DIOPHANTINE RECIPROCITY ON THE ONE-HOLED TORUS

JUNHO PETER WHANG

Abstract. We prove a basic reciprocity law for special linear rank two integral local systems on the one-holed torus and their monodromy along simple loops.

1. Introduction

1.1. This note concerns a basic Diophantine reciprocity phenomenon for certain local systems on surfaces, or representations of surface groups. Let Σ be a one-holed torus, that is, a compact oriented surface of genus one with one boundary curve. We define the *discriminant* of a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ to be the number $\operatorname{disc}\rho = \operatorname{tr}\rho(c) - 2$ where c denotes the boundary of Σ. We remark that $\operatorname{disc}\rho = 0$ if and only if ρ is reducible. An essential curve on Σ is for us a simple closed curve on Σ which is neither contractible nor isotopic to the boundary.

Question 1. Given $d \in \mathbb{Z}$, which integers arise as monodromy traces of essential curves under representations $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{Z})$ with discriminant d?

We shall make basic partial progress toward this question. Given a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace, let us define its *discriminant field* to be the field $\mathbb{Q}(\sqrt{\operatorname{disc}\rho})$, and let us say that a real quadratic field L is *represented* by ρ if it is generated by the monodromy eigenvalues of ρ along some essential curve $a \subset \Sigma$. Relaxing Question 1, we may ask which real quadratic fields are represented by representations $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{Z})$ with a given discriminant field. Given a quadratic field K and a real quadratic field L, let us introduce the symbol

$$\left[\frac{K}{L}\right] \in \mathrm{Br}(\mathbb{Q})$$

defined as the Brauer class of *any*[1] quaternion algebra over $\mathbb{Q}$ with an integral order O such that L is represented by some representation $\rho : \pi_1\Sigma \to \mathrm{SL}_1(O) \hookrightarrow \mathrm{SL}_2(\mathbb{C})$ with discriminant field K. Thus, assuming $[K/L]$ is well-defined, we have $[K/L] = 1$ if and only if L is represented by an $\mathrm{SL}_2(\mathbb{Z})$-representation with discriminant field K. Let us denote the discriminant of a number field $K/\mathbb{Q}$ by D_K, and let $(-,-)_{\mathbb{Q}}$ be the usual symbol for quaternion algebras over $\mathbb{Q}$. We shall prove the following.

Theorem 2. *We have $[K/L] = (D_K, D_L)_{\mathbb{Q}}$ for any quadratic field K and any real quadratic field L. In particular, if K and L are real quadratic fields, then*

$$\left[\frac{K}{L}\right] = \left[\frac{L}{K}\right].$$

Date: June 15, 2019.

[1] It is not *a priori* clear that such an algebra exists and determines a unique class.

In fact, as our work in Section 2 will show, an integer n with $|n| > 2$ arises as the monodromy trace of an essential curve under some representation $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{Z})$ with discriminant field K if and only if $n^2 - 4$ is the norm of some $x \in K$ over $\mathbb{Q}$. Another property of the symbol $[K/L]$, which is not obvious from the definition but immediate from Theorem 2, is the multiplicativity

$$\left[\frac{K_1}{L}\right]\left[\frac{K_2}{L}\right] = \left[\frac{\mathbb{Q}(\sqrt{D_{K_1}D_{K_2}})}{L}\right]$$

for distinct quadratic fields K_1 and K_2, and real quadratic field L. Question 1 and the study of representations $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{Z})$ invites certain analogies with the classical arithmethic theory of binary quadratic forms. Theorem 2 is motivated in this regard by the law of quadratic reciprocity, albeit not sharing the latter's depth. The *existence* of the analogy, however, seems worth noting and possibly indicative of deeper arithmetic, which we continue to pursue in future work.

The well-known parametrization of narrow ideal classes of real quadratic fields by primitive closed geodesics on the modular surface brings geometric and spectral methods to bear on arithmetic questions. It is natural to conjecture, conversely, that other geometric objects on the modular surface also have similar arithmetic significance or interpretation. This note arises from our first study, in this spirit, of the arithmetic structure behind one-holed torus mappings into the modular surface.

2. Proof of the main result

We shall prove Theorem 2 in two steps. Namely, given the surface Σ as before, as well as a quadratic field K and real quadratic field L, we shall show:

(1) (Existence) L is represented by some representation $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace and discriminant field K; and
(2) (Uniqueness) the image of any representation obtained in (1) generates a quaternion algebra isomorphic to $(D_K, D_L)_{\mathbb{Q}}$.

In Section 2.1, we prove (1) using an elementary observation on the integral points of moduli of local systems. In Section 2.2, we prove (2).

2.1. **Moduli spaces.** Let Σ be a smooth compact oriented surface of genus one with one boundary curve. Recall that the mapping class group Γ of Σ is the group of isotopy classes of orientation-preserving diffeomorphisms of Σ fixing the boundary pointwise. The natural action of Γ on the set of isotopy classes of essential curves on Σ is transitive. Throughout this section, let us fix a base point of Σ and a pair $\{\alpha, \beta\}$ of simple loops intersecting transversely at the base point, so that $\{\alpha, \beta\}$ freely generates the fundamental group $\pi_1\Sigma$ of the surface.

Let V denote the coarse moduli space of SL_2-representations of the fundamental group of Σ. It is an affine scheme over $\mathbb{C}$ whose complex points parametrize the Jordan equivalence classes of representations $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$. By classical invariant theoretic results (see e.g. [5] for reference) we have an identification

$$(\mathrm{tr}_\alpha, \mathrm{tr}_\beta, \mathrm{tr}_{\alpha\beta}) : V \xrightarrow{\sim} \mathbb{A}^3_{x,y,z}$$

where tr_α is the regular function on V defined by $\rho \mapsto \mathrm{tr}\,\rho(\alpha)$, etc. Note that the loop $\alpha\beta$ is also homotopic to a simple loop on Σ. The variety V has a natural model over $\mathbb{Z}$ such that $V(\mathbb{Z})$ consists precisely of representations with integral trace.

Recall from Section 1 that the *discriminant* of a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ is $\operatorname{disc}\rho = \operatorname{tr}\rho(c) - 2$ where c is the boundary curve of Σ. For each $d \in \mathbb{C}$, let $V_d \subset V$ be the subvariety of the moduli space parametrizing those representations with discriminant d. Under the identification $V \simeq \mathbb{A}^3$ given above, V_d has presentation as an affine algebraic surface with equation

$$x^2 + y^2 + z^2 - xyz - 4 = d.$$

This is easily seen by expressing the trace $\mathrm{tr}_{[\alpha,\beta]}$ of the commutator of α and β in terms of the coordinate functions tr_α, tr_β, and $\mathrm{tr}_{\alpha\beta}$. We note that V_0 parametrizes precisely the reducible representations of $\pi_1\Sigma$. The mapping class group Γ naturally acts via pullback on each V_d, and if d is a nonzero integer the associated nonlinear descent decomposes $V_d(\mathbb{Z})$ into finitely many orbits in an effective manner, as first observed by Markoff [7]. (The analogous descent for moduli of SL_2-local systems on general surfaces was established in [9].) The above presentation of the moduli spaces V_d provides inspiration for the following result.

Proposition 3. *Fix $z, d \in \mathbb{Z}$ with $|z| > 2$ and $d \neq 0$. The affine quadric given by*

$$x^2 + y^2 + z^2 - xyz - 4 = e^2 d$$

in variables (x, y, e) has a Zariski dense set of integral points.

Proof. Let us denote by W the quadric in question. First, we notice that the point $(x, y, e) = (z, 2, 0)$ lies in $W(\mathbb{Z})$. Let G denote the special orthogonal group of the nondegenerate indefinite ternary quadratic form

$$Q(x, y, e) = x^2 + y^2 - zxy - de^2.$$

The quadric surface W is the level set $Q(x, y, e) = 4 - z^2$, and the group $G(\mathbb{C})$ acts transitively on $W(\mathbb{C})$. Since Q is indefinite, $G(\mathbb{R})$ is a noncompact semisimple Lie group isomorphic to $\mathrm{SO}(2, 1)$ or $\mathrm{SO}(1, 2)$, and the arithmetic group $G(\mathbb{Z})$, being a lattice in $G(\mathbb{R})$ by work of Borel–Harish-Chandra [1], is Zariski dense in G by the Borel density theorem. Hence, the orbit $G(\mathbb{Z}) \cdot (z, 2, 0)$ is Zariski dense in W. □

We record two corollaries of Proposition 3. Corollary 4 establishes the first step of our proof of Theorem 2. Corollary 5 will not be used in this note, but might be of independent interest.

Corollary 4. *For any quadratic fields K and L with L real, there is a representation $\pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace and discriminant field K representing L.*

Proof. By Dirichlet's unit theorem, the ring of integers O_L of L contains a unit η of norm one such that $L = \mathbb{Q}(\eta)$. Let $z = \mathrm{tr}(\eta)$ be the trace of η over $\mathbb{Q}$. Let d be the discriminant of K. By Proposition 3, there is $(x, y, e) \in \mathbb{Z}^3$ with $e \neq 0$ so that

$$(x, y, z) \in V_{e^2 d}(\mathbb{Z}).$$

By the moduli interpretation, the point (x, y, z) corresponds to a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace, with the property that its discriminant field is K and $\operatorname{tr}\rho(a) = z$ for some essential curve $a \subset \Sigma$. The latter implies that the monodromy eigenvalues of a under ρ are η and η^{-1}, so L is represented by ρ. □

Corollary 5. *For each $d \in \mathbb{Z}$, we have $V_{e^2 d}(\mathbb{Z}) \neq \emptyset$ for infinitely many $e \in \mathbb{Z}$.*

Ghosh–Sarnak [4] recently established a remarkable exact fundamental domain for an extension of the mapping class group action on $V_d(\mathbb{Z})$, and used it to analyze the asymptotics of the class numbers (i.e. numbers of integral orbits) as $|d| \to \infty$. They proved that almost all of the admissible V_d have nonzero class number, but at the same time infinitely many V_d are integral Hasse failures, having no integral points despite passing all congruence obstructions. Colliot-Thélène–Wei–Xu [3] and Loughran–Mitankin [6] studied the integral Brauer–Manin obstructions for these varieties, and showed that they do not account for all of the Hasse failures produced in [4]. These results underscore the difficulty of understanding the behavior of the integral points $V_d(\mathbb{Z})$. Corollary 5 suggests that, nonetheless, some basic structure emerges if one groups the varieties V_d together.

2.2. **Quaternion algebras.** Our main reference on quaternion algebras is [8]. Let us recall that an associative algebra B over a field $\mathbb{Q}$ is a *quaternion algebra* if B admits a $\mathbb{Q}$-linear basis $\{1, i, j, k\}$ with

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ij = -ji = k$$

for some $a, b \in \mathbb{Q}^\times$. Given $a, b \in \mathbb{Q}^\times$, we denote the quaternion algebra determined by a, b and the multiplication rules above by $(a, b)_\mathbb{Q}$. A quaternion algebra $B/\mathbb{Q}$ defines a class in the Brauer group of $\mathbb{Q}$. This class is trivial if and only if B is isomorphic to the algebra $M_2(\mathbb{Q})$ of 2×2 rational matrices. Given a quaternion algebra B over $\mathbb{Q}$, a *quaternion order* in B is a subring of B which is also a $\mathbb{Z}$-lattice.

Consider a quadratic field K, a real quadratic field L, and a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace and discriminant field K representing L. Note that ρ is irreducible since $\operatorname{disc}\rho \neq 0$. Let O_ρ denote the $\mathbb{Z}$-subalgebra generated by the image of ρ in the algebra $M_2(\mathbb{C})$ of 2×2 complex matrices. It is not difficult to see that O_ρ is a quaternion order; we provide a short proof below.

Proposition 6. *For any ρ given as above, the ring O_ρ is quaternion order, and the associated quaternion algebra $B_\rho = O_\rho \otimes \mathbb{Q}$ is isomorphic to $(D_K, D_L)_\mathbb{Q}$.*

Proof. For convenience, we shall identify the integers $\mathbb{Z}$ with their image in $M_2(\mathbb{C})$ under the natural embedding. The isomorphism class of O_ρ depends only on the $\mathrm{SL}_2(\mathbb{C})$-conjugacy and mapping class group equivalence class of ρ, so we may assume without loss of generality that $\mathbb{Q}(\rho(\alpha)) = \mathbb{Q}1 \oplus \mathbb{Q}\rho(\alpha) \subset M_2(\mathbb{C})$ is isomorphic to L, where $\{\alpha, \beta\}$ is the set of free generators for $\pi_1\Sigma$ we fixed. We claim that

$$(*) \qquad O_\rho = \mathbb{Z}1 \oplus \mathbb{Z}\rho(\alpha) \oplus \mathbb{Z}\rho(\beta) \oplus \mathbb{Z}(\alpha\beta) \quad \text{in} \quad M_2(\mathbb{C}).$$

Since the matrix equation $a + a^{-1} = \operatorname{tr}(a)1$ holds for any $a \in \mathrm{SL}_2(\mathbb{C})$, it follows that the ring O_ρ coincides with the $\mathbb{Z}$-algebra generated by $\rho(\alpha)$ and $\rho(\beta)$ in $M_2(\mathbb{C})$. In particular, O_ρ lies in the $\mathbb{Z}$-span of $\{\rho(\gamma) : \gamma \in M\}$ where M is the submonoid of $\pi_1\Sigma$ generated by $\{\alpha, \beta\}$. Next, we claim that each $\rho(\gamma)$, $\gamma \in M$, belongs to the $\mathbb{Z}$-span of

$$S = \{1, \rho(\alpha), \rho(\beta), \rho(\alpha\beta)\}.$$

Indeed, this follows by induction on the $\{\alpha, \beta\}$-word length of γ together with the observation that $a^2 - \operatorname{tr}(a)a + 1 = 0$ for $a \in \mathrm{SL}_2(\mathbb{C})$, as well as

$$\begin{aligned}
\rho(\beta\alpha) &= \operatorname{tr}(\rho(\beta))\rho(\alpha) + \rho(\beta)\operatorname{tr}(\rho(\alpha)) - \operatorname{tr}(\rho(\beta))\operatorname{tr}(\rho(\alpha)) + \operatorname{tr}(\alpha\beta) - \rho(\alpha\beta), \\
\rho(\alpha\beta\alpha) &= \operatorname{tr}\rho(\beta) - \rho(\beta) + \operatorname{tr}(\rho(\beta\alpha))\rho(\alpha), \quad \text{and} \\
\rho(\beta\alpha\beta) &= \operatorname{tr}\rho(\alpha) - \rho(\alpha) + \operatorname{tr}(\rho(\alpha\beta))\rho(\beta)
\end{aligned}$$

which can be verified using the mentioned matrix identities. To complete the proof of $(*)$, it remains to show that S is linearly independent over $\mathbb{Z}$, or equivalently over $\mathbb{Q}$. This follows from the linear independence of $\{1, \rho(\beta)\}$ over the field $\mathbb{Q}(\rho(\alpha))$, which is in turn a consequence of the irreducibility of ρ. In particular, it follows by $(*)$ that the algebra $B_\rho = O_\rho \otimes \mathbb{Q}$ has dimension 4 over $\mathbb{Q}$. Now, consider the elements $i = 2\rho(\alpha) - \operatorname{tr}\rho(\alpha)$ and $j = \rho(\alpha\beta) - \rho(\beta\alpha)$ in B_ρ (cf. [8, Section 22.1]). Arguing as above, we see that $\{1, i, j, ij\}$ forms a $\mathbb{Q}$-basis of B_ρ, and

$$i^2 = (\operatorname{tr}\rho(\alpha))^2 - 4, \quad j^2 = \operatorname{disc}\rho, \quad \text{and} \quad ij = -ji.$$

It follows that B_ρ is a quaternion algebra over $\mathbb{Q}$, and we have the identification $B_\rho \simeq \big((\operatorname{tr}\rho(\alpha))^2 - 4, \operatorname{disc}\rho\big)_{\mathbb{Q}} \simeq (D_L, D_K)_{\mathbb{Q}} \simeq (D_K, D_L)_{\mathbb{Q}}$ as desired. □

Remark. There is a natural one-to-one correspondence between isomorphism classes of quaternion orders over $\mathbb{Z}$ and equivalence classes of nondegenerate integral ternary quadratic forms [8, Section 22.1], under which the order O_ρ above maps to the form

$$X^2 + Y^2 + Z^2 + xYZ + yXZ + zXY \in \mathbb{Z}[X, Y, Z]$$

where $(x, y, z) \in \mathbb{A}^3(\mathbb{Z}) \simeq V(\mathbb{Z})$ is the point corresponding to ρ. This is the ternary quadratic form of discriminant $-\operatorname{disc}(\rho)$ considered by Cohn [2], and its equivalence class is an invariant of the mapping class group orbit $\Gamma \cdot (x, y, z)$.

2.3. **Proof of Theorem 2.** Let K and L be given as in the statement of Theorem 2. By Corollary 4, there is a representation $\rho : \pi_1\Sigma \to \mathrm{SL}_2(\mathbb{C})$ with integral trace and discriminant field K representing L, and by Proposition 6 the image of any such ρ generates a quaternion algebra isomorphic to $(D_K, D_L)_{\mathbb{Q}}$. It follows that the symbol $[K/L]$ is well-defined and moreover

$$\left[\frac{K}{L}\right] = (D_K, D_L)_{\mathbb{Q}},$$

thus proving Theorem 2.

References

[1] Borel, Armand; Harish-Chandra. *Arithmetic subgroups of algebraic groups.* Ann. of Math. (2) 75 1962 485–535.

[2] Cohn, Harvey. *Ternary forms as invariants of Markoff forms and other* $\mathrm{SL}_2(Z)$*-bundles.* Linear Algebra and Appl. 21 (1978), no. 1, 3–12.

[3] Colliot-Thélène, J.-L.; Wei, Dasheng; Xu, Fei. *Brauer-Manin obstruction for Markoff surfaces.* preprint. arXiv:1808.01584

[4] Ghosh, A.; Sarnak, P. *Integral points on Markoff type cubic surfaces.* Preprint. arXiv: 1706.06712

[5] Goldman, William M. *Trace coordinates on Fricke spaces of some simple hyperbolic surfaces.* Handbook of Teichmüller theory. Vol. II, 611–684, IRMA Lect. Math. Theor. Phys., 13, Eur. Math. Soc., Zürich, 2009.

[6] Loughran, Daniel; Mitankin, Vladimir. *Integral Hasse principle and strong approximation for Markoff surfaces.* preprint. arXiv:1807.10223

[7] Markoff, A. *Sur les formes quadratiques binaires indéfinies.* Math. Ann. 17 (1880), no. 3, 379-399.

[8] Voight, J. *Quaternion algebras*, version 0.9.14 (July 7, 2018). Available at: https://www.math.dartmouth.edu/~jvoight/quat.html

[9] Whang, Junho Peter. *Nonlinear descent on moduli of local systems.* Submitted. Preprint available at: https://math.mit.edu/~jwhang/