Arithmetic Chern–Simons Theory II

Hee-Joong Chung, Dohyeong Kim, Minhyong Kim, Jeehoon Park, and Hwajong Yoo

with "Appendix 2: Conjugation Action on Group Cochains: Categorical Approach" by Behrang Noohi.

Abstract In this paper, we apply ideas of Dijkgraaf and Witten [6, 32] on 3 dimensional topological quantum field theory to arithmetic curves, that is, the spectra of rings of integers in algebraic number fields. In the first three sections, we define

H.-J. Chung
Yau Mathematical Sciences Center, Tsinghua University, Haidian District,
Beijing 100084, China
e-mail: heejoongchung@gmail.com

D. Kim
Department of Mathematical Science and Research Institute of Mathematics,
Seoul National University, Gwanak-Ro 1, Gwanak-Gu, Seoul 08826, Republic of Korea
e-mail: dohyeongkim@snu.ac.kr

M. Kim (✉)
Mathematical Institute, University of Oxford, Woodstock Road,
Oxford OX2 6GG, UK
e-mail: minhyong.kim@maths.ox.ac.uk

Korea Institute for Advanced Study, 85 Hoegiro, Dongdaemun-gu, Seoul 02455,
Republic of Korea

J. Park
Department of Mathematics, Pohang University of Science and Technology,
77 Cheongam-Ro, Nam-Gu, Pohang, Gyeongbuk 37673, Republic of Korea
e-mail: jpark.math@gmail.com

H. Yoo
College of Liberal Studies, Seoul National University, Gwanak-Ro 1,
Gwanak-Gu, Seoul 08826, Republic of Korea
e-mail: hwajong@snu.ac.kr

B. Bhatt and M. Olsson (eds.), *p-adic Hodge Theory*, Simons Symposia,
https://doi.org/10.1007/978-3-030-43844-9_3

classical Chern–Simons actions on spaces of Galois representations. In the subsequent sections, we give formulas for computation in a small class of cases and point towards some arithmetic applications.

1 The Arithmetic Chern–Simons Action: Introduction and Definition

The purpose of this paper is to cast in concrete mathematical form the ideas presented in the preprint [17]. The reader is referred to that paper for motivation and speculation. Since there is no plan to submit it for separate publication, we repeat here the basic constructions before going on to a family of examples. This paper adheres, however, to a rather strict mathematical presentation. As we remind the reader below, the analogies in the background have come to be somewhat well-known under the heading of 'arithmetic topology.' The emphasis of this paper, however, will be less on analogies, and more on the possibility that specific technical tools of topology and physics can be imported into number theory.

Let $X = \mathrm{Spec}(\mathcal{O}_F)$, the spectrum of the ring of integers in a number field F. We assume that F is totally imaginary. Denote by $\mathbb{G}_{\mathrm{m}}$ the étale sheaf that associates to a scheme the units in the global sections of its coordinate ring. We have the following canonical isomorphism [20, p. 538]:

$$\mathrm{inv} : H^3(X, \mathbb{G}_{\mathrm{m}}) \simeq \mathbb{Q}/\mathbb{Z}. \qquad (*)$$

This map is deduced from the 'invariant' map of local class field theory. We will therefore use the same name for a range of isomorphisms having the same essential nature, for example,

$$\mathrm{inv} : H^3(X, \mathbb{Z}_p(1)) \simeq \mathbb{Z}_p, \qquad (**)$$

where $\mathbb{Z}_p(1) = \varprojlim_i \mu_{p^i}$, and $\mu_n \subset \mathbb{G}_{\mathrm{m}}$ is the sheaf of nth roots of 1. This follows from the exact sequence

$$0 \to \mu_n \to \mathbb{G}_{\mathrm{m}} \overset{(\cdot)^n}{\to} \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}/(\mathbb{G}_{\mathrm{m}})^n \to 0.$$

That is, according to *loc. cit.*,

$$H^2(X, \mathbb{G}_{\mathrm{m}}) = 0,$$

while by *op. cit.*, p. 551, we have

$$H^i(X, \mathbb{G}_{\mathrm{m}}/(\mathbb{G}_{\mathrm{m}})^n) = 0$$

for $i \geq 1$. If we break up the above into two short exact sequences,

$$0 \to \mu_n \to \mathbb{G}_{\mathrm{m}} \overset{(\cdot)^n}{\to} \mathcal{K}_n \to 0,$$

and

$$0 \to \mathcal{K}_n \to \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}/(\mathbb{G}_{\mathrm{m}})^n \to 0,$$

we deduce

$$H^2(X, \mathcal{K}_n) = 0,$$

from which it follows that

$$H^3(X, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

the n-torsion inside $\mathbb{Q}/\mathbb{Z}$. Taking the inverse limit over $n = p^i$ gives the second isomorphism above. The pro-sheaf $\mathbb{Z}_p(1)$ is a very familiar coefficient system for étale cohomology and (**) is reminiscent of the fundamental class of a compact oriented three manifold for singular cohomology. Such an analogy was noted by Mazur around 50 years ago [21] and has been developed rather systematically by a number of mathematicians, notably, Masanori Morishita [23]. Within this circle of ideas is included the analogy between knots and primes, whereby the map

$$\mathrm{Spec}(\mathcal{O}_F/\mathfrak{P}_v) \rightarrowtail X$$

from the residue field of a prime $\mathfrak{P}_v$ should be similar to the inclusion of a knot. Let F_v be the completion of F at the prime v and $\mathcal{O}_{F_v}$ its valuation ring. If one takes this analogy seriously (as did Morishita), the map

$$\mathrm{Spec}(\mathcal{O}_{F_v}) \to X,$$

should be similar to the inclusion of a handle-body around the knot, whereas

$$\mathrm{Spec}(F_v) \to X$$

resembles the inclusion of its boundary torus.[1] Given a finite set S of primes, we consider the scheme

$$X_S := \mathrm{Spec}(\mathcal{O}_F[1/S]) = X \setminus \{\mathfrak{P}_v\}_{v \in S}.$$

Since a link complement is homotopic to the complement of a tubular neighbourhood, the analogy is then forced on us between X_S and a three manifold with boundary given by a union of tori, one for each 'knot' in S. These of course are basic morphisms in 3 dimensional topological quantum field theory [1]. From this perspective, perhaps

[1] It is not clear to us that the topology of the boundary should really be a torus. This is reasonable if one thinks of the ambient space as a three-manifold. On the other hand, perhaps it's possible to have a notion of a knot in a *homology three-manifold* that has an exotic tubular neighbourhood?

the coefficient system $\mathbb{G}_{\mathrm{m}}$ of the first isomorphism should have reminded us of the S^1-coefficient important in Chern–Simons theory [6, 32]. A more direct analogue of $\mathbb{G}_{\mathrm{m}}$ is the sheaf $O_M^{\times}$ of invertible analytic functions on a complex variety M. However, for compact Kähler manifolds, the comparison isomorphism

$$H^1(M, S^1) \simeq H^1(M, O_M^{\times})_0,$$

where the subscript refers to the line bundles with trivial topological Chern class, is a consequence of Hodge theory. This indicates that in the étale setting with no natural constant sheaf of S^1's, the familiar $\mathbb{G}_{\mathrm{m}}$ has a topological nature, and can be regarded as a substitute.[2] One problem, however, is that the $\mathbb{G}_{\mathrm{m}}$-coefficient computed directly gives divisible torsion cohomology, whence the need for considering coefficients like $\mathbb{Z}_p(1)$ in order to get functions of geometric objects having an analytic nature as arise, for example, in the theory of torsors for motivic fundamental groups [4, 13–16].

We now move to the definition of the arithmetic Chern–Simons action. Let

$$\pi := \pi_1(X, \mathfrak{b}),$$

be the profinite étale fundamental group of X, where we take

$$\mathfrak{b} : \mathrm{Spec}(\overline{F}) \to X$$

to be the geometric point coming from an algebraic closure of F. Assume now that the group $\mu_n(\overline{F})$ of nth roots of unity is in F and fix a trivialisation $\zeta_n : \mathbb{Z}/n\mathbb{Z} \simeq \mu_n$. This induces the isomorphism

$$\mathrm{inv} : H^3(X, \mathbb{Z}/n\mathbb{Z}) \simeq H^3(X, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Now let A be a finite group and fix a class $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. Let

$$M(A) := \mathrm{Hom}_{cont}(\pi, A)/A$$

be the set of isomorphism classes of principal A-bundles over X. Here, the subscript refers to continuous homomorphisms, on which A is acting by conjugation. For $[\rho] \in M(A)$, we get a class

$$\rho^*(c) \in H^3(\pi, \mathbb{Z}/n\mathbb{Z})$$

that depends only on the isomorphism class $[\rho]$; if $\rho_2 = \mathrm{Ad}_a \circ \rho_1$ for some $a \in A$, then $\rho_2^*(c) = \rho_1^*(\mathrm{Ad}_a^*(c))$, but c and $\mathrm{Ad}_a^*(c)$ are cohomologous by Lemma 7.2. Denote

[2] Recall, however, that it is of significance in Chern–Simons theory that one side of this isomorphism is purely topological while the other has an analytic structure.

by inv also the composed map

$$H^3(\pi, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^3(X, \mathbb{Z}/n\mathbb{Z}) \xrightarrow[\simeq]{\text{inv}} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

We get thereby a function

$$\begin{aligned} CS_c : M(A) &\longrightarrow \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}; \\ [\rho] &\longmapsto \text{inv}(\rho^*(c)). \end{aligned}$$

This is the basic and easy case of the classical Chern–Simons action[3] in the arithmetic setting.

Section 2 sets down some definitions for 'manifolds with boundary,' that is, X_S as above. In fact, it turns out that the Chern–Simons action with boundaries is necessary for the computation of the action even in the 'compact' case, in a manner strongly reminiscent of computations in topology (see [7, Theorem 1.7 (d)], for example). That is, we will compute the Chern–Simons invariant of a representation ρ of π using a suitable decomposition

$$X\text{``} = \text{''}X_S \cup [\cup_v \text{Spec}(\mathcal{O}_{F_v})]$$

and restrictions of π to X_S and the $\text{Spec}(\mathcal{O}_{F_v})$.

To describe the construction, we need more notations. We assume that all primes of F dividing n are in the finite set of primes S. Let

$$\pi_S := \pi_1(X_S, \mathfrak{b})$$

and

$$\pi_v := \text{Gal}(\overline{F}_v/F_v)$$

equipped with maps

$$i_v : \pi_v \to \pi_S$$

given by choices of embeddings $\overline{F} \hookrightarrow \overline{F}_v$. The collection

$$\{i_v\}_{v \in S}$$

will be denoted by i_S. There is a natural quotient map

$$\kappa_S : \pi_S \to \pi.$$

[3] The authors realise that this terminology is likely to be unfamiliar, and maybe even appears pretentious to number-theorists. However, it does seem to encourage the reasonable view that concepts and structures from geometry and physics can be specifically useful in number theory.

Let

$$Y_S(A) := \mathrm{Hom}_{cont}(\pi_S, A)$$

and denote by $\mathcal{M}_S(A)$ the action groupoid whose objects are the elements of $Y_S(A)$ with morphisms given by the conjugation action of A. We also have the local version

$$Y_S^{loc}(A) := \prod_{v \in S} \mathrm{Hom}_{cont}(\pi_v, A)$$

as well as the action groupoid $\mathcal{M}_S^{loc}(A)$ with objects $Y_S^{loc}(A)$ and morphisms given by the action of $A^S := \prod_{v \in S} A$ conjugating the separate components in the obvious sense. Thus, we have the restriction functor

$$r_S : \mathcal{M}_S(A) \to \mathcal{M}_S^{loc}(A),$$

where a homomorphism $\rho : \pi_S \to A$ is restricted to the collection

$$r_S(\rho) = i_S^* \rho := (\rho \circ i_v)_{v \in S}.$$

We will construct, in Sect. 2, a functor L from $\mathcal{M}_S^{loc}(A)$ to the $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsors as a finite arithmetic version of the Chern–Simons line bundle [7] over $\mathcal{M}_S^{loc}(A)$. To a global representation $\rho \in \mathcal{M}_S(A)$, the Chern–Simons action will then associate an element (Eq. (2.3))

$$CS_c([\rho]) \in L(r_S(\rho)).$$

Now, given $[\rho] \in \mathcal{M}(A)$, we pull it back to $[\rho \circ \kappa_S] \in \mathcal{M}_S(A)$ and apply the Chern–Simons action with boundary to get an element

$$CS_c([\rho \circ \kappa_S]) \in L([r_S(\rho \circ \kappa_S)]).$$

On the other hand, for each $v \in S$, we can pull back ρ to a local unramified representation

$$\rho_v^{\mathrm{ur}} : \pi_v^{\mathrm{ur}} \to \pi \to A,$$

where π_v^{ur} is the unramified quotient of π_v. The extra structure of the unramified representation will then allow us to canonically associate an element

$$\sum_{v \in S} (\beta_v) \in L([r_S(\rho \circ \kappa_S)]),$$

which can be interpreted as the Chern–Simons action of $(\rho_v^{\mathrm{ur}})_{v \in S}$ on $\cup_{v \in S} \mathrm{Spec}(\mathcal{O}_{F_v})$.

Theorem 1.1 (The Decomposition Formula) *Let A be a finite group and fix a class $c \in H^3(A, \mathbb{Z}/n\mathbb{Z})$. Then*

$$CS_c([\rho]) = \sum_{v\in S}(\beta_v) - CS_c([\rho \circ \kappa_S])$$

for $[\rho] \in \mathcal{M}(A)$.

Section 4 is devoted to a proof of Theorem 1.1. The key point of this formula is that $CS_c([\rho])$ can be computed as the difference between two trivialisations of the torsor, a ramified global trivialisation and an unramified local trivialisation.

In Sect. 5, we use this theorem to compute the Chern–Simons action for a class of examples. It is amusing to note the form of the action when A is finite cyclic. That is, let $A = \mathbb{Z}/n\mathbb{Z}$, $\alpha \in H^1(A, \mathbb{Z}/n\mathbb{Z})$ the class of the identity, and $\beta \in H^2(A, \mathbb{Z}/n\mathbb{Z})$ the class of the extension

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{n} \mathbb{Z}/n^2\mathbb{Z} \longrightarrow A \longrightarrow 0.$$

Then $\beta = \delta\alpha$, where $\delta : H^1(A, \mathbb{Z}/n\mathbb{Z}) = H^1(A, A) \to H^2(A, \mathbb{Z}/n\mathbb{Z})$ is the boundary map arising from the extension. Put

$$c := \alpha \cup \beta = \alpha \cup \delta\alpha \in H^3(A, \mathbb{Z}/n\mathbb{Z}).$$

Then

$$CS_c([\rho]) = \mathrm{inv}[\rho^*(\alpha) \cup \delta\rho^*(\alpha)],$$

in close analogy to the[4] formulas of abelian Chern–Simons theory.

However, our computations are not limited to the case where A is an abelian cyclic group. Along similar lines, we will provide an infinite family of number fields F and representations ρ such that $CS_c([\rho])$ is non-vanishing for $[\rho] \in M(A)$ with a different class $c \in H^3(A, \mathbb{Z}/2\mathbb{Z})$ and both abelian A (see Propositions 5.14, 5.16, and 5.19) and non-abelian A (see Proposition 5.23).

In Sect. 6, we provide arithmetic applications to a class of Galois embedding problems using the fact that the existence of an unramified extension forces a Chern–Simons invariant to be zero.

In this paper, we do not develop a p-adic theory in the case where the boundary is empty. In future papers, we hope to apply local trivialisations using Selmer complexes to remedy this omission and complete the theory begun in Sect. 3. To get actual p-adic functions, one needs of course to come to an understanding of explicit cohomology classes on p-adic Lie groups, possibly by way of the theory of Lazard [18]. Suitable quantisations of the theory of this paper in a manner amenable to arithmetic applications will be explored as well in future work, as in [3], where a precise arithmetic analogue of a 'path-integral formula' for arithmetic linking numbers is proved. In that preprint, a connection is made also to the class invariant homomorphism from additive Galois module structure theory. A pro-p version of this homomorphism is related to p-adic L-functions and heights, providing some evidence for the speculation from [17].

[4] In fact, every cohomology class in $H^3(A, \mathbb{Z}/n\mathbb{Z})$ can be written as this form (cf. [25, Sect. 1.7]).

2 The Arithmetic Chern–Simons Action: Boundaries

We keep the notations as in the introduction. We will now employ a cocycle $c \in Z^3(A, \mathbb{Z}/n\mathbb{Z})$ to associate a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor to each point of $Y_S^{loc}(A)$ in an A^S-equivariant manner. We use the notation

$$C_S^i := \prod_{v \in S} C^i(\pi_v, \mathbb{Z}/n\mathbb{Z})$$

for the continuous cochains,

$$Z_S^i := \prod_{v \in S} Z^i(\pi_v, \mathbb{Z}/n\mathbb{Z}) \subset C_S^i$$

for the cocycles, and

$$B_S^i := \prod_{v \in S} B^i(\pi_v, \mathbb{Z}/n\mathbb{Z}) \subset Z_S^i \subset C_S^i$$

for the coboundaries. In particular, we have the coboundary map (see Appendix "Appendix 1: Conjugation on Group Cochains" for the sign convention)

$$d : C_S^2 \to Z_S^3.$$

Let $\rho_S := (\rho_v)_{v \in S} \in Y_S^{loc}(A)$ and put

$$c \circ \rho_S := (c \circ \rho_v)_{v \in S},$$

$$c \circ \mathrm{Ad}_a := (c \circ \mathrm{Ad}_{a_v})_{v \in S}$$

for $a = (a_v)_{v \in S} \in A^S$, where Ad_{a_v} refers to the conjugation action. To define the arithmetic Chern–Simons line associated to ρ_S, we need the intermediate object

$$H(\rho_S) := d^{-1}(c \circ \rho_S)/B_S^2 \subset C_S^2/B_S^2.$$

This is a torsor for

$$H_S^2 := \prod_{v \in S} H^2(\pi_v, \mathbb{Z}/n\mathbb{Z}) \simeq \prod_{v \in S} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

([25, Theorem (7.1.8)]). We then use the sum map

$$\Sigma : \prod_{v \in S} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

to push this out to a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor. That is, define

$$L(\rho_S) := \Sigma_*[H(\rho_S)]. \tag{2.1}$$

The natural map $H(\rho_S) \to L(\rho_S)$ will also be denoted by the sum symbol Σ.

In fact, L extends to a functor from $\mathcal{M}_S^{loc}(A)$ to the category of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsors. To carry out this extension, we just need to extend H to a functor to H_S^2-torsors. According to Appendices "Appendix 1: Conjugation on Group Cochains" and "Appendix 2: Conjugation Action on Group Cochains: Categorical Approach", for $a = (a_v)_{v\in S} \in A^S$ and each v, there is an element $h_{a_v} \in C^2(A, \mathbb{Z}/n\mathbb{Z})/B^2(A, \mathbb{Z}/n\mathbb{Z})$ such that

$$c \circ \mathrm{Ad}_{a_v} = c + dh_{a_v}.$$

Also,

$$h_{a_v b_v} = h_{a_v} \circ \mathrm{Ad}_{b_v} + h_{b_v}.$$

Hence, given $a : \rho_S \to \rho'_S$, so that $\rho'_S = \mathrm{Ad}_a \circ \rho_S$, we define

$$H(a) : H(\rho_S) \to H(\rho'_S)$$

to be the map induced by

$$x \mapsto x' = x + (h_{a_v} \circ \rho_v)_{v\in S}.$$

Then

$$dx' = dx + (d(h_{a_v} \circ \rho_v))_{v\in S} = (c \circ \rho_v)_{v\in S} + ((dh_{a_v}) \circ \rho_v)_{v\in S} = (c \circ \mathrm{Ad}_{a_v} \circ \rho_v)_{v\in S}.$$

So

$$x' \in d^{-1}(c \circ \rho'_S)/B_S^2,$$

and by the formula above, it is clear that H is a functor.[5] That is, ab will send x to

$$x + h_{ab} \circ \rho_S,$$

while if we apply b first, we get

$$x + h_b \circ \rho_S \in H(\mathrm{Ad}_b \circ \rho_S),$$

which then goes via a to

[5] While the functor H does depend on the choices of h_a, they are intrinsic to A, in that they are cochains on A, not a priori related to the Galois representations. So we may regard them as part of the data defining the field theory, similar to c.

$$x + h_b \circ \rho_S + h_a \circ \mathrm{Ad}_b \circ \rho_S.$$

Thus,

$$H(ab) = H(a)H(b).$$

Defining

$$L(a) = \Sigma_* \circ H(a)$$

turns L into a functor from $\mathcal{M}_S^{loc}$ to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsors. Even though we are not explicitly laying down geometric foundations, it is clear that L defines thereby an A^S-equivariant $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor on $Y_S^{loc}(A)$, or a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor on the stack $\mathcal{M}_S^{loc}(A)$.

We can compose the functor L with the restriction $r_S : \mathcal{M}_S(A) \to \mathcal{M}_S^{loc}(A)$ to get an A-equivariant functor L^{glob} from $Y_S(A)$ to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsors.

Lemma 2.1 *Let $\rho \in Y_S(A)$ and $a \in \mathrm{Aut}(\rho)$. Then $L^{glob}(a) = 0$.*

Proof By assumption, $\mathrm{Ad}_a\rho = \rho$, and hence, $dh_a \circ \rho = 0$. That is, $h_a \circ \rho \in H^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$. Hence, by the reciprocity law for $H^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$ ([25, Theorem (8.1.17)]), we get

$$\Sigma_*(h_a \circ \rho) = 0.$$

By the argument of [7, p. 439], we see that there is a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor

$$L^{\mathrm{inv}}([\rho])$$

of invariant sections for the functor L^{glob} depending only on the orbit $[\rho]$. This is the set of families of elements

$$x_{\rho'} \in L^{glob}(\rho')$$

as ρ' runs over $[\rho]$ with the property that every morphism $a : \rho_1 \to \rho_2$ takes x_{ρ_1} to x_{ρ_2}. Alternatively, $L^{\mathrm{inv}}([\rho])$ is the inverse limit of the $L^{glob}(\rho')$ with respect to the indexing category $[\rho]$.

Since

$$H^3(\pi_S, \mathbb{Z}/n\mathbb{Z}) = 0$$

([25, Proposition (8.3.18)]), the cocycle $c \circ \rho$ is a coboundary

$$c \circ \rho = d\beta \tag{2.2}$$

for $\beta \in C^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$. This element defines a class

$$CS_c([\rho]) := \Sigma([i_S^*(\beta)]) \in L^{\mathrm{inv}}([\rho]). \tag{2.3}$$

A different choice β' will be related by

$$\beta' = \beta + z$$

for a 2-cocycle $z \in Z^2(\pi_S, \mathbb{Z}/n\mathbb{Z})$, which vanishes when mapped to $L((\rho \circ i_v)_{v \in S})$ because of the reciprocity sequence

$$\begin{tikzcd} 0 \arrow[r] & H^2(\pi_S, \mathbb{Z}/n\mathbb{Z}) \arrow[r] & H^2_S \arrow[r, "\sum_v \mathrm{inv}_v"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

Thus, the class $CS_c([\rho])$ is independent of the choice of β and defines a global section

$$CS_c \in \Gamma(\mathcal{M}_S(A), L^{glob}).$$

Within the context of this paper, a 'global section' should just be interpreted as an assignment of $CS_c([\rho])$ as above for each orbit $[\rho]$.

3 The Arithmetic Chern–Simons Action: The p-adic Case

Now fix a prime p and assume all primes of F dividing p are contained in S. Fix a compatible system $(\zeta_{p^n})_n$ of p-power roots of unity, giving us an isomorphism

$$\zeta : \mathbb{Z}_p \simeq \mathbb{Z}_p(1) := \varprojlim_n \mu_{p^n}.$$

In this section, we will be somewhat more careful with this isomorphism. Also, it will be necessary to make some assumptions on the representations that are allowed.

Let A be a p-adic Lie group, e.g., $GL_n(\mathbb{Z}_p)$. Assume A is equipped with an open homomorphism[6] $t : A \to \Gamma := \mathbb{Z}_p^\times$ and define A^n to be the kernel of the composite map

$$A \to \mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times =: \Gamma_n.$$

Let

$$A^\infty = \cap_n A^n = \mathrm{Ker}(t).$$

In this section, we denote by $Y_S(A)$ the continuous homomorphisms

$$\rho : \pi_S \to A$$

such that $t \circ \rho$ is a power χ^s of the p-adic cyclotomic character χ of π_S by a p-adic unit s. (We note that s itself is allowed to vary.) Of course this condition will be satisfied by any geometric Galois representations or natural p-adic families containing one.

As before, A acts on $Y_S(A)$ by conjugation. But in this section, we will restrict the action to A^∞ and use the notation $\mathcal{M}_S(A)$ for the corresponding action groupoid.

Similarly, we denote by Y_S^{loc} the collections of continuous homomorphisms

[6] For example, one may choose t to be the determinant when $A = GL_n(\mathbb{Z}_p)$.

$$\rho_S := (\rho_v : \pi_v \to A)_{v \in S}$$

for which there exists a p-adic unit s such that $t \circ \rho_v = (\chi|_{\pi_v})^s$ for all v. $\mathcal{M}_S^{loc}(A)$ then denotes the action groupoid defined by the product $(A^\infty)^S$ of the conjugation action on the ρ_S.

We now fix a continuous cohomology class

$$c \in H^3(A, \mathbb{Z}_p[[\varGamma]]),$$

where

$$\mathbb{Z}_p[[\varGamma]] = \varprojlim_n \mathbb{Z}_p[\varGamma_n].$$

We represent c by a cocycle in $Z^3(A, \mathbb{Z}_p[[\varGamma]])$, which we will also denote by c. Given $\rho \in Y_S(A)$, we can view $\mathbb{Z}_p[[\varGamma]]$ as a continuous representation of π_S, where the action is left multiplication via $t \circ \rho$. We denote this representation by $\mathbb{Z}_p[[\varGamma]]_\rho$. The isomorphism $\zeta : \mathbb{Z}_p \simeq \mathbb{Z}_p(1)$, even though it's not π_S-equivariant, does induce a π_S-equivariant isomorphism

$$\zeta_\rho : \mathbb{Z}_p[[\varGamma]]_\rho \simeq \varLambda := \mathbb{Z}_p[[\varGamma]] \otimes \mathbb{Z}_p(1).$$

Here, $\mathbb{Z}_p[[\varGamma]]$ written without the subscript refers to the action via the cyclotomic character of π_S (with $s = 1$ in the earlier notation). The isomorphism is defined as follows. If $t \circ \rho = \chi^s$, then we have the isomorphism

$$\mathbb{Z}_p[[\varGamma]] \simeq \mathbb{Z}_p[[\varGamma]]_\rho$$

that sends γ to γ^s. On the other hand, we also have

$$\mathbb{Z}_p[[\varGamma]] \simeq \varLambda$$

that sends γ to $\gamma \otimes \gamma\zeta(1)$. Thus, ζ_ρ can be taken as the inverse of the first followed by the second.

Combining these considerations, we get an element

$$\zeta_\rho \circ \rho^* c = \zeta_\rho \circ c \circ \rho \in Z^3(\pi_S, \varLambda).$$

Similarly, if $\rho_S := (\rho_v)_{v \in S} \in Y_S^{loc}$, we can regard $\mathbb{Z}_p[[\varGamma]]_{\rho_v}$ as a representation of π_v for each v, and we get π_v-equivariant isomorphisms

$$\zeta_{\rho_v} : \mathbb{Z}_p[[\varGamma]]_{\rho_v} \simeq \varLambda.$$

We also use the notation

$$\zeta_{\rho_S} : \prod_{v \in S} \mathbb{Z}_p[[\Gamma]]_{\rho_v} \simeq \prod_{v \in S} \Lambda$$

for the isomorphism given by the product of the ζ_{ρ_v}.

It will be convenient to again denote by $C^i_S(\Lambda)$ the product $\prod_{v \in S} C^i(\pi_v, \Lambda)$ and use the similar notations $Z^i_S(\Lambda)$, $B^i_S(\Lambda)$ and $H^i_S(\Lambda)$. The element $\zeta_{\rho_S} \circ \rho_S^* c$ is an element in $Z^3_S(\Lambda)$. We then put

$$H(\rho_S, \Lambda) := d^{-1}(\zeta_{\rho_S} \circ \rho_S^* c)/B^2_S(\Lambda) \subset C^2_S(\Lambda)/B^2_S(\Lambda).$$

This is a torsor for

$$H^2_S(\Lambda) \simeq \prod_{v \in S} H^2(\pi_v, \Lambda).$$

The augmentation map

$$a : \Lambda \to \mathbb{Z}_p(1)$$

for each v can be used to push this out to a torsor

$$a_*(H(\rho_S, \Lambda))$$

for the group

$$\prod_{v \in S} H^2(\pi_v, \mathbb{Z}_p(1)) \simeq \prod_{v \in S} \mathbb{Z}_p,$$

which then can be pushed out with the sum map

$$\Sigma : \prod_{v \in S} \mathbb{Z}_p \to \mathbb{Z}_p$$

to give us a $\mathbb{Z}_p$-torsor

$$L(\rho_S, \mathbb{Z}_p) := \Sigma_*(a_*(H(\rho_S, \Lambda))).$$

As before, we can turn this into a functor $L(\cdot, \mathbb{Z}_p)$ on $\mathcal{M}^{loc}_S(A)$, taking into account the action of $(A^\infty)^S$. By composing with the restriction functor

$$r_S : \mathcal{M}_S(A) \to \mathcal{M}^{loc}_S(A),$$

we also get a $\mathbb{Z}_p$-torsor $L^{glob}(\cdot, \mathbb{Z}_p)$ on $\mathcal{M}_S(A)$.

We now choose an element $\beta \in C^2(\pi_S, \Lambda)$ such that

$$d\beta = \zeta_\rho \circ c \circ \rho \in Z^3(\pi_S, \Lambda) = B^3(\pi_S, \Lambda)$$

to define the p-adic Chern–Simons action

$$CS_c([\rho]) := \Sigma_* a_* i_S^*(\beta) \in L^{glob}([\rho], \mathbb{Z}_p).$$

The argument that this action is independent of β and equivariant is also the same as before, giving us an element

$$CS_c \in \Gamma(\mathcal{M}_S(A), L^{glob}(\cdot, \mathbb{Z}_p)).$$

4 Towards Computation: The Decomposition Formula

In this section, we indicate how one might go about computing the arithmetic Chern–Simons invariant in the unramified case with finite coefficients. That is, we assume that we are in the setting of Sect. 1. We provide a proof of Theorem 1.1 in a slightly generalized setting.

Let $X = \mathrm{Spec}(\mathcal{O}_F)$ and M a continuous representation of $\pi = \pi_1(X, \mathfrak{b})$ regarded as a locally constant sheaf on X. Assume $M = \varprojlim M_i$ with M_i finite representations such that there is a finite set T of primes in $\mathcal{O}_F$ containing all primes dividing the order of any $|M_i|$. Let $U = \mathrm{Spec}(\mathcal{O}_{F,\ T})$, $\pi_T = \pi_1(U, \mathfrak{b})$, and $\pi_v = \mathrm{Gal}(\overline{F}_v/F_v)$ for a prime v of F. Fix natural homomorphisms

$$\kappa_T : \pi_T \to \pi \quad \text{and} \quad \kappa_v : \pi_v \to \pi.$$

We denote by ρ_T (resp. ρ_v) the composition of κ_T (resp. k_v) with

$$\rho \in \mathrm{Hom}_{cont}(\pi, M).$$

Finally, we write $\mathfrak{P}_v$ for the maximal ideal of $\mathcal{O}_F$ corresponding to the prime v and r_v for the restriction map of cochains or cohomology classes from π_T to π_v.

Denote by $C_c^*(\pi_T, M)$ the complex defined as a mapping fiber

$$C_c^*(\pi_T, M) := \mathrm{Fiber}[C^*(\pi_T, M) \to \prod_{v \in T} C^*(\pi_v, M)].$$

So

$$C_c^n(\pi_T, M) = C^n(\pi_T, M) \times \prod_{v \in T} C^{n-1}(\pi_v, M),$$

and

$$d(a, (b_v)_{v\in T}) = (da, (r_v(a) - db_v)_{v \in T})$$

for $(a, (b_v)_{v\in T}) \in C_c^n(\pi_T, M)$. As in [10, p. 18–19], since there are no real places in F, there is a quasi-isomorphism

$$C_c^*(\pi_T, M) \simeq R\Gamma(X, j_! j^*(M)),$$

where $j : U \to X$ is the inclusion. But there is also an exact sequence

$$0 \longrightarrow j_! j^*(M) \longrightarrow M \longrightarrow i_* i^*(M) \longrightarrow 0,$$

where $i : T \to X$ is the closed immersion complementary to j. Thus, we get an exact sequence

$$\prod_{v\in T} H^2(k_v, i^*(M)) \longrightarrow H^3(C_c^*(\pi_T, M)) \longrightarrow H^3(X, M) \longrightarrow \prod_{v\in T} H^3(k_v, i^*(M)),$$

where $k_v := \mathrm{Spec}(O_F/\mathfrak{P}_v)$, from which we get an isomorphism

$$H_c^3(U, M) := H^3(C_c^*(\pi_T, M)) \simeq H^3(X, M),$$

since k_v has cohomological dimension 1.

We interpret this as a statement that the cohomology of X

$$H^3(X, M)$$

can be identified with cohomology of a 'compactification' of U with respect to the 'boundary,' that is, the union of the $\mathrm{Spec}(F_v)$ for $v \in T$. This means that a class $z \in H^3(X, M)$ is represented by $(a, (b_v)_{v\in T})$, where $a \in Z^3(\pi_T, M)$ and $b_v \in C^2(\pi_v, M)$ in such a way that

$$db_v = r_v(a).$$

There is also the exact sequence

$$\longrightarrow H^2(\pi_T, M) \longrightarrow \prod_{v\in T} H^2(\pi_v, M) \longrightarrow H_c^3(U, M) \longrightarrow 0,$$

the last zero being $H^3(U, M) := H^3(\pi_T, M) = 0$. We can use this to compute the invariant of z when $M = \mu_n$. (Note that F contains μ_n and hence it is in fact isomorphic to the constant sheaf $\mathbb{Z}/n\mathbb{Z}$.) We have to lift z to a collection of classes $x_v \in H^2(\pi_v, \mu_n)$ and then take the sum

$$\mathrm{inv}(z) = \sum_v \mathrm{inv}_v(x_v).$$

This is independent of the choice of the x_v by the reciprocity law (cf. [20, p. 541]). The lifting process may be described as follows. The map

$$\prod_{v\in T} H^2(\pi_v, \mu_n) \longrightarrow H_c^3(U, \mu_n)$$

just takes a tuple of 2-cocycles $(x_v)_{v\in T}$ to $(0, (x_v)_{v\in T})$. But by the vanishing of $H^3(U, \mu_n)$, given $z = (a, (b_{-,v})_{v\in T})$, we can find a global cochain $b_+ \in C^2(\pi_T, \mu_n)$ such that $db_+ = a$. We then put

$$x_v := b_{-,v} - r_v(b_+).$$

Note that $(0, (x_v)_{v\in T})$ is cohomologous to $z = (a, (b_{-,v})_{v\in T})$.

As before, we start with a class $c \in H^3(A, \mu_n) \simeq H^3(A, \mathbb{Z}/n\mathbb{Z})$. Then, we get a class

$$z = j^3 \circ \rho^*(c) \in H^3(X, \mu_n),$$

where $j^i : H^i(\pi, \mu_n) \to H^i(X, \mu_n)$ is the natural map from group cohomology to étale cohomology (cf. [22, Theorem 5.3 of Chap. I]). Let w be a cocycle representing $\rho^*(c) \in H^3(\pi, \mu_n)$. Let $I_v \subset \pi_v$ be the inertia subgroup. We now can trivialise $\kappa_v^*(w)$ by first doing it over π_v/I_v to which it factors. That is, the $b_{-,v}$ as above can be chosen as cochains factoring through π_v/I_v. This is possible because $H^3(\pi_v/I_v, \mu_n) = 0$. The class $(\kappa_T^*(w), (b_{-,v})_{v\in T})$ chosen in this way is independent of the choice of the $b_{-,v}$. This is because $H^2(\pi_v/I_v, \mu_n)$ is also zero. The point is that the representation of z as $(\kappa_T^*(w), (b_{-,v})_{v\in T})$ with unramified $b_{-,v}$ is essentially canonical. More precisely, given $\kappa_v^*(w)|_{(\pi_v/I_v)} \in Z^3(\pi_v/I_v, \mu_n)$, there is a canonical

$$b_{-,v} \in C^2(\pi_v/I_v, \mu_n)/B^2(\pi_v/I_v, \mu_n)$$

such that $db_{-,v} = \kappa_v^*(w)|_{(\pi_v/I_v)}$. This can then be lifted to a canonical class in

$$C^2(\pi_v, \mu_n)/B^2(\pi_v, \mu_n).$$

Now we trivialise $\kappa_T^*(w)$ globally as above, that is, by the choice of $b_+ \in C^2(\pi_T, \mu_n)$ such that $db_+ = \kappa_T^*(w)$. Then $(b_{-,v} - b_{+,v})_{v\in T}$ will be cocycles, where $b_{+,v} := r_v(b_+)$, and we compute

$$\mathrm{inv}(z) = \sum_{v\in T} \mathrm{inv}_v(b_{-,v} - b_{+,v}).$$

Thus, for a given homomorphism $\rho : \pi \to A$, it suffices to find various trivialisations of $\rho^*(c)$ after restriction to π_T and to π_v for $v \in T$.

- We are free to choose a finite set T of primes in a convenient way as long as T contains all primes dividing n. And then, for any $v \in T$, solve

$$db_{-,v} = \rho_v^*(c) \in Z^3(\pi_v, \mu_n).$$

  In fact, $b_{-,v}$ comes from an element in $C^2(\pi_v/I_v, \mu_n)$ by inflation, so $b_{-,v}$ is unramified.
- For chosen T, solve

$$db_+ = \rho_T^*(c) \in Z^3(\pi_T, \mu_n),$$

and we set $b_{+,v} = r_v(b_+) \in C^2(\pi_v, \mu_n)$.

Then, we have the decomposition formula

$$CS_c([\rho]) = \sum_{v \in T} \mathrm{inv}_v([b_{-,v} - b_{+,v}]). \tag{†}$$

In the case $M = \mu_n$ and $S = T$, a finite set of primes in O_F containing all primes dividing n, a simple inspection implies that

$$\sum_{v \in T} \mathrm{inv}_v([b_{-,v} - b_{+,v}]) = \sum_{v \in S} (\beta_v) - CS_c([\rho \circ \kappa_S]).$$

Thus, the formula (†) provides a proof of Theorem 1.1. In general, $b_{-,v}$ and $b_{+,v}$ are not cocycles but their difference is. This corresponds to the fact that $\sum_{v \in S} (\beta_v)$ and $CS_c([\rho \circ \kappa_S])$ are not an element of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ but their difference is.

A few remarks about this method:

1. Underlying this is the fact that the compact support cohomology $H_c^3(U, \mu_n)$ can be computed relative to the somewhat fictitious boundary of U or as relative cohomology $H^3(X, T; \mu_n)$. Choosing the unramified local trivialisations corresponds to this latter representation.

2. To summarise the main idea again, starting from a cocycle $z \in Z^3(\pi, \mu_n)$ we have canonical unramified trivialisations at each v and a non-canonical global ramified trivialisation.

The invariant of z measures the discrepancy between the unramified local trivialisations and a ramified global trivialisation.

The fact that the non-canonicality of the global trivialisation is unimportant follows from the reciprocity law (cf. [20, p. 541]).

3. The description above that computes the invariant by comparing the local unramified trivialisation with the global ramified one is a precise analogue of the so-called 'gluing formula' for Chern–Simons invariants when applied to $\rho^*(c)$ for a representation $\rho : \pi \to \mathbb{Z}/n\mathbb{Z}$ and a 3-cocycle c on $\mathbb{Z}/n\mathbb{Z}$.

5 Examples

In this section, we provide several explicit examples of computation of $CS_c([\rho])$. We still assume that we are in the setting of Sect. 1.

5.1 General Strategy

To compute the arithmetic Chern–Simons invariants, we essentially use the decomposition formula (†) in Sect. 4. The most difficult part in the above method is finding an element $b_+ \in C^2(\pi_T, \mu_n)$ that gives a global trivialisation.

To simplify our problem, we assume that a cocycle $c \in Z^3(A, \mu_n)$ is defined by the cup product:

$$c = \alpha \cup \epsilon,$$

where $\alpha \in Z^1(A, \mu_n) = \mathrm{Hom}(A, \mu_n)$ and $\epsilon \in Z^2(A, \mathbb{Z}/n\mathbb{Z})$ is a cocycle representing an extension

$$E : 0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \Gamma \xrightarrow[\varphi]{} A \longrightarrow 1.$$

We note that if we take a section σ of φ that sends e_A to e_Γ, then

$$\epsilon(x, y) = \sigma(x) \cdot \sigma(y) \cdot \sigma(xy)^{-1} \in \mathrm{Ker}\, \varphi = \mathbb{Z}/n\mathbb{Z}$$

(cf. [30, p. 183]). As discussed in Sect. 1, this assumption is vacuous if $A = \mathbb{Z}/n\mathbb{Z}$.

To find $b_{-,v}$ and $b_{+,v}$ in the decomposition formula (†), we first trivialise ϵ in π_v and π_T, respectively. Namely, let

$$d\gamma_{-,v} = \rho_v^*(\epsilon) \quad \text{and} \quad d\gamma_+ = \rho_T^*(\epsilon).$$

Here, the precise choice of $\gamma_{-,v}$ will be unimportant, except it should be unramified and normalised so that $\gamma_{-,v}(e_A) = 0$. Hence, we will be inexplicit below about this choice. Again, let $\gamma_{+,v} = r_v(\gamma_+)$. Then, we have

$$d(\rho_v^*(\alpha) \cup \gamma_{-,v}) = -\rho_v^*(\alpha) \cup d\gamma_{-,v} = -\rho_v^*(\alpha \cup \epsilon) = -\rho_v^*(c)$$

and

$$d(\rho_T^*(\alpha) \cup \gamma_+) = -\rho_T^*(\alpha) \cup d\gamma_+ = -\rho_T^*(\alpha \cup \epsilon) = -\rho_T^*(c).$$

Therefore, we can find

$$b_{-,v} = -\rho_v^*(\alpha) \cup \gamma_{-,v} \quad \text{and} \quad b_{+,v} = r_v(b_+) = r_v(-\rho_T^*(\alpha) \cup \gamma_+) = -\rho_v^*(\alpha) \cup \gamma_{+,v}.$$

In summary, we get the following formula.

Theorem 5.1 *For ρ and c as above, we have*

$$CS_c([\rho]) := CS_{[c]}([\rho]) = \sum_{v \in T} \mathrm{inv}_v(\rho_v^*(\alpha) \cup \psi_v), \tag{5.1}$$

where $\psi_v = \gamma_{+,v} - \gamma_{-,v} \in Z^1(\pi_v, \mathbb{Z}/n\mathbb{Z}) = H^1(\pi_v, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\pi_v, \mathbb{Z}/n\mathbb{Z})$.

So, to evaluate the arithmetic Chern–Simons action, we need to study

- a trivialisation of certain pullback of a 2-cocycle ϵ, and
- the local invariant of a cup product of two characters on π_v.

In the following two subsections, we will see how this idea can be realised.

5.2 Trivialisation of a Pullback of ϵ

As before, let $\epsilon \in Z^2(A, \mathbb{Z}/n\mathbb{Z})$ denote a 2-cocycle representing an extension

$$\begin{tikzcd} E\,:\, 0 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \Gamma \arrow[r, "\varphi"'] & A \arrow[l, bend right, dashed, "\sigma"'] \arrow[r] & 1 \end{tikzcd}$$

with a section σ such that $\sigma(e_A) = e_\Gamma$.

Suppose that we have the following commutative diagram of group homomorphisms:

$$\begin{tikzcd} & \mathrm{Ker}(f) \arrow[r, hook] \arrow[dl, dashed, "\tilde{f}|_{\mathrm{Ker}(f)}"'] & \widetilde{A} \arrow[dl, "\tilde{f}"'] \arrow[d, "f"] \\ \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & \Gamma \arrow[r, "\varphi"'] & A. \end{tikzcd} \qquad (\star)$$

Then, we can easily trivialise $f^*(\epsilon) \in Z^2(\widetilde{A}, \mathbb{Z}/n\mathbb{Z})$ using the following lemma.

Lemma 5.2 *For any $g \in \widetilde{A}$, let*

$$\gamma(g) := \sigma(f(g)) \cdot \tilde{f}(g)^{-1}.$$

Then, $\gamma(g) \in \mathrm{Ker}(\varphi) = \mathbb{Z}/n\mathbb{Z}$ and $d\gamma = f^*(\epsilon) \in Z^2(\widetilde{A}, \mathbb{Z}/n\mathbb{Z})$. Furthermore, we have $\gamma(e_{\widetilde{A}}) = 0$ and $\gamma(g \cdot h) = \gamma(g) + \gamma(h)$ for any $g, h \in \mathrm{Ker}(f)$.

Proof First, we note that $\gamma(g) \in \mathrm{Ker}(\varphi)$ because $\varphi \circ \sigma$ is the identity and $\varphi \circ \tilde{f} = f$. By definition and the fact that $\mathrm{Ker}(\varphi)$ is in the center of Γ,

$$\begin{aligned} d\gamma(x, y) &= \gamma(y) \cdot \gamma(xy)^{-1} \cdot \gamma(x) = \gamma(y) \cdot \gamma(x) \cdot \gamma(xy)^{-1} \\ &= \{\sigma(f(y)) \cdot \tilde{f}(y)^{-1}\} \cdot \{\sigma(f(x)) \cdot \tilde{f}(x)^{-1}\} \cdot \{\sigma(f(xy)) \cdot \tilde{f}(xy)^{-1}\}^{-1} \\ &= \{\sigma(f(y)) \cdot \tilde{f}(y)^{-1}\} \cdot \sigma(f(x)) \cdot \tilde{f}(x)^{-1} \cdot \tilde{f}(x) \cdot \tilde{f}(y) \cdot \sigma(f(xy))^{-1} \\ &= \sigma(f(x)) \cdot \{\sigma(f(y)) \cdot \tilde{f}(y)^{-1}\} \cdot \tilde{f}(y) \cdot \sigma(f(xy))^{-1} \\ &= \sigma(f(x)) \cdot \sigma(f(y)) \cdot \sigma(f(x \cdot y))^{-1} \\ &= f^*(\epsilon)(x, y). \end{aligned}$$

Therefore the first claim follows. Also, $\gamma(e_{\widetilde{A}}) = 0$ because $\sigma(f(e_{\widetilde{A}})) = \sigma(e_A) = e_\Gamma$ and $\widetilde{f}(e_{\widetilde{A}}) = e_\Gamma$. Finally, for any $g \in \mathrm{Ker}(f)$, $\gamma(g) = -\widetilde{f}(g)$, so it is a homomorphism because $\widetilde{f}$ is a homomorphism and the image of $\widetilde{f}|_{\mathrm{Ker}(f)}$, which is contained in $\mathbb{Z}/n\mathbb{Z}$, is abelian.

Remark 5.3 In Diagram ($\star$), we can take $\widetilde{A} = \Gamma$, $f = \varphi$ and $\widetilde{f}$ is the identity. For the rest of this section, we always fix such a choice.

5.3 Local Invariant Computation

In this subsection, we investigate several conditions to ensure

$$\mathrm{inv}_v(\phi \cup \psi) \neq 0 \in \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

where $\phi \in H^1(\pi_v, \mu_n)$=$\mathrm{Hom}(\pi_v, \mu_n)$ and $\psi \in Z^1(\pi_v, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\pi_v, \mathbb{Z}/n\mathbb{Z})$.

Lemma 5.4 *Suppose that ϕ is unramified, i.e., ϕ factors through π_v/I_v. Then,*

$$\mathrm{inv}_v(\phi \cup \psi) = 0$$

if one of the following holds.

1. $\phi = 1$, *the trivial character.*
2. ψ *is unramified.*

Proof If $\phi = 1$, then $\phi \cup \psi = 0 \in H^2(\pi_v, \mu_n)$. Thus, $\mathrm{inv}_v(\phi \cup \psi) = 0$. Also, if ψ is unramified, then $\phi \cup \psi$ arises from $H^2(\pi_v/I_v, \mu_n)$ by inflation, which is 0. Therefore, $\phi \cup \psi = 0 \in H^2(\pi_v, \mu_n)$ and the result follows.

If v does not divide n, then we can prove more.

Lemma 5.5 *Assume that v does not divide n. And assume that ϕ is an unramified generator of* $\mathrm{Hom}(\pi_v, \mu_n)$*, i.e., a generator of* $\mathrm{Hom}(\pi_v/I_v, \mu_n)$*. Then,*

$$\mathrm{inv}_v(\phi \cup \psi) \neq 0 \Longleftrightarrow \psi \textit{ is ramified.}$$

Proof Using a fixed primitive nth root ζ of unity, we fix an isomorphism

$$\begin{aligned} \eta : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mu_n \\ a &\longmapsto \zeta^a \end{aligned}$$

and using η, we get natural isomorphisms

$$\begin{tikzcd}
\mathrm{Hom}(\pi_v, \frac{1}{n}\mathbb{Z}/\mathbb{Z}) & \mathrm{Hom}(\pi_v, \mathbb{Z}/n\mathbb{Z}) \arrow[l, "\frac{1}{n}\cdot(-)"'] \arrow[r, bend left, "\eta\circ(-)"] & \mathrm{Hom}(\pi_v, \mu_n). \arrow[l, bend left, "\eta^{-1}\circ(-)"]
\end{tikzcd}$$

In this proof, we will regard ϕ as an element of $\mathrm{Hom}(\pi_v, \frac{1}{n}\mathbb{Z}/\mathbb{Z})$ and ψ as one of $\mathrm{Hom}(\pi_v, \mu_n)$ using the above isomorphisms.

If ψ is unramified, $\mathrm{inv}_v(\phi \cup \psi) = 0$ by the above lemma. Since $\mu_n \subset F_v$, by the Kummer theory we can find an element $a \in F_v^*$ such that $\delta(a) = \psi$, where $\delta : F_v^*/(F_v^*)^n \simeq H^1(\pi_v,\ \mu_n) = \mathrm{Hom}(\pi_v, \mu_n)$. Let

$$\mathrm{ord}_v : F_v^* \longrightarrow \mathbb{Z}$$

be the normalized valuation on F_v^* that sends a uniformiser ϖ of $\mathcal{O}_{F_v}$ to 1. Then,

$$\psi \text{ is ramified} \iff \mathrm{ord}_v(a) \not\equiv 0 \pmod{n}.$$

Since ϕ is an unramified[7] generator, $\phi(\mathrm{Frob}) = \frac{t}{n}$ for some $t \in (\mathbb{Z}/n\mathbb{Z})^\times$, where Frob is a lift of the Frobenius in π_v/I_v to π_v. Then,

$$\mathrm{inv}_v(\phi \cup \psi) = \mathrm{inv}_v(\phi \cup \delta(a)) = \phi(\mathrm{Frob}^{\mathrm{ord}_v(a)}) = \frac{t \cdot \mathrm{ord}_v(a)}{n}.$$

Combining the above two results, we obtain

$$\psi \text{ is ramified} \iff \mathrm{inv}_v(\phi \cup \psi) \neq 0$$

as desired.

Remark 5.6 When $n = 2$, the above lemmas are enough for the computation of local invariants.

5.4 Construction of Examples

From now on, we assume that $n = 2$.

As a corollary of Sect. 5.2, if we have the following commutative diagrams

[7] This is where our assumption that $v \nmid n$ is used.

$$\begin{tikzcd}
\pi_T \arrow[r, two heads, "\widetilde{\rho_+}"] \arrow[d, two heads, "\kappa_T"'] \arrow[dr, "\rho_+"] & \Gamma \arrow[d, two heads, "\varphi"] \\
\pi \arrow[r, two heads, "\rho"'] & A
\end{tikzcd} \quad \text{and} \quad \begin{tikzcd}
\pi_v \arrow[r, two heads, "\widetilde{\rho_v}"] \arrow[d, "\kappa_v"'] \arrow[dr, "\rho_v"] & \Gamma \arrow[d, two heads, "\varphi"] \\
\pi \arrow[r, two heads, "\rho"'] & A,
\end{tikzcd} \qquad (\star\star)$$

then we get

$$\gamma_+ = (\widetilde{\rho_+})^*(\gamma) \quad \text{and} \quad \gamma_{-,v} = (\widetilde{\rho_v})^*(\gamma).$$

Thus we can explicitly compute $CS_c([\rho])$ using the previous strategy when we are in the following situation:

Assumption 5.7

1. F is a totally imaginary field.
2. $c = \alpha \cup \epsilon$ with $\alpha : A \to \mu_2$ surjective, and ϵ representing an extension

$$E : 0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \Gamma \longrightarrow A \longrightarrow 1.$$

3. There are Galois extensions of F:

$$F \subset F^{\alpha} \subset F^{\text{ur}} \subset F^{+}$$

such that

- $\text{Gal}(F^{\text{ur}}/F)$ is isomorphic to A and F^{ur}/F is unramified everywhere.
- $\text{Gal}(F^{+}/F)$ is isomorphic to Γ and F^{+}/F is unramified at the primes above 2.
- F^{α} is the fixed field of the kernel of the composition

$$\text{Gal}(F^{\text{ur}}/F) \xrightarrow{\sim} A \xrightarrow{\alpha} \mu_2$$

and hence we get a commutative diagram

$$\begin{tikzcd}
 & A \arrow[dr, bend left=15] \arrow[drr, bend left=20, "\alpha"] & & \\
\pi \arrow[ur, two heads, "\rho"] \arrow[r, two heads] & \text{Gal}(F^{\text{ur}}/F) \arrow[u, "\simeq"'] \arrow[r, two heads] & \text{Gal}(F^{\alpha}/F) \arrow[r, "\simeq"] & \mu_2.
\end{tikzcd}$$

Suppose we are in the above assumption. Let S be the set of primes of O_F ramified in F^{+}, and S_2 the set of primes of O_F dividing 2. Then by our assumption, $S \cap S_2 = \emptyset$. Let $T = S \cup S_2$. Then, we can find a global trivialisation γ_+ of $\rho_T^*(\epsilon)$ from the following commutative diagram

$$\begin{tikzcd}
 & \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Ker}(\phi) = \mathrm{Gal}(F^+/F^{\mathrm{ur}}) \arrow[r] \arrow[dl, dashed, "\widetilde{\phi}|_{\mathrm{Ker}(\phi)}=\mathrm{Id}"'] & \mathrm{Gal}(F^+/F) \arrow[d, two heads, "\phi"] \arrow[dl, "\widetilde{\phi}=\mathrm{Id}"'] \\
\mathbb{Z}/2\mathbb{Z} \arrow[r] & \Gamma \simeq \mathrm{Gal}(F^+/F) \arrow[r, two heads] & A \simeq \mathrm{Gal}(F^{\mathrm{ur}}/F).
\end{tikzcd}$$

For each $v \in T$, let $D(v)$ be the decomposition group of $\mathrm{Gal}(F^+/F)$ at v. In other words,

$$D(v) = \{g \in \mathrm{Gal}(F^+/F) : gv = v\} \simeq \mathrm{Gal}(F^+_\nu/F_v),$$

where ν is a prime of F^+ lying above v. And let $I(v)$ be the inertia subgroup of $D(v)$. Then, $I(v) = 0$ if and only if v divides 2. Thus,

$$\gamma_{+,v} \text{ is unramified} \Longleftrightarrow v \in S_2.$$

Since $\psi_v := \gamma_{+,v} - \gamma_{-,v}$ and we always take $\gamma_{-,v}$ unramified,

$$\psi_v \text{ is unramified} \Longleftrightarrow v \in S_2.$$

Furthermore,

$$\rho_v^*(\alpha) \text{ is trivial} \Longleftrightarrow f(D(v)) = 0,$$

where f is the natural projection from $\mathrm{Gal}(F^+/F)$ to $\mathrm{Gal}(F^\alpha/F)$. And $f(D(v)) = 0$ exactly occurs when v splits in F^α. Note that $\rho_v^*(\alpha)$ is always an unramified generator of $\mathrm{Hom}(\pi_v, \mu_2)$ if it is not trivial.

Now we are ready to compute the arithmetic Chern–Simons invariants.

Theorem 5.8 *Suppose we are in Assumption 5.7. Then,*

$$CS_c([\rho]) = \sum_{v \in T} \mathrm{inv}_v(\rho_v^*(\alpha) \cup \psi_v) = \frac{r}{2} \mod \mathbb{Z},$$

where $\psi_v = \gamma_{+,v} - \gamma_{-,v}$ and r is the number of primes in S which are inert in F^α.

Proof The first equality follows from Theorem 5.1. Thus, it suffices to compute $\mathrm{inv}_v(\rho_v^*(\alpha) \cup \psi_v)$ for $v \in T$. By Lemma 5.4, $\mathrm{inv}_v(\rho_v^*(\alpha) \cup \psi_v) = 0$ if either $\rho_v^*(\alpha)$ is trivial or ψ_v is unramified. By the above discussion, $\rho_v^*(\alpha)$ is trivial if and only if $f(D(v)) = 0$, i.e., v splits in F^α; and ψ_v is unramified if and only if $v \in S_2$. Furthermore, if $\rho_v^*(\alpha)$ is not trivial and ψ_v is ramified, then by Lemma 5.5, $\mathrm{inv}_v(\rho_v^*(\alpha) \cup \psi_v) = \frac{1}{2}$. Thus the result follows.

Therefore to provide an example of calculation of the arithmetic Chern–Simons invariants, it suffices to construct a tower of fields satisfying Assumption 5.7, which is essentially the embedding problem in the inverse Galois theory. Instead, we will consider the similar problems over $\mathbb{Q}$, which are much easier to solve (or find from the table). Then, we will construct a tower satisfying Assumption 5.7 from a tower of fields over $\mathbb{Q}$.

Assumption 5.9 Suppose we have a number field L with its subfield K such that

1. $\mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma$.
2. d_L, the (absolute) discriminant of L, is an odd integer.[8]
3. $\mathrm{Gal}(K/\mathbb{Q}) \simeq A$.
4. $\mathbb{Q}(\sqrt{D})$ is a quadratic subfield of K, where D is a divisor of d_K.[9]
5. $K/\mathbb{Q}(\sqrt{D})$ is unramified at any finite primes.

Then, we have the following.

Proposition 5.10 *Let $F = \mathbb{Q}(\sqrt{-|D| \cdot t})$ be an imaginary quadratic field, where t is a positive squarefree integer prime to D so that $F \cap L = \mathbb{Q}$. Then, there is a tower of fields $F \subset F^{\mathrm{ur}} \subset F^{+}$ satisfies Assumption 5.7. In fact, we can take*

$$F^{\mathrm{ur}} = KF \quad \textit{and} \quad F^{+} = LF.$$

Proof First, it is clear that F is totally imaginary. Next, since $F \cap L = \mathbb{Q}$

$$\mathrm{Gal}(LF/F) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma \quad \text{and} \quad \mathrm{Gal}(KF/F) \simeq \mathrm{Gal}(K/\mathbb{Q}) \simeq A.$$

Since the discriminant of L is odd, L/K is unramified at the primes above 2, and so is LF/KF. Finally, it suffices to show that KF/F is unramified everywhere. Since $K/\mathbb{Q}(\sqrt{D})$ is unramified everywhere, $K/\mathbb{Q}$ is only ramified at the primes dividing D. (Note that the discriminant of K is odd, hence it is unramified at 2.) Moreover, the ramification degree of any prime divisor p of D is 2, and the same is true for $F/\mathbb{Q}$. Since p is odd, KF/F is unramified at the primes above p by Abhyankar's lemma [5, Theorem 1], which implies our claim.

Remark 5.11 Since the ramification indices of any prime divisor p of D are 2 in both $F/\mathbb{Q}$ and $K/\mathbb{Q}$, we can use Abhyankar's lemma in both directions. (Note that our assumption implies that D is odd.) In other words, KF/K is always unramified at the primes dividing D.

The remaining part to check Assumption 5.7 is the choice of F^{α}. Let

$$B := \{F_1, \ldots, F_m\}$$

be the set of quadratic subfields of F^{ur}. Then, there is one-to-one correspondence between the set of surjective homomorphisms $\mathrm{Gal}(F^{\mathrm{ur}}/F) \to \mu_2$ and B. Therefore

[8] We may consider when d_L is even. Then later, it is not clear that FL/FK is unramified at the primes above 2. Some choices of t (for F) can make it ramified. Then, it is hard to determine the value of local invariants unless 2 splits in F^{α}/F.

[9] Here, we always take that d_K is odd because we cannot use Abhyankar's lemma when $p = 2$, and hence we may not remove ramification in the extension FK/F at the primes above 2. In some nice situation, we may directly prove that $F(\sqrt{D})/F$ is unramified at the primes above 2 even though D is even. If so, our assumption on d_K can be removed.

$m = \#\mathrm{Hom}(A, \mu_2) - 1$ and we can define $\alpha_i : A \to \mu_2$ so that $F^{\alpha_i} = F_i$ due to the (chosen) isomorphism $\mathrm{Gal}(F^{\mathrm{ur}}/F) \simeq A$.

Now, suppose $F^\alpha = F(\sqrt{M}) \subset F^{\mathrm{ur}}$ for some divisor M of D. Let $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{M})$ and $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{N})$, where $N = (-|D| \cdot t)/M$. Then, we have the following commutative diagram:

$$\begin{tikzcd}
 & F^\alpha = F(\sqrt{M}) = F(\sqrt{N}) \arrow[dl, dash] \arrow[d, dash, "\text{unramified}"] \arrow[dr, dash] & \\
\mathbb{Q}_1 = \mathbb{Q}(\sqrt{M}) \arrow[dr, dash] & F = \mathbb{Q}(\sqrt{MN}) \arrow[d, dash] & \mathbb{Q}_2 = \mathbb{Q}(\sqrt{N}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

For a prime p, let $\wp$ denote a prime of O_F lying above p. We want to understand the splitting behaviour of $\wp$ in F^α.

Lemma 5.12 *Let p be an odd prime.*

1. *Assume that p divides Dt. Then*

$$\wp \text{ is inert in } F^\alpha \iff p \text{ is inert either in } \mathbb{Q}_1 \text{ or in } \mathbb{Q}_2.$$

2. *If p is inert in F, then $\wp$ always splits in F^α.*
3. *Assume that p splits in F. Then*

$$\wp \text{ splits in } F^\alpha \iff p \text{ splits in } \mathbb{Q}_1.$$

Proof

1. In this case, p is ramified in F, and p is ramified either in $\mathbb{Q}_1$ or in $\mathbb{Q}_2$. Without loss of generality, let p is ramified in $\mathbb{Q}_2$. Then, $\wp$ is inert in F^α if and only if p is inert in $\mathbb{Q}_1$ from the above commutative diagram.
2. Let $\left(\frac{a}{b}\right)$ denote the Legendre symbol. If p is inert in F, then $\left(\frac{MN}{p}\right) = -1$. Therefore either $\left(\frac{M}{p}\right) = 1$ or $\left(\frac{N}{p}\right) = 1$. Without loss of generality, let $\left(\frac{M}{p}\right) = 1$ and $\left(\frac{N}{p}\right) = -1$. Then, p splits in $\mathbb{Q}_1$ and hence there are at least two primes in F^α above p. Since $\wp$ is the unique prime of F above p, $\wp$ splits in F^α.
3. Since $\left(\frac{MN}{p}\right) = 1$, either $\left(\frac{M}{p}\right) = \left(\frac{N}{p}\right) = 1$ or $\left(\frac{M}{p}\right) = \left(\frac{N}{p}\right) = -1$. If $\left(\frac{M}{p}\right) = -1$, then there is only one prime in $\mathbb{Q}_1$ above p. Thus, there are at most two primes in F^α above p. Since p already splits in F, $\wp$ is inert in F^α. On the other hand, if $\left(\frac{M}{p}\right) = 1$, then p splits completely in F^α because p splits completely both in $\mathbb{Q}_1$ and F. Thus, $\wp$ splits in F^α.

Let $D_L = d_L/d_K^2$ be the norm (to $\mathbb{Q}$) of the relative discriminant of L/K. Then, L/K is precisely ramified at the primes dividing D_L, and hence

$$S \subset \{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F) : \mathfrak{p} \mid D_L\}.$$

(Note that S is the set of primes in $\mathcal{O}_F$ that ramify in F^+.) Let s be the number of prime divisors of (D_L, D), which are inert either in $\mathbb{Q}_1$ or in $\mathbb{Q}_2$. Then, we have the following.

Theorem 5.13 *Assume that we have ρ and c as above. Then,*

$$CS_c([\rho]) \equiv \frac{s}{2} \pmod{\mathbb{Z}}.$$

Proof First, we show that

$$S = \{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F) : \mathfrak{p} \mid D_L \;\text{ but }\; \mathfrak{p} \nmid t\}.$$

For a prime divisor p of D_L which does not divide t, we show that KF/K is unramified at any primes above p, which implies that LF/KF is ramified at the primes above p. If p does not divide D, then this is done because p is unramified in F. On the other hand, if p divides D, KF/K is unramified at the primes above p by Remark 5.11. Now, assume that p divides (D_L, t), and let $\wp$ be a prime of $\mathcal{O}_K$ lying above p. Then, $\wp$ is ramified both in L/K and in KF/K. (Note that since $(t, D) = 1$, $K/\mathbb{Q}$ is unramified at p but $F/\mathbb{Q}$ is ramified at p.) Therefore by the same argument as in Remark 5.11, LF/KF is unramified at the primes above p, which proves the above claim.

Next, by Theorem 5.8 it suffices to compute the number of primes in S which are inert in F^α. Let $\wp \in S$ be a prime above an odd prime p. Assume that p does not divide D. (Then p is unramified in F.) If p is inert in F, then $\wp$ always splits in F^α by Lemma 5.12. If p splits in F and $p\mathcal{O}_F = \wp \cdot \wp'$, then $\wp$ is inert (in F^α) if and only if $\wp'$ is inert. Therefore to compute the invariant, the contribution from such split primes can be ignored. So, we may assume that p divides D. Then, there is exactly one (ramified) prime $\wp$ in $\mathcal{O}_F$ above p, and our claim follows from Lemma 5.12.

We remark that the computation of s is completely easy because $\mathbb{Q}_1/\mathbb{Q}$ and $\mathbb{Q}_2/\mathbb{Q}$ are just quadratic fields. And this also illustrates that we only need information on the primes dividing (D_L, D) for the computation.

5.5 Case 1: Cyclic Group

Let $A = \mathbb{Z}/2\mathbb{Z}$, and $\Gamma = \mathbb{Z}/4\mathbb{Z}$. Then, we can easily find Galois extensions $L/K/\mathbb{Q}$ in Assumption 5.9 by the theory of cyclotomic fields.

Let p be a prime congruent to 1 modulo 4. Then, we can take L as the degree 4 subfield of $\mathbb{Q}(\mu_p)$, and $K = \mathbb{Q}(\sqrt{p})$. Moreover, $d_L = p^3$ and $d_K = p$.

Let $F = \mathbb{Q}(\sqrt{-p \cdot t})$, where t is a positive squarefree integer prime to p. (Then, $F \cap L = \mathbb{Q}$.)

Proposition 5.14 *Let ρ and c be chosen so that $F^{\alpha} = F^{\mathrm{ur}} = FK$ and $F^{+} = FL$. Then,*

$$CS_c([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{p}\right) = -1.$$

Proof By Theorem 5.13, it suffices to check whether p is inert in $\mathbb{Q}(\sqrt{-t})$. If it is inert, then $CS_c([\rho]) = \frac{1}{2}$, and 0 otherwise. Since $p \equiv 1 \pmod 4$, the result follows.

5.6 Case 2: Non-cyclic Abelian Group

Let $A = V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein four group, and $\Gamma = \mathcal{Q}_8 = \mathcal{Q}$, the quaternion group. To find Galois extensions $L/K/\mathbb{Q}$ in Assumption 5.9, we first study quaternion extensions of $\mathbb{Q}$ in general.

Proposition 5.15 *Let $L/\mathbb{Q}$ be a Galois extension whose Galois group is isomorphic to $\mathcal{Q}$. Suppose that d_L is odd. Let K be a subfield of L with* $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z}$. *Then,*

1. *$K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ for some positive squarefree d_1 and d_2.*
2. *$d_1 \equiv d_2 \equiv 1 \pmod 4$.*
3. *Let p be a prime divisor of $d_1 d_2$. Then, p divides $D_L := d_L/d_K^2$.*

Proof Since K is a subfield of L, d_K is also odd. And since $\mathcal{Q}$ has a unique subgroup of order 2, which is normal, $K/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Therefore $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, where d_1 and d_2 are products of prime discriminants. If L is totally real, then K must be totally real as well. If L is not totally real, then the complex conjugation generates a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ of order 2. Since $\mathcal{Q}$ has a unique subgroup of order 2, K must be a fixed field of the complex conjugation, which implies that K is totally real. So, d_1 and d_2 can be taken as positive squarefree integers. Moreover, since they are products of prime discriminants and odd, $d_1 \equiv d_2 \equiv 1 \pmod 4$.

Finally, let p be a prime divisor of d_1, which does not divide d_2. Note that $\mathbb{Q}(\sqrt{d_1}) \subset K \subset L$ and $L/\mathbb{Q}(\sqrt{d_1})$ is a cyclic extension of degree 4. Since p does not divide d_2, $\mathbb{Q}(\sqrt{d_2})/\mathbb{Q}$ is unramified at p and hence $K/\mathbb{Q}(\sqrt{d_2})$ is ramified at the primes dividing p. By [19, Corollary 3], L/K is ramified at the primes above p and hence p divides D_L. By the same argument, the claim follows when p is a divisor of d_2, which does not divide d_1. Let p be a prime divisor of (d_1, d_2). Then, since $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_1 d_2}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{\frac{d_1 d_2}{p^2}})$ and p does not divide $\frac{d_1 d_2}{p^2}$, the result follows by the same argument as above.

Now, let d_1 and d_2 be two squarefree positive integers such that

- $d_1 \equiv d_2 \equiv 1 \pmod 4$.
- $(d_1, d_2) = 1$.[10]

[10] This is not a vacuous condition. In fact, there is a $\mathcal{Q}$-extension L containing $\mathbb{Q}(\sqrt{21}, \sqrt{33})$ [35].

Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Suppose that there is a number field L such that

- $L/\mathbb{Q}$ is Galois and $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{Q}$.
- L contains K and the discriminant d_L of L is odd.

Let $F = \mathbb{Q}(\sqrt{-d_1 d_2 \cdot t})$, where t is a positive squarefree integer prime to $d_1 d_2$. Then $L \cap F = \mathbb{Q}$ because all quadratic subfields of L are contained in K, which is totally real. Since $\mathrm{Hom}(A, \mu_2)$ is of order 4, there are three quadratic subfield of FK over F:

$$F_1 := F(\sqrt{d_1}),\ \ F_2 := F(\sqrt{d_2}), \text{and } F_3 := F(\sqrt{d_1 d_2}) = F(\sqrt{-t}).$$

Proposition 5.16 *Let ρ and $c_i = \alpha_i \cup \epsilon$ be chosen so that $F^{\alpha_i} = F_i$, $F^{\mathrm{ur}} = FK$ and $F^{+} = FL$. Then,*

$$CS_{c_1}([\rho]) = \frac{1}{2} \iff \prod_{p|d_1} \left(\frac{-d_2 \cdot t}{p}\right) \times \prod_{p|d_2} \left(\frac{d_1}{p}\right) = -1.$$

$$CS_{c_2}([\rho]) = \frac{1}{2} \iff \prod_{p|d_1} \left(\frac{d_2}{p}\right) \times \prod_{p|d_2} \left(\frac{-d_1 \cdot t}{p}\right) = -1.$$

$$CS_{c_3}([\rho]) = \frac{1}{2} \iff \prod_{p|d_1 d_2} \left(\frac{-t}{p}\right) = -1.$$

Proof By the above lemma and Theorem 5.13, it suffices to compute the number of prime divisors of $d_1 d_2$, which are inert in $\mathbb{Q}_1$ or in $\mathbb{Q}_2$.

First, compute $CS_{c_1}([\rho])$. In this case, $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{-d_2 \cdot t})$. If p is a divisor of d_1, it is inert in $\mathbb{Q}_2$ if and only if

$$\left(\frac{-d_2 \cdot t}{p}\right) = -1.$$

Therefore, the number of such prime divisors of d_1 is odd if and only if

$$\prod_{p|d_1} \left(\frac{-d_2 \cdot t}{p}\right) = -1.$$

Similarly, the number of prime divisors of d_2, which are inert in $\mathbb{Q}_1$, is odd if and only if

$$\prod_{p|d_2} \left(\frac{d_1}{p}\right) = -1.$$

Thus, we have

$$CS_{c_1}([\rho]) = \frac{1}{2} \iff \prod_{p|d_1} \left(\frac{-d_2 \cdot t}{p}\right) \times \prod_{p|d_2} \left(\frac{d_1}{p}\right) = -1.$$

The remaining two cases can easily be done by the same method as above.

We can find Galois extensions $L/K/\mathbb{Q}$ satisfying the above assumptions from the database. Here, we take $L/K/\mathbb{Q}$ from the LMFDB [36] as follows. Let

$$g(x) = x^8 - x^7 + 98x^6 - 105x^5 + 3191x^4 + 1665x^3 + 44072x^2 + 47933x + 328171$$

be an irreducible polynomial over $\mathbb{Q}$, and β be a root of $g(x)$. Let

$$L = \mathbb{Q}(\beta) \quad \text{and} \quad K = \mathbb{Q}(\sqrt{5}, \sqrt{29}).$$

So, $d_1 = 5$ and $d_2 = 29$. Moreover, $D_L = 3^2 \cdot 5^2 \cdot 29^2$.

Let $F = \mathbb{Q}(\sqrt{-5 \cdot 29 \cdot t})$, where t is a positive squarefree integer prime to $5 \cdot 29$.

Corollary 5.17 *Let ρ and $c_i = \alpha_i \cup \epsilon$ be chosen as above. Then,*

$$CS_{c_1}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{5}\right) = -1 \Longleftrightarrow t \equiv \pm 2 \pmod 5.$$

$$CS_{c_2}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{29}\right) = -1.$$

$$CS_{c_3}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{5}\right) = -\left(\frac{t}{29}\right).$$

Now, we provide another example. Let $L/K/\mathbb{Q}$ from the the LMFDB [37] as follows. Let

$$g(x) = x^8 - x^7 - 34x^6 + 29x^5 + 361x^4 - 305x^3 - 1090x^2 + 1345x - 395$$

be an irreducible polynomial over $\mathbb{Q}$, and β be a root of $g(x)$. Let

$$L = \mathbb{Q}(\beta) \quad \text{and} \quad K = \mathbb{Q}(\sqrt{5}, \sqrt{21}).$$

So, $d_1 = 5$ and $d_2 = 21$. Moreover, $D_L = 3^2 \cdot 5^2 \cdot 7^2$.

Let $F = \mathbb{Q}(\sqrt{-105 \cdot t})$, where t is a positive squarefree integer prime to 105.

Corollary 5.18 *Let ρ and $c_i = \alpha_i \cup \epsilon$ be chosen as above. Then,*

$$CS_{c_1}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{5}\right) = -1 \Longleftrightarrow t \equiv \pm 2 \pmod 5.$$

$$CS_{c_2}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{3}\right) = -\left(\frac{t}{7}\right) \Longleftrightarrow 2, 8, 10, 11, 13, 19 \pmod{21}.$$

$$CS_{c_3}([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{t}{3}\right) \cdot \left(\frac{t}{5}\right) \cdot \left(\frac{t}{7}\right) = -1.$$

Now, we take $A = V_4$, but $\Gamma = D_4$, the dihedral group of order 8. We found $L/K/\mathbb{Q}$ from the LMFDB [38] as follows. Let

$$g(x) = x^8 - 3x^7 + 4x^6 - 3x^5 + 3x^4 - 3x^3 + 4x^2 - 3x + 1$$

be an irreducible polynomial over $\mathbb{Q}$, and β be a root of $g(x)$. Let

$$L = \mathbb{Q}(\beta) \quad \text{and} \quad K = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}).$$

If we take $D = 21$, then this choice satisfies Assumption 5.9. Moreover, $d_L = 3^6 \cdot 7^4$ and $d_K = 3^2 \cdot 7^2$.

Let $F = \mathbb{Q}(\sqrt{-21 \cdot t})$, where t is a positive squarefree integer prime to 21. (Then, $F \cap L = \mathbb{Q}$ because all imaginary quadratic subfields of L are $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$.) Since $\mathrm{Hom}(A, \mu_2)$ is of order 4, there are three quadratic subfield of FK over F:

$$F_1 := F(\sqrt{-3}),\ \ F_2 := F(\sqrt{-7}), \text{and } F_3 := F(\sqrt{21}).$$

Proposition 5.19 *Let ρ and $c_i = \alpha_i \cup \epsilon$ be chosen so that $F^{\alpha_i} = F_i$, $F^{\mathrm{ur}} = FK$ and $F^+ = FL$. Then,*

$$\begin{aligned} CS_{c_1}([\rho]) &= \frac{1}{2} \Longleftrightarrow \left(\frac{t}{3}\right) = -1 \Longleftrightarrow t \equiv 2 \pmod 3. \\ CS_{c_2}([\rho]) &= \frac{1}{2} \qquad \textit{for all } t. \\ CS_{c_3}([\rho]) &= \frac{1}{2} \Longleftrightarrow \left(\frac{t}{3}\right) = 1 \Longleftrightarrow t \equiv 1 \pmod 3. \end{aligned}$$

Proof Since $D_L = 3^2$, the result follows from Theorem 5.13.

5.7 Case 3: Non-abelian Group

Let $A = S_4$, the symmetric group of degree 4. Then, $H^1(A, \mu_2) \simeq \mathbb{Z}/2\mathbb{Z}$ and $H^2(A, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, there is a unique surjective map $\alpha : A \twoheadrightarrow \mu_2$ and three non-trivial central extensions Γ_i of A by $\mathbb{Z}/2\mathbb{Z}$:

- $\Gamma_1 = 2^+S_4 \simeq \mathrm{GL}(2, \mathbb{F}_3)$, the general linear group of degree 2 over $\mathbb{F}_3$.
- $\Gamma_2 = 2^-S_4$, the transitive group '$16T65$' in [33].
- $\Gamma_3 = 2^{\det}S_4$, corresponding to the cup product of the signature with itself.

Let ϵ_i be a cocycle representing the extension

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & \Gamma_i \arrow[r] & A = S_4 \arrow[r] & 0. \end{tikzcd}$$

In this subsection, we will consider the first two cases. There are another descriptions of the groups Γ_1 and Γ_2. Let

$$\mathcal{E} : 1 \longrightarrow \mathrm{SL}(2, \mathbb{F}_3) \longrightarrow \Gamma \longrightarrow \mathbb{F}_3^\times \simeq \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

If $\mathcal{E}$ splits, then $\Gamma \simeq \Gamma_1$, otherwise $\Gamma \simeq \Gamma_2$.

Let $c = \alpha \cup \epsilon_1$. (So, $\Gamma = \Gamma_1$.) Suppose $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D}) \subset K \subset L$ is a tower of fields satisfying Assumption 5.9. Let $F = \mathbb{Q}(\sqrt{-|D| \cdot t})$, where t is a squarefree integer prime to D and greater than 1. Then, $F \cap L = F \cap \mathbb{Q}(\sqrt{D}) = \mathbb{Q}$. (The first equality holds because Γ has a unique subgroup of order 24.)

Proposition 5.20 *Let ρ and c be chosen so that $F^\alpha = F(\sqrt{D})$, $F^{\mathrm{ur}} = FK$ and $F^+ = FL$. Then,*

$$CS_c([\rho]) = 0.$$

Proof Since the extension

$$\mathcal{E} : 1 \longrightarrow \mathrm{SL}(2, \mathbb{F}_3) \longrightarrow \mathrm{GL}(2, \mathbb{F}_3) \longrightarrow \mathbb{F}_3^\times \simeq \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

splits, $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/\mathbb{Q}(\sqrt{D})) \rtimes \mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$.

Let p be a prime divisor of (D_L, D). By our assumption, p is odd. Let I_p be an inertia subgroup of $\mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma = \mathrm{GL}(2, \mathbb{F}_3)$. Since L/K and $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ are ramified at p but $K/\mathbb{Q}(\sqrt{D})$ is not, the ramification index of p in $L/\mathbb{Q}$ is 4, and $I_p \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On the other hand, since p is odd, $L/\mathbb{Q}$ is tamely ramified at p and hence I_p must be cyclic, which is a contradiction. Therefore $(D_L, D) = 1$ and hence the result follows by Theorem 5.13.

We can find several examples of such towers from the LMFDB. Let

$$\begin{aligned} g_1(x) &= x^8 - 4x^7 + 7x^6 + 7x^5 - 51x^4 + 50x^3 + 61x^2 - 107x - 83 \\ g_2(x) &= x^4 - x - 1 \end{aligned}$$

be irreducible polynomials over $\mathbb{Q}$ [39, 40], and let L (resp. K) be the the splitting field of $g_1(x)$ (resp. $g_2(x)$). Then, $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{GL}(2, \mathbb{F}_3)$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_4$. Moreover, $d_L = 3^{24} \cdot 283^{24}$ and $d_K = 283^{12}$. Thus, $D = -283$ satisfies Assumption 5.9. Note that since the discriminant D of $g_2(x)$ is squarefree, $K/\mathbb{Q}(\sqrt{D})$ is unramified everywhere (cf. [12, p. 1]).

Let $F = \mathbb{Q}(\sqrt{-283 \cdot t})$, where t is a squarefree integer prime to 283, and $t > 1$.

Corollary 5.21 *Let ρ and c be chosen so that $F^\alpha = F(\sqrt{-283})$, $F^{\mathrm{ur}} = FK$ and $F^+ = FL$. Then,*

$$CS_c([\rho]) = 0.$$

Now, we consider another case. Let $c = \alpha \cup \epsilon_2$. (So, $\Gamma = \Gamma_2$.) Let L be the splitting field of

$$\begin{aligned} f(x) &= x^{16} + 5x^{15} - 790x^{14} - 4654x^{13} + 234254x^{12} + 1612152x^{11} - 33235504x^{10} \\ &- 263221982x^9 + 2331584048x^8 + 21321377994x^7 - 74566280958x^6 - 825209618478x^5 \\ &+ 922238608476x^4 + 13790070608536x^3 - 6704968288135x^2 - 80794234036917x + 87192014930816. \end{aligned}$$

Let K be the splitting field of

$$g(x) = x^4 - x^3 - 4x^2 + x + 2.$$

Then, $\mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma = \Gamma_2$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_4 = A$.[11] (See [33, 34].)

Lemma 5.22 *We have the following.*

1. $K/\mathbb{Q}(\sqrt{2777})$ *is unramified everywhere.*
2. $\mathbb{Q}(\sqrt{2777})$ *is a unique quadratic subfield of* L.
3. $\mathbb{Q}(\sqrt{2777}) \subset K \subset L$.
4. D_L *is a multiple of* 2777, *i.e.,* L/K *is ramified at the primes above* 2777.

Proof For simplicity, let $E := \mathbb{Q}(\sqrt{2777})$ and $p = 2777$.

1. Since S_4 has a unique subgroup of order 12, K has a unique quadratic subfield K'. Since the discriminant of $g(x)$ is p, a prime, $K' = E$ and K/E is unramified everywhere (cf. [12, p. 1]).
2. Let β_i be the roots of $f(x)$. Then, $L = \cup\, \mathbb{Q}(\beta_i)$. Since the discriminant of the field $\mathbb{Q}[x]/(f(x))$ is p^{12}, $\mathbb{Q}(\beta_i)$ contains E, and so does L. On the other hand, since Γ has also a unique subgroup of order 24, E is a unique quadratic subfield of L.
3. Since

$$f(x) \equiv (x + 1372)^4 \cdot (x + 1791)^4 \cdot (x + 1822)^4 \cdot (x + 2653)^4 \pmod{p},$$

the ramification index of p in $\mathbb{Q}(\beta_i)/\mathbb{Q}$ is 4. Since $L = \cup\, \mathbb{Q}(\beta_i)$ and p is odd, the ramification index of p in $L/\mathbb{Q}$ is 4 by Abhyankar's lemma. Since $L/\mathbb{Q}$ is tamely ramified at p, the inertia subgroup I_p of $\mathrm{Gal}(L/\mathbb{Q}) \simeq \Gamma$ is cyclic of order 4. Since Γ has a unique subgroup C of order 2, I_p contains C. Thus, L/M is ramified at the primes above p, where M is the fixed field of C in L. Since $E/\mathbb{Q}$ is also ramified at p, M/E is unramified at the primes above p, and hence M/E is unramified everywhere.

[11] This example is provided us by Dr. Kwang–Seob Kim.

$$\begin{tikzcd}
 & L \arrow[d, dash, "\text{ramified only at the primes above } p"] \\
\text{unique } S_4\text{-subextension} \arrow[r, dash] & M \arrow[d, dash, "\text{unramified everywhere } A_4\text{-extension}"] \\
\text{unique quadratic subextension} \arrow[r, dash] & E \arrow[d, dash, "\text{ramified only at } p"] \\
 & \mathbb{Q}
\end{tikzcd}$$

Now, it suffices to show that $K = M$. Let $N = K \cap M$. Then, since K and M are Galois over E, so is N. Also since the normal subgroups of $\mathrm{Gal}(K/E) \simeq A_4 \simeq \mathrm{Gal}(M/E)$ are either $\{1\}$, V_4 or A_4,

$$\mathrm{Gal}(N/E) \simeq \text{ either } \{1\}, \mathbb{Z}/3\mathbb{Z} \text{ or } A_4.$$

Note that the class group of E is $\mathbb{Z}/3\mathbb{Z}$. Let H be the Hilbert class field of E. Then, the class group of H is V_4. (This can easily be checked because the degree of $H/\mathbb{Q}$ is small.) If $\mathrm{Gal}(N/E) \simeq \{1\}$, then E has two different degree 3 unramified extensions given by K^{V_4} and M^{V_4}, which is a contradiction. If $\mathrm{Gal}(N/E) \simeq \mathbb{Z}/3\mathbb{Z}$, then $N = H$ and N has two different unramified V_4 extensions K and M, which is a contradiction. Thus, $\mathrm{Gal}(N/E) \simeq A_4$ and hence $K = N = M$, as desired.

4. This is proved in (3).

Thus, we can take $D = 2777$. Let $F = \mathbb{Q}(\sqrt{-2777 \cdot t})$ for a positive squarefree integer t prime to 2777. Then, $F \cap L = \mathbb{Q}$ because L has a unique quadratic subfield $\mathbb{Q}(\sqrt{2777})$, which is real.

Proposition 5.23 *Let ρ and c be chosen so that $F^{\alpha} = F(\sqrt{D})$, $F^{\mathrm{ur}} = FK$ and $F^{+} = FL$. Then,*

$$CS_c([\rho]) = \frac{1}{2} \Longleftrightarrow \left(\frac{-t}{2777}\right) = \left(\frac{t}{2777}\right) = -1.$$

Proof Since $(D_L, D) = 2777$ and $F^{\alpha} = F(\sqrt{D}) = F(\sqrt{-t})$, the result follows from Theorem 5.13.

Remark 5.24 Even in the non-abelian case, we have infinite family of non-vanishing arithmetic Chern–Simons invariants!

6 Application

In this section, we give a simple arithmetic application of our computation. Namely, we show non-solvability of a certain case of the embedding problem based on our examples of non-vanishing arithmetic Chern–Simons invariants.

For an odd prime p, let $p^* = (-1)^{\frac{p-1}{2}} p$. Let

$$d_1 = \prod_{i=1}^{s} p_i^* \quad \text{and} \quad d_2 = \prod_{j=1}^{t} q_j^*,$$

where p_i, q_j are distinct odd prime numbers, and $d_1, d_2 > 0$. Let

$$A_i := \left(\frac{d_2}{p_i}\right) = \prod_{1 \leq j \leq t} \left(\frac{q_j}{p_i}\right) \quad \text{and} \quad B_j := \left(\frac{d_1}{q_j}\right) = \prod_{1 \leq i \leq s} \left(\frac{p_i}{q_j}\right).$$

Let

$$\Delta(d_1, d_2) := \prod_{1 \leq i \leq s} A_i \quad \text{and} \quad \Delta(d_2, d_1) := \prod_{1 \leq j \leq t} B_j.$$

Lemma 6.1 $\Delta(d_1, d_2) = \Delta(d_2, d_1)$.

Proof Note that $\Delta(d_1, d_2) = \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq t}} \left(\frac{p_i}{q_j}\right)$. Since d_1 is positive, the number of prime divisors of d_1 which are congruent to 3 modulo 4 is even. And the same is true for d_2. Thus by the quadratic reciprocity law,

$$A_i = \prod_{1 \leq j \leq t} \left(\frac{q_j}{p_i}\right) = \prod_{1 \leq j \leq t} \left(\frac{p_i}{q_j}\right).$$

By taking product for all $1 \leq i \leq s$, we get the result.

Recall that $\mathcal{Q}$ denotes the quaternion group.

Proposition 6.2 *Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. If $\Delta(d_1, d_2) = -1$, then there cannot exist a number field L with odd discriminant, such that* $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathcal{Q}$ *and $K \subset L$.*

A referee of an earlier version of this paper has pointed out that this result can also be obtained using the theorem[12] of Witt in [31, p. 244] (or (7.7) on [8, p. 106]). (In our situation, if such a field L exists, the theorem implies $\Delta(d_1, d_2) = 1$, which gives us a contradiction.) So this proposition should be viewed as a new perspective rather than a new result. In fact, Propositions 6.2 and 6.4 deal with a class of embedding problems wherein the existence of an unramified extension forces a Chern–Simons invariant to be zero. The outline of proof together with the explicit formulas for computing the Chern–Simons invariant should make clear that even the simplest $\mathbb{Z}/2\mathbb{Z}$-valued case is likely to have a non-trivial range of applications. We consider the point of view presented here as a simple and rough analogue of the classical theorem of Herbrand, whereby the existence of certain unramified extensions of cyclotomic fields forces

[12] K extends to a quaternion extension if and only if the Hilbert symbols (d_1, d_2) and $(d_1 d_2, -1)$ agree in the Brauer group.

some L-values to be congruent to zero ([29, Sect. 6.3]). In future papers, we hope to discuss this analogy in greater detail and investigate the possibility of 'converse Herbrand' type results in the spirit of Ribet's theorem [27].

Proof Suppose that there does exist such a field $L/\mathbb{Q}$ satisfying all the given properties above. Choose a prime ℓ such that

- ℓ does not divide d_1d_2.
- $\ell \equiv 3 \pmod 4$.
- $\left(\frac{-\ell}{p_i}\right) = A_i$ and $\left(\frac{-\ell}{q_j}\right) = B_j$ for all i and j.

In fact, $\ell \equiv a \pmod{4d_1d_2}$ for some a with $(a, 4d_1d_2) = 1$, and hence there are infinitely many such primes by Dirichlet's theorem.

Now let $d_3 := \ell^* = -\ell$. And let $F = \mathbb{Q}(\sqrt{d_1d_2d_3})$. Then by direct computation using the quadratic reciprocity law, we get

$$\left(\frac{d_1d_2}{\ell}\right) = \prod_{1\le i\le s}\left(\frac{p_i}{\ell}\right)\prod_{1\le j\le t}\left(\frac{q_j}{\ell}\right) = \prod_{1\le i\le s}\left(\frac{-\ell}{p_i}\right)\prod_{1\le j\le t}\left(\frac{-\ell}{q_j}\right) = \varDelta(d_1, d_2)\cdot\varDelta(d_2, d_1).$$

Thus by the above lemma, we get

$$\left(\frac{d_1d_2}{\ell}\right) = 1.$$

Furthermore, for all i and j

$$\left(\frac{d_2d_3}{p_i}\right) = A_i^2 = 1 \quad\text{and}\quad \left(\frac{d_3d_1}{q_j}\right) = B_j^2 = 1.$$

Therefore by [19, Theorem 1], there is a Galois extension $M/\mathbb{Q}$ such that M/F is unramified everywhere, and $\mathrm{Gal}(M/F) \simeq \mathcal{Q}$. Furthermore $KF = F(\sqrt{d_1}, \sqrt{d_2})$ is the unique subfield of M with $\mathrm{Gal}(M/KF) \simeq \mathbb{Z}/2\mathbb{Z}$.

Let $A = V_4$, and let $c_i = \alpha_i \cup \epsilon$, where $\alpha_i \in H^1(A, \mu_2)$ and $\epsilon \in Z^2(A, \mathbb{Z}/2\mathbb{Z})$ represents the extension $\mathcal{Q}$. Since M/F is an unramified $\mathcal{Q}$-extension, $[\epsilon] = 0 \in H^2(\pi, \mathbb{Z}/2\mathbb{Z})$, where $\pi = \pi_1(\mathrm{Spec}(O_F), \mathfrak{b})$ as before. Thus, $[c_i] = 0 \in H^3(X, \mu_2)$ for all i. This implies that $CS_{c_i}([\rho]) = 0$ for all i, where $\rho \in \mathrm{Hom}(\pi, A)$ factors through

$$\pi \twoheadrightarrow \mathrm{Gal}(KF/F) \simeq A.$$

Take α_1 so that $F^{\alpha_1} = F(\sqrt{d_1})$. Since

$$\prod_{1\le i\le s}\left(\frac{-d_2\cdot\ell}{p_i}\right)\times\prod_{1\le j\le t}\left(\frac{d_1}{q_j}\right) = \prod_{1\le j\le t} B_j = \varDelta(d_2, d_1) = \varDelta(d_1, d_2) = -1$$

by assumption, we get

Table 1 Some biquadratic fields and quaternionic extensions

d_1	d_2	Δ	$\exists L$?	d_1	d_2	Δ	$\exists L$?	d_1	d_2	Δ	$\exists L$?
5	13	-1	No	13	17	1	Yes [44]	17	21	1	Yes [48]
5	17	-1	No	13	21	-1	No	17	29	-1	No
5	21	1	Yes [37]	13	29	1	Yes [45]	17	33	1	Yes [49]
5	29	1	Yes [41]	13	33	-1	No	17	37	-1	No
5	33	-1	No	13	37	-1	No	17	41	-1	No
5	37	-1	No	13	41	-1	No	17	53	1	Yes [50]
5	41	1	Yes [42]	13	53	1	Yes [46]	17	57	-1	No
5	53	-1	No	13	57	-1	No	17	61	-1	No
5	57	-1	No	13	61	1	Yes [47]	17	65	-1	No
5	61	1	Yes [43]	13	69	1	No	17	69	1	Yes [51]

$$CS_{c_1}([\rho]) = \frac{1}{2}$$

by Proposition 5.16, which is a contradiction. Thus, there cannot exist such L.

Remark 6.3 For the explicit construction of quaternion extensions L of $\mathbb{Q}$, see [9] or [28, Theorem 4.5].

In the LMFDB, you can search for $\mathcal{Q}$-extensions L over $\mathbb{Q}$ with odd discriminants. We make a table for readers, which verifies our theorem numerically. Here $\Delta = \Delta(d_1, d_2)$ (Table 1).

When $d_1 = 13$ and $d_2 = 3 \cdot 23 = 69$, there cannot exist such L even though $\Delta(d_1, d_2) = 1$. This follows from the following proposition which is already known to experts (e.g. [28]). For the sake of readers, we provide a complete proof as well.

Proposition 6.4 *Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ as above. Let p be a prime divisor of d_i, which is congruent to* 3 *modulo* 4. *If $\left(\frac{d_{3-i}}{p}\right) = 1$, then there cannot exist a number field L such that* $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathcal{Q}$ *and $K \subset L$.*

Proof Let p be a prime divisor of d_2, which is congruent to 3 modulo 4. Suppose that $\left(\frac{d_1}{p}\right) = 1$ and there exists such a field L. Then by the same argument as in Proposition 5.15, the ramification index of p in $L/\mathbb{Q}$ is 4. Let $\mathcal{O} = \mathbb{Z}[\sqrt{d_1}]$ be the ring of integers of $\mathbb{Q}(\sqrt{d_1})$. Then, since $\left(\frac{d_1}{p}\right) = 1$, $p\mathcal{O} = \wp \cdot \wp'$ for two different maximal ideals $\wp$ and $\wp'$. Thus, $D(\wp) = I(\wp) \simeq \mathbb{Z}/4\mathbb{Z}$, where $D(\wp)$ (resp. $I(\wp)$) is the decomposition group (resp. inertia group) of $\wp$ in $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathcal{Q}$. Since $O_{\wp} \simeq \mathbb{Z}_p$, the $D(\wp) = I(\wp) \simeq \mathbb{Z}/4\mathbb{Z}$ can be regarded as a quotient of $\mathbb{Z}_p^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Because $p - 1 \equiv 2 \pmod 4$, this is a contradiction and hence the result follows.

Acknowledgements M.K. owes a tremendous debt of gratitude to many people for conversations, communications, and tutorials about a continuous stream of facts and theories that he barely understands even now. These include John Baez, Alan Barr, Bruce Bartlett, Jean Bellissard, Philip Candelas, Ted Chinburg, John Coates, Tudor Dimofte, Dan Freed, Sergei Gukov, Jeff Harvey, Yang-Hui He, Lars Hesselholt, Mahesh Kakde, Kazuya Kato, Philip Kim, Kobi Kremnitzer, Julien Marché, Behrang Noohi, Xenia de la Ossa, Jaesuk Park, Alexander Schekochihin, Alexander Schmidt, Urs Schreiber, Graeme Segal, Adam Sikora, Peter Shalen, Romyar Sharifi, Junecue Suh, Kevin Walker, and Andrew Wiles. All authors are grateful to Dr. Kwang-Seob Kim for his invaluable help in producing a number of the examples. They are also grateful to the authors of [2] for sending a preliminary version of their paper. D.K. was supported by IBS-R003-D1 and Simons Foundation grant 550033. M.K. was supported by EPSRC grant EP/M024830/1. J.P. was supported by Samsung Science & Technology Foundation (SSTF-BA1502-01). H.Y. was supported by IBS-R003-D1.

7 Appendix 1: Conjugation on Group Cochains

We compute cohomology of a topological group G with coefficients in a topological abelian group M with continuous G-action using the complex whose component of degree i is $C^i(G, M)$, the continuous maps from G^i to M. The differential

$$d : C^i(G, M) \to C^{i+1}(G, M)$$

is given by

$$df(g_1, g_2, \dots, g_{i+1}) = g_1 f(g_2, \dots, g_{i+1})$$

$$+\sum_{k=1}^{i} f(g_1, \dots, g_{k-1}, g_k g_{k+1}, g_{k+2}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, g_2, \dots, g_i).$$

We denote by

$$B^i(G, M) \subset Z^i(G, M) \subset C^i(G, M)$$

the images and the kernels of the differentials, the coboundaries and the cocycles, respectively. The cohomology is then defined as

$$H^i(G, M) := Z^i(G, M)/B^i(G, M).$$

There is a natural right action of G on the cochains given by

$$a : c \mapsto c^a := a^{-1} c \circ \mathrm{Ad}_a,$$

where Ad_a refers to the conjugation action of a on G^i.

Lemma 7.1 *The G action on cochains commutes with d:*

$$d(c^a) = (dc^a)$$

for all $a \in G$.

Proof If $c \in C^i(G, M)$, then

$$d(c^a)(g_1, g_2, \ldots, g_{i+1}) = g_1 a^{-1} c(\mathrm{Ad}_a(g_2), \ldots, \mathrm{Ad}_a(g_{i+1}))$$

$$+ \sum_{k=1}^{i} a^{-1} c(\mathrm{Ad}_a(g_1), \ldots, \mathrm{Ad}_a(g_{k-1}), \mathrm{Ad}_a(g_k)\mathrm{Ad}_a(g_{k+1}), \mathrm{Ad}_a(g_{k+2}), \ldots, \mathrm{Ad}_a(g_{i+1}))$$

$$+(-1)^{i+1} a^{-1} c(\mathrm{Ad}_a(g_1), \mathrm{Ad}_a(g_2), \ldots, \mathrm{Ad}_a(g_i))$$

$$= a^{-1} \mathrm{Ad}_a(g_1) c(\mathrm{Ad}_a(g_2), \ldots, \mathrm{Ad}_a(g_{i+1}))$$

$$+ \sum_{k=1}^{i} a^{-1} c(\mathrm{Ad}_a(g_1), \ldots, \mathrm{Ad}_a(g_{k-1}), \mathrm{Ad}_a(g_k)\mathrm{Ad}_a(g_{k+1}), \mathrm{Ad}_a(g_{k+2}), \ldots, \mathrm{Ad}_a(g_{i+1}))$$

$$+(-1)^{i+1} a^{-1} c(\mathrm{Ad}_a(g_1), \mathrm{Ad}_a(g_2), \ldots, \mathrm{Ad}_a(g_i))$$

$$= a^{-1} (dc)(\mathrm{Ad}_a(g_1), \mathrm{Ad}_a(g_2), \ldots, \mathrm{Ad}_a(g_{i+1}))$$

$$= (dc)^a(g_1, g_2, \ldots, g_{i+1}).$$

We also use the notation $(g_1, g_2, \ldots, g_i)^a := \mathrm{Ad}_a(g_1, g_2, \ldots, g_i)$. It is well-known that this action is trivial on cohomology. We wish to show the construction of explicit h_a with the property that

$$c^a = c + dh_a$$

for cocycles of degree 1, 2, and 3. The first two are relatively straightforward, but degree 3 is somewhat delicate. In degree 1, first note that $c(e) = c(ee) = c(e) + ec(e) = c(e) + c(e)$, so that $c(e) = 0$. Next, $0 = c(e) = c(gg^{-1}) = c(g) + gc(g^{-1})$, and hence, $c(g^{-1}) = -g^{-1}c(g)$. Therefore,

$$c(aga^{-1}) = c(a) + ac(ga^{-1}) = c(a) + ac(g) + agc(a^{-1}) = c(a) + ac(g) - aga^{-1}c(a).$$

From this, we get

$$c^a(g) = c(g) + a^{-1}c(a) - ga^{-1}c(a).$$

That is,

$$c^a = c + dh_a$$

for the zero cochain $h_a(g) = a^{-1}c(a)$.

Lemma 7.2 *For each $c \in Z^i(G, M)$ and $a \in G$, we can associate an*

$$h_a^{i-1}[c] \in C^{i-1}(G, M)/B^{i-1}(G, M)$$

in such a way that

$$\begin{aligned} &(1) \quad c^a - c = dh_a^{i-1}[c]; \\ &(2) \quad h_{ab}^{i-1}[c] = (h_a^{i-1}[c])^b + h_b^{i-1}[c]. \end{aligned}$$

Proof This is clear for $i = 0$ and we have shown above the construction of $h_a^0[c]$ for $c \in Z^1(G, M)$ satisfying (1). Let us check the condition (2):

$$h_{ab}^0[c](g) = (ab)^{-1}c(ab)$$

$$= b^{-1}a^{-1}(c(a) + ac(b)) = b^{-1}h_a^0[c](\mathrm{Ad}_b(g)) + h_b^0[c](g) = (h_a^0[c])^b(g) + h_b^0[c](g).$$

We prove the statement using induction on i, which we now assume to be ≥ 2. For a module M, we have the exact sequence

$$0 \to M \to C^1(G, M) \to N \to 0,$$

where $C^1(G, M)$ has the right regular action of G and $N = C^1(G, M)/M$. Here, we give $C^1(G, M)$ the topology of pointwise convergence. There is a canonical linear splitting $s : N \to C^1(G, M)$ with image the group of functions f such that $f(e) = 0$, using which we topologise N. According to [24, Proof of 2.5], the G-module $C^1(G, M)$ is acyclic,[13] that is,

$$H^i(G, C^1(G, M)) = 0$$

for $i > 0$. Therefore, given a cocycle $c \in Z^i(G, M)$, there is an

$$F \in C^{i-1}(G, C^1(G, M))$$

such that its image $f \in C^{i-1}(G, N)$ is a cocycle and $dF = c$. Hence, $d(F^a - F) = c^a - c$. Also, by induction, there is a $k_a \in C^{i-2}(G, N)$ such that $f^a - f = dk_a$ and

[13] The notation there for $C^1(G, M)$ is $F_0^0(G, M)$. One difference is that Mostow uses the complex $E^*(G, M)$ of equivariant homogeneous cochains in the definition of cohomology. However, the isomorphism $E^n \to C^n$ that sends $f(g_0, g_1, \ldots, g_n)$ to $f(1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_n)$ identifies the two definitions. This is the usual comparison map one uses for discrete groups, which clearly preserves continuity.

$k_{ab} = (k_a)^b + k_b + dl$ for some $l \in C^{i-3}(G, N)$ (zero if $i = 2$). Let $K_a = s \circ k_a$ and put

$$h_a = F^a - F - dK_a.$$

Then the image of h_a in N is zero, so h_a takes values in M, and $dh_a = c^a - c$. Now we check property (2). Note that

$$K_{ab} = s \circ k_{ab} = s \circ (k_a)^b + s \circ k_b + s \circ dl.$$

But $s \circ (k_a)^b - (s \circ k_a)^b$ and $s \circ dl - d(s \circ l)$ both have image in M. Hence, $K_{ab} = K_a^b + K_b + d(s \circ l) + m$ for some cochain $m \in C^{i-2}(G, M)$. From this, we deduce

$$dK_{ab} = (dK_a)^b + dK_b + dm,$$

from which we get

$$h_{ab} = F^{ab} - F - dK_{ab} = (F^a)^b - F^b + F^b - F - (dK_a)^b - dK_b - dm = (h_a)^b + h_b + dm.$$

8 Appendix 2: Conjugation Action on Group Cochains: Categorical Approach

In this section, an alternative and conceptual proof of Lemma 7.2 is outlined. Although not strictly necessary for the purposes of this paper, we believe that a functorial theory of secondary classes in group cohomology will be important in future developments. This point has also been emphasised to M.K. by Lawrence Breen. More details and elaborations will follow in a forthcoming publication by B.N.

8.1 Notation

In what follows G is a group and M is a left G-module. The action is denoted by ${}^a m$. The left conjugation action of $a \in G$ on G is denoted $\mathrm{Ad}_a(x) = axa^{-1}$. We have an induced right action on n-cochains $f\ G^n \to M$ given by

$$f^a(\mathbf{g}) := {}^{a^{-1}}(f(\mathrm{Ad}_a\,\mathbf{g})).$$

Here, $\mathbf{g} \in G^n$ is an n-chain, and $\mathrm{Ad}_a\,\mathbf{g}$ is defined componentwise.

In what follows, $[n]$ stands for the ordered set $\{0, 1, \dots, n\}$, viewed as a category.

8.2 Idea

The above action on cochains respects the differential, hence passes to cohomology. It is well known that the induced action on cohomology is trivial. That is, given an n-cocycle f and any element $a \in G$, the difference $f^a - f$ is a coboundary. In this appendix we explain how to construct an $(n-1)$-cochain $h_{a,f}$ such that $d(h_{a,f}) = f^a - f$. The construction, presumably well known, uses standard ideas from simplicial homotopy theory [26, Sect. 1]. The general case of this construction, as well as the missing proofs of some of the statements in this appendix will appear in a separate article.

Let $\mathcal{G}$ denote the one-object category (in fact, groupoid) with morphisms G. For an element $a \in G$, we have an action of a on $\mathcal{G}$ which, by abuse of notation, we will denote again by $\mathrm{Ad}_a : \mathcal{G} \to \mathcal{G}$; it fixes the unique object and acts on morphisms by conjugation by a.

The main point in the construction of the cochain $h_{a,f}$ is that there is a "homotopy" (more precisely, a natural transformation) H_a from the identity functor id: $\mathcal{G} \to \mathcal{G}$ to $\mathrm{Ad}_a : \mathcal{G} \to \mathcal{G}$. The homotopy between id and Ad_a is given by the functor $H_a : \mathcal{G} \times [1] \to \mathcal{G}$ defined by

$$H_a|_0 = \mathrm{id}, \quad H_a|_1 = \mathrm{Ad}_a, \text{ and } H_a(\iota) = a^{-1}.$$

It is useful to visualise the category $\mathcal{G} \times [1]$ as

$$\begin{tikzcd} 0 \arrow[loop above, "G"] \arrow[r, "\iota"] & 1 \arrow[loop above, "G"] \end{tikzcd} .$$

8.3 Cohomology of Categories

We will use multiplicative notation for morphisms in a category, namely, the composition of $g \colon x \to y$ with $h \colon y \to z$ is denoted $gh \colon x \to z$.

Let $\mathcal{C}$ be a small category and M a left $\mathcal{C}$-module, that is, a functor $M : \mathcal{C}^{\mathrm{op}} \to \mathbf{Ab}$, $x \mapsto M_x$, to the category of abelian groups (or your favorite linear category). Note that when $\mathcal{G}$ is as above, this is nothing but a left G-module in the usual sense. For an arrow $g \colon x \to y$ in $\mathcal{C}$, we denote the induced map $M_y \to M_x$ by $m \mapsto {}^g m$.

Let $\mathcal{C}^{[n]}$ denote the set of all n-tuples $\mathbf{g}$ of composable arrows in $\mathcal{C}$,

$$\mathbf{g} = \bullet \xrightarrow{g_1} \bullet \xrightarrow{g_2} \cdots \xrightarrow{g_n} \bullet.$$

We refer to such a $\mathbf{g}$ as an n**-cell** in $\mathcal{C}$; this is the same thing as a functor $[n] \to \mathcal{C}$, which we will denote, by abuse of notation, again by $\mathbf{g}$.

An n-**chain** in $\mathcal{C}$ is an element in the free abelian group $\mathrm{C}_n(\mathcal{C}, \mathbb{Z})$ generated by the set $\mathcal{C}^{[n]}$ of n-cells. For an n-cell $\mathbf{g}$ as above, we let $s\mathbf{g} \in \mathrm{Ob}\,\mathcal{C}$ denote the source of g_1.

By an n-**cochain** on $\mathcal{C}$ with values in M we mean a map f that assigns to any n-cell $\mathbf{g} \in \mathcal{C}^{[n]}$ an element in $M_{s\mathbf{g}}$. Note that, by linear extension, we can evaluate f on any n-chain in which all n-cells share a common source point.

The n-cochains form an abelian group $\mathrm{C}^n(\mathcal{C}, M)$. The **cohomology** groups $\mathrm{H}^n(\mathcal{C}, M)$, $n \geq 0$, are defined using the cohomology complex $\mathrm{C}^\bullet(\mathcal{C}, M)$:

$$0 \to \mathrm{C}^0(\mathcal{C}, M) \xrightarrow{d} \mathrm{C}^1(\mathcal{C}, M) \xrightarrow{d} \cdots \xrightarrow{d} \mathrm{C}^n(\mathcal{C}, M) \xrightarrow{d} \mathrm{C}^{n+1}(\mathcal{C}, M) \xrightarrow{d} \cdots$$

where the differential

$$d\colon \mathrm{C}^n(\mathcal{C}, M) \to \mathrm{C}^{n+1}(\mathcal{C}, M)$$

is defined by

$$df(g_1, g_2, \ldots, g_{n+1}) = {}^{g_1}(f(g_2, \ldots, g_{n+1})) + \sum_{1 \leq i \leq n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, g_2, \ldots, g_n).$$

A left G-module M in the usual sense gives rise to a left module on $\mathcal{G}$, which we denote again by M. We sometimes denote $\mathrm{C}^\bullet(\mathcal{G}, M)$ by $\mathrm{C}^\bullet(G, M)$. Note that the corresponding cohomology groups coincide with the group cohomology $\mathrm{H}^n(G, M)$.

The cohomology complex $\mathrm{C}^\bullet(\mathcal{C}, M)$ and the cohomology groups $\mathrm{H}^n(\mathcal{C}, M)$ are functorial in M. They are also functorial in $\mathcal{C}$ in the following sense. A functor φ: $\mathcal{D} \to \mathcal{C}$ gives rise to a $\mathcal{D}$-module $\varphi^* M := M \circ \varphi\ \mathcal{D}^{op} \to \mathbf{Ab}$. We have a map of complexes

$$\varphi^*\colon \mathrm{C}^\bullet(\mathcal{C}, M) \to \mathrm{C}^\bullet(\mathcal{D}, \varphi^* M), \tag{8.1}$$

which gives rise to the maps

$$\varphi^*\colon \mathrm{H}^n(\mathcal{C}, M) \to \mathrm{H}^n(\mathcal{D}, \varphi^* M)$$

on cohomology, for all $n \geq 0$.

8.4 Definition of the Cochains $h_{a,f}$

The flexibility we gain by working with chains on general categories allows us to import standard ideas from topology to this setting. The following definition of the cochains $h_{a,f}$ is an imitation of a well known construction in topology.

Let $f \in \mathrm{C}^{n+1}(G, M)$ be an $(n+1)$-cochain, and $a \in G$ an element. Let $H_a : \mathcal{G} \times [1] \to \mathcal{G}$ be the corresponding natural transformation. We define $h_{a,f} \in \mathrm{C}^n(G, M)$

by

$$h_{a,f}(\mathbf{g}) = f(H_a(\mathbf{g} \times [1])).$$

Here, $\mathbf{g} \in \mathcal{C}^{[n]}$ is an n-cell in $\mathcal{G}$, so $\mathbf{g} \times [1]$ is an $(n+1)$-chain in $\mathcal{G} \times [1]$, namely, the cylinder over $\mathbf{g}$.

To be more precise, we are using the notation $\mathbf{g} \times [1]$ for the image of the fundamental class of $[n] \times [1]$ in $\mathcal{G} \times [1]$ under the functor $\mathbf{g} \times [1]$ $[n] \times [1] \to \mathcal{G} \times [1]$. We visualize $[n] \times [1]$ as

$$\begin{tikzcd}
(0,1) \arrow[r] & (1,1) \arrow[r] & \cdots \arrow[r] & (n,1) \\
(0,0) \arrow[r] \arrow[u] & (1,0) \arrow[r] \arrow[u] & \cdots \arrow[r] & (n,0) \arrow[u]
\end{tikzcd}$$

Its fundamental class is the alternating sum of the $(n+1)$-cells

$$\begin{tikzcd}
 & & (r,1) \arrow[r] & \cdots \arrow[r] & (n,1) \\
(0,0) \arrow[r] & \cdots \arrow[r] & (r,0) \arrow[u] & &
\end{tikzcd}$$

in $[n] \times [1]$, for $0 \leq r \leq n$. Therefore,

$$h_{a,f}(\mathbf{g}) = \sum_{0 \leq r \leq n} (-1)^r f(g_1, \ldots, g_r, a^{-1}, \mathrm{Ad}_a\, g_{r+1}, \ldots, \mathrm{Ad}_a\, g_n). \tag{8.2}$$

The following proposition can be proved using a variant of Stokes' formula for cochains.

Proposition 8.1 *The graded map $h_{-,a}\colon \mathrm{C}^{\bullet+1}(G, M) \to \mathrm{C}^{\bullet}(G, M)$ is a chain homotopy between the chain maps*

$$\mathrm{id}, (-)^a\colon \mathrm{C}^{\bullet}(G, M) \to \mathrm{C}^{\bullet}(G, M).$$

That is,

$$h_{a,df} + d(h_{a,f}) = f^a - f$$

for every $(n+1)$-cochain f. In particular, if f is an $(n+1)$-cocycle, then $d(h_{a,f}) = f^a - f$.

8.5 Composing Natural Transformations

Given an $(n+1)$-cochain f, and elements $a, b \in G$, we can construct three n-cochains: $h_{a,f}$, $h_{b,f}$ and $h_{ab,f}$. A natural question to ask is whether these three cochains satisfy a cocycle condition. It turns out that the answer is yes, but only up to a coboundary $dh_{a,b,f}$. Below we explain how $h_{a,b,f}$ is constructed. In fact, we construct cochains $h_{a_1,\ldots,a_k,f}$, for any k elements $a_i \in G$, $1 \le i \le k$, and study their relationship.

Let $f \in \mathrm{C}^{n+k}(G, M)$ be an $(n+k)$-cochain. Let $\mathbf{a} = (a_1, \ldots, a_k) \in G^{\times k}$. Consider the category $\mathcal{G} \times [k]$,

$$\begin{tikzcd}
0 \arrow[loop above, "G"] \arrow[r, "\iota_0"] & 1 \arrow[loop above, "G"] \arrow[r, "\iota_1"] & \cdots \arrow[r, "\iota_{k-1}"] & k. \arrow[loop above, "G"]
\end{tikzcd}$$

Let $H_{\mathbf{a}} : \mathcal{G} \times [k] \to \mathcal{G}$ be the functor such that $\iota_i \mapsto a_{k-i}^{-1}$ and $H_{\mathbf{a}}|_{\{0\}} = \mathrm{id}_G$. (So, $H_{\mathbf{a}}|_{\{k-i\}} = \mathrm{Ad}_{a_{i+1}\cdots a_k}$.) Define $h_{\mathbf{a},f} \in \mathrm{C}^n(G, M)$ by

$$h_{\mathbf{a},f}(\mathbf{g}) = f(H_{\mathbf{a}}(\mathbf{g} \times [k])). \tag{8.3}$$

Here, $\mathbf{g} \in \mathcal{C}^{[n]}$ is an n-cell in $\mathcal{G}$, so $\mathbf{g} \times [k]$ is an $(n+k)$-chain in $\mathcal{G} \times [k]$.

To be more precise, we are using the notation $\mathbf{g} \times [k]$ for the image of the fundamental class of $[n] \times [k]$ in $\mathcal{G} \times [k]$ under the functor $\mathbf{g} \times [k]$ $[n] \times [k] \to \mathcal{G} \times [k]$. We visualize $[n] \times [k]$ as

$$\begin{tikzcd}
(0,k) \arrow[r] & (1,k) \arrow[r] & \cdots \arrow[r] & (n,k) \\
\vdots \arrow[u] & \vdots \arrow[u] & & \vdots \arrow[u] \\
(0,1) \arrow[r] \arrow[u] & (1,1) \arrow[r] \arrow[u] & \cdots \arrow[r] & (n,1) \arrow[u] \\
(0,0) \arrow[r] \arrow[u] & (1,0) \arrow[r] \arrow[u] & \cdots \arrow[r] & (n,0) \arrow[u]
\end{tikzcd}$$

Its fundamental class is the $(n+k)$-chain

$$\sum_P (-1)^{|P|} P,$$

where P runs over (length $n+k$) paths starting from $(0,0)$ and ending in (n,k). Note that such paths correspond to (k,n) shuffles; $|P|$ stands for the parity of the shuffle (which is the same as the number of squares above the path in the $n \times k$ grid).

The most economical way to describe the relations between various $h_{\mathbf{a},f}$ is in terms of the cohomology complex of the right module

$$\mathbb{M}^\bullet := \underline{\mathrm{Hom}}\,(\mathrm{C}^\bullet(G, M), \mathrm{C}^\bullet(G, M))\,.$$

Here, $\underline{\text{Hom}}$ stands for the enriched hom in the category of chain complexes, and the right action of G on $\mathbb{M}^\bullet$ is induced from the right action $f \mapsto f^a$ of G on the $\mathrm{C}^\bullet(G, M)$ sitting on the right. The differential on $\mathbb{M}^\bullet$ is defined by

$$d_{\mathbb{M}^\bullet}(u) = (-1)^{|u|} u \circ d_{\mathrm{C}^\bullet(G,M)} - d_{\mathrm{C}^\bullet(G,M)} \circ u,$$

where $|u|$ is the degree of the homogeneous $u \in \mathrm{C}^\bullet(G, M)$.

Note that, for every $\mathbf{a} \in G^{\times k}$, we have $h_{\mathbf{a},f} \in \mathbb{M}^{-k}$. This defines a k-cochain on G of degree $-k$ with values in $\mathbb{M}^\bullet$,

$$h^{(k)}\colon\ \mathbf{a}\ \mapsto h_{\mathbf{a},-},\ \ \mathbf{a} \in G^{\times k}.$$

We set $h^{(-1)} := 0$. Note that $h^{(0)}$ is the element in $\mathbb{M}^0$ corresponding to the identity map id: $\mathrm{C}^\bullet(G, M) \to \mathrm{C}^\bullet(G, M)$.

The relations between various $h_{\mathbf{a},f}$ can be packaged in a simple differential relation. As in the case $k = 0$ discussed in Proposition 8.1, this proposition can be proved using a variant of Stokes' formula for cochains.

Proposition 8.2 *For every $k \geq -1$, we have $d_{\mathbb{M}^\bullet}(h^{(k+1)}) = d(h^{(k)})$.*

In the above formula, the term $d_{\mathbb{M}^\bullet}(h^{(k+1)})$ means that we apply $d_{\mathbb{M}^\bullet}$ to the values (in $\mathbb{M}^\bullet$) of the cochain $h^{(k+1)}$. The differential on the right hand side of the formula is the differential of the cohomology complex $\mathrm{C}^\bullet(G, \mathbb{M}^\bullet)$ of the (graded) right G-module $\mathbb{M}^\bullet$.

More explicitly, let $f \in \mathrm{C}^{n+k}(G, M)$ be an $(n + k)$-cochain. Then, Proposition 8.2 states that, for every $\mathbf{a} \in G^{\times(k+1)}$, we have the following equality of n-cochains:

$$\begin{aligned}(-1)^{(k+1)} h_{a_1,\ldots,a_{k+1},df} - dh_{a_1,\ldots,a_{k+1},f} = \quad & h_{a_2,\ldots,a_{k+1},f} + \\ & \sum_{1\leq i\leq k} (-1)^i h_{a_1,\ldots,a_i a_{i+1},\ldots,a_{k+1},f} + \\ & (-1)^{k+1} h^{a_{k+1}}_{a_1,\ldots,a_k,f}.\end{aligned}$$

Corollary 8.3 *Let $f \in \mathrm{C}^{n+k}(G, M)$ be an $(n + k)$-cocycle. Then, for every $\mathbf{a} \in G^{\times(k+1)}$, the n-cochain*

$$h_{a_2,\ldots,a_{k+1},f} + \sum_{1\leq i\leq k} (-1)^i h_{a_1,\ldots,a_i a_{i+1},\ldots,a_{k+1},f} + (-1)^{k+1} h^{a_{k+1}}_{a_1,\ldots,a_k,f}$$

is a coboundary. In fact, it is the coboundary of $-h_{a_1,\ldots,a_{k+1},f}$.

Example 8.4 Let us examine Corollary 8.3 for small values of k.

(i) For $k = 0$, the statement is that, for every cocycle f, $f - f^a$ is a coboundary. In fact, it is the coboundary of $-h_{f,a}$. We have already seen this in Proposition 8.1.

(ii) For $k = 1$, the statement is that, for every cocycle f, the cochain

$$h_{b,f} - h_{ab,f} + h^b_{a,f}$$

is a coboundary. In fact, it is the coboundary of $-h_{a,b,f}$.

8.6 Explicit Formula for $h_{a_1,\ldots,a_k,f}$

Let $f\colon G^{\times(n+k)} \to M$ be an $(n+k)$-cochain, and $\mathbf{a} := (a_1, a_2, \ldots, a_k) \in G^{\times k}$. Then, by Eq. (8.3), the effect of the n-cochain $h_{a_1,\ldots,a_k,f}$ on an n-tuple $\mathbf{x} := (x_0, x_1, \ldots, x_{n-1}) \in G^{\times n}$ is given by:

$$h_{a_1,\ldots,a_k,f}(x_0, x_1, \ldots, x_{n-1}) = \sum_P (-1)^{|P|} f(\mathbf{x}^P),$$

where $\mathbf{x}^P$ is the $(n+k)$-tuple obtained by the following procedure.

Recall that P is a path from $(0, 0)$ to (n, k) in the n by k grid. The l^{th} component $\mathbf{x}^P_l$ of $\mathbf{x}^P$ is determined by the l^{th} segment on the path P. Namely, suppose that the coordinates of the starting point of this segment are (s, t). Then,

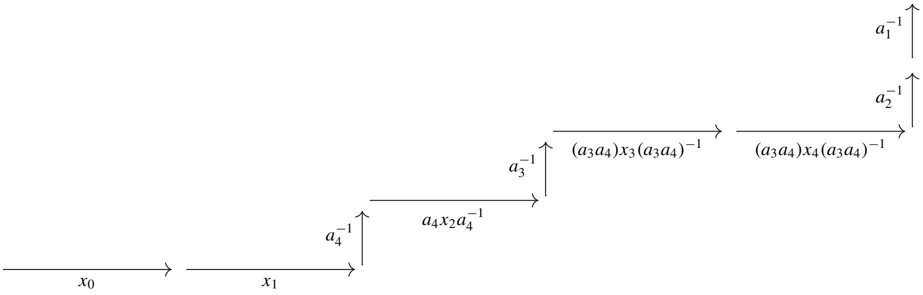
$$\mathbf{x}^P_l = a^{-1}_{k-t}$$

if the segment is vertical, and

$$\mathbf{x}^P_l = (a_{k-t+1} \cdots a_k) x_s (a_{k-t+1} \cdots a_k)^{-1},$$

if the segment is horizontal. Here, we use the convention that $a_0 = 1$.

The following example helps visualize $\mathbf{x}^P$:



The corresponding term is

$$-f(x_0, x_1, a_4^{-1}, a_4x_2a_4^{-1}, a_3^{-1}, (a_3a_4)x_3(a_3a_4)^{-1}, (a_3a_4)x_4(a_3a_4)^{-1}, a_2^{-1}, a_1^{-1}).$$

The sign of the path is determined by the parity of the number of squares in the n by k grid that sit above the path P (in this case 15).

References

1. Atiyah, Michael *Topological quantum field theories*. Inst. Hautes Études Sci. Publ. Math. No. 68 (1988), 175–186.
2. Bleher, F. M.; Chinburg, T.; Greenberg, R.; Kakde, M.; Pappas, G.; Taylor, M. J. Cup products inthe étale cohomology of number fields. New York J. Math. 24 (2018), 514–542.
3. Chung, Hee-Joong; Kim, Dohyeong; Kim, Minhyong; Pappas, Georgios; Park, Jeehoon; Yoo, HwajongAbelian arithmetic Chern-Simons theory and arithmetic linking numbers. Int. Math. Res. Not. 2019, no. 18, 5674–5702.
4. Coates, John; Kim, Minhyong *Selmer varieties for curves with CM Jacobians*. Kyoto J. Math. 50 (2010), no. 4, 827–852.
5. Cornell, Gary *Abhyankar's lemma and the class group*. Lecture Notes in Math. Vol. 751 (1979), 82–88.
6. Dijkgraaf, Robbert; Witten, Edward *Topological gauge theories and group cohomology*. Comm. Math. Phys. 129 (1990), no. 2, 393–429.
7. Freed, Daniel S.; Quinn, Frank *Chern-Simons theory with finite gauge group*. Comm. Math. Phys. 156 (1993), no. 3, 435–472.
8. Fröhlich, Albrecht *Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse- Witt invariants*. J. Reine. Angew. Math. 360 (1985), 84–123.
9. Fujisaki, Genjiro. *An elementary construction of Galois quaternion extension*. Proc. Japan Acad. Ser. Math Sci. Vol 66 (1990), no. 3, 80–83.
10. Fukaya, Takako; Kato, Kazuya *A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory*. Proceedings of the St. Petersburg Mathematical Society. Vol. XII, 1–85, Amer. Math. Soc. Transl. Ser. 2, 219, Amer. Math. Soc., Providence, RI, 2006.
11. Hornbostel, Jens; Kings, Guido *On non-commutative twisting in étale and motivic cohomology*. Ann. Inst. Fourier (Grenoble) 56 (2006), no. 4, 1257–1279.
12. Kedlaya, Kiran *A construction of polynomials with squarefree discriminants*. Proc. Amer. Math. Sco. Vol. 140. (2012), 3025–3033.
13. Kim, Minhyong *The motivic fundamental group of* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*. Invent. Math. 161 (2005), no. 3, 629–656.
14. Kim, Minhyong *p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication*. Ann. of Math. (2) 172 (2010), no. 1, 751–759.
15. Kim, Minhyong *Massey products for elliptic curves of rank 1*. J. Amer. Math. Soc. 23 (2010), no. 3, 725–747.
16. Kim, Minhyong *Tangential localization for Selmer varieties*. Duke Math. J. 161 (2012), no. 2, 173–199.
17. Kim, Minhyong *Arithmetic Chern-Simons Theory I*. arXiv:1510.05818. Preprint available in https://arxiv.org/pdf/1510.05818.pdf
18. Lazard, Michel *Groupes analytiques p-adiques*. Inst. Hautes Études Sci. Publ. Math. No. 26 (1965), 389–603.
19. Lemmermeyer, Franz *Unramified quaternion extensions of quadratic number fields*. Journal de Théories des Nombres de Bordeaux, tome 9 (1997), 51–68.

20. Mazur, Barry *Notes on etale cohomology of number fields*. Ann. Sci. École Norm. Sup. (4) 6 (1973), 521–552.
21. Mazur, Barry *Remarks on the Alexander polynomial*. Unpublished notes.
22. Milne, James *Étale cohomology*, Princeton Mathematics Series 33, Princeton University Press (1980).
23. Morishita, Masanori *Knots and primes. An introduction to arithmetic topology*. Universitext. Springer, London, 2012.
24. Mostow, George D. *Cohomology of Topological Groups and Solvmanifolds*. Annals of Mathematics(2), Vol. 73, No. 1 (Jan., 1961), 20–48
25. Neukirch, Jürgen; Schmidt, Alexander; Wingberg, Kay *Cohomology of number fields*. Second edition. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2008.
26. Quillen, D. *Higher algebraic K-theory. I*. Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972, pp. 85–147. Lecture Notes in Math., Vol. 341, Springer, Berlin 1973.
27. Ribet, Kenneth A. *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$. Invent. Math. 34 (1976), no. 3, 151–162.
28. Vaughan, Theresa P. *Constructing quaternionic fields*. Glasgow Math. Jour. Vol 34 (1992), 43–54.
29. Washington, Lawrence C. *Introduction to cyclotomic fields*. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.
30. Weibel, Charles *Introduction to homological algebra*. Cambridge Univ. Press, 1994.
31. Witt, Ernst *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. J. Reine. Angew. Math. 174 (1936), 237–245.*
32. Witten, Edward *Quantum field theory and the Jones polynomial*. Comm. Math. Phys. 121 (1989), no. 3, 351–399.
33. A database for Number fields created by Jürgen Klüners and Gunter Malle. http://galoisdb.math.upb.de/groups/view/discriminant?deg=16&num=65&sig=16&poly_id=3013654
34. A database for Number fields created by Jürgen Klüners and Gunter Malle. http://galoisdb.math.upb.de/groups/view/discriminant?deg=4&num=5&sig=4&poly_id=3579015
35. LMFDB(The L-functions and modular form database). http://www.lmfdb.org/NumberField/8.0.151939915084881.1
36. LMFDB. http://www.lmfdb.org/NumberField/8.0.752823265640625.1
37. LMFDB. http://www.lmfdb.org/NumberField/8.8.1340095640625.1
38. LMFDB. http://www.lmfdb.org/NumberField/8.0.1750329.1
39. LMFDB. http://www.lmfdb.org/NumberField/8.2.1835880147.3
40. LMFDB. http://www.lmfdb.org/NumberField/4.2.283.1
41. LMFDB. http://www.lmfdb.org/NumberField/8.8.9294114390625.1
42. LMFDB. http://www.lmfdb.org/NumberField/8.8.74220378765625.1
43. LMFDB. http://www.lmfdb.org/NumberField/8.0.805005849390625.1
44. LMFDB. http://www.lmfdb.org/NumberField/8.8.116507435287321.1
45. LMFDB. http://www.lmfdb.org/NumberField/8.0.2871098559212689.1
46. LMFDB. http://www.lmfdb.org/NumberField/8.8.1069831377767073611.1
47. LMFDB. http://www.lmfdb.org/NumberField/8.8.248679006649044049.1
48. LMFDB. http://www.lmfdb.org/NumberField/8.8.2070185663499849.1
49. LMFDB. http://www.lmfdb.org/NumberField/8.0.31172897213027361.1
50. LMFDB. http://www.lmfdb.org/NumberField/8.0.534993796092155401.1
51. LMFDB. http://www.lmfdb.org/NumberField/8.8.2604882107720890089.1