

## Cyclic quotients of knot like groups

Daryl Cooper<sup>1</sup>

Department of Mathematics, University of California, Santa Barbara, CA 93106, USA

Received 27 July 1994; revised 21 July 1995

---

### Abstract

We generalize a somewhat weakened form of the cyclic surgery theorem to a wider class of knot like groups.

*Keywords:* 3-manifold; Kleinian group

*AMS classification:* Primary 57M50, Secondary 30F40; 57M25

---

### 1. Introduction

We will say that  $(G, H)$  is *knot like* if it satisfies the following conditions:

- $G$  is a finitely generated group,
- $H$  is a subgroup of  $G$  and  $H \cong \mathbb{Z} \times \mathbb{Z}$ ,
- $H$  maps onto the abelianization of  $G$  which is  $\mathbb{Z}$ .

Let  $G$  be a knot like group. Given an element  $\mu \in H$  let  $G(\mu)$  be the quotient of  $G$  obtained by killing  $\mu$ , clearly  $G(\mu) = G(\mu^{-1})$ . In this paper we study the question of when  $G(\mu)$  is cyclic.

**Definition 1.1.** An element  $\alpha$  in  $H$  is a *cyclic class* if  $G(\alpha)$  is cyclic.

This question arises in the theory of Dehn surgery on 3-manifolds where  $G$  is the fundamental group of a 3-manifold  $M$  with boundary a torus  $T$ . Then  $G = \pi_1(M)$  and  $H = \pi_1(T)$ . The Cyclic Surgery Theorem [2] gives a good answer when  $M$  is not Seifert fibered: there are at most 3 distinct pairs  $\mu^{\pm 1}$  which give a cyclic  $G(\mu)$ . In fact the Cyclic Surgery Theorem says rather more. Let  $\langle, \rangle$  be a skew symmetric integer valued pairing of determinant 1 on  $H$ , then if  $G(\mu)$  and  $G(\nu)$  are both cyclic then  $\Delta(\mu, \nu) = |\langle \mu, \nu \rangle| \leq 1$ .

---

<sup>1</sup> Partially supported by the NSF.

**Definition 1.2.** We say that  $(G, H)$  has property NCIS if  $G$  cannot be expressed as a graph of groups with  $H$  in a vertex group. We say that  $(G, H)$  has property NCIS<sup>-</sup> if there is no sequence in  $\text{Hom}(G, \text{SL}_2\mathbb{C})$  which blows up but is bounded on  $H$ .

For example if a knot complement contains no closed incompressible surface then its fundamental group has property NCIS. We will see in Section 2 that NCIS implies NCIS<sup>-</sup> and also explain the meaning of the term “blows up”.

The set  $R(G) = \text{Hom}(G, \text{SL}_2\mathbb{C})$  is an affine algebraic set, let  $R_0$  be a component (in the sense of algebraic sets) of  $R(G)$ . If  $\rho \in R(G)$  kills  $\mu$  then  $\rho$  factors through  $G(\mu)$  and we will often regard  $\rho$  as a homomorphism from  $G(\mu)$ . The main result of this paper is:

**Theorem 1.3.** *Suppose that  $(G, H)$  is a knot like group with property NCIS<sup>-</sup> and that there is a component  $R_0$  of  $R(G)$  such that  $R_0$  contains representations  $\rho, \rho'$  with  $\rho|_H$  parabolic and  $\rho'|_H$  not parabolic and  $\rho'$  irreducible. Suppose  $\mu, \nu \in H$  are primitive and  $G(\mu), G(\nu)$  do not have noncyclic representations in  $R_0$ . Then there is  $\gamma \in H$  such that  $\Delta(\mu, \gamma), \Delta(\nu, \gamma) \leq 1$ .*

**Corollary 1.4.** *With the hypotheses of Theorem 1.3*

- either there are  $\gamma, \delta \in H$  with  $\Delta(\gamma, \delta) = 1$  and for all primitive  $\mu$  for which  $G(\mu)$  has no noncyclic representation in  $R_0$  then  $\pm\mu = \gamma$  or  $\pm\mu = \delta + n\gamma$  for some integer  $n$ ;
- or there are  $p, q, r \in \mathbb{Z}^2$  such that the only points of  $\mathbb{Z}^2$  in the convex hull of  $\{\pm p, \pm q, \pm r\}$  are these points and the origin. Furthermore for all primitive  $\mu$  for which  $G(\mu)$  has no noncyclic representation in  $R_0$  then  $\pm\mu \in \{p \pm q, q \pm r, r \pm p\}$ .

**Addendum 1.5** (to Theorem 1.3). *Suppose in addition to the hypotheses of the theorem that  $\rho'$  may be chosen so that for every  $\alpha \neq 0 \in H$  that  $\text{trace}(\rho'\alpha) \neq \pm 2$ . Then there are only finitely many primitive  $\mu \in H$  such that  $G(\mu)$  does not have a cyclic representation in  $R_0$ .*

The techniques used to prove the Cyclic Surgery Theorem are part algebraic and part 3-manifold topology. We have extracted and substantially modified the algebraic argument to obtain information about a more general class of groups. The technique is to study representations of  $G$  in  $\text{SL}_2\mathbb{C}$  and reduce the question to one about divisibility properties of integer polynomials in 2 variables. These questions are resolved using “geometry of numbers” type arguments based on elementary estimates involving complex roots of unity. Here are some examples of knot like groups:

### 1.1. Examples

(1) The fundamental group of the trefoil knot has a presentation  $\langle \alpha, \beta: \alpha^2 = \beta^3 \rangle$  and the boundary torus is generated by a meridian  $\mu = \alpha\beta^{-1}$  and  $\lambda = \alpha^2\mu^{-6}$ . The element  $\mu \cdot (\mu^6\lambda)^q$  is a cyclic class for every integer  $q$ . This is because  $\mu^6\lambda$  is central thus the relation  $\mu \cdot (\mu^6\lambda) = 1$  implies  $\mu$  is central and thus abelianizes the group which is

normally generated by  $\mu$ . This is an example of a knot with Seifert fibered complement to which the Cyclic Surgery Theorem does not apply. Theorem 1.3 applies to this example, but the extra hypothesis of the addendum is not satisfied.

(2) The  $(-2, 3, 7)$  pretzel knot has a hyperbolic complement. Using  $\lambda, \mu$  for the longitude and meridian, then Fintushel and Stern have shown that  $\mu, \mu\lambda^{18}, \mu\lambda^{19}$  are cyclic classes. In addition the class  $\mu\lambda^{20}$  is not a cyclic class but a computer calculation reveals that there is no noncyclic representation into  $SL_2\mathbb{C}$  of the knot group which kills this class.

(3) Let  $(G, H)$  be the fundamental group of a (hyperbolic knot, boundary torus) containing no nonboundary parallel closed incompressible surface and take  $G' = G *_H (\mathbb{Z} \times \mathbb{Z})$  where the amalgamation map  $H \rightarrow \mathbb{Z} \times \mathbb{Z}$  is an isomorphism onto  $n(\mathbb{Z} \times \mathbb{Z})$  for some positive integer  $n$ . Let  $H'$  be the image of the  $\mathbb{Z} \times \mathbb{Z}$  subgroup in the amalgamated product. Then  $(G', H')$  is knot like, and if  $\mu \in H$  is a cyclic class for  $(G, H)$  and if  $\nu \in H'$  and if  $\mu$  is a multiple of  $\nu$  then  $\nu$  is a cyclic class for  $(G', H')$ . This shows that the hypothesis in Theorem 1.3 that the cyclic classes be primitive is necessary.

(4) Let  $(G, H)$  be as in the preceding example and let  $K$  be a perfect group then set  $G' = G \times K$  and let  $H'$  be the group generated by  $\{\lambda\alpha, \mu\beta\}$  where  $\lambda, \mu$  generated  $H$  and  $\alpha, \beta \in K$  commute.

(5) Let  $(G, H)$  satisfy the hypotheses of the theorem and add a generator  $\beta$  and a relation  $\mu = \beta.\alpha.\beta^{-1}.\alpha.\beta$  to  $G$  where  $\alpha$  is any element of  $G$  and  $\mu$  is a meridian. Let  $G'$  be the resulting group and  $H'$  the image of  $H$  in  $G'$ . A calculation reveals that the restriction map  $i^* : R(G') \rightarrow R(G)$  is onto. Thus if  $G$  is the fundamental group of a hyperbolic knot then  $G$  is a subgroup of  $G'$ , and it is then clear that  $(G', H')$  is knot like. Suppose that a sequence  $\rho_n \in R(G')$  blows up, then some calculations reveal that  $\rho_n|G$  also blows up. Therefore Theorem 1.3 and Addendum 1.5 apply to  $(G', H')$ .

## 2. Curves of eigenvalues

Choose a basis  $\{\lambda, \mu\}$  of  $H$ . Since  $H$  is abelian we may conjugate  $\rho \in R(G)$  so that  $\rho|H$  is upper triangular, thus

$$\rho(\lambda) = \begin{bmatrix} \ell & * \\ 0 & \ell^{-1} \end{bmatrix}, \quad \rho(\mu) = \begin{bmatrix} m & * \\ 0 & m^{-1} \end{bmatrix},$$

the numbers  $\ell^{\pm 1}, m^{\pm 1}$  are the eigenvalues of  $\rho(\lambda), \rho(\mu)$  respectively. Note that the conjugacy used to make  $\rho(\lambda), \rho(\mu)$  upper triangular is not unique. In particular the pair  $(\ell, m)$  may be replaced by the pair  $(\ell^{-1}, m^{-1})$  by a suitable conjugacy. We will define a double valued eigenvalue map by

$$ev : R(G) \rightarrow (\mathbb{C} - 0)^2 \quad \text{by } ev(\rho) = (\ell(\rho), m(\rho)).$$

**Proposition 2.1.** *Suppose that  $R_0$  contains an irreducible representation and  $p, q$  are coprime integers, and that  $\exists \rho \in R_0$  with  $ev(\rho) = (\ell, m)$  and  $\ell^p m^q = \pm 1$  and either  $\ell$  or  $m$  is not  $\pm 1$ . Then there is a noncyclic  $\rho$  in  $R_0$  such that  $\rho(\lambda^p \mu^q) = \pm I$ . In particular  $G(\lambda^p \mu^q)$  is not cyclic.*

**Proof.** It follows from the hypotheses on  $\ell, m$  that  $\rho|_H$  is diagonalizable and therefore that  $\rho(\lambda^p \mu^q) = \pm I$ . If  $\rho$  does not have cyclic image in  $\text{PSL}_2\mathbb{C}$  the result is now clear. Otherwise we can conjugate so that  $\rho = \rho_{ab}$  is diagonal.

A representation  $\rho$  into  $\text{SL}_2\mathbb{C}$  is reducible if and only if the character of  $\rho$  restricted to the commutator subgroup of  $G$  takes only the value 2. The function  $X_\alpha : R_0 \rightarrow \mathbb{C}$  given by  $X_\alpha(\rho) = \text{trace}(\rho\alpha)$  is a polynomial therefore  $S = X_\alpha^{-1}(2)$  is an algebraic subset of  $R_0$ . Since  $R_0$  is irreducible either  $S = R_0$  or  $S$  is an algebraic subset of  $R_0$  with  $\dim S < \dim R_0$  and  $R_0 - S$  dense in  $R_0$ . Since  $R_0$  contains an irreducible representation  $\rho$  there is a commutator  $\alpha \in G$  with  $\text{trace}(\rho\alpha) \neq 2$ , thus the set of irreducible representations is dense in  $R_0$ .

It follows that there is a sequence of irreducible representations  $\rho_n \in R_0$  which converge to  $\rho_{ab}$ . Fix a generating set  $\alpha_1, \alpha_2, \dots, \alpha_k$  of  $G$  and choose  $A_n \in \text{SL}_2\mathbb{C}$  such that  $\rho'_n = A_n \rho_n A_n^{-1}$  has the following properties:

- $\rho'_n|_H$  is diagonal;
- for  $n$  large the off-diagonal entries of  $\rho'_n(\alpha_i)$  have modulus at most 1 for  $1 \leq i \leq k$ ;
- there is  $i_n$  such that one of the off-diagonal entries of  $\rho'_n(\alpha_{i_n})$  has modulus 1.

Then choose a subsequence  $n_k$  such that  $\rho'_{n_k}(\alpha_i)$  converges for each  $i$ . Since  $R_0$  is closed in the classical topology, the subsequence  $\rho_{n_k}$  converges to a representation  $\rho_{\text{red}}$  in  $R_0$ . Since the normal closure of  $H$  is  $G$  it follows that  $\rho_{\text{red}}$  does not kill  $H$  therefore there is  $h \in H$  such that  $\rho(h) \neq \pm I$ . Also  $\rho_{\text{red}}(\alpha_{i_n})$  is not diagonal so  $\rho_{\text{red}}$  has noncyclic image.  $\square$

Recall that a subset  $A$  of  $\mathbb{C}^n$  is *constructible* if

- either  $A$  is finite;
- or  $A = B - C$  where  $B$  is an affine algebraic set, and  $C$  is a constructible set of smaller dimension than  $A$ .

We now show that the set  $C = \text{ev}(R_0)$  is constructible. Let  $U$  be the algebraic subset of  $R_0$  of representations which are upper triangular on  $H$ . Then  $C = \text{ev}(U)$  because  $R_0$  is a Zariski open subset of  $R(G)$  and is therefore closed under conjugacy. Now  $\text{ev}|_U$  is given by a coordinate projection namely take the top left entries from the matrices  $\rho(\lambda), \rho(\mu)$ . Coordinate projection is a polynomial map, and the image of an affine algebraic subset under a polynomial map is a constructible set.

It follows that the closure of  $C$  is an affine algebraic set  $\overline{C}$ . If  $\dim_{\mathbb{C}} C = 0$  then  $C$  consists of finitely many points. In this case our methods give no information. If  $\dim_{\mathbb{C}} C = 1$  or 2 then  $C$  contains a constructible subset of (complex) dimension 1. In what follows we will work with a 1-dimensional constructible subset of  $C$ , which we also denote by  $C$ .

Thus  $C = \overline{C} - F$  where  $F$  is a finite subset of  $\overline{C}$ . We claim that if  $G$  has property NCIS<sup>-</sup> then  $F$  is contained in  $\mathbb{C} \times 0 \cup 0 \times \mathbb{C}$ . This follows in a standard way from the Culler–Shalen theory [4, 2.2.1]. Briefly if  $x \in F - (\mathbb{C} \times 0 \cup 0 \times \mathbb{C})$  then there is a sequence  $\rho_n \in R_0$  with  $\lim_{n \rightarrow \infty} \text{ev}(\rho_n) = x$ . Then  $\rho_n$  must *blow up*, i.e., there is  $\alpha \in G$  with  $\text{trace}(\rho_n \alpha) \rightarrow \infty$  otherwise we could conjugate  $\rho_n$  to obtain a subsequence which converges to a representation  $\rho$  with  $\text{ev}(\rho) = x$  giving a contradiction see [3]. One

obtains from the sequence  $\rho_n$  via Bass–Serre theory an action without edge inversions of  $G$  on a simplicial tree and this gives a graph of groups decomposition of  $G$ . Since  $\rho_n|_H$  has bounded trace,  $H$  is contained in a conjugate of a vertex group, contradicting property NCIS<sup>-</sup> for  $G$ . This shows NCIS implies NCIS<sup>-</sup>.

**Proposition 2.2.** *Suppose that  $(G, H)$  is a knot like group with property NCIS<sup>-</sup> and that there is a component  $R_0$  of  $R(G)$  such that  $R_0$  contains representations  $\rho, \rho'$  with  $\rho|_H$  parabolic and  $\rho'|_H$  not parabolic. Then there is an affine curve  $C^*$  in  $(\mathbb{C} - 0)^2$  lying in  $\text{ev}(R_0)$ .*

**Proof.** The set  $(\mathbb{C} - 0)^2$  is an affine algebraic variety. We have that  $\text{ev}(\rho) \neq \text{ev}(\rho')$  thus  $\text{ev}(R_0)$  contains more than one point, but  $R_0$  is connected therefore  $\text{ev}(R_0)$  has complex dimension at least 1. The preceding discussion implies the existence of  $C^*$ .  $\square$

**Definition 2.3.** Let  $\text{ab}: G \rightarrow \mathbb{Z}$  be the abelianization map. We will call  $\nu \in H$  odd if  $\text{ab}(\nu)$  is odd.

Given  $\rho \in R(G)$  define  $\rho^-$  by  $\rho^-(\alpha) = (-1)^{\text{ab}(\alpha)}\rho(\alpha)$ . This is clearly a representation and if  $\lambda$  is even and  $\mu$  is odd and  $\text{ev}(\rho) = (\ell, m)$  then  $\text{ev}(\rho^-) = (\ell, -m)$ . This defines an involution  $\tau: R(G) \rightarrow R(G)$ , given by  $\tau(\rho) = \rho^-$ . Observe that  $\rho(\nu) = \pm I \Leftrightarrow \rho^-(\nu) = \pm I$ . We now define a new curve  $C = C^* \cup \tau_{\text{ev}}(C^*)$  in  $R(G)$  which is invariant under  $\tau_{\text{ev}}$ , where  $\tau_{\text{ev}}(\ell, m) = (\ell, -m)$ .

Now the curve  $C$  in  $(\mathbb{C} - 0)^2$  is the zero set of a Laurent polynomial  $A(\lambda, \mu)$ , and it is shown in [1] that this polynomial can be chosen to have integer coefficients. We will now study the relationship of this polynomial to cyclic classes.

**Lemma 2.4.** *If  $\mu$  is odd and  $\lambda$  is even, then  $A(\lambda, \mu)$  involves only even powers of  $\mu$ .*

**Proof.** Note that  $\tau_{\text{ev}}(C) = C$  thus  $(\ell, m) \in \text{ev}(C) \Leftrightarrow (\ell, -m) \in \text{ev}(C)$  which implies the result.  $\square$

**Proposition 2.5.** *With the hypotheses of Proposition 2.2, suppose  $(\ell, m)$  is a zero of  $A(\lambda, \mu)$  and  $\ell^p m^q = \pm 1$  and either  $\ell$  or  $m$  is not  $\pm 1$ . Then there is a noncyclic  $\rho$  in  $R_0 \cup \tau(R_0)$  such that  $\rho(\lambda^p \mu^q) = I$ . In particular  $\lambda^p \mu^q$  is not a cyclic class.*

**Proof.** There is  $\rho \in R_0 \cup \tau(R_0)$  with  $\text{ev}(\rho) = (\ell, m)$  so the result follows from Proposition 2.1.  $\square$

**Corollary 2.6.** *If  $\mu$  is a cyclic class then  $A(\lambda, \mu = \pm 1) = 0 \Rightarrow \lambda = 0, \pm 1$ .*

**Corollary 2.7.** *Suppose the hypotheses of Proposition 2.2 and that  $\mu$  is an odd cyclic class then*

$$A(\lambda, 1) = a\lambda^b(\lambda - 1)^c(\lambda + 1)^d$$

and  $a \neq 0$  and at least one of  $c, d$  is nonzero.

**Proof.** By the previous corollary, there are integers  $a, b, c$  possibly zero, so that  $A(\lambda, 1)$  is as claimed. If  $a = 0$  then there is a representation with  $\mu = 1$  and  $\lambda$  arbitrary which by Proposition 2.1 contradicts that  $\mu$  is a cyclic class, hence  $a \neq 0$ . The hypotheses of Proposition 2.2 gives a representation  $\rho$  with  $\rho|_H$  parabolic thus  $\text{trace}(\rho(\mu)) = \pm 2$ . Replacing  $\rho$  by  $\rho^-$  if needed, we may assume that  $\text{trace}(\rho(\mu)) = 2$ . Now  $\text{trace}(\rho(\lambda)) = \pm 2$  and so either  $\text{ev}(\rho) = (\lambda, \mu) = (1, 1)$  or  $(-1, 1)$  is a zero of  $A(\lambda, \mu)$  and thus at least one of  $c, d$  is not zero.  $\square$

We will often change the basis of  $H$ . If  $\kappa, \nu$  is a new basis then  $\kappa = \lambda^p \mu^q, \nu = \lambda^r \mu^s$  and  $ps - qr = 1$ . Using these coordinates, the curve  $C$  in  $(\mathbb{C} - 0)^2$  is the zero set of  $B(\kappa, \nu)$  where  $B(\kappa, \nu) = A(\kappa^s \nu^{-q}, \kappa^{-r} \nu^p)$ .

### 3. Odd cyclic classes

From now all the cyclic classes that we consider are primitive. In this section we assume that there is an odd cyclic class, and we choose a basis  $\lambda, \mu$  of  $H$  so that  $\mu$  is an odd cyclic class and  $\lambda$  is even. We will consider the case of even cyclic classes later. From Corollary 2.7 it follows that

$$A(\lambda, 1) = a \cdot \lambda^b (\lambda - 1)^c (\lambda + 1)^d.$$

Now  $(\mu - 1)[A(\lambda, \mu) - A(\lambda, 1)]$  and so by Lemma 2.4  $(\mu^2 - 1)[A(\lambda, \mu) - A(\lambda, 1)]$  thus

$$A(\lambda, \mu) = a \cdot \lambda^b (\lambda - 1)^c (\lambda + 1)^d + (\mu^2 - 1)B(\lambda, \mu) \tag{1}$$

where  $B(\lambda, \mu)$  is some integer polynomial. Suppose that  $\nu = \lambda^p \mu^q$  is a cyclic class with  $\text{hcf}(p, q) = 1$  then there are integers  $r, s$  such that  $ps - qr = 1$ . Set  $\kappa = \lambda^r \mu^s$  then  $\lambda = \kappa^{-q} \nu^s$  and  $\mu = \kappa^p \nu^{-r}$ . Then

$$\nu = \pm 1 \quad \text{and} \quad A(\nu^s \kappa^{-q}, \nu^{-r} \kappa^p) = 0 \Rightarrow \kappa = 0, \pm 1.$$

Putting  $\nu = 1$  it follows that

$$A(\kappa^{-q}, \kappa^p) = u \cdot \kappa^{v_1} (\kappa - 1)^{v_2} (\kappa + 1)^{v_3}$$

combining this with (1) gives

$$\begin{aligned} & u \cdot \kappa^{v_1} (\kappa - 1)^{v_2} (\kappa + 1)^{v_3} \\ &= a \kappa^{-qb} (\kappa^{-q} - 1)^c (\kappa^{-q} + 1)^d + (\kappa^{2p} - 1)B(\kappa^{-q}, \kappa^p). \end{aligned} \tag{2}$$

The following is the main algebraic result that we need.

**Lemma 3.1.** *Suppose that  $\text{hcf}(p, q) = 1$  and that there are integers (not all zero)  $a, b, c, d \geq 0$  and  $m, n \neq 0$  such that*

$$m(1 - x)^a (1 + x)^b = n(1 - x^q)^c (1 + x^q)^d$$

in  $\mathbb{Z}[x]/\langle x^{2p} - 1 \rangle$ . Then  $q \equiv \pm 1, \pm 2 \pmod{p}$ .

**Proof.** We first deal with the case that  $q$  is odd. Set  $\omega = e^{\pi i/p}$  and  $f(x) = (1-x)^a(1+x)^b/(1-x^q)^c(1+x^q)^d$  then  $f(\omega^t) = n/m = K$  whenever  $p \nmid t$ . Now  $(-\omega)^{2p} = 1$  and  $(-\omega)^q = -\omega^q$  thus

$$K^2 = f(\omega)f(-\omega) = (1-\omega^2)^{a+b}/(1-\omega^{2q})^{c+d}. \tag{3}$$

Let  $r, s$  be chosen so that  $2pr + qs = 1$  then

$$K^2 = f(\omega^s)f(-\omega^s) = (1-\omega^{2s})^{a+b}/(1-\omega^{2qs})^{c+d}.$$

We have  $qs \equiv 1 \pmod{2p}$ , thus

$$K^2 = f(\omega^s)f(-\omega^s) = (1-\omega^{2s})^{a+b}/(1-\omega^2)^{c+d}. \tag{4}$$

Combining (3) and (4) gives

$$(1-\omega^2)^{a+b+c+d} = (1-\omega^{2s})^{a+b}(1-\omega^{2q})^{c+d}. \tag{5}$$

Now  $|1-\omega^2| \leq |1-\omega^{2q}|, |1-\omega^{2s}|$  and so for equality in (5) either  $2q \equiv \pm 2 \pmod{2p}$  or  $2s \equiv \pm 2 \pmod{2p}$ . In either case this gives  $q \equiv \pm 1 \pmod{p}$ .

Now consider the case that  $q$  is even. Let  $\omega = e^{2\pi i/p}$  then since replacing  $\omega$  by  $-\omega$  does not change  $\omega^q$

$$m(1-\omega)^a(1+\omega)^b = n(1-\omega^q)^c(1+\omega^q)^d = m(1+\omega)^a(1-\omega)^b. \tag{6}$$

hence

$$\left(\frac{1+\omega}{1-\omega}\right)^{b-a} = 1$$

and considering moduli we see that  $a = b$ . Now let  $\omega$  be a  $p$  root of unity other than 1, then

$$K = f(\omega) = (1-\omega^2)^a/(1-\omega^q)^c(1+\omega^q)^d. \tag{7}$$

Now choose  $s$  so that  $qs \equiv 1 \pmod{p}$  then

$$\begin{aligned} K &= f(\omega^s) = (1-\omega^{2s})^a/(1-\omega^{qs})^c(1+\omega^{qs})^d \\ &= (1-\omega^{2s})^a/(1-\omega)^c(1+\omega)^d. \end{aligned} \tag{8}$$

Combining (7) and (8) gives:

$$(1-\omega^2)^a(1-\omega)^c(1+\omega)^d = (1-\omega^{2s})^a(1-\omega^q)^c(1+\omega^q)^d. \tag{9}$$

**Lemma 3.2.** *If  $p$  is odd and  $p \nmid r$  then*

$$k(r) = |1 - e^{2\pi ir/p}|^c |1 + e^{2\pi ir/p}|^d$$

*has a minimum either when  $r \equiv \pm 1$  or when  $r \equiv \pm(p-1)/2 \pmod{p}$  or both.*

**Proof.** The functions  $g_{\pm}(\theta) = |1 \pm e^{i\theta}|$  for  $0 \leq \theta \leq \pi$  are easily seen to be convex. It follows that

$$h(\theta) = |1 - e^{i\theta}|^c |1 + e^{i\theta}|^d$$

is convex. Thus the only possible local minima of  $h$  are  $\theta = 0, \pi$  and it follows that  $k(r)$  is a minimum when  $h(\pm 2\pi r/p)$  is a minimum which therefore either occurs when  $r \equiv \pm 1$  or  $r \equiv \pm(p-1)/2 \pmod{p}$ .  $\square$

The first case we consider is that the minimum of  $k$  is when  $r \equiv \pm(p-1)/2$ . Set  $\omega = e^{2\pi i(p-1)/2p}$  then  $\omega^2 = e^{-2\pi i/p}$ . Using Lemma 3.2

$$|(1 - \omega)^c(1 + \omega)^d| \leq |(1 - \omega^q)^c(1 + \omega^q)^d| \tag{10}$$

from (9) it follows that

$$|1 - \omega^2| \geq |1 - \omega^{2s}|. \tag{11}$$

Thus  $2s \equiv \pm 1, \pm 2 \pmod{p}$  but since  $qs \equiv \pm 1$  it follows that  $q \equiv \pm 2, \pm 1 \pmod{p}$  as required.

The remaining case is that the minimum of  $k(r)$  occurs when  $r \equiv \pm 1$ . Set  $\omega = e^{2\pi i/p}$  then again we must have

$$|1 - \omega^2| \geq |1 - \omega^{2s}| \tag{12}$$

and the conclusion follows as before.  $\square$

**Lemma 3.3.** *Suppose  $p \geq 5$  and that there are integers  $a, b, c, d \geq 0$  and  $m, n \neq 0$  with*

$$m(1-x)^a(1+x)^b = n(1-x)^c(1+x)^d$$

*in  $\mathbb{Z}[x]/\langle(x^p - 1)\rangle$ . Then  $a = c, b = d$ .*

**Proof.** Let  $\omega = e^{t2\pi i/p}$  where  $0 < t < p$  is chosen so that  $\omega, \omega^2 \neq \pm 1$  then combining the given equation for  $x = \omega$  and  $x = \omega^2$  gives

$$\begin{aligned} (1 - \omega)^{a-c}(1 + \omega)^{b-d} &= (1 - \omega^2)^{a-c}(1 + \omega^2)^{b-d} \\ \Rightarrow (1 + \omega)^{b-d+c-a} &= (1 + \omega^2)^{b-d} \\ \Rightarrow (b - d + c - a) \log |1 + \omega| &= (b - d) \log |1 + \omega^2|. \end{aligned}$$

This gives a linear equation in  $(b-d)$  and  $(c-a)$ . Using the two values  $\omega = \omega_1 = e^{2\pi i/p}$  and  $\omega = \omega_2 = e^{2\pi i(p-1)/2p}$  we see that (since  $p \geq 5$ )

$$\frac{\log |1 + \omega_1|}{\log |1 + \omega_1^2|} < 1, \quad \frac{\log |1 + \omega_2|}{\log |1 + \omega_2^2|} > 1.$$

It follows that  $b - d = 0 = a - c$  which gives the result.  $\square$

**Addendum 3.4** (to Lemma 3.1). *With the hypotheses of Lemma 3.1, if  $p \geq 5$  and  $q \equiv \pm 2 \pmod{p}$  then  $d = 0$ .*



**Proof.** The hypothesis of Lemma 3.1 is that

$$\begin{aligned} m(1-x)^a(1+x)^b &= n(1-x^q)^c(1+x^q)^d \\ \Rightarrow m(1-x)^a(1+x)^b &= n(-x^q)^c(1-x^{-q})^c x^{qd}(1+x^{-q})^d \\ \Rightarrow m^{2p}(1-x)^{2pa}(1+x)^{2pb} &= n^{2p}(1-x^{-q})^{2pc}(1+x^{-q})^{2pd}. \end{aligned}$$

The last step uses that  $x^{2p} = 1$ . We may use this to reduce to the case  $q \equiv 2 \pmod p$  and since  $\text{hcf}(p, q) = 1$  it follows that  $p$  is odd. We will now work in the quotient  $\mathbb{Z}[x]/\langle(x^p - 1)\rangle$  of  $\mathbb{Z}[x]/\langle(x^{2p} - 1)\rangle$ . Then we may assume that  $q = 2$  and the conclusion of Lemma 3.1 is that

$$m(1-x)^a(1+x)^b = n(1-x^2)^c(1+x^2)^d$$

replacing  $x$  by  $-x$  gives

$$m(1+x)^a(1-x)^b = n(1-x^2)^c(1+x^2)^d$$

and combining these gives

$$m^2(1-x^2)^{a+b} = n^2(1-x^2)^{2c}(1+x^2)^{2d}.$$

Choose  $s$  so that  $2s \equiv 1 \pmod p$  and replace  $x$  by  $x^s$  in the above to get

$$m^2(1-x)^{a+b} = n^2(1-x)^{2c}(1+x)^{2d}.$$

Now Lemma 3.3 implies that  $2d = 0$ .  $\square$

**Lemma 3.5.** *With the hypotheses of Theorem 1.3, if  $\nu = \lambda^p \mu^q$  is a primitive cyclic class, and  $\mu$  is an odd primitive cyclic class then  $q \equiv \pm 1 \pmod p$ .*

**Proof.** If  $p \leq 4$  and using that  $q$  is coprime to  $p$  there is nothing to prove. From equation (2) and Lemma 3.1 we have that  $q \equiv \pm 1, \pm 2 \pmod p$ . So suppose that  $q \equiv \pm 2 \pmod p$  then there are  $r, s$  such that  $ps - qr = 1$  and we may choose  $s$  to be odd. This is because either  $q$  is even and  $s$  must be odd, or else  $q$  is odd and we can replace  $(r, s)$  by  $(r - p, s - q)$ . We have from Lemma 3.1 and Addendum 3.4 that  $d = 0$  in (1) and putting  $\nu = -1$  gives

$$\begin{aligned} A((-1)^s \kappa^{-q}, (-1)^r \kappa^p) \\ &= u' \cdot \kappa^{v'} (\kappa - 1)^{v'_2} (\kappa + 1)^{v'_3} \\ &= \pm a \kappa^{-qb} ((-1)^s \kappa^{-q} - 1)^c + (\kappa^{2p} - 1) B(-\kappa^{-q}, \pm 1 \kappa^p). \end{aligned}$$

Since  $s$  is odd Addendum 3.4 now implies that  $c = 0$  also. This contradicts Corollary 2.7.  $\square$

#### 4. Even cyclic classes

Throughout this section we will assume that  $\mu$  is an even primitive cyclic class, and we extend Lemma 3.5 to the case that  $\mu$  is even.

**Lemma 4.1.** *With the hypotheses of Theorem 1.3, if  $\nu = \lambda^p \mu^q$  is a primitive cyclic class, and  $\mu$  is an even primitive cyclic class then  $q \equiv \pm 1 \pmod p$ .*

**Proof.** Let  $\lambda$  be chosen so that  $\{\lambda, \mu\}$  is a basis of  $H$ , thus  $\lambda$  is odd since  $\mu$  is even. Since  $\mu$  is a cyclic class by Corollary 2.6  $\mu = \pm 1 \Rightarrow \lambda = \pm 1, 0$ . Now by Lemma 2.4 the  $A$  polynomial expressed in terms of  $\lambda, \mu$  involves only even powers of  $\lambda$  since  $\lambda$  is odd and  $\mu$  is even. Thus

$$A(\lambda, \mu) = a_1 \cdot \lambda^{b_1} (1 - \lambda^2)^{c_1} (\mu - 1) + a_2 \cdot \lambda^{b_2} (1 - \lambda^2)^{c_2} (\mu + 1) + (\mu^2 - 1)B(\lambda, \mu).$$

Here  $a_1, a_2 \in \frac{1}{2}\mathbb{Z}$  and if they are not integral, we may multiply by 2 to arrange that they are integral. Now we repeat the earlier analysis of a cyclic class  $\nu = \lambda^p \mu^q$ , with the notation used before we get

$$\begin{aligned} u \cdot \kappa^{v_1} (1 - \kappa)^{v_2} (1 + \kappa)^{v_3} &= a_1 \cdot \kappa^{-qb_1} (1 - \kappa^{-2q})^{c_1} (\kappa^p - 1) \\ &\quad + a_2 \cdot \kappa^{-qb_2} (1 - \kappa^{-2q})^{c_2} (\kappa^p + 1) \\ &\quad + (\kappa^{2p} - 1)B(\kappa^{-q}, \kappa^p). \end{aligned} \tag{13}$$

We may replace  $\kappa$  by  $-\kappa$  in the above equation to ensure that  $v_2 \geq v_3$ . We claim that both  $a_1, a_2$  must be nonzero. Otherwise substitute for  $\kappa$  a suitable  $2p$  root of unity  $\kappa \neq \pm 1$  to make the right hand side vanish. This implies that  $u = 0$  and hence that  $a_1 = 0 = a_2$  and thus

$$A(\lambda, \mu) = (\mu^2 - 1)B(\lambda, \mu).$$

Now  $\mu = 1$  and  $\lambda$  arbitrary satisfies this equation, but  $\mu$  is a cyclic class and Corollary 2.6 yields a contradiction which proves the claim. We need the following:

**Lemma 4.2.** *Suppose that  $\text{hcf}(p, q) = 1$  and that there are integers  $a \geq b \geq 0, c > 0$  and  $m, n \neq 0$  with*

$$m(1 - x)^a (1 + x)^b = n(1 - x^{2q})^c$$

*in  $\mathbb{Z}[x]/\langle x^p + 1 \rangle$ . Then  $q \equiv \pm 1 \pmod p$ .*

**Proof.** The result is obvious for  $p < 5$ . Suppose that  $x, y \in \mathbb{C}$  with  $x^p = -1 = y^p$  then

$$(1 - x^2)^b (1 - x)^{a-b} (1 - y^{2q})^c = (1 - y^2)^b (1 - y)^{a-b} (1 - x^{2q})^c.$$

There are integers  $r, s$  such that  $pr + qs = 1$ , as in the proof of Lemma 3.5 we may assume that  $s$  is odd. Put  $x = e^{\pi i/p}$  and  $y = x^s$  then  $x^p = -1 = y^p$  then we have  $|1 - x| \leq |1 - y|$  with equality only if  $y = x^{\pm 1}$ . Furthermore  $|1 - x^2| \leq |1 - y^2|$ , this is because for parity reasons  $y^2 \neq x^{\pm 1}$ , and equality holds only if  $y = x^{\pm 1}$ . Finally  $y^{2q} = x^{2qs} = x^{2-2pr} = x^2$  thus  $|1 - y^{2q}| \leq |1 - x^{2q}|$ . Taking moduli in the above equation we thus see that for equality if either  $a - b \neq 0$  or  $b \neq 0$  then  $y = x^{\pm 1}$ . Since  $c \neq 0$  one of  $a$  or  $b$  must be nonzero. Thus for equality  $s \equiv \pm 1 \pmod p$  and thus  $q \equiv \pm 1 \pmod p$ .  $\square$

If  $c_1 \neq 0$  then Lemma 4.2 proves Lemma 4.1. If  $c_1 = 0$  then (13) gives

$$u.\kappa^{v_1}(1 - \kappa)^{v_2}(1 + \kappa)^{v_3} = a_1.\kappa^{-qb_1}(\kappa^p - 1) + a_2.\kappa^{-qb_2}(1 - \kappa^{-2q})^{c_2}(\kappa^p + 1) + (\kappa^{2p} - 1)B(\kappa^{-q}, \kappa^p)$$

now suppose that  $\kappa \in \mathbb{C}$  with  $\kappa^p = -1$  then

$$u.\kappa^{v_1}(1 - \kappa)^{v_2}(1 + \kappa)^{v_3} = a_1.\kappa^{-qb_1}(-2)$$

taking the  $2p$ th power of this gives

$$m(1 - \kappa)^{2pv_2}(1 + \kappa)^{2pv_3} = n$$

as  $\kappa$  varies over  $p$ th roots of  $-1$  one easily obtains from this that  $v_2 = v_3 = 0$ . This implies that  $c_2 = 0$  thus

$$A(\lambda, \mu) = a_1.\lambda^{b_1}(\mu - 1) + a_2.\lambda^{b_2}(\mu + 1) + (\mu^2 - 1)B(\lambda, \mu).$$

Now there is a representation which is parabolic on  $H$  say  $\mu = 1$  for this representation. Then  $0 = a_2$ , which we saw above was impossible. Hence  $c_1 \neq 0$  and the proof of Lemma 4.1 is complete.  $\square$

### 5. Proofs of main results

**Proof of Theorem 1.3.** By Lemmas 3.5 and 4.1  $\nu = \lambda^p \mu^q$  with  $q \equiv \pm 1 \pmod p$  thus  $q = np \pm 1$ . We may suppose that  $\lambda$  was chosen so that  $\langle \mu, \lambda \rangle = 1$ . Then take  $\gamma = \lambda \mu^n$  then  $\nu = \gamma^p \mu^{\pm 1}$  thus  $\langle \mu, \gamma \rangle = 1$  and  $\langle \nu, \gamma \rangle = \pm 1$  as asserted.  $\square$

Suppose that  $0 \neq \alpha \in \mathbb{Z}^2$  then

$$L(\alpha) = \{ \beta \in \mathbb{R}^2 : \Delta(\alpha, \beta) = 1 \}$$

is the union of two parallel lines symmetric with respect to the origin. If  $\alpha$  and  $\beta$  are primitive cyclic classes then by Theorem 1.3 each component of  $L(\alpha)$  meets  $L(\beta)$  in a lattice point. Furthermore, the lattice points lying between the two components of  $L(\alpha)$  all lie on the line through the origin parallel to  $L(\alpha)$ . In particular there is at most one lattice point on each component of  $L(\beta)$  lying between the 2 points of intersection of that component with  $L(\alpha)$ . Symmetric statements hold for  $L(\alpha)$ . The following result in plane geometry is used to deduce Corollary 1.4 from Theorem 1.3.

**Proposition 5.1.** *Let  $L_i$  be a collection of lines in  $\mathbb{R}^2$  with the following properties.*

- (i) *Each  $L_i$  contains 2 lattice points but not the origin;*
- (ii)  *$L_i \cap (L_j \cup -L_j)$  contains a lattice point;*
- (iii) *let  $L_i^0$  be the line parallel to  $L_i$  passing through the origin, then  $L_i^0$  contains all the lattice points lying between  $L_i$  and  $-L_i$ .*

*Then there are two cases:*

- *Either there is a lattice point  $a$  which lies in  $(L_i \cup -L_i)$  for all except possibly one value of  $i$  and this remaining line pair is parallel to a  $(-a)$ ,*

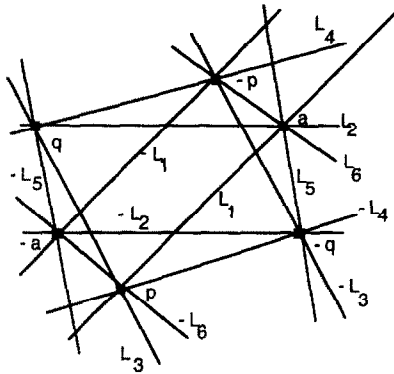


Fig. 1.

- or there are  $p, q, a \in \mathbb{Z}^2$  such that the only points of  $\mathbb{Z}^2$  in the convex hull  $C$  of  $\{\pm p, \pm q, \pm a\}$  are these points and the origin. There are at most 6 pairs  $\pm L_i$  and each of these contains a side of  $C$ . The lines are a subset of the exceptional configuration shown in Fig. 1.

Let  $S_i$  be the closed strip between  $L_i$  and  $-L_i$ , then the only lattice points in the interior of  $S_i$  are those in  $L_i^0$ . The intersection of any two distinct strips  $S_i \cap S_j$  is a parallelogram  $P$ . The boundary of  $P$  consists of segments of  $\pm L_i, \pm L_j$  and we classify  $P$  into one of 3 types as follows:

- (I) there are 2 lattice points in  $\partial P$  and these are vertices of  $P$ ;
- (II) there are 4 lattice points in  $\partial P$  and these are vertices of  $P$ ;
- (III) there are 8 lattice points in  $\partial P$  and these are the vertices and midpoints of sides of  $\partial P$ .

We now show that these are the only possibilities. First since  $P$  is symmetric through the origin, there must be an even number of lattice points in  $\partial P$ . Now  $\pm L_i$  must meet  $\pm L_j$  in at least a pair  $\pm a$  of lattice points by the hypothesis (ii) of Proposition 5.1. Furthermore, if there is a lattice point in the interior of the side  $e$  (contained in  $L_i$  say) of  $\partial P$  then this lattice point must lie on  $L_j^0$  (by hypothesis (iii) of 5.1) and therefore is the midpoint of  $e$ . Since one of the ends of  $e$  is a lattice point, the other end of  $e$  is also a lattice point. This implies that the ends of  $e$  are 2 lattice spacings apart and so the same is true of  $L_i^0 \cap P$ . Thus the intersection of  $L_i^0$  with  $L_j$  is also a lattice point and so there is a lattice point in the middle of every side of  $\partial P$ . Therefore all the vertices of  $\partial P$  are also lattice points and  $P$  is type (III). The proof of Proposition 5.1 will be based on the following lemmas:

**Lemma 5.2.** *With the hypotheses of Proposition 5.1, suppose that every parallelogram  $S_i \cap S_j$  is type (II) or type (III). Let  $P = S_1 \cap S_2$ , then either  $L_3$  contains a vertex of  $P$  or  $P$  is type (III) and  $L_3$  contains two of the midpoints of adjacent sides of  $P$ .*

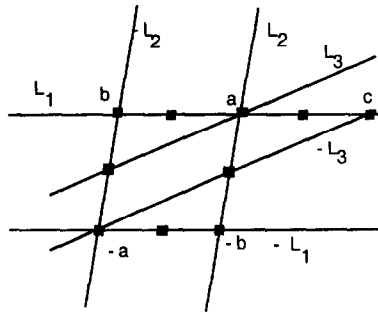


Fig. 2.

**Proof.** Since every parallelogram is type (II) or (III) the intersection of every pair of lines  $L_i \cap L_j$  with  $i \neq j$  is a lattice point. Note that  $P$  is not contained in the interior of  $S_3$  because the vertices of  $\partial P$  cannot all lie in  $L_3^0$ . We may suppose that  $\pm L_3$  contains no vertex of  $\partial P$ , and thus  $\pm L_3$  meets  $\partial P$  in 4 distinct points which are therefore lattice points in the interiors of edges of  $\partial P$ . But the only lattice point in the interior of an edge of  $\partial P$  is its midpoint, so the result follows.  $\square$

**Corollary 5.3.** *With the hypotheses of Proposition 5.1, suppose that every parallelogram  $S_i \cap S_j$  is type (III). Then  $L_3$  contains two of the midpoints of adjacent sides of  $P$ .*

**Proof.** By Lemma 5.2 (after relabeling  $L_3$  as  $-L_3$  if necessary) the other possibility is that  $L_3$  contains  $a = L_1 \cap L_2$ . Consider the parallelogram  $R = S_1 \cap S_3$  then  $\pm a$  are two of the vertices of  $R$ . Since  $R$  is type (III) one of the other vertices of  $\partial R$ ,  $c$  say, is on  $L_1$  and there is exactly one lattice point on  $L_1$  between  $a$  and  $c$ . Let  $P = S_1 \cap S_2$ . Let  $\pm b$  be the other two vertices of  $\partial P$ . Then either  $c = b$  in which case  $L_3 = L_2$  a contradiction. Otherwise the situation is as shown in Fig. 2, from which one sees that  $S_2 \cap S_3$  is type (II) again a contradiction.  $\square$

**Lemma 5.4.** *With the hypotheses of Proposition 5.1, suppose that  $P = S_1 \cap S_2$  is type (I). After replacing  $L_2$  by  $-L_2$  if necessary we may assume that  $a = L_1 \cap L_2$  is a lattice point. Then either  $\pm L_3$  contains  $\pm a$  or  $\pm L_3 \cap L_1$  contains the lattice point  $p$  which is the unique lattice point on  $L_1$  closest to  $a$  and such that  $a$  and  $p$  are separated by  $-L_2$ .*

**Proof.** Suppose that  $\pm L_3$  does not contain either  $\pm a$ . We claim that  $S_3$  contains a vertex of  $\partial P$ . Otherwise  $S_3$  meets only 2 of the sides  $\pm e$  of  $\partial P$  and therefore  $e$  contains a lattice point  $p \in \pm L_3 \cap e$  in its interior thus  $P$  is type (III) which is a contradiction. Let  $\pm b$  be the pair of vertices of  $P$  which are not lattice points.

First suppose that  $S_3$  contains  $\pm b$ , the situation is shown in Fig. 3. Now  $\pm L_3$  meets  $L_1$  in two points  $p, r$  and one of these points,  $r$  say, is on an edge  $e$  of  $P$  and is therefore not a lattice point. Thus  $p$  is separated from  $a$  on  $L_1$  by  $b$ . We claim that there is no lattice point on  $L_1$  between  $p$  and  $a$ . There is no lattice point between  $a$  and  $b$  because

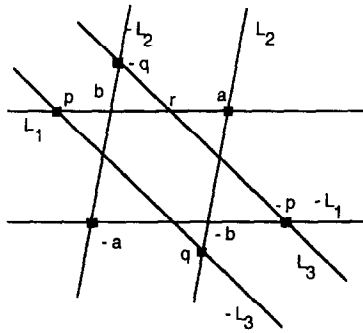


Fig. 3.

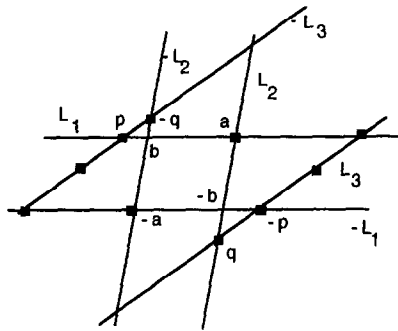


Fig. 4.

$P$  is type (I). If there is a lattice point  $c$  on  $L_1$  between  $p$  and  $b$  then it lies in the interior of  $S_3$  and therefore lies on  $L_3^0$ , and since  $L_3^0 \cap L_1$  and  $-L_3 \cap L_1$  are lattice points then  $L_3 \cap L_1 = r$  is also a lattice point on  $e$  which is a contradiction.

The other possibility is that  $S_3$  contains  $\pm a$  then  $R = S_3 \cap S_1$  must be type (III) since  $R$  contains  $\pm a$  in the interior of its sides. The situation is shown in Fig. 4, and the conclusion follows.  $\square$

**Corollary 5.5.** *With the hypotheses of Lemma 5.4 (replacing  $L_3$  by  $-L_3$  if necessary) either  $L_3$  contains  $a$  or  $L_3$  contains  $\bar{p}(-q)$  or  $\bar{p}\bar{q}$ . Here  $q$  is the unique lattice point on  $L_2$  closest to  $a$  and such that  $a$  and  $q$  are separated by  $-L_1$ . See Fig. 4.*

**Proof.** Apply Lemma 5.4 twice swapping the roles of  $L_1$  and  $L_2$ .  $\square$

**Proof of Proposition 5.1.** The proof is split into several cases.

Case (1): there is some parallelogram  $P$  of type (I), we may suppose  $P = S_1 \cap S_2$ , refer to Fig. 5. After replacing  $L_2$  by  $-L_2$  if needed, we may assume that  $L_1 \cap L_2$  is a lattice point  $a$ . By Corollary 5.5 if none of the line pairs contains  $\bar{p}\bar{q}$  then all the line

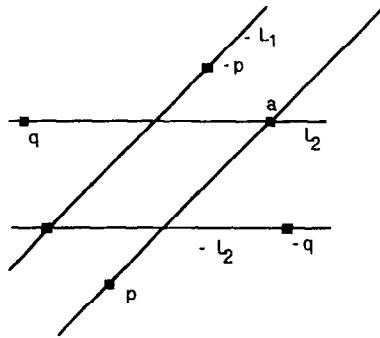


Fig. 5.

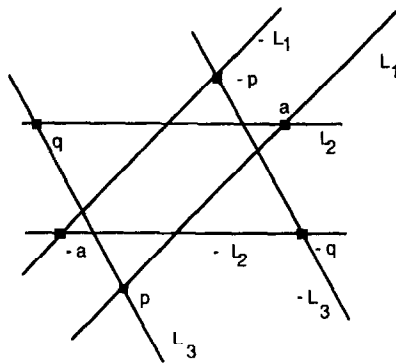


Fig. 6.

pairs contain  $a$  except one possible line pair containing  $\overline{p(-q)}$ . From Fig. 4 we see that  $\overline{p(-q)}$  is parallel to  $\overline{a(-a)}$  since  $S_3 \cap S_1$  is type (III) and we are done. The remaining case is that there is a line, which we may assume is  $L_3$  containing  $\overline{p(-q)}$ .

The configuration of  $L_1, L_2, L_3$  is shown in Fig. 6. Observe that  $S_3$  does not contain  $\pm a$  because these are lattice points which cannot lie on  $L_3^0$ . From Fig. 6 we see that every pair of lines chosen from  $\{L_1, L_2, L_3\}$  gives a parallelogram of type (I). This is because there are no lattice points between  $a$  and  $q$  by Corollary 5.5 and similarly none between  $a$  and  $p$ . Therefore by Lemma 5.4 every line must contain 2 of the points  $\pm a, \pm p, \pm q$ . This implies that the entire set of lines  $\{L_i\}$  must be a subset of the exceptional configuration shown in Fig. 1. The convex hull  $C$  of  $\pm a, \pm p, \pm q$  is contained in  $S_4 \cap S_5$ . Therefore the only lattice points in  $C$  are its vertices and the origin, completing this case.

Case (2): there is no type (I) parallelogram and there is a type (II) parallelogram. After re-labeling we may assume that  $P = S_1 \cap S_2$  is a type (II) parallelogram see Fig. 7. Then by Lemma 5.2  $L_i$  contains a vertex of  $\partial P$  for  $i \geq 3$ . We may relabel so that  $L_3$  contains  $a = L_1 \cap L_2$ . Now  $S_3 \cap \partial P$  contains an interval containing  $a$  which we may suppose

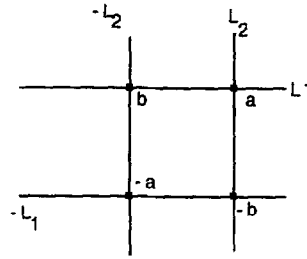


Fig. 7.

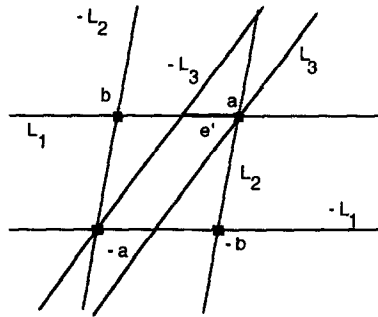


Fig. 8.

is in the edge  $e = \overline{ab}$  of  $\partial P$ . If  $e' = S_3 \cap L_1$  is contained in the edge  $e$  then  $S_3 \cap S_1$  is a type (I) parallelogram (see Fig. 8), a contradiction. Thus we may suppose that  $S_3$  contains  $b$  and since  $L_3 \neq L_2$  that  $b \notin \pm L_3$  which implies that  $b$  lies on  $L_3^0$  and therefore  $L_3$  is parallel to the line through the origin containing  $b$ . This gives the configuration shown in Fig. 9. Repeating this analysis we see that there can be at most one more line pair  $\pm L_4$  and this must give the configuration shown in Fig. 10. In this case there are 4 line pairs, and 3 of these line pairs  $\pm L_1, \pm L_2, \pm L_3$  contain  $a$ , and the remaining one  $\pm L_4$  is parallel to  $\overline{a(-a)}$  so we are done.

Case (3): all parallelograms are of type (III) hence  $P = S_1 \cap S_2$  is type (III) and by Corollary 5.3, after relabeling if necessary, we may assume that  $L_3$  contains the midpoints  $p$  and  $q$  of two adjacent sides of  $P$ , refer to Fig. 11. Applying 5.3 to the line pair  $\pm L_4$  and  $P$  we see that, after replacing  $L_4$  by  $-L_4$  if needed,  $L_4$  contains both  $p$  and  $-q$ . But then  $S_3 \cap S_4$  is type (II) a contradiction. Thus the configuration is a subset of Fig. 11 and there are at most 3 line pairs. Furthermore these lines each contain two of the points  $\pm a, \pm p, \pm q$ . Comparing Fig. 11 and Fig. 1 we see that the configuration in Fig. 11 is contained in the configuration of Fig. 1. Thus the lines are a subset of the exceptional configuration in this case.  $\square$



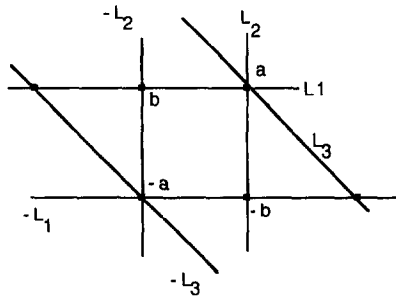


Fig. 9.

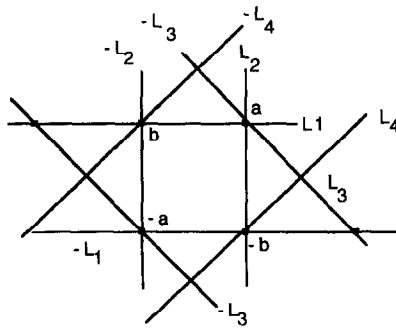


Fig. 10.

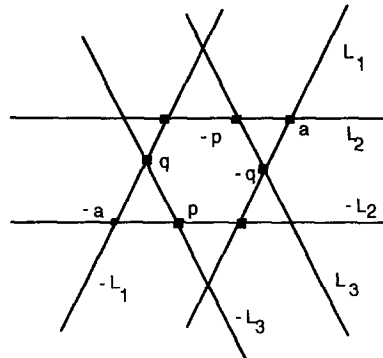


Fig. 11.

**Proof of Corollary 1.4.** The conclusion of Theorem 1.3 is that the cyclic classes are lattice points  $\{a_i\}$  such that if  $L_i = L(\alpha_i)$  then the lines  $L_i$  satisfy the hypotheses of Proposition 5.1. The conclusion of Proposition 5.1 is that lines are configured in one of two ways.

The first case is that there is a lattice point  $a$  which is contained in each pair  $\pm L_i$  with at most one exception,  $L_1$  say. We have that  $\Delta(a, \alpha_i) = \pm 1$  for all  $i \geq 2$ . Choose a lattice point  $b$  so that  $\{a, b\}$  is a basis of  $\mathbb{Z}^2$  then  $\pm \alpha_i = b + n_i a$  for  $i \geq 2$ . Since the remaining line is parallel to  $a$  ( $-a$ ) then  $\alpha_1 = \pm a$  giving the conclusion.

For the exceptional configuration, there are 3 points  $p, q, a \in \mathbb{Z}^2$  such that each line contains two of these points. Thus the directions of these lines are given by

$$\{a \pm p, p \pm q, q \pm a\}$$

now  $L(\alpha)$  is parallel to  $\alpha$  since the pairing is skew-symmetric, so the result follows.  $\square$

**Proof of Addendum 1.5.** If there are more than 6 pairs of cyclic classes  $\mu^{\pm 1}$  then by Corollary 1.4 there is a basis  $\gamma, \delta$  of  $H$  such that if  $\mu \neq \gamma^{\pm 1}$  is a cyclic class then  $\mu = \delta \gamma^n$  for some integer  $n$ . Then by Proposition 2.7

$$A(\gamma, \delta) = a \cdot \gamma^b (\gamma - 1)^c (\gamma + 1)^d + (\delta \gamma^n - 1) B(\gamma, \delta).$$

If  $B(\gamma, \delta) = 0$  then  $\gamma = 0, \pm 1$  everywhere on  $R_0$  which contradicts the hypothesis on  $\rho'$  in the addendum. Thus we may suppose that  $B(\gamma, \delta) \neq 0$  and so the right hand side contains a term  $\delta^p \gamma^q$  for some  $q \geq n$  and  $p \geq 1$  and therefore  $|n| \leq \text{degree}_\gamma [A(\gamma, \delta)]$ .  $\square$

**Remark.** The fundamental group of the trefoil knot has  $A(\lambda, \mu) = \lambda \mu^6 + 1$  and as remarked in example (1) there are infinitely many cyclic classes, this corresponds to the case  $B(\lambda, \mu) = 0$  in the above proof.

**Questions.** Is there a universal bound on the number of primitive cyclic quotients of a knot like group satisfying the hypotheses of Addendum 1.5? In the case of the fundamental group of a knot, there is a stringent condition placed on the  $A$  polynomial by the condition that the volume form is exact, see [1]. Does this condition give a universal bound for these groups?

## References

- [1] D. Cooper, M. Culler, H. Gillett, D.D. Long and P.B. Shalen, Plane curves associated to character varieties of knot complements, *Invent. Math.* 118 (1994) 47–84.
- [2] M. Culler, C.McA. Gordon, J. Lucke and P.B. Shalen, Dehn surgery on knots, *Ann. of Math.* (1987) 237–300.
- [3] D. Cooper and D.D. Long, Roots of unity and the character variety of a knot complement, *J. Austral. Math. Soc.* 55 (1993) 90–99.
- [4] M. Culler and P.B. Shalen, Varieties of group representations and splittings of 3-manifolds, *Ann. of Math.* 117 (1983) 109–146.
- [5] D. Mumford, *Algebraic Geometry I: Complex Projective Varieties*, Grundlehren der Mathematischen Wissenschaften 221 (Springer, Berlin, 1976).
- [6] J.-P. Serre, *Trees* (Springer, Berlin, 1980).
- [7] M. Tretkoff, A topological approach to the theory of groups acting on trees, *J. Pure Appl. Algebra* 16 (1980) 323–333.