HECKE’S THEOREM ON THE DIFFERENT FOR 3-MANIFOLDS

WILL SAWIN AND MARK SHUSTERMAN

Abstract. Hecke has shown that the different of an extension of number fields is a square in the class group. We prove an analog for branched covers of closed 3-manifolds saying that the branch divisor is a square in the first homology group.

1. Introduction

Let $E/F$ be an extension of number fields, let $\mathcal{O}_E$ be the ring of integers of $E$, and let $\text{Cl}(\mathcal{O}_E)$ be the class group of $\mathcal{O}_E$. One associates to the extension $E/F$ the different $\mathcal{D}_{E/F}$, an ideal in $\mathcal{O}_E$, see [Ser79, Chapter 3]. Hecke has shown that as an element of $\text{Cl}(\mathcal{O}_E)$, the different $\mathcal{D}_{E/F}$ is a square, namely there exists an ideal class $J \in \text{Cl}(\mathcal{O}_E)$ such that $J^2 = \mathcal{D}_{E/F}$ in $\text{Cl}(\mathcal{O}_E)$. Hecke’s proof uses a reciprocity formula for Gauss sums, see [Arm67] and [Fro78] for a proof and a discussion of related results.

An analog of Hecke’s theorem for finite separable extensions of fields of fractions of Dedekind domains fails in general, see [FST62]. However, there exists an analog in case $E/F$ is a finite separable extension of function fields of curves over finite fields of odd characteristic, see [Arm67]. Another geometric analog of Hecke’s theorem, based on similarities between the inverse of the different and the canonical bundle on a curve, is the theory of theta characteristics.

In this work we consider an analog of Hecke’s theorem for 3-manifolds, as suggested by arithmetic topology. We refer to [Mor12] for the analogy between rings of integers and primes on the one hand, and 3-manifolds and knots on the other hand. The analog of $\text{Spec}(\mathcal{O}_F)$ is a closed (not necessarily oriented) 3-manifold $M$. The map $\text{Spec}(\mathcal{O}_E) \to \text{Spec}(\mathcal{O}_F)$ is replaced by a cover $\pi: \tilde{M} \to M$ branched over a link $L \subset M$, so $\tilde{M}$ is a closed 3-manifold and $\pi^{-1}(M \setminus L)$ is a covering space of $M \setminus L$. The inverse image of $L$ under $\pi$ is a link $\tilde{L}$ in $\tilde{M}$.

For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_E$ we denote by $e_\mathfrak{p}$ its ramification index, namely the largest positive integer $e$ for which $\mathfrak{p}^e$ contains $\mathfrak{p} \cap \mathcal{O}_F$. We view $\text{Spec}(\mathcal{O}_F)$ as branched over the primes of $\mathcal{O}_E$ that ramify, so $\tilde{L}$ is our analog for $\mathcal{R}_{E/F} = \{ \mathfrak{p} \in \text{Spec}(\mathcal{O}_E) : e_\mathfrak{p} > 1 \}$. The analogy is perhaps closest in case $\text{Spec}(\mathcal{O}_E) \to \text{Spec}(\mathcal{O}_F)$ is tamely ramified, namely $e_\mathfrak{p}$ is coprime to $|\mathcal{O}_E/\mathfrak{p}|$ for every $\mathfrak{p} \in \text{Spec}(\mathcal{O}_E)$. In this case the different of $E/F$ is given by

$$\mathcal{D}_{E/F} = \prod_{\mathfrak{p} \in \mathcal{R}_{E/F}} \mathfrak{p}^{e_\mathfrak{p}-1}.$$

The prime ideals in $\mathcal{R}_{E/F}$ are analogous to the components of the link $\tilde{L}$. For each component $\tilde{K}$ of this link, let the ramification index $e_{\tilde{K}}$ be the number of times the image under $\pi$ of a small loop around $\tilde{K}$ wraps around $\pi(\tilde{K})$. An analog of $\text{Cl}(\mathcal{O}_E)$ is $H_1(\tilde{M}, \mathbb{Z})$, and a homology class is a square if and only if its image in $H_1(\tilde{M}, \mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} \cong H_1(\tilde{M}, \mathbb{Z}/2\mathbb{Z})$ vanishes. Our analogy of $\mathcal{D}_{E/F}$, or rather of its class in $\text{Cl}(\mathcal{O}_E)/\text{Cl}(\mathcal{O}_E)^2$, is the branch divisor

$$\mathcal{D}_\pi = \sum_{\tilde{K} \text{ a component of } \tilde{L}} (e_{\tilde{K}} - 1)[\tilde{K}] \in H_1(\tilde{M}, \mathbb{Z}/2\mathbb{Z})$$

W.S. served as a Clay Research Fellow while working on this paper.
of $\pi$. Since we are working with $\mathbb{Z}/2\mathbb{Z}$-coefficients, it is not necessary to fix an orientation of $\tilde{K}$, nor is the sign of $e_{\tilde{K}}$ significant.

**Theorem 1.1.** Let $\tilde{M}$ and $M$ be closed 3-manifolds, and let $\pi\colon \tilde{M} \to M$ be a cover branched over a link in $M$. Then the branch divisor $D_\pi$ represents the trivial class in $H_1(\tilde{M}, \mathbb{Z}/2\mathbb{Z})$.

2. A CENTRAL EXTENSION OF THE HYPEROCTAHEDRAL GROUP

Let $n$ be a positive integer, and let $S_n$ be the symmetric group. Recall the hyperoctahedral group

$$B_n = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$$

where $S_n$ acts on $(\mathbb{Z}/2\mathbb{Z})^n$ by permuting the coordinates.

Let $H_n$ be the group consisting of pairs $(a, b) \in (\mathbb{Z}/2\mathbb{Z})^n \times \mathbb{Z}/2\mathbb{Z}$ with group law

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2 + \sum_{1 \leq i < j \leq n} a_{1,i}a_{2,j}).$$

A straightforward computation shows that this law is associative, and that the inverse of $(a, b)$ is

$$(a, b + \sum_{1 \leq i < j \leq n} a_{i,j}).$$

Projection onto the first factor exhibits $H_n$ as a central extension of $(\mathbb{Z}/2\mathbb{Z})^n$ by $\mathbb{Z}/2\mathbb{Z}$.

For $1 \leq i \leq n$ we denote by $e_i$ the $i$th unit vector in $(\mathbb{Z}/2\mathbb{Z})^n$, set $x_i = (e_i, 0) \in H_n$, and $\epsilon = (0, 1) \in H_n$. We denote the unit element $(0, 0) \in H_n$ by 1. We can check that

(2.1) $$x_i^2 = \epsilon^2 = 1, \quad 1 \leq i \leq n,$$

that

(2.2) $$x_i x_j = \epsilon x_j x_i, \quad 1 \leq i, j \leq n, \quad i \neq j,$$

and that

(2.3) $$\epsilon x_i = x_i \epsilon, \quad 1 \leq i \leq n.$$

Furthermore, the relations in Eq. (2.1), Eq. (2.2), and Eq. (2.3) among the generators $x_1, \ldots, x_n, \epsilon$ define the group $H_n$ since using these relations every word in $x_1, \ldots, x_n, \epsilon$ can be brought to the form $x_{i_1} \cdots x_{i_k} \epsilon^\delta$ with $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ and $\delta \in \{0, 1\}$.

We therefore have an action of $S_n$ on $H_n$ by automorphisms via

$$\sigma(x_i) = x_{\sigma(i)}, \quad \sigma(\epsilon) = \epsilon, \quad \sigma \in S_n, \quad 1 \leq i \leq n.$$  

Let $G_n = H_n \rtimes S_n$ be the semidirect product defined using this action. Since $\epsilon \in H_n$ is central and $S_n$-invariant, it lies in the center of $G_n$, so

$$G_n/\langle \epsilon \rangle = G_n/\{1, \epsilon\} \cong (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n = B_n.$$

We see that $G_n$ is a central extension of $B_n$ by $\mathbb{Z}/2\mathbb{Z}$. We denote by $\beta_n$ the class in $H^2(B_n, \mathbb{Z}/2\mathbb{Z})$ corresponding to this extension.

Let $\sigma, \tau \in B_n$ be two elements that commute, let $\tilde{\sigma}, \tilde{\tau}$ be lifts to $G_n$, and define

$$\phi(\sigma, \tau) = [\tilde{\sigma}, \tilde{\tau}] = \tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1} \in \langle \epsilon \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$  

Since $G_n$ is a central extension of $B_n$, the above is indeed independent of the choice of lifts. As every element in $\mathbb{Z}/2\mathbb{Z}$ is its own inverse, we see that

(2.4) $$\phi(\sigma, \tau) = [\tilde{\sigma}, \tilde{\tau}] = [\tilde{\tau}, \tilde{\sigma}]^{-1} = [\tilde{\tau}, \tilde{\sigma}] = \phi(\tau, \sigma).$$

We denote by

$$C_{B_n}(\sigma) = \{\tau \in B_n : \sigma\tau = \tau\sigma\}$$

the centralizer of $\sigma$ in $B_n$.  

Proposition 2.1. For every σ ∈ B_2 we have that φ(σ, τ) is a homomorphism.

Proof. For every τ ∈ B_2 we have

\[ \phi(σ, τ) = \sigma \cdot \phi(σ, 1) + \tau. \]

From Proposition 2.1, Corollary 2.2, and Proposition 2.3 we therefore get that

\[ \phi(σ, τ) = \sigma \cdot \phi(σ, 1) + \tau. \]

so after cancelling, it remains to check that

\[ \phi(σ, τ) = \sigma \cdot \phi(σ, 1) + \tau. \]

After multiplying by σ from the left, we just need to check that [σ, τ] commutes with τ. This is indeed the case because [σ, τ] lies in the central subgroup \{1, e\} of G_2.

□

Corollary 2.2. For every τ ∈ B_2 we have that φ(σ, τ) is a homomorphism.

Proof. For σ, τ ∈ B_2 we get from Eq. (2.5) and Proposition 2.1 that

\[ \phi(στ, τ) = \phi(σ, τ) \cdot \phi(τ, 1). \]

as required.

□

Proposition 2.3. For a k-cycle σ = (i_1 \ldots i_k) ∈ S_n ≤ B_n, and

\[ \tau = e_{i_1} + \cdots + e_{i_k} \in (\mathbb{Z}/2\mathbb{Z})^n ≤ B_n \]

we have φ(σ, τ) = e^k. For every α ∈ S_n ≤ B_n with α(i_1) = i_1, \ldots, α(i_k) = i_k we have φ(α, τ) = 1.

Proof. We take \( \sigma = (i_1 \ldots i_k), \tau = x_{i_1} \cdots x_{i_k} \) and get that

\[ \phi(σ, τ) = \sigma \phi(σ, 1) \cdot τ = e^{k-1}. \]

Taking \( \sigma = α \), we see that

\[ \phi(α, τ) = e^{k-1}. \]

as claimed.

□

Corollary 2.4. Let σ ∈ S_n ≤ B_n whose disjoint cycles are

\[ C_1 = (i_{1,1} \ldots i_{1,j_1}), \ldots, C_j = (i_{j,1} \ldots i_{j,j}), \quad \sum_{r=1}^{j} d_r = n, \]

and let τ ∈ C_B_(n,σ). Then there exists a (unique) choice of τ’ ∈ C_S_(n,σ) and λ_1, \ldots, λ_j ∈ \mathbb{Z}/2\mathbb{Z} such that

\[ (2.5) \quad τ = τ’v, \quad v = \sum_{r=1}^{j} λ_r(e_{i_{r,1}} + \cdots + e_{i_{r,d_r}}) \]

and

\[ \phi(σ, τ) = e^{λ_r(d_r-1)}. \]

Proof. The ability to express τ as in Eq. (2.5) is immediate from the definition of the group law in B_n.

From Proposition 2.1 Corollary 2.2 and Proposition 2.3 we therefore get that

\[ \phi(σ, τ) = \phi(σ, τ’) \cdot \prod_{r=1}^{j} \phi(σ, e_{i_{r,1}} + \cdots + e_{i_{r,d_r}})^{λ_r} \]

\[ = [σ, τ’] \cdot \prod_{r=1}^{j} \prod_{s=1}^{j} \phi(C_s, e_{i_{r,1}} + \cdots + e_{i_{r,d_r}})^{λ_r} = 1 \cdot \prod_{r=1}^{j} e^{λ_r(d_r-1)} = e^{∑_{r=1}^{j} λ_r(d_r-1)} \]

as required.
We keep the notation of Corollary 2.4 and denote by $O_1, \ldots, O_z$ the orbits of the action by conjugation of the subgroup of $S_n$ generated by $\tau'$ on $\{C_1, \ldots, C_j\}$. For $1 \leq y \leq z$ we let $I_y \subseteq \{1, \ldots, n\}$ be the set of all indices that appear in one of the cycles in $O_y$, and define the permutation $\tau'_y \in S_n$ by

$$\tau'_y(i) = \begin{cases} 
\tau'(i) & i \in I_y \\
i & i \notin I_y.
\end{cases}$$

We have a disjoint union

$$\bigcup_{y=1}^z I_y = \{1, \ldots, n\}$$

hence $\tau' = \tau'_1 \cdots \tau'_z$ and the permutations $\tau'_1, \ldots, \tau'_z$ commute. We put 

$$\tau_y = \tau'_y v_y, \quad v_y = \sum_{1 \leq r \leq j \\text{C}_r \in O_y} \lambda_r (e_{i_{r,1}} + \cdots + e_{i_{r,d_r}})$$

and get that

$$(2.6) \quad \tau = \tau'_1 v_1 \cdots \tau'_z v_z$$

where the factors $\tau'_1 v_1, \ldots, \tau'_z v_z$ commute.

3. Proof of Theorem 1.1

It suffices to show, for each $\alpha \in H^1(\tilde{M}, \mathbb{Z}/2\mathbb{Z})$, that the pairing of the branch divisor $D_\pi$ with $\alpha$ vanishes, namely

$$\sum_{\tilde{K} \text{ a component of } \tilde{L}} (e_{\tilde{K}} - 1) \langle [\tilde{K}], \alpha \rangle = 0$$

or equivalently

$$\sum_{K \text{ a component of } L} \sum_{\tilde{K} \text{ a component of } \pi^{-1}(K)} (e_{\tilde{K}} - 1) \langle [\tilde{K}], \alpha \rangle = 0.$$

Associated to $\alpha$ is a degree two covering space $N \to \tilde{M}$. Let $n$ be the degree of $\pi : \tilde{M} \to M$ which is locally constant away from $L$, thus constant. Away from $L$, we get that $N$ is a degree 2 covering space of a degree $n$ covering space, hence has monodromy group contained in the wreath product

$$S_2 \rtimes S_n = (\mathbb{Z}/2\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})^n \times S_n = B_n.$$

We thus have a map $H^2(B_n, \mathbb{Z}/2\mathbb{Z}) \to H^2(M \setminus L, \mathbb{Z}/2\mathbb{Z})$, and we denote by $\gamma \in H^2(M \setminus L, \mathbb{Z}/2\mathbb{Z})$ the image of $\beta_n$.

Consider a tubular neighborhood $Q$ of $L$ and let $S = \partial Q$ be its boundary, a union of tori. Each such torus $T$ corresponds to a unique component $K$ of $L$ - the boundary of a tubular neighborhood of $K$ is $T$. Since $S$ bounds a 3-manifold in $M \setminus L$, i.e. the complement of the tubular neighborhood $Q$, our cohomology class $\gamma$ integrates to 0 on $S$. It follows that

$$\sum_{T \text{ a component of } S} \int_T \gamma = 0.$$

It is therefore sufficient to prove that

$$(3.1) \quad \int_T \gamma = \sum_{\tilde{K} \text{ a component of } \pi^{-1}(K)} (e_{\tilde{K}} - 1) \langle [\tilde{K}], \alpha \rangle.$$
Since $T$ is a torus, a covering of $T$ with monodromy $B_n$, i.e. a homomorphism from $\pi_1(T)$ to $B_n$, is given by a pair of elements $m, \ell \in B_n$ that commute, where $m$ represents a meridian and $\ell$ represents a longitude. From the standard cell decomposition of the torus, we can see that

$$
\int_T \gamma = \phi(m, \ell).
$$

Since the $\mathbb{Z}/2\mathbb{Z}$-covering $N \to \tilde{M}$ is unbranched over every component $\tilde{K}$ of $\pi_1(K)$, the monodromy of the meridian $m$ does not swap the two components of the covering, and therefore $m$ is (up to conjugation) contained in $S_n \leq B_n$.

We shall use here the notation of Corollary 2.4 and the paragraph following it for $\sigma = m$ and $\tau = \ell$, in particular we write $\ell = \ell' v$ as in Eq. (2.5). The components of $\pi_1(K)$ are naturally in bijection with the orbits of the action by conjugation of the subgroup of $S_n$ generated by $\ell'$ on the set of disjoint cycles $\{C_1, \ldots, C_j\}$ of $m$. We denote by $O_{\tilde{K}}$ the orbit corresponding to a component $\tilde{K}$ of $\pi_1(K)$. As in Eq. (2.6), we can write

$$
\ell = \prod_{\tilde{K}} \ell_{\tilde{K}}, \quad \ell_{\tilde{K}} = \ell' v_{\tilde{K}}, \quad v_{\tilde{K}} = \sum_{1 \leq r < j, C_r \in O_{\tilde{K}}} \lambda_r (e_{r,1} + \cdots + e_{r,dr}).
$$

We denote the number of cycles in $O_{\tilde{K}}$ by $t_{\tilde{K}}$, note that each such cycle is of length $e_{\tilde{K}}$, and set

$$
d_{\tilde{K}} = \# \{1 \leq r \leq j : C_r \in O_{\tilde{K}}, \lambda_r = 1\}.
$$

It follows from Corollary 2.4 that $\phi(m, \ell_{\tilde{K}}) \equiv (e_{\tilde{K}} - 1)d_{\tilde{K}} \mod 2$, so from Corollary 2.2 we get that

$$
\phi(m, \ell) = \sum_{\tilde{K} \text{ a component of } \pi_1(K)} \phi(m, \ell_{\tilde{K}}) \equiv \sum_{\tilde{K} \text{ a component of } \pi_1(K)} (e_{\tilde{K}} - 1)d_{\tilde{K}} \mod 2.
$$

It is therefore enough to show that $d_{\tilde{K}} \equiv ([\tilde{K}], \alpha) \mod 2$.

Let $C$ be a longitude curve in a tubular neighborhood of $\tilde{K}$. Then $[C] = [\tilde{K}]$ as homology classes in $H_1(\tilde{M}, \mathbb{Z}/2\mathbb{Z})$, so it suffices to show that $d_{\tilde{K}} \equiv ([C], \alpha) \mod 2$. The projection of $[C]$ to $T$ is $a[m] + t_{\tilde{K}}[\ell]$ for some $a \in \mathbb{Z}$. Thus, the action of $C$ on the covering space $N \to \tilde{M}$ is given by $m^a \ell^t_{\tilde{K}}$. We have

$$
m^a \ell^t_{\tilde{K}} = m^a (\ell' v)^t_{\tilde{K}} = m^a \ell^t_{\tilde{K}} \cdot (v + \ell'(v) + \cdots + \ell'^t_{\tilde{K}} - 1(v)).
$$

The pairing $([C], \alpha)$ is nonzero if and only if the monodromy along $C$ of the covering $N \to \tilde{M}$ is nontrivial, which happens if and only if the action of $m^a \ell^t_{\tilde{K}}$ sends one branch of this covering to the other, and that occurs if and only if the $k$th entry of $v + \ell'(v) + \cdots + \ell'^t_{\tilde{K}} - 1(v)$ is nonzero for some (equivalently, every) index $1 \leq k \leq n$ that belongs to one of the cycles in $O_{\tilde{K}}$. It is therefore sufficient to show that

$$
d_{\tilde{K}} \equiv (v + \ell'(v) + \cdots + \ell'^t_{\tilde{K}} - 1(v))_k \mod 2.
$$

We have

$$(v + \ell'(v) + \cdots + \ell'^t_{\tilde{K}} - 1(v))_k = v_k + \ell'(v)_k + \cdots + \ell'^t_{\tilde{K}} - 1(v)_k = v_k + v_{t-1}(k) + \cdots + v_{t-1}(k).$$

By the orbit-stabilizer theorem, each of the $t_{\tilde{K}}$ cycles in $O_{\tilde{K}}$ contains exactly one of the $t_{\tilde{K}}$ elements $k, \ell'^{-1}(k), \ldots, \ell'^{-t_{\tilde{K}}}(k)$. Thus, from Eq. (2.5) we get that

$$
v_k + v_{t-1}(k) + \cdots + v_{t-1}(k) = \sum_{1 \leq r < j, C_r \in O_{\tilde{K}}} \lambda_r \equiv d_{\tilde{K}} \mod 2,
$$

as desired.
References

[Arm67] J. V. Armitage, *On a Theorem of Hecke in Number Fields and Function Fields*, Inventiones math. 2, 238–246 (1967).

[Fro78] A. Fröhlich, *On parity problems*, Séminaire de Théorie des Nombres de Bordeaux (1978): 1-8.

[FST62] A. Fröhlich, J-P. Serre, J. Tate, *A different with an odd class*, J. für die reine u. angew. Math. 209, 6–7 (1962).

[Mor12] M. Morishita, *Knots and Primes*, An introduction to arithmetic topology, Universitext. Springer, London, 2012.

[Ser79] J-P. Serre, *Local Fields*, GTM 67, Springer-Verlag, 1979.