INTERSECTION-NUMBER OPERATORS FOR CURVES ON DISCS AND CHEBYSHEV POLYNOMIALS

Stephen P. Humphries

Dedicated to Joan Birman with gratitude and respect.

Abstract. We prove the following result and show a connection with geometric intersection-number functions of curves on punctured discs and algebraic intersection functions for curves on surfaces:

Let R be an associative ring with identity and fix $r \in Z(R)$, where $Z(R)$ is the centre of R. Define polynomials $p_n = p_n(r)$ recursively by $p_0 = -2, p_1 = r, p_n = -(rp_{n-1} + p_{n-2})$. Let $\sigma : R \to R$ be a ring homomorphism and assume that $\sigma(r) = r$. Define operators $\mathfrak{A}_n = \mathfrak{A}_n(\sigma, r), n \geq 0$, by $\mathfrak{A}_0 = \sigma - 1$ and for $n > 0$, we let $\mathfrak{A}_n = \sigma^2 + p_n\sigma + 1$. Define operators $\mathfrak{B}_n = \mathfrak{B}_n(\sigma, r), n \geq 0$ by $\mathfrak{B}_n = \mathfrak{A}_0\mathfrak{A}_1 \dots \mathfrak{A}_n$.

Suppose that $u, v \in R$ and that $\mathfrak{B}_n(u) = \mathfrak{B}_m(v) = 0$ for $n, m \geq 0$. Then $\mathfrak{B}_{n+m}(uv) = 0$.

§1. Introduction.

In this paper we prove the following result and indicate connections with Chebyshev polynomials, symmetric polynomials, Dickson polynomials, the theory of geometric intersection-number functions on punctured discs and algebraic intersection functions for curves on surfaces. This result thus gives a common method for defining both geometric and algebraic intersection numbers.

Theorem 1.1. *Let R be an associative ring with identity and fix $r \in Z(R)$, where $Z(R)$ is the centre of R. Define polynomials $p_n = p_n(r)$ recursively by*

$$p_0 = -2, \quad p_1 = r, \quad p_n = -(rp_{n-1} + p_{n-2}).$$

Let $\sigma : R \to R$ be a ring homomorphism and assume that $\sigma(r) = r$. Define operators $\mathfrak{A}_n = \mathfrak{A}_n(\sigma, r), n \geq 0$, by $\mathfrak{A}_0 = \sigma - 1$ and for $n > 0$, we let $\mathfrak{A}_n = \sigma^2 + p_n\sigma + 1$. Now define operators $\mathfrak{B}_n = \mathfrak{B}_n(\sigma, r), n \geq 0$, by $\mathfrak{B}_n = \mathfrak{A}_0\mathfrak{A}_1 \dots \mathfrak{A}_n$.

Suppose that $u, v \in R$ and that $\mathfrak{B}_n(u) = \mathfrak{B}_m(v) = 0$ for $n, m \geq 0$. Then $\mathfrak{B}_{n+m}(uv) = 0$.

The polynomials p_n are polynomials in the variable $p_1 = r$ that are related to Chebyshev polynomials $T(n)$ and Dickson polynomials. Recall that the Chebyshev polynomials are defined by $T_0(x) = 1, T_1(x) = x$ and $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ for $n \geq 2$ [Ri, p. 35]. Then comparing the recurrence for $p_n(x)$ with this recurrence we see that

$$p_n(x) = (-1)^{n+1} 2T_n(x/2). \tag{1.1}$$

These polynomials are also related to the Dickson polynomials $D_n(x, a)$ [LMT] by $p_n(x) = (-1)^{n+1} D_n(x, 1)$.

One of the results that we use to prove Theorem 1.1 is

Theorem 1.2. *Let $n \geq m \geq 0$. Suppose that α_n, α_m are roots of the polynomials determined by $\mathfrak{A}_n$ and $\mathfrak{A}_m$, respectively, so that $\alpha_n^2+p_n\alpha_n+1=0$ and $\alpha_m^2+p_m\alpha_m+1=0$. Then $\alpha_n\alpha_m$ is a root of either $\mathfrak{A}_{n+m}$ or $\mathfrak{A}_{n-m}$.*

Let D_n denote the disc with n punctures $\pi_1,\dots,\pi_n$. Let $a_1,\dots,a_{n-1}$ be a set of arcs in D_n having disjoint interiors and such that a_i joins the punctures π_i and π_{i+1}. See Figure 1 in §5. Let $\mathcal{C}^\infty=\mathcal{C}_n^\infty$ denote the set of isotopy classes of positively-oriented simple closed curves on D_n.

Then the braid group B_n acts as (isotopy classes of) diffeomorphisms of D_n [Bi, Ch.1]. The group B_n has standard generators $\sigma_1,\dots,\sigma_{n-1}$ and presentation

$$\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1},\ \text{for } i=1,\dots,n-2$$

$$\sigma_i\sigma_j=\sigma_j\sigma_i,\qquad \text{for } |i-j|>1.$$

Here the generator σ_i acts as a half-twist on D_n and has a representative diffeomorphism which is supported in a tubular neighbourhood of the arc a_i. For $1\leq i<j\leq n$ let γ_{ij} be a simple closed curve isotopic to the boundary of a tubular neighbourhood of $a_i\cup a_{i+1}\cup\cdots\cup a_{j-1}$. Given any $c,d\in\mathcal{C}^\infty$ we let $\iota(c,d)$ denote the geometric intersection-number of c and d. This is the minimum number of points of $c'\cap d'$, where c' and d' are any simple closed curves isotopic to c and d. Note that $\iota(c,d)$ is always even since D_n is planar.

Note that in the context of Theorem 1.1, if $m>n\geq 0$ and $\mathfrak{B}_n(u)=0$, then $\mathfrak{B}_m(u)=0$. The first part of the following result comes from [H1]:

Theorem 1.3. *For $n\geq 2$ and a commutative ring R let*

$$R_n=R[a_{12},a_{13},\dots,a_{1n},a_{21},a_{23},\dots,a_{2n},\dots,a_{n1},\dots,a_{n\,n-1}]$$

be the polynomial ring in commuting indeterminates a_{ij}, $1\leq i\neq j\leq n$. Then there is an action of B_n on R_n whose kernel is the centre of B_n.

Let $r=a_{12}a_{21}+2\in R_n$ and let $\sigma=\sigma_1\in Aut(R_n)$. Then $\sigma_1(r)=r$. Further, there is a function $\phi:\mathcal{C}^\infty\to R_n$ such that for all $c\in\mathcal{C}^\infty$ there is $N=N(c)\geq 0$ such that $\mathfrak{B}_n(\sigma,r)(\phi(c))=0$. Let $\Omega(c)$ be the minimal such $N(c)$. Then we have

$$\Omega(c)=\iota(c,\gamma_{12})/2.$$

This result thus gives a method for calculating geometric intersection-number functions that can be compared to existing such algorithms of Reinhart [R], Zieschang [Z1, Z2], Chillingworth [C1, C2], Birman and Series [BS], Cohen and Lustig [CL] and Tan [T].

The representation of B_n in $Aut(R_n)$ will be described later, but should be thought of in the following way. Let $F_n=<x_1,\dots,x_n>$ denote the free group of rank n, which we identify with the fundamental group of D_n. The Magnus expansion M of F_n [Ma,MKS] is defined as follows: Let $\mathcal{P}_n$ be the algebra of formal power series in non-commutative variables $X_1,\dots,X_n$ over $\mathbb{C}$. Then M is the homomorphism $M:F_n\to\mathcal{P}$ given by

$$M(x_i)=1+X_i,\quad M(x_i^{-1})=1-X_i+X_i^2-X_i^3+\dots.$$

Then M is injective, has connections with Fox's free differential calculus and is used to define interesting representations of the braid groups [Bi]. We obtain our representation of B_n in $Aut(F_n)$ by looking at the situation where in $\mathcal{P}_n$ we have the relations $X_i^2 = 0$ for all $i = 1, \ldots, n$. This is accomplished very concretely by representing the free group F_n using transvections. This is all explained in more detail in §5. A quotient of this algebra was used by Milnor [Mi1,Mi2] to study links.

We prove Theorem 1.1 in §4 after some preliminaries in §2 and §3 (where we prove Theorem 1.2). In §5 we explain the connection between our polynomials p_n and interscetion-number functions for curves on planar surfaces and in §6 we give a normal form for words representing simple closed curves on such surfaces. In §7 we study the combinatorial properties of a certain 'trace' of such words. In §8 we prove Theorem 1.3 and in §9 we show that in the context of §2 and §3 there is an associated infinite monotone family of commuting projections [AG, §33] which gives rise to an infinite family of orthogonal idempotents (Theorem 9.3). In §10 we indicate how Theorem 1.1 applies to algebraic intersection functions for curves on surfaces.

§2. Basic Results.

We note from the above definition of $\mathfrak{B}_n = \mathfrak{B}_n(\sigma, r)$ that $\mathfrak{B}_n$ has degree $2n+1$ when thought of as a polynomial in σ (as we often will). Define

$$\mathfrak{B}_n(\sigma) = \sum_{i=0}^{2n+1} q_{n\,i}\sigma^i,$$

where the $q_{n\,i}$ are polynomials in p_1. Then since $\mathfrak{B}_{n+1} = \mathfrak{B}_n(\sigma^2 + p_{n+1}\sigma + 1)$ we see that the $q_{n\,i}$ satisfy the following recursion:

$$q_{n+1\,i} = q_{n\,i-2} + p_{n+1}q_{n\,i-1} + q_{n\,i}. \tag{2.1}$$

We also note that $q_{n,0} = -1$ and that $q_{n,2n+1} = 1$ for $n \geq 0$.

Now assume that for $u \in R$ we have $\mathfrak{B}_n(u) = 0$. Then since $q_{n,2n+1} = 1$ we have

$$\sigma^{2n+1}(u) = -\sum_{i=0}^{2n} q_{n\,i}\sigma^i(u) \tag{2.2}$$

and so for $j \geq 2n+1$ we can write $\sigma^j(u)$ as a sum of multiples of $\sigma^i(u)$ for $i = 1, \ldots, 2n$. Specifically we will define

$$\sigma^j(u) = \sum_{i=0}^{2n} r_{n,j,i}\sigma^i(u)$$

where each $r_{n,j,i}$ is a polynomial in p_1. Then the $r_{n,j,i}$ satisfy the recursion given in the following result.

Lemma 2.1. *We have (i) $r_{n,j,i} = \delta_{ij}$ if $0 \leq j \leq 2n$;*
(ii) $r_{n,2n+1,i} = -q_{n\,i}$;
(iii) $r_{n,j+1,i} = -q_{n\,i}r_{n,j,2n} + r_{n,j,i-1}$; and
(iv) if $0 < i \leq 2n+1$ then the degree of q_{ni} is $(2n-i+1)i/2$.

Proof. (i) is clear, while (ii) follows from (2.2). For (iii) we note that if $\sigma^j(u) = \sum_{i=0}^{2n} r_{n,j,i}\sigma^i(u)$, then (2.2) also gives:

$$\begin{aligned}
\sigma^{j+1}(u) &= \sum_{i=0}^{2n} r_{n,j,i}\sigma^{i+1}(u) = \left(\sum_{i=0}^{2n-1} r_{n,j,i}\sigma^{i+1}(u)\right) + r_{n,j,2n}\sigma^{2n+1}(u) \\
&= \sum_{i=0}^{2n-1} r_{n,j,i}\sigma^{i+1}(u) - r_{n,j,2n}\sum_{i=0}^{2n} q_{n\,i}\sigma^i(u).
\end{aligned}$$

The recursion (iii) follows.

The formula for the degree of q_{ni} follows by induction from the recursion (2.1). The initial cases are easily checked and then one notes that $deg(p_{n+1}) = n+1$ and that since $0 \le i \le 2n+1$ one finds that (using (2.1))

$$(2n-i+3)i/2 = deg(p_{n+1}q_{ni-1}) \ge max(deg(q_{n\,i-2}), deg(q_{ni}))$$

with equality only occuring when $i = 0$. □

The following result indicates how we will prove Theorem 1.1.

Proposition 2.2. *Theorem 1.1 will follow if we have*

$$\sum_{i=0}^{2(n+m)+1} q_{n+m\,i}r_{n,i,j}r_{m,i,k} = 0$$

for all $n, m, j, k \ge 0$.

Proof. Suppose that $u, v \in R$ and that $\mathfrak{B}_n(u) = \mathfrak{B}_m(v) = 0$. Then, since p_1 is central in R, the $r_{n,j,i}$ are also central and we have

$$\begin{aligned}
\mathfrak{B}_{n+m}(uv) &= \sum_{i=0}^{2(n+m)+1} q_{n+m\,i}\sigma^i(uv) \\
&= \sum_{i=0}^{2(n+m)+1} q_{n+m\,i}\sigma^i(u)\sigma^i(v) \\
&= \sum_{i=0}^{2(n+m)+1} q_{n+m\,i}\sum_{a=0}^{2n} r_{n,i,a}\sigma^a(u)\sum_{b=0}^{2m} r_{m,i,b}\sigma^b(v) \\
&= \sum_{a=0}^{2n}\sum_{b=0}^{2m}\left(\sum_{i=0}^{2(n+m)+1} q_{n+m\,i}r_{n,i,a}r_{m,i,b}\right)\sigma^a(u)\sigma^b(v).
\end{aligned}$$

The result follows. □

Proposition 2.3. *For* $n, y, t \ge 0$ *we have*

$$r_{n,2n+1+t,y} = \sum_{j=1}^{t+1}\sum_{s=0}^{t}\sum_{\substack{1\le i_1,i_2,\dots,i_s\le t\\ \sum_k i_k = t+1-j}} (-1)^{s+1}q_{n\,y+1-j}\prod_{k=1}^{s} q_{n\,2n+1-i_k}.$$

Here we interpret the case $s=0$ in this formula as $r_{n,2n+1+0,y} = (-1)^{0+1} q_{n\, y+1-1}$.

Proof. This will be by induction on $t \geq 0$, the case $t=0$ following from Lemma 2.1 (ii) and the rest following from the recursion given in Lemma 2.1 (iii), as follows. First note that

$$\begin{aligned} r_{n,2n+1+t,y-1} &= \sum_{j=1}^{t+1} \sum_{s=0}^{t} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t \\ \sum_k i_k = t+1-j}} (-1)^{s+1} q_{n\, y-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &= \sum_{j=1}^{t+1} \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t \\ \sum_k i_k = t+1-j}} (-1)^{s+1} q_{n\, y-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k}. \end{aligned}$$

We now consider the sum in Proposition 2.3 for $t+1$. We split this sum up into the cases $j=1$ and $j>1$ as follows:

$$\begin{aligned} &\sum_{j=1}^{t+2} \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+2-j}} (-1)^{s+1} q_{n\, y+1-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &\quad = \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+1}} (-1)^{s+1} q_{n\, y} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &\qquad\qquad + \sum_{j=2}^{t+2} \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+2-j}} (-1)^{s+1} q_{n\, y+1-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &\quad = \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+1}} (-1)^{s+1} q_{n\, y} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &\qquad\qquad + \sum_{j=1}^{t+1} \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+1-j}} (-1)^{s+1} q_{n\, y-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &\quad = r_{n,2n+1+t,y-1} + \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t+1 \\ \sum_k i_k = t+1}} (-1)^{s+1} q_{n\, y} \prod_{k=1}^{s} q_{n\, 2n+1-i_k}. \end{aligned}$$

Now we also have

$$\begin{aligned} -q_{ny} r_{n,2n+1+t,2n} &= -q_{ny} \sum_{j=1}^{t+1} \sum_{s=0}^{t} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t \\ \sum_k i_k = t+1-j}} (-1)^{s+1} q_{n\, 2n+1-j} \prod_{k=1}^{s} q_{n\, 2n+1-i_k} \\ &= \sum_{j=1}^{t+1} \sum_{s=0}^{t} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t \\ \sum_k i_k = t+1-j}} (-1)^{s+2} q_{n\, y} \left(\prod_{k=1}^{s} q_{n\, 2n+1-i_k} \right) q_{n\, 2n+1-j} \\ &= \sum_{s=0}^{t+1} \sum_{\substack{1 \leq i_1, i_2, \ldots, i_s \leq t \\ \sum_k i_k = t+1}} (-1)^{s+2} q_{n\, y} \left(\prod_{k=1}^{s} q_{n\, 2n+1-i_k} \right) \end{aligned}$$

Putting this together with the previous calculation and the recursion from Lemma 2.1 (iii) gives the result. $\square$

The following result indicates a connection with symmetric polynomials.

Proposition 2.4. *For $n, m \geq 0$ we have*

$$q_{n\,m} = \sum_{k=0}^{m} (-1)^{m+k+1} \binom{n-k}{\lfloor \frac{m-k}{2} \rfloor} \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n} p_{i_1} p_{i_2} \dots p_{i_k}.$$

Proof. The proof is by induction on the pair (n, m), ordered lexicographically, where $n, m \geq 0$, the cases $m = 0$ following since $q_{n\,0} = -1$. We will use the following notation $\Sigma_{nk} = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n} p_{i_1} p_{i_2} \dots p_{i_k}$. Using the recursion (2.1) for $q_{n\,m}$ we have

$$\begin{aligned}
q_{n+1,m} &= q_{n,m-2} + p_{n+1} q_{n,m-1} + q_{n,m} \\
&= \sum_{k=0}^{m-2} (-1)^{m+k+1} \binom{n-k}{\lfloor \frac{m-2-k}{2} \rfloor} \Sigma_{nk} + p_{n+1} \sum_{k=0}^{m-1} (-1)^{m+k} \binom{n-k}{\lfloor \frac{m-1-k}{2} \rfloor} \Sigma_{nk} \\
&\qquad + \sum_{k=0}^{m} (-1)^{m+k+1} \binom{n-k}{\lfloor \frac{m-k}{2} \rfloor} \Sigma_{nk}.
\end{aligned}$$

Now $\Sigma_{n+1\,k} = \Sigma_{nk} + p_{n+1} \Sigma_{n\,k-1}$ and so the coefficient of $\Sigma_{n\,s}$ in the above sum is

$$(-1)^{m+s+1} \binom{n-s}{\lfloor \frac{m-2-s}{2} \rfloor} - (-1)^{m+s+1} \binom{n-s+1}{\lfloor \frac{m-s}{2} \rfloor} + (-1)^{m+s+1} \binom{n-s}{\lfloor \frac{m-s}{2} \rfloor}$$

which is equal to zero by a standard binomial coefficient identity. One similarly finds that the coefficient of $\Sigma_{n+1\,k}$ is $(-1)^{m+k+1} \binom{n+1-k}{\lfloor \frac{m-k}{2} \rfloor}$ as required. $\square$

Proposition 2.5. *For $n, t, y \geq 0$ we have*

$$\sum_{i=0}^{2n+1} q_{n\,i} r_{n,i+t,y} = 0.$$

Proof. By Proposition 2.3 and Lemma 2.1 (i) we have

$$\begin{aligned}
\sum_{i=0}^{2n+1} q_{n\,i} r_{n,i+t,y} &= q_{n\,y-t} + \sum_{k=2n+1}^{2n+1+t} q_{n\,k-t} r_{n,k,y} \\
&= q_{n\,y-t} + \sum_{u=0}^{t} q_{n\,2n+1+u-t} r_{n,2n+1+u,y} \\
&= q_{n\,y-t} + \sum_{u=0}^{t} q_{n\,2n+1+u-t} \Bigg(\sum_{j=1}^{u+1} q_{n\,y+1-j} \\
&\qquad \sum_{s=0}^{u} \sum_{\substack{1 \leq i_1, \dots, i_s \leq u+1-j \\ \sum_k i_k = u+1-j}} (-1)^{s+1} \prod_{k=1}^{s} q_{n\,2n+1-i_k} \Bigg).
\end{aligned}$$

We will show how the terms in this sum cancel in pairs. Each summand in the above sum is determined by a 4-tuple $(u, j, s, (i_1, \ldots, i_s))$ where the values in this 4-tuple satisfy

$$0 \le u \le t, \quad 1 \le j \le u+1, \quad 0 \le s \le u \quad \text{and} \quad \sum_{k=1}^{s} i_k = u+1-j.$$

We will think of this latter condition as determining the value of j.

The summand corresponding to $(u, j, s, (i_1, \ldots, i_s))$ is

$$q_{n\ 2n+1+u-t} q_{n\ y+1-j} (-1)^{s+1} \prod_{k=1}^{s} q_{n\ 2n+1-i_k}$$

where $j = u+1-\sum_{k=1}^{s} i_k$. Also note that since $j \ge 1$, $u \le t$ and $\sum_{k=1}^{s} i_k = u+1-j$, we must have $i_k \le t$ for all $k = 1, \ldots, s$.

Assume that $s > 0$. Thus, since $q_{n\ 2n+1} = 1$, to the 4-tuple $(t, j, s, (i_1, \ldots, i_s))$ we associate the summand

$$q_{n\ 2n+1} q_{n\ y+1-j} (-1)^{s+1} \prod_{k=1}^{s} q_{n\ 2n+1-i_k} = q_{n\ y+1-j} (-1)^{s+1} \prod_{k=1}^{s} q_{n\ 2n+1-i_k}$$

where $j = t+1-\sum_{k=1}^{s} i_k$.

Further, to the 4-tuple $(t-i_s, j', s-1, (i_1, \ldots, i_{s-1}))$ we associate the summand

$$q_{n\ 2n+1-i_s} q_{n\ y+1-j'} (-1)^{s} \prod_{k=1}^{s-1} q_{n\ 2n+1-i_k}.$$

But we have

$$j' = (t-i_s)+1-\sum_{k=1}^{s-1} i_k = t+1-\sum_{k=1}^{s} i_k = j.$$

Then the two summands corresponding to the 4-tuples $(t, j, s, (i_1, \ldots, i_s))$ and $(t-i_s, j, s-1, (i_1, \ldots, i_{s-1}))$ cancel if $s > 0$.

Now the only summands of the sum not accounted for in the above argument are the initial summand $q_{n\ y-t}$ and the summand corresponding to the 4-tuple $(t, t+1, 0, ())$. This latter 4-tuple gives the summand $q_{n\ 2n+1} q_{n\ y-t}(-1) = -q_{n\ y-t}$ which thus cancels with $q_{n\ y-t}$. Thus all terms cancel in pairs and Proposition 2.5 follows. □

Now by repeated application of (2.1) we may write

$$q_{n+m\ i} = \sum_{k=0}^{2m} w_{n,m,k} q_{n\ i-k} \tag{2.3}$$

for all $n, m, i \ge 0$, where $w_{n,m,k}$ are polynomials in p_1.

Proposition 2.6. *(i) The $w_{n,m,k}$ satisfy the recursion*

$$w_{n,m+1,k} = w_{n,m,k-2} + p_{n+m+1} w_{n,m,k-1} + w_{n,m,k},$$

with initial conditions $w_{n,1,0} = w_{n,1,2} = 1, \ w_{n,1,1} = p_{n+1}$.
(ii) For $N, n, m \geq 0$ we have

$$w_{N,n,m} = \sum_{k=0}^{m} \binom{n-k}{\left[\frac{m-k}{2}\right]} \sum_{1 \leq i_1, i_2, \ldots, i_k \leq n} p_{N+i_1} p_{N+i_2} \cdots p_{N+i_k}.$$

Proof. (i) follows immediately from (2.1), while the proof of (ii) is the same as that for Proposition 2.4 with (2.1) replaced by the recursion given in (i). □

Proposition 2.7. *For $t, n, j, k \geq 0$ we have*

$$\sum_{i=0}^{2(n+k)+1} q_{k+n\,i} r_{n,i+t,y} = 0.$$

Proof. This follows from Proposition 2.5 together with the formula (2.3) allowing us to express $q_{k+n\,i}$ as a linear combination of $q_{n\,i-u}$'s with coefficients not depending on i. □

We remark that Propositions 2.5 and 2.7 do not rely on the polynomials p_n satisfying the recursion given in Theorem 1.1.

Lemma 2.8. *(i) For non-negative integers $n \geq m$ we have*

$$p_n p_m = -(p_{n+m} + p_{n-m}).$$

(ii) For non-negative integers $n \geq m$ we have

$$(p_{n+m} + 2)(p_{n-m} + 2) = (p_n - p_m)^2.$$

(iii) For all $m, n \geq 0$ we have

$$\frac{1}{4\pi} \int_{-2}^{2} \frac{p_n p_m}{\sqrt{1 - p_1^2/4}} dp_1 = \delta_{mn}$$

(iv) For all $m, n \geq 0$ we have

$$p_{mn} = -(p_m p_{m(n-1)} + p_{m(n-2)}).$$

Proof. (i) From [R, p. 5] we have the following relation for $T_n(x)$: $T_n(x)T_m(x) = \frac{1}{2}(T_{n+m}(x) + T_{|m-n|}(x))$. The result follows by substituting for $p_n(x)$ using (1.1). (ii) From [R, p. 5] we also have $(T_n(x) - 1)(T_m(x) - 1) = (T_n(x) - T_m(x))^2$. Our relation for p_n follows from this. For (iii) use the well-known orthogonality condition for Chebyshev polynomials [R, p.30]. For (iv) use (1.1) and the relation $T_n(T_m(x)) = T_{mn}(x)$ for all $m, n \geq 0$ [R, p.5]. □

§3 Results on roots

In this section we will prove Theorem 1.2.

Proposition 3.1. *We have*
(i) $p_{2n} - 2 = -p_n^2$*;*
(ii) $p_{2n+1} - 2 = (p_1 - 2)(1 + \sum_{i=0}^n (-1)^i p_i)^2$*;*
(iii) (a) $p_{4n} + 2 = -(p_1 + 2)(p_1 - 2)(\sum_{i=1}^n p_{2i-1})^2$*;*
(iii) (b) $p_{4n+2} + 2 = -(p_1 + 2)(p_1 - 2)(1 + \sum_{i=0}^n p_{2i})^2$;
(iv) $p_{2n+1} + 2 = (p_1 + 2)(1 + \sum_{i=0}^n p_i)^2$*.*

Proof. (i) follows by putting $m = n$ in Lemma 2.8 (i). To prove the rest of this result we will need

Lemma 3.2. *We have*
(i) $(1 + \sum_{i=0}^n p_i)^2 = 2n + 1 - \sum_{i=0}^{2n-1} (i + 1)p_{2n-i}$;
(ii) $(1 + \sum_{i=0}^n (-1)^i p_i)^2 = 2n + 1 - \sum_{i=0}^{2n-1} (-1)^i (i + 1)p_{2n-i}$;
(iii) $(\sum_{i=1}^n p_{2i-1})^2 = n - \sum_{i=1}^{2n-2} (i + 1)p_{4n-2-2i}$;
(iv) $(1 + \sum_{i=0}^n p_{2i})^2 = 2n + 1 - \sum_{i=1}^{2n} i p_{4n+2-2i}$.

Proof. (i) This is by induction on $n \geq 0$, the cases $n = 0, 1$ being easily checked. Assume that $(1 + \sum_{i=0}^n p_i)^2 = 2n + 1 - \sum_{i=0}^{2n-1} (i + 1)p_{2n-i}$. Then

$$\begin{aligned}
(1 + \sum_{i=0}^{n+1} p_i)^2 &= ((1 + \sum_{i=0}^{n} p_i) + p_{n+1})^2 \\
&= (1 + \sum_{i=0}^{n} p_i)^2 + 2p_{n+1}(1 + \sum_{i=0}^{n} p_i) + p_{n+1}^2 \\
&= 2n + 1 - \sum_{i=0}^{2n-1} (i + 1)p_{2n-i} + 2p_{n+1} \\
&\qquad - 2\sum_{i=0}^{n} (p_{n+1+i} + p_{n+1-i}) - (p_{2n+2} + p_0) \\
&= 2n + 3 - \sum_{i=0}^{2n-1} (i + 1)p_{2n-i} - 2p_1 - 2p_{n+1} \\
&\qquad - 2\sum_{i=1}^{n} (p_{n+1+i} + p_{n+1-i}) - p_{2n+2} \\
&= 2n + 3 - \sum_{i=0}^{2n-1} (i + 1)p_{2n-i} - 2\sum_{i=1}^{n+1} (p_{n+1+i} + p_{n+1-i}) \\
&= 2n + 3 - \sum_{i=0}^{2n+1} (i + 1)p_{2n+2-i}.
\end{aligned}$$

The result follows.

The proofs of (ii), (iii) and (iv) are similar to the above. □

Now we use Lemma 3.2 (i) to prove Propositon 3.1 (iv):

$$(p_1+2)(1+\sum_{i=0}^{n}p_i)^2 = (p_1+2)(2n+1-\sum_{i=0}^{2n-1}(i+1)p_{2n-i})$$
$$= (2n+1)(p_1+2) - \sum_{i=0}^{2n-1}(i+1)(2p_{2n-i}-p_{2n+1-i}-p_{2n-1-i}).$$

One now sees that for $k \neq 0, 1, 2n+1$ the coefficient of p_k is

$$2(2n-k+1)-(2n+2-k)-(2n-k)=0,$$

as required. The constant term in the above is seen to be 2,the coefficient of p_1 is 0 while the coefficient of p_{2n+1} is 1. The result follows.

The proofs of the rest of Proposition 3.1 follow similarly from Lemma 3.2. □

Let $\alpha_{0\,\pm 1} = 1$ and for $n \geq 1$ let $\alpha_{n\,\epsilon}$, $\epsilon = \pm 1$, be the roots of the quadratic equation $\mathfrak{A}_n(x) = 0$, where $\alpha_{n\epsilon} = (-p_n + \epsilon\sqrt{p_n^2-4})/2$. By Lemma 2.8 (i) we have $p_n^2 - 4 = -p_{2n} - 2$; thus

$$\alpha_{n\,\epsilon} = (-p_n + \epsilon\sqrt{p_n^2-4})/2 = (-p_n + \epsilon\sqrt{-p_{2n}-2})/2$$

and by Proposition 3.1 the discriminant $-p_{2n} - 2$ can be written as $(p_1^2-4)u_n^2$ where u_n is given in Proposition 3.1 (iii) (a) and (b):

$$u_{2m} = \sum_{i=1}^{m} p_{2i-1} \quad \text{and} \quad u_{2m+1} = 1 + \sum_{i=0}^{m} p_{2i}.$$

We now wish to specify $\alpha_{n\,\epsilon}$ more explicitly by taking the square root of u_n^2 so as to be able to write

$$\alpha_{n\,\epsilon} = (-p_n + \epsilon u_n\sqrt{p_1^2-4})/2.$$

Lemma 3.3. *For positive integers $n \geq m$ we have*
(i) $p_{2n}\sum_{i=1}^{m} p_{2i-1} \pm p_{2m}\sum_{i=1}^{n} p_{2i-1} = -2\sum_{i=1}^{n\pm m} p_{2i-1}$;
(ii) $p_{2n}p_{2m} \pm (p_1^2-4)(\sum_{i=1}^{n} p_{2i-1})(\sum_{i=1}^{m} p_{2i-1}) = -2p_{2(n\pm m)}$;
(iii) (a) $p_{2n}(1+\sum_{i=0}^{m} p_{2i}) + p_{2m+1}\sum_{i=1}^{n} p_{2i-1} = 2 - 2\sum_{i=1}^{n+m} p_{2i}$;
(iii) (b) $p_{2n}(1+\sum_{i=0}^{m} p_{2i}) - p_{2m+1}\sum_{i=1}^{n} p_{2i-1} = 2 - 2\sum_{i=1}^{n-m-1} p_{2i}$;
(iv) $p_{2n}p_{2m+1} \pm (p_1^2-4)(\sum_{i=1}^{n} p_{2i-1})(1+\sum_{i=0}^{m} p_{2i}) = -2p_{2(n\pm m)\pm 1}$;
(v) (a) $p_{2n+1}(1+\sum_{i=0}^{m} p_{2i}) + p_{2m+1}(1+\sum_{i=0}^{n} p_{2i}) = -2\sum_{i=1}^{n+m+1} p_{2i-1}$;
(v) (b) $p_{2n+1}(1+\sum_{i=0}^{m} p_{2i}) - p_{2m+1}(1+\sum_{i=0}^{n} p_{2i}) = 2\sum_{i=1}^{n-m} p_{2i-1}$.
(vi) (a) $p_{2n+1}p_{2m+1} + (p_1^2-4)(\sum_{i=0}^{n} p_{2i})(1+\sum_{i=0}^{m} p_{2i}) = -2p_{2(n+m+1)}$;
(vi) (b) $p_{2n+1}p_{2m+1} - (p_1^2-4)(\sum_{i=0}^{n} p_{2i})(1+\sum_{i=0}^{m} p_{2i}) = -2p_{2(n-m)}$.

Proof. All of the proofs are straightforward applications of Lemma 2.8 (i). One uses the relations:

$$\begin{cases} p_n u_m = -u_{n+m} - u_{m-n}, & \text{if} \quad m \geq n \quad \text{and} \\ p_n u_m = -u_{n+m} + u_{n-m} & \text{if} \quad n \geq m \end{cases}$$

which are also proved using Lemma 2.8. □

The following result proves Theorem 1.2.

Proposition 3.4. *For all positive integers $n \geq m$ and $\epsilon, \delta \in \{\pm 1\}$ there are integers N, Δ with $\Delta \in \{\pm 1\}$ and $N = n \pm m$ such that $\alpha_{n\,\epsilon}\alpha_{m\,\delta} = \alpha_{N\,\Delta}$. In particular we have*
(i) $\alpha_{n\,\epsilon}\alpha_{n\,-\epsilon} = 1$, for all $n \geq 0$ and $\epsilon \in \{\pm 1\}$.
(ii) $\alpha_{2n\,\epsilon}\alpha_{2m\,\delta} = \alpha_{2(n+\epsilon\delta m)\,\epsilon}$, for all $n \geq m \geq 1$ and $\epsilon, \delta \in \{\pm 1\}$;
(iii) $\alpha_{2n\,\epsilon}\alpha_{2m+1\,\delta} = \alpha_{2n+\epsilon\delta(2m+1)\,\epsilon}$, for all $2n \geq 2m+1 \geq 1$ and $\epsilon, \delta \in \{\pm 1\}$;
(iv) $\alpha_{2n+1\,\epsilon}\alpha_{2m\,\delta} = \alpha_{2n+1+\epsilon\delta 2m\,\epsilon}$, for all $2n+1 \geq 2m \geq 1$ and $\epsilon, \delta \in \{\pm 1\}$;
(iv) $\alpha_{2n+1\,\epsilon}\alpha_{2m+1\,\delta} = \alpha_{2n+1+\epsilon\delta(2m+1)\,\epsilon}$, for all $2n+1 \geq 2m+1 \geq 1$ and $\epsilon, \delta \in \{\pm 1\}$.

Proof. (i) is obvious since $\alpha_{n\epsilon}$ is a root of $s^2 + p_n s + 1$. We will now prove (ii) and (iii), the rest being similar. For (ii) we have, using Proposition 3.1 (iii) (a) and Lemma 3.3 (i) and (ii),

$$\begin{aligned}
\alpha_{2n\,\epsilon}\alpha_{2m\,\delta} &= \left(-p_{2n} + \epsilon u_{2n}\sqrt{p_1^2 - 4}\right)/2\left(-p_{2m} + \delta u_{2m}\sqrt{p_1^2 - 4}\right)/2 \\
&= \left(p_{2n}p_{2m} + \epsilon\delta(p_1^2 - 4)\sum_{i=1}^{n} p_{2i-1}\sum_{i=1}^{m} p_{2i-1}\right)/4 \\
&\qquad - \left(\epsilon p_{2m}\sum_{i=1}^{n} p_{2i-1}\sqrt{p_1^2 - 4} + \delta p_{2n}\sum_{i=1}^{m} p_{2i-1}\sqrt{p_1^2 - 4}\right)/4 \\
&= \left(-2p_{2(n+\epsilon\delta m)} + \epsilon 2\sum_{i=1}^{n+\epsilon\delta m} p_{2i-1}\sqrt{p_1^2 - 4}\right)/4 \\
&= \alpha_{2(n+\epsilon\delta m)\,\epsilon}.
\end{aligned}$$

For (iii) we have to consider two cases, $\epsilon = \pm\delta$, so that for $\epsilon = -\delta$ we have

$$\begin{aligned}
\alpha_{2n\,\epsilon}\alpha_{2m+1\,-\epsilon} &= \frac{1}{4}\left(-p_{2n} + \epsilon u_{2n}\sqrt{p_1^2 - 4}\right)\left(-p_{2m+1} - \epsilon u_{2m+1}\sqrt{p_1^2 - 4}\right) \\
&= \frac{1}{4}\left(p_{2n}p_{2m+1} - (p_1^2 - 4)\sum_{i=1}^{n} p_{2i-1}(1 + \sum_{i=0}^{m} p_{2i})\right) \\
&\qquad - \frac{1}{4}\left(\epsilon p_{2m+1}\sum_{i=1}^{n} p_{2i-1} - \epsilon p_{2n}(1 + \sum_{i=1}^{m} p_{2i})\right)\sqrt{p_1^2 - 4} \\
&= \frac{1}{4}\left(-2p_{2n-2m-1} + \epsilon(2 - 2\sum_{i=0}^{n-m-1} p_{2i}\sqrt{p_1^2 - 4})\right) = \alpha_{2n-2m-1,\epsilon}.
\end{aligned}$$

The other case is proved similarly. $\square$

§4 Proof of Theorem 1.1

Since the roots $\alpha_{n,j}$ are distinct the recursion given by Proposition 2.5, together with standard results about recursions (see for example [B] Ch. 7) allow us to conclude that for fixed n, y there are constants $c_{n,y,j,k}$ such that

$$r_{n,i,y} = c_{n,y,0,0} + \sum_{j=1}^{n}(c_{n,y,j,-}\alpha_{j,-}^{i} + c_{n,y,j,+}\alpha_{j,+}^{i}) \tag{4.1}$$

for each $i \geq 0$.

Conversely, we note that for $N \geq n$ and for any constants $c_{n,y,j,k}$ we have

$$\sum_{i=0}^{2N+1} q_{N,i} \left(c_{n,y,0,0} + \sum_{j=1}^{n} (c_{n,y,j,-}\alpha_{n,-}^{i} + c_{n,y,j,+}\alpha_{n,+}^{i}) \right) = 0. \tag{4.2}$$

But by (4.1) we see that for fixed n, m, j, k and varying i any product $r_{n,i,j}r_{m,i,k}$ can be written as a linear sum of terms each of which is either constant or has the form $\alpha_{n,u}^{i}$ or $\alpha_{n,u}^{i}\alpha_{m,v}^{i}$. But by Proposition 3.4 any such term is of the form $\alpha_{N,w}^{i}$ where $N \leq n+m$. Thus by (4.2) the sum $\sum_{i=0}^{2(n+m)+1} q_{n+m,i}r_{n,i,j}r_{m,i,k}$ is zero, as required. $\square$

§5 Braid group action on simple closed curves on surfaces

Let $\mathcal{C}^m = \mathcal{C}_n^m$ denote the set of isotopy classes of oriented simple closed curves on D_n where each such simple closed curve surrounds m of the punctures.

In [H2] we used the action of B_n on $\mathcal{C}^2$ to obtain linear representations of the braid groups B_n over $\mathbb{Z}[t]$ by first finding a natural map from $\mathcal{C}^2$ to a polynomial algebra, and then considering the induced action of B_n on certain quotients of ideals in this polynomial algebra. We need to explain some of this more carefully now.

For R a commutative ring with identity we defined the ring $R_n[a_{ij}]$ in §1. It will be convenient for us to let $a_{ii} = 0$ for all $i = 1, \ldots, n$.

For $i, j, k, \ldots, r, s \in \{1, 2, \ldots, n\}$ let $c_{ijk\ldots rs}$ denote the *cycle* $a_{ij}a_{jk}\ldots a_{rs}a_{si} \in R_n[a_{ij}]$. Then the cycles generate a subalgebra of $R_n[a_{ij}]$ denoted Y_n. A cycle $c_{ijk\ldots rs}$ will be called *simple* if $i, j, k, \ldots, r, s$ are all distinct. The ring Y_n is generated by the (finite number of) simple cycles.

Note that the action of B_n on D_n fixes the boundary of D_n and so there is an induced action of B_n on the fundamental group of D_n (where we choose a base point p on the boundary of D_n). This fundamental group is the free group F_n of rank n. We choose a standard set of generators $x_1, \ldots, x_n$ for F_n, where x_i is a simple closed curve enclosing the ith puncture π_i and such that $x_1x_2\ldots x_n$ is parallel to the boundary of D_n. See Figure 1.

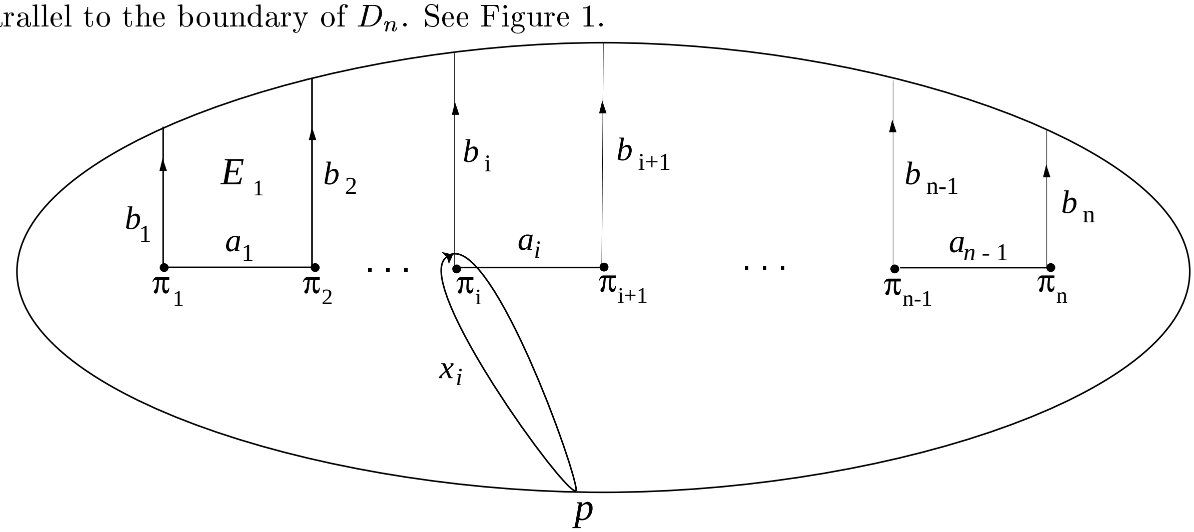

Figure 1

In Figure 1 we have shown the arcs a_i and the generators x_i; we have also shown some *cut arcs* $b_1, \ldots, b_n$ for the generators $x_1, \ldots, x_n$. Thus if c is an oriented simple closed curve in D_n which is based at p and which is in general position with all the arcs b_i, then the word $w(c)$ in F_n corresponding to c is determined by the sequence of oriented intersections of c with the oriented arcs $b_1, \ldots, b_n$.

The action of B_n on the generators x_i is as follows:

$$\sigma_j(x_i) = x_i \quad \text{if } i \neq j, j+1, \quad \sigma_j(x_j) = x_j x_{j+1} x_j^{-1}, \quad \sigma_j(x_{j+1}) = x_j.$$

We now find a particularly convenient representation of the free group F_n. For $i = 1, \ldots, n$ define the following $n \times n$ matrices (transvections)

$$T_i = \begin{pmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \ldots & \vdots & \vdots \\ a_{i1} & a_{i2} & \ldots & 1 & \ldots & a_{in-1} & a_{in} \\ \vdots & \vdots & \ldots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & \ldots & 0 & 1 \end{pmatrix}$$

where the non-zero off-diagonal entries occur in the ith row. Here a *transvection* [A] is a matrix $M = I_n + A$ where I_n is the identity matrix, $det(M) = 1$ and $A^2 = 0$. In particular, conjugates of transvections are transvections.

Then $< T_1, \ldots, T_n >$ is a free group of rank n (see [H1]). This allows us to identify x_i and T_i for $i = 1, \ldots, n$ and so to identify F_n and $< T_1, \ldots, T_n >$.

Now, from the above, B_n acts by automorphisms on F_n in such a way that for $\alpha \in B_n$ the matrix $\alpha(T_i)$ is a conjugate of some T_j, $1 \leq j \leq n$ i.e. $\alpha(T_i)$ is also a transvection. Further, if $c \in \mathcal{C}^\infty$, then c represents a conjugacy class in F_n and so its *trace* is well-defined (the trace of the corresponding product of transvections in $F_n =< T_1, \ldots, T_n >$). In fact one easily sees that $trace(c) \in Y_n$ [H1]. Then a map $\phi : \mathcal{C} \to R_n$ is defined uniquely by

$$\phi(c) = trace(c) - n.$$

Thus ϕ can be thought of as being defined on certain conjugacy classes of elements of F_n (namely those representing simple closed curves). This map can be extended to act on all of F_n, by the requirement that for $s \in F_n$ we have $\phi(s) = trace(s) - n$.

Now for $m \geq n$ and $s \in F_n$ we may also consider s as an element of F_m under the natural inclusion of F_n in F_m. In this case we note that $\phi(s)$ has the same value whether we consider s as an element of F_n or F_m.

Now for all i, j we have $trace(T_i T_j) = a_{ij} a_{ji} + n$ and in general if $A, B \in F_n$, then

$$trace(A T_i A^{-1} B T_j B^{-1}) = b_{ij} b_{ji} + n$$

where $b_{ij} \in R_n[a_{ij}]$ (see [H1]; in fact this also follows from Proposition 7.1). It is also easy to see that there is a natural choice so that

$$b_{ij} = a_{ij} + \text{terms of higher degree.}$$

Now for $\alpha \in B_n$ the image $\alpha(T_i)$ is a conjugate $A T_j A^{-1}$ for some $A \in F_n$ and $1 \leq j \leq n$. Here the action of α on the a_{ij} is defined by

$$trace(\alpha(T_i)\alpha(T_j)) = \alpha(a_{ij})\alpha(a_{ji}) + n,$$

(see [H1] for more details) so that it has the following naturality property (with respect to the action of B_n on F_n): for all $w \in < T_1, \dots, T_n >$ we have

$$\phi(\alpha(w)) = \alpha(\phi(w)). \tag{5.1}$$

For example the action of σ_i is given by

$$\begin{aligned}
&\sigma_i(a_{i\,i+1}) = a_{i+1\,i}, \quad \sigma_i(a_{i+1\,i}) = a_{i\,i+1}, \quad \sigma_i(a_{h\,i}) = a_{h\,i+1},\\
&\sigma_i(a_{h\,i+1}) = a_{h\,i} - a_{h\,i+1}a_{i+1,i}, \quad \sigma_i(a_{i\,j}) = a_{i+1\,j},\\
&\sigma_i(a_{i+1\,j}) = a_{i\,j} + a_{i\,i+1}a_{i+1\,j}, \quad \text{etc.}
\end{aligned}$$

where $1 \le h < i$, $i+1 < j \le n$.

It follows from Theorem 2.5 and Theorem 6.2 of [H1] that the kernel of the action of B_n on R_n is the centre of B_n and that if B_n and R_n are thought of as sub-objects of B_{n+1} and R_{n+1} (respectively), then the action of B_n on R_{n+1} is faithful. We note as in [Hu2] that there is a natural ring involution $*$ on $R_{(n)}[a_{ij}]$ which commutes with the action of B_n; this involution is determined by its action on the generators a_{ij} which is as follows: $a_{ij}^* = -a_{ji}$. This involution has the following property:

$$trace(A^{-1}) = trace(A)^*,$$

for all $A \in F_n$. Thus $\phi(c^{-1}) = \phi(c)^*$, where c^{-1} is the curve c with its orientation reversed.

If c is a simple closed curve in D_n surrounding k punctures, then we let $\Sigma(c)$ denote the *spine* of γ, so that $\Sigma(\gamma)$ is an embedded tree in $D_n \cup \{\pi_1, \dots, \pi_n\}$ whose k vertices are in $\{\pi_1, \dots, \pi_n\}$ and such that c is isotopic to the boundary of a small tubular neighbourhood of $\Sigma(c)$ (with some orientation).

Suppose that c is a simple closed curve which is disjoint from γ_{12}. Then $\sigma_1(c) = c$ and so $\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)(\phi(c)) = 0$ which shows that $\Omega(c) = 0$. It easily follows that for such a curve $2\Omega(c) = \iota(\gamma_{12}, c)$. The key observation that indicates a connection with the previous sections was made in [H2] and is

Lemma 5.1. *Let $\alpha, \beta_1, \beta_2, \gamma_1, \gamma_2 \in \mathcal{C}^2$ be curves with spines as shown in Figure 2, where we assume that there are no punctures inside the heart-shaped diagram other than the three shown (π_i, π_j and π_k).*

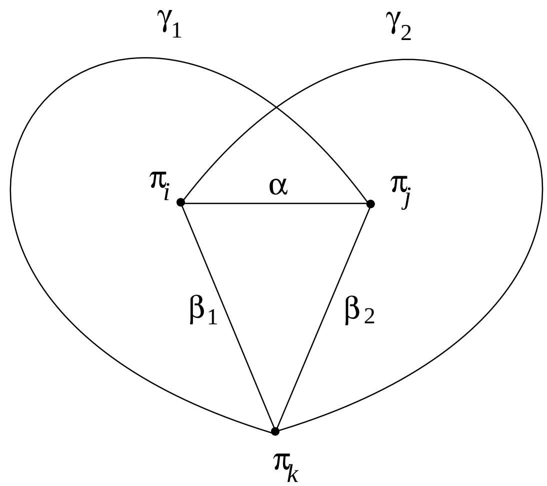

Figure 2

Then we have the following relation:

$$[\phi(\gamma_1) - \phi(\gamma_2)] + (1 + a_{12}a_{21})[\phi(\beta_1) - \phi(\beta_2)] = 0. \tag{5.2}$$

Now note that we may take $\gamma_1 = \sigma_1^2(\gamma_{23})$, $\gamma_2 = \sigma_1^{-1}(\gamma_{23})$, $\beta_1 = \gamma_{23}$ and $\beta_2 = \sigma_1(\gamma_{23})$. (In fact the proof of Lemma 5.1 consists essentially of checking that the relation holds in this case, which is easily done.) Thus we can write (5.2) as $(\sigma_1^2 - \sigma_1^{-1} - (1 + a_{12}a_{21})(1 - \sigma_1))[\gamma_{23}] = 0$. Upon acting on this equation by σ_1 on the left and factoring this gives (since $\sigma_1(a_{12}a_{21}) = a_{12}a_{21}$)

$$(\sigma_1 - 1)(\sigma_1^2 + (2 + a_{12}a_{21})\sigma_1 + 1)\phi(\gamma_{23}) = 0. \tag{5.3}$$

Thus if $p_1 = a_{12}a_{21} + 2$, then the above operator is $\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)$ and we have $\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(\phi(\gamma_{23})) = 0$. Now if c is any curve such that if $\iota(\gamma_{12}, c) = 2$, then the pair (γ_{12}, c) is diffeomorphic to the pair $(\gamma_{12}, \gamma_{23})$ and we check that $\mathfrak{B}_0(\sigma_1, a_{12}a_{21} + 2)(\phi(\gamma_{23})) \neq 0$. The above gives $\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(\phi(\gamma_{23})) = 0$. Thus $\mathfrak{B}_0(\sigma_1, a_{12}a_{21} + 2)(\phi(c)) \neq 0$ and $\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(\phi(c)) = 0$.

Now we note that up to diffeomorphism there are only two ways in which we can have $\iota(\gamma_{12}, c) = 4$. These are (i) $w(c) = x_2(x_3 \ldots x_u)x_2^{-1}(x_{u+1}x_{u+2} \ldots x_v)$; and (ii) $w(c) = x_2(x_3 \ldots x_v)x_1(x_3 \ldots x_u)^{-1}$ where $2 < u < v \leq n$. One easily checks that $\mathfrak{B}_2(\sigma_1, a_{12}a_{21} + 2)(\phi(c)) = 0$ and $\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(\phi(c)) \neq 0$ in each case. Thus we have proved

Lemma 5.3. *If c is a simple closed curve on D_n with $\iota(\gamma_{12}, c) \leq 2$, then $2\Omega(c) = \iota(\gamma_{12}, c)$.* $\square$

This indicates the initial connection of the operators $\mathfrak{B}_n(\sigma, a_{12}a_{21} + 2)$ with intersection-number functions. We now prove:

Proposition 5.4. *Let U_n be the subring of R_n which is generated by all elements of the form a_{ij} for $2 < i, j \leq n$ and all*

$$a_{i1}a_{1j},\ a_{i2}a_{2j},\ a_{12}a_{21},\ a_{i1}a_{12}a_{2j},\ a_{i2}a_{21}a_{1j}$$

for $2 < i, j \leq n$. Then U_n contains Y_n and for $u \in U_n$ there is a positive integer $N = N(u)$ such that $\mathfrak{B}_N(\sigma_1, a_{12}a_{21} + 2)(u) = 0$.

Proof. As we noted before Y_n is generated by the simple cycles and it is easily seen that each such simple cycle is in U_n. Next we check that for $2 < i, j \leq n$ we have $\mathfrak{B}_0(a_{ij}) = 0$ and

$$\begin{aligned} \mathfrak{B}_1(a_{i1}a_{1j}) = 0,\ \mathfrak{B}_1(a_{i2}a_{2j}) = 0,\ \mathfrak{B}_0(a_{12}a_{21}) = 0, \\ \mathfrak{B}_1(a_{i1}a_{12}a_{2j}) = 0,\ \mathfrak{B}_1(a_{i2}a_{21}a_{1j}) = 0. \end{aligned} \tag{5.4}$$

The result now follows from Theorem 1.1. $\square$

For $u \in U_n$ we will let $\Omega(u)$ denote the minimal N such that $\mathfrak{B}_N(\sigma_1, a_{12}a_{21} + 2)(u) = 0$.

We note that the operators $\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)$ act on some R_n and so depend on the number n. However it will be convenient for us to ignore this dependency, so that $\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)$ will be considered as acting on all of the $R_n, n \geq 2$. This is consistent with considering D_n as a subspace of D_{n+1} for all n.

§6 A normal form for curves on D_n

Let c be a simple closed curve on D_n and let $w(c) \in F_n$ represent c. Note that we may (and will) choose $w(c)$ to be cyclically reduced. We will say that a cyclically reduced word $w \in F_n$ is *1,2-reduced* if w is cyclically conjugate to a word of the form $w' = A_1B_1 \dots A_rB_r$, where

$$A_i \in < T_3, T_4, \dots, T_n > \quad \text{and} \quad B_i \in \{T_1^{\pm 1}, T_2^{\pm 1}, (T_1T_2)^{\pm 1}\}$$

with $A_i \neq id$ for $i = 1, \dots r$.

In this section we prove the following result which gives a normal form for an element of F_n representing a simple closed curve on D_n and derive some relevant consequences.

Theorem 6.1. *Let c be a simple closed curve on D_n. Then there is $k \in \mathbb{Z}$ such that $w(\sigma_1^k(c))$ is $1,2$-reduced.*

Proof. Considering Figure 1 in §5 we see that the arcs a_1, b_1, b_2 cut off a simply-connected subset E_1 of D_n. See Figure 3. Let O_1 denote a tubular neighbourhood of the union of E_1 and the interior of the curve x_1 in D_n such that O_1 contains only the punctures π_1, π_2 together with the base point p.

Let c be a simple closed curve on D_n. Then $w(c)$ certainly has a cyclic conjugate w' which can be written $w' = A_1B_1 \dots A_rB_r$, where $A_i \in < T_3, T_4, \dots, T_n >$, $B_i \in < T_1, T_2 >$ and $A_i, B_i \neq id$ for $i = 1, \dots r$. Fix $1 \leq i \leq r$ and let $T_u^{\pm 1}, T_v^{\pm 1}$ be the terminal and initial letters of A_i and A_{i+1} respectively. Since $u, v \geq 3$ we see that there is a subarc c' of c, with end points on the cut arcs b_u and b_v, representing the subword $T_u^{\pm 1}B_iT_v^{\pm 1}$. Now note that we can homotope c' so that the end points go to p, while all the points of $c' \cap E_1$ are held fixed during the homotopy. Call the resulting curve $c'' = c_i''$. We may also require that c'' is in O_1. Now O_1 is a twice-puctured disc and c'' is a simple closed curve in O_1 based at p. Further, the fundamental group of O_1 based at p is generated by x_1, x_2. It follows that either (i) $c'' = \sigma_1^k(x_1^{\pm 1})$ for some $k = k(i) \in \mathbb{Z}$, or (ii) $c'' = \gamma_{12}^{\pm 1}$. These two cases occur when the interior of c'' has one or two punctures inside it (respectively).

If for all $i = 1, \ldots, r$ we have case (ii), then w' is $1,2$-reduced and the Theorem follows. If, on the other hand, there is some $1 \leq i \leq r$ such that we have case (i), then we replace c by $\sigma_1^{-k}(c)$. This means that we can assume that $A_1 = T_1^{\pm 1}$ (cyclically permute w' as necessary). Now if for any $1 < j \leq r$ we now have $k(j) \neq 0$, then the curve c_j'' can be homotoped so as to meet x_1 only at the base point p. It follows that c_j'' is either (a) $x_1^{\pm 1}$; (b) $x_2^{\pm 1}$; (c) $\gamma_{12}^{\pm 1}$; or (d) the curve $\sigma_1(x_1)$, this being the curve $x_1 x_2 x_1^{-1}$. The first three cases are covered by Theorem 6.1, while if we have the fourth case, then we act on c by σ_1^{-1} so that now we have $A_1 = T_2^{\pm 1}$ and $A_j = T_1^{\pm 1}$.

Now suppose that we are in this latter case where $A_1 = T_2^{\pm 1}$ and $A_j = T_1^{\pm 1}$. Let $1 < i \leq r$, $i \neq j$. Then c_i'' can be homotoped so as to meet x_1 and x_2 only at the point p. One easily sees that either (i) $c_i'' = x_1^{\pm 1}$; or (ii) $c_i'' = x_2^{\pm 1}$; or (iii) $c_i'' = (x_1 x_2)^{\pm 1}$, and so w' is $1,2$-reduced. □

For c and k as in Theorem 6.1 we will call $w(\sigma_1^k(c))$ the *normal form* for c. We note that the normal form is not unique.

Lemma 6.2. *Let $k \in \mathbb{Z}$ and let c be a simple closed curve on D_n and let $c' = \sigma_1^k(c)$; for example c' could be the normal form for c. If $\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)(\phi(c)) = 0$, then $\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)(\phi(\sigma_1^k(c))) = 0$. In particular, we have $\Omega(c') = \Omega(c)$.*

Proof. Since $\sigma_1(a_{12}a_{21}) = a_{12}a_{21}$ it follows that σ_1 commutes with the operator $\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)$. Also, we have $\phi(\sigma_1^k(c)) = \sigma_1^k(\phi(c))$ by (5.1). Thus

$$\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)(\phi(\sigma_1^k(c))) = \sigma_1^k(\mathfrak{B}_m(\sigma_1, a_{12}a_{21} + 2)(\phi(c))) = 0.$$

The rest follows from this. □

We now show the connection of the above normal form with intersection-numbers.

Theorem 6.3. *Let c be a simple closed curve on D_n and let $c' = \sigma_1^k(c)$ be its normal form. Suppose that $w(c') = A_1 B_1 \ldots A_r B_r$, where $A_i \in < T_3, T_4, \ldots, T_n >$, $B_i \in \{T_1^{\pm 1}, T_2^{\pm 1}, (T_1 T_2)^{\pm 1}\}$ and $A_i \neq id$ for $i = 1, \ldots r$. Let h be the number of i such that $B_i \in \{T_1^{\pm 1}, T_2^{\pm 1}\}$. Then $h = \iota(\gamma_{12}, c') = \iota(\gamma_{12}, c)$.*

Proof. It is clear that $\iota(\gamma_{12}, c') = \iota(\gamma_{12}, c)$ from Lemma 6.2. Now note that in a neighbourhood of E_1 (oriented) arcs coming from any B_i are as shown in Figure 3.

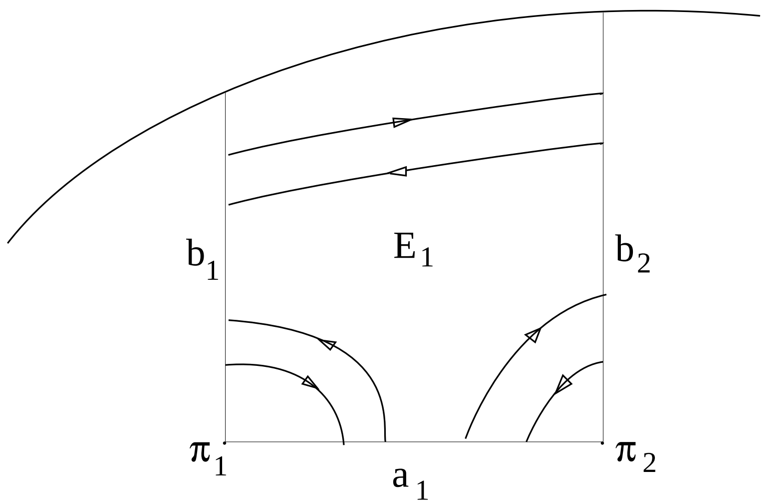

Figure 3

Now any $B_i = T_1^{\pm 1}$ corresponds to an arc of $c \cap E_1$ which crosses the arc b_1 once and does not cross b_2. It thus crosses a_1 and contributes 1 to the intersection number $\iota(\gamma_{12}, c)$. Similarly for any $B_i = T_2^{\pm 1}$. Lastly, any $B_i = (T_1 T_2)^{\pm 1}$ corresponds to an arc of $c \cap E_1$ which does not cross a_1. The result follows. $\square$

§7 Combinatorial results on traces

In this section we will introduce a way of grouping together terms of $\phi(c)$ and use this to prove that $\Omega(c) \leq \iota(c, \gamma_{12})/2$.

Let $w = T_{i_1}^{e_1} T_{i_2}^{e_2} \dots T_{i_r}^{e_r} \in F_n =< T_1, \dots, T_n >$ where $e_i = \pm 1$ for $i = 1, \dots, r$. Then by a *subword* of w we mean any $w' = T_{i_a}^{e_a} T_{i_b}^{e_b} \dots T_{i_z}^{e_z}$ where $1 \leq a < b < \cdots < z \leq r$. In fact we will really be thinking of w' as being the sequence $1 \leq a < b < \cdots < z \leq r$, but it will be convenient to write $w' = T_{i_a}^{e_a} T_{i_b}^{e_b} \dots T_{i_z}^{e_z}$. We will need the following generalisation of [H1, Lemma 2.3].

Proposition 7.1. *Let $w = T_{i_1}^{e_1} T_{i_2}^{e_2} \dots T_{i_r}^{e_r} \in F_n$. Then $trace(w) - n$ is equal to the sum of all terms of the form*

$$(e_h e_i e_j e_k \dots e_m) a_{hi} a_{ij} a_{jk} \dots a_{mh},$$

where $T_h^{e_h} T_i^{e_i} T_j^{e_j} T_k^{e_k} \dots T_m^{e_m}$ is a non-empty subword of w.

Proof. We first prove the following result by induction. The induction hypothesis is: the hk entry of the matrix w is the sum of all terms of the kind

$$(e_{j_1} e_{j_2} e_{j_3} e_{j_4} \dots e_{j_m}) a_{j_1 j_2} a_{j_2 j_3} a_{j_3 j_4} \dots a_{j_m k},$$

where $T_{j_1}^{e_{j_1}} \dots T_{j_m}^{e_{j_m}}$ is a subword of w and $j_1 = h$. This is easily proved (similar to the proof of Lemma 2.3 of [H1]) and Lemma 7.1 follows directly from this. $\square$

Thus, for example, if $n = 4$ and $w = T_1 T_2^2 T_3^3 T_2^{-1}$, then

$$trace(w) - 4 = a_{12}a_{21} + 3a_{13}a_{31} + 3a_{23}a_{32} - 3a_{13}a_{32}a_{21} + 6a_{12}a_{23}a_{31} - 6a_{12}a_{21}a_{23}a_{32}.$$

We introduce the following notation: Fix a word $w = T_{i_1}^{e_1}T_{i_2}^{e_2}\dots T_{i_r}^{e_r} \in F_n$, which we will think of as a cyclic word. Then by Lemma 7.1 for any subword $s = T_h^{e_h}T_i^{e_i}T_j^{e_j}\dots T_m^{e_m}$ of w we obtain the contribution

$$\eta(s) = (e_he_ie_je_k\dots e_m)a_{hi}a_{ij}a_{jk}\dots a_{mh}$$

to the trace of w. Such a contribution we call a *term*. Note that by Lemma 7.1 $trace(w) - n$ is the sum of all such terms $\eta(s)$ for all such non-empty subwords s of w. We now look for a way of grouping together some of these terms in a way that will be compatible with the action of the operators $\mathfrak{B}_n(\sigma_1, a_{12}a_{21}+2)$.

Let s be a subword of w. Then we can write $\eta(s)$ uniquely as

$$\eta(s) = Ca_1b_1a_2b_2\dots a_ub_ua_{u+1},$$

where C is a constant, a_i is either 1 or is a monomial in the generators a_{rs} where $r, s \geq 3$ and b_i is a monomial of the form $a_{ri_1}a_{i_1i_2}\dots a_{i_{t-1}i_t}a_{i_ts}$ where $r, s \geq 3$ and $i_j \in \{1,2\}$ for $j = 1,\dots,t$. Note that $\Omega(a_i) = 0$ for all i and so by Theorem 1.1 we see that

$$\Omega(a_1b_1a_2b_2\dots a_ub_ua_{u+1}) \leq \Omega(b_1) + \Omega(b_2) + \cdots + \Omega(b_u). \tag{7.1}$$

Now we define a *12 -reduction* of s to be any subword s' of s which can be obtained from s by deleting any (or all) of the letters $T_1^{\pm1}$ or $T_2^{\pm1}$ occuring in s.

Let $\psi_{\hat{1}\hat{2}}(s)$ denote the sum of all of the $\eta(s')$ where s' is a 12 -reduction of s. From the above we see the following:

Lemma 7.2. *Let s be a subword of w as above and write $a = A_1B_1\dots A_uB_uA_{u+1}$ where $A_i \in < T_3,\dots,T_n >$ and $B_i \in < T_1, T_2 > \setminus\{id\}$. Then the element $\psi_{\hat{1}\hat{2}}(s)$ has a factorization*

$$\psi_{\hat{1}\hat{2}}(s) = E_1G_1E_2G_2\dots G_{u-1}E_uG_uE_{u+1}$$

where $E_i = 1$ or $E_i = \psi_{\hat{1}\hat{2}}(A_i) \in R[a_{rs}|3 \leq r \neq s \leq n]$ and $G_i = \psi_{\hat{1}\hat{2}}(t_i)$ where t_i is the subword $T_{y_i}^pB_iT_{z_i}^q$ for some $p, q = \pm1$ and $y_i, z_i \geq 3$. □

Example 7.3. Let $s = T_3T_1T_2T_4T_6T_4T_2^{-1}T_5T_1T_5$. Then

$$\psi_{\hat{1}\hat{2}}(s) = (a_{31}a_{12}a_{24} + a_{31}a_{14} + a_{32}a_{24} + a_{34})a_{46}a_{64}(-a_{42}a_{25} + a_{45})(a_{51}a_{15})a_{53}.$$

We now calculate the $G_i = \psi_{\hat{1}\hat{2}}(t_i)$ in the above Lemma.

Lemma 7.4. *Choose integers $3 \leq r, s \leq n$ and $u \geq 0$. Then*

$$\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(T_r(T_1T_2)^uT_s)) = 0, \quad \text{and}$$
$$\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(T_r(T_2^{-1}T_1^{-1})^uT_s)) = 0,$$

while if $y \in < T_1, T_2 >$, then

$$\mathfrak{B}_1(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(T_ryT_s)) = 0.$$

Proof. Now any monomial summand of $\psi_{\hat{1}\hat{2}}(T_ryT_s)$ is of the form $Ca_{ri_1}a_{i_1i_2}\dots a_{i_us}$ where C is a constant and $i_1, i_2, \dots, i_u = 1, 2$. Any such word can be factored as

$C(a_{12}a_{21})^kQ$ where Q is one of $a_{r1}a_{1s}, a_{r1}a_{12}a_{2s}, a_{r2}a_{2s}, a_{r2}a_{21}a_{1s}$. Now the second part of the result follows from Theorem 1.1 and equations (5.4) which show that $\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)((a_{12}a_{21})^k) = 0$ and $\mathfrak{B}_1(\sigma_1, a_{12}a_{21}+2)(Q) = 0$.

Now consider the element $w = T_r(T_1T_2)^kT_s$. Then by Lemma 7.1 we have

$$trace(w) - n = \psi_{\hat{1}\hat{2}}(w)a_{sr} + U,$$

where each monomial summand μ of U is a product of a_{ij}'s where the set of such subscripts i, j for this fixed μ contains only one of r, s.

But w represents a closed curve c on D_n which, since $r, s > 2$, does not meet the arc a_1. Thus we have $\sigma_1(c) = c$ which implies (by (5.1)) that $\sigma_1(trace(w) - n) = trace(w) - n$. Since $\sigma_1(a_{sr}) = a_{sr}$ we see that we must have $\sigma_1(\psi_{\hat{1}\hat{2}}(w)) = \psi_{\hat{1}\hat{2}}(w)$ from which it follows that $\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(w)) = 0$. $\square$

Refering back to Lemma 7.2 we now have

Lemma 7.5. *Let $w \in F_n$. Let $\eta(s) = A_1B_1A_2B_2\dots B_uA_{u+1}$, for a subword s of w.*

Suppose that k of the B_i are of the form T_1^u or T_2^u. Then

$$\mathfrak{B}_k(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(s)) = 0.$$

Proof. This follows from Lemma 7.2, Lemma 7.4 and equation (7.1). $\square$

Let c be a simple closed curve and let $w = w(c)$. Let $\eta(w) = A_1B_1\dots B_uA_{u+1}$. Let w' be the word $w' = w'(w) = A_1A_2\dots A_{u+1}$. Now to every subword of w' there corresponds naturally a subword of $\eta(w)$; conversely, we can *project* any subword s of $\eta(w)$ to a subword $\zeta(s)$ of w' by just deleting from the subword s all T_1^j's and T_2^j's that are in it.

Now let $\mathcal{S}$ denote the set of all subwords of $\eta(w)$ (including the empty subword). Let $\mathcal{S}'$ denote the set of all subwords of $\eta(w')$. Then we have a natural map $\beta : \mathcal{S} \to \mathcal{S}'$, which consists of deleting from any element of $\mathcal{S}$ all elements of the form T_1^j or T_2^j. We partition the elements of $\mathcal{S}$ into preimages of β. This in turn gives a way of collecting together terms of $\phi(c) = trace(w) - n$ into sums each of which has the form $E_1G_1E_2G_2\dots G_{u-1}E_uG_uE_{u+1}$ indicated in Lemma 7.2. Now if k is as defined in Lemma 7.5, then at most k of the G_i in $E_1G_1E_2G_2\dots G_{u-1}E_uG_uE_{u+1}$ can satisfy $\mathfrak{B}_0(\sigma_1, a_{12}a_{21}+2)(G_i) \neq 0$. So by Theorem 1.1 we have

$$\mathfrak{B}_k(\sigma_1, a_{12}a_{21}+2)(E_1G_1E_2G_2\dots G_{u-1}E_uG_uE_{u+1}) = 0,$$

as required to prove that $\Omega(c) \leq \iota(c, \gamma_{12})/2$.

Example 7.6. For $n = 4$ consider the curve c represented by the conjugacy class $w = w(c) = T_1T_2T_3T_2T_3^{-1}T_2^{-1}T_4$. One easily sees that $\iota(\gamma_{12}, c) = 2$. Also

$$\mathcal{S}' = \{\emptyset, T_3, T_3^{-1}, T_4, T_3T_3^{-1}, T_3T_4, T_3^{-1}T_4, T_3T_3^{-1}T_4\}.$$

For example we have

$$\begin{aligned}\beta^{-1}(T_3T_3^{-1}T_4) = \{&T_3T_3^{-1}T_4, T_1T_3T_3^{-1}T_4, T_2T_3T_3^{-1}T_4, T_1T_2T_3T_3^{-1}T_4, T_3T_2T_3^{-1}T_4,\\ &T_1T_3T_2T_3^{-1}T_4, T_2T_3T_2T_3^{-1}T_4, T_1T_2T_3T_2T_3^{-1}T_4, T_3T_3^{-1}T_2^{-1}T_4,\\ &T_1T_3T_3^{-1}T_2^{-1}T_4, T_2T_3T_3^{-1}T_2^{-1}T_4, T_1T_2T_3T_3^{-1}T_2^{-1}T_4, T_3T_2T_3^{-1}T_2^{-1}T_4,\\ &T_1T_3T_2T_3^{-1}T_2^{-1}T_4, T_2T_3T_2T_3^{-1}T_2^{-1}T_4, T_1T_2T_3T_2T_3^{-1}T_2^{-1}T_4\}.\end{aligned}$$

This gives rise to the product

$$\pi = (a_{32}a_{23})(-a_{34} + a_{32}a_{24})(a_{43} + a_{42}a_{23} + a_{41}a_{13} + a_{41}a_{12}a_{24}).$$

which occurs as a summand of $trace(w) - 4$ of the kind indicated in Lemma 7.2. Now

$$\begin{aligned}
&\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(a_{32}a_{23}) = 0,\\
&\mathfrak{B}_1(\sigma_1, a_{12}a_{21} + 2)(-a_{34} + a_{32}a_{24}) = 0, \quad \text{and}\\
&\mathfrak{B}_0(\sigma_1, a_{12}a_{21} + 2)(a_{43} + a_{42}a_{23} + a_{41}a_{13} + a_{41}a_{12}a_{23}) = 0.
\end{aligned}$$

This shows that $\mathfrak{B}_2(\sigma_1, a_{12}a_{21} + 2)(\pi) = 0$. At the other extreme one has that for the trivial subword $\emptyset \in \mathcal{S}'$ we see that $\beta^{-1}(\emptyset)$ contributes $a_{12}a_{21}$. One similarly calculates the contributions made by each of the other members of $\mathcal{S}'$.

Lemma 7.7. *For any simple closed curve c with $\eta(w) = A_1B_1 \dots B_uA_{u+1}$ where $w = w(c)$ as in the above we have*

$$\phi(c) = trace(w) - n = \sum_s \psi_{\hat{1}\hat{2}}(s)$$

where the sum is over all subwords $s \in \mathcal{S}'$. Moreover each $\psi_{\hat{1}\hat{2}}(s)$ has the form $E_1G_1 \dots E_uG_uE_{u+1}$ given in Lemma 7.2 where each G_i is one of

$$\pm\, a_{r1}a_{1r},\ \ \pm a_{r2}a_{2r},\ \ \pm a_{rs}a_{sr} \pm a_{r1}a_{1s},\ \ \pm a_{r2}a_{2s} \pm a_{r2}a_{2s},$$
$$\pm(a_{uv} + a_{u2}a_{2v} + a_{u1}a_{1v} + a_{u1}a_{12}a_{2v}),\ \ \pm(a_{uv} - a_{u2}a_{2v} - a_{u1}a_{1v} + a_{u2}a_{21}a_{1v}),$$

where $u, v, r \neq s \geq 3$.

Proof. The exact nature of the G_i is the only thing that hasn't been noticed and this follows from the fact that B_i has one of the forms

$$T_r^{\pm1}T_1^{\pm1}T_s^{\pm1},\quad T_r^{\pm1}T_2^{\pm1}T_s^{\pm1},\quad T_u^{\pm1}T_1T_2T_v^{\pm1},\quad T_u^{\pm1}T_2^{-1}T_1^{-1}T_v^{\pm1}$$

where $r, s, u, v \geq 3$. A calculation of each such G_i shows that those given in Lemma 7.7 are the only possibilities. □

§8 Proof of Theorem 1.3

Let $x = a_{r1}a_{1s}$ or $x = a_{r2}a_{2s}$ for some $3 \leq r, s \leq n$. Then using the action of σ_1 given in §5 we see that for any $k \in \mathbb{Z}, k \geq 0$, we can write

$$\sigma_1^k(x) = c_{k11}(a_{r1}a_{1s}) + c_{k12}(a_{r1}a_{12}a_{2s}) + c_{k21}(a_{r2}a_{21}a_{1s}) + c_{k22}(a_{r2}a_{2s}), \quad (8.1)$$

where the $c_{kij} = c_{kij}(x)$ are polynomials in $a_{12}a_{21} = p_1 - 2$.

Lemma 8.1. *The polynomials c_{kij} satisfy the following recursion:*

$$c_{kij} + p_1c_{k-1\,ij} + c_{k-2\,ij} = d_{ij} \quad (8.2)$$

for all $k \geq 2$ *where* $d_{ij} = d_{ij}(x)$ *are polynomials in* p_1 *also. In particular for* $x = a_{r1}a_{1s}, a_{r2}a_{2s}$ *we have*

$$d_{11}(x) = 2, d_{11}(x) = 1, d_{21}(x) = -1, d_{22}(x) = 2.$$

We also have

$$c_{k-1\,11} = c_{k\,22}, \quad c_{k12} = -c_{k21}, \quad c_{k11} + 2a_{12}a_{21}c_{k12} = a_{12}a_{21}c_{k-1\,11} + c_{k-211}. \quad (8.3)$$

Proof. This will be by induction on $k \geq 2$. We will only deal with the case $x = a_{r1}a_{1s}$, the other case being similar. A calculation shows that we have

$$c_{011} = 1,\ c_{012} = 0, c_{021} = 0, c_{022} = 0, c_{111} = -a_{12}a_{21}, c_{112} = 1, c_{121} = -1, c_{122} = 1,$$
$$c_{211} = (a_{12}a_{21} + 1)^2, c_{212} = -a_{12}a_{21} - 1, c_{221} = a_{12}a_{21} + 1, c_{222} = -a_{12}a_{21}.$$

This allows one to check the first case ($k = 2$).

Now assume that for some $k \geq 2$ we have (8.1). Then, since $\sigma_1(c_{kij}) = c_{kij}$ for all k, i, j, we have (using the action of σ_1 given in §5)

$$\sigma_1^{k+1}(x) = c_{k11}(a_{r2} + a_{r1}a_{12})(a_{2s} - a_{21}a_{1s}) + c_{k12}(a_{r2} + a_{r1}a_{12})a_{21}a_{1s}$$
$$+ c_{k21}a_{r1}a_{12}(a_{2s} - a_{21}a_{1s}) + c_{k22}a_{r1}a_{1s}.$$

From this we obtain:

$$c_{k+1\,11} = -c_{k11}a_{12}a_{21} + c_{k12}a_{12}a_{21} - c_{k21}a_{12}a_{21} + c_{k22};$$
$$c_{k+1\,12} = c_{k11} + c_{k21}; \quad c_{k+1\,21} = -c_{k11} + c_{k12}; \quad c_{k+1\,22} = c_{k11}.$$

Using these latter equations we can check that the equations (8.3) for $k+1$ follow from (8.3) for k. Then one uses (8.3) to likewise prove (8.2) for $k+1$. □

Using the recurrence given in Lemma 8.1 we see that standard results for solving non-homogeneous recurrence equations [B] allow one to conclude that

$$c_{kij} = e_{ij+}\left(\frac{-p_1 + \sqrt{p_1^2 - 4}}{2}\right)^k + e_{ij-}\left(\frac{-p_1 - \sqrt{p_1^2 - 4}}{2}\right)^k,$$

where

$$e_{ij-} = \frac{1}{\sqrt{p_1^2 - 4}}\left(\left(c_{0ij} - \frac{d_{ij}}{2 + p_1}\right)\left(\frac{-p_1 + \sqrt{p_1^2 - 4}}{2}\right) - c_{1ij} + \frac{d_{ij}}{2 + p_1}\right),$$

and $e_{ij+} = c_{0ij} - \frac{d_{ij}}{2+p_1} - e_{ij-}$. One then finds that

$$e_{11-} = \frac{p_1 + \sqrt{p_1^2 - 4}}{2(p_1 + 2)}, \quad e_{11+} = \frac{p_1 - \sqrt{p_1^2 - 4}}{2(p_1 + 2)},$$

and so

$$c_{k11} = \frac{-1}{p_1 + 2}\left(\left(\frac{-p_1 + \sqrt{p_1^2 - 4}}{2}\right)^{k+1} + \left(\frac{-p_1 - \sqrt{p_1^2 - 4}}{2}\right)^{k+1} - 2\right). \quad (8.4)$$

Lemma 8.2. *For an integer $k \geq 0$ the degree of*

$$\left(\frac{-p_1 + \sqrt{p_1^2 - 4}}{2}\right)^k + \left(\frac{-p_1 - \sqrt{p_1^2 - 4}}{2}\right)^k$$

is k.

Proof. Expanding the kth powers in this sum using the binomial theorem we see that all terms involving the square root cancel and the term of highest degree is $\pm p_1^k$. $\square$

We use the above ideas to prove:

Proposition 8.3. *Let $n, m \geq 0$, $r_i, s_i, t_i, u_i \geq 3$ and*

$$w = \prod_{i=1}^{n} a_{r_i 1} a_{1 s_i}, \quad w' = \prod_{i=1}^{m} a_{t_i 2} a_{2 u_i}$$

Then $\Omega(w) = n$, $\Omega(w') = m$ and $\Omega(ww') = n + m$.

Proof. We will prove the third of these results, the proofs of the first and second being similar. We will prove this result by induction on $n+m \geq 0$, the cases $n+m \leq 1$ following from equations (5.4). By Theorem 1.1 we see that $\mathfrak{B}_{n+m}(ww') = 0$ so that $\Omega(ww') \leq n + m$. We will show that $\mathfrak{B}_{n+m-1}(ww') \neq 0$.

Now

$$\begin{aligned}
\mathfrak{B}_{n+m-1}(ww') &= \sum_{i=0}^{2(n+m-1)+1} q_{n+m-1\,i} \sigma_1^i(ww') \\
&= \sum_{i=0}^{2(n+m)-1} q_{n+m-1\,i} \sigma_1^i \left(\prod_{j=1}^{n} a_{r_j 1} a_{1 s_j}\right) \times \sigma_1^i \left(\prod_{j=1}^{m} a_{t_j 2} a_{2 u_j}\right).
\end{aligned}$$

But by (8.1) and (8.3) we have

$$\sigma_1^i(a_{r_j 1} a_{1 s_j}) = c_{i11} a_{r_j 1} a_{1 s_j} + \ldots \quad \text{and} \quad \sigma_1^i(a_{t_j 2} a_{2 u_j}) = c_{i-1\,11} a_{t_j 1} a_{1 u_j} + \ldots.$$

Thus the coefficient of $\prod_{j=1}^{n} a_{r_j 1} a_{1 s_j} \times \prod_{j=1}^{m} a_{t_j 2} a_{2 u_j}$ in $q_{n+m-1\,i} \sigma_1^i(ww')$ is

$$q_{n+m-1\,i} \prod_{j=1}^{n} c_{i11} \prod_{j=1}^{m} c_{i-1\,11} = q_{n+m-1\,i} c_{i11}^n c_{i-1\,11}^m.$$

Now using Lemma 2.1, Lemma 8.2 and equation (8.4) (where we can ignore the -2 and the initial factor of $\frac{-1}{p_1+2}$) we see that this term has degree

$$d(i) = (2(n + m - 1) - i + 1)i/2 + n(i + 1) + mi.$$

Now as a function of i (for fixed n, m) $d(i)$ is a quadratic function with a maximum value at $i = 2(n + m) - 1/2$ and so on the interval $[0, 2(n + m) - 1]$ the function $d(i)$ is increasing. Thus for integer values of i in this interval the maximum value is attained at the unique value $i = 2(n+m)-1$. Thus the sum for $\mathfrak{B}_{n+m-1}(ww')$ cannot be zero. This proves that $\Omega(ww') = n+m$ as required. $\square$

We now conclude the proof of Theorem 1.3. Let c be a simple closed curve on D_n and let $w = w(c)$. Let $\eta(w) = A_1B_1\dots A_uB_uA_{u+1}$. Recall the decomposition of $trace(w) - n$ given in Lemma 7.7 relative to the set $\mathcal{S}'$. Then the set $\mathcal{S}'$ has a maximal element i.e. there is an element S of $\mathcal{S}'$ such that every other element of $\mathcal{S}'$ is a subword of S. Thus every monomial in $\psi_{\hat{1}\hat{2}}(S)$ has more indices in its a_{rs} factors with $r > 2$ or $s > 2$ than does any other $\psi_{\hat{1}\hat{2}}(s')$ for $s' \in \mathcal{S}', s' \neq S$. Suppose that k of the B_i are $T_1^{\pm 1}$ or $T_2^{\pm 1}$. Theorem 1.3 will follow if we can show that $\mathfrak{B}_{k-1}(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(S)) \neq 0$.

Now $\psi_{\hat{1}\hat{2}}(S) = E_1G_1\dots E_uG_uE_{u+1}$ where the E_i are monomials in a_{rs} with $r, s \geq 3$ and the G_i are in the list given in Lemma 7.7. Now $\mathfrak{B}_0(E_i) = 0, \mathfrak{B}_0(a_{rs} + a_{r2}a_{2s} + a_{r1}a_{1s} + a_{r1}a_{12}a_{2s}) = 0$ and $\mathfrak{B}_0(a_{rs} - a_{r2}a_{2s} - a_{r1}a_{1s} + a_{r2}a_{21}a_{1s}) = 0$ and so we may ignore all terms that come from E_i and from terms of the latter two forms. What is left is a product

$$u = \prod_{i=1}^{n} a_{r_i1}a_{1s_i} \times \prod_{i=1}^{m} a_{t_i2}a_{2u_i}$$

for some $n, m \geq 0$ with $k = n+m$. The fact that $\mathfrak{B}_{k-1}(\sigma_1, a_{12}a_{21}+2)(u) \neq 0$, which implies that $\mathfrak{B}_{k-1}(\sigma_1, a_{12}a_{21}+2)(\psi_{\hat{1}\hat{2}}(S)) \neq 0$, now follows from Proposition 8.3. This proves Theorem 1.3. $\square$.

Remark 8.4. We here remark that our method gives a way of finding intersection numbers of any two simple closed curves c, c' on D_n. If one of the curves (say c) surrounds 2 punctures, then we can find a diffeomorphism α so that $\alpha(c) = \gamma_{12}$. Thus $\iota(c, c') = \iota(\gamma_{12}, \alpha(c'))$. One then finds the intersection number of γ_{12} and $\alpha(c')$ using the operators $B_n(\sigma_1, a_{12}a_{21}+2)$.

On the other hand, if c does not surround two punctures, then we think of D_n as a subset of D_{n+2} and consider the curve d such that $w(d) = w(c)x_{n+1}w(c)^{-1}x_{n+2}$. Then d surrounds two punctures and we can calculate the intersection $\iota(d, c') = 2\iota(c, c')$ using the operators $B_n(\sigma_1, a_{12}a_{21}+2)$. See Figure 4 for the relationship between c and d, where we have drawn the curve c and the spine $\Sigma(d)$ in a particular example.

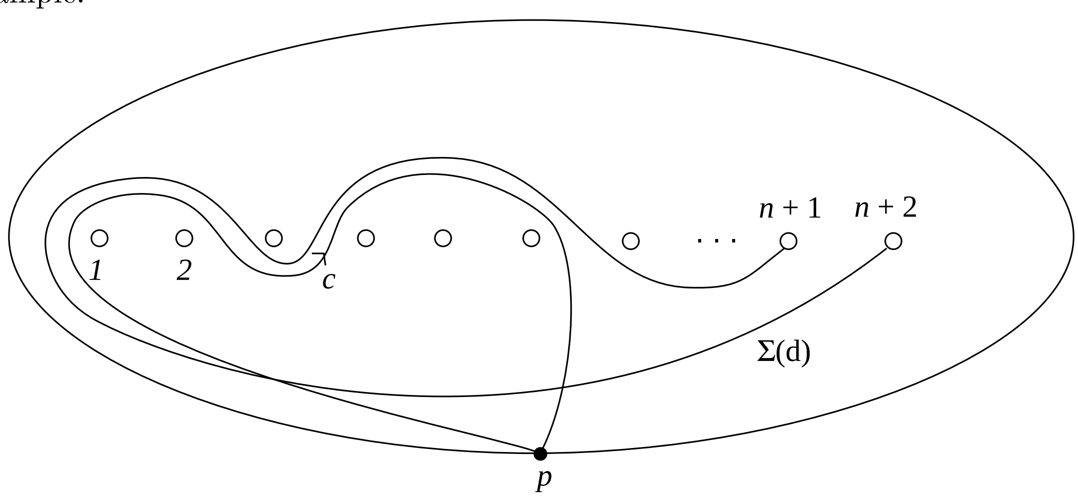

Figure 4

§9 A matrix interpretation

For $n \geq 1$ let R_n be the infinite matrix whose ij entry is r_{nij} for $i, j \geq 0$. Then by Lemma 2.1 R_n has the following block form

$$\begin{pmatrix} I_{2n+1} & 0 \\ U_n & 0 \end{pmatrix} \tag{9.1}$$

where I_{2n+1} is the identity matrix of rank $2n+1$ and each 0 is a matrix of zeros.

Proposition 9.1. *For $n \geq 1$ we have*
(i) $R_n^2 = R_n$;
(ii) $R_n R_m = R_n$ if $n \leq m$;
(iii) $R_n R_m = R_m R_n$ for $n, m \geq 1$.

Proof. (i) and (ii) are obvious from the block form (9.1) for R_n and R_m. (iii) will follow from the following result:

Lemma 9.2. *For all $m \geq n \geq 1$ and for all $j, k \geq 0$ we have*

$$\sum_{i=0}^{2m} r_{mji} r_{nik} = r_{njk}.$$

Proof. The proof will be by induction on $j \geq 0$. If $j = 0$, then we note from Lemma 2.1 that $r_{mji} = \delta_{ji}$ and so $\sum_{i=0}^{2m} r_{m0i} r_{nik} = r_{n0k}$ as required. Now assume that $\sum_{i=0}^{2m} r_{mji} r_{nik} = r_{njk}$. Then since $r_{mj\,2m+1} = 0$ we have (using Lemma 2.1)

$$\begin{aligned}
\sum_{i=0}^{2m} r_{m\,j+1\,i} r_{nik} &= \sum_{i=0}^{2m+1} r_{m\,j+1\,i} r_{nik} \\
&= \sum_{i=0}^{2m+1} (-q_{mi} r_{m\,j\,2m} + r_{mj\,i-1}) r_{nik} \\
&= -r_{mj\,i-1} \sum_{i=0}^{2m+1} -q_{mi} r_{nik} + \sum_{i=0}^{2m+1} r_{mj\,i-1} r_{nik}.
\end{aligned}$$

Note that by Proposition 2.7 the first sum is equal to 0. Thus the above is equal to

$$\begin{aligned}
\sum_{i=0}^{2m+1} r_{mj\,i-1} r_{nik} &= \sum_{i=0}^{2m+1} r_{mj\,i-1}(-q_{nk} r_{n\,i-1\,2n} + r_{n\,i-1\,k-1}) \\
&= -q_{nk} \sum_{i=0}^{2m+1} r_{mj\,i-1} r_{n\,i-1\,2n} + \sum_{i=0}^{2m+1} r_{mj\,i-1} r_{n\,i-1\,k-1} \\
&= -q_{nk} \sum_{i=0}^{2m} r_{mj\,i} r_{n\,i\,2n} + \sum_{i=0}^{2m+1} r_{mj\,i} r_{n\,i\,k-1} \\
&= -q_{nk} r_{n\,j\,2n} + r_{n\,j\,k-1} = r_{n\,j+1\,k},
\end{aligned}$$

as required. In this last calculation we used Lemma 2.1 and the inductive hypothesis. □

This now proves Proposition 9.1 □

Let Q_n be the infinite diagonal matrix $diag(q_{n0}, q_{n1}, \ldots, q_{n\,2n+1}, 0, 0, \ldots)$ and let (1) denote the infinite all 1 vector. Let T denote transpose.

Theorem 9.3. *a) The set $\{R_n\}_{n\geq 1}$ is an infinite family of independent commuting idempotents.*
b) If $P_1 = R_1$ and $P_n = R_n - R_{n-1}$ for $n > 1$, then $\{P_n\}_{n\geq 1}$ is an infinite family of independent orthogonal idempotents.
c) For $n, m \geq 1$ we have $R_m^T Q_{n+m} R_n = 0$.
d) For $1 \leq m \leq n$ we have $R_m^T Q_n(1) = 0$.

Proof. a) Follows from Proposition 9.1. b) Using Proposition 9.1 one easily checks that $P_n^2 = P_n$ and $P_n P_m = 0$ if $n \neq m$. The commutativity of P_n and P_m follows from Proposition 9.1.

Now c) is a direct consequence of the fact that $\sum_{i=0}^{2(n+m)+1} q_{n+m\,i} r_{n,i,j} r_{m,i,k} = 0$ for all $n, m \geq 1$ and $j, k \geq 0$ which was what we proved on the way to proving Theorem 1.1 (see Proposition 2.2 and §4). Lastly, d) follows from Proposition 2.7. $\square$

§10 An application to algebraic intersection numbers of curves on surfaces

Let S_g be a closed orientable surface of genus $g \geq 1$ and let M_g denote the mapping class group of S_g [Bi]. Let $a_1, \ldots, a_g, b_1, \ldots, b_g$ be a symplectic basis [MKS] for the first homology group $H_1 = H_1(S_g, \mathbb{Z}) \cong \mathbb{Z}^{2g}$, which we will write multiplicatively. Let $<,>$ denote the symplectic form or 'algebraic intersection number function', this being well-defined on homology classes. Thus $a_1, \ldots, a_g, b_1, \ldots, b_g$ satisfy $< a_i, b_i >= 1$ for $i = 1, \ldots, g$ all other products being zero. Let RH_1 denote the group algebra of H_1 over the commutative ring with identity R.

Now an element of H_1 can be represented by a simple closed curve if and only if it is primitive i.e. if and only if its coordinates relative to some (any) basis are relatively prime. For any element $c \in H_1$ we let

$$r(c) = -c - c^{-1} \in RH_1.$$

We also define the element $T_c \in Aut(H_1) = Sp_{2g}(\mathbb{Z})$ by

$$T_c(x) = xc^{<c,x>}$$

for all $x \in H_1$. Then in the situation where c is primitive and represents the simple closed curve γ we note that T_c is the symplectic transvection [A] which is the image of the Dehn twist $\Gamma \in M_g$ about γ under the canonical map $\pi_g : M_g \to Sp_{2g}(\mathbb{Z})$. Here π_g just gives the action of M_g on H_1 [MKS]. Then T_c extends to an automorphism of the group ring RH_1.

Theorem 10.1. *Let $c \in H_1$ be primitive and let $d \in H_1$. Let $\mathfrak{B}_n(T_c, r(c))$, $n > 0$, be the operators on the group ring RH_1 defined in Theorem 1.1. Then $| < c, d > |$ is equal to the minimal number $m \geq 0$ such that $\mathfrak{B}_m(T_c, r(c))(d) = 0$.*

Proof. Up to an action of $Sp_{2g}(\mathbb{Z})$ we can assume that $c = a_1$ (since M_g acts transitively on non-bounding simple closed curves in S_g). Then we can write $d = a_1^{e_1} b_1^{f_1} \ldots a_g^{e_g} b_g^{f_g}$ where $< c, d >= f_1$. Now note that $T_{a_1}(a_i) = a_i$ for $i = 1, \ldots, g$ and that $T_{a_1}(b_j) = b_j$ for $j = 2, \ldots, g$. It follows that we may as well take $d = b_1^k$ where $k =< c, d >$. Now if the polynomials $p_n = p_n(r(c))$ are as defined in Theorem 1.1, then it is easy to check that

$$p_n(r(c)) = -c^n - c^{-n}$$

for all $n \geq 0$. We also have $T_{a_1^m}(d) = T_{a_1^m}(b_1^k) = (a_1^m b_1)^k$ for all $m, k \in \mathbb{Z}$. Now $\mathfrak{B}_0(T_{a_1}, r(a_1))(b_1) = a_1 b_1 - b_1 \neq 0$ and

$$\begin{aligned}
\mathfrak{B}_1(T_{a_1}, r(a_1))(b_1) &= (T_{a_1}^2 - (a_1 + a_1^{-1})T_{a_1} + 1)(T_{a_1} - 1)(b_1) \\
&= (T_{a_1}^2 - (a_1 + a_1^{-1})T_{a_1} + 1)(a_1 b_1 - b_1) \\
&= a_1^3 b_1 - a_1^2 b_1 - (a_1 + a_1^{-1})(a_1^2 b_1 - a_1 b_1) + a_1 b_1 - b_1 \\
&= 0, \qquad (10.1)
\end{aligned}$$

and similarly that $\mathfrak{B}_1(T_{a_1}, r(a_1))(b_1^{-1}) = 0$ as required. It follows from Theorem 1.1 that $\mathfrak{B}_{|k|}(T_{a_1}, r(a_1))(b_1^k) = 0$ for all $k \in \mathbb{Z}$. Theorem 10.1 will follow if we can show that $\mathfrak{B}_k(T_{a_1}, r(a_1))(b_1^{k+1}) \neq 0$ for all $k \geq 0$ (the cases where $k < 0$ are similar).

Lemma 10.2. *Let $1 \leq n < j$. Then*

$$\mathfrak{B}_n(T_{a_1}, r(a_1))(b_1^j) = (\sum_i \mu_i(n,j) a_1^i) b_1^j, \qquad (10.2)$$

where $\mu_i(n,j) \in R$ and $\mu_{j(2n+1)}(n,j) = 1$ and $\mu_i(n,j) = 0$ for $i > j(2n+1)$.

Proof. Since the action of $T_{a_1}^k$ only multiplies each element of H_1 by some power of a_1 and since $\mathfrak{B}_i(T_{a_1}, r(a_1))$ is a sum of such operators with coefficients in $R[a_1]$ one sees that we do have (10.2). We prove the rest by induction on n for all values of $j > n$. The case $n = 1$ follows (for all $j > n$) from a calculation similar to (10.1). Now assume that we for some n we have $\mathfrak{B}_n(T_{a_1}, r(a_1))(b_1^j) = (\sum_i \mu_i(n,j) a_1^i) b_1^j$ where $\mu_{j(2n+1)}(n,j) = 1$ and $\mu_i(n,j) = 0$ for $i > j(2n+1)$. Note that according to the theorem, in order to consider the $n+1$ case, we must assume $j > n+1$ and so we have

$$\begin{aligned}
\mathfrak{B}_{n+1}(T_{a_1}, r(a_1))(b_1^j) &= \mathfrak{A}_{n+1}(T_{a_1}, r(a_1))\mathfrak{B}_n(T_{a_1}, r(a_1))(b_1^j) \\
&= (T_{a_1}^2 - (a_1^{n+1} + a_1^{-(n+1)})T_{a_1} + 1)(a_1^{j(2n+1)} b_1^j + \dots)
\end{aligned}$$

where $\dots$ indicates terms of lower degree. Thus the terms of highest degree in the above are

$$\begin{aligned}
T_{a_1}^2(a_1^{j(2n+1)} b_1^j) &= a_1^{j(2n+1)}(a_1^2 b_1)^j \qquad \text{and} \\
a_1^{n+1} T_{a_1}(a_1^{j(2n+1)} b_1^j) &= a_1^{j(2n+1)} a_1^{n+1}(a_1 b_1)^j.
\end{aligned}$$

But since $j > n+1$ one checks that the first of these has the largest degree. Lemma 10.2 and Theorem 10.1 now both follow. □

Remark 10.3. We remark that Theorem 10.1 can easily be extended to the situation of any orientable surface. In fact it can be generalised to any compact triangulated orientable homology $(4n+2)$-manifold X $(n \geq 0)$, where we consider the symplectic structure on the cohomology group $H^{2n+1}(X; \mathbb{Q})$ given by the cup product.

References

[A] Artin E., *Geometric Algebra*, New York: Interscience, 1957.

[AG] Akhiezer, N. I. Glazman, I. M., *Theory of linear operators in Hilbert space.*, Dover, 1993.

[Bi] Birman J., *Braids, Links and Mapping class Groups*, Ann. Math. Studies **82** (1974).

[BS] Birman, J. S.; Series, C., *An algorithm for simple curves on surfaces.*, J. London Math. Soc. (2) **29** (1984 no. 2,), 331–342.

[B] Brualdi R. A., *Introductory Combinatoris*, Prentice Hall, 1992.

[C1] Chillingworth, D. R. J., *Simple closed curves on surfaces.*, Bull. London Math. Soc. **1** (1969), 310–314..

[C2] ———, *An algorithm for families of disjoint simple closed curves on surfaces.*, Bull. London Math. Soc. **3** (1971), 23–26.

[CL] Cohen, M. Lustig, M., *Paths of geodesics and geometric intersection numbers. I.*, Combinatorial group theory and topology, Princeton Univ. Press., 1984, pp. 479–500 Ann. of Math. Stud. 111,.

[Hu1] Humphries S. P., *An Approach to Automorphisms of Free Groups and Braids via Transvections*, Math. Zeit. **209** (1992), 131-152.

[Hu2] ———, *Some linear representations of Braid Groups*, preprint (1996).

[LMT] Lidl, R., Mullen, G. L., Turnwald, G., *Dickson polynomials.*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65. Longman, 1993.

[Ma] Magnus W., *Rings of Fricke Characters and Automorphism groups of Free groups*, Math. Zeit. **170** (1980), 91-103.

[Mi1] Milnor, J., *Isotopy of links. Algebraic geometry and topology.*, A symposium in honor of S. Lefschetz,, Princeton University Press,, 1957, pp. 280–306..

[Mi2] ———, *Link groups.*, Ann. of Math. **59,** (1954), 177–195.

[MKS] Magnus W., Karrass A., Solitar D., *Combinatorial Group Theory*, Dover, 1976.

[R] Reinhart, B. L., *Algorithms for Jordan curves on compact surfaces.*, Ann. of Math. (2) **75** (1962), 209–222.

[Ri] Rivlin, T. J., *The Chebyshev Polynomials*, Wiley, 1974.

[T] Tan, S. P., *Self-intersections of curves on surfaces.*, Geom. Dedicata **62** (1996 no. 2,), 209–225.

[Z1] Zieschang, H., *Algorithmen für einfache Kurven auf Fächen.*, Math. Scand. **17** (1965), 17–40.

[Z2] ———, *Algorithmen für einfache Kurven auf Flächen. II.*, Math. Scand. **25** (1969), 49–58.