On singular Artin monoids and contributions to Birman’s conjecture

Noelle Antony

March 5, 2004

Abstract

Baez and Birman introduced the singular braid monoid on \( n+1 \) strings, \( SB_{n+1} \), which Birman uses in understanding knot invariants. \( SB_{n+1} \) is the type \( A_n \) case of an infinite class of monoids known as singular Artin monoids and denoted by \( SGM \), for a Coxeter matrix \( M \). Birman conjectured and Paris proved that \( SB_{n+1} \) embeds in the complex algebra of the braid group under the desingularisation map or Vassiliev homomorphism, \( \eta \), induced by \( \sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}, \, \tau_i \mapsto \sigma_i - \sigma_i^{-1} \). In effect Birman’s conjecture generalises to arbitrary types since, as noted by Corran, the Vassiliev homomorphism from \( SGM \) to the algebra of the corresponding Artin group is well defined. We deduce general combinatorial results regarding divisibility in positive singular Artin monoids and, when \( M \) is of finite type, a well-defined positive form for \( SGM \) is produced. These facts are then invoked to infer that, when \( M \) is of finite type, \( \eta \) is injective on pairs of words such that a common multiple exists for their positive form.

1 Introduction and preliminaries

Let \( \Gamma^M \) be a labelled graph with \( n \) vertices in one-to-one correspondence with a finite indexing set \( I \), and with edge labels from the set \( \{3, 4, 5, \ldots, \infty\} \). For \( i \neq j \) let \( m_{ij} \) denote the label of the edge between nodes \( i \) and \( j \), or set \( m_{ij} = 2 \) if there is no such edge. Put \( m_{ii} = 1 \) for all \( i \in I \). Let \( \langle xy \rangle^m \) denote the alternating product \( xyx \ldots \) of length \( m \). Let \( S = \{ \sigma_i \mid i \in I \} \), \( T = \{ \tau_i \mid i \in I \} \) and let \( S^{-1} = \{ \sigma_i^{-1} \mid i \in I \} \), the set of formal inverses of \( S \). If \( X \) is a set then \( X^* \) denotes the free monoid generated by \( X \). The Artin group of type \( M \), denoted \( G_M \) is the group generated by \( S \) subject to the relations

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

denoted \( \mathcal{R}_1 \) and called the braid relations. The positive Artin monoid of type \( M \), \( G_M^+ \), is the monoid generated by \( S \) subject to the braid relations \( \mathcal{R}_1 \). 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 \( I \). If the Coxeter group of type \( M \) is finite, then \( M \) is said to be of finite type. The
singular Artin monoid of type $M$, denoted $SG_M$, is the monoid generated by $S \cup S^{-1} \cup T$ and has as its defining relations $R_1$, the free group relations $\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = 1$ and the relations $R_2$ listed below,

\[
\tau_i \tau_j = \tau_j \tau_i \quad \text{if } m_{ij} = 2,
\]

\[
\tau_i (\sigma_j \sigma_i)^{m_{ij}-1} = \begin{cases} 
(\sigma_j \sigma_i)^{m_{ij}-1} \tau_j & \text{if } m_{ij} < \infty \text{ and is odd, or} \\
(\sigma_j \sigma_i)^{m_{ij}-1} \tau_i & \text{if } m_{ij} < \infty \text{ and is even,}
\end{cases}
\]

\[
\tau_i \sigma_i = \sigma_i \tau_i \quad \text{for all } i \in I.
\]

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 $X^2 = \{(U, V) \mid (U, V) \text{ or } (V, U) \in X\}$. 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 $SG_M$, and $A = B$ if the two words are equal letter by letter.

We define the positive singular Artin monoid denoted by $SG_M^+$, to be the monoid generated by $S \cup T$ and defining relations $R$ comprising of both $R_1$ and $R_2$ listed above. Where it does not cause confusion we denote elements of $G_M$, $G_M^+$, $SG_M$ and $SG_M^+$ by words which represent them. If $A$ and $B$ are words over $S \cup T$ we write $A \sim B$ if $A$ can be transformed into $B$ by the use of $R$. By Theorem 20 of [Cor1] we know that $SG_M^+$ embeds into $SG_M$ whenever $M$ is of finite type. We denote by $\ell(A)$ the length of any word $A$ in $(S \cup T)^*$. It is easy to see, by inspection of the defining relations, that $SG_M^+$ is homogenous. Corran [Cor1, p. 258] defined the reduction property and showed [Cor1, Lemma 15] that cancellativity and the reduction property also hold in $SG_M^+$. By reduction we mean an application of the reduction property.

Let $A$ and $B$ be words in $(S \cup T)^*$. We say $A$ divides $B$ or $B$ is a multiple of $A$ if there exists a word $X$ in $SG_M^+$ such that $B = AX$ in which case we write $A \divides B$. We say $A$ right divides $B$, or $B$ is a right multiple of $A$, if there is a word $X$ in $SG_M^+$ such that $B \sim AX$, in which case we write $B \rdivides A$.

Let $\Omega = \{A_1, A_2, \ldots, A_k\}$ be a set of words in $(S \cup T)^*$. If $\Omega$ has a common multiple then by [Cor1], $\Omega$ has a common multiple (unique up to equivalence) of minimal length which we denote by $\lcm(A_1, A_2, \ldots, A_k)$ or $\lcm(\Omega)$. If $\Omega$ has no common multiple then we write $\lcm(A_1, A_2, \ldots, A_k) = \infty$.

The singular braid monoid on $n + 1$ strings, denoted by $SB_{n+1}$, was simultaneously introduced in [Bae] and [Bir]. $SB_{n+1}$ is the singular Artin monoid of type $A_n$, whilst the braid group on $n + 1$ strings is the Artin group of type $A_n$; the special cases obtained when the indexing set $I = \{1, \ldots, n\}$, $m_{ij} = 3$ when $|i - j| = 1$ and $m_{ij} = 2$ when $|i - j| \geq 2$. The map $\eta$ from $SB_{n+1}$ to the group algebra $\mathbb{Z}B_{n+1}$ induced by

$\sigma_i \mapsto \sigma_i, \quad \sigma_i^{-1} \mapsto \sigma_i^{-1}, \quad \tau_i \mapsto \sigma_i - \sigma_i^{-1}$

is easily verified to be a monoid homomorphism; $\eta$ is sometimes referred to as the Vassiliev homomorphism [Vas] or desingularisation map [Par2]. In [Bir, Remark 1] Birman conjectured that $\eta$ is faithful, so that the singular braid monoid embeds into the group alge-
bra of the braid group. Paris [Par2] proved the truth of the conjecture, East [Eas] demonstrated that it holds for singular Artin monoids of type $I_2(p)$ and, in a recent preprint, Godelle and Paris [GP] showed that Birman’s conjecture holds for right-angled singular Artin monoids. In effect Birman’s conjecture generalises to arbitrary Artin types since the Vassiliev homomorphism, $\eta$, from any singular Artin monoid to the group algebra of the corresponding Artin group is well defined. This fact was observed by Corran in [Cor, Remark 25]. Analogously the map, also denoted by $\eta$, from $SG_M^+$ 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. If $I$ and $J$ are equal elements of $\text{Im}(\eta)$ we write $I = J$, in which case the context of the equality signs should be made clear.

In Section 2 we deduce general combinatorial properties, including the “FRZ” property, which apply to $SG_M^+$, extending results found in [Ant]. In Section 3 we assume $M$ is of finite type and give a well-defined positive form for elements of $SG_M$. Moreover for non-trivial positive words $U, V$, we show that if $\eta(U) = \eta(V)$ and $\gcd(U, V) = 1$ then $\text{lcm}(U, V)$ does not exist and neither $U$ nor $V$ is divisible by any generator from the corresponding positive Artin monoid. From this it follows that $\eta$ is injective on pairs of words such that a common multiple exists for their positive form.

2 Divisibility theory

In [Cor1], Corran solved the division and word problems for an infinite class of monoids, called chainable, which include all positive singular Artin monoids. Moreover, the conjugacy, word and division problems for $SG_M$, have been solved in [Cor2] for finite type $M$ whilst the word problem for singular Artin monoids of type $FC$ (which include those of finite type) has recently been solved in [GP]. In this section we deduce some results regarding divisibility in $SG_M^+$. These facts are interesting in their own right but they also allow us to prove the result of Section 3.

The ensuing definitions are obtained from Section 2 of [Cor1]. 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 $(aP, CbQ)$ is a relation in $\mathcal{R}^E$. We call $C$ an $a$-chain if $C = C_1 \ldots C_k$ for simple chains $C_1, \ldots, C_k$ where the source of $C_1$ is $a$ and the source of $C_{i+1}$ is the target of $C_i$ for $i = 1, \ldots, k - 1$. 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.

Lemmas 2.1, 2.2 and 2.3 below are restatements of Lemmas 3, 5 and 4(2) respectively of [Cor1], whilst a proof of Lemma 2.4 can be found in [Ant, Lemma 2.7]:

**Lemma 2.1.** 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 2.2.** If $W$ is a word in $(S \cup T)^*$, $a \in S \cup T$, such that $a$ does not divide $W$ but $\text{lcm}(a, W)$ exists, then $W$ either is empty or there is an $a$-chain $C$ such that $W \sim C$.

**Lemma 2.3.** If $C$ is an $a$-chain such that $a$ divides $Cb$ then $b$ is the target of $C$. 


Lemma 2.4. If $C$ is an $a$-chain to $b$, for some generator $a$ in $S$, then $b$ also lies in $S$.

Define a map $+ : (S \cup T)^* \to S^*$ by $+ : \alpha_i \mapsto \sigma_i$, where $\alpha = \sigma$ or $\tau$; thus $+$ turns every letter from $T$ into a corresponding one in $S$ and induces a homomorphism $SG_M^+ \to G_M^+$.

Lemma 2.5. Let $C$ be a $\tau_j$-chain to $\tau_k$, for some $j, k \in I$ and let $\alpha = \sigma$ or $\tau$. Then

(1) $\alpha_j C \sim C \alpha_k$ and

(2) $C^+$ is an $\alpha_j$-chain to $\alpha_k$ if $\sigma_j \neq C$.

Proof: Write $C = C_1 \ldots C_s$ where each $C_i$ is simple and suppose $d$ is the target of $C_1$. Since the target of $C$ is an element of $T$, Lemma 2.4 tells us that $d = \tau_i$ for some $i \in I$. Thus there exist words $P, Q$ in $SG_M^+$ such that $(C_1 \tau_i P, \tau_j Q) \in R$. Since $C_1 \neq 1$, inspection of $R$ tells us that $P = 1, C_1 = Q$ and $\alpha_j C_1 \sim C_1 \alpha_i$.

If $s = 1$ then $i = k, C = C_1$ and we are done. Otherwise putting $C' = C_2 \ldots C_s$ we see that $C'$ is a $\tau_i$-chain to $\tau_k$ giving, by induction, $\alpha_i C' \sim C' \alpha_k$ whence

$$\alpha_j C = \alpha_j C_1 C' \sim C_1 \alpha_i C' \sim C_1 C' \alpha_k = C \alpha_k$$

as required and the result now follows by induction.

(2) Suppose $\sigma_j \neq C$. Then inspection of $R$ gives $C_1 = \tau_i$, where $m_{ij} = 2$ or $C_1 = (\sigma_i \sigma_j)^{m_{ij} - 1}$, $m_{ij} \geq 2$. In both cases $C_1^+$ is an $\alpha_j$-chain with target $\alpha_i$. If $s = 1$ then $i = k$, $C^+ = C_1^+$ and we are done. So assume that $s \geq 2$ and put $C' = C_2 \ldots C_s$ noting that it is a $\tau_i$-chain to $\tau_k$. If $\sigma_i$ were to divide $C'$ then since $\alpha_i C_1 \sim C_1 \alpha_i$, this would imply that $\sigma_j \ll C_1 C' = C$, a contradiction. Hence $\sigma_i \notin C'$ from which we infer, by induction, that $C^+$ is an $\alpha_j$-chain to $\alpha_k$. Thus $C^+ = C_1^+ C''$ is an $\alpha_j$-chain to $\alpha_k$ as required. The result now follows by induction.

Lemma 2.6 below is part of a general result proved by Corran in [Cor1, Intermediate Lemma (c)].

Lemma 2.6. Let $U, V$ be words in $(S \cup T)^*$ such that $\tau_i U \sim \tau_j V$. Then $i = j$ or $m_{ij} = 2$.

Lemma 2.7. Let $a \in S$, $b \in T$ and $W$ be any word over $S \cup T$. If $a \prec Wb$ then $a \prec W$. If $bW \succ a$ then $W \succ a$.

Proof: Suppose $a$ divides $Wb$ yet $a \neq W$. By Lemma 2.2 there exists an $a$-chain $C$ such that $W \sim C$ so $a \prec Cb$. By Lemma 2.3, $b$ must be the target of $C$ which contradicts Lemma 2.4. Hence $a \prec Wb$ implies $a \prec W$. Reversal yields the last statement of the lemma.
Lemma 2.8. Let $C$ be a $\tau_j$-chain such that $\text{lcm}(\tau_j, C) \neq \infty$. Then there exists a word $P$ over $S$ and $\tau_k \in T$ such that

$$\text{lcm}(\tau_j, C) = \tau_j C P \sim CP\tau_k.$$ 

Furthermore the target of $C$ is an element of $T$ precisely when $P = 1$.

Proof: Suppose the target of $C$ is $\alpha_r$, for $\alpha = \sigma$ or $\tau$, and put $L = \text{lcm}(\tau_j, C) \neq \infty$. By Lemma 2.1 we infer that $C$ is not divisible by $\tau_j$ giving $\ell(L) \geq \ell(C) + 1$. Now $L \sim \tau_j W \sim CU$, for some words $W, U$, $\ell(U) \geq 1$. Lemma 2.1 again and cancellation tell us that the target of $C, \alpha_r$, divides $U$ so that $U \sim \alpha_r U_1$, for some word $U_1$ in $SG^+_M$. Thus

$$L \sim \tau_j W \sim CU \sim C \alpha_r U_1.$$ 

(2.1)

We show that $L \sim CP\tau_k \sim \tau_j CP$, for some $P$ over $S$ and some $\tau_k \in T$, by induction on $\ell(U) \geq 1$. Suppose first that $\ell(U) = 1$ so that $U = \alpha_r$. Then $\tau_j W \succ \alpha_r$ so if $\alpha = \sigma$ then, by Lemma 2.7, $W \sim W_1 \sigma_r$ for some word $W_1$, giving $L \sim \tau_j W \sim \tau_j W_1 \sigma_r \sim C \sigma_r$, by (2.1), and showing, by cancellation, $\tau_j \prec C$, a contradiction, since $C$ is a $\tau_j$-chain. Hence the target of $C$ is $\alpha_r = \tau_r$, from which we infer by Lemma 2.5(1) $C \tau_r \sim \tau_j C$ yielding $L \sim \tau_r \sim \tau_j C$ as required (taking $P = 1$ and $\tau_k = \tau_r$).

Now suppose $\ell(U) \geq 2$. If the target of $C, \alpha_r$, were an element of $T$, then by Lemma 2.5(1) again we would deduce that $C \alpha_r = C \tau_r \sim \tau_j C$ is a common multiple of $\tau_j$ and $C$ of length strictly less than $\ell(L)$, a contradiction. Hence $\alpha = \sigma$. Put $C' = C \sigma_r$, $L' = \text{lcm}(\tau_j, C')$ which exists by (2.1) and divides $L$. Also by (2.1),

$$L \sim \tau_j W \sim C \sigma_r U_1 = C' U_1 \prec L'$$ 

(2.2)

and since $\ell(U_1) \geq 1$, we deduce that $\tau_j \not\sim C'$. Thus $L' \sim L$; this yields, by Lemma 2.2, the existence of a $\tau_j$-chain $C''$ such that $C' \sim C''$. Hence

$$L' \sim L \sim \tau_j W \sim C' U_1 \sim C'' U_1$$

and $\ell(U_1) < \ell(U)$. By the inductive hypothesis we infer that $L' \sim C'' P \tau_k \sim \tau_j C'' P'$, for some word $P'$ over $S$ and $\tau_k \in T$. Recalling $C'' \sim C' = C \sigma_s$ we now obtain

$$C \sigma_s P' \tau_k \sim C'' P' \tau_k \sim L' \sim \tau_j C'' P' \sim \tau_j C \sigma_s P'.$$

Putting $P = \sigma_s P'$, the result now follows by induction. The last statement of the lemma is implied by Lemma 2.5(1). \[\square\]

If $W = a_1 \ldots a_n$, for some $a_i \in S \cup T$, then $\text{Rev}(W) = a_n \ldots a_1$.

Lemma 2.9. If $\tau_j$ [right] divides $V \tau_r W$, for some words $V, W$ over $S$ then $V \tau_r \sim \tau_j V [\tau_r W \sim W \tau_j]$. 
Proof: Assuming \( \tau_j \) divides \( V \tau_r W \) we first show that \( \tau_j \prec V \tau_r \). Suppose not. Put \( L = \text{lcm}(\tau_j, V \tau_r) \) which, since \( \tau_j \) divides \( V \tau_r W \), must exist and divide \( V \tau_r W \). Since \( \tau_j \nprec V \tau_r \), Lemma 2.2 implies the existence of a \( \tau_j \)-chain \( C \), such that \( C \sim V \tau_r \), and Lemma 2.8 in turn shows that

\[
L \sim \text{lcm}(\tau_j, C) = \tau_j CP \sim CP \tau_k,
\]

for some word \( P \) over \( S \) and some \( \tau_k \in T \). But \( \tau_j V \tau_r P \sim \tau_j CP \sim L \prec V \tau_r W \) showing that \( V \tau_r W \) contains at least two elements from \( T \) which is a contradiction since both \( V \) and \( W \) are over \( S \). Hence \( \tau_j \) divides \( V \tau_r \). Now \( \tau_j \nprec V \), since \( V \) is over \( S \), and \( \text{lcm}(\tau_j, V) \) also exists since \( \tau_j \prec V \tau_r \). Thus \( V \sim C \) for some \( \tau_j \)-chain \( C \), by Lemma 2.2, whence \( \tau_j \prec V \tau_r \sim C \tau_r \). Lemma 2.3 now tells us that the target of \( C \) must be \( \tau_r \), so that

\[
V \tau_r \sim C \tau_r \sim \tau_j C \sim \tau_j V,
\]

by Lemma 2.5(1), as stated. Finally, if \( V \tau_r W \) is right divisible by \( \tau_j \) then \( \tau_j \prec \text{Rev}(V \tau_r W) = \text{Rev}(W)\tau_r \text{Rev}(V) \) showing, by the previous argument, that \( \text{Rev}(W)\tau_r \sim \tau_j \text{Rev}(W) \) whence \( \tau_j \tau_r W \sim W \tau_j \) as required.

\( \square \)

**Lemma 2.10.** Let \( C \) be a \( \tau_j \)-chain to \( \sigma_s \) such that \( \text{lcm}(C, \tau_j) \) exists. Then \( \text{lcm}(\tau_j, C \tau_s) = \infty \).

Proof: Noting the target of \( C \) lies in \( S \) we obtain immediately by Lemma 2.8 that

\[
\text{lcm}(\tau_j, C) = \tau_j CP \sim CP \tau_k,
\]

(2.3)

for some non-empty word \( P \) over \( S \) and some \( \tau_k \in T \). Suppose, by way of contradiction, that \( \text{lcm}(\tau_j, C \tau_s) \) exists. Then, since \( \tau_s \) is a \( \sigma_s \)-chain to \( \sigma_s \), \( C \tau_s \) is a \( \tau_j \)-chain to \( \sigma_s \), giving, again by Lemma 2.8,

\[
\text{lcm}(\tau_j, C \tau_s) = \tau_j C \tau_s Q \sim C \tau_s Q \tau_l,
\]

(2.4)

for some non-empty word \( Q \) over \( S \) and some \( \tau_l \in T \). Now \( C \tau_s Q \tau_l \) is a common of multiple of \( \tau_j \) and \( C \), so by (2.3) we infer that \( CP \tau_k \prec C \tau_s Q \tau_l \) yielding, by cancellation, \( P \tau_k \) divides \( \tau_s Q \tau_l \). Put \( L = \text{lcm}(\tau_s, P \tau_k) \) which, since \( P \tau_k \prec \tau_s Q \tau_l \), must exist. Then \( L \prec \tau_s Q \tau_l \), so that

\[
CL \prec C \tau_s Q \tau_l \sim \text{lcm}(\tau_j, C \tau_s),
\]

(2.5)

by (2.4). Since \( \tau_s \) clearly divides \( L \) it follows that \( C \tau_s \prec CL \); whilst (2.3) gives

\[
\tau_j CP \sim CP \tau_k \prec CL
\]

showing that \( \tau_j \) divides \( CL \). This implies that \( \text{lcm}(\tau_j, C \tau_s) \) divides \( CL \). Combined with (2.5) we deduce that

\[
CL \sim \text{lcm}(\tau_j, C \tau_s) \sim C \tau_s Q \tau_l
\]

and by cancellation we obtain

\[
\tau_s Q \tau_l \sim L = \text{lcm}(\tau_s, P \tau_k).
\]

(2.6)
If \( \tau_s \) were to divide \( P \tau_k \) then \( L \sim P \tau_k \sim \tau_s Q_{\bar{\tau}_1} \), by (2.6), contradicting that \( P \) is over \( S \). Hence \( \tau_s \neq P \tau_k \) and \( \text{lcm}(\tau_s, P \tau_k) \) clearly exists, from which we infer, by Lemma 2.2, the existence of a \( \tau_s \)-chain \( C' \) such that \( P \tau_k \sim C' \) giving \( L \sim \text{lcm}(\tau_s, C') \), by (2.6). Lemma 2.8 now implies that

\[
L \sim \text{lcm}(\tau_s, C') \sim C' U \tau_s \sim \tau_s C' U,
\]

for some word \( U \) over \( S \), integer \( r \in I \). The latter equivalence combined with (2.6) thus yield

\[
\tau_s Q_{\bar{\tau}_1} \sim L \sim P \tau_k U \tau_r \sim \tau_s P \tau_k U, \tag{2.7}
\]

so that \( Q_{\bar{\tau}_1} \sim P \tau_k U \), by cancellation, giving \( \tau_k U \sim U_{\bar{\tau}_1} \), by Lemma 2.9. Hence \( Q_{\bar{\tau}_1} \sim P \tau_k U \sim PU_{\bar{\tau}_1} \) from which we deduce, again by cancellation, that \( Q \sim PU \) so

\[
\tau_k U \sim U_{\bar{\tau}_1} \quad \text{and} \quad Q \sim PU. \tag{2.8}
\]

Thus

\[
\tau_j C \tau_s PU \sim \tau_j C \tau_s Q \sim \text{lcm}(\tau_j, C \tau_s) \quad \text{by (2.8) and (2.4)}
\sim C \tau_s Q_{\bar{\tau}_1} \quad \text{by (2.4)}
\sim C \tau_s P \tau_k U \quad \text{by (2.7)}
\]

showing, by cancellation, \( C \tau_s P \tau_k \sim \tau_j C \tau_s P \) is a common multiple of \( C \tau_s \) and \( \tau_j \) which divides \( \text{lcm}(\tau_j, C \tau_s) \). This tells us that \( U = 1 \) so by (2.8) we deduce that

\[
Q \sim P \quad \text{and} \quad l = k \tag{2.9}
\]
yielding \( L \sim \tau_s P \tau_k \sim P \tau_k \tau_r \), by (2.7). Lemma 2.6 and Rev applied to the latter equivalence shows that \( m_{kr} = 2 \) or \( k = r \) whence

\[
\tau_s P \tau_k \sim P \tau_k \tau_r \sim P \tau_r \tau_k \tag{2.10}
\]

so that \( \tau_s P \sim P \tau_r \), by cancellation, which (noting \( + \) is a homomorphism) gives

\[
\sigma_s P \sim P \sigma_r \quad \text{and} \quad m_{kr} \leq 2. \tag{2.11}
\]

Since the target of \( C \) is \( \sigma_s \), Lemma 2.1 and cancellation applied to (2.3) imply that \( \sigma_s \) divides \( P \tau_k \) and so, by Lemma 2.7, \( \sigma_s \prec P \); whence \( P \sim \sigma_s P' \), for some word \( P' \). Thus

\[
\sigma_s^2 P' \sim \sigma_s P \sim P \sigma_r \sim \sigma_s P' \sigma_r
\]

by (2.11), yielding, by cancellation, \( P \sim P' \sigma_r \) and \( m_{kr} \leq 2 \). The latter equivalence combined with (2.3) now gives

\[
\tau_j C P' \sigma_r \sim \tau_j C P \sim \text{lcm}(\tau_j, C)
\sim C P \tau_k \sim C P' \sigma_r \tau_k \sim C P' \tau_k \sigma_r
\]

whence \( \tau_j C P' \sim C P' \tau_k \), by cancellation, is a common multiple of \( \tau_j \) and \( C \) of length strictly less than \( \ell (\text{lcm}(\tau_j, C)) \), a contradiction. \( \Box \)
**Remark 1.** Lemmas 2.10 and 2.5(1) can be invoked to give yet another proof of, what is called in [GP], the “FRZ” property for $SG_M^+$ (where $M$ is of any, not necessarily finite, type). The property was originally discovered in [FRZ] for $SB_{n+1}$ and was extended in [Cor2] and [GP] to show that it holds for $SG_M$ where $M$ is respectively of finite and $FC$ type. However, as this property is not required for our current purposes we prove it in the appendix.

**Lemma 2.11.** Let $\alpha = \sigma$ or $\tau$ and let $C$ be a $\tau_j$-chain to $\sigma_s$. Then $C^+$ is an $\alpha_j$-chain to $\sigma_s$, whenever

1. $C$ is simple or
2. $\sigma_j \not\in C$ and $\text{lcm}(\tau_j, C)$ exists.

**Proof:** (1) By definition there exist words $P$, $Q$ such that $(C\sigma_sP, \tau_jQ) \in \mathcal{R}^S$. Since $C \neq 1$ and the target of $C$ lies in $S$ we obtain immediately, by inspection of $\mathcal{R}$, that $C = C^+$ and $(C^+\sigma_sP^+, \sigma_jQ) \in \mathcal{R}^S$, showing that $C^+$ is also an $\alpha_j$-chain to $\sigma_s$.

(2) Write $C = C_1 \ldots C_k$ where each $C_i$ is simple. If $k = 1$ then $C = C_1$ is a simple $\tau_j$-chain to $\sigma_s$ and the result follows by (1). So suppose $k \geq 2$ and put $C' = C_1 \ldots C_{k-1}$. Assume the target of $C'$ is $\beta_s$, where $\beta = \sigma$ or $\tau$, and hence the source of $C_k$. If $\beta = \tau$ then $C'$ is a $\tau_j$-chain to $\tau_s$, so, noting $\sigma_j \not\in C = C'C_k$ we deduce that $\sigma_j \not\in C'$ giving $C'^+$ is an $\alpha_j$-chain to $\alpha_s$, by Lemma 2.5(2); noting $C_k$ is a simple $\tau_s$-chain to $\sigma_s$ we infer, by (1), that $C_k^+$ is an $\alpha_s$-chain with target $\sigma_s$ whence $C'^+C_k^+ = C^+$ is an $\alpha_j$-chain to $\sigma_s$ as required.

Suppose then that the target of $C'$, $\beta_s$, lies in $S$. Since $\text{lcm}(\tau_j, C'C_k) = \text{lcm}(\tau_j, C)$ exists, by assumption, we deduce that $\text{lcm}(\tau_j, C')$ also exists yielding, by the inductive hypothesis,

$$C'^+ \text{ is an } \alpha_j\text{-chain to } \sigma_s. \tag{2.12}$$

Observe that $C_k$ is a simple $\sigma_s$-chain to $\sigma_s$. If $\sigma_s$ were to divide $C_k^+$ inspection of $\mathcal{R}$ would give $C_k = \tau_s$ whence $C = C'^\tau_s$; recalling the target of $C'$ is $\tau_s$, Lemma 2.10 in turn would imply that $\text{lcm}(\tau_j, C'^\tau_s) = \text{lcm}(\tau_j, C) = \infty$ and hence contradict the hypothesis. Thus $C_k$ is not divisible by $\sigma_s$ and so, again by inspecting the defining relations, we deduce that $C_k^+$ is a $\sigma_s$-chain to $\sigma_s$, giving $C^+ = C'^+C_k^+$ is an $\alpha_j$-chain to $\sigma_s$, by (2.12), as required. The result now follows by induction. \hfill $\Box$

**Proposition 2.1.** Let $W$ be any word in $(S \cup T)^+$ such that $\text{lcm}(\tau_j, W)$ exists. Then $\alpha_j$ divides $W$, for $\alpha = \sigma$ or $\tau$, precisely when $\sigma_j$ divides $W^+$.

**Proof:** It is clear that $\sigma_j$ divides $W^+$ whenever $W$ is divisible by $\sigma_j$ (since $+$ is a homomorphism). So suppose that $\sigma_j \not\in W$ for both $\alpha = \sigma$ and $\alpha = \tau$. If $W = 1$ there is nothing to show so we may assume that $\ell(W) \geq 1$. Thus $W$ is a non-empty word that is not divisible by $\tau_j$ and $\text{lcm}(\tau_j, W)$ exists; this implies, by Lemma 2.2, the existence of a $\tau_j$-chain $C$ such that $W \sim C$. Also, $\sigma_j \not\in W \sim C$. Lemmas 2.5(2) and 2.11 now tell us that $C^+$ is a $\sigma_j$-chain and so, by Lemma 2.1, cannot be divisible by $\sigma_j$. Hence $\sigma_j \not\in C^+ \sim W^+$ as required. \hfill $\Box$
3 Birman’s conjecture

In [Jár, Lemma 1] Járai showed that we can replace η with a simpler homomorphism ψ introduced below and that the group algebra $\mathbb{Z}B_{n+1}$ contains no zero divisors. Lemma 3.1 below is obtained by replacing $SB_{n+1}$ with $SG_M$ in the proof of [Jár, Lemma 1].

**Lemma 3.1.** Define the homomorphism $\psi : SG_M \to \mathbb{Z}G_M$, by $\psi(\tau_i) = \sigma_i + \sigma_i^{-1}$ and $\psi(\sigma_i^{\pm1}) = \sigma_i^{\pm1}$. Then for any words $C, A$ and $B$ in $SG_M$,

1. $\eta(A) = \eta(B)$ if and only if $\psi(A) = \psi(B)$ and
2. $\psi(CA) = \psi(CB) \iff \psi(A) = \psi(B) \iff \psi(AC) = \psi(BC)$.

Define the homomorphism $\psi : SG^+_M \to \mathbb{Z}G_M$ as in the preceding Lemma 3.1. A proof of the following lemma can be found in [Ant, Lemma 3.2]:

**Lemma 3.2.** If $U, V$ are elements of $SG^+_M$ such that $\psi(U) = \psi(V)$ then $\ell(U) = \ell(V)$.

**Remark 2.** Whenever $U$ and $V$ are elements of $SG^+_M$ with the same image under $\psi$, $U^+ \sim V^+$ as they both represent the unique monomial of maximal exponent sum of $\psi(U) = \psi(V)$; this implies $U^+ \sim V^+$ by a theorem of Paris [Par1] that all Artin monoids embed naturally in their associated Artin groups.

Let $\Delta = \text{lcm}(\sigma_1, \ldots, \sigma_n)$ and write $\zeta = \Delta^2$. The first statement of Theorem 3.1 below is due to Brieskorn and Saito ([BS, Theorem 5.6]); the second is a combination of discoveries made by Corran and Brieskorn and Saito in [Cor1, Lemma 18] and [BS, Theorem 7.2] respectively.

**Theorem 3.1.** $M$ is of finite type if and only if $\Delta$ exists. Whenever $M$ is of finite type the centre of $SG_M$ is generated by $\Delta$ except for types $A_n$, when $n \geq 2$, $D_{2k+1}$, $E_6$ and $I_2(2q + 1)$, in which case $\Delta^2$ represents the generator of the centre.

The remainder of this paper assumes that $M$ is of finite type; so by Theorem 3.1 $\Delta$ exists. Let $W$ be a word over $S \cup S^{-1} \cup T$. Then there are words $W_1$ over $S \cup T$ and generators $\sigma_{\alpha}^{-1} \in S^{-1}$ such that $W = W_0\sigma_{\alpha_1}^{-1}W_1\sigma_{\alpha_2}^{-1}W_2\ldots W_{k-1}\sigma_{\alpha_k}^{-1}W_k$. According to [Cor1, p.278] define maps $\theta_1$ and $\theta_2$ by

$$\theta_1(W) = W_0 \zeta_{\alpha_1} W_1 \zeta_{\alpha_2} W_2 \ldots W_{k-1} \zeta_{\alpha_k} W_k$$

and

$$\theta_2(W) = k.$$

So $\theta_1$ turns $W$ into a word over $S \cup T$ by replacing each letter $\sigma_{\alpha_i}^{-1}$ from $S^{-1}$ with a corresponding $\zeta_{\alpha}$, whilst $\theta_2$ counts the number of occurrences of letters from $S^{-1}$ in $W$. Furthermore, $\theta_1$ 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 $\zeta_\alpha \sim \zeta_\beta$ for any generator $\alpha$ in $S \cup T$, by centrality, it can be shown [Cor1, p.278] that $\theta_1(W) \approx \zeta^{\theta_2(W)}W$, for any word $W$.

Let $U$, $V$ be words over $S \cup S^{-1} \cup T$. We say $U$ and $V$ differ by an elementary transformation if there are words $X$ and $Y$ and a relation $\langle \rho_1, \rho_2 \rangle \in \prod_\Sigma$ such that $V = X\rho_1 Y$ and $U = X\rho_2 Y$. We say that a word $V$ is obtained from $U$ by a trivial insertion if there are words $X, Y$ and a letter $a \in S \cup S^{-1}$ such that $U = XY$ and $V = Xaa^{-1}Y$. In this case we also say that $U$ is obtained from $V$ by a trivial deletion. The next result is a restatement of Lemma 19 of [Cor1]:

---

**Remark 2.** Whenever $U$ and $V$ are elements of $SG^+_M$ with the same image under $\psi$, $U^+ \sim V^+$ as they both represent the unique monomial of maximal exponent sum of $\psi(U) = \psi(V)$; this implies $U^+ \sim V^+$ by a theorem of Paris [Par1] that all Artin monoids embed naturally in their associated Artin groups.

Let $\Delta = \text{lcm}(\sigma_1, \ldots, \sigma_n)$ and write $\zeta = \Delta^2$. The first statement of Theorem 3.1 below is due to Brieskorn and Saito ([BS, Theorem 5.6]); the second is a combination of discoveries made by Corran and Brieskorn and Saito in [Cor1, Lemma 18] and [BS, Theorem 7.2] respectively.

**Theorem 3.1.** $M$ is of finite type if and only if $\Delta$ exists. Whenever $M$ is of finite type the centre of $SG_M$ is generated by $\Delta$ except for types $A_n$, when $n \geq 2$, $D_{2k+1}$, $E_6$ and $I_2(2q + 1)$, in which case $\Delta^2$ represents the generator of the centre.

For the remainder of this paper we assume that $M$ is of finite type; so by Theorem 3.1 $\Delta$ exists. Let $W$ be a word over $S \cup S^{-1} \cup T$. Then there are words $W_1$ over $S \cup T$ and generators $\sigma_{\alpha}^{-1} \in S^{-1}$ such that $W = W_0\sigma_{\alpha_1}^{-1}W_1\sigma_{\alpha_2}^{-1}W_2\ldots W_{k-1}\sigma_{\alpha_k}^{-1}W_k$. According to [Cor1, p.278] define maps $\theta_1$ and $\theta_2$ by

$$\theta_1(W) = W_0 \zeta_{\alpha_1} W_1 \zeta_{\alpha_2} W_2 \ldots W_{k-1} \zeta_{\alpha_k} W_k$$

and

$$\theta_2(W) = k.$$

So $\theta_1$ turns $W$ into a word over $S \cup T$ by replacing each letter $\sigma_{\alpha_i}^{-1}$ from $S^{-1}$ with a corresponding $\zeta_{\alpha}$, whilst $\theta_2$ counts the number of occurrences of letters from $S^{-1}$ in $W$. Furthermore, $\theta_1$ 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 $\zeta_\alpha \sim \zeta_\beta$ for any generator $\alpha$ in $S \cup T$, by centrality, it can be shown [Cor1, p.278] that $\theta_1(W) \approx \zeta^{\theta_2(W)}W$, for any word $W$.

Let $U$, $V$ be words over $S \cup S^{-1} \cup T$. We say $U$ and $V$ differ by an elementary transformation if there are words $X$ and $Y$ and a relation $\langle \rho_1, \rho_2 \rangle \in \prod_\Sigma$ such that $V = X\rho_1 Y$ and $U = X\rho_2 Y$. We say that a word $V$ is obtained from $U$ by a trivial insertion if there are words $X, Y$ and a letter $a \in S \cup S^{-1}$ such that $U = XY$ and $V = Xaa^{-1}Y$. In this case we also say that $U$ is obtained from $V$ by a trivial deletion. The next result is a restatement of Lemma 19 of [Cor1]:

---
Lemma 3.3. Suppose that $U$ and $V$ are words over $S \cup S^{-1} \cup T$. If $U$ and $V$ differ by an elementary transformation then $\theta_1(U) \sim \theta_1(V)$. If $V$ is obtained from $U$ by a trivial insertion then $\zeta \theta_1(U) \sim \theta_1(V)$.

Lemma 3.4. Let $U$, $V$ be words over $S \cup S^{-1} \cup T$ such that $U \approx V$ and $\theta_2(U) = \theta_2(V)$. Then $\theta_1(U) \sim \theta_1(V)$.

Proof: There is a sequence $U_1, \ldots, U_k$ of words over $S \cup S^{-1} \cup T$ such that $U = U_1 \approx U_2 \approx \ldots \approx U_k = V$ and $U_{i+1}$ is obtained from $U_i$ by an elementary transformation or by insertion or deletion of $aa^{-1}$ for some $a \in S \cup S^{-1}$. If $k = 1$ then the result is trivial and if $k = 2$ then since $\theta_2(U) = \theta_2(V)$, $U = U$ must be obtained from $U_2 = V$ by an elementary transformation giving $\theta_1(U) \sim \theta_1(V)$ by Lemma 3.3 and so starting an induction. Suppose then that $k \geq 3$ and put $r = \theta_2(U_1) = \theta_2(V_1)$. If there exists $s$ such that $2 \leq s \leq k - 1$ and $\theta_2(U_s) = r$ then by the inductive hypothesis $\theta_1(U_1) \sim \theta_1(U_s) \sim \theta_1(U_k)$ and we are done. So assume that $\theta_2(U_s) \neq r$ whenever $2 \leq s \leq k - 1$. Then $\theta_2(U_2) = \theta_2(U_{k-1}) = r \pm 1$, giving, by the inductive hypothesis, $\theta_1(U_2) \sim \theta_1(U_{k-1})$. If $\theta_2(U_2) = \theta_2(U_{k-1}) = r + 1$, $U_2$ and $U_{k-1}$ must be obtained from $U_1$ and $U_k$ respectively by trivial insertions; by Lemma 3.3, this implies

$$\zeta \theta_1(U_1) \sim \theta_1(U_2) \sim \theta_1(U_{k-1}) \sim \zeta \theta_1(U_k)$$

yielding $\theta_1(U_1) \sim \theta_1(U_k)$, by cancellation. If $\theta_2(U_2) = \theta_2(U_{k-1}) = r - 1$, $U_1$ and $U_k$ must be obtained from $U_2$ and $U_{k-1}$ respectively by trivial insertions so that

$$\theta_1(U_1) \sim \zeta \theta_1(U_2) \sim \zeta \theta_1(U_{k-1}) \sim \theta_1(U_k)$$

by Lemma 3.3, as required.

For every word $U$ over $S \cup S^{-1} \cup T$, let $\overline{U}$ denote an element of minimal length which represents $U$. Thus $\theta_2(\overline{U}) \leq \theta_2(U)$ and if $V$ is any word over $S \cup S^{-1} \cup T$ such that $U \approx V$ then $\theta_2(\overline{U}) = \theta_2(\overline{V})$ and so, by Lemma 3.4, $\theta_1(\overline{U}) \sim \theta_1(\overline{V})$. Noting $W \approx \zeta^{-\theta_2(W)} \theta_1(W)$, for any word $W$ in $(S \cup S^{-1} \cup T)^*$ the preceding remarks thus show:

Lemma 3.5. For every element $U$ in $SG_M$ there exists a unique integer $p(U) \leq 0$ and word $N(U)$ in $SG^+_M$ such that $U \approx \zeta^{p(U)} N(U)$.

The next result is a restatement of Corollary 4.2 of [Ant]:

Lemma 3.6. Let $U$, $V$ be words in $(S \cup T)^*$ also regarded as elements of $SG^+_M$ such that $\psi(U) = \psi(V)$ and $C$ any word over $S$. Then $C$ divides $U$ if and only if $C$ divides $V$.

Lemma 3.7. Let $U$, $V$ be words in $(S \cup T)^*$ also regarded as elements of $SG^+_M$ such that $\psi(U) = \psi(V)$. Suppose $\tau_j$ divides $U$ and $\text{lcm}(\tau_j, V)$ exists. Then $\alpha_j$ is a common divisor of $U$ and $V$, for $\alpha = \sigma$ or $\tau$.

Proof: We have $\sigma_j \prec U^+ \sim V^+$ so by Proposition 2.1 we infer that $V \sim \alpha_j V'$ for some word $V'$ over $S \cup T$ and $\alpha = \sigma$ or $\tau$. If $\alpha = \tau$ then $\tau_j$ is a common divisor of $U$ and $V$; whilst if $\alpha = \sigma$ then by Lemma 3.6 we see that $\sigma_j$ also divides $U$ and hence is a common divisor of $U$ and $V$. \qed
Proposition 3.1. In $SG^+_M$, $\eta$ is injective on pairs of words for which a common multiple exists.

Proof: By Lemma 3.1(1) it suffices to prove the result for $\psi$. Let $U, V$ be words in $(S \cup T)^*$ such that $\psi(U) = \psi(V)$ and lcm$(U, V)$ exists. We prove $U \sim V$. By Lemma 3.2 we obtain that $\ell(U) = \ell(V)$. If $U$ is the empty word there is nothing to show, whilst the result clearly holds for $\ell(U) = 1$ and so starts an induction. If $\tau_j \preceq U$ then $\alpha_j$ is a common divisor of $U$ and $V$, by Lemma 3.7; whilst if $\sigma_j \preceq U$ then $\sigma_j$ also divides $V$, by Lemma 3.6. In either case we see that $U \sim \sigma_j U'$ and $V \sim \sigma_j V'$ for some words $U', V'$ and some $\alpha = \sigma$ or $\tau$. This implies, by Lemma 3.1(2) that $\psi(U') = \psi(V')$ and, since lcm$(\alpha_j U', \alpha_j V') \sim \text{lcm}(U, V) \neq \infty$ we infer that lcm$(U', V')$ also exists. By the inductive hypothesis we deduce that $U' \sim V'$ whence $U \sim \alpha_j U' \sim \alpha_j V' \sim V$ as required and the result now follows by induction.

Corollary 3.1. Let $U, V$ be words in $SG_M$ such that $\eta(U) = \eta(V)$ and lcm$(N(U), N(V))$ exists. Then $U \approx V$.

Proof: By Lemma 3.5 we deduce the existence of integers $k_1, k_2 \geq 0$ and words $N(U), N(V)$ in $SG^+_M$ such that

$$U \approx \zeta^{-k_1} N(U) \quad \text{and} \quad V \approx \zeta^{-k_2} N(V).$$

Suppose, without loss of generality, $k = k_1 - k_2 \geq 0$. Multiplying $U$ on the left by $\zeta^{k_1}$ yields $\zeta^{k_1} U \approx N(U)$, whence

$$\eta(N(U)) = \eta(\zeta^{k_1} U) = \eta(\zeta^{k_1} V) = \eta(\zeta^{k_1} \zeta^{-k_2} N(V)) = \eta(\zeta^k N(V)).$$

Observe that, by Theorem 3.1, $\zeta = \Delta^2$ is a central element of $SG^+_M$. Thus, since a common multiple of $N(U)$ and $N(V)$ exists and $k \geq 0$, we infer that lcm$(N(U), \zeta^k N(V))$ must also exist, yielding $N(U) \sim \zeta^k N(V)$ by Proposition 3.1. The latter equivalence combined with (3.1) now gives

$$U \approx \zeta^{-k_1} N(U) \approx \zeta^{-k_1} \zeta^k N(V) = \zeta^{-k_2} N(V) \approx V,$$

as required. □

A Appendix

Lemma A.1. Let $C$ be a word over $S \cup T$, $s, t \in I$. Then the following are equivalent:

1. $\sigma_s C \sim C \sigma_t$.
2. There exists $k \in \mathbb{N}\setminus\{0\}$ such that $\sigma^k_s C \sim C \sigma^k_t$.
3. $\tau_s C \sim C \tau_t$.
(4) There exists $k \in \mathbb{N}\setminus\{0\}$ such that $\tau^k_C \sim C\tau^k_C$.

**Proof:** It is obvious that $(1) \Rightarrow (2)$ and $(3) \Rightarrow (4)$. We prove $(2) \Rightarrow (3)$ and $(4) \Rightarrow (1)$ by induction on $\ell(C)$. If $\ell(C) = 0$ there is nothing to deduce so we may suppose that $\ell(C) \geq 1$ and that both results hold for words of length $< \ell(C)$.

Suppose first that $\tau^k_C \sim C\tau^k_C$. If $\tau_s \prec C$ then $(1)$ follows by cancellation, the inductive hypothesis and since $\tau_s$ and $\sigma_s$ commute. So assume that $\tau_s \not\prec C$. Clearly $\text{lcm}(\tau_s, C')$ exists and divides $C\tau^k_1$ whence $C \sim C'$ for some $\tau_s$-chain $C'$. By Lemma 2.1 and cancellation the target of $C'$ is $\tau_s$. By Lemma 2.5(1) $\sigma_s C \sim \sigma_s C' \sim C'\sigma_t \sim C\sigma_t$. This shows that $(4)$ implies $(1)$.

Now suppose that $\sigma_s C \sim C\sigma_t^k$, for some positive integer $k$. We show $\tau_s C \sim C\tau_t$. If $\sigma_s \not\prec C$ the result follows as before by the inductive hypothesis. So assume that $\sigma_s \not\prec C$. Then $C = \beta_r C''$ for some word $C''$, generator $\beta_r \not\prec \sigma_s$ where $\beta = \sigma$ or $\tau$ so,

$$\sigma_s^k \beta_r C'' = \sigma_s^k C \sim C\sigma_t^k \sim \beta_r C''\sigma_t^k \tag{A.1}$$

Assume $\beta = \sigma$ so that $r \neq s$ and $\sigma_s^k C \sim \sigma_r C'\sigma_t^k$. By reduction we deduce the existence of a word $C''$ such that $C \sim \langle \sigma_r, \sigma_s \rangle^{m_{rs} - 1}C''$ and $\sigma_d \not\prec C''$ where $\sigma_d$ is the target of $\langle \sigma_r, \sigma_s \rangle^{m_{rs} - 1}$. Hence $\sigma_r \sigma_d^{m_{rs} - 1} \sigma_s^k C'' \sim \sigma_s^k C \sim \langle \sigma_r, \sigma_s \rangle^{m_{rs} - 1}C''\sigma_t^k$ from which we infer, by cancellation, $\sigma_d^k C'' \sim C''\sigma_t^k$. The inductive hypothesis now gives $\tau_d C'' \sim C''\tau_t$ so that,

$$\tau_s C \sim \tau_s \langle \sigma_r, \sigma_s \rangle^{m_{rs} - 1}C'' \sim \langle \sigma_r, \sigma_d \rangle^{m_{rs} - 1}\tau_d C'' \sim \langle \sigma_r, \sigma_s \rangle^{m_{rs} - 1}C''\tau_t \sim C\tau_t$$

as required. Assume then that $\beta = \tau$. Observe that $\sigma_s^k$ is a $\tau_s$-chain to $\gamma_r$ where $\gamma = \sigma$ if $m_{rs} \geq 3$ and $\gamma = \tau$ if $m_{rs} \leq 2$. Since $\text{lcm}(\sigma_s^k, \tau_r)$ exists and divides $C\sigma_t^k$, by (A.1), Lemma 2.10 tells us that the first possibility is excluded. Hence $m_{rs} \leq 2$. Combined with (A.1), this implies $\beta_s \sigma_s^k C'' \sim \beta_r C''\sigma_t^k$, giving, by cancellation, $\sigma_s^k C'' \sim C''\sigma_t^k$. By the inductive hypothesis $\tau_s C'' \sim C''\tau_t$ whence

$$\tau_s C \sim \tau_s \beta_r C'' \sim \beta_r \tau_s C'' \sim \beta_r C''\tau_t \sim C\tau_t$$

and our proof is complete. \qed

**References**


