BULL. AUSTRAL. MATH. SOC. 20F36, 20M05, 20M30
VOL. 70 (2004) [401–422]

ON THE INJECTIVITY OF THE VASSILIEV HOMOMORPHISM OF SINGULAR ARTIN MONOIDS

NOELLE ANTONY

I prove general combinatorial properties which apply to singular Artin monoids and examine their relationship with the Vassiliev homomorphism η. I show that η preserves the Intermediate Property, discovered by Corran, which holds in positive singular Artin monoids of finite type. From this it follows that η is injective for a class of monoids which include singular Artin monoids of type $I_2(p)$, generalising a result of East.

1. INTRODUCTION AND PRELIMINARIES

We begin with a finite indexing set I, and we let Γ^M be a complete labelled graph with n vertices in one-to-one correspondence with I and with edge labels from the set $\{3, 4, \dots, \infty\}$. For $i \neq j$ let m_{ij} denote the label of the edge between the vertices i and j, or set $m_{ij} = 2$ if there is no such edge. Put $m_{ii} = 1$ for every $i \in I$. Such a graph is known as a *Coxeter graph of type M* where $M = (m_{ij})_{i,j \in I}$ is the associated *Coxeter matrix*. It is conventional to suppress the edge label whenever $m_{ij} = 3$.

Now let $S = \{\sigma_i \mid i \in I\}$, and let $\langle xy \rangle^q$ denote the alternating product

$$\underbrace{xyx\dots}_{q\text{ terms}}$$

of length q. The *Artin group of type M*, denoted G_M, is the group generated by S subject to the relations

$$\langle \sigma_i \sigma_j \rangle^{m_{ij}} = \langle \sigma_j \sigma_i \rangle^{m_{ij}} \quad \text{for } i, j \in I \text{ and } m_{ij} \neq \infty$$

(these are denoted by $\mathfrak{R}_1$ and called the *braid relations*). The *Coxeter group of type M* is the group generated by S subject to the preceding relations and the relations $\sigma_i^2 = 1$ for every i in I. In this way we see that Coxeter groups arise as quotient groups of Artin groups. If the Coxeter group of type M is finite then M is said to be of *finite type*. For a classification of finite Coxeter groups see, for example, [14].

The first, and arguably the most well-known, (non-Abelian) example of an Artin group is the braid group established in [1] by Artin; thus the terminology *Artin group* is suggested by

Received 17th May, 2004
Supported by an Australian Postgraduate Award. The author is indebted to supervisor David Easdown for his encouragement and for many useful discussions and would also like to recognise the referee's helpful suggestions.

Brieskorn and Saito in [4]. Observe that $\mathcal{B}_{n+1}$, the braid group on $n+1$ strings, arises from the special case when $I = \{1, \ldots, n\}$, $m_{ij} = 3$ when $|i-j| = 1$ and $m_{ij} = 2$ when $|i-j| \geqslant 2$. Its associated Coxeter graph is referred to as type A_n, whilst the corresponding Coxeter group is the symmetric group on $n+1$ letters. When the indexing set $I = \{1, 2\}$ and the edge label $m_{12} = p$ for some $p \geqslant 3$, the Coxeter graph is said to be of type $M = I_2(p)$.

In their study of knot invariants, Baez [2] and Birman [3] extended the braid group $\mathcal{B}_{n+1}$ by introducing the *singular braid monoid on* $n+1$ *strings*, $\mathcal{SB}_{n+1}$. Analogously Artin groups are extended in [6] and [12] as follows: Put $T = \{\tau_i \mid i \in I\}$ and let $S^{-1} = \{\sigma_i^{-1} \mid i \in I\}$, the set of formal inverses of S. The *singular Artin monoid of type M*, denoted $\mathcal{SG}_M$, is the monoid generated by $S \cup S^{-1} \cup T$ and has as its defining relations $\mathfrak{R}_1$, the free group relations $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1$ and the relations $\mathfrak{R}_2$ listed below:

$$\begin{aligned}
\tau_i\tau_j &= \tau_j\tau_i \quad \text{if } m_{ij} = 2,\\
\tau_i\langle\sigma_j\sigma_i\rangle^{m_{ij}-1} &= \begin{cases} \langle\sigma_j\sigma_i\rangle^{m_{ij}-1}\tau_j & \text{if } m_{ij} < \infty \text{ and is odd, or}\\ \langle\sigma_j\sigma_i\rangle^{m_{ij}-1}\tau_i & \text{if } m_{ij} < \infty \text{ and is even,}\end{cases}\\
\tau_i\sigma_i &= \sigma_i\tau_i \quad \text{for all } i \text{ in } I.
\end{aligned}$$

REMARK. When the Coxeter graph is of type A_n, the special case mentioned above, the corresponding singular Artin monoid, $\mathcal{SG}_{A_n}$, coincides with the singular braid monoid on $n+1$ strings, $\mathcal{SB}_{n+1}$. It is worth noting here that, although singular Artin monoids are defined (in an abstract sense) by the above generators and relations, $\mathcal{SB}_{n+1}$ was originally introduced geometrically in [2] and [3] and was then shown (in [3, Lemma 3] and [13, a subcase of Theorem 2.1]) to admit the preceding presentation.

Let $\mathfrak{A}$ be a finite set called an *alphabet*. Elements of $\mathfrak{A}$ are referred to as *letters*, whilst $\mathfrak{A}^*$ denotes the free monoid generated by $\mathfrak{A}$, elements of which are said to be *words*. In arguments below we may regard a relation formally as an ordered pair of words. If X is a set of ordered pairs of words then $X^\Sigma = \{(U, V) \mid (U, V) \text{ or } (V, U) \in X\}$.

If A and B are words in the above generators, we write $A \approx B$ if A can be transformed into B by the use of the defining relations of $\mathcal{SG}_M$, and write $A = B$ if the two words are equal letter by letter. Whenever $W = x_1 \ldots x_t$ for some $x_1, \ldots, x_t \in S \cup S^{-1} \cup T$, $\mathrm{Rev}(W) = x_t \ldots x_1$.

The *positive Artin monoid of type M*, G_M^+, is the monoid generated by S subject to the braid relations $\mathfrak{R}_1$. We define the *positive singular Artin monoid*, denoted $\mathcal{SG}_M^+$, to be the monoid generated by $S \cup T$ and the set $\mathfrak{R}$ of relations comprised of both $\mathfrak{R}_1$ and $\mathfrak{R}_2$ listed above. Where it does not cause confusion we denote elements of G_M, G_M^+, $\mathcal{SG}_M$ and $\mathcal{SG}_M^+$ by words which represent them. If A and B are words in the generators from the sets S and T, we write $A \sim B$ if A can be transformed into B by the use of $\mathfrak{R}$. The following Theorems 1.1(1) and (2) are proved in [16] and [6] respectively:

THEOREM 1.1.

(1) *If A, B are words over S and $A \approx B$ then $A \sim B$.*

(2) *Let M be of finite type. If A, B are words over $S \cup T$ and $A \approx B$ then $A \sim B$.*

Thus G_M^+ always injects into G_M, whilst $\mathcal{S}G_M^+$ embeds into $\mathcal{S}G_M$ whenever M is of finite type.

We denote by $\ell(A)$ the length of any word A. It is easy to see, by inspection of the set $\mathfrak{R}$ of defining relations, that the following property holds in $\mathcal{S}G_M^+$:

Whenever U, V are over $S \cup T$ and $U \sim V$, $\ell(U) = \ell(V)$.

We call this property, in accordance with [**6**, p. 258], *homogeneity*. Thus the length of an element is defined to be the length of any word representing it. The *reduction property* is defined as in [**6**, p. 258]. By [**6**, Lemma 15], the cancellation law and the reduction property hold in $\mathcal{S}G_M^+$. By *reduction* we mean an application of the reduction property.

Let A and B be words in $(S \cup T)^*$. We say A *(left) divides* B or B is a *(left) multiple* of A if there exists a word X in $\mathcal{S}G_M^+$ such that $B \sim AX$, in which case we write $A \prec B$. We say A *right divides* B or B is a *right multiple* of A if there is a word X in $\mathcal{S}G_M^+$ such that $B \sim XA$, in which case we write $B \succ A$.

Let $\Omega = \{A_1, A_2, \dots, A_k\}$ be a set of words in $(S \cup T)^*$. If Ω has a common multiple then by [**6**, Corollary 13], Ω has a least common multiple (unique up to equivalence under $\sim$) which we denote by $\mathrm{lcm}(A_1, A_2, \dots, A_k)$ or $\mathrm{lcm}(\Omega)$. By homogeneity, $\mathrm{lcm}(\Omega)$ when it exists has minimal length. If Ω has no common multiple then we write $\mathrm{lcm}(A_1, A_2, \dots, A_k) = \infty$.

In Section 2 we discover properties pertaining to fundamental elements in addition to general results regarding divisibility in $\mathcal{S}G_M^+$. In Section 3 the Vassiliev homomorphism η is defined, we state Birman's conjecture and show that if Birman's conjecture is true for $\mathcal{S}G_M^+$, where M is of finite type, then it is true for $\mathcal{S}G_M$; this is followed by some observations regarding η. The results of Sections 4 and 5 hold for finite type M. In Section 4 we study the relationship between divisibility in $\mathcal{S}G_M^+$ and the support of η. In particular, we show that if U, $V \in \mathcal{S}G_M^+$, $C \in G_M^+$ and $\eta(U) = \eta(V)$ then C divides U if and only if C divides V. Finally, in Section 5 we prove that η preserves the Intermediate Property which holds in $\mathcal{S}G_M^+$; namely, if $\eta(\tau_i U) = \eta(\tau_j V)$ then $m_{ij} \leqslant 2$. From this it follows that η is injective for a class of monoids which include singular Artin monoids of type $I_2(p)$, generalising [**9**, Theorem 14].

2. The fundamental word Δ

The following refers to a construction developed in [**6**, Section 2]. For every generator α and word W in $(S \cup T)^*$, the word $K_\alpha(W)$ is defined and begins with α if and only if W is divisible by α, in which case we write $W_\alpha = (W/\alpha)$ for the word obtained by removing the letter α from $K_\alpha(W)$. Then the word (W/V) is defined recursively and exists precisely when $V \prec W$ and has the property that $W \sim V(W/V)$.

2.1. Properties of Δ. Suppose in this subsection that M is of finite type. Let $\Delta = \mathrm{lcm}(S)$. We call Δ, in accordance with [**11**, Section 2], *the fundamental word* of $\mathcal{S}G_M$ and write

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

$\zeta = \Delta^2$. In [**4**, Theorem 5.6] tells us that Δ exists precisely when M is of finite type, whilst by [**6**, Section 5], the following holds:

THEOREM 2.1. *Let $T_1 \subseteq T$, and let W be a word over $S \cup S^{-1} \cup T_1$. Then there exists an integer p and a word $\overline{W}$ over $S \cup T_1$ such that $W \approx \Delta^p \overline{W}$.*

In [**6**, Section 4], Corran showed that there exists a uniquely determined involutionary automorphism of $\mathcal{S}G_M$, which we denote by $\mathcal{R}$, with the following property:

1. $\mathcal{R}$ sends letters to letters, so that for any $i \in I$, $\alpha = \sigma$ or τ, $\mathcal{R}(\alpha_i) = \alpha_{\phi(i)}$ and $\sigma_i\Delta \sim \Delta\mathcal{R}(\sigma_i)$. Hence $\mathcal{R}$ arises from a permutation ϕ of I with $\phi^2 = \text{id}$ and $m_{\phi(i)\phi(j)} = m_{ij}$.

(See also [**4**, Lemma 5.2]). We write $\alpha_i' = \alpha_{i'}$ for $\mathcal{R}(\alpha_i)$. By [**6**, Lemma 18], we have the ensuing property of Δ:

LEMMA 2.1. *Let W be any word in $(S \cup T)^*$. Then $W\Delta \sim \Delta\mathcal{R}(W)$. In particular, W is left divisible by Δ if and only if W is right divisible by Δ.*

The previous result tells us that Δ acts almost like a central element of $\mathcal{S}G_M^+$, but not quite, as Lemma 2.2 below shows. The first part of the lemma is a restatement of [**4**, Lemmas 5.2(ii) and 5.1(ii)]; the second part of the result is a combination of [**6**, Lemma 18] and [**4**, Theorem 7.2]. All the undefined notation in Lemma 2.2(2) comes from the cited references.

LEMMA 2.2.

(1) *$\mathcal{R}(\Delta) \sim \Delta$ and $\mathrm{Rev}(\Delta) \sim \Delta$.*

(2) *The centre of the singular Artin monoid is generated by the fundamental element Δ if the associated involution $\mathcal{R}$ is trivial. The involution $\mathcal{R}$ is non-trivial only for types A_n (when $n \geqslant 2$), D_{2k+1}, E_6 and $I_2(2q+1)$, in which case Δ^2 represents the generator of the centre.*

Since Δ is the lowest common multiple of the set S, the word $K_a(\Delta)$ is defined, and so Δ_a exists for every $a \in S$. By recalling that $\zeta = \Delta^2$, we analogously obtain the existence of the word ζ_a for every $a \in S$.

LEMMA 2.3.

(1) *For any a in S, $\mathcal{R}(\Delta_a) \sim \Delta_{a'}$.*

(2) *For $\alpha = \sigma$ or τ and $i \in I$, $\alpha_i\Delta_{\sigma_i} \sim \Delta_{\sigma_i}\alpha_i'$. In particular, $a\Delta_a \sim \Delta \sim \Delta_a a'$ whenever $a \in S$.*

PROOF: (1) Let a be a generator in S. By Lemma 2.2(1) and since $\Delta \sim b\Delta_b$ for any b in S, it follows that

$$a'\mathcal{R}(\Delta_a) \sim \mathcal{R}(a\Delta_a) \sim \mathcal{R}(\Delta) \sim \Delta \sim a'\Delta_{a'}.$$

Hence $\mathcal{R}(\Delta_a) \sim \Delta_{a'}$ by cancellation, as required.

(2) Let σ_i be any generator in S, and let $\alpha_i = \sigma_i$ or τ_i. Then $\alpha_i\sigma_i \sim \sigma_i\alpha_i$, and by Lemma 2.1, $\alpha_i\Delta \sim \Delta\alpha_i'$, so

$$\sigma_i\alpha_i\Delta_{\sigma_i} \sim \alpha_i\sigma_i\Delta_{\sigma_i} \sim \alpha_i\Delta \sim \Delta\alpha_i' \sim \sigma_i\Delta_{\sigma_i}\alpha_i'.$$

The result now follows by cancellation. ∎

The reader is referred to [**5**, Lemma 2.3] for variations of the preceding Lemmas 2.2 and 2.3.

2.2. DIVISIBILITY THEORY. The results of this subsection hold for positive singular Artin monoids of any (not necessarily finite) type. The ensuing definitions are obtained from [**6**, Section 2]. Let C be a non-empty word and a, $b \in S \cup T$. We say C is a *simple a-chain* with *source a* and *target b* if there is a (non-empty) word P and (possibly empty) word Q such that $(aP, Cb\,Q)$ is a relation in $\mathfrak{R}^\Sigma$. We call C an *a-chain* if $C = C_1 \dots C_k$ for simple chains $C_1, \dots, C_k$ where the source of C_1 is a and the source of C_{i+1} is the target of C_i for $i = 1, \dots, k-1$. In this case, the *source* and *target* of C are defined to be the source of C_1 and the target of C_k respectively.

REMARK 1. In G_M^+, if C is a σ_a-chain to σ_b then $\mathrm{Rev}(C)$ is a σ_b-chain to σ_a. However this does not always hold in SG_M^+. For example, if $3 \leqslant m_{ab} < \infty$ then σ_b is a τ_a-chain to σ_a, but $\mathrm{Rev}(\sigma_b) = \sigma_b$ is a σ_a-chain to $\sigma_a \neq \tau_a$. Moreover, $\tau_a\sigma_b$ is a simple σ_b-chain to σ_a, but the target of the non-simple σ_a-chain $\mathrm{Rev}(\tau_a\sigma_b) = \sigma_b\tau_a$ is σ_a, not equal to the source of $\tau_a\sigma_b$.

Lemmas 2.4, 2.5 and 2.6 below are restatements of [**6**, Lemmas 3, 5 and 4(2)].

LEMMA 2.4. *If C is an a-chain to b and W is a common multiple of a and C then W is also a common multiple of a and Cb. In particular, a does not divide C.*

LEMMA 2.5. *Suppose $a \in S \cup T$, and let W be a word over $S \cup T$ such that a does not divide W but $\mathrm{lcm}(a, W)$ exists. Then either W is empty or there is an a-chain C such that $W \sim C$.*

LEMMA 2.6. *If C is an a-chain such that a divides Cb then b is the target of C.*

The following two results are also proved in [**7**, Lemma 6.5].

LEMMA 2.7. *If C is an a-chain to b and a is an element of S then b also lies in S.*

PROOF: Write $C = C_1 \dots C_k$ where each C_i is simple, and suppose d is the target of C_1. Then $(aP,\ C_1dQ) \in \mathfrak{R}^\Sigma$ for some generator d and words P, Q. If $d \in T$, inspection of the set $\mathfrak{R}$ of defining relations shows that $Q = 1$ (since $C_1 \neq 1$) and $a \in T$. Hence d must lie in S. If $k = 1$ then $b = d$, and we are done. Otherwise, $C_2 \dots C_k$ is a d-chain to b and $d \in S$, so by induction, b must be an element of S as stated. ∎

LEMMA 2.8. *If C is a σ_a-chain to σ_b then C is not right divisible by σ_b.*

PROOF: Write $C = C_1 \dots C_k$ where each C_i is simple. Since σ_a clearly lies in S, we deduce from Lemma 2.7 that the source of C_k is σ_c for some c in I. Hence there exist words P, Q in SG_M^+ such that $(C_k\sigma_bP, \sigma_cQ) \in \mathfrak{R}^\Sigma$. Inspection of $\mathfrak{R}$ immediately shows that C_k is not right divisible by its target σ_b. If $k = 1$ then $C = C_k \not\succ \sigma_b$, and we are done. So suppose that $k \geqslant 2$, and put $C' = C_1 \dots C_{k-1}$. By noting that the source of C_k, σ_c, is the target of C_{k-1}, we see that C' is a σ_a-chain to σ_c, and thus by induction, $C' \not\succ \sigma_c$. Thus

$$\sigma_c \not\prec \mathrm{Rev}(C'). \tag{2.1}$$

Now put $W = \mathrm{Rev}(C) = \mathrm{Rev}(C_k)\mathrm{Rev}(C')$. We show that W is not divisible by σ_b, so that $C \not\succ \sigma_b$ as required. Recall that C_k is a simple σ_c-chain to σ_b. If C_k is over S then $\mathrm{Rev}(C_k)$ is a σ_b-chain to σ_c; so if W were divisible by σ_b, W would be a common multiple of $\mathrm{Rev}(C_k)$ and σ_b, thus σ_c would divide $\mathrm{Rev}(C')$ (by Lemma 2.4 and cancellation), and this would obviously contradict (2.1). Suppose then that C_k is not over S. Then either $C_k = \tau_c$ or $C_k = \tau_d \langle \sigma_c \sigma_d \rangle^q$ for some non-negative integer q such that $q \leqslant m_{cd} - 2$.

If $C_k = \tau_c$ then $b = c$ since C_k is a σ_c chain to σ_b; so if $\sigma_b = \sigma_c$ were to divide $W = \tau_c \,\mathrm{Rev}(C')$, reduction would show that $\sigma_c \prec \mathrm{Rev}(C')$ which would contradict (2.1). So assume that

$$C_k = \tau_d \langle \sigma_c \sigma_d \rangle^q \quad \text{for some } q \text{ such that } 0 \leqslant q \leqslant m_{cd} - 2.$$

Thus C_k is a σ_c-chain to σ_b where $b = c$ if q is even and $b = d$ if q is odd. Hence

$$\begin{aligned} W = \mathrm{Rev}(C_k)\mathrm{Rev}(C') &\sim \mathrm{Rev}\big(\langle \sigma_c \sigma_d \rangle^q\big)\tau_d \mathrm{Rev}(C') \\ &= \begin{cases} \langle \sigma_d \sigma_c \rangle^q \tau_d \mathrm{Rev}(C') & \text{if } q \text{ is even,} \\ \langle \sigma_c \sigma_d \rangle^q \tau_d \mathrm{Rev}(C') & \text{if } q \text{ is odd.} \end{cases} \end{aligned}$$

Suppose that σ_b divides W. By recalling that $q \leqslant m_{cd} - 2$, reduction and cancellation yield a word R such that

$$\tau_d \mathrm{Rev}(C') \sim \langle \sigma_d \sigma_c \rangle^{m_{cd} - q} R = \sigma_d \sigma_c \, \langle \sigma_d \sigma_c \rangle^{m_{cd} - (q+2)} R.$$

Another application of reduction tells us that τ_d divides $\sigma_c \, \langle \sigma_d \sigma_c \rangle^{m_{cd} - (q+2)} R$, so that yet again by reduction,

$$\sigma_c \, \langle \sigma_d \sigma_c \rangle^{m_{cd} - (q+2)} R \sim \langle \sigma_c \sigma_d \rangle^{m_{cd} - 1} R'$$

for some word R'. Thus

$$\tau_d \mathrm{Rev}(C') \sim \sigma_d \, \sigma_c \langle \sigma_d \sigma_c \rangle^{m_{cd} - (q+2)} R \sim \sigma_d \, \langle \sigma_c \sigma_d \rangle^{m_{cd} - 1} R' \sim \langle \sigma_c \sigma_d \rangle^{m_{cd}} R'.$$

A final application of reduction now shows that $\sigma_c \prec \mathrm{Rev}(C')$ which contradicts (2.1). This implies that σ_b does not divide $W = \mathrm{Rev}(C)$, thus $C \not\succ \sigma_b$ as required. The result now follows by induction. ∎

REMARK 2. The condition in Lemma 2.8 above, for the source of C to be an element of S, is necessary. Let $m_{ab} = 3$ and put $U = \sigma_a^2 \sigma_b \sigma_a$. Then U is clearly right divisible by σ_a. Furthermore $U \sim (\sigma_a \sigma_b)(\sigma_a)(\sigma_b)$, the latter being a non-simple τ_b-chain with target σ_a.

2.3. THE STRUCTURE OF Δ. For the remainder of this section we resume our supposition that M is of finite type. The ensuing Proposition 2.1 provides an important property of the fundamental word. It was originally discovered for the positive braid monoid in [**11**, Theorem 8] and was generalised in [**4**, Lemma 5.3] to show that it holds for positive Artin monoids of finite type. As a preliminary result, we deduce the following:

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

LEMMA 2.9. *Let $a \in S$, and let W be a non-empty word in $(S \cup T)^*$. Then $a \not\prec W$ if and only if $W \sim C$ for some a-chain C.*

PROOF: It is evident that a divides Δ, so by Lemma 2.1, $W\Delta \sim \Delta\mathcal{R}(W)$ is a common multiple of a and W; this shows that $\operatorname{lcm}(a, W)$ exists. Thus if a does not divide W then Lemma 2.5 yields the existence of an a-chain C such that $W \sim C$. On the other hand, if $W \sim C$ where C is an a-chain then $a \not\prec C \sim W$ by Lemma 2.4. ∎

PROPOSITION 2.1. *Let X and Y be in $(S \cup T)^*$. If $\Delta \prec XY$ then for every $i \in I$ either $X \succ \sigma_i$ or $\sigma_i \prec Y$.*

PROOF: Suppose there exists an $i \in I$ such that σ_i does not right divide X nor does it divide Y. We show $\Delta \not\prec XY$ by induction on $\ell(Y) \geqslant 0$. The result certainly is true if $\ell(X) = 0$, whilst if $\ell(Y) = 0$ the claim holds by Lemma 2.1. So suppose that both X and Y are non-empty. Since $X \not\succ \sigma_i$, we infer from Lemma 2.1 that X cannot be right divisible and so divisible by Δ, the lowest common multiple of the set S. Hence $\sigma_j \not\prec X$ for some $j \in I$. By noting that X is non-empty, Lemma 2.9 may be applied and this yields a σ_j-chain C such that $X \sim C$. By Lemma 2.7, we deduce that the target of C is σ_k for some $k \in I$, so by Lemma 2.8, $C \not\succ \sigma_k$. Hence

$$(2.2) \qquad C \text{ is a } \sigma_j\text{-chain to } \sigma_k, \quad C \sim X \not\succ \sigma_i \text{ and } \sigma_k.$$

If σ_k does not divide Y then by another application of Lemma 2.9, we infer the existence of a σ_k-chain C' such that $Y \sim C'$, so that CC' is a σ_j-chain by (2.2); this implies, by Lemma 2.4, that σ_j, and hence Δ, cannot divide $CC' \sim XY$. So suppose that $\sigma_k \prec Y$. Then $i \neq k$ since $\sigma_i \not\prec Y$. Thus there exists a largest integer q and word Y' such that

$$(2.3) \qquad Y \sim \langle \sigma_k \sigma_i \rangle^q Y' \quad \text{and} \quad \sigma_d \not\prec Y'$$

where $d = k$ if q is even and $d = i$ if q is odd. Since $\langle \sigma_k \sigma_i \rangle^{m_{ik}} \sim \langle \sigma_i \sigma_k \rangle^{m_{ik}}$ and $\sigma_i \not\prec Y$, we have that $1 \leqslant q \leqslant m_{ik} - 1$. Put $X' = X\langle \sigma_k \sigma_i \rangle^q$. Then

$$XY \sim X\langle \sigma_k \sigma_i \rangle^q Y' = X'Y'$$

and $\ell(Y') < \ell(Y)$. If σ_d were to right divide $X' = X\langle \sigma_k \sigma_i \rangle^q$, reduction and reversal would yield a word X'' such that $X\langle \sigma_k \sigma_i \rangle^q \sim X''\langle \sigma_k \sigma_i \rangle^{m_{ik}}$; so by noting that $q < m_{ik}$, σ_i or σ_k would right divide X (by cancellation) which would contradict (2.2). Hence $X' \not\succ \sigma_d$, and by (2.3), $\sigma_d \not\prec Y'$. Since $\ell(Y') < \ell(Y)$, we deduce by an inductive hypothesis that $\Delta \not\prec X'Y' \sim XY$ as required. The result now follows by induction. ∎

COROLLARY 2.1. *Let a be in S and $S' = S \backslash \{a\}$. Then $\operatorname{lcm}(S') \prec \Delta_a$, so that $\operatorname{lcm}(\Delta_a, a) = \Delta$.*

PROOF: By the previous proposition applied to $\Delta \sim a\Delta_a$, we immediately obtain that $\operatorname{lcm}(S') \prec \Delta_a$. The last statement of the corollary follows since $\Delta = \operatorname{lcm}(S)$ and $\Delta_a \prec \Delta$ by Lemma 2.3(2). ∎

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

COROLLARY 2.2. *Let a be a letter in S, U a word over $S \cup T$, r any integer such that $r \geqslant 2$, and suppose Δ divides $a^r U$. Then for any m such that $1 \leqslant m \leqslant r-1$, Δ also divides $a^{r-m}U$.*

PROOF: Put $U' = a^{r-m}U$. Then Δ divides $a^r U = a^m U'$, so by Proposition 2.1, $b \prec U'$ for every b in S such that $b \neq a$. But $U' = a^{r-m}U$ is also divisible by a since $1 \leqslant m \leqslant r-1$, thus $\operatorname{lcm}(S) = \Delta \prec U'$ as required. □

LEMMA 2.10. *Let I and J be words in $(S \cup T)^*$ and a an element in S. Then the following are equivalent:*

(1) $\Delta \prec I\Delta_a\Delta_{a'}J$;

(2) $\Delta \prec I\Delta_a$ or $\Delta \prec \Delta_{a'}J$;

(3) $I \succ a$ or $a \prec J$.

In particular, $(\Delta_a\Delta_{a'})^m$ is not divisible by Δ for any a in S and any positive integer m.

PROOF: Suppose $\Delta \prec I\Delta_a\Delta_{a'}J$. By Proposition 2.1, either $I \succ a$ or $a \prec \Delta_a\Delta_{a'}J$. If $I \succ a$ then $I \sim I_1 a$ for some word I_1 in $(S \cup T)^*$, hence $I\Delta_a \sim I_1 a\Delta_a \sim I_1\Delta$; thus $I\Delta_a$ is right divisible and so (by Lemma 2.1) is left divisible by Δ. If $a \prec \Delta_a\Delta_{a'}J$ then $\Delta \prec \Delta_a\Delta_{a'}J$ (since $\operatorname{lcm}(\Delta_a, a) = \Delta$); by Lemma 2.3(2) and cancellation, we then obtain that $a' \prec \Delta_{a'}J$ which gives $\Delta \prec \Delta_{a'}J$. Hence (2) follows from (1).

Now assume that Δ divides $I\Delta_a$ or $\Delta_{a'}J$. If $\Delta \prec I\Delta_a$ then Δ right divides $I\Delta_a$ by Lemma 2.1, hence there is a word I_1 in $(S \cup T)^*$ such that $I\Delta_a \sim I_1\Delta \sim I_1 a\Delta_a$, so by cancellation, $I \succ a$. That $\Delta \prec \Delta_{a'}J$ implies $a \prec J$ is deduced immediately by Lemma 2.3(2) and cancellation. Hence (3) follows from (2). That (3) implies (1) is inferred from Lemmas 2.3(2) and 2.1. Observe that (3) yields $\ell(I)$ or $\ell(J)$ is at least 1; thus by a simple induction on m, the last statement of the lemma is proved. □

3. BIRMAN'S CONJECTURE

Except when explicitly stated, we assume throughout this section that M is of any type. The reader is reminded that $\mathcal{SB}_{n+1}$ refers to the singular braid monoid on $n+1$ strings, whilst $\mathcal{B}_{n+1}$ denotes the braid group on $n+1$ strings. Moreover, $\mathcal{SB}_{n+1}$ is precisely the singular Artin monoid of type A_n mentioned in the introduction. The map η from $\mathcal{SB}_{n+1}$ to the group algebra $\mathbb{Z}\mathcal{B}_{n+1}$, induced by

$$\sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}, \quad \tau_i \mapsto \sigma_i - \sigma_i^{-1} \quad \text{for } i \in I,$$

is easily proved to be a monoid homomorphism; η is sometimes referred to as the *Vassiliev homomorphism* **[18]** or *desingularisation map* **[17]**. In **[3**, Remark 1**]**, Birman conjectured that η is faithful, so that the singular braid monoid embeds into the group algebra of the braid group. In 1996, Fenn, Rolfsen and Zhu **[10]** showed that the above map is injective on the set comprised of singular braids with up to two singularities (where a singularity is denoted by a τ_i); the following year, Zhu **[19]** extended this result by showing that it holds for up to three singular points. Dasbach and Gemein **[8]**, simultaneously but independently of Járai **[15]**, discovered that the conjecture holds for the singular braid monoid on three strings. The conjecture was proved in its entirety by Paris **[17]**, whilst East **[9]** demonstrated that it holds for all singular Artin monoids of type $I_2(p)$. Godelle and Paris later proved the truth of the conjecture for right-angled singular Artin monoids in **[12]**. In effect, Birman's conjecture generalises to arbitrary Artin monoids since the Vassiliev homomorphism, η, from any singular Artin monoid to the group algebra of the corresponding Artin group is well defined by the above rule. This fact was observed in [**6**, Remark 25]. Thus we may conjecture the following.

CONJECTURE 1. The Vassiliev homomorphism $\eta : \mathcal{S}G_M \longrightarrow \mathbb{Z}G_M$ is faithful, so that the singular Artin monoid embeds into the group algebra of the Artin group.

We write $X = Y$ if X and Y are equal elements of $\mathrm{Im}(\eta)$, in which case the context of the equality signs should be made clear.

Analogously the map, also denoted by η, from $\mathcal{S}G_M^+$ to $\mathbb{Z}G_M$, induced by $\sigma_i \mapsto \sigma_i$, $\tau_i \mapsto \sigma_i - {\sigma_i}^{-1}$, is a monoid homomorphism, again referred to as the *Vassiliev homomorphism.*

CONJECTURE 2. The Vassiliev homomorphism : $\mathcal{S}G_M^+ \to \mathbb{Z}G_M$ is injective.

Indeed for finite type M, Conjecture 2 implies Conjecture 1, as the following result demonstrates:

OBSERVATION 1. Whenever M is of finite type, Conjecture 2 implies Conjecture 1.

PROOF: Suppose Conjecture 2 holds and that $\eta(U) = \eta(V)$ for some words U and V in $\mathcal{S}G_M$ where, without causing confusion, we denote the equivalence class of a word by the word itself. By Theorem 2.1, there are integers $p(U)$, $p(V)$ and words $\overline{U}$, $\overline{V}$ in $\mathcal{S}G_M^+$ such that $U \approx \Delta^{p(U)}\,\overline{U}$ and $V \approx \Delta^{p(V)}\,\overline{V}$. Then there exist positive integers k_1, k_2 and k such that

$$\Delta^k U \approx \Delta^{k_1}\,\overline{U} \quad \text{and} \quad \Delta^k V \approx \Delta^{k_2}\,\overline{V}. \tag{3.1}$$

By recalling that Δ is over S, we thus deduce that

$$\eta(\Delta^{k_1}\,\overline{U}) = \eta(\Delta^k\,U) = \eta(\Delta^k V) = \eta(\Delta^{k_2}\,\overline{V}).$$

But k_1 and k_2 are positive integers, whilst $\overline{U}$ and $\overline{V}$ are over $S \cup T$, so that $\Delta^{k_1}\,\overline{U}$ and $\Delta^{k_2}\,\overline{V}$ also represent elements of $\mathcal{S}G_M^+$, and their images under η are the same, in either interpretation of η. Hence since Conjecture 2 holds, $\Delta^{k_1}\,\overline{U} \sim \Delta^{k_2}\overline{V}$. By (3.1) we infer that $\Delta^k U \approx \Delta^k V$. The result now follows by cancellation. ∎

Observation 1 thus shows that, when M is of finite type, it is sufficient to prove Birman's conjecture in the positive singular Artin monoid. Many properties hold only in $\mathcal{S}G_M^+$ and not in $\mathcal{S}G_M$; the most obvious such property is preservation of word length, which allows for inductive arguments. In what follows we make some elementary observations about the Vassiliev homomorphism and its relationship with $\mathcal{S}G_M^+$.

Define monoid homomorphisms ε and $\mathcal{N}$ from $\mathcal{S}G_M$ to $(\mathbb{Z}, +)$ by

$$\varepsilon : {\sigma_i}^{\pm 1} \mapsto \pm 1,\ \tau_i \mapsto 0, \quad \mathcal{N} : \sigma_i^{\pm 1} \mapsto 0,\ \tau_i \mapsto 1$$

and a map $^+$ from $(S \cup T)^*$ to S^* by $^+ : \alpha_i \mapsto \sigma_i$, where $\alpha = \sigma$ or τ. So $\varepsilon(A)$ is the exponent sum of sigmas in any word A in $\mathcal{S}G_M$; $\mathcal{N}(A)$ counts the number of singularities (taus) of any word in $\mathcal{S}G_M$; and $^+$ turns every letter from T into a corresponding one in S. Moreover, $^+$ induces a homomorphism : $\mathcal{S}G_M^+ \to G_M^+$, and for any word A in $\mathcal{S}G_M^+$, $\varepsilon(A^+) = \varepsilon(A) + \mathcal{N}(A)$. In [**15**, Lemma 1], Járai showed that we can replace η with a simpler homomorphism ψ introduced below and that the group algebra $\mathbb{Z}\mathcal{B}_{n+1}$ contains no zero divisors. Lemma 3.1 below is obtained by replacing $\mathcal{S}\mathcal{B}_{n+1}$ with $\mathcal{S}G_M$ in [**15**, proof of Lemma 1].

LEMMA 3.1. *Define the homomorphism $\psi : \mathcal{S}G_M \to \mathbb{Z}G_M$ by $\psi(\tau_i) = \sigma_i + \sigma_i^{-1}$ and $\psi({\sigma_i}^{\pm 1}) = {\sigma_i}^{\pm 1}$. Then for any words C, A and B in $\mathcal{S}G_M$:*

(1) *$\eta(A) = \eta(B)$ if and only if $\psi(A) = \psi(B)$, and*

(2) *$\psi(CA) = \psi(CB) \iff \psi(A) = \psi(B) \iff \psi(AC) = \psi(BC)$.*

We define the homomorphism $\psi : \mathcal{S}G_M^+ \to \mathbb{Z}G_M$ as in Lemma 3.1. From the above definitions and result, we deduce the following:

LEMMA 3.2. *Let U and V be in $\mathcal{S}G_M^+$, and suppose $\psi(U) = \psi(V)$. Then $\ell(U) = \ell(V)$ and $\mathcal{N}(U) = \mathcal{N}(V)$.*

PROOF: Observe that $U^+ \approx V^+$ since they both represent the unique monomial of maximal exponent sum of $\psi(U) = \psi(V)$. But

$$\ell(U) = \varepsilon(U) + \mathcal{N}(U) = \varepsilon(U^+) = \varepsilon(V^+) = \varepsilon(V) + \mathcal{N}(V) = \ell(V). \tag{3.2}$$

Notice that for every word A in $\mathcal{S}G_M$ there is a unique monomial, represented by A^-, obtained by replacing each τ_i by ${\sigma_i}^{-1}$ in the support of $\psi(A)$, with minimal exponent sum $\varepsilon(A) - \mathcal{N}(A)$. Then since $\psi(U) = \psi(V)$, it follows that $U^- \approx V^-$, so

$$\varepsilon(U) - \mathcal{N}(U) = \varepsilon(U^-) = \varepsilon(V^-) = \varepsilon(V) - \mathcal{N}(V). \tag{3.3}$$

By (3.2) and (3.3), $\mathcal{N}(U) = \mathcal{N}(V)$. ∎

4. COMMON DIVISORS AND THE VASSILIEV HOMOMORPHISM

For the remainder of this paper we resume our assumption that M is of finite type. In this section we provide a criterion (expressed in Corollary 4.2 below) for determining when two elements of $\mathcal{S}G_M^+$ with the same image under ψ have a non-trivial common divisor.

4.1. THE POSITIVE FORM. The reader is reminded that Δ is the lowest common multiple of the set S, that $\zeta = \Delta^2$, and that the words ζ_a, for $a \in S$, are defined as in Section 2.1.

Now let W be a word over $S \cup S^{-1} \cup T$. Then there are words W_i over $S \cup T$ and generators $\sigma_{a_i}^{-1} \in S^{-1}$ such that

$$W = W_0 \sigma_{a_1}^{-1} W_1 \sigma_{a_2}^{-1} W_2 \ldots W_{k-1} \sigma_{a_k}^{-1} W_k.$$

In accordance with [**6**, Section 5], we can define maps θ_1 and θ_2 by

$$\theta_1(W) = W_0\, \zeta_{a_1}\, W_1\, \zeta_{a_2}\, W_2 \ldots W_{k-1}\, \zeta_{a_k}\, W_k \quad \text{and} \quad \theta_2(W) = k.$$

So θ_1 turns W into a word over $S \cup T$ by replacing each letter σ_a^{-1} from S^{-1} with a corresponding ζ_a, whilst θ_2 counts the number of occurrences of letters from S^{-1} in W. Furthermore, θ_1 acts as the identity on $S \cup T$, and for any words X and Y, $\theta_1(XY) = \theta_1(X)\theta_1(Y)$. Since $\zeta\alpha \sim \alpha\zeta$ for any generator α in $S \cup T$, by centrality, it can be shown (for example, [6, p. 278]) that $\theta_1(W) \approx \zeta^{\theta_2(W)}W$.

For every W over $S \cup S^{-1} \cup T$ let $q(W)$ be the largest integer such that the word $\left(\theta_1(W)/\Delta^{q(W)}\right)$ is defined. Observe that, for any word W and any a in S, $q(a^{-1}) = 1$ and $q(W) \geqslant \theta_2(W) \geqslant 0$. This follows from the fact that (by Lemmas 2.1 and 2.3(1)) $\theta_1(a^{-1}) = \zeta_a \sim \Delta_a\Delta \sim \Delta\Delta_{a'}$ and $\alpha\Delta \sim \Delta\alpha'$ for every generator α in $S \cup T$. Moreover, by Lemma 2.1 again, $\Delta^{q(X)+q(Y)} \prec \theta_1(X)\theta_1(Y) = \theta_1(XY)$, we have $q(XY) \geqslant q(X)+q(Y) \geqslant 0$ for any words X and Y over $S \cup S^{-1} \cup T$. Since $q(W) \geqslant \theta_2(W) \geqslant 0$, the word $\left(\theta_1(W)/\Delta^{\theta_2(W)}\right)$ is always defined and we shall denote it by $N(W)$. Hence $N(W)$ is also a word over $S \cup T$ and N fixes elements of $(S \cup T)^*$. Notice that for any words X and Y over $S \cup S^{-1} \cup T$,

$$\Delta^{\theta_2(XY)}N(XY) \sim \theta_1(XY) = \theta_1(X)\,\theta_1(Y) \sim \Delta^{\theta_2(X)}\,N(X)\,\Delta^{\theta_2(Y)}\,N(Y).$$

Thus, since $\theta_2(XY) = \theta_2(X) + \theta_2(Y)$, Lemmas 2.1 and 2.2(2) yield

$$N(XY) \sim \begin{cases} N(X)\,N(Y) & \text{if } \theta_2(Y) \text{ is even,} \\ \mathcal{R}\big(N(X)\big)\,N(Y) & \text{if } \theta_2(Y) \text{ is odd,} \end{cases} \tag{4.1}$$

by cancellation. Since $N(\Delta) = \Delta$, and by Lemma 2.2(1), $\mathcal{R}(\Delta) \sim \Delta$, we obtain immediately that $N(\Delta\, Y) \sim \Delta\, N(Y)$ for any Y over $S \cup S^{-1} \cup T$.

We call a word W in $(S \cup S^{-1} \cup T)^*$ *minimal* if $q(W) = \theta_2(W)$. We call a word W over $S \cup T$ *prime* if it is not divisible by Δ. By recalling that $q(W)$ is the largest integer such that $\Delta^{q(W)}$ divides $\theta_1(W)$, we see that if W is minimal then $N(W) = \left(\theta_1(W)/\Delta^{q(W)}\right)$ is prime; whereas $\Delta \not\prec N(W) = \left(\theta_1(W)/\Delta^{\theta_2(W)}\right)$ implies that $q(W) = \theta_2(W)$. Thus W is minimal if and only if $N(W)$ is prime.

LEMMA 4.1. *Let X and Y be words over $S \cup S^{-1} \cup T$ such that $X \approx Y$; and let a, b be distinct elements in S. Then:*

(1) *$N(X) \sim N(Y)$ if and only if $\theta_2(X) = \theta_2(Y)$.*

(2) *If $X = a^{-1}X_1$, $Y = b^{-1}Y_1$ and $N(X) \sim N(Y)$ then X and Y are not minimal.*

PROOF: (1) If $\theta_2(X) = \theta_2(Y)$ then since $X \approx Y$,

$$\theta_1(X) \approx \zeta^{\theta_2(X)}X \approx \zeta^{\theta_2(Y)}Y \approx \theta_1(Y);$$

when combined with Theorem 1.1(2), this yields $\theta_1(X) \sim \theta_1(Y)$, so that

$$N(X) = \left(\theta_1(X)/\Delta^{\theta_2(X)}\right) \sim \left(\theta_1(Y)/\Delta^{\theta_2(Y)}\right) = N(Y).$$

Now suppose $N(X) \sim N(Y)$, and suppose further, without loss of generality, that $\theta_2(X) - \theta_2(Y) \geqslant 0$. By multiplying $\left(\theta_1(X)/\Delta^{\theta_2(X)}\right) = N(X)$ through on the left by $\Delta^{\theta_2(X)}$, we

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

obtain

$$\begin{aligned}\theta_1(X) \sim \Delta^{\theta_2(X)}N(X) &\sim \Delta^{\theta_2(X)}N(Y)\\ &= \Delta^{\theta_2(X)-\theta_2(Y)}\,\Delta^{\theta_2(Y)}\big(\theta_1(Y)/\Delta^{\theta_2(Y)}\big)\\ &\approx \Delta^{\theta_2(X)-\theta_2(Y)}\,\theta_1(Y)\\ &\approx \Delta^{\theta_2(X)-\theta_2(Y)}\,\zeta^{\theta_2(Y)}Y\\ &\approx \Delta^{\theta_2(X)+\theta_2(Y)}X \quad (\text{since } X \approx Y, \zeta = \Delta^2).\end{aligned}$$

Thus $\Delta^{2\theta_2(X)}X = \zeta^{\theta_2(X)}X \approx \theta_1(X) \approx \Delta^{\theta_2(X)+\theta_2(Y)}\,X$, and we have $\Delta^{2\theta_2(X)} \sim \Delta^{\theta_2(X)+\theta_2(Y)}$ by cancellation and Theorem 1.1(2), so that $\theta_2(X) = \theta_2(Y)$.

(2) Suppose $X = a^{-1}X_1, Y = b^{-1}Y_1$ and $N(X) \sim N(Y)$. By (1), $\theta_2(X) = \theta_2(Y)$ so

$$1 + \theta_2(X_1) = \theta_2(a^{-1}X_1) = \theta_2(b^{-1}Y_1) = 1 + \theta_2(Y_1),$$

thus $\theta_2(X_1)$ is even if and only if $\theta_2(Y_1)$ is even. When combined with (4.1), this implies

$$N(a^{-1})\,N(X_1) \sim N(X) \sim N(Y) \sim N(b^{-1})\,N(Y_1)$$

if $\theta_2(X_1)$ is even, and

$$\mathcal{R}\big(N(a^{-1})\big)N(X_1) \sim N(X) \sim N(Y) \sim \mathcal{R}\big(N(b^{-1})\big)N(Y_1)$$

if $\theta_2(X_1)$ is odd. Let $L = \operatorname{lcm}\big(N(a^{-1}),\ N(b^{-1})\big)$ which exists by either of the preceding chains of equivalences. Then $L \sim \operatorname{lcm}(\Delta_{a'},\ \Delta_{b'})$ (see Lemma 4.2(1) below), and since $a \neq b$, we infer from Corollary 2.1 that $\Delta \prec L$. Since $\mathcal{R}(\Delta) \sim \Delta$, it follows that Δ also divides $\mathcal{R}(L)$. Thus $\Delta \prec N(X) \sim N(Y)$, so that X and Y are not minimal. ∎

Lemma 4.2. *For any positive integers r, s and generator a in S,*

(1) *the word a^{-r} is minimal and*

$$N(a^{-r}) \sim \begin{cases} (\Delta_a\,\Delta_{a'})^m & \text{if } r = 2m,\\ (\Delta_{a'}\,\Delta_a)^m\,\Delta_{a'} & \text{if } r = 2m+1;\end{cases}$$

(2) *the word $(a^{-r}a^s)$ is not minimal.*

Proof: (1) The claim certainly holds for $r = 1 = \theta_2(a^{-1})$ since by Lemmas 2.1 and 2.3(1), we obtain that $\theta_1(a^{-1}) = \zeta_a \sim \Delta_a\Delta \sim \Delta\,\Delta_{a'}$, so $N(a^{-1}) \sim \Delta_{a'}$ which is clearly prime. For $r = 2 = \theta_2(a^{-2})$ we deduce from (4.1) and Lemma 2.3(1) that

$$N(a^{-2}) \sim \mathcal{R}\big(N(a^{-1})\big)\,N(a^{-1}) \sim \Delta_a\,\Delta_{a'}.$$

Thus $N(a^{-2}) \sim \Delta_a\,\Delta_{a'}$ which is prime by Lemma 2.10. So suppose that r is any integer such that $r \geqslant 3$ and that the claim holds for all $l < r$. If $r = 2m$ then

$$\begin{aligned}\theta_1(a^{-r}) = \zeta_a^r = \zeta_a^{r-1}\zeta_a &\sim \Delta^{2m-1}\,(\Delta_{a'}\,\Delta_a)^{m-1}\,\Delta_{a'}\,\zeta_a &&(4.2)\\ &\sim \Delta^{2m-1}\,(\Delta_{a'}\,\Delta_a)^{m-1}\,\Delta_{a'}\,\Delta_a\,\Delta\\ &\sim \Delta^{2m}\,(\Delta_a\,\Delta_{a'})^{m-1}\,\Delta_a\,\Delta_{a'} &&(4.3)\\ &= \Delta^{2m}\,(\Delta_a\,\Delta_{a'})^m.\end{aligned}$$

Note that (4.2) was obtained inductively (since $2m - 1 < r$), and (4.3) holds by Lemmas 2.1 and 2.3(1). Hence $N(a^{-r}) \sim (\Delta_a\, \Delta_{a'})^m$ and is prime by Lemma 2.10. For $r = 2m+1$, (4.1) yields

$$\begin{aligned} N(a^{-r}) \;=\; N(a^{-1}\, a^{-2m}) &= N(a^{-1})\, N(a^{-2m}) \\ &\sim \Delta_{a'}\, (\Delta_a \Delta_{a'})^m \end{aligned}$$

which is also prime by Lemma 2.10. The result for all r now follows by induction.

(2) Since $\theta_2(a^s) = 0$, (4.1) gives $N(a^{-r}a^s) \sim N(a^{-r})N(a^s) \sim N(a^{-r})\, a^s$, from which we infer, by the first part of this lemma, that

$$N(a^{-r}a^s) \;\sim\; \begin{cases} (\Delta_a\, \Delta_{a'})^m\, a^s & \text{if } r = 2m, \\ (\Delta_{a'}\, \Delta_a)^m\, \Delta_{a'}\, a^s & \text{if } r = 2m+1. \end{cases}$$

But by Lemma 2.3(2), $\Delta \sim \Delta_{a'}a$. Hence Δ divides $N(a^{-r}a^s)$ by Lemma 2.1. Thus $N(a^{-r}a^s)$ is not prime, and so the word $(a^{-r}a^s)$ cannot be minimal. ∎

4.2. Minimal words and the support of ψ. Let U be any word over $S \cup T$, also regarded as an element of SG_M^+. A *summand* of $\psi(U)$ is any word over $S \cup S^{-1}$ obtained by replacing any given instance of τ by σ or σ^{-1}. The *support* of $\psi(U)$ is the set of summands of $\psi(U)$. Let $\mathcal{M}_U$ denote the summands of $\psi(U)$ that are minimal. For example, in type A_2, $\psi(\tau_1\tau_2\sigma_2\tau_1)$ has summands $\sigma_1\sigma_2^2\sigma_1$, $\sigma_1\sigma_2^2\sigma_1^{-1}$, $\sigma_1\sigma_2^{-1}\sigma_2\sigma_1$, $\sigma_1\sigma_2^{-1}\sigma_2\sigma_1^{-1}$, $\sigma_1^{-1}\sigma_2^2\sigma_1$, $\sigma_1^{-1}\sigma_2^2\sigma_1^{-1}$, $\sigma_1^{-1}\sigma_2^{-1}\sigma_2\sigma_1$, $\sigma_1^{-1}\sigma_2^{-1}\sigma_2\sigma_1^{-1}$, and a routine calculation shows

$$\mathcal{M}_{\tau_1\tau_2\sigma_2\tau_1} = \{\sigma_1\sigma_2^2\sigma_1,\ \sigma_1\sigma_2^2\sigma_1^{-1},\ \sigma_1^{-1}\sigma_2^2\sigma_1,\ \sigma_1^{-1}\sigma_2^2\sigma_1^{-1}\}.$$

Lemma 4.3. *Let U, V be words in $(S \cup T)^*$ also regarded as elements of SG_M^+ such that $\psi(U) = \psi(V)$. For every summand F of $\psi(U)$ there is a corresponding summand G of $\psi(V)$ such that $F \approx G$, $\theta_2(F) = \theta_2(G)$, $N(F) \sim N(G)$ and $F \in \mathcal{M}_U$ if and only if $G \in \mathcal{M}_V$.*

Proof: Let F be any element in the support of $\psi(U)$. Since F represents an element of the Artin group G_M and $\psi(U) = \psi(V)$, there is an element G in the support of $\psi(V)$ such that $F \approx G$. Thus F and G are equivalent monomials in G_M, so their exponent sums must be the same; that is, $\varepsilon(F) = \varepsilon(G)$. Since $\varepsilon(A) = \ell(A) - 2\theta_2(A)$ for any word A in $(S \cup S^{-1})^*$, we have $\ell(F) - 2\theta_2(F) = \ell(G) - 2\theta_2(G)$. By Lemma 3.2, $\ell(F) = \ell(U) = \ell(V) = \ell(G)$. Hence $\theta_2(F) = \theta_2(G)$ and $F \approx G$, so that $N(F) \sim N(G)$ by Lemma 4.1(1).

Now let F be an element of $\mathcal{M}_U$. Then F is a minimal word in the support of $\psi(U)$. By the previous argument we deduce the existence of an element G in the support of $\psi(V)$ such that $F \approx G$, $\theta_2(F) = \theta_2(G)$ and $N(F) \sim N(G)$. But F is minimal, so that $N(F) \sim N(G)$ is prime. This shows that G is a minimal word in the support of $\psi(V)$; that is, $G \in \mathcal{M}_V$. ∎

Lemma 4.4. *Let U be a word over $S \cup T$ that is divisible by Δ. Then $\mathcal{M}_U = \emptyset$.*

Proof: Since Δ divides U, there exists a word U_1 over $S \cup T$ such that $U \sim \Delta U_1$. Thus $\psi(U) = \psi(\Delta U_1) = \Delta\, \psi(U_1)$. Now let X be any summand of $\psi(U)$. Then by Lemma 4.3, there is a word Y in the support of $\psi(\Delta U_1)$ such that $X \approx Y$ and $N(X) \sim N(Y)$. But $Y = \Delta Y_1$ for some word Y_1 in the support of $\psi(U_1)$. Hence,

$$\Delta \prec \Delta N(Y_1) \sim N(\Delta Y_1) = N(Y) \sim N(X);$$

this implies that X is not minimal and therefore not an element of $\mathcal{M}_U$. □

Corollary 4.2 below motivates the next proposition.

PROPOSITION 4.1. *Let C be a σ_a-chain to σ_b. Then there exists a word $Z \in \mathcal{M}_C$ such that $N(Z) \sim C'$ where C' is a σ_a [σ_a']-chain to σ_b if $\theta_2(Z)$ is even [odd].*

PROOF: By Lemma 2.4, σ_a does not divide C. Write $C = C_1 \dots C_k$ where each C_i is simple. Lemma 2.7 tells us that the target of C_1 must lie in S. So suppose that σ_c is the target of C_1. Then there exist words P, Q such that $(\sigma_a P,\ C_1\sigma_c Q) \in \mathfrak{R}^\Sigma$. If C_1 is over S, we have that $\sigma_a \not\prec C_1 = C_1^+$ is a σ_a-chain to σ_c, $C_1^+ \in \mathcal{M}_{C_1}$, and $\theta_2(C_1^+) = 0$ is even. Otherwise, inspection of the set $\mathfrak{R}$ of definig relations shows that either

$$C_1 = \tau_j\langle\sigma_a\sigma_j\rangle^q \quad \text{for some } q \text{ such that } 0 \leqslant q \leqslant m_{ja} - 2$$

or $C_1 = \tau_a$. Suppose first that $C_1 = \tau_j\langle\sigma_a\sigma_j\rangle^q$. Then

$$\sigma_a \not\prec N(C_1^+) = C_1^+ = \sigma_j\langle\sigma_a\sigma_j\rangle^q = \langle\sigma_j\sigma_a\rangle^{q+1}$$

since $q + 1 < m_{ja}$. Clearly, C_1^+ is a summand of $\psi(C_1)$ which (since it is not divisible by σ_a) is prime and so must lie in $\mathcal{M}_{C_1}$. Moreover, $\theta_2(C_1^+) = 0$ is even, and C_1^+ is a simple σ_a-chain to σ_c (by definition). So assume that $C_1 = \tau_a$. Then the target of C_1 is $\sigma_c = \sigma_a$. Put $X = \sigma_a^{-1}$ which is obviously a summand of $\psi(C_1)$, and note that $\theta_2(X) = 1$ is odd. By Lemma 4.2(1), X is minimal and $N(X) \sim \Delta_{\sigma_a'}$. Corollary 2.1 tells us that σ_a' does not divide $N(X)$, and thus by Lemma 2.9, $N(X) \sim D$ for some σ_a'-chain D. Since

$$\sigma_a' \prec \Delta \sim \Delta_{\sigma_a'}\sigma_a \sim D\sigma_a$$

by Lemma 2.3(2), the target of D must be $\sigma_a = \sigma_c$ by Lemma 2.6. Hence, in all cases, there exists a word X in $\mathcal{M}_{C_1}$ such that $N(X) \sim C_1'$ where

(4.4) $\quad C_1'$ is a σ_a [σ_a']-chain to σ_c if $\theta_2(X)$ is even [odd].

Now if $k = 1$ then $C = C_1$, $\sigma_b = \sigma_c$, and we are done. Otherwise, $C_2 \dots C_k$ is a σ_c-chain to σ_b, from which we deduce, by induction, a word Y in $\mathcal{M}_{C_2 \dots C_k}$ such that $N(Y) \sim C_2'$ where

(4.5) $\quad C_2'$ is a σ_c [σ_c']-chain to σ_b if $\theta_2(Y)$ is even [odd].

Put $Z = XY$, and note that it is a summand of $\psi(C) = \psi(C_1C_2 \dots C_k)$. Then (4.1) gives

$$N(Z) \sim \begin{cases} C_1'\, C_2' & \text{if } \theta_2(Y) \text{ is even,} \\ \mathcal{R}(C_1')\, C_2' & \text{if } \theta_2(Y) \text{ is odd.} \end{cases}$$

CASE 1. $\theta_2(Y)$ is even.

Put $C' = C_1'C_2'$ so that $N(Z) \sim C'$. Then C_2' is a σ_c-chain to σ_b by (4.5). If $\theta_2(Z)$ is even then $\theta_2(X)$ is also even, so by (4.4), C_1' is a σ_a-chain to σ_c, thus C' is a σ_a-chain to σ_b and $C' \sim N(Z)$. On the other hand, if $\theta_2(Z)$ is odd then $\theta_2(X)$ is odd, and by (4.4) again, C_1' is a σ_a'-chain to σ_c; this shows that C' is a σ_a'-chain to σ_b as required.

CASE 2. $\theta_2(Y)$ is odd.

Put $C' = \mathcal{R}(C_1')\, C_2'$ so that $N(Z) \sim C'$. By (4.5), C_2' is a σ_c'-chain to σ_b. By recalling that $\mathcal{R}$ is an involutionary automorphism of $(S \cup T)^*$ which preserves the set of relations $\mathfrak{R}$, we deduce from (4.4) that

(4.6) $$\mathcal{R}(C_1') \text{ is a } \sigma_a' \ [\sigma_a]\text{-chain to } \sigma_c' \text{ if } \theta_2(X) \text{ is even [odd].}$$

Thus, if $\theta_2(Z)$ is even then $\theta_2(X)$ is odd, so by (4.6), $\mathcal{R}(C_1')$ is a σ_a-chain to σ_c'; this implies that C' is a σ_a-chain to σ_b. On the other hand, if $\theta_2(Z)$ is odd then $\theta_2(X)$ is even, so by (4.6) again, $\mathcal{R}(C_1')$ is a σ_a'-chain to σ_c', and thus C' is a σ_a'-chain to σ_b.

Cases 1 and 2 both show that $N(Z) \sim C'$ where

$$C' \text{ is a } \sigma_a \ [\sigma_a']\text{-chain to } \sigma_b \text{ if } \theta_2(Z) \text{ is even [odd].}$$

Moreover, by Lemma 2.9, C_1' is prime. Since Z is a minimal element in the support of $\psi(C)$, it must (by definition) lie in $\mathcal{M}_C$, and our proof is complete. ∎

COROLLARY 4.1. *Let U be a non-empty word in $(S \cup T)^*$ and a any generator in S. Suppose that $a \not\prec U$. Then $\mathcal{M}_U$ contains an element Z such that $a\ [a'] \not\prec N(Z)$ if $\theta_2(Z)$ is even [odd]. In particular, $\mathcal{M}_U \neq \emptyset$ whenever U is prime.*

PROOF: Since $a \in S$, we deduce from Lemma 2.9 that $U \sim C$ for some a-chain C. Proposition 4.1 now yields a word Z in $\mathcal{M}_C$ such that $N(Z) \sim C'$ where C' is an $a\ [a']$-chain if $\theta_2(Z)$ is even [odd]. By Lemma 2.9 again, we infer that $a\ [a'] \not\prec N(Z)$ if $\theta_2(Z)$ is even [odd]. Certainly $\psi(U) = \psi(C)$ where U and C are regarded as (the same) elements of $\mathcal{S}G_M^+$. By Lemma 4.3, there exists $Z' \in \mathcal{M}_U$ such that $N(Z') \sim N(Z)$. Hence

$$a\ [a'] \not\prec N(Z') \text{ if } \theta_2(Z') \text{ is even [odd],}$$

and the result is proved. ∎

COROLLARY 4.2. *Let U, V be words in $(S \cup T)^*$ also regarded as elements of $\mathcal{S}G_M^+$ such that $\psi(U) = \psi(V)$, and let C be any word over S. Then C divides U if and only if C divides V.*

PROOF: We first prove the 'only if' part of the statement. Suppose first that $U \sim aU_1$ for some generator a in S and word U_1 over $S \cup T$. Put $F = \Delta_{a'}\, U$ and $G = \Delta_{a'}\, V$. Then $\Delta \prec \Delta_{a'} a\, U_1 \sim F$ by Lemma 2.3(2), and $\psi(F) = \Delta_{a'}\, \psi(U) = \Delta_{a'}\, \psi(V) = \psi(G)$ giving a one-one correspondence between the sets $\mathcal{M}_F$ and $\mathcal{M}_G$ by Lemma 4.3. Since Δ divides F, we deduce from Lemma 4.4 that $\mathcal{M}_F = \emptyset$; whilst if G is prime, Corollary 4.1 yields $\mathcal{M}_G \neq \emptyset$ which contradicts the existence of the bijection between $\mathcal{M}_F$ and $\mathcal{M}_G$. Hence Δ also divides $G = \Delta_{a'}V$, so by Lemma 2.3(2) and cancellation, $a \prec V$. This proves the result for $\ell(C) = 1$, and by noting that it holds trivially for $\ell(C) = 0$, starts an induction. So assume that C divides U and $\ell(C) \geqslant 2$. Then there exists a letter a in S and non-empty word C_1 over S such that $C = C_1 a$ and $U \sim C_1 a U_1$ for some word U_1 over $S \cup T$. By induction, we infer the existence of a word V_1 over $S \cup T$ such that $V \sim C_1 V_1$. Thus $\psi(C_1 a U_1) = \psi(U) = \psi(V) = \psi(C_1 V_1)$ which gives $\psi(aU_1) = \psi(V_1)$ (by Lemma 3.1(2)) and shows that a divides V_1. Hence $C = C_1 a$ also divides $V \sim C_1 V_1$ as required, and the result for any $\ell(C)$ follows by induction. Swapping the roles of U and V in the preceding argument proves the converse of the result. ∎

5. The Intermediate Lemma

In this section we prove that the Intermediate Property – discovered in [6, Intermediate Lemma] and expressed in Lemma 5.1 below – is preserved under the Vassiliev homomorphism. As a corollary we deduce that η is injective for a class of monoids which include singular Artin monoids of type $I_2(p)$.

Lemma 5.1. *Let U, V be words in $(S \cup T)^*$ such that $\tau_i U \sim \tau_j V$. Then $m_{ij} \leqslant 2$.*

The proofs of the ensuing Lemmas 5.2 and 5.3, although technical, are straightforward and lead to Proposition 5.1 below.

Lemma 5.2. *Let F be a minimal word in $(S \cup S^{-1} \cup T)^*$, and let q be any integer such that $q \geqslant 1$. If $\theta_2(F)$ is even [odd] then*

(1) *$\sigma_s^q F$ is minimal whenever σ_s $[\sigma_s']$ $\prec$ $N(F)$, and*

(2) *$\sigma_s^{-q} F$ is minimal whenever σ_s $[\sigma_s']$ $\not\prec$ $N(F)$.*

Proof: Suppose F is minimal so $N(F)$ is prime.

Case 1. $\theta_2(F)$ is even.

Suppose first that σ_s divides $N(F)$, so that $N(F) \sim \sigma_s F_1$ for some word F_1 over $S \cup T$. Put $F' = \sigma_s^q F$. By noting that $\theta_2(F)$ is even, (4.1) gives

$$N(F') = N(\sigma_s^q\, F) \sim N(\sigma_s^q)\, N(F) \sim \sigma_s^q\, N(F).$$

Now $\Delta \not\prec N(F) \sim \sigma_s F_1$, so by Corollary 2.2, it follows that

$$\Delta \not\prec \sigma_s^{q+1}\, F_1 = \sigma_s^q\, \sigma_s F_1 \sim \sigma_s^q\, N(F) \sim N(F').$$

Hence $N(F')$ is prime, and thus $F' = \sigma_s^q F$ is minimal. Now assume that $\sigma_s \not\prec N(F)$, and put $F' = \sigma_s^{-q} F$. Then since $\theta_2(F)$ is even, we infer that

$$N(F') = N(\sigma_s^{-q}\, F) \sim N(\sigma_s^{-q})\, N(F)$$

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

by (4.1) again; thus

$$N(F') \sim N(\sigma_s^{-q})\, N(F) \sim \begin{cases} (\Delta_{\sigma_s}\, \Delta_{\sigma_{s'}})^m\, N(F) & \text{if } q = 2m, \\ (\Delta_{\sigma_{s'}}\, \Delta_{\sigma_s})^m\, \Delta_{\sigma_{s'}}\, N(F) & \text{if } q = 2m+1, \end{cases}$$

by Lemma 4.2(1). Since $\sigma_s \not\prec N(F)$, Lemma 2.10 yields that $N(F')$ is prime, so $F' = \sigma_s^{-q}F$ is minimal as required.

CASE 2. $\theta_2(F)$ is odd.

Assume $F' = \sigma_s^{\pm q}F$. By recalling that $\mathcal{R}$ is an involution, we deduce from (4.1) that

$$N(F') \sim \mathcal{R}\big(N(\sigma_s^{\pm q})\big)N(F), \text{ so } \mathcal{R}\big(N(F')\big) \sim N(\sigma_s^{\pm q})\mathcal{R}\big(N(F)\big).$$

Since $\mathcal{R}(\sigma_s) = \sigma_s' \prec N(F)$ if and only if $\sigma_s \prec \mathcal{R}\big(N(F)\big)$ and $\mathcal{R}\big(N(F')\big)$ is prime if and only if $N(F')$ is prime, the argument proceeds exactly as that of each alternative in the previous case. ∎

LEMMA 5.3. *Let $F = \sigma_s F_1$ be a minimal word in $(S \cup S^{-1} \cup T)^*$ such that Δ divides $N(\sigma_r F)$. Then $\sigma_s^{-1}F_1$ is minimal or $m_{rs} = 2$.*

PROOF: Suppose $m_{rs} \neq 2$. We show that $\sigma_s^{-1}F_1$ is minimal.

CASE 1. $\theta_2(F_1)$ is even.

By (4.1) we obtain that $N(F) = N(\sigma_s F_1) \sim \sigma_s N(F_1)$. Since $N(F)$ is prime, by assumption, Lemma 2.1 thus shows that $N(F_1)$ is also prime. Now Δ divides $N(\sigma_r F) = N(\sigma_r\sigma_s F_1)$, so by (4.1) again,

$$\Delta \prec N(\sigma_r\sigma_s F_1) \sim N(\sigma_r\sigma_s)N(F_1) \sim \sigma_r\sigma_s N(F_1). \tag{5.1}$$

By noting that $m_{rs} \neq 2$, it is evident that σ_s is the only generator which right divides $\sigma_r\sigma_s$, hence an application of Proposition 2.1 to (5.1) yields that $\sigma_j \prec N(F_1)$ for every $j \neq s$. Since $N(F_1)$ is prime, this implies that σ_s does not divide $N(F_1)$. Hence $\sigma_s^{-1}F_1$ is minimal by Lemma 5.2(2), as required.

CASE 2. $\theta_2(F_1)$ is odd.

By (4.1) we obtain that $N(F) = N(\sigma_s F_1) \sim \sigma_s' N(F_1)$. Since $N(F)$ is prime, by assumption, Lemma 2.1 thus shows that $N(F_1)$ is also prime. Now Δ divides $N(\sigma_r F) = N(\sigma_r\sigma_s F_1)$, so by (4.1) again,

$$\Delta \prec N(\sigma_r\sigma_s F_1) \sim \mathcal{R}\left(N(\sigma_r\sigma_s)\right)\, N(F_1) \sim \sigma_r'\sigma_s' N(F_1). \tag{5.2}$$

By recalling that $m_{r's'} = m_{rs} \neq 2$, it is clear that $\sigma_{s'} = \sigma_s'$ is the only generator which right divides $\sigma_r'\sigma_s'$, hence an application of Proposition 2.1 to (5.2) yields that $\sigma_{j'} = \sigma_j'$ divides $N(F_1)$ for every $j' \neq s'$. Since $N(F_1)$ is prime, this implies that σ_s' does not divide $N(F_1)$. Hence $\sigma_s^{-1}F_1$ is minimal by Lemma 5.2(2), as required. ∎

Proposition 5.1. *Let $U = \tau_i U_1$, $V = \tau_j V_1$ be words in $(S \cup T)^*$ also regarded as elements of SG_M^+ such that $\psi(U) = \psi(V)$. Then $m_{ij} \leqslant 2$.*

Proof: Suppose $U = \tau_i U_1$ and $V = \tau_j V_1$ provide a counter-example. That is, $\psi(\tau_i U_1) = \psi(\tau_j V_1)$ but $m_{ij} \geqslant 3$. Suppose further that this counter-example is minimal with respect to $\ell(U)$, which by Lemma 3.2, is equal to $\ell(V)$. Then $\ell(U) \geqslant 2$, since $\ell(U) = \ell(V) = 1$ gives $\sigma_i + \sigma_i^{-1} = \psi(U) = \psi(V) = \sigma_j + \sigma_j^{-1}$ which holds precisely when $i = j$. We first show that $V = \tau_j V_1$ is not divisible by σ_j. Suppose, by way of contradiction, that it is. Reduction yields a word P such that $V_1 \sim \sigma_j P$, and by recalling that $\psi(U) = \psi(V)$, Corollary 4.2 implies that σ_j also divides $U = \tau_i U_1$; this gives, by reduction again, a word Q such that $U_1 \sim \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} Q$. Put $C = \langle \sigma_j \sigma_i \rangle^{m_{ij}-1}$. Then

$$U = \tau_i U_1 \sim \tau_i C Q \sim C \tau_d Q \tag{5.3}$$

where τ_d is the target of C. By noting that C is over S, we deduce, from Corollary 4.2 again, that

$$C = \sigma_j \langle \sigma_i \sigma_j \rangle^{m_{ij}-2} \prec V \sim \tau_j \sigma_j P \sim \sigma_j \tau_j P.$$

Since $m_{ij} \geqslant 3$, we infer that $\sigma_i \prec \tau_j P$ by cancellation, so that $P \sim \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} P'$ for some word P' over $S \cup T$. Thus

$$\begin{aligned} V \sim \sigma_j \tau_j P \sim \sigma_j \tau_j \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} P' &\sim \sigma_j \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} \tau_c P' \\ &\sim \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \sigma_d \tau_c P' \\ &= C \sigma_d \tau_c P', \end{aligned}$$

and since $\{c, d\} = \{i, j\}$, $m_{cd} \geqslant 3$. When combined with the preceding equivalence, (5.3) gives

$$\psi(C \sigma_d \tau_c P') = \psi(V) = \psi(U) = \psi(C \tau_d Q),$$

so that $\psi(\sigma_d \tau_c P') = \psi(\tau_d Q)$ by Lemma 3.1(2). Another application of Corollary 4.2 shows that σ_d divides $\tau_d Q$ and this yields a word Q' such that $Q \sim \sigma_d Q'$. Hence

$$\psi(\sigma_d \tau_c P') = \psi(\tau_d Q) = \psi(\tau_d \sigma_d Q') = \psi(\sigma_d \tau_d Q'),$$

so $\psi(\tau_c P') = \psi(\tau_d Q')$ again by Lemma 3.1(2), and $m_{cd} \geqslant 3$. This contradicts the minimality of $\ell(U) = \ell(V)$ (since $\ell(V) > \ell(\tau_c P')$). Thus $\sigma_j \not\prec V$, from which we deduce, by a final application of Corollary 4.2, that $\sigma_j \not\prec U$. This shows that the latter word is prime, and we have $\mathcal{M}_U \neq \emptyset$ by Corollary 4.1. So let X be an element of $\mathcal{M}_U$ such that

$$\sigma_j \; [\sigma_j'] \; \not\prec N(X) \quad \text{if } \theta_2(X) \text{ is even [odd]}, \tag{5.4}$$

the existence of which is guaranteed also by Corollary 4.1. Assume further that $\theta_2(X) = k$ is maximal; that is, if G is any other word in $\mathcal{M}_U$ such that

$$\sigma_j \; [\sigma_j'] \; \not\prec N(G) \quad \text{if } \theta_2(G) \text{ is even [odd]}$$

https://doi.org/10.1017/S0004972700034651 Published online by Cambridge University Press

then $\theta_2(G) \leqslant k$. Now since $U = \tau_i U_1$, we deduce that either $X = \sigma_i^{-1} X_1$ or $X = \sigma_i X_1$ for some summand X_1 of $\psi(U_1)$. We consider each case separately and show that each implies a contradiction.

CASE 1. $X = \sigma_i^{-1} X_1$.

Then $\theta_2(X) = 1 + \theta_2(X_1)$, so $\theta_2(X)$ is even precisely when $\theta_2(X_1)$ is odd. Thus

$$N(X) = N(\sigma_i^{-1} X_1) \sim \begin{cases} N(\sigma_i^{-1}) N(X_1) & \text{if } \theta_2(X_1) \text{ is even,} \\ \mathcal{R}\left(N(\sigma_i^{-1})\right) N(X_1) & \text{if } \theta_2(X_1) \text{ is odd,} \end{cases}$$

by (4.1), and so

$$N(X) \sim \begin{cases} \Delta_{\sigma_i'} N(X_1) & \text{if } \theta_2(X) \text{ is odd,} \\ \Delta_{\sigma_i} N(X_1) & \text{if } \theta_2(X) \text{ is even,} \end{cases}$$

by Lemmas 4.2(1) and 2.3(1). This implies, by Corollary 2.1, that σ_j $[\sigma_j'] \prec N(X)$ if $\theta_2(X)$ is even [odd] which clearly contradicts (5.4).

CASE 2. $X = \sigma_i X_1$.

Since $\psi(U) = \psi(V)$ and $X \in \mathcal{M}_U$, Lemma 4.3 yields the existence of a word Y in $\mathcal{M}_V$ such that

$$N(\sigma_i X_1) = N(X) \sim N(Y) \quad \text{and} \quad \theta_2(X) = \theta_2(Y) = k. \tag{5.5}$$

By noting that $V = \tau_j V_1$, we deduce that $Y = \sigma_j^{\pm 1} Y_1$ for some word Y_1 in the support of $\psi(V_1)$. If $Y = \sigma_j Y_1$ then $\theta_2(X) = \theta_2(Y) = \theta_2(Y_1)$ by (5.5); this gives

$$N(X) \sim N(\sigma_j Y_1) \sim \begin{cases} \sigma_j \, N(Y_1) & \text{if } \theta_2(X) \text{ is even,} \\ \sigma_j' \, N(Y_1) & \text{if } \theta_2(X) \text{ is odd,} \end{cases}$$

by (4.1) and contradicts (5.4). Hence $Y = \sigma_j^{-1} Y_1$. Observe that the word $\sigma_j Y = \sigma_j \sigma_j^{-1} Y_1$ is not minimal by Lemma 4.2(2), so (4.1) and (5.5) imply

$$\begin{aligned} \Delta \prec N(\sigma_j Y) &\sim \begin{cases} \sigma_j \, N(X) & \text{if } \theta_2(X) \text{ is even,} \\ \sigma_j' \, N(X) & \text{if } \theta_2(X) \text{ is odd,} \end{cases} \\ &\sim N(\sigma_j X) = N(\sigma_j \sigma_i X_1). \end{aligned}$$

By recalling that $m_{ij} \geqslant 3$ and that the word $X = \sigma_i X_1$ is minimal, we deduce from Lemma 5.3 that the word $\sigma_i^{-1} X_1$ is also minimal. Since $U = \tau_i U_1$ and X_1 is a summand of $\psi(U_1)$, this shows that $\sigma_i^{-1} X_1 \in \mathcal{M}_U$. Put $F_1 = \sigma_i{}^{-1} X_1$. Then

$$\theta_2(F_1) = 1 + \theta_2(X_1) = 1 + \theta_2(\sigma_i X_1) = 1 + \theta_2(X) = 1 + k,$$

and

$$N(F_1) \sim \begin{cases} \Delta_{\sigma_i'}\, N(X_1) & \text{if } \theta_2(X_1) \text{ is even,} \\ \Delta_{\sigma_i}\, N(X_1) & \text{if } \theta_2(X_1) \text{ is odd,} \end{cases}$$

by (4.1), Lemmas 4.2(1) and 2.3(1). Since F_1 is an element of $\mathcal{M}_U$, Lemma 4.3 yields the existence of a word G_1 in $\mathcal{M}_V$ such that $F_1 \approx G_1$,

$$N(F_1) \sim N(G_1) \quad \text{and} \quad \theta_2(G_1) = \theta_2(F_1) = 1 + k. \tag{5.6}$$

By noting that $V = \tau_j V_1$, we deduce that $G_1 = \sigma_j^{\pm 1} Y_2$ for some summand Y_2 of $\psi(V_1)$. If $G_1 = \sigma_j^{-1} Y_2$ then this would contradict that F_1 is minimal by (5.6) and Lemma 4.1(2). Thus $G_1 = \sigma_j Y_2$, so by (5.4),

$$N(\sigma_i^{-1} X_1) = N(F_1) \sim N(G_1) = N(\sigma_j Y_2), \tag{5.7}$$

and

$$1 + k = \theta_2(F_1) = \theta_2(G_1) = \theta_2(\sigma_j Y_2). \tag{5.8}$$

Observe that the word $\sigma_i F_1 = \sigma_i \sigma_i^{-1} X_1$ is not minimal by Lemma 4.2(2), so

$$\begin{aligned} \Delta \prec N(\sigma_i F_1) &\sim \begin{cases} \sigma_i\, N(G_1) & \text{if } \theta_2(G_1) \text{ is even,} \\ \sigma_i'\, N(G_1) & \text{if } \theta_2(G_1) \text{ is odd,} \end{cases} \\ &\sim N(\sigma_i G_1) = N(\sigma_i \sigma_j Y_2) \end{aligned}$$

by (4.1), (5.7) and (5.8). Since $m_{ij} \geqslant 3$ and the word $G_1 = \sigma_j Y_2$ is an element of $\mathcal{M}_V$, we deduce from Lemma 5.3 that the word $\sigma_j^{-1} Y_2$ is also minimal. This shows that Y_2 must lie in $\mathcal{M}_V$ (since $V = \tau_j V_1$ and Y_2 is a summand of $\psi(V_1)$). Put $G_2 = \sigma_j^{-1} Y_2$. Then (5.8) gives

$$\theta_2(G_2) = \theta_2(\sigma_j^{-1} Y_2) = 1 + \theta_2(Y_2) = 2 + k, \tag{5.9}$$

and since G_2 is minimal, we obtain

$$\Delta \not\prec N(G_2) = N(\sigma_j^{-1} Y_2) \sim \begin{cases} \Delta_{\sigma_j'}\, N(Y_2) & \text{if } \theta_2(Y_2) \text{ is even,} \\ \Delta_{\sigma_j}\, N(Y_2) & \text{if } \theta_2(Y_2) \text{ is odd,} \end{cases}$$

by (4.1), Lemmas 4.2(1) and 2.3(1). This implies, by Corollary 2.1, that

$$\sigma_j\ [\sigma_j'] \not\prec N(G_2) \ \text{ if } \theta_2(G_2) \text{ is even [odd]} \tag{5.10}$$

since $\theta_2(G_2)$ is even if and only if $\theta_2(Y_2)$ is odd by (5.9). By recalling that $G_2 \in \mathcal{M}_V$, a final application of Lemma 4.3 yields the existence of a word F_2 in $\mathcal{M}_U$ such that

$$N(F_2) \sim N(G_2) \quad \text{and} \quad \theta_2(F_2) = \theta_2(G_2).$$

When combined with (5.9) and (5.10), this gives $\theta_2(F_2) = 2 + k > k = \theta_2(X)$ and

$$\sigma_j\ [\sigma_j']\ \not\prec N(F_2) \text{ if } \theta_2(F_2) \text{ is even [odd]},$$

which contradicts the maximality of $\theta_2(X)$ and (5.4). ∎

Recall that $\mathcal{S}G_M$ denotes the monoid of type M generated by $S \cup S^{-1} \cup T$ where $S = \{\sigma_i \mid i \in I\}$, $T = \{\tau_i \mid i \in I\}$, and S^{-1} consists of the set of formal inverses of S. Recall also that the singular braid monoid on $n+1$ strings, $\mathcal{SB}_{n+1}$, is the singular Artin monoid of type A_n; the special case obtained when $I = \{1, 2, \ldots n\}$, $m_{ij} = 3$ when $|i-j| = 1$ and $m_{ij} = 2$ whenever $|i-j| \geqslant 2$. The singular Artin monoid of type $I_2(p)$ is the special case when $I = \{1, 2\}$ and $m_{12} = p \geqslant 3$. Thus if $p = 3$, types A_2 and $I_2(3)$ coincide; the singular braid monoid on three strings, $\mathcal{SB}_3$, is also the singular Artin monoid of type $I_2(3)$. Both types A_n and $I_2(p)$ are finite (see, for example, [**14**, Chapter 2]).

For any $i, j \in I$ such that $m_{ij} \geqslant 3$ let T_{ij} denote the monoid generated by $S \cup S^{-1} \cup \{\tau_i, \tau_j\}$ subject to the same defining relations as $\mathcal{S}G_M$. Let T_{ij}^+ denote the set of equivalence classes of words in $\left(S \cup \{\tau_i, \tau_j\}\right)^*$ under $\sim$. Then T_{ij} and T_{ij}^+ are both submonoids of $\mathcal{S}G_M$ and $\mathcal{S}G_M^+$ respectively.

PROPOSITION 5.2. *The restriction of η from T_{ij} to the group algebra $\mathbb{Z}G_M$ is injective. In particular, the Vassiliev homomorphism $\eta : \mathcal{S}G_{I_2(p)} \longrightarrow \mathbb{Z}G_I$ is faithful.*

PROOF: By Lemma 3.1(1), it suffices to prove the result for ψ. We first prove the result for the positive monoid T_{ij}^+. Suppose that U, V in $\left(S \cup \{\tau_i, \tau_j\}\right)^*$ provide a counter-example. That is, assume $U \not\sim V$ but $\psi(U) = \psi(V)$. Suppose further that this counter-example is minimal with respect to $\ell(U)$, which by Lemma 3.2, is the same as $\ell(V)$. Clearly $\ell(U) \geqslant 2$. If $U \sim CU'$, $V \sim CV'$ for some non-empty word C then $\psi(U') = \psi(V')$ by Lemma 3.1(2), $U' \not\sim V'$, $\ell(U') < \ell(U)$, and hence the minimality of $\ell(U)$ is contradicted. Thus U, V have no common divisor, from which we infer, by Corollary 4.2, that U and V are not divisible by any generator from S. This tells us that $U = \tau_r U_1$ and $V = \tau_s V_1$ for some words U_1, V_1 in T_{ij}^+ and generators τ_r, $\tau_s \in \{\tau_i, \tau_j\}$. By noting that $m_{ij} \geqslant 3$, we deduce from Proposition 5.1 that $r = s$; this shows that τ_r is a common divisor of U and V and so contradicts that gcd $(U, V) = 1$. The result thus holds for T_{ij}^+.

Observe that $\zeta^{-\theta_2(W)}\theta_1(W) \approx W$ for any word W in T_{ij} and $\theta_1(W)$ is an element of T_{ij}^+. The result for T_{ij} thus follows by an argument identical to that of Observation 1. By putting $I = \{1, 2\}$ and $m_{12} = p \geqslant 3$ we obtain $\mathcal{S}G_{I_2(p)} = T_{12}$, and this proves the second statement of the proposition. ∎

REFERENCES

[1] E. Artin, 'Theorie der Zöpfe', *Hamburg Abh.* **4** (1925), 47–72.

[2] J. Baez, 'Link invariants of finite type and perturbation theory', *Lett. Math. Phys.* **26** (1992), 43–51.

[3] J.S. Birman, 'New points of view in knot theory', *Bull. Amer. Math. Soc. (N.S.)* **28** (1993), 253–286.

[4] E. Brieskorn and K. Saito, 'Artin-Gruppen und Coxeter-Gruppen', *Invent. Math.* **17** (1972), 245–271.

[5] R. Charney, 'Artin groups of finite type are biautomatic', *Math. Ann.* **292** (1992), 671–683.

[6] R. Corran, 'A normal form for a class of monoids including the singular braid monoid', *J. Algebra* **223** (2000), 256-282.

[7] R. Corran, *On monoids related to braid groups*, Ph.D. Thesis (School of Mathematics and Statistics, University of Sydney, 2000).

[8] O.T. Dasbach and B. Gemein, 'A faithful representation of the singular braid monoid on three strands', *Ser. Knots Everything* **24** (2000), 48–58.

[9] J. East, 'Birman's conjecture is true for $I_2(p)$', (preprint) http://www.maths.usyd.edu.au:8000/u/pubs/publist/ preprints/2002/east-8.html.

[10] R. Fenn, D. Rolfsen and J. Zhu, 'Centralizers in the braid group and the singular braid monoid', *Enseign. Math.* **42** (1996), 75–96.

[11] F.A. Garside, 'On the braid group and other groups', *Quart. J. Math. Oxford Ser. (2)* **20** (1969), 235–254.

[12] E. Godelle and L. Paris, 'On singular Artín monoids', http://math.u-bourgogne.fr/topolog/IMB2-publication.html année 2003, n.356.

[13] J. González-Meneses, 'Presentations for the monoids of singular braids on closed surfaces', *Comm. Algebra* **30** (2002), 2829–2836..

[14] J.E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics **29** (Cambridge Univ. Press, Cambridge, U.K., 1990).

[15] A. Járai Jr., 'On the monoid of singular braids', *Topology Appl.* **96** (1999), 109–119.

[16] L. Paris, 'Artin monoids inject in their groups', *Comment. Math. Helv.* **77** (2002), 609–637.

[17] L. Paris, 'The proof of Birman's conjecture on singular braid monoids', (preprint) http://math.u-bourgogne.fr/topolog/IMB2-publication.html année 2003, n.338 ArXiv:math.GR/0306422 v1.

[18] V. Vassiliev, *Cohomology of knot spaces*, (V.I. Arnold, Editor), Theory of Singularities and its Applications **1** (Amer. Math. Soc., Profidence, R.I., 1990).

[19] J. Zhu, 'On singular braids', *J. Knot Theory Ramifications* **6** (1997), 427–440.

School of Mathematics and Statistics
University of Sydney
New South Wales 2006
Australia.