, \\ \mathbb{Q}[S_3/S_3] &\cong 1, \end{aligned}$$

[1] Here and in the rest of the essay, AG denotes the group algebra of the group G over A

whence we obtain the relation

$$[S_3/1] - 2[S_3/C_2] - [S_3/C_3] + 2[S_3/S_3],$$

which, being not divisible by an integer, generates the 1-dimensional lattice of S_3-relations.

In general, the number of irreducible $\mathbb{Q}G$-representations is equal to the number of conjugacy classes of cyclic subgroups of G. Since the number of transitive G-sets, which form a $\mathbb{Z}$-basis for the Burnside ring of G, is equal to the number of conjugacy classes of all subgroups, the lattice of G-relations has $\mathbb{Z}$-rank equal to the number of conjugacy classes of non-cyclic subgroups of G.

Notation. For an AG-relation $\sum_k \alpha_k[G/H_k]$ we will just write $\sum_k \alpha_k H_k$. Collecting the positive and the negative coefficients, we may also write $\sum_i H_i - \sum_j H'_j$ where neither the H_i nor the H'_j need be distinct. For example the relation from the previous example can then be written as $1 + 2S_3 - (2C_2 + C_3)$.

Definition 1.5. Let G be a finite group, let $\Theta = \sum_i H_i - \sum_j H'_j$ be an AG-relation and let R be a principal ideal domain such that its field of fractions K has characteristic not dividing $|G|$. Given an R-free finite dimensional RG-module Γ such that $\Gamma \otimes K$ is self-dual we fix a non-degenerate G-invariant bilinear pairing $\langle , \rangle$ on Γ. For any subgroup H of G, the fixed points Γ^H are also R-free since R is a PID, and the pairing is also non-degenerate when restricted to Γ^H by [7, Lemma 2.15]. We may thus define the regulator constant of Γ with respect to Θ to be

$$C_\Theta(\Gamma) = \frac{\prod_i \det\left(\frac{1}{|H_i|}\langle , \rangle|\Gamma^{H_i}\right)}{\prod_j \det\left(\frac{1}{|H'_j|}\langle , \rangle|\Gamma^{H'_j}\right)} \in \bar{K}^\times/(R^\times)^2,$$

where each inner product matrix is evaluated with respect to some basis on the fixed submodule. If the matrix of the pairing on Γ^H with respect to some fixed basis is M then changing the basis by the change of basis matrix $X \in \mathrm{GL}(\Gamma^H)$ changes the matrix of the pairing to $X^{\mathrm{tr}}MX$. So the regulator constant is indeed a well-defined element of $\bar{K}^\times/(R^\times)^2$.

Convention. From now on, R will be assumed to be a PID with field of fractions K of characteristic not dividing $|G|$, all RG-modules that we will consider will be assumed to be free over R of finite rank and their base change to K will be assumed to be self-dual. When we refer to subgroups we will always mean subgroups up to conjugation. So the subgroups H and H' will be treated as being the same if the G-sets G/H and G/H' give the same element of the Burnside ring.

The choice of pairing is not present in the notation of regulator constants and indeed we have:

Theorem 1.6. *The value of $C_\Theta(\Gamma)$ is independent of the choice of the pairing.*

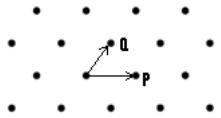
Proof. See [7, Theorem 2.17]. □

In particular, the pairing can always be chosen to be K-valued and so we see that the regulator constant is in fact an element of $K^\times/(R^\times)^2$. Note that if $R = \mathbb{Z}$ then the regulator constant is just a rational number. If $R = \mathbb{Z}_p$ then at least the p-adic order of the regulator constant is well-defined. If on the other hand $R = \mathbb{Q}$ then the regulator constant is only defined up to rational squares, and if $R = \mathbb{Q}_p$ then only the parity of the p-adic order is defined.

Example 1.7. If $G = S_3$ then we saw in Example 1.4 that there is, up to integer multiples, a unique relation

$$1 - 2C_2 - C_3 + 2S_3$$

and it is easy to check that the corresponding regulator constants of all three irreducible representations are equal to 3 modulo rational squares. The representations 1 and ϵ contain a unique G-invariant $\mathbb{Z}$-lattice each (up to isomorphism) and their regulator constants are $1/3$ and 3, respectively. The 2-dimensional representation ρ contains two non-isomorphic G-invariant $\mathbb{Z}$-lattices. Both can be visualised as hexagonal lattices, generated by two shortest distance vectors P and Q, on which the 3-cycles act as rotations by 120°.



On one, the 2-cycles act by reflection through a shortest distance vector (eg. through P) and on the other the 2-cycles act by reflection through the long diagonal of the fundamental parallelograms (which are $P + Q$ and its rotations by 120° in the sketch). Each one of the two can be embedded into the other G-equivariantly with index 3, but there is no G-equivariant bijection between them. The regulator constants of the two lattices are easily computed to be 1/3 and 3, which incidentally provides a quick proof that they are not isomorphic as $\mathbb{Z}G$-representations.

1.2 Some properties of relations and regulator constants

We will collect here some results from [5] and [7] about regulator constants.

Proposition 1.8 ([7], Corollary 2.18)**.** *$C_\Theta(\Gamma)$ is multiplicative in Θ and in Γ, i.e.*

$$C_\Theta(\Gamma \oplus \Gamma') = C_\Theta(\Gamma)C_\Theta(\Gamma'),$$
$$C_{\Theta+\Theta'}(\Gamma) = C_\Theta(\Gamma)C_{\Theta'}(\Gamma).$$

In particular, if we want to determine all regulator constants of all RG-modules, it suffices to determine them for indecomposable representations. Moreover, the following result shows that, at least for $\mathbb{Q}G$-modules, only *finitely many* primes p can appear in the regulator constants:

Proposition 1.9. *If $R = \mathbb{Q}$ or $\mathbb{Q}_p$ and $p \nmid |G|$ then $\mathrm{ord}_p(C_\Theta(\Gamma))$ is even for any G-relation Θ.*

Proof. See [7, Corollary 2.28]. □

In section 3.1 we will generalise this statement to $R = \mathbb{Z}$ and $R = \mathbb{Z}_p$ and we will further restrict the possible primes.

Relations can be restricted to subgroups, induced from subgroups and lifted from quotients as follows: let $\Theta = \sum_i H_i - \sum_j H'_j$ be an AG-relation.

- **Induction.** If G' is a group containing G then by transitivity of induction, Θ can be induced to a relation $\Theta\uparrow^{G'} = \sum_i H_i - \sum_j H'_j$ of G'.

- **Inflation.** If $G \cong \tilde{G}/N$ then each H_i corresponds to a subgroup $\tilde{H}_i$ of $\tilde{G}$ containing N and similarly for H'_j and, inflating the permutation representations from a quotient, we see that $\tilde{\Theta} = \sum_i \tilde{H}_i - \sum_j \tilde{H}'_j$ is a $\tilde{G}$-relation.
- **Restriction.** If H is a subgroup of G then by Mackey decomposition Θ can be restricted to an AH-relation $\Theta{\downarrow_H} = \sum_i \sum_{g \in H_i \backslash G / H} H \cap H_i^g - \sum_j \sum_{g \in H'_j \backslash G / H} H \cap H_j'^g$.

We have the following compatibility between these operations and the corresponding operations applied to representations Γ:

Proposition 1.10. *Let G be a finite group and Γ an RG-representation.*

- *If $H < G$ and Θ is an AH-relation then $C_\Theta(\Gamma{\downarrow_H}) = C_{\Theta{\uparrow^G}}(\Gamma)$*
- *If $G \cong \tilde{G}/N$ and Θ is an AG-relation with $\tilde{\Theta}$ the lifted relation then $C_\Theta(\Gamma) = C_{\tilde{\Theta}}(\Gamma)$ where Γ can also be regarded as a $\tilde{G}$-representation.*
- *If $G < G'$ and Θ is an AG'-relation then $C_\Theta(\Gamma{\uparrow^{G'}}) = C_{\Theta{\downarrow_G}}(\Gamma)$.*

Proof. See [7, Proposition 2.45]. □

2 Alternative definition of regulator constants

The definition of regulator constants that we have given above is somewhat unsatisfactory, since it involves making an arbitrary choice (that of a pairing) on which the result does not depend. It would be nice to have a definition that avoids any arbitrary choices. As a first step in the investigation of the properties of regulator constants, we will provide an alternative definition which depends on fixing more specific information about the relation (on which the result again does not depend) but not on any choices connected with the representation. This construction is inspired by the proof of [6, Lemma 3.2].

Let $\Theta = \sum_i H_i - \sum_j H'_j$ be an AG-relation. Define the G-sets $S_1 = \bigsqcup_i G/H_i$ and $S_2 = \bigsqcup_j G/H'_j$. Then to say that $\mathbb{Q}[S_1] \cong \mathbb{Q}[S_2]$ is equivalent to saying that there exists an embedding of $\mathbb{Z}G$-modules

$$\phi : \mathbb{Z}[S_1] \hookrightarrow \mathbb{Z}[S_2]$$

with finite cokernel. Also, to say that $\mathbb{Z}_{(p)}[S_1] \cong \mathbb{Z}_{(p)}[S_2]$ is equivalent to saying that there is such a ϕ with finite cokernel of order coprime to p.

With these remarks in mind, let R be a PID containing $\mathbb{Z}$, let Γ be an RG-module and fix an injection

$$\phi : R[S_1] \hookrightarrow R[S_2].$$

Since permutation modules are canonically self-dual, we also have a map

$$\phi^{\mathrm{tr}} : R[S_2] \hookrightarrow R[S_1]$$

and we get induced maps

$$\phi^* : \mathrm{Hom}_R(R[S_2], \Gamma) \to \mathrm{Hom}_R(R[S_1], \Gamma)$$

and

$$(\phi^{\mathrm{tr}})^* : \mathrm{Hom}_R(R[S_1], \Gamma) \to \mathrm{Hom}_R(R[S_2], \Gamma).$$

Upon restricting to the G-invariant subspaces we obtain maps ϕ^*_G and $(\phi^{\mathrm{tr}})^*_G$ between the coresponding spaces of G-homomorphisms. Since R is a PID, the spaces of G-homomorphisms are R-free. Also, since $\phi \otimes K$ and $\phi^{\mathrm{tr}} \otimes K$ are both isomorphisms, so are $\phi^*_G \otimes K$ and $(\phi^{\mathrm{tr}})^*_G \otimes K$. Thus both ϕ^*_G and $(\phi^{\mathrm{tr}})^*_G$ have non-zero determinants.

Definition 2.1. Define the regulator constant of Γ with respect to Θ to be

$$C_\Theta(\Gamma) = \frac{\det(\phi^{\mathrm{tr}})^*_G}{\det \phi^*_G} \in K^\times/(R^\times)^2$$

with both determinants computed with respect to the same bases on $\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)$ and on $\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)$. If we change the basis on $\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)$, say, then the quotient changes by the square of the determinant of change of basis, so it really is a well-defined element of $K^\times/(R^\times)^2$.

The injection ϕ is not present in the notation and indeed:

Proposition 2.2. *The value $C_\Theta(\Gamma)$ is independent of the choice of injection.*

Proof. Let $S_1 = \{s_1, \ldots, s_n\}$ and choose a basis γ_j, $j = 1, \ldots, r$ for Γ. Define $f_{i,j} \in \mathrm{Hom}_R(R[S_1], \Gamma)$ by $f_{i,j}(s_i) = \gamma_j$, $f_{i,j}(s) = 0\ \forall s \neq s_i$. Then $f_{i,j}$, $i = 1, \ldots, n$, $j = 1, \ldots, r$ is a basis of $\mathrm{Hom}_R(R[S_1], \Gamma)$. Fix the analogous basis $f'_{i,j}$ for $\mathrm{Hom}_R(R[S_2], \Gamma)$ where $S_2 = \left\{s'_1, \ldots, s'_n\right\}$. If M is the matrix of ϕ with respect to the bases corresponding to s_i, s'_j then the matrix N of ϕ^* with respect to the corresponding bases just described is block diagonal with $\dim(\Gamma)$ blocks, each equal to M^{tr} and the matrix of $(\phi^{\mathrm{tr}})^*$ is equal to N^{tr}.

Let $v'_1, \ldots, v'_m$ be a basis of $\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)$ and extend it to a basis $v'_1, \ldots, v'_{nr}$ of $\mathrm{Hom}_R(R[S_2], \Gamma)$ and let X_2 be the $nr \times nr$ matrix of change of basis from v'_k to $f'_{i,j}$. Similarly, extend a basis $v_1, \ldots, v_m$ of $\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)$ to a basis $v_1, \ldots, v_{nr}$ of $\mathrm{Hom}_R(R[S_1], \Gamma)$ and let X_1 be the matrix of change of basis from v_k to $f_{i,j}$. Then the matrix of ϕ^*_G with respect to $v'_1, \ldots, v'_m$ and $v_1, \ldots, v_m$ is obtained by taking the submatrix of $X_2 N X_1^{-1}$ consisting of the first m rows and the first m columns. We will write this as $(X_2 N X_1^{-1})_{m\times m}$. With this notation, the matrix of $\left(\phi^{\mathrm{tr}}\right)^*_G$ with respect to the same bases is given by $(X_1 N^{\mathrm{tr}} X_2^{-1})_{m\times m}$. It is clear that these matrices do not depend on the way we have extended the bases of the G-invariant subspaces to the whole homomorphism spaces. Moreover, it suffices to extend these bases to bases of $\mathrm{Hom}_K(K[S_i], \Gamma \otimes K)$, $i = 1, 2$ and the result will be the same. With this remark in mind we consider two cases:

Case 1: Suppose, that the basis $v'_1, \ldots, v'_m$ of $\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)$ can be chosen to be orthogonal and that the basis $v_1, \ldots, v_m$ of $\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)$ can be chosen to be orthogonal, where we use the inner products which make the basis $f'_{i,j}$, respectively the basis $f_{i,j}$ orthonormal. Each of these bases can be extended to an orthogonal basis of $\mathrm{Hom}_K(K[S_i], \Gamma \otimes K)$, $i = 1, 2$ (this is not true over R, in general). We get that

$$\begin{aligned}
\det((X_2 N X_1^{-1})_{m\times m}) &= \det((X_2 N X_1^{-1})^{\mathrm{tr}}_{m\times m}) \\
&= \det(((X_1^{-1})^{\mathrm{tr}} N^{\mathrm{tr}} X_2^{\mathrm{tr}})_{m\times m}) \\
&= \frac{\prod_{i=1}^m a_i}{\prod_{i=1}^m b_i} \cdot \det((X_1 N^{\mathrm{tr}} X_2^{-1})_{m\times m})
\end{aligned}$$

where $a_i = \left\langle v'_i, v'_i \right\rangle$ and $b_i = \langle v_i, v_i \rangle$ with the inner products as indicated above. It is now clear that in this case

$$C_\Theta(\Gamma) = \det((X_1 N^{\mathrm{tr}} X_2^{-1})_{m\times m}) / \det((X_2 N X_1^{-1})_{m\times m}) = \frac{\prod_{i=1}^m b_i}{\prod_{i=1}^m a_i}$$

does not depend on the matrix N and so is independent of ϕ.

Case 2: If there is no orthogonal basis of $\mathrm{Hom}_{R[G]}(R[S_i],\Gamma)$ for $i = 1$ or 2 then we can still choose orthogonal bases of $\mathrm{Hom}_{R[G]}(R[S_i],\Gamma)\otimes K$, $i = 1,2$ and the same argument as in Case 1 applies. Computing the determinants of $\phi_G^*\otimes K$ and $\left(\phi^{\mathrm{tr}}\right)_G^*\otimes K$ with respect to these bases gives a wrong result since it changes it by squares of determinants of change of bases but does not make it dependant on the choice of ϕ. □

We will now prove that the definition of regulator constants given in this section is equivalent to the one in section 1.1:

Theorem 2.3. *Let G be a finite group, R a principal ideal domain, $\Theta = \sum_i H_i - \sum_j H'_j$ an AG-relation, where A is either $\mathbb{Q}$ or $\mathbb{Z}_{(p)}$, and Γ an R-free RG-module. Fix an injection $\phi : R[S_1] \hookrightarrow R[S_2]$ and obtain ϕ_G^* and $(\phi^{\mathrm{tr}})_G^*$ as above. Fix a G-invariant non-degenerate bilinear pairing $\langle,\rangle$ on Γ. Then*

$$\frac{\det(\phi^{\mathrm{tr}})_G^*}{\det\phi_G^*} \equiv \frac{\prod_i det\left(\frac{1}{|H_i|}\langle,\rangle|\Gamma^{H_i}\right)}{\prod_j det\left(\frac{1}{|H'_j|}\langle,\rangle|\Gamma^{H'_j}\right)} \mod (R^\times)^2.$$

Proof. Define a pairing $(,)_1$ on $\mathrm{Hom}_R(R[S_1],\Gamma)$ by

$$(f_1,f_2)_1 = \frac{1}{|G|}\sum_{s\in S_1}\langle f_1(s), f_2(s)\rangle$$

and define an analogous pairing $(,)_2$ on $\mathrm{Hom}_R(R[S_2],\Gamma)$. It is immediate that this pairing, when restricted to the spaces of G-homomorphisms, is G-invariant. We first claim that $(\phi^{\mathrm{tr}})^*$ is the adjoint of ϕ^* with respect to these pairings. Indeed, it suffices to check this for the bases $f_{i,j}(s_k) = \delta_{i,k}\gamma_j$ and $f'_{i,j}(s'_k) = \delta_{i,k}\gamma_j$ from the proof of Proposition 2.2. So writing $S_1 = \{s_1,\dots,s_n\}$ and $S_2 = \left\{s'_1,\dots,s'_n\right\}$ and $\phi(s_i) = \sum_j \phi_{i,j}s'_j$ we compute

$$\begin{aligned}
|G|\cdot(f_{i,j},\phi^* f'_{r,t})_1 &= \sum_{s\in S_1}\left\langle f_{i,j}(s), f'_{r,t}(\phi(s))\right\rangle = \left\langle\gamma_j, f'_{r,t}(\phi(s_i))\right\rangle \\
&= \left\langle\gamma_j,\phi_{i,r}\gamma_t\right\rangle = \left\langle\phi_{i,r}\gamma_j,\gamma_t\right\rangle = \left\langle f_{i,j}(\phi^{\mathrm{tr}}s_r),\gamma_t\right\rangle \\
&= \sum_{s\in S_2}\left\langle f_{i,j}(\phi^{\mathrm{tr}}s), f'_{r,t}(s)\right\rangle = |G|\cdot((\phi^{\mathrm{tr}})^* f_{i,j}, f'_{r,t})_2 \qquad (2)
\end{aligned}$$

as required. Next, for a subgroup H of G we can identify $\mathrm{Hom}_G(G/H,\Gamma)$ with Γ^H via $f\mapsto f(1)$. We claim that under this identification, we have

$$\det\left((,)_1|\mathrm{Hom}_{R[G]}(R[S_1],\Gamma)\right) \equiv \prod_i \det\left(\frac{1}{|H_i|}\langle,\rangle|\Gamma^{H_i}\right) \mod (R^\times)^2 \qquad (3)$$

and similarly for S_2. Indeed, if for subgroups $H_i \neq H_k$, we have that $R[G/H_i]$ and $R[G/H_k]$ are summands of $R[S_1]$, then an element of $\mathrm{Hom}_{R[G]}(R[S_1],\Gamma)$ which is trivial outside of G/H_i is orthogonal to an element which is trivial outside of G/H_k. So it suffices to prove the claim for $S_1 = G/H$. We compute

$$\begin{aligned}
(f_1,f_2)_1 &= \frac{1}{|G|}\sum_{s\in G/H}\langle f_1(s), f_2(s)\rangle = \frac{1}{|G|}\sum_{s\in G/H}\langle s\cdot f_1(1), s\cdot f_2(1)\rangle \\
&= \frac{1}{|G|}\sum_{s\in G/H}\langle f_1(1), f_2(1)\rangle = \frac{1}{|H|}\langle f_1(1), f_2(1)\rangle,
\end{aligned}$$

which immediately implies the claim. Now, fix bases $v_1, \dots, v_m$ and $v'_1, \dots, v'_m$ on $\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)$ and $\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)$, respectively. Then

$$\begin{aligned}
\frac{\prod_i \det\left(\frac{1}{|H_i|}\langle , \rangle|\Gamma^{H_i}\right)}{\prod_j \det\left(\frac{1}{|H'_j|}\langle , \rangle|\Gamma^{H'_j}\right)} &\overset{\text{by (3)}}{\equiv} \frac{\det\left((v_i, v_j)_1|\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)\right)}{\det\left((v'_k, v'_l)_2|\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)\right)} \\
&\equiv \frac{\det\left((v_i, \phi_G^* v'_j)_1|\mathrm{Hom}_{R[G]}(R[S_1], \Gamma)\right) / \det(\phi_G^*)}{\det\left(((\phi^{\mathrm{tr}})_G^* v'_k, v'_l)_2|\mathrm{Hom}_{R[G]}(R[S_2], \Gamma)\right) / \det((\phi^{\mathrm{tr}})_G^*)} \\
&\overset{\text{by (2)}}{\equiv} \det((\phi^{\mathrm{tr}})_G^*)/\det(\phi_G^*) \mod (R^\times)^2,
\end{aligned}$$

which concludes the proof. □

3 General theory of regulator constants for integral and rational representations

In this section we will develop the theory of regulator constants in two very different contexts. Before beginning, we will briefly point out the different difficulties that await us.

For a finite group G, there exist in general inifintely many non-isomorphic indecomposable $\mathbb{Z}G$-representations. More precisely, this is the case if and only if there is at least one prime p for which the Sylow p-subgroups of G are either non-cyclic or of order greater than p^2. There is no known procedure to write down all integral representations of a finite group, say in parametric families. It is therefore unreasonable to expect to be able to compute all regulator constants of all integral representations for any given group G. This however raises the interesting question, how these regulator constants can grow with the rank of the representations, which is the subject of the first subsection. Note that this question is completely trivial for rational representations due to Proposition 1.8.

In the case of rational representations, there are no great algorithmic difficulties in determining all regulator constants in a given finite group. However, there are several theoretical questions. For example, given a prime p and a finite group G, we would like to have an intrinsic description of the sets of rational representations $\{\rho_i\}$ such that there exists a relation Θ with the property that $\{\rho_i\}$ is exactly the set of all those representations for which $\mathrm{ord}_p(C_\Theta(\rho_i))$ is odd. The second subsection will deal with this problem. This is very much work in progress. We will give a conjectural answer which we will derive as a consequence of Conjecture 3.8, proposed to us in oral communication by Tim and Vladimir Dokchitser, and then provide theoretical evidence in certain important special cases. We will start with a general lemma:

Lemma 3.1. *Let G be a finite group, $\Theta = \sum_H \alpha_H H$ a G-relation and ρ an RG-representation. Then $C_\Theta(\rho) = C_\Theta(\rho^{\cap H})$, where $\rho^{\cap H}$ is the subrepresentation of ρ which is fixed by all subgroups appearing in the relation.*

Proof. This is immediate from the definition of regulator constants. □

3.1 Integral representations

If for a given relation Θ there exists a $\mathbb{Z}G$-module Γ_0 such that $C_\Theta(\Gamma_0)$ is non-trivial, then by taking direct sums of Γ_0 we see that there exists a constant c and a sequence

of $\mathbb{Z}G$-modules Γ_i of $\mathbb{Z}$-ranks r_i such that $C_\Theta(\Gamma_i) = c^{r_i}$. But can there be faster growth? And if not, can we say something about bounds on the constant c? The alternative definition of regulator constants provides a very satisfactory answer:

Theorem 3.2. *Let G be a finite group and $\Theta = \sum_i H_i - \sum_j H'_j$ a G-relation. Then there exists a positive constant c such that for all $\mathbb{Z}G$-modules Γ and for all primes p we have*

$$-\mathrm{rank}(\Gamma) \cdot \mathrm{ord}_p(c) \leq \mathrm{ord}_p(C_\Theta(\Gamma)) \leq \mathrm{rank}(\Gamma) \cdot \mathrm{ord}_p(c).$$

Moreover, if

$$\phi : \mathbb{Z}[S_1] \hookrightarrow \mathbb{Z}[S_2]$$

is an injection of $\mathbb{Z}G$-modules with finite cokernel then we can take $c = |\det \phi|$.

Proof. Let ϕ be an injection like in the statement of the theorem. Then by Theorem 2.3 we have

$$C_\Theta(\Gamma) = \frac{\det(\phi^{\mathrm{tr}})^*_G}{\det \phi^*_G}.$$

It suffices to show that $|\det \phi^*_G| \mid |\det \phi|^{\mathrm{rank}(\Gamma)}$. The same will be true for $(\phi^{\mathrm{tr}})^*_G$ by symmetry. As in the proof of 2.2, write $S_1 = \{s_1, \ldots, s_n\}$ and choose a basis γ_j, $j = 1, \ldots, r$ for Γ. Define $f_{i,j} \in \mathrm{Hom}_R(R[S_1], \Gamma)$ by $f_{i,j}(s_i) = \gamma_j$, $f_{i,j}(s) = 0 \ \forall s \neq s_i$. Then $f_{i,j}$, $i = 1, \ldots, n$, $j = 1, \ldots, r$ is a basis of $\mathrm{Hom}_R(R[S_1], \Gamma)$. Fix the analogous basis $f'_{i,j}$ for $\mathrm{Hom}_R(R[S_2], \Gamma)$ where $S_2 = \left\{s'_1, \ldots, s'_n\right\}$. Then, as in the said proof, we observe that if ϕ is given by the matrix M with respect to the bases corresponding to s_i, s'_j then the matrix N of ϕ^* with respect to the corresponding bases just described is block diagonal with $\dim(\Gamma)$ blocks, each equal to M^{tr}. Thus, $\det \phi^* = (\det \phi)^{\mathrm{rank}(\Gamma)}$. To conclude the proof we simply note that for a homomorphism of free $\mathbb{Z}$-modules with finite cokernel, the absolute value of the determinant is equal to the order of the cokernel. But the cokernel of ϕ^*_G is a subgroup of the cokernel of ϕ^*, so we are done by taking $c = \det \phi$. □

A natural question arises: how small can c be chosen? According to the above theorem we can take $c = \det \phi$ for any G- injection $\phi : \mathbb{Z}[S_1] \hookrightarrow \mathbb{Z}[S_2]$ with finite cokernel. Can we make a judicious choice of a collection of such injections to get good bounds on $\mathrm{ord}_p(C_\Theta(\Gamma))$ prime by prime? In particular, when do we have $\mathrm{ord}_p(C_\Theta(\Gamma)) = 0$ for all $\mathbb{Z}G$-modules Γ? We will now provide a considerable generalisation of Proposition 1.9. We need a preliminary definition and a result we will use:

Definition 3.3. A finite group is called *p-hypo-elementary* if it has a normal Sylow p-subgroup with quotient a cyclic p'-group for some prime p'. Equivalently, a p-hypo-elementary group is a semi-direct product of a p-group acted on by a cyclic p'-group for primes $p \neq p'$.

Theorem 3.4 (Conlon's Induction Theorem)**.** *Given any finite group H and any commutative ring $\tilde{R}$ in which every prime divisor of $|H|$ except possibly p is invertible, there exist integers $\alpha_{H'}$ such that some integer multiple of the trivial representation of H over $\tilde{R}$ is equal to $\sum_{H'} \alpha_{H'} R[H/H']$ in the representation ring over R, where the sum is taken over p-hypo-elementary subgroups of H.*

A proof can be found e.g. in [4], (80.60).

Proposition 3.5. *Let $R = \mathbb{Z}$ or $\mathbb{Z}_p$. Let G be a finite group, let N be a normal subgroup such that the quotient group $C = G/N$ is cyclic. Let p be a prime not dividing the order of N. Then*

$$\mathrm{ord}_p(C_\Theta(\Gamma)) = 0$$

for all RG-modules Γ and all G-relations Θ.

Proof. We will be done if we can show that any $\mathbb{Q}G$-relation is in fact a $\mathbb{Z}_{(p)}G$-relation (see Definition 1.3). Then, for any G-relation Θ there exists a G-injection $\phi : \mathbb{Z}[S_1] \hookrightarrow \mathbb{Z}[S_2]$ which is an isomorphism when base changed to $\mathbb{Z}_{(p)}$ and the result will follow from Theorem 3.2 and the Remark following it.

Recall that the rank of the lattice of $\mathbb{Q}G$-relations is equal to the number of conjugacy classes of non-cyclic subgroups of G. Also, by Conlon's Induction Theorem, for any subgroup of G which is not p-hypo-elemetary we get a $\mathbb{Z}_{(p)}G$-relation by inducing Conlon's relation from this subgroup to G as explained in section 1.2. Explicitely, for each subgroup H of G which is not p-hypo-elemntary, we get a $\mathbb{Z}_{(p)}G$-relation $\alpha_H H - \sum_{H'} \alpha_{H'} H'$, the sum taken over p-hypo-elementary subgroups of H. All relations obtained in this way are clearly linearly independent, since each one contains a unique 'maximal' subgroup which has the property that all other subgroups featuring in the relation are contained in this one. In summary, we deduce that the lattice of all $\mathbb{Z}_{(p)}G$ relations has rank greater than or equal to the number of non-p-hypo-elemetary subgroups of G. Clearly, any $\mathbb{Z}_{(p)}G$-relation is also a $\mathbb{Q}G$-relation. The result will now follow from the claim that the lattice of $\mathbb{Z}_{(p)}G$- relations is a full rank sublattice of the lattice of $\mathbb{Q}G$-relations. This will suffice because it implies that for any G-relation Θ some integer multiple of Θ is a $\mathbb{Z}_{(p)}G$- relation. But then clearly Θ itself must be a $\mathbb{Z}_{(p)}G$- relation. In other words, the sublattice of $\mathbb{Z}_{(p)}G$-relations is saturated in the lattice of G-relations. Thus we need to show that any non-cyclic subgroup is non-p-hypo-elementary.

So take $H = P \rtimes Z$ where P is a p-group and Z is a cyclic p'-group with $p' \neq p$. Since p does not divide $|N|$ we have that

$$P \cong P/P \cap N \cong PN/N \leq G/N$$

is cyclic. Further, since H/P is abelian, the commutator subgroup H' of H must lie in P so it is a p-group. But also, $H' \leq G' \leq N$ since G/N is abelian and therefore $H' = \{1\}$ since p does not divide $|N|$. Thus H is abelian, $H = P \times C$ and so cyclic. □

In the most general case, finding tight bounds on the growth of regulator constants can be rather difficult. The question of finding such bounds is not only of interest in its own right, but also of importance for number theoretic applications which we will describe in the last section.

3.2 Rational representations

The most general goal in the theory of regulator constants of rational representations is to understand, for any finite group G, for which primes p, G-representations ρ and G-relations Θ we have that $\mathrm{ord}_p(C_\Theta(\rho))$ is odd. From a number theoretic point of view, the following object is of particular importance (see also [7, 1.iii]):

Definition 3.6. Let G be a finite group and p a prime number. Let $\mathbb{T}_p$ be the set of all self-dual $\bar{\mathbb{Q}}_p G$-representations τ for which there exists a G-relation Θ such that

$$\langle \tau, \rho \rangle \equiv \mathrm{ord}_p(C_\Theta(\rho)) \mod 2$$

for all self-dual $\mathbb{Q}_pG$-representations ρ, where $\langle\tau,\rho\rangle$ is the usual inner product of characters. An element of $\mathbb{T}_p$ will be called a p-computable representation.

The significance of the set $\mathbb{T}_p$ is that in [7] the p-parity conjecture [7, Conjecture 1.2b] for twists by p-computable representations has been proved for a large class of abelian varieties, including all semi-stable ones when p is odd. This raises the problem of describing this set of all p-computable representations in purely representation theoretic terms, without referring to regulator constants.

First, we note that if a representation τ is in $\mathbb{T}_p$ then so is $\tau\oplus 2\rho$ for any self-dual $\mathbb{Q}_pG$-representation ρ. For any such ρ, 2ρ is trivially in $\mathbb{T}_p$. The elements of $\mathbb{T}_p$ that we are primarily interested in are of the following form: let Θ be a relation and let $\{\rho_i\}$ be the set of all the irreducible self-dual $\mathbb{Q}_pG$-representations for which $\mathrm{ord}_p(C_\Theta(\rho_i))$ is odd. For each ρ_i let ρ_i' be an absolutely irreducible summand of ρ_i. Then $\bigoplus_i\rho_i'\in\mathbb{T}_p$ (see [7, Remark 1.8]).

Example 3.7. Let p be an odd prime and let $G=D_{2p}$ be the dihedral group of order $2p$. The irreducible $\mathbb{Q}_pG$ representations are the trivial representation 1, a non-trivial 1-dimensional representation ϵ and a $p-1$ dimensional representation ρ. All three are self-dual. There is one unique G-relation up to scalar multiples

$$\bar\Theta=\{1\}-2C_2-C_p+2G$$

and the regulator constants of all three representations with respect to $\bar\Theta$ are p up to squares. Thus, the 'interesting' p-computable representations are of the form $1\oplus\epsilon\oplus\rho_i$ where ρ_i is any absolutely irreducible 2-dimensional summand of ρ.

We have seen in Proposition 3.5 that if G has a normal subgroup N with cyclic quotient and if p does not divide the order of N then there are no non-trivial p-computable representations. The following far-reaching conjecture has been proposed by Tim and Vladimir Dokchitser in oral communication:

Conjecture 3.8. *All G-relations Θ for which there exists a self-dual $\mathbb{Q}_pG$-representation ρ such that* $\mathrm{ord}_p(C_\Theta(\rho))$ *is odd come from dihedral sub-quotients. More precisely, there exists a basis of G-relations in which for every Θ, either* $\mathrm{ord}_p(C_\Theta(\rho))$ *is even for all self-dual $\mathbb{Q}_pG$-representations or Θ is obtained by lifting and then inducing the relation from Example 3.7 from a sub-quotient isomorphic to D_{2p}.*

One consequence of this conjecture would in particular be a complete classificaton of the sets

$$\left\{\rho\text{ irreducible }\mathbb{Q}_pG\text{-representation}\mid \mathrm{ord}_p(C_\Theta(\rho))\text{ is odd}\right\}$$

and thus a representation theoretic description of $\mathbb{T}_p$ as follows: if Θ is not lifted and induced from a dihedral sub-quotient then this set is empty. Otherwise, let $K\triangleleft H\leq G$ be such that $H/K\cong D_{2p}$ and let Θ be the induction from H to G of the lift $\tilde\Theta$ of the D_{2p}-relation $\bar\Theta$ from Example 3.7. Then

$$C_\Theta(\rho)=C_{\tilde\Theta}(\rho{\downarrow_H})=C_{\bar\Theta}((\rho{\downarrow_H})^K)$$

where $(\rho{\downarrow_H})^K$ is the fixed subrepresentation of $\rho{\downarrow_H}$ under K. The first equality follows from the Frobenius reciprocity type statement in section 1.2 and the second one from Lemma 3.1. Example 3.7 then immediately shows that $\mathrm{ord}_p(C_\Theta(\rho))$ is odd if and only

if $(\rho\downarrow_H)^K$ decomposes as a sum of an odd number of irreducible D_{2p}-representations, which is a purely representation-theoretic criterion.

Proposition 3.5 can be regarded as evidence for Conjecture 3.8 since the group G in the statement of the Proposition has no D_{2p}-subquotients. In fact, the proof of the Proposition shows that if the only p-hypo-elementary subgroups of a group G are cyclic (which in particular implies that G has no D_{2p}-subquotients) then $\mathrm{ord}_p(C_\Theta(\Gamma)) = 0$ for all G-relations Θ and all $\mathbb{Z}_pG$-representations Γ. We will now provide very strong support for the conjecture in the opposite extreme case: when G itself is p-hypo-elementary (p odd), i.e. when all subgroups of G are p-hypo-elementary. This is work in progress and we believe that the strategy that we will now describe should eventually lead to a proof of the full conjecture.

Given a p-hypo-elementary group G (p odd) we will construct a sublattice of the lattice of G-relations of large rank such that for any relation Θ in this sublattice, $\mathrm{ord}_p(C_\Theta(\rho))$ is even for all self-dual $\mathbb{Q}_pG$-representations ρ. By large rank we mean that the rank of the sublattice of those relations for which some regulator constant is divisible by p will always be at most the number of dihedral subquotients of G and usually much smaller.

Recall that the rank of the lattice of G-relations is equal to the number of non-cyclic subgroups of G up to conjugation. Let G be a p-hypo-elementary group where p is an odd prime. For each non-cyclic subgroup H (as usual up to conjugacy) of G, apart from some of those which have a D_{2p}-quotient, we will construct a G-relation which will only consist of H and its subgroups. All relations obtained in this way will clearly be linearly independent since each one will contain a unique maximal subgroup with the property that all other subgroups in this relation will be contained in the maximal one.

So let $H = P \rtimes C$ be a non-cyclic subgroup of G where P is a p-group and $C = \langle x \rangle$ is a cyclic p'-group with $p \neq p'$. If p' is odd then G has odd order and by [7, Theorem 2.47] all regulator constants are trivial. So we will henceforth assume that $p' = 2$. It suffices to construct an H-relation which contains H itself, since this relation can then be induced to G. Moreover, it suffices to construct a relation in any non-cyclic quotient of H since we can lift relations from quotients. The construction will procede in 6 steps:

Step 1: We will assign to H a non-cyclic quotient $\phi(H)$ of a particular kind. First note that the Frattini subgroup $\Phi(P)$ of P is characteristic in P, so it is fixed by C and is therefore normal in H.

We claim that $H/\Phi(P)$ is also non-cyclic. Indeed, if it is cyclic then in particular, $P/\Phi(P)$ is cyclic, hence P is cyclic, generated by g, say, for it is a general fact that the Frattini subgroup consists of 'non-generators' of a p-group. But then the automorphism of P associated with the generator x of C sends g to some g^i, and since it acts trivially modulo the Frattini subgroup, we must have $i = kp + 1$ for some integer k. Since this automorphism must be of order 2^m, we get that

$$(kp + 1)^{2^m} \equiv 1 \mod p^n,$$

where p^n is the order of P. Thus

$$\mathrm{ord}_p\left(\sum_{r=1}^{2^m} \binom{2^m}{r} k^r p^r\right) \geq p^n$$

and so

$$\begin{aligned}\mathrm{ord}_p(kp) = \mathrm{ord}_p\left(\binom{2^m}{1}kp\right) &= \min_r\left(\mathrm{ord}_p\left(\binom{2^m}{r}k^r p^r\right)\right)\\ &= \mathrm{ord}_p\left(\sum_{r=1}^{2^m}\binom{2^m}{r}k^r p^r\right) \geq p^n\end{aligned}$$

since $\mathrm{ord}_p\left(\binom{2^m}{1}kp\right) < \mathrm{ord}_p\left(\sum_{r=2}^{2^m}\binom{2^m}{r}k^r p^r\right)$. We deduce that $i = k'p^n + 1$ and so $g^i = g$. But this implies that the automorphism of P is trivial, so $P \rtimes C$ is in fact a direct product and thus cyclic, contradicting the choice of H.
So, setting $\phi(H) = H/\Phi(P)$ we get a p-hypo-elementary quotient of the form $P' \rtimes C$ where P' is elementary abelian, i.e. can be regarded as an $\mathbb{F}_p$-vector space. Thus the action of C on P' can be viewed as an $\mathbb{F}_p$-representation of C.

Step 2: Consider two cases: if the action of C on P' is trivial then C is a normal subgroup and we can replace $\phi(H)$ by $\phi(H)/C$. This is a non-cyclic p-group. By Artin's induction theorem, there exists a $\phi(H)$-relation which contains $\phi(H)$ and cyclic subgroups of $\phi(H)$. Moreover, Artin's theorem guarantees that the coefficient of $\phi(H)$ in the relation divides the order of $\phi(H)$ and so is odd. This observation will be important later. Let Θ_H be the lift of this relation to an H-relation. By [7, Theorem 2.47], the regulator constants for this relation are trivial. If the action of C on P' is non-trivial then the kernel K of the map $C \to \mathrm{Aut}(P')$ is a normal subgroup of $\phi(H)$ and we can replace $\phi(H)$ by $\phi(H)/K$. This case will occupy us until Step 6. So, in summary, we now assume that $\phi(H) = C' \rtimes P'$ where P' is an elementary abelian p-group and the action of C' on P' is faithful.

Step 3: If the $\mathbb{F}_p$-representation P' of C' is a direct sum of copies of the sign representation, i.e. if the generator of C' acts as inversion on all elements of P', then we will not create a relation in this case. Note that then H has at least one dihedral quotient.
Otherwise, any direct summand of the representation P' of C' is a normal subgroup of $\phi(H)$ and so we can replace $\phi(H)$ by a quotient, such that P' becomes an irreducible faithful $\mathbb{F}_p$-representation of C' which is not trivial and not the sign representation. In particular, $|C'| \geq 4$.

Step 4: Write C_i for the unique index i subgroup of C', $i = 2, 4$. We claim that

$$C_4 - C_2 - 2C' - P' \rtimes C_4 + P' \rtimes C_2 + 2\phi(H) \tag{4}$$

is a $\phi(H)$-relation. To prove this we first recall the description of the irreducible characters of $\phi(H)$ from [13, II 9.2], taking into account that in our case the action of C' on P', and thus also on the group of characters of P', is faithful. For simplicity, write $H' = \phi(H)$. There is a natural faithful action of C' on the characters of P' via

$$x(\rho)(g) = \rho(x^{-1}gx).$$

Let $\rho_1, \ldots, \rho_l$ be a full set of representatives of orbits of non-trivial characters of P' under this action. Let $1 = \chi_1, \epsilon = \chi_2, \chi_i = \chi_3, \bar{\chi_i} = \chi_4, \ldots, \chi_k$ be the irreducible characters of $C' \cong H'/P'$, regarded as linear characters of H', where $\chi_1, \ldots, \chi_4$ are lifted from the quotient of order 4. Then the full set of irreducible characters of H' is given by $\left\{\chi_1, \ldots \chi_k, \rho_1\uparrow^{H'}, \ldots, \rho_l\uparrow^{H'}\right\}$. We can now write

down the decomposition of the permutation characters that appear in the above relation:

$$\begin{aligned}
\mathbb{C}[H'/H'] &= 1, \\
\mathbb{C}[H'/P' \rtimes C_2] &= 1 + \epsilon, \\
\mathbb{C}[H'/P' \rtimes C_4] &= 1 + \epsilon + \chi_i + \bar{\chi}_i, \\
\mathbb{C}[H'/C'] &= 1 + \rho_1\uparrow^{H'} + \ldots + \rho_l\uparrow^{H'}, \\
\mathbb{C}[H'/C_2] &= 1 + \epsilon + 2\rho_1\uparrow^{H'} + \ldots + 2\rho_l\uparrow^{H'}, \\
\mathbb{C}[H'/C_4] &= 1 + \epsilon + \chi_i + \bar{\chi}_i + 4\rho_1\uparrow^{H'} + \ldots + 4\rho_l\uparrow^{H'} .
\end{aligned}$$

It is now clear that the expression (4) really is a relation. Let Θ_H be the inflated H-relation.

Step 5: We claim that for all relations Θ_H that we have constructed so far, we have $C_{\Theta_H}(\tau) \equiv 1 \mod (\mathbb{Q}_p^\times)^2$ for all self-dual $\mathbb{Q}_pH$-representations τ. Note that if we write $\phi(H) = H/N$ then all subgroups of H that appear in Θ_H contain N, so by Lemma 3.1 and by Proposition 1.10 it suffices to prove the claim for all $\phi(H)$-representations, where Θ_H is regarded as an H/N-relation. Thus, we already know this when $\phi(H)$ is of odd order (see Step 2) so take $\phi(H)$ to be as in Step 4. First, by Lemma 3.1 we may without loss of generality replace τ by τ^{C_4}, the fixed subrepresentation under C_4. But the only irreducible representations of $\phi(H) = H'$ for which the C_4-invariant subspace is not trivial are 1, ϵ, the two non-selfdual χ_i and $\bar{\chi}_i$ and the induced representations $\rho_j\uparrow^{H'}$. For 1 and ϵ the claim is trivial to check. For $\chi_i + \bar{\chi}_i$ it follows from [7, Corollary 2.25]. For the induced representations, the claim follows from a straighforward but slightly tedious explicit computation with the following pairing: fix a non-degenerate bilinear pairing $\langle , \rangle$ on ρ_j and define

$$(u, v) = \frac{1}{|H'|} \sum_{h \in H'/P'} \langle u(h), v(h) \rangle$$

where u, v are P'-equivariant maps from H' to the vector space of ρ_j, i.e. vectors in the induced representation. (It is a trivial check that this pairing is non-degenerate and H'-invariant.)

Step 6: We summarise that so far we have assigned to each non-cyclic subgroup $H = P \rtimes C$ of G a quotient $\phi(H)$ of H obtained by the above procedure: first divide out the Frattini subgroup of P, then divide out the kernel K of the map $C \to \mathrm{Aut}(P/\Phi(P))$. If the resulting quotient is of odd order, then set this to be $\phi(H)$. Otherwise, divide out all but one representation of $C/K = C'$ in $P' = P/\Phi(P)$ such that the remaining representation is not trivial and, if possible, not the sign representation. Again, divide out the kernel of the resulting map $C' \to \mathrm{Aut}(P')$ and set $\phi(H)$ to be the resulting quotient. So, in summary, $\phi(H)$ is always non-cyclic and either an elementary p-group or the dihedral group D_{2p} or a p-hypo-elementary group $P' \rtimes C'$ where C' is of order at least 4 and acts faithfully, irreducibly on P'. In the first and the last case, we have assigned a G-relation Θ_H to H such that H itself appears in the relation and in the first case its coefficient is odd, while in the last case we have written down the relation explicitely in Step 4. Let Λ be the lattice of relations, spanned by Θ_H for all H for which

$\phi(H)$ is not dihedral, the announced lattice of 'large' rank. We have seen above, that for all relations in Λ all regulator constants are trivial. However, Λ might not be saturated in the lattice of all G-relations, i.e. if for some G-relation Θ an integer multiple of it is in Λ, it does not follow that Θ is in Λ. Since we are computing the regulator constants up to squares, this fact could potentially make our construction meaningless, since we could instead have just taken the sublattice of the lattice of all G-relations consisting of relations that are divisible by 2. It would be of full rank and would yield trivial regulator constants. So it remains to show that Λ has odd index in its saturation.
Clearly, the lattice of relations spanned by all those Θ_H for which $\phi(H)$ is odd has odd index in its saturation, since in each such Θ_H there exists a maximal group whose coefficient is odd. So, take some H for which $\phi(H)$ is even but not dihedral and suppose that there exists $\Theta \in \Lambda$ such that $\Theta_H + \Theta$ is divisible by 2. In particular, the index 2 subgroup H_2 of H must appear in Θ with odd coefficient, say it appears in $\Theta_{H'}$ for some $H' \neq H$. Since H_2 is of even order, we must have that $\Theta_{H'}$ is as in Step 4 and so H_2 must be either of index 2 or 4 in H'. In the former case, this implies that either $H' = H$ or $\langle H', H\rangle$, the smallest group containing both, has a non-cyclic Sylow 2-subgroup, contradicting the assumption that G is p-hypo-elementary. In the latter case, this implies that either H is the index 2 subgroup of H', in which case we can repeat the same argument with H replaced by H', or we arrive at the same contradiction that G is not p-hypo-elementary. This completes our construction.

Although Conjecture 3.8 seems very strong we should remark that it is not the end of the story as far as the question of p-computable representations goes. For, while the conjecture gives an explicit representation theoretic method of finding all the p-computable representations in any concrete case, it gives no theoretical prediction on the size of $\mathbb{T}_p$. We have explained at the beginning of this subsection that if we have a basis Θ_i of the lattice of G-relations then $\mathbb{T}_p$ is generated by 2ρ for any $\mathbb{Q}_pG$-representation ρ and by representations of the form $\bigoplus_j \rho'_{i,j}$ where $\rho'_{i,j}$ is an absolutely irreducible summand of $\rho_{i,j}$ and for each i, the set $\{\rho_{i,j}\}$ is precisely the set of those irreducible self-dual $\mathbb{Q}_p$-representations for which $\mathrm{ord}_p(C_{\Theta_i}(\rho_{i,j}))$ is odd. Conjecture 3.8 gives an upper bound on the number of generators for the p-computable representations of the latter type, namely the number of D_{2p}-subquotients of G, but this bound is not tight, as we will demonstrate by an explicit example. This example will also demostrate our construction in practice:

Example 3.9. Take the p-hypo-elementary group

$$G = \left\langle a, b, x \mid a^3 = b^3 = x^4 = 1, x^{-1}ax = b^{-1}, x^{-1}bx = a \right\rangle.$$

It is a semi-direct product of an elementary abelian 3-group and the cyclic group C_4. The $\mathbb{F}_3$-representation of C_4 given by its action on $C_3 \times C_3$ is the two-dimensional irreducible $\mathbb{F}_3$ representation, which decomposes as a sum of two non-selfdual representations over $\bar{\mathbb{F}}_3$. Here is a list of the non-cyclic subgroups of G (as usual up to conjugation) together with names that we shall give them:

- $\langle a, b\rangle = C_{3,3}$,
- $\left\langle a, x^2\right\rangle = S_3^a$,
- $\left\langle ab, x^2\right\rangle = S_3^b$,

- $\left\langle a, b, x^2 \right\rangle = H_{18}$,
- $\langle a, b, x \rangle = G$

We will now demonstrate the above procedure of constructing relations with trivial p-parts of regulator constants. We have chosen the group in such a way that $\phi(H) = H$ for each non-cyclic subgroup H of G. First we note that the group G has four dihedral subquotients: there are two subgroups isomorphic to S_3 and the group H_{18} has two such quotients. Thus, Conjecture 3.8 predicts that there is a basis of relations in which at least one relation has trivial p-parts of regulators for all self-dual $\mathbb{Q}_p G$-representations. Our construction in fact gives us a basis with two such relations: we do not construct Θ_H when H is S_3^a, S_3^b or H_{18} since they are as at the beginning of Step 3. But we do obtain the relations

$$\begin{aligned} \Theta_{C_{3,3}} &\overset{\text{Step 2}}{=} 1 - 2C_3^a - 2C_3^b + 3C_{3,3}, \\ \Theta_G &\overset{\text{Step 4}}{=} 1 - C_2 - 2C_4 - C_{3,3} + H_{18} + 2G. \end{aligned}$$

So in a certain sense the construction sometimes does even better than the conjecture. But it turns out that this is still not good enough. Here is a table with a basis of relations and all corresponsing regulator constants:

G	ρ_1 1	ρ_2 1	ρ_3 2	ρ_4 4	ρ_5 4
$C_3^a - C_3^b - C_4 - S_3^a + 3S_3^b - 2H_{18} + G$	1	1	1	1	1
$1 - 2C_3^a - 2C_3^b + 3C_{3,3}$	1	1	1	1	1
$C_3^a - C_3^b - 2S_3^a + 2S_3^b$	1	1	1	3	3
$C_3^a - 2S_3^a - C_{3,3} + 2H_{18}$	3	3	1	1	3
$1 - C_2 - 2C_4 - C_{3,3} + H_{18} + 2G$	1	1	1	1	1
$p = 3$				*	*
	*	*			*

The dimensions of the representations are written underneath their labels. The representation ρ_3 is not absolutely irreducible but is a sum of two non-selfdual components. The two lines of stars denote the sets that we referred to as $\{\rho_{i,j}\}$ just before this example. Our construction shows that there are at most three such distinct sets (since we have constructed 2 lineraly independent relations with trivial 3-parts of regulator constants and there are 5 lineraly independent relations in total) but in fact there are only two of them.

4 Regulator constants in the dihedral group D_{2p}

In view of Conjecture 3.8 and for number theoretic applications which will be explained in the last section, it is important to understand the regulator constants in $G = D_{2p}$. Since all the Sylow subgroups of D_{2p} are cyclic of prime order, there is a finite number of non-isomorphic indecomposable integral G-representations (see remarks at the beginning of section 3.1). These were explicitely described in [9]. We will recall this classification and then compute the regulator constants of all these integral representations with respect to the relation from Example 3.7. We note that it is not clear a priori that this is a finite task, since the number of isomorphism classes of indecomposable integral representations, while finite for a given p, grows with p.

Let $\mathbb{Q}(\zeta_p)^+$ be the maximal real subfield of the p-th cyclotomic field and let $\mathcal{O}^+$ be its ring of integers. Let $\{U_i\}$ be a full set of representatives of the ideal class group of $\mathbb{Q}(\zeta_p)^+$ and take $U_1 = U = \mathcal{O}^+$ to represent the principal ideals. Write $G = \langle a, b : a^2 = b^p = (ab)^2 = 1\rangle$. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\zeta_p)$. Write A_i for the $\mathbb{Z}G$-module $U_i\mathcal{O}$ on which a acts as complex conjugation and b as multiplication by ζ_p. Let A_i' be the module $(\bar{\zeta_p} - \zeta_p)U_i\mathcal{O}$ with the same G-action. Set $A = A_1$, $A' = A_1'$.

Finally write $\mathbb{1}$ for the 1-dimensional trivial $\mathbb{Z}G$-module, ϵ for the 1-dimensional module sending a to -1 and b to 1 and ρ for the 2-dimensional module $\mathbb{Z}[G/C_p]$ which is an extension of $\mathbb{1}$ by ϵ. The following is a complete list of indecomposable $\mathbb{Z}G$-lattices (see [9]):

- $\mathbb{1}$;
- ϵ;
- ρ;
- for each i, A_i;
- for each i, A_i';
- for each i, a non-trivial extension of $\mathbb{1}$ by A_i', denoted by $(A_i', \mathbb{1})$;
- for each i, a non-trivial extension of ϵ by A_i, denoted by (A_i, ϵ);
- for each i, a non-trivial extension of ρ by A_i, denoted by (A_i, ρ);
- for each i, a non-trivial extension of ρ by A_i', denoted by (A_i', ρ);
- for each i, a non-trivial extension of ρ by $A_i \oplus A_i'$, denoted by $(A_i \oplus A_i', \rho)$;

It is a trivial check that $C_\Theta(\mathbb{1}) = 1/p$, $C_\Theta(\epsilon) = p$, $C_\Theta(\rho) = 1$.

Lemma 4.1. *The regulator constants of A and of A' are p and $1/p$, respectively.*

Proof. The matrices of a, b acting on A' on the left with respect to the basis $(\bar{\zeta_p} - \zeta_p)\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ are

$$\begin{bmatrix} -1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & -1 \\ 0 & 1 & 0 & \cdots & 0 & -1 & 0 \\ \vdots & \vdots & \vdots & \iddots & \iddots & \iddots & \vdots \\ 0 & 1 & 0 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -1 \\ 1 & 0 & 0 & \ldots & 0 & -1 \\ 0 & 1 & 0 & \ldots & 0 & -1 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & -1 \\ 0 & \ldots & 0 & 0 & 1 & -1 \end{bmatrix},$$

respectively. It is immediately seen that the same matrices represent the G-action by multiplication on the submodule

$$\left\langle b^{\frac{p-1}{2}} - b^{\frac{p+1}{2}}, b^{\frac{p+1}{2}} - b^{\frac{p+3}{2}}, \ldots, b^{p-1} - 1, 1 - b, \ldots, b^{\frac{p-5}{2}} - b^{\frac{p-3}{2}} \right\rangle_{\mathbb{Z}}$$

of $\mathbb{Z}[G/C_2]$ with respect to the indicated basis. But this is just the submodule

$$\left\langle 1 - b^i : i \in \{1, \ldots, p-1\} \right\rangle_{\mathbb{Z}}$$

of the permutation lattice $\mathbb{Z}[G/C_2]$. We can choose the standard pairing on the latter which makes the different coset representatives an orthonormal $\mathbb{Z}$-basis. It is easy to see that the fixed sublattices under 1 and under $\langle a\rangle = C_2$ are

$$\left\langle 1 - b^i : i = 1, \dots, p-1 \right\rangle_{\mathbb{Z}} \text{ and } \left\langle 2 - b^i - b^{p-i} : i = 1, \dots, \frac{p-1}{2} \right\rangle_{\mathbb{Z}},$$

respectively. The subgroup C_p only fixes the trivial lattice. The matrices of the pairing on these modules with respect to the bases indicated are then

$$\begin{bmatrix} 2 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \cdots & 1 & 2 & 1 \\ 1 & 1 & \cdots & 1 & 2 \end{bmatrix} \text{ and } \begin{bmatrix} 6 & 4 & 4 & \cdots & 4 \\ 4 & 6 & 4 & \cdots & 4 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 4 & \cdots & 4 & 6 & 4 \\ 4 & 4 & \cdots & 4 & 6 \end{bmatrix}$$

of sizes $p-1$ and $\frac{p-1}{2}$ with determinants p and $2^{\frac{p-1}{2}}p$, respectively, as can be checked by elementary row operations. So, taking into account the normalisation by the sizes of the subgroups, we get

$$\frac{\det\left(\frac{1}{|1|}\langle,\rangle|A'^1\right)\det\left(\frac{1}{|G|}\langle,\rangle|A'^G\right)^2}{\det\left(\frac{1}{|C_2|}\langle,\rangle|A'^{C_2}\right)^2\det\left(\frac{1}{|C_p|}\langle,\rangle|A'^{C_p}\right)} = \frac{p}{p^2} = 1/p$$

as claimed.

Now consider the $\mathbb{Z}G$-module $\mathbb{Z}[G/C_2]\otimes_{\mathbb{Z}}\epsilon$ with diagonal G-action. It is now clear from above that A is isomorphic to the submodule of $\mathbb{Z}[G/C_2]\otimes_{\mathbb{Z}}\epsilon$ given by $\left\langle 1 - b^i : i = 1, \dots, p-1\right\rangle$. The fixed submodules under 1 and under C_2 are

$$\left\langle 1 - b^i : i = 1, \dots, p-1\right\rangle \text{ and } \left\langle b^i - b^{p-i} : i = 1 \dots \frac{p-1}{2}\right\rangle,$$

respectively, and an entirely similar calculation using the same natural pairing as above shows that $C_\Theta(A) = p$. □

Lemma 4.2. *We have* $(A', 1) \cong \mathbb{Z}[G/C_2]$ *and* $C_\Theta((A', 1)) = 1$.

Proof. Take the $\mathbb{Z}$-basis $\{1, b, \dots, b^{p-1}\}$ for $\mathbb{Z}[G/C_2]$. Then there is the submodule $\left\langle\sum_{i=0}^{p-1} b^i\right\rangle$ isomorphic to 1 and the submodule $\left\langle 1 - b^i : i \in \{1, \dots, p-1\}\right\rangle$ isomorphic to A' but their direct sum is the submodule $\left\{\sum_i \alpha_i b^i : \sum \alpha_i \equiv 0(\bmod p)\right\}$ which is an index p sublattice. In fact $\mathbb{Z}[G/C_2]$ is indecomposable since $\mathbb{F}_p[G/C_2]$ is. Thus it must be a non-trivial extension of 1 by A' and the first claim follows from the classification of integral representations. The regulator constant of $(A', 1)$ must then be trivial by [7, Lemma 2.46]. □

By Proposition 3.5 we know that all the regulator constants will be powers of p. It is instructive to see explicitely that the unique (up to scalar multiples) relation Θ from Example 3.7 exists not just over $\mathbb{Q}$ but over $\mathbb{Z}_{(2)}$. We noted in the proof of Lemma 4.2 that the lattice $\mathbb{Z}[G/C_2]$ contains $A' \oplus 1$ as an index p sublattice. Thus, upon tensoring with $\mathbb{Z}_{(2)}$ we have an isomoprhism. On the other hand $\mathbb{Z}_{(2)}\left[G/C_p\right]$ remains indecomposable.

Write $\bar{\Gamma}$ for $\Gamma \otimes \mathbb{Z}_{(2)}$ for any $\mathbb{Z}G$-lattice Γ. Since $\mathbb{Z}_{(2)}[G/1] = \mathbb{Z}_{(2)}[G/C_2] \otimes \mathbb{Z}_{(2)}[G/C_p]$ we have

$$\begin{aligned}
&\mathbb{Z}_{(2)}[G/1] \oplus \mathbb{Z}_{(2)}[G/G]^{\oplus 2} = \mathbb{Z}_{(2)}[G/C_2]^{\oplus 2} \oplus \mathbb{Z}_{(2)}[G/C_p] \\
&\quad \Leftrightarrow \quad \left(\mathbb{Z}_{(2)}[G/C_2] \otimes \mathbb{Z}_{(2)}[G/C_p]\right) \oplus \mathbb{Z}_{(2)}[G/G] \oplus \mathbb{Z}_{(2)}[G/G] = \\
&\qquad\quad \mathbb{Z}_{(2)}[G/C_2] \oplus \mathbb{Z}_{(2)}[G/C_2] \oplus \mathbb{Z}_{(2)}[G/C_p] \\
&\quad \Leftarrow \quad \left(\bar{A}' \oplus \bar{1}\right) \otimes \mathbb{Z}_{(2)}[G/C_p] \oplus \bar{1} \oplus \bar{1} = \\
&\qquad\quad \bar{A}' \oplus \bar{1} \oplus \bar{A}' \oplus \bar{1} \oplus \mathbb{Z}_{(2)}[G/C_p] \\
&\quad \Leftarrow \quad \bar{A}' \otimes \mathbb{Z}_{(2)}[G/C_p] = \bar{A}' \oplus \bar{A}'.
\end{aligned}$$

Note that if we had worked over $\mathbb{Z}_2$ the implications would have gone both ways since over complete discrete valuation rings the Krull-Schmidt theorem and therefore the cancellation property hold.

The last equality is easily seen to be true since $A' \otimes \mathbb{Z}[G/C_p]$ gives upon tensoring with $\mathbb{Q}$ the direct sum of the two rational irreducible representations of dimension $p-1$. From the discussion above we see that all the lattices that can be embedded into this rational representation (A_i and A_i') can be embedded into each other with index a power of p and so they are all isomorphic over $\mathbb{Z}_{(2)}$.

Lemma 4.3. *The regulator constants of the remaining lattices in the above list for $i = 1$ are as follows:*

- $C_\Theta((A, \epsilon)) = 1$*;*
- $C_\Theta((A, \rho)) = 1/p$*;*
- $C_\Theta((A', \rho)) = p$*;*
- $C_\Theta((A \oplus A', \rho)) = 1$*;*

Proof. It is noted in [9] §4 that $(A \oplus A', \rho) \cong \mathbb{Z}[G/1]$ and so $C_\Theta((A \oplus A', \rho)) = 1$ by [7, Lemma 2.46].

For the other three lattices since we only need to determine the p-parts it suffices to work up to squares of elements with trivial p-valuation so we will work over $\mathbb{Z}_p$ rather than over $\mathbb{Z}$. So write $\widetilde{(A, \epsilon)} = (A, \epsilon) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and similarly for the other lattices. Since $1 \oplus \epsilon$ is an index 2 sublattice of ρ, over $\mathbb{Z}_p$ we have $\tilde{1} \oplus \tilde{\epsilon} \cong \tilde{\rho}$. Now, $(A, \epsilon) \otimes \epsilon \cong (A', 1)$ and so

$$\begin{aligned}
\widetilde{(A, \epsilon)} \oplus \widetilde{(A', 1)} &\overset{4.2}{=} \mathbb{Z}_p[G/C_2] \otimes (\tilde{1} \oplus \tilde{\epsilon}) \\
&\cong \mathbb{Z}_p[G/C_2] \otimes \tilde{\rho} \\
&\cong \mathbb{Z}_p[G/C_2] \otimes \mathbb{Z}_p[G/C_p] \\
&\cong \mathbb{Z}_p[G/1]
\end{aligned}$$

which has trivial regulator constant by [7, Lemma 2.46]. By multiplicativity of regulator constants and by Lemma 4.2 $C_\Theta(\widetilde{(A, \epsilon)}) = 1$. Similarly, $\widetilde{(A, \rho)} \cong (\tilde{A}, \tilde{1} \oplus \tilde{\epsilon})$ and since $\mathrm{Ext}(1, A) = 0$ ([9] Lemma 2.1) it is easy to see that

$$(\tilde{A}, \tilde{1} \oplus \tilde{\epsilon}) \cong \tilde{1} \oplus \widetilde{(A, \epsilon)},$$

whence, by multiplicativity of regulator constants, we deduce that

$$C_\Theta(\widetilde{(A, \rho)}) = 1/p \in \mathbb{Q}_p / \left(\mathbb{Z}_p^\times\right)^2.$$

Also $\mathrm{Ext}(\epsilon, A') = 0$ and

$$(\tilde{A'}, \tilde{1} \oplus \tilde{\epsilon}) \cong \tilde{\epsilon} \oplus \widetilde{(A', 1)},$$

whence

$$C_\Theta(\widetilde{(A, \rho)}) = p \in \mathbb{Q}_p / \left(\mathbb{Z}_p^\times\right)^2.$$

□

Theorem 4.4. *The regulator constants of all the indecomposable $\mathbb{Z}D_{2p}$-modules for p an odd prime are as follows:*

Γ	$C_\Theta(\Gamma)$
1	$1/p$
ϵ	p
ρ	1
A_i	$p\ \forall i$
A_i'	$1/p\ \forall i$
$(A_i', 1)$	$1\ \forall i$
(A_i, ϵ)	$1\ \forall i$
(A_i, ρ)	$1/p\ \forall i$
(A_i', ρ)	$p\ \forall i$
$(A_i \oplus A_i', \rho)$	$1\ \forall i$

Proof. For $i = 1$ this is Lemma 4.1, Lemma 4.2 and Lemma 4.3. It will suffice to show that $C_\Theta(A_i) = C_\Theta(A)$ and $C_\Theta(A_i') = C_\Theta(A')$ for all i. Recall that A_i, A_i' are given by $(\bar{\zeta_p} - \zeta_p)^j U_i \mathcal{O}$ for $j = 0, 1$, respectively, where U_i runs through representatives of the ideal class group of $\mathbb{Q}(\zeta_p)^+$. Take each U_i to be of norm coprime to $2p$. Then A_i is a sublattice of $A = A_1$ of index coprime to $2p$ and the two are therefore isomorphic over $\mathbb{Z}_2$ and over $\mathbb{Z}_p$. Thus they have the same regulator constants. Similarly, A_i' all have the same regulator constants as $A' = A_1'$. □

The proof of the proposition exhibits an important feature of regulator constants which we will now summarise.

Definition 4.5. Given a finite group G and a principal ideal domain R, two finitely generated R-free RG-modules M and N are said to lie in the same genus if $M \otimes R_\mathfrak{p} \cong N \otimes R_\mathfrak{p}$ as $R_\mathfrak{p}G$-modules for all completions $R_\mathfrak{p}$ at prime ideals $\mathfrak{p}$ of R. This is clearly an equivalence relation.

We can summarise the idea of the proof of the proposition as follows:

Theorem 4.6. *The regulator constants of an RG-module only depend on its genus.*

Proposition 4.7. *There exist at most 10 genera of $\mathbb{Z}D_{2p}$-modules. Each genus has a representative of the kind considered in Lemma 4.1, Lemma 4.2 and Lemma 4.3.*

5 Elliptic curves and regulator constants

In this section we want to apply our results on regulator constants to questions about the growth of Selmer groups of elliptic curves in extensions of number fields. Given a prime p, an extension of number fields F/K and an elliptic curve E/K, write $S_p(E/F)$ for the p-Selmer group of E over F. Many papers have been written which deal with

questions about the possible size of $S_p(E/F)$ subject to restrictions on E or on the degree of F/K. We refer e.g. to the Introduction in [1] or to [2, section 1.3] for discussions of known results. The main result of this section is:

Theorem 5.1. *Let p be a prime number and M a quadratic number field, $M \neq \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \bmod 4$. Given any positive integer d there exists a Galois extension $F/\mathbb{Q}$ with Galois group D_{2p} and an elliptic curve $E/\mathbb{Q}$ such that F contains M and $\#S_p(E/F) \geq p^d$.*

This is already known for $p \leq 7$ so we will prove the statement for $p > 7$. Using the explicit computations of regulator constants in dihedral extensions we can give a quantitative result as follows:

Theorem 5.2. *Let $p > 7$ be a prime, let $E/\mathbb{Q}$ be a semi-stable elliptic curve and $F/\mathbb{Q}$ a Galois extension with Galois group D_{2p}. Let M be the unique quadratic subfield of F. Let $\mathcal{S}$ be the set of all primes of split multiplicative reduction of E which are either inert in $M/\mathbb{Q}$ and totally ramified in F/M or totally ramified in $F/\mathbb{Q}$. Assume further that all primes not in $\mathcal{S}$ are either primes of good reduction or have cyclic decomposition groups in $F/\mathbb{Q}$. Then*

$$p^{r(E/F)/(p-1)} \cdot \#Ш(E/F)[p^\infty] \geq p^{|\mathcal{S}|-r(E/M)+2r(E/\mathbb{Q})}.$$

Before explaining the connection between regulator constants and elliptic curves we shall fix some notation:

Notation. Throughout the rest of the paper K will be a number field, $\bar{K}$ will denote an algebraic closure. If v is a place of K then $|.|_v$ will denote the normalised absolute value at v. The absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K will be denoted G_K. Given an elliptic curve E/K we use the following notation:

$\mathrm{r}(E/K)$	the Mordell-Weil rank of E/K;
$c_v(E/K)$	the local Tamagawa number at a place v of K;
$c_v(E/F)$	the product of the local Tamagawa numbers at all places of F above v where F/K is an extension of number fields and v is a place of K;
$c(E/K)$	the product of the local Tamagawa numbers at all finite places of K;
$W_{F/K}(E)$	the Weil restriction of scalars of E from F to K;
$S_p(E/F)$	the p-Selmer group of E/F, defined as $\ker\left(H^1(G_F, E[p]) \to \prod_v H^1(G_v, E)\right)$, where $G_v = \mathrm{Gal}(\bar{F}_v/F_v)$, the map is the restriction and the product is taken over all places of F.

Fix an invariant differential ω on E. At each finite place v of K take a Néron differential ω_v^0. Then we set $C_v(E/K) = c_v\left|\frac{\omega}{\omega_v^0}\right|_v$ and

$$C(E/K) = \prod_{v \nmid \infty} C_v(E/K).$$

Here we followed [17] in writing $\frac{\omega}{\omega_v^0}$ for the unique v-adic number δ such that $\omega = \delta\omega_v^0$, which exists because the space of holomorphic differentials on a curve is one-dimensional. The definition of $C(E/K)$ depends on the choice of the invariant differential ω but this dependence will not cause any ambiguity as long as we always choose the same differential when we have the analogous expression for number fields L_i/K.

5.1 Artin formalism and regulator constants

Our starting point is the conjecture of Birch, Swinnerton-Dyer and Tate [17] the second part of which predicts that, for an abelian variety A/K, the leading coefficient of the

L-function of A/K at $s = 1$ equals a certain expression in terms of arithmetic data of the abelian variety, which we will call the BSD-quotient of A/F. If, for some elliptic curves E_i/K_i and E'_j/K'_j, we have an equality

$$\prod_i L(E_i/K_i, s) = \prod L(E'_j/K'_j, s)$$

then the conjecture of Birch, Swinnerton-Dyer and Tate predicts an equality of the corresponding BSD-quotients. In fact, as explained in [7, footnote on page 7], if one assumes that Tate-Shaffarevich groups of abelian varieties over number fields are finite then such an equality is a consequence of several deep results like the compatibility of the conjecture with taking Weil restrictions of scalars and Faltings's result that abelian varieties are determined up to isogeny by their Tate modules. Now, let F/K be a Galois extension with Galois group G and let E/K be an elliptic curve. Let $\Theta = \sum_i H_i - \sum_j H'_j$ be a G-relation and write $L_i = F^{H_i}$, $L'_j = F^{H'_j}$ for the corresponding fixed subfields of F (since the subgroups are only defined up to conjugation, the fields are only defined up to isomorphism). By Artin formalism for L-functions, we get an equality of L-functions

$$\prod_i L(E/L_i, s) = \prod_j L(E/L'_j, s)$$

and hence an equality of BSD-quotients, assuming that all relevant Tate-Shaffarevich groups are finite. More precisely, we have

$$\prod_i \frac{\#Ш(E/L_i)\mathrm{Reg}(E/L_i)C(E/L_i)}{|E(L_i)_{\mathrm{tors}}|^2} = \prod_j \frac{\#Ш(E/L'_j)\mathrm{Reg}(E/L'_j)C(E/L'_j)}{|E(L'_j)_{\mathrm{tors}}|^2}. \tag{5}$$

Moreover, if one only assumes that the p-primary parts of the Tate-Shaffarevich groups are finite then the same equality holds but with Ш replaced by its p-primary part.

Note that the real and the complex periods as well as the discriminants of the fields, which are present in the conjecture of Birch and Swinnerton-Dyer, cancel in our situation, provided that one chooses the same invariant differential ω over K for each term.
Notation. Let F/K be a Galois extension of number fields with Galois group G. Given a G-relation Θ as above, set $L_i = F^{H_i}$ and $L'_j = F^{H'_j}$. Write $\mathrm{Reg}(E/\Theta)$ for the corresponding quotient $\prod_i \mathrm{Reg}(E/L_i) \big/ \prod_j \mathrm{Reg}(E/L'_j)$ and similarly for $\#Ш(E/\Theta)$, $C(E/\Theta)$ and $|E(\Theta)_{\mathrm{tors}}|$ or indeed for any function to $\mathbb{C}$ associated with E which depends on the field extension. In this shorthand language equation (5) reads as

$$\#Ш(E/\Theta)\mathrm{Reg}(E/\Theta) = \frac{|E(\Theta)_{\mathrm{tors}}|^2}{C(E/\Theta)}. \tag{6}$$

Example 5.3. Let $G = \left\langle a, b : a^p = b^2 = (ab)^2 \right\rangle$ be the dihedral group of order $2p$ for an odd prime p. Then we have the G-relation

$$\Theta = 1 - 2C_2 - C_p + 2G$$

from Example 3.7, which is unique up to scalar multiples. Suppose now that E/K is an elliptic curve. Take the subgroups $H = \langle a \rangle = C_p$, $H' = \langle b \rangle = C_2$. Let F/K be a Galois extension of number fields with Galois group G and let $L = F^{H'}$, $M = F^H$ be intermediate extensions. Let v be a finite place of K. If E has split multiplicative reduction at v of K then for any extension K'/K and any place w of K' above v we have

$c_w(E/K') = -w(j(E))$ where $j(E)$ is the j-invariant of the elliptic curve (see e.g. [16, Ch. IV Cor. 9.2]). Thus, if v is a place of split multiplicative reduction of E with only one prime of F above v with ramification index p then

$$c_v(E/\Theta) = \frac{c_v(E/K)^2 c_v(E/F)}{c_v(E/M)c_v(E/L)^2} = \frac{p c_v(E/K)^3}{p^2 c_v(E/K)^3} = \frac{1}{p}.$$

Similarly, it is easily seen that if a place v of split multiplicative reduction is totally ramified in F/K then the associated Tamagawa quotient is $1/p$ and in all other cases it is 1.

Remark 5.4. Given any relation Θ, if E is semi-stable then $C(E/\Theta) = c(E/\Theta)$. Indeed, it is easy to see that in a relation the Tamagawa quotient

$$\prod_i C_v(E/L_i) \Big/ \prod_j C_v(E/L'_j)$$

above each finite place v of K does not depend on the choice of the invariant differential ω. But when v is a place of semi-stable reduction of E we can choose ω to be a Néron differential at v. Then ω stays minimal at all places above v and so in a relation we can replace C_v by c_v in this case. Thus, for semi-stable elliptic curves E we can replace the products $C(E/L)$ of the modified Tamagawa numbers in a relation by just the product of the local Tamagawa numbers $c(E/L)$.

The quotient of regulators $\mathrm{Reg}(E/\Theta)$ is precisely equal to the regulator constant $C_\Theta(E(F)/E(F)_{\mathrm{tors}})$ of the free part of the F-rational points of E, which is a $\mathbb{Z}G$-module in a natural way. So, to construct elliptic curves with large Selmer groups, we will control the Tamagawa quotients and the torsion subgroups of E/F to make the left hand side of equation (6) large. The result will then follow from Theorem 3.2.

5.2 Proof of Theorem 5.2

We will assume throughout this subsection that the p-primary part of Tate-Shaffarevich groups of abelian varieties over number fields is always finite. When this is not the case, the statement of Theorem 5.2 is trivial. We start with a lemma which will help us to control the quotient of Tamagawa numbers in a relation:

Lemma 5.5. *Let G be a finite group and let $\Theta = \sum_i H_i - \sum_j H'_j$ be a G-relation. Let E/K be an elliptic curve over a number field and let F/K be a Galois extension with Galois group G. If v is a place of K which is unramified in F/K (or more generally for which all decomposition groups are cyclic) then $C_v(E/\Theta) = 1$.*

Proof. Quite generally, if $D < G$ is a subgroup and ψ is a function on the Burnside ring of G (such as $C_v : H \mapsto C_v(E/F^H)$ for example) which can be written as

$$\psi(H) = \prod_{x \in H\backslash G/D} \psi_D(H^{x^{-1}} \cap D)$$

for ψ_D a function on the Burnside ring of D (i.e. if ψ is "D-local" in the language of [7]) and if ψ_D is trivial on all D-relations then ψ is trivial on all G-relations. This follows from Mackey decomposition and a rather intricate formalism introduced in [7, 2.iii]. In our case, if D is the decomposition group of some w/v in G then the function C_v is D-local. But we assumed that D was cyclic and cyclic groups have no non-trivial relations. Therefore we are done. □

Proof of Theorem 5.2. Let Θ be the D_{2p}-relation from Example 3.7. By Example 5.3 and by Lemma 5.5 we have, under the conditions of the theorem, $C(E/\Theta) = 1/p^{|S|}$. Since $E/\mathbb{Q}$ is semi-stable, by [10] and [11] $E/\mathbb{Q}$ has no p-torsion ($p > 7$) and by [14, §21 Proposition 21 and remark following Lemma 6] the absolute Galois group of $\mathbb{Q}$ acts on $E[p]$ as $\mathrm{GL}_2(\mathbb{F}_p)$ (this result applies to elliptic curves without complex multiplication, but that condition is automatic for semi-stable elliptic curves over $\mathbb{Q}$). Thus adjoining the co-ordinates of a p-torsion point to $\mathbb{Q}$ defines an extension which is the fixed field of a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and so has degree $p^2 - 1 > 2p$ over $\mathbb{Q}$. It follows that E can have no p-torsion over F. We immediately deduce that

$$C_\Theta(E(F)/E(F)_{\mathrm{tors}})\#Ш(E/\Theta) = p^{|S|}.$$

Recall that the numerator of $\#Ш(E/\Theta)$ is $\#Ш(E/\mathbb{Q})^2 \cdot \#Ш(E/F)$. But by the inflation-restriction exact sequence, the kernel of

$$Ш(E/\mathbb{Q}) \to Ш(E/F)$$

is contained in $H^1(G(F/\mathbb{Q}), E(F))$ and the p-part of this is 0 since the p-part of $E(F)_{\mathrm{tors}}$ is 0 as explained above. We get that

$$C_\Theta(E(F)/E(F)_{\mathrm{tors}})\#Ш(E/F) \geq p^{|S|}.$$

By the computation of regulator constants for dihedral groups, we know that each copy of the trivial lattice in the Mordell-Weil group of E/F contributes $1/p$ to the regulator quotient, while each copy of the one-dimensional lattice ϵ contributes p to the regulator quotient. The 2- dimensional lattice $\mathbb{Z}[D_{2p}/C_p]$ has trivial regulator constant and the indecomposable lattice of the next highest rank is $p-1$-dimensional. But the number of copies of the trivial lattice is precisely $r(E/\mathbb{Q})$ while $r(E/M)$ is the sum of the number of trivial lattices and the number of ϵ. No indecomposable lattice contributes more than p to the regulator quotient and the result follows immediately. □

To prove Theorem 5.1 under the assumption that Tate-Shaffarevich groups are finite, all we now need to do is to show that the set $\mathcal{S}$ can be arbitrarily large. This will be done through an explicit construction of the required number fields via class field theory and by explicitely writing down the required elliptic curves in Legendre normal form. We also need to replace $Ш[p^\infty]$ by $Ш[p]$ which will be done in the last subsection.

5.3 Dihedral extension of number fields via class field theory

We will follow the notation in [3] so that the construction is readily implementable on a computer using the algorithms described there.

Notation. For a number field M we fix the following notation:

$\mathfrak{m} = (\mathfrak{m}_0,\ \mathfrak{m}_\infty)$	a modulus of M, where $\mathfrak{m}_0$ is an integral ideal of the field and $\mathfrak{m}_\infty$ is a set of real embeddings.
$I_\mathfrak{m}$	for a given modulus $\mathfrak{m}$, the multiplicative group of fractional ideals which are coprime to $\mathfrak{m}_0$.
$P_\mathfrak{m}$	for a given modulus $\mathfrak{m}$, the subgroup of $I_\mathfrak{m}$ generated by all principal ideals (a), $a \in M^\times$, such that $a \equiv 1 \bmod {}^*\mathfrak{m}$ by which we mean that $\mathrm{ord}_\mathfrak{p}(a-1) \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)$ for all $\mathfrak{p}$ above $\mathfrak{m}_0$ and $\sigma(a) > 0$ for all embeddings $\sigma \in \mathfrak{m}_\infty$.
$(\mathfrak{m}, U)$	a congruence subgroup, i.e. $\mathfrak{m}$ is a modulus and $P_\mathfrak{m} \leq U \leq I_\mathfrak{m}$.

Definition 5.6. Two congruence subgroups $(\mathfrak{m}, U_{\mathfrak{m}})$ and $(\mathfrak{n}, U_{\mathfrak{n}})$ are said to be equivalent if $I_{\mathfrak{m}} \cap U_{\mathfrak{n}} = I_{\mathfrak{n}} \cap U_{\mathfrak{m}}$. The smallest $\mathfrak{n}$ such that $(\mathfrak{m}, U_{\mathfrak{m}})$ is equivalent to $(\mathfrak{n}, U_{\mathfrak{m}} P_{\mathfrak{n}})$ is called the conductor associated to $(\mathfrak{m}, U_{\mathfrak{m}})$. This is equivalent to saying that the conductor is the smallest modulus $\mathfrak{n}$ such that the natural map $I_{\mathfrak{m}}/U_{\mathfrak{m}} \to I_{\mathfrak{n}}/U_{\mathfrak{m}} P_{\mathfrak{n}}$ is injective.

The following is one of the main results of global class field theory (see e.g. [8, Chapter X]):

Theorem 5.7. *Given any modulus $\mathfrak{m}$ of M and any congruence subgroup U, there exists a unique abelian extension F/M such that*

$$\begin{array}{rcl} I_{\mathfrak{m}}/U & \xrightarrow{\sim} & \mathrm{Gal}(F/M) \\ \alpha & \mapsto & (\alpha, F/M) \end{array}$$

is a group isomorphism, where for a prime ideal $\mathfrak{p}$ of M $(\mathfrak{p}, F/M)$ is the Frobenius automorphism at $\mathfrak{p}$. This isomorphism is called the Artin map. Moreover, two congruence subgroups $(\mathfrak{m}, U_{\mathfrak{m}})$ and $(\mathfrak{n}, U_{\mathfrak{n}})$ give the same field extension if and only if they are equivalent. We have

$$(\tau\alpha, F/M) = \tau^{-1}(\alpha, F/M)\tau \quad \forall \tau \in \mathrm{Aut}(M). \tag{7}$$

If K is a subfield of M and M/K is Galois then F/K is Galois if and only if $\tau(U)$ is equivalent to U for all $\tau \in \mathrm{Gal}(M/K)$. If $\tau(\mathfrak{m}) = \mathfrak{m}$ for all $\tau \in \mathrm{Gal}(M/K)$ then this condition simplifies to $\tau(U) = U$ for all $\tau \in \mathrm{Gal}(M/K)$.

The primes that ramify in F/M are precisely the ones that divide the conductor $\mathfrak{f}$ of $(\mathfrak{m}, U_{\mathfrak{m}})$ and a prime $\mathfrak{p}$ is wildly ramified if and only if $\mathfrak{p}^2$ divides $\mathfrak{f}$.

We will now use this result to construct dihedral extensions of $\mathbb{Q}$ with a prescribed intermediate field and arbitrarily many ramified primes:

Theorem 5.8. *Let $M = \mathbb{Q}(\sqrt{d})$ be a quadratic number field, and p any odd prime number. Define the following sets of primes:*

$$\begin{array}{rcl} \mathfrak{S}_1 & := & \left\{ q \text{ rational odd prime} : q \text{ splits in } M/\mathbb{Q},\ q \equiv 1 \bmod p \right\} \\ \mathfrak{S}_2 & := & \left\{ q \text{ rational odd prime} : q \text{ is inert in } M/\mathbb{Q},\ q \equiv -1 \bmod p \right\}. \end{array}$$

Given any positive integers k_1 and k_2 there exists a Galois extension $F/\mathbb{Q}$ with Galois group D_{2p} such that F contains M and

1. *at least k_1 primes from $\mathfrak{S}_1$ ramify in $F/\mathbb{Q}$ and*
2. *unless $d = p \equiv 1 \bmod 4$, at least k_2 primes from $\mathfrak{S}_2$ ramify in $F/\mathbb{Q}$.*

Proof. We will find infinitely many dihedral extensions F_i of $\mathbb{Q}$ containing M with disjoint sets of ramified primes in F_i/M. By taking "diagonal" subfields in their compositum we will create the required extension. To construct the extensions F_i we will use the above results from class field theory by constructing moduli $\mathfrak{m}$ which will be fixed by the Galois group of $M/\mathbb{Q}$ and such that $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ will have a quotient $I_{\mathfrak{m}}/U$ of order p with U fixed by the Galois group of $M/\mathbb{Q}$ and this Galois group acting as $x \mapsto x^{-1}$ on the quotient.

Let $\mathfrak{U}$ be the group of units of M and for a modulus $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ of M define

$$\mathfrak{U}_{\mathfrak{m}} = \{u \in \mathfrak{U} : u \equiv 1 \bmod {}^*\mathfrak{m}\}.$$

Further define

$$I'_{\mathfrak{m}} = \{a \in M^{\times} : \ \mathrm{ord}_{\mathfrak{p}}(a) = 0 \ \forall \mathfrak{p} | \mathfrak{m}_0\}$$

and

$$P'_{\mathfrak{m}} = \{a \in I'_{\mathfrak{m}} : \ a \equiv 1 \bmod {}^{*}\mathfrak{m}\}.$$

Then we have the exact sequence

$$0 \to \mathfrak{U}/\mathfrak{U}_{\mathfrak{m}} \to I'_{\mathfrak{m}}/P'_{\mathfrak{m}} \to I_{\mathfrak{m}}/P_{\mathfrak{m}} \to Cl(\mathcal{O}_M) \to 0. \tag{8}$$

The map $I'_{\mathfrak{m}}/P'_{\mathfrak{m}} \to I_{\mathfrak{m}}/P_{\mathfrak{m}}$ simply sends an element to the ideal it generates (or rather its equivalence class). We will concentrate on the term $I'_{\mathfrak{m}}/P'_{\mathfrak{m}}$ for now.

First, we claim that by Dirichlet's prime number theorem both sets $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are infinite, unless $d = p \equiv 1 \bmod 4$, in which case $\mathfrak{S}_1$ is infinite and $\mathfrak{S}_2$ is empty. Indeed, this is clear when $p \neq d$. If $p = d$ and $p \equiv 3 \bmod 4$ then

$$q \text{ splits in } M \Leftrightarrow \left(\frac{p}{q}\right) = 1 \Leftrightarrow \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}$$

and so again both sets are infinite since the congruence condition modulo 4 and the congruence condition modulo p can be satisfied simultaneously. If $p = d$ and $p \equiv 1 \bmod 4$ then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ and so $q \equiv \pm 1 \bmod p \Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1 \Rightarrow q$ splits in M.

We will henceforth assume that both sets are infinite since the proof (or rather the relevant part) just carries over to the other case. Define the following sequences of distinct moduli, always taking $\mathfrak{m}_\infty$ to be empty and dropping the subscript from $\mathfrak{m}_0$ to avoid index overload:

$$\mathfrak{m}_i = q_i q'_i, \ q_i, q'_i \in \mathfrak{S}_1, \quad \widetilde{\mathfrak{m}_j} = \widetilde{q_j}\widetilde{q_j}', \ \widetilde{q_j}, \widetilde{q_j}' \in \mathfrak{S}_2$$

with all $q_i, q'_i, \widetilde{q_j}, \widetilde{q_j}'$ distinct. Let τ be the non-trivial element of the Galois group of $M/\mathbb{Q}$. It is clear that τ fixes all the chosen moduli. We make several easy observations:

- By the Chinese Remainder Theorem there is an isomorphism

$$\begin{aligned} I'_{\mathfrak{m}}/P'_{\mathfrak{m}} &\cong \left(I'_{\mathfrak{m}} \cap \mathcal{O}_M\right) / \left(P'_{\mathfrak{m}} \cap \mathcal{O}_M\right) \\ &\cong (\mathcal{O}_M/\mathfrak{m}_0)^{\times} \\ &\cong (\mathcal{O}_M/q)^{\times} \times \left(\mathcal{O}_M/q'\right)^{\times} \end{aligned}$$

  for $\mathfrak{m} = \mathfrak{m}_i$ or $\mathfrak{m} = \widetilde{\mathfrak{m}_j}$ and $q = q_i, q' = q'_i$ or $q = \widetilde{q_j}, q' = \widetilde{q_j}'$, respectively.

- If $q \in \mathfrak{S}_1$ then writing $(q) = \mathfrak{q}\mathfrak{q}'$ in M we get that

$$(\mathcal{O}/q)^{\times} = (\mathcal{O}/\mathfrak{q})^{\times} \times \left(\mathcal{O}/\mathfrak{q}'\right)^{\times} \cong \left(\mathbb{F}_q\right)^{\times} \times \left(\mathbb{F}_q\right)^{\times}.$$

  If $(\mathcal{O}/\mathfrak{q})^{\times} = \langle x \rangle$ then $(\mathcal{O}/\mathfrak{q}')^{\times} = \langle y \rangle$ where $y = \tau(x)$. Since $q \equiv 1 \bmod p$ we have that $R_{\mathfrak{m}} = \langle (x^p, 1), (1, y^p), (x, y) \rangle$ is a subgroup of $(\mathcal{O}/q)^{\times}$ of index p. Moreover, $\tau(R_{\mathfrak{m}}) = R_{\mathfrak{m}}$ and $\tau((x, 1)) = (1, y) \equiv (x, 1)^{-1} \bmod R_{\mathfrak{m}}$.

- If $q \in \mathfrak{S}_2$ then $(\mathcal{O}/q)^{\times} = \left(\mathbb{F}_{q^2}\right)^{\times} = \langle x \rangle$, say, with the action of τ being given by $\tau(x) = x^q$. Since $q \equiv -1 \bmod p$, $R_{\mathfrak{m}} = \langle x^p \rangle$ is a subgroup of index p. Moreover, $\tau(R_{\mathfrak{m}}) = R_{\mathfrak{m}}$ and $\tau(x) = x^q \equiv x^{-1} \bmod R_{\mathfrak{m}}$.

- So, for $\mathfrak{m} = \mathfrak{m}_i$ or $\mathfrak{m} = \widetilde{\mathfrak{m}_j}$, $I'_{\mathfrak{m}}/P'_{\mathfrak{m}}$ contains a quotient which is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ on which τ acts as $x \mapsto x^{-1}$. Since, for p an odd prime, in a quadratic field any quotient of $\mathfrak{U}$ can contain at most one copy of $\mathbb{Z}/p\mathbb{Z}$ we deduce from the exact sequence (8) that there exists a subgroup of $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ which has a quotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and on which τ acts as $x \mapsto x^{-1}$. The structure theorem for finitely generated abelian groups now implies that $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ itself has such a quotient, $I_{\mathfrak{m}}/U_{\mathfrak{m}}$, say.

- By Theorem 5.7 we get, for each $\mathfrak{m} = \mathfrak{m}_i$ or $\mathfrak{m} = \widetilde{\mathfrak{m}_j}$, an abelian extension $F_{\mathfrak{m}}$ of M of degree p with conductor dividing $\mathfrak{m}$. Moreover, we have chosen $R_{\mathfrak{m}}$ and thus also $U_{\mathfrak{m}}$ in such a way that the extension $F_{\mathfrak{m}}/\mathbb{Q}$ is Galois and by equation (7) the Galois group is D_{2p}.

Since only finitely many of the extensions $F_{\mathfrak{m}}/M$ can be unramified, we have constructed two sequences of distinct Galois extensions $F_i = F_{\mathfrak{m}_i}$ and $F'_j = F_{\widetilde{\mathfrak{m}_j}}$ of $\mathbb{Q}$ with Galois groups D_{2p} with disjoint sets of primes which ramify over M. In one sequence these primes lie above primes from $\mathfrak{S}_1$ and in the other from $\mathfrak{S}_2$. These extensions are all independent over M. Let $\mathfrak{q}_i$ ramify in F_i/M. We will now inductively construct an extension of M which is Galois over $\mathbb{Q}$ with galois group D_{2p} and in which arbitrarily many primes from $\mathfrak{S}_1$ ramify. The case for $\mathfrak{S}_2$ is completely analogous.

Suppose we have constructed an extension F/M which is Galois over $\mathbb{Q}$ with Galois group D_{2p} and in which the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ ramify. Consider the compositum of F and F_{k+1}. Since the two fields are disjoint over M, the Galois group of their compositum is $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \langle g \rangle \times \langle h \rangle$, say. Clearly, F is the maximal extension of M inside $F_{k+1}F$ which is unramified at $\mathfrak{q}_{k+1}$ and similarly F_{k+1} is the maximal extension which is unramified at $\mathfrak{q}$ for any $\mathfrak{q} \in \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$. Thus, taking the fixed field inside $F_{k+1}F$ of (g, h) we get a Galois extension of $\mathbb{Q}$ with Galois group D_{2p} which is ramified at all the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_{k+1}$. This inductive procedure completes our construction. □

Remark 5.9. There are algorithms for computing the ray class group of a given modulus and for computing a defining polynomial for the field associated to a congruence subgroup. They are particularly well suited in our situation since there is a specialised efficient algorithm for totally real fields and another one for complex quadratic fields. Both are described in [3, Chapter 6].

5.4 Elliptic curves in Legendre normal form and main result

The last easy ingredient we need is:

Lemma 5.10. *Let E be an elliptic curve over $\mathbb{Q}$ given in Legendre normal form by*

$$E : y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in \mathbb{Z}$ is odd. Then

- *E has split multiplicative reduction at all odd $q|(\lambda - 1)$;*
- *E has multiplicative reduction at all $q|\lambda$ and it is split multiplicative if and only if $q \equiv 1 \bmod 4$;*
- *E has potentially good reduction at 2 if and only if $\lambda \not\equiv 1 \bmod 32$. Moreover, if $\lambda \equiv 17 \bmod 32$ then E has good reduction at 2.*

- *E has good reduction at all other primes.*

Proof. We use the standard notation for the invariants Δ and c_4 associated to a Weierstrass equation for E (see [15, Ch. III §1]). If E is given in Legendre normal form as above then we have

$$c_4 = 16(\lambda^2 - \lambda + 1) \text{ and } \Delta = 16\lambda^2(\lambda - 1)^2.$$

Thus the primes of bad reduction must divide λ or $\lambda - 1$. Moreover for any such odd prime q, c_4 is a q-adic unit and so E has multiplicative reduction at q ([15, Ch. VII Prop. 5.1]). To determine whether it is split or non-split we use the following criterion ([16, p. 366]): let E/K be given by a Weierstrass equation with the coefficients $a_1, \ldots, a_6$ and assume that it has multiplicative reduction at a prime $\mathfrak{q}$, the singular point being $(0, 0)$. Then the reduction is split multiplicative if and only if the polynomial $T^2 + a_1T - a_2$ splits over the residue field at $\mathfrak{q}$.

In our case, if $q|\lambda$ then the singular point of the reduction modulo q is $(0, 0)$ and $a_1 = 0$, $a_2 = -\lambda - 1 \equiv -1 \bmod q$. So the polynomial splits if and only if -1 is a square modulo q.

If $q|\lambda - 1$ then perform the change of variables $x = x' + 1$. Then the singular point again becomes $(0, 0)$ and $a_1 = 0$, $a_2 = 2 - \lambda \equiv 1 \bmod q$ and so the polynomial always splits.

Finally, E has potentially good reduction at 2 if and only if the j-invariant is a 2-adic integer. But λ is odd, so

$$j = c_4^3/\Delta = 16^2(\lambda^2 - \lambda + 1)/\lambda^2(\lambda - 1)^2$$

is a 2-adic integer if and only if $\lambda - 1$ is not divisible by 32. If $\lambda \equiv 17 \bmod 32$ then it is easily seen that the substitution $x = 4x' + 1$, $y = 8y' + 4x'$ gives a Weierstrass equation which is integral with respect to 2 and with Δ a 2-adic unit. □

Theorem 5.11. *Let p be an odd prime number, $M/\mathbb{Q}$ any quadratic field but if $p \equiv 1 \bmod 4$ then assume that $M \neq \mathbb{Q}(\sqrt{p})$. Assume that p-primary parts of Tate-Shaffarevich groups of elliptic curves over number fields are always finite. Then the quantity*

$$p^{r(E/F)} \cdot \#Ш(E/F)[p^\infty]$$

is unbounded as E varies over elliptic curves over $\mathbb{Q}$ and $F/\mathbb{Q}$ varies over Galois extensions with dihedral Galois group of order $2p$ containing M.

Proof. Given any positive integer n, take a dihedral extension F of $\mathbb{Q}$ containing M such that n primes $q_1, \ldots, q_n$ that are inert in $M/\mathbb{Q}$ ramify in F/M and no other primes of M ramify in F. Such an F exists by Theorem 5.8. Take

$$\lambda = 16 \prod_{i=1}^{n} q_i + 1.$$

Then by Lemma 5.10, $E : y^2 = x(x-1)(x-\lambda)$ is semi-stable and has split multiplicative reduction at all these q_i. All other primes are unramified in F/M and thus have cyclic decomposition groups. The result follows from 5.2. □

We now only need to prove that in fact the p-Selmer gets large in our extensions and not just the p^∞-Selmer. This will be more naturally done in the next subsection. We will

close this subsection by illustrating the power of the technique of regulator constants by an explicit example. While classical questions about the arithmetic of elliptic curves only deal with the order of the torsion subgroups of the Mordell-Weil groups or with their ranks, ultimatelly one would like to know the full Galois structure of the Mordell-Weil group, not just the rank of its free component. We will demonstrate that regulator constants can provide such information, as usual dependent on the knowledge on the size of the Tate-Shaffarevich group:

Example 5.12. Recall from Example 1.4 that the group $G = S_3$ has two non-isomorphic indecomposable 2-dimensional $\mathbb{Z}G$-modules Γ and Γ' with regulator constants 3 and $1/3$, respectively. Let E/K be a semi-stable elliptic curve and F/K a Galois extension of number fields with Galois group G and set $L = F^{C_2}$, $M = F^{C_3}$. Among the primes of K which are inert in M/K and ramified in F/M, suppose that there are n more of split multiplicative reduction than of non-split multiplicative reduction. For simplicity, assume that $r(E/K) = r(E/M) = 0$. We easily compute that

$$\mathrm{ord}_3(C(E/\Theta)) = -n.$$

If we assume that $E(\Theta)[3^\infty] = 1$ and that 3-primary parts of all relevant Tate-Shaffarevich groups are finite then we conclude that either

$$\frac{\#Ш(E/K)[3^\infty]^2 \#Ш(E/F)[3^\infty]}{\#Ш(E/L)[3^\infty]^2 \#Ш(E/M)[3^\infty]} \geq 3^n \tag{9}$$

or the Galois module $E(F)/E(F)_{\mathrm{tors}}$ contains at least one copy of Γ. Moreover, in the former case, unless we have equality in equation (9), the Galois module $E(F)/E(F)_{\mathrm{tors}}$ must contain at least one copy of Γ'.

5.5 Unconditional proof of the main result

We now want to drop the assumption that Tate-Shaffarevich groups are finite. In this case we need to replace the usual BSD-quotient by a similar expression involving Selmer groups instead of Tate-Shaffarevich groups. We recall the relevant result from [5].

Definition 5.13. Given an isogeny $\psi : A \to B$ of abelian varieties over K, define

$$\begin{aligned} Q(\psi) = |\mathrm{coker}(\psi : A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}})| \times \\ \times |\ker(\psi : Ш(A/K)_{\mathrm{div}} \to Ш(B/K)_{\mathrm{div}})| \end{aligned}$$

where $Ш_{\mathrm{div}}$ denotes the divisible part of the Tate-Shaffarevich group.

Theorem 5.14. *Let $\phi : A \to B$ be an isogeny of abelian varieties over a number field K and $\phi^t : B^t \to A^t$ its dual isogeny. Let ω_A and ω_B be holomorphic n-forms on A and B, respectively, where $n = \dim A$ and set*

$$\Omega_A = \prod_{\substack{v|\infty \\ real}} \int_{A(K_v)} |\omega_A|. \prod_{\substack{v|\infty \\ complex}} 2 \int_{A(K_v)} \omega_A \wedge \overline{\omega_A}$$

and write $Ш_0(A/K)$ for $Ш(A/K)$ modulo its divisible part, define Ω_B and $Ш_0(B/K)$ similarly. Then we have

$$\frac{|A(K)_{\mathrm{tors}}|}{|B(K)_{\mathrm{tors}}|} \cdot \frac{|B^t(K)_{\mathrm{tors}}|}{|A^t(K)_{\mathrm{tors}}|} \cdot \frac{C(A/K)}{C(B/K)} \cdot \frac{\Omega_A}{\Omega_B} \prod_{p|\deg\phi} \frac{\#Ш_0(A/K)[p^\infty]}{\#Ш_0(B/K)[p^\infty]} = \frac{Q(\phi^t)}{Q(\phi)}. \tag{10}$$

Proof. See [5, Theorem 4.3]. □

Now let G be a finite group and

$$\Theta = \sum_i H_i - \sum_j H'_j$$

a G-relation. Let E/K be an elliptic curve and F/K be a Galois extension with Galois group G, let $L_i = F^{H_i}$ and $L'_j = F^{H'_j}$ and denote by $W_{L_i/K}(E)$, $W_{L'_j/K}(E)$ the Weil restrictions of scalars. As explained in [12, §2] and in [5, §4], given a G-injection

$$f : \oplus_i \mathbb{Z}[G/H_i] \to \oplus_j \mathbb{Z}[G/H'_j]$$

with finite cokernel of order d, we can construct an isogeny of abelian varieties

$$\phi : \prod_i W_{L_i/K}(E) \to \prod_j W_{L'_j/K}(E)$$

of degree d^2. If we set $A = \prod_i W_{L_i/K}(E)$ and $B = \prod_j W_{L'_j/K}(E)$ then $C(A/K)/C(B/K) = C(E/\Theta)$. We have already shown in Theorem 5.11 that if we take $K = \mathbb{Q}$ and $G = D_{2p}$ then we can choose E and F such that the Tamagawa-quotient gets arbitrarily large and such that F contains a predetermined quadratic subfield (subject to the restriction in the theorem). Also, if we take $p > 7$ and $E/\mathbb{Q}$ semi-stable, as in the proof of Theorem 5.2 then the p-part of

$$\frac{|A(K)_{\text{tors}}|}{|B(K)_{\text{tors}}|} \cdot \frac{|B^t(K)_{\text{tors}}|}{|A^t(K)_{\text{tors}}|}$$

is trivial as explained in the proof of Theorem 5.2. Finally, the real and complex periods cancel as before since they are equal to the corresponding periods of the elliptic curve as explained in [12]. Equation (10) implies that then at least one of $Ш_0(E/F)[p^\infty]$, $|\ker(\psi : Ш(A/K)_{\text{div}} \to Ш(B/K)_{\text{div}})|$ or $r(E/F)$ must get large. But for an isogeny like ϕ above of degree d^2 there exists an isogeny in the opposite direction such that their composition is multiplication by d^2 and thus induces the multiplication-by-d^2 map on the Tate-Shaffarevich group. Thus ϕ can kill at most $p^{2\text{ord}_p(d)}$ elements of the Tate-Shaffarevich group for each cyclic (divisible or non-divisible) component. It follows immediately that the p-Selmer group gets arbitrarily large when the Tamagawa quotient does. We therefore deduce

Theorem 5.15. *Given a prime number $p > 7$, any non-negative integer n and a quadratic field M (if $p \equiv 1 \bmod 4$ then assume $M \neq \mathbb{Q}(\sqrt{p})$), there exists a semi-stable elliptic curve $E/\mathbb{Q}$ and infinitely many cyclic extensions F/M of degree p which are Galois over $\mathbb{Q}$ such that $S_p(E/F) \geq p^n$.*

References

[1] A. Bartel. Large Selmer groups over number fields. *arXiv:0805.1231v3*, 2008.

[2] P. L. Clark and S. Sharif. Period, index and potential sha. *arXiv:0811.3019v1*, 2008.

[3] H. Cohen. *Advanced Topics in Computational Number Theory*. GTM 193. Springer-Verlag, 2000.

[4] C. Curtis and I. Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders*, volume II. John Wiley and Sons, 1987.

[5] T. Dokchitser and V. Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *arxiv: math.NT/06102920v2*, 2007.

[6] T. Dokchitser and V. Dokchitser. Self-duality of Selmer groups. *arXiv:0705.1899v1 [math.NT]*, 2007.

[7] T. Dokchitser and V. Dokchitser. Regulator constants and the parity conjecture. *arxiv: math.NT/0709.2852v2*, 2008.

[8] S. Lang. *Algebraic Number Theory*. GTM 110. Springer, second edition, 1994.

[9] M. P. Lee. Integral representations of dihedral groups of order $2p$. *Trans. American Math. Soc.*, 110(2):213–231, Feb. 1964.

[10] B. Mazur. Modular curves and the Eisenstein ideal. *IHES Publ. Math.*, 47:33–186, 1977.

[11] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44:129–162, 1978.

[12] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[13] J.-P. Serre. *Représentation Linéaires des Groupes finis*. Herman Paris, 1967.

[14] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[15] J. H. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106. Springer Verlag, 1985.

[16] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. GTM 151. Springer-Verlag, 1994.

[17] J. Tate. On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki*, 18e année(no. 306), 1965/66.