ARTIN GROUPS AND COXETER GROUPS

Egbert Brieskorn and Kyoji Saito

A translation, with notes, of the paper,

Artin-Gruppen und Coxeter-Gruppen, Inventiones math. **17**, 245 – 271, (1972).

Translated by:

C. Coleman, R. Corran, J. Crisp, D. Easdown,

R. Howlett, D. Jackson and A. Ram

at the University of Sydney, 1996.

Introduction

An Artin group is a group G with a presentation by a system of generators $a_i, i \in I$, and relations

$$a_i a_j a_i \cdots = a_j a_i a_j \cdots \quad , \quad i, j \in I$$

where the words on each side of these relations are sequences of m_{ij} letters where a_i and a_j alternate in the sequence. The matrix of values m_{ij} is a *Coxeter matrix* $M = (m_{ij})_{i,j \in I}$ on I. These groups generalize the braid groups established in 1925 by E. Artin in a natural way and therefore we suggest naming them Artin groups.

If one adds the relations $a_i^2 = 1$ to the relations in the presentation of an Artin group then one gets a presentation of a Coxeter group $\overline{G}$. Thus the Coxeter groups are quotient groups of the Artin groups. It is well known that in the case of the braid group one gets the symmetric group in this way.

Since their introduction by Coxeter in 1935 the Coxeter groups have been well studied and a nice presentation of the results can be found in Bourbaki [1]. Other than the free groups, the braid group is the only class of Artin groups that has had a serious line of investigation, in particular, recently the solution of the conjugation problem was given by Garside. For the other Artin groups, a few isolated results appear in [2], [3] and [5]. These references, as well as our own work here, concentrate, for the most part, on the case that the Artin group G corresponds to a finite Coxeter group. The Coxeter groups were already classified by Coxeter himself: these are the finite reflection groups - the irreducible cases being, the groups of Types A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2, H_3, H_4 and $I_2(p)$ with $p = 5$ or $p \geq 7$ (see [1] VI §4.1). It was proved in [2] that for these finite reflection groups the Artin group G is the fundamental group of the spaces X_G of regular orbits for which $\overline{G}$ is the corresponding complex reflection group. In [3] we conjectured, and for a few cases proved, that X_G is an Eilenberg-McLane space so that the cohomology of X_G is isomorphic to the cohomology of G, and thus a few statements were proved about the cohomology of G.

In the following work we study the Artin groups by combinatorial methods, which are very similar to those of Garside. For G with finite $\overline{G}$ we solve the word problem and the conjugation problem and we determine the centre of G. For irreducible $\overline{G}$ the centre of G is infinite cyclic and generated by an appropriate power of the product $a_i \cdots a_n$ of the generators of G. For some cases these results were already known, and J.P. Serre asked us whether this was always the case. This question was the starting point of our work and we would like to thank J.P. Serre for his direction.

Deligne told us that he had constructed in the manner of Tits simplicial complexes on which G operates, and has proved that X_G is an Eilenberg-McLane space for all G with finite $\overline{G}$. We hope that our own work is not made superfluous by the very interesting work of Deligne, which we have not yet seen.

§1. Definition of Artin Groups

In these paragraphs we shall define the Artin groups, and fix some of the nota-

tions and ideas which will follow.

1.1 Let I be an index set, F_I the free group generated by I and F_I^+ the free semigroup generated by I inside F_I. In the following we drop the subscript I when it is clear from the context.

We call the elements of F_I words and the elements of F_I^+ positive words. The empty word is the identity element of F_I^+. The positive words have unique representations as products of elements of I and the number of factors is the length L of a positive word. The elements of I are called letters. Frequently we shall denote the letters $i \in I$ with the more practical notation a_i often also with a, b, c, etc. The equivalence relation on positive words A and B is called letterwise agreement and denoted by $A \equiv B$.

In the following we will very often consider positive words with factors beginning with a and in which only letters a and b occur. Such a word of length q will be denoted $\langle ab \rangle^q$ so that

$$\langle ab \rangle^q \equiv \underbrace{aba\cdots}_{q \text{ factors}}$$

1.2 Let $M = (m_{ij})_{i,j \in I}$ be a Coxeter matrix on I. The *Artin group* G_M corresponding to M is the quotient of F_I by the smallest normal subgroup generated by the relations $\langle ab \rangle^{m_{ab}} (\langle ba \rangle^{m_{ab}})^{-1}$ where a, $b \in I$ and $m_{ab} \neq \infty$. In other words: The Artin group G_M corresponding to M is the group with generators a_i, $i \in I$, and the relations

$$\langle a_i a_j \rangle^{m_{ij}} = \langle a_j a_i \rangle^{m_{ij}} \text{ for } i, j \in I, \text{ and } m_{ij} \neq \infty \, .$$

When the Coxeter matrix M is clear from the context we drop the index M. We denote the images of the letters and words under the quotient homomorphism

$$F_I \longrightarrow G_M$$

by the same symbols and the equivalence relation on elements A and B in G_M is denoted by $A = B$.

If M is a Coxeter matrix on I then the *Coxeter group* $\overline{G}_M$ corresponding to M is the group given by generators a_i, $i \in I$ and the relations

$$\begin{aligned} a_i^2 &= 1 \quad \text{for} \quad i \in I \, , \\ \langle a_i a_j \rangle^{m_{ij}} &= \langle a_j a_i \rangle^{m_{ij}} \quad \text{for} \quad i, j \in I \quad \text{with} \quad m_{ij} \neq \infty \, . \end{aligned}$$

Obviously this is the same group as the one which is defined by the generators a_i, $i \in I$, and the usual relations

$$(a_i a_j)^{m_{ij}} \;=\; 1, \quad \text{for} \quad i,j \in I \quad \text{and} \quad m_{ij} \neq \infty \,.$$

The images of the elements A of G_M under the canonical homomorphism

$$G_M \longrightarrow \overline{G}_M$$

are denoted by $\overline{A}$ and the generating system $\{\overline{a}_i\}_{i\in I}$ by $\overline{I}$. The pair $(\overline{G}_M, \overline{I})$ is a *Coxeter System* in the sense of Bourbaki [1] IV 1.3.

In order to describe the Coxeter matrix M we occasionally use the *Coxeter graph* Γ_M in the sense of Bourbaki [1] IV 1.9.

An Artin group G_M is of *finite type* resp. *irreducible* resp. *of type* A_n, B_n, C_n, D_n etc, when the Coxeter system $(\overline{G}_M, \overline{I})$ is finite resp. irreducible resp. of type A_n, B_n, C_n, D_n etc.

1.3 Let M be a Coxeter matrix. An *elementary transformation* of positive words is a transformation of the form

$$A\langle ab\rangle^{m_{ab}} B \longrightarrow A\langle ba\rangle^{m_{ab}} B$$

where A, $B \in F^+$ and a, $b \in I$. A *positive transformation of length* t from a positive word V to a positive word W is a composition of t elementary transformations that begins with V and ends at W. Two words are *positive equivalent* if there is a positive transformation that takes one into the other. We indicate positive equivalence of V and W by $V \dot{=} W$.

The semigroup of positive equivalence classes of positive words relative to M is denoted G_M^+. The quotient homomorphism $F^+ \longrightarrow G_M^+$ factors over natural homomorphisms:

$$F^+ \longrightarrow G_M^+ \longrightarrow G_M,$$

and for G_M of finite type we will show that $G_M^+ \longrightarrow G_M$ is injective. The equivalence relation on elements $V, W \in G_M^+$ is denoted $V \dot{=} W$.

§2. Reduction Rule

In these paragraphs we prove that one can always reduce in the *Artin semigroup*.

2.1 The main result in this section is the reduction lemma which will be used again and again in this work.

Lemma 2.1. Reduction lemma. *For each Coxeter matrix we have the following reduction rule:*

If X and Y are positive words and a and b are letters such that $aX \doteq bY$ then there exists a positive word W such that

$$X \doteq \langle ba \rangle^{m_{ab}-1} W \quad \textit{and} \quad Y \doteq \langle ab \rangle^{m_{ab}-1} W \ .$$

Proof. The proof is by a double induction, first on the length $L(X)$ of the word X and then on the length t of the positive transformation from aX to bY.

Let A_λ be the statement of the lemma for words of length $L(X) = \lambda$ and let $A_{\lambda,\tau}$ be the statement under the additional condition that aX can be transformed into bY by a positive transformation of length τ. The base cases A_0 and $A_{\lambda,0}$ are trivial. Thus we assume now that A_λ for $\lambda < l$ and $A_{l,\tau}$ for $\tau < t$ hold and prove $A_{l,t}$.

Assume that aX is transformed into bY by a positive transformation of length t. Then there is a positive word cZ such that aX becomes cZ under an elementary transformation and cZ becomes bY by a positive transformation of length $t-1$. If either $c \equiv a$ or $c \equiv b$ then it follows immediately from $A_{l,\tau}$ for $\tau < t$ that $X \doteq Z$, resp. $Y \doteq Z$, and through renewed application of $A_{l,\tau}$, the assertion of the lemma follows.

Hence we suppose that $c \not\equiv a$ and $c \not\equiv b$. Since cZ arises from an elementary transformation of aX, and the induction assumption $A_{l,\tau}$ is applicable to cZ and bY, then there exist positive words U and V such that:

$$X \doteq \langle ca \rangle^{m_{ac}-1} U \quad \text{and} \quad Z \doteq \langle ac \rangle^{m_{ac}-1} U \ ,$$
$$Y \doteq \langle cb \rangle^{m_{ac}-1} V \quad \text{and} \quad Z \doteq \langle bc \rangle^{m_{bc}-1} V \ .$$

If $a \equiv b$ then it follows from the two relations for Z that $U \doteq V$, by using the induction hypothesis for A_λ, $\lambda < l$. Then it follows from the other two relations that $X \doteq Y$, completing the case when $a \equiv b$.

From this point we assume that a, b and c are pairwise distinct. Let $M_{a,b,c}$ be the Coxeter matrix on $\{a,b,c\}$ defined by m_{ab}, m_{ac} and m_{bc}. The proof of the induction step for certain cases is already set out by Garside - namely for the cases in which $M_{a,b,c}$ defines a finite Coxeter group. This is known to be precisely the when the corresponding Graph is one of the following three vertex Coxeter graphs:

$3 \leq p$

$3 \leq p \leq 5$

The cases are completed by reproducing exactly the line of reasoning in the proof of Garside [5] p. 237 and 253. Thus the proof will be complete when we can show that the other cases, in which $M_{a,b,c}$ does not define a finite group, can be dealt with. The remainder of the proof of 2.1 follows from the induction assumption A_λ for $\lambda < l$ and the following Lemma 2.2. $\square$

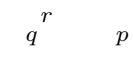
2.2 The reason that we can deal with the above mentioned case is that the relation $aX \doteq bY \doteq cZ$ is only possible for finite $\overline{G}_{M_{a,b,c}}$. To see this we must first prove the following somewhat complicated lemma.

Lemma 2.2. *Let M be a Coxeter matrix for which the statement of the reduction lemma hold for words X such that $L(X) < l$. Let a, b, c be pairwise distinct letters for which the Coxeter matrix $M_{a,b,c}$ does not define a finite Coxeter group. Then there do not exist positive words U, V, and Z with $L(Z) \leq l$ and*

$$Z \doteq \langle ac \rangle^{m_{ac}-1} U \doteq \langle bc \rangle^{m_{bc}-1} V \ .$$

Proof. We assume that U, V and Z are positive words for which the given relation holds and derive a contradiction. We will consider the different cases for the graph Γ of $M_{a,b,c}$. We get from the classification of Coxeter systems of rank three that we have the following possibilities.

Case 1: Γ is a cycle with $p, q, r \geq 3$.

Case 2: Γ is a tree  with $p, q > 3$.

Case 3: Γ is a tree with $p > 5$.

In cases 2 and 3 we will also have to distinguish the different possibilities for the choice of the vertex c in these graphs.

Case 1: We will prove in this case the stronger statement: There do not exist positive words Z, W_1, W_2 with $L(Z) < \ell$ and

$$Z \doteqdot aW_1 \doteqdot bcW_2 \ .$$

Assume that there are such words. Let these be chosen such that $L(Z)$ is minimal. By repeated applications of the reduction rule on the last equality of the given relation we get the existence of words W_3, W_4, W_5 for which

$$\begin{aligned} aW_1 &\doteqdot bcW_2 \\ cW_2 &\doteqdot abW_3 \\ bW_3 &\doteqdot caW_4 \\ aW_4 &\doteqdot bcW_5. \end{aligned}$$

Setting $W_1' \equiv W_4$ and $W_2' \equiv W_5$ and $Z' \equiv aW_4$ we get

$$Z' \ \doteqdot \ aW_1' \ \doteqdot \ bcW_2',$$

and $L(Z') < L(Z)$, contradicting the minimality of $L(Z)$. The remaining cases are similar and we shall be more brief.

Case 2: There are two cases to consider:

(i) c is one of the two end points of Γ,

(ii) c is the middle point of Γ.

(i) Let us suppose that a is the other end point. Suppose that we are given a relation between positive words of minimal length

$$aW_1 \doteqdot bcW_2 \ .$$

From successive applications of the reduction lemma we have the existence of W_3, W_4, W_5, W_6 with

$$\begin{aligned} aW_1 &\doteqdot bcW_2 \\ cW_2 &\doteqdot abaW_3 \\ baW_3 &\doteqdot cW_4 \\ aW_3 &\doteqdot cbcW_5 \\ bcW_5 &\doteqdot aW_6 \ . \end{aligned}$$

On account of the last relation $L(W_6) < L(W_1)$ contradicting the minimality of $L(W_1)$.

(ii) From a relation $aW_1 \doteq bcbW_2$ between positive words of minimal length and successive applications of the reduction lemma we have the existence of W_3, W_4 with

$$bW_2 \doteq acaW_3$$
$$aW_3 \doteq babW_4 \ .$$

The last relation combined with $L(W_3) < L(W_1)$ gives a contradiction.

Case 3: We distinguish three cases:

(i) c is the "middle" point of Γ (thus $m_{ac} = 3, m_{bc} = p$),

(ii) c is the "left" point of Γ (thus $m_{ac} = 2, m_{bc} = 3$),

(iii) c is the "right" point of Γ (thus $m_{ac} = 2, m_{bc} = p$).

(i) Assume that there is a relation

$$aW_1 \doteq bcbcW_2$$

between positive words, the relevant words being of minimal length. By a four fold application of the reduction lemma it follows that there exist words W_3 and W_4 with

$$bcW_2 \doteq acW_3$$
$$W_3 \doteq \langle bc \rangle^{m_{bc}-1} W_4 \ .$$

Substituting the second equation into the first, applying the defining relation and the reduction lemma gives

$$cW_2 \doteq a\langle cb \rangle^{m_{bc}-1} W_4 \ .$$

Again, a two fold application of the reduction lemma gives the existence of a word W_5 with

$$aW_5 \doteq \langle bc \rangle^{m_{bc}-2} W_4 \ .$$

This relation combined with $L(W_5) < L(W_1)$ contradicts the minimality of $L(W_1)$.

(ii) Assume that there is a relation

$$aW_1 \doteq bcW_2$$

between words of length less than l. It follows from the reduction lemma that there exists a word W_3 with

$$cW_2 \doteq \langle ab\rangle^{m_{ab}-1}W_3 \ .$$

One such relation can from (i) not be valid, and the same analysis as in (i) except for only some changes in the markings of the letters and the words.

(iii) Assume that there is a relation

$$aW_1 \doteq bcbcbW_2$$

between words of length $< \ell$. It follows from the reduction lemma that there exists a word W_3 with

$$aW_3 \doteq cbcbW_2$$

Again, by (i), such a relation cannot hold.

Thus all cases are settled and Lemma 2.2 is proved. □

2.3 We shall derive a few easy conclusions from the reduction lemma.

First we note the following. From 2.1 and 2.2 it follows that a positive word can only be divisible by 3 different letters a, b, c if the associated Coxeter matrix $M_{a,b,c}$ defines a finite Coxeter group. Later this statement will be generalized even further.

In addition we remark that in analogy to 2.1 we naturally get a reduction lemma for reduction on the right side. One can reach this conclusion as follows. For each positive word

$$A \equiv a_{i_1} \cdots a_{i_k}$$

define the positive word *rev* A by

$$\text{rev } A \equiv a_{i_k} \cdots a_{i_1} \ .$$

Clearly $A \doteq B$ implies rev $A \doteq$ rev B since the passage from A to rev A is compatible with elementary transformations. It is clear that the application of rev to the words in Lemma 2.1 gives the right hand analog.

¿From Lemma 2.1 and the right hand analog we get the following:

Proposition 2.3. *If A, B and X, Y are positive words with $AXB \doteq AYB$ then $X \doteq Y$.*

The Artin monoid G_M^+ thus satisfies the cancellation condition.

§3. The Division Algorithm

Let U, V and W be positive words. Say U *divides* W (*on the left*) if

$$W \equiv UV \quad \text{(if working in } F^+\text{)},$$
$$W \doteq UV \quad \text{(if working in } G_M^+\text{)},$$

and write $U \mid W$ (interpreted in the context of F^+ or G_M^+).

We present an algorithm which is used later in the theory of divisibility in G_M^+. For example the algorithm can be used to decide whether a given letter divides a positive word, and to determine the smallest common multiple of a letter and a word if it exists.

3.1. Let $a \in I$ be a letter. The simplest positive words which are not multiples of a are clearly those in which a does not appear. Further, the words of the form $\langle ba \rangle^q$ with $q < m_{ab}$ and $m_{ab} \neq 2$ are also not divisible by a. Of course many other quite simple words have this property, for example concatenations of the previous types of words in specific order, called a-chains, which we will define shortly. At the same time we will define what we mean by the *source* and *target* of an a-chain.

Definition. (i) A *primitive a-chain* is a positive word W such that $m_{ab} = 2$ for all letters b in W (so $b \not\equiv a$ and $ab = ba$).

We call a the *source* and *target* of W. (Note vacuously the empty word is a primitive a-chain.)

(ii) An *elementary a-chain* is a positive word of the form $\langle ba \rangle^q$ with $m_{ab} > 2$ and $0 < q < m_{ab}$. The *source* is a, and the *target* is b if q is even, and a if q is odd.

(iii) An *a-chain* is a product $C \equiv C_1 \cdots C_k$ where for each $i = 1, \ldots, k$, C_i is a primitive or elementary a_i-chain for some $a_i \in I$, such that $a_1 = a$ and the target of C_i is the source of C_{i+1}.

[*Ed: This may be expressed as:*

$$a \equiv a_1 \xrightarrow{C_1} a_2 \xrightarrow{C_2} a_3 \longrightarrow \cdots \xrightarrow{C_{n-1}} a_k \xrightarrow{C_k} a_{k+1} \equiv b$$

]

The *source* of C is a and the *target* of C is the target of C_k. If this target is b we say: C is a *chain from a to b.*

[**Example.** $I = \{a, b, c, d\}$, $m_{ab} = m_{bc} = 2$, $m_{cd} = 4$, $m_{ac} = m_{ad} = m_{bd} = 2$.
c, cd, dcd, c^2dcd^7 *are primitive a-chains.*
b, ba *are elementary a-chains.*
a, ab, c, cb *are elementary b-chains.*
dcd, dc, d *are elementary c-chains.*
$\underbrace{a\,b\,a}_{C_1}\ \underbrace{c\,d}_{C_2}\ \underbrace{b\,c}_{C_3}\ \underbrace{a\,b}_{C_4}\ \underbrace{d\,c^2\,d^2}_{C_5}\ \underbrace{b\,a}_{C_6}$ *is a d-chain.*

$$d \xrightarrow[\text{prim}]{C_1} d \xrightarrow[\text{el.}]{C_2} c \xrightarrow[\text{el.}]{C_3} b \xrightarrow[\text{el.}]{C_4} a \xrightarrow[\text{prim}]{C_5} a \xrightarrow[\text{el.}]{C_6} b. \qquad]$$

(iv) There is a unique decomposition of a given a-chain into primitive and elementary factors if one demands that the primitive factors are as large as possible. The number of elementary factors is the *length* of the chain.

Remark. If C is a chain from a to b then rev$C$ is a chain from b to a.

Lemma 3.1. *Let $C \equiv C_1 \cdots C_k$ be a chain from a to b (where C_i is a primitive or elementary chain from a_i to a_{i+1} for $i = 1, \cdots, k$) and D a positive word such that a divides CD. Then b divides D, and in particular a does not divide C.*

Proof. The last claim follows from the first by putting D equal to the empty word. We prove the first claim by induction on k. Suppose $k = 1$.

(a) Suppose $C \equiv x_1 ... x_m$ is primitive, so $m_{ax_i} = 2$ for all i. Then $x_1 ... x_m D \doteq aV$ for some positive word V. [Recall the Reduction Lemma (2.1): If X, Y are positive words and $a, b \in I$ such that $aX \doteq bY$ then there exists a positive word W such that

$$X \doteq \langle ba \rangle^{m_{ab}-1} W \quad \text{and}$$
$$Y \doteq \langle ab \rangle^{m_{ab}-1} W.]$$

By (2.1), $x_2 \cdots x_m D \doteq \langle ax_1 \rangle^{m_{ax_1}-1} W \equiv aW$ for some positive word W. Continuing in this fashion yields that a divides D and we are done (since a is the target of C).

(b) Suppose $C \equiv \langle ba\rangle^q$ is elementary, where $m_{ab} > 2$ and $0 < q < m_{ab}$. Then

$$D \equiv \langle ba\rangle^q D \doteqdot aV$$

for some positive word V. By (2.1), $\langle ab\rangle^{q-1} D \doteqdot \langle ab\rangle^{m_{ab}-1} W$ for some positive word W. So by cancellation (special case of (2.1)),

$$D \doteqdot \begin{cases} \langle ab\rangle^{m_{ab}-q} W & \text{if } q \text{ is odd, or} \\ \langle ba\rangle^{m_{ab}-q} W & \text{if } q \text{ is even.} \end{cases}$$

So D is divisible by a if q is odd, and b if q is even, which is in each case the target of C and we are done.

This begins the induction. Suppose now $k > 1$. By the inductive hypothesis a_k divides $C_k D$, and by (a) and (b), $b \equiv a_{k+1}$ divides D and we are done. □

3.2. For all positive words W and letters $a \in I$ we will define a recursively calculable positive word $T_a(W)$ such that $W \doteqdot T_a(W)$ and either $T_a(W)$ begins with a or $T_a(W)$ is an a-chain. To simplify the description we need other operations on positive words:

(i) Every positive W has a unique factorization

$$W \equiv C_a(W) D_a(W)$$

where $C_a(W) \equiv C_0$ or $C_a(W) \equiv C_0 C_1$ where C_0 is a primitive a-chain and C_1 and elementary a-chain such that the word length of $C_a(W)$ is as large as possible.

(ii) If C is a primitive a-chain put

$$C^+ \equiv aC$$

which is positive equivalent to Ca by commutativity.

If $C \equiv C_0\langle ba\rangle^q$ where C_0 is primitive, put

$$C^+ \equiv \begin{cases} aC & \text{if } q = m_{ab} - 1, \text{ or} \\ C_0\langle ba\rangle^{q+1} & \text{otherwise.} \end{cases}$$

In each case $C^+ \doteqdot Cc$ where c is the target of C.

[*Ed: Note that, if* $q = m_{ab} - 1$,

$$C^+ \equiv aC \doteqdot C_0 a\langle ba\rangle^q \equiv C_0\langle ab\rangle^{m_{ab}} \doteqdot C_0\langle ba\rangle^{m_{ab}} \equiv Cc\ ,$$

where c is the target of C.

N.B.: *The point of this definition is to construct a word C^+ which is positive equivalent to Cc ($C \equiv C_0C_1$ a chain from a to c) and such that either C^+ starts with a, or $C^+ \equiv C_0C_1^+$ where C_1^+ is also elementary, but longer than C_1.*]

(iii) If D is any nonempty positive word denote by D^- the word obtained by deleting the first letter of D. [*Ed: Thus $CD \doteq C^+D^-$.*]

Definition. For W empty or beginning with a put

$$T_a(W) \equiv W.$$

For all other words define $T_a(W)$ recursively: let $L(W) = \ell$ and suppose the a-chain $C_a(W)$ has target c. Then put

$$S_a(W) \equiv \begin{cases} C_a(W)T_c(D_a(W)) & \text{if } c \text{ is not the first letter of } T_c(D_a(W)) \\ C_a(W)^+T_c(D_a(W))^- & \text{otherwise,} \end{cases}$$

and $T_a(W) \equiv S_a^\ell(W)$ (the result of applying S_a ℓ times).

[**Observations.** Let W be positive and $a \in I$. Then

(A) $T_a(W) \equiv S_a(W) \equiv W$ if W is an a-chain or begins with a,

(B) $T_a(W) \doteq S_a(W) \doteq W$.

Proof. (A) The result if clear if W begins with a or is empty. Suppose W is a nonempty a-chain, so $W \equiv C_a(W)D_a(W)$ where $C_a(W)$ is a nonempty chain from a to c, say and $D_a(W)$ is a c-chain. By an inductive hypothesis, since $L(D_a(W)) < L(W)$, $T_c(D_a(W)) \equiv S_c(D_a(W)) \equiv D_a(W)$ so that $S_a(W) \equiv C_a(W)D_a(W) \equiv W$ noting that c cannot be the first letter of $D_a(W)$, whence $T_a(W) \equiv S_a^\ell(W) \equiv W$, and (i) is proved.

(B) Again the result is clear if W begins with a or is empty. Otherwise, we may suppose that $C_a(W)$ is nonempty. Thus $L(D_a(W)) < L(W)$, and by an inductive hypothesis $T_c(D_a(w)) \doteq D_a(W)$. Since $C^+D^- \doteq CD$ it is clear (either way) that

$$S_a(W) \doteq C_a(W)T_c(D_a(W)) \doteq C_a(W)D_a(W) \equiv W\ .$$

Now since $L(S_a(W)) = L(W)$ we may repeat this step ℓ times to show that $T_a(W) \doteq S_a(W) \doteq W$. □]

Lemma 3.2. *Let W be positive and $a \in I$. Then*

(i) *$T_a(W)$ is an a-chain or begins with a,*

(ii) *$T_a(W) \equiv W$ if and only if W is an a-chain or begins with a,*

(iii) *$T_a(W) \doteq W$.*

Proof. The proof for all three parts follows by induction on the wordlength, where the induction basis is trivial. [*Ed: Namely when $L(W) = 0$, $T_a(W) \equiv W$. More concretely, if L(W)=1, then W is a or an a-chain, and the algorithm again leaves W unchanged.*]

(i) [*We may suppose that $L(W) > 0$*]. From the definition of $S_a(W)$ and the induction hypothesis the following is true. If $S_a(W)$ is neither an a-chain nor a word beginning with a, then $C_a(S_a(W))$ has length strictly greater than $C_a(W)$. Hence the result $S_a^k(W)$ of k successive applications of S_a must eventually, for $k = \ell$ at least, be either an a-chain or word beginning with a.

[*Note: If W is an a-chain or begins with a then the first statement is clear since, by Observation (A), $S_a(W) \equiv W$. Otherwise, $C_a(W)$ is non-empty. Then, by the induction hypothesis, if c is not its first letter $T_c(D_a(W))$ is a c-chain and composes with $C_a(W)$ to make $S_a(W)$ an a-chain. Otherwise $S_a(W) = C_a(W)^+T_c(D_a(W))^-$ and, by the* **N.B.** *above, $C_a(W)^+$ either starts with a or is of such a form that is must divide $C_a(S_a(W))$. This last implies that*

$$L(C_a(S_a(W))) \geq L(C_a(W)^+) = L(C_a(W)) + 1\,.$$

Note that, by Observation (A), each further application of S_a either leaves the word unchanged (when it is already either an a-chain or a word beginning with a) or strictly increases the prefix C_a. Thus, after k successive applications, either $S_a^k(W)$ is an a-chain or starts with a, or $L(C_a(S_a^k(W))) \geq L(C_a(W)) + k > k$. This last case gives an obvious contradiction once $k = L(W) = \ell$, since S_a preserves the total word length, so that $L(C_a(S_a^k(W))) \leq L(W)$. Hence $T_a(W)$ must either be an a-chain or start with a. (One may like to observe that, once $k > L(D_a(W))$, the contradiction is already reached).

Claims (ii) and (iii) are immediate from Observations (A) and (B) respectively. The original text reads as follows.]

(ii) From the definition of $S_a(W)$ and the induction hypothesis it follows that, for an a-chain or word W beginning with a, $S_a(W) \equiv W$ and thence that $T_a(W) \equiv W$. The converse follows by (i).

(iii) The proof by induction is trivial, given that $C^+ \doteqdot Cc$. □

3.3. With the help of the projection operators T_a defined in 3.2 one gets a simple algorithm for producing a common multiple of a letter a and a word W, if one exists. If a positive word V begins with a, put

$$R_a(V) \equiv V .$$

If V is a chain from a to b then put

$$R_a(V) \equiv T_a(Vb).$$

Definition. Let W be a positive word and $a \in I$. Then the *a-sequence of* W is the sequence at positive words W_i, for $i = 1, 2, \cdots$ where

$$W_1 \equiv T_a(W) \quad \text{and}$$
$$W_{i+1} \equiv R_a(W_i)$$

for all $i > 1$.

[*Ed: Note that the following lemma anticipates the following section (§4) by effectively demonstrating that if a common multiple exists then the a-sequence of* W *terminates in a word* W' *which is a least common multiple for* a *and* W*. That is both* a *and* W *divide* W'*, and* W' *divides any other common multiple of* a *and* W*.*

The original text is translated below, but we give here an expanded version as follows:

Lemma 3.3. *(i) If* V *is a common multiple of* a *and* W *then* W_i *divides* V *for all* $i > 0$*, and* $W_j \equiv W_{j+1}$ *for* $j > L(V) - L(W)$ *(the sequence terminates).*

(ii) Conversely, if $W_j \equiv W_{j+1}$ *for some* j*, then* W_j *is a common multiple of* a *and* W *(and, by (i), a least common multiple).*

Proof. (ii) Suppose $W_j \equiv W_{j+1}$. By definition W_j begins with a. Certainly $W \doteqdot T_a(W) \equiv W_1$ (by Lemma 3.2). Suppose W divides W_i. Now

$$W_{i+1} \equiv \begin{cases} W_i & \text{if } W_i \text{ begins with } a \\ T_a(W_i b) & \text{if } W_i \text{ is a chain from } a \text{ to } b \end{cases}$$

But $T_a(W_ib) \doteq W_ib$ which is divisible by W_i and hence by W. By induction W divides W_j, so W_j is a common multiple of a and W.

(i) Suppose now that V is a common multiple of a and W. Since $W \doteq T_a(W)$, W_1 divides V. Suppose W_i divides V. Either W_i begins with a, in which case $W_{i+1} \equiv W_i$ and certainly W_{i+1} divides V, or W_i is an a-chain and $W_{i+1} \equiv R_a(W_j) \equiv T_a(W_ib)$ where b is the target of W_i. But $V \doteq aY \doteq W_iZ$ for some positive words T and Z, so by (3.1)

$$V \doteq W_ibZ' \doteq T_a(W_ib)Z \equiv W_{i+1}Z'$$

for some positive word Z. By induction this shows W_i divides V for all i. If $W_i \not\equiv W_{i+1}$ then $L(W_{i+1}) = L(W) + i$. Since $L(W_{i+1}) \leq L(V)$, we must then have $i \leq L(V) - L(W)$. Thus $W_j \equiv W_{j+1}$ for all $j > L(V) - L(W)$. □]

Lemma 3.3. *Let W be a positive word, a a letter, and W_i, $i = 1, 2, ..,$ the a-sequence of W. Then there exists a common multiple V of a and W precisely when $W_j \equiv W_{j+1}$ for $j > L(V) - L(W)$.*

Proof. When $W_j \equiv W_{j+1}$, it follows by the definition of the a-sequence that a divides W_j. Because each W_i clearly divides W_{i+1} [*Ed: and because* $W_1 \doteq W$], then every W_j is a common multiple of a and W. Conversely, if V is a common multiple, then it follows by the definition of W_i together with (3.1) and (3.2) that V is divisible by every W_i. From $W_j \not\equiv W_{j+1}$ it follows that $L(W_{j+1}) = L(W) + j$. From $W_{j+1}|V$ it then follows that $L(W) + j \leq L(V)$. Thus $j > L(V) - L(W)$ implies that $W_j \equiv W_{j+1}$. □

3.4. When a positive word W is of the form $W \equiv UaaV$ where U and V are positive words and a is a letter then we say W has a *quadratic factor.* A word is *square-free* relative to a Coxeter matrix M when W is not positive equivalent to a word with a quadratic factor. The image of a square free word in G_M^+ is called *square-free.*

Lemma 3.4. *Let W be a square-free positive word and a a letter such that aW is not square free. Then a divides W.*

Proof. First we prove the following lemma.

Lemma. *Let V be a positive word which is divisible by a and contains a square. Then there is a positive word $\widetilde{V}$ with $\widetilde{V} \doteq V$ which contains a square and which begins with a.*

The proof of the Lemma is by induction on the length of V. Decompose V, as in 3.2, in the form

$$V \equiv C_a(V)D_a(V) .$$

Without loss of generality we may assume that V is a representative of its positive equivalence class which contains a square and is such that $L(C_a(V))$ is maximal.

When $C_a(V)$ is the empty word it follows naturally that $\widetilde{V} \equiv V$ satisfies the conditions for $\widetilde{V}$. For nonempty $C_a(V)$ we have three cases

(i) $C_a(V)$ contains a square. Then $\widetilde{V} \equiv T_a(V)$ satisfies the conditions for $\widetilde{V}$.

(ii) $D_a(V)$ contains a square. By the induction assumption, one can assume, without loss of generality that $D_a(V)$ begins with the target of the a-chain $C_a(V)$. Thus, since the length of $C_a(V)$ is maximal, $C_a(V)$ is of the form $C_0\langle ba\rangle^{m_{ab}-1}$, where C_0 is a primitive a-chain. From this if follows that when $D_a(V)^-$ contains a square then $\widetilde{V} \equiv aC_a(V)D_a(V)^-$ satisfies the conditions for $\widetilde{V}$, and otherwise $\widetilde{V} \equiv a^2C_a(V)D_a(V)^{--}$ does.

(iii) Neither $C_a(V)$ or $D_a(V)$ contain a square. Then V is of the form $V \equiv C_0\langle ba\rangle^q D_a(V)$ where $q \geq 1$, and $D_a(V)$ begins with a if q is even, and b if q is odd. Then from the fact that a divides V the reduction lemma is applicable and the relations imply that there exists E such that

$$D_a(V) \doteq \langle ba\rangle^{m_{ab}} E .$$

Then

$$\widetilde{V} \equiv aC_0\langle ba\rangle^{m_{ab}-1}\langle ba\rangle^q E \text{ if } m_{ab} \text{ is even}$$
$$\widetilde{V} \equiv aC_0\langle ba\rangle^{m_{ab}-1}\langle ab\rangle^q E \text{ if } m_{ab} \text{ is odd} ,$$

satisfy the conditions.

This finishes the proof of the lemma.

Proof of 3.4. By the Lemma there exists a positive word U, such that U contains a square and $aW \doteq aU$. It follows from the reduction lemma that $U \doteq W$ and, since

W is square free that U does not contain a square. So U begins with a and W is divisible by a.

3.5. By applying 3.4 we get the following lemma which will be needed later.

Lemma 3.5. *If W is a square free positive word and a is a letter then the a-sequences W_i of W are also square free.*

Proof. W_1 is square free since $W_1 \doteq W$. Assume W_i is square free. Then either $W_{i+1} \equiv W_i$ or $W_{i+1} \doteq W_i b_i$ where b_i is the target of the chain W_i. If $W_i b_i$ is not square free then $b_i \mathrm{rev} W_i$ is not square free and by 3.4, the b_i chain W_i is not divisible by b_i, in contradiction to 3.1.

3.6. Using the operators T_a we can give a division algorithm, which, when given positive words V and W such that W divides V, constructs a positive word $V : W$ such that

$$V \doteq W \cdot (V : W) \, .$$

Definition. For $W \equiv a_1 \cdots a_k$, $V : W$ is the word

$$V : W \;\equiv\; T_{a_k}(T_{a_{k-1}}(\cdots T_{a_2}(T_{a_1}(V))^{-})^{-} \cdots)^{-} \, .$$

§4. Divisibility Theory

4.1. By a *common divisor* of a system g_j, $j \in J$ of elements of a semigroup G^+ we mean an element of G^+ which divides each g_j (or more exactly, divides on the left). Similarly, a *common multiple* is an element which is (left) divisible by all g_j, $j \in J$. A *greatest common divisor (g.c.d.)* is a divisor into which all other common divisors divide, and a *least common multiple (l.c.m.)* is a common multiple which divides all other common multiples. The analogous concepts of divisibility on the right are similarly defined.

Because the reduction rule (2.3) holds in the Artin semigroup G_M^+ and no element of G_M^+ other than the identity has an inverse, when greatest common divisors and least common multiples exist, they are uniquely determined. For the

system $g_1, \cdots, g_k \in G^+$, we denote the least common multiple (w.r.t. left divisibility) by $[g_1, \cdots, g_k]_l$ or just $[g_1, \cdots, g_k]$ and the greatest common divisor by $(g_1, \cdots, g_k)_l$ or $(g_1, \cdots, g_k)$. The corresponding notation for divisibility from the right is $[g_1, \cdots, g_k]_r$ and $(g_1, \cdots, g_m)_r$ respectively. Corresponding ideas and notations apply for the positive words (in F^+) which these elements represent.

It is clear that infinite subsets of an Artin semigroup can have no common multiples. But for finite subsets:

Proposition (4.1). *A finite set of elements of an Artin semigroup G_M^+ either has a least common multiple or no common multiple at all.*

Proof. Since one can carry out an induction on the number of elements, it suffices to show that for any two positive words V and W which have a common multiple a least common multiple exists. We prove this simultaneously for all W by induction on the length of V.

Starting the induction: Let $V \equiv a$ and U a common multiple of a and W. Then from (3.3) there is a term W_i in the a-series of W with $W_i \equiv W_{i+1}$. This W_i is then a least common multiple of a and W, since by (3.3) both a and W divide W_i, and from the construction of the a-series and (3.1) it follows that W_j divides U for $j = 1, 2, \ldots, i$.

[*Aside: Recall*

(3.1) If C is a chain from a to b and D a positive word such that CD is divisible by a, then D is divisible by b.

So if $W|U$, then either $W_{k+1} \equiv W_k$ so $W_{k+1}|U$, or W_k is an a-chain from a to b say, and $W_k K \doteq U$ for some word K, and $a|W_k K$, so K must be divisible by b, so $U \doteq W_k b K'$ for some word K', but $W_{k+1} \equiv T_a(Wb)$. So $U \doteq W_{k+1} K'$, and $W_{k+1}|U$.

So we have that W_i is a least common multiple.]

Completing the induction: Let $V \equiv aV'$ and U be a common multiple of V and W with $U \equiv aU'$. Since U is a common multiple of a and W, by the first induction step there is a least common multiple aW' of a and W. By the reduction lemma, U' is a common multiple of V' and W', so by induction hypothesis there exists a least common multiple $[V', W']$. Then $a[V', w']$ is the least common multiple of V and W. $\square$.

4.2 While in certain Artin semigroups there are pairs of elements without a least

common multiple, the greatest common divisor always exists:

Proposition (4.2). *Every non-empty set of elements of an Artin semigroup G_M^+ has a greatest common divisor.*

Proof. Let $X \subseteq G_M^+$ and $W \in X$. The set of common divisors of the elements of X is a finite set $\{A_1, \ldots, A_k\}$, since each of these elements must divide W, and there are only finitely many divisors of W.

[*Aside: A divisor of W cannot be longer than W, and (given a finite indexing set / set of letters) there are only finitely many words of length less than or equal to W in F^+.*]

Since W is a common multiple of all $A_1, \cdots, A_k$, by (4.1), (*Existence of least common multiple*), the least common multiple $[A_1, \cdots, A_k]$ exists, and this is clearly the greatest common divisor of the elements of X.

[*Aside: Let $N = [A_1, \cdots, A_k]$. For all $W \in X$, W is a common multiple of $\{A_1, \cdots, A_k\}$, so since N is the least common multiple, $N|W$. So N is a common divisor of X. So $N \in \{A_1, \cdots, A_k\}$, and since it is a common multiple of this set, it must be the greatest common divisor.*] □

Comment. The only letters arising in the greatest common divisor and least common multiple of a set of words are those occurring in the words themselves.

Proof. For the greatest common divisor it is clear, because in any pair of positive equivalent words exactly the same letters occur. For the least common multiple, the proof is an exact analogue of the existence proof in (4.1).

[*Aside: Recall how we found $[a, W]$: $W_1 \equiv T_a(W)$, and $W_{i+1} \equiv W_i$ if W_i starts with a, or $W_{i+1} \equiv T_a(W_i b)$ if W_i is an a-chain from a to b. But if $b \neq a$, then the only way we can have an a-chain from a to b is if there is an elementary sub-chain somewhere in the a-chain containing b. So W_{i+1} only contains letters which are already in W_i.*]

(4.3) From application of the operation rev to the result of (4.1), it is easy to get the following Lemma:

Lemma (4.3).

(i) *$[A_1, \cdots, A_k]_l$ exists precisely when $[revA_1, \cdots, revA_k]_r$ exists, and then the*

following holds:

$$[A_1, \cdots, A_k]_l \doteq rev\,([rev\,A_1, \cdots,\ rev\,A_k]_r)\ ,$$

(ii) $(A_1, \cdots, A_k)_l \doteq rev\,((rev\,A_1, \cdots,\ rev\,A_k)_r)$.

□

§5. The Fundamental Element

Definition. Let M be a Coxeter-Matrix over I. Let $J \subset I$ be a subset such that the letters[1] of J in G_M^+ possess a common multiple. Then the uniquely determined least common multiple of the letters of J in G_M^+ is called the *fundamental element* Δ_J for J in G_M^+.

The word "fundamental", introduced by Garside, refers to the fundamental role which these elements play. We will show for example that if G_M is irreducible and if there exists a fundamental word Δ_I, then Δ_I or Δ_I^2 generates the centre of G_M. The condition for the existence of Δ_I is very strong: Δ_I exists exactly when G_M is of finite type (cf 5.6).

5.1. The lemmas of the following sections are proven foremost because they will be required in later proofs, but they already indicate the important properties of fundamental elements.

Lemma 5.1. *Let $J \subset I$ be a finite set $J = \{j_1, \cdots, j_k\}$, for which a fundamental element Δ_J in G_M^+ exists. Then we have:*

(i) $\Delta_J \doteq [a_{j_1}, \cdots, a_{j_k}]_l \doteq [a_{j_1}, \cdots, a_{j_k}]_r$.

(ii) $rev\ \Delta_J \doteq \Delta_J$.

Proof. (i) If $[a_{j_1}, \cdots, a_{j_k}]_r$ were not left-divisible by an a_j with $j \in J$ then by 3.2 it could be represented by a chain from a_j to an $a_{j'}'$, $j' \in J$ and thus it would not be right-divisible by $a_{j'}'$ in contradiction to its definition. Hence $[a_{j_1}, \cdots, a_{j_k}]_r$ is divisible by $[a_{j_1}, \cdots, a_{j_k}]_l$. Analogously one shows that $[a_{j_1}, \cdots, a_{j_k}]_l$ is divisible by $[a_{j_1}, \cdots, a_{j_k}]_r$ and hence both these elements of G^+ are equivalent to one another.

[1] For the sake of simplicity we call the images of letters of F^+ in G^+ also letters, and we also denote them as such.

(ii) The assertion (ii) follows trivially from (1) and 4.3. □

5.2. Let M be a certain Coxeter-matrix over I, and G^+ the corresponding Artin-semigroup. If $J \subset I$ is an arbitrary subset, then we denote by G_J^+ the subsemigroup of G^+ which is generated by the letters $a_j,\ j \in J$. Of course, G_J^+ is canonically isomorphic to $G_{M_J}^+$, where M_J is the Coxeter-matrix over J obtained by restriction of M.

Lemma 5.2. *If a fundamental element Δ_J in G^+ exists for $J \subset I$, then there is a uniquely determined involutionary automorphism σ_J of G_J^+ with the following properties:*

(i) *σ_J sends letters to letters, i.e. $\sigma_J(a_j) = a_{\sigma(j)}$ for all $j \in J$. Hence σ is a permutation of J with $\sigma^2 = id$ and $m_{\sigma(i)\sigma(j)} = m_{ij}$.*

(ii) *For all $W \in G_J^+$,*

$$W\Delta_J \doteq \Delta_J \sigma_J(W)\,.$$

Proof. $W\Delta_J$ is left-divisible by Δ_J by the same argument as in the proof of 5.1. So by 2.3 there is a uniquely determined $\sigma_J(W)$ such that (ii) holds. From 2.3 it also follows immediately that σ_J is an automorphism of G_J^+. Since σ_J preserves lengths it takes letters to letters, and hence arises from a permutation σ of J. From $\sigma(a)\Delta_J \doteq \Delta_J \sigma^2(a)$ it follows by application of rev that $\sigma^2(a)\Delta_J \doteq \Delta_J \sigma(a)$. The right hand side is positive equivalent to $a\Delta_J$ and hence from 2.3, $\sigma^2(a) \doteq a$. Thus σ is an involution and clearly σ_J is too. Finally, since for all i, j,

$$< \sigma(a_i)\sigma(a_j) >^{m_{ij}} \doteq < \sigma(a_j)\sigma(a_j) >^{m_{ij}}$$

it follows that $m_{ij} = m_{\sigma(i)\sigma(j)}$. Thus (i) is proved. □

Remark. The converse of 5.2 also holds: let G_J^+ be irreducible, $\sigma : J \longrightarrow J$ a permutation and $\Delta \in G_J^+$ a nontrivial element such that $a\Delta \doteq \Delta\sigma(a)$ for all letters a of J. Then there exists a fundamental element Δ_J.

Proof. It suffices to show that Δ is a common multiple of the letters of J. At least, one letter a from J divides Δ. Hence let $\Delta \doteq a\Delta'$. If b is any letter of J with $m_{ab} > 2$, $ba\Delta \doteq \Delta\sigma(b)\sigma(a) \doteq a\Delta'\sigma(b)\sigma(a)$, so by the reduction lemma 2.1, we have that $a\Delta$ is divisible by $\langle ab \rangle^{m_{ab}-1}$ and thus b is a divisor of Δ. Hence Δ is divisible

by all the letters of J since the Coxeter-graph of M_J is assumed connected. By 4.1 the existence of Δ_J then follows.

5.3. The first part of the following lemma follows immediately from 5.2 (ii).

Lemma 5.3. *Suppose there exists a fundamental element Δ_J. Then for all U, V, $W \in G_J^+$:*

(i) *Δ_J left-divides U exactly when it right-divides U.*

(ii) *If Δ_J divides the product VW, then each letter a_j, for $j \in J$, either right-divides the factor V or left-divides W.*

Proof. (ii) If a_j neither right-divides V nor left-divides W then, by 3.2, one can represent V by a chain with target a_j and W by a chain with source a_j. Thus one can represent VW by a chain [*Ed: a word in the letters of J*] which, by 3.1, is not divisible by its source, and hence neither by Δ_J.

5.4. The following lemma contains an important characterization of fundamental elements.

Lemma 5.4. *If a fundamental element Δ_J exists for $J \subset I$, the following hold:*

(i) *$U \in G_J^+$ is square free if and only if U is a divisor of Δ_J.*

(ii) *The least common multiple of square free elements of G_J^+ is square free.*

Proof. (i) From 3.5 it follows immediately by induction on the number of elements of J that Δ_J is square free; and consequently so are its divisors. The converse is shown by induction on the length of U. Let $U \doteq Va$. By the induction assumption there exists a W with $\Delta_J \doteq VW$. Since a does not right-divide V, it left divides W by 5.3 and hence U is a divisor of Δ_J.

(ii) The assertion (ii) follows trivially from (i). □

5.5. Let M be a Coxeter-matrix over I. The Artin semigroups G_M^+ with fundamental element Δ_I can be described by the type of embedding in the corresponding Artin group G_M. Instead of Δ_I, resp. σ_I, we will write simply Δ, resp. σ, when there is no risk of confusion.

Proposition 5.5. *For a Coxeter-matrix M the following statements are equivalent:*

(i) *There is a fundamental element Δ in G_M^+.*

(ii) *Every finite subset of* G_M^+ *has a least common multiple.*

(iii) *The canonical map* $G_M^+ \longrightarrow G_M$ *is injective, and for each* $A \in G_M$ *there exist* $B, C \in G_M^+$ *with* $A = BC^{-1}$. [2]

(iv) *The canonical map* $G_M^+ \longrightarrow G_M$ *is injective, and for each* $A \in G_M$ *there exist* B, $C \in G_M^+$ *with* $A = BC^{-1}$, *where the image of* C *lies in the centre of* G_M.

Proof. [*Ed: In this proof* G_M^+ *is written* G^+ *for simplicity*]

We will show first of all the equivalence of (i) and (ii), where clearly (ii) trivially implies (i). Let $\Lambda \doteq \Delta$ or $\Lambda \doteq \Delta^2$ according to whether $\sigma = 1$ or not. Then Λ is, by 5.2, a central element in G^+ and for each letter a_i, $i \in I$, there is by 5.1 a Λ_i with $\Lambda = a_i \Lambda_i$. Now, if $A \doteq a_{i_1} \dots a_{i_m}$ is an arbitrary element of G^+ then

$$\Lambda^m \doteq a_{i_m} \Lambda_{i_m} \cdots a_{i_1} \Lambda_{i_1} \doteq A \Lambda_{i_m} \cdots \Lambda_{i_1}.$$

Hence Λ^m is divisible by each element A of G^+ with $L(A) \leq m$. In particular, a finite set of elements always has a common multiple and thus by 4.1 a least common multiple. This proves the equivalence of (i) and (ii).

If (ii), then (iv). Since to all B, $C \in G^+$ there exists a common multiple, and thus B', $C' \in G^+$ with $BC' \doteq CB'$. From this and cancellativity, 2.3, it follows by a general theorem of Öre that G^+ embeds in a group. Thence follows the injectivity of $G^+ \to G$ and also that each element $A \in G$ can be represented in the form $A = C^{-1}B$ or also $B'C^{-1}$ with $B, B', C, C' \in G^+$. That C can moreover be chosen to be central follows from the fact that — as shown above — to every C with $L(C) \leq m$ there exists $D \in G^+$ with $\Lambda^m \doteq CD$ so that, therefore, $C^{-1} = \Lambda^{-m} D = D\Lambda^{-m}$.

[*Ed: As an alternative to applying Öre's condition we provide the following proof of the injectivity of* $G^+ \to G$ *when there exists a fundamental element* Δ.

By (5.2) it is clear that Δ^2 *is a central element in* G^+. *Let* W, W' *be positive words such that* $W = W'$ *in* G. *Then there is some sequence* $W_1, W_2, \dots, W_k$ *of words in the letters of* I *and their inverses such that* $W \equiv W_1 = W_2 = \cdots = W_k \equiv W'$ *where at each step* W_{i+1} *is obtained from* W_i *either by a positive transformation (cf 1.3.) or (so-called trivial) insertion or deletion of a subword* aa^{-1} *or* $a^{-1}a$ *for*

[2] We denote elements of G_M^+ and their images in G_M by the same letters.

some letter a. Note that the number of inverse letters appearing in any word is bounded by k.

Let C denote the central element Δ^2 of G^+. Then we may define positive words V_i for $i = 1, \ldots, k$ such that $V_i = C^k W_i$ as follows. Write $W_i \equiv U a^{-1} U'$ for U a positive word, a a letter. Then $CU \doteq UC$, so if we let C_a denote the unique element of G^+ such that $C_a a \doteq C$, $CW_i = CUa^{-1}U' = UCa^{-1}U' = UCa^{-1}U' = UC_aU'$ where UC_a is positive. Repeating this step for successive inverses in U' yields a positive word V_i' equal in G to $C^r W_i$ for some $r \leq k$. Put $V_i \equiv C^{k-r} V_i'$. Essentially, V_i is obtained from W_i by replacing each occurrence of a^{-1} with the word C_a, and then attaching unused copies of C to the front.

Now we check that $V_i \doteq V_{i+1}$.

If W_{i+1} differs from W_i by a positive transformation, then W_{i+1} is W_i with some positive subword U switched with a positive subword U', and so the same transformation applied to V_i gives the word V_{i+1}, so they are positive equivalent.

If W_{i+1} is obtained from W_i by insertion of aa^{-1} or $a^{-1}a$ Then $V_{i+1} \equiv C^r UC_a aV$ or $C^r UaC_a V$ for positive words U, V, where $V_i \equiv C^{r+1} UV$. By the centrality of C and the fact that $C \doteq aC_a \doteq C_a a$, V_i and V_{i+1} are positive equivalent.

If W_{i+1} is obtained by a trivial deletion, then the proof is identical as above, but with the roles of W_{i+1} and W_i reversed.

Hence we have a sequence of words $V_1, V_2, \ldots, V_k$ such that each is positive equivalent to its predecessor, so that V_1 is positive equivalent to V_k. But $V_1 \equiv C_k W$ and $V_k \equiv C_k W'$ so by cancellativity, W is positive equivalent to W'.

So G^+ embeds in G.]

Assuming (iv), (iii) follows trivially. And from (iii), (ii) follows easily. Since for B, $C \in G^+$ there exist B', $C' \in G^+$ with $C^{-1}B = B'C'^{-1}$, and thus $BC' = CB'$ and consequently $BC' \doteq CB'$ so by 4.1 B and C have a least common multiple. Thus 5.5 is proved. □

5.6. Let QFG_M^+ be the set of square free elements of G_M^+. For the canonical map $QFG_M^+ \longrightarrow \overline{G}_M$ defined by composition of inclusion and the residue class map it follows immediately from Theorem 3 of Tits in [6] that

$$QFG_M^+ \longrightarrow \overline{G}_M \text{ is bijective .}$$

Theorem 5.6. *Let M be a Coxeter-matrix. Then there exists a fundamental element Δ in G_M^+ if and only if $\overline{G}_M$ is finite.*

Proof. By Tits, $\overline{G}_M$ is finite exactly when QFG_M^+ is finite. By 5.4 and 3.5 this is the case if and only if Δ exists. Since, if Δ exists, by 5.4 QFG_M^+ consists of the divisors of Δ. And if Δ does not exist, by 3.5 there exists a sequence of infinitely many distinct square free elements. □

5.7. By the length $l(w)$ of an element w in a Coxeter group $\overline{G}_M$ we mean the minimum of the lengths $L(W)$ of all positive words W which represent w. The image of a positive word W or an element W of G_M^+ in $\overline{G}_M$ we denote by $\overline{W}$. The theorem of Tits already cited immediately implies the following:

The square free elements of G_M^+ are precisely those W with $L(W) = l(\overline{W})$

[*Ed: Proof. If an element is not square free, then it is represented by a word W which contains a square. But this is clearly not a reduced word for the Coxeter element $\overline{W}$, and so $l(\overline{W}) \leq L(W) - 2$ (the square cancels).*

Conversely, suppose that W represents a square free element of G_M^+. By definition of length there is a $V \in G_M^+$ such that $\overline{V} = \overline{W}$ and $L(W) = l(\overline{V}) = l(\overline{W})$. Then by above V is square free. But $\overline{V} = \overline{W}$ and hence by Tits theorem $V \doteq W$ and $L(W) = L(V) = l(\overline{W})$. □]

Proposition 5.7. *Let $\overline{G}_M$ be finite. The following hold for the fundamental element Δ of G_M^+:*

(i) *Δ is the uniquely determined square free element of maximal length in G_M^+.*

(ii) *There exists a uniquely determined element of maximal length in $\overline{G_M}$, namely $\overline{\Delta}$. The fundamental element Δ is represented by the positive words W with $\overline{W} = \overline{\Delta}$ and $L(W) = l(\overline{\Delta})$.*

Proof. (i) By 5.4, the elements of QFG_M^+ are the divisors of Δ. A proper divisor W of Δ clearly has $L(W) < L(\Delta)$. Thus Δ is the unique square free element of maximal length.

(ii) By the theorem of Tits and (i) there is also in $\overline{G}_M$ only one unique element of maximal length, namely $\overline{\Delta}$. A positive word with $\overline{W} = \overline{\Delta}$ and $L(W) = l(\overline{\Delta})$ is according to Tits square-free and it has maximal length, so by (i) it represents Δ. That only such positive words can represent Δ is clear.

5.8. Let $\overline{G}_M$ be a finite Coxeter group and for simplicity let the Coxeter system $(\overline{G}_M, \overline{I})$ be irreducible.

[*Note: Bourbaki defines a Coxeter system* (W, S) *to be a group* W *and a set* S *of elements of order 2 in* W *such that the following holds: For* s, s' *in* S*, let* $m(s, s')$ *be the order of* ss'*. Let* I *be the set of pairs* (s, s') *such that* $m(s, s')$ *is finite. The generating set* S *and relations* $(ss')^{m(s,s')} = 1$ *for* (s, s') *in* I *form a presentation of the group* W*.*

A Coxeter system (W, S) *is irreducible if the associated Coxeter graph* Γ *is connected and non empty.*

Note also that Bourbaki, Groupes et Algèbres de Lie, IV §1 ex 9 gives an example of a group W *and two subsets* S *and* s' *of elements of order 2 such that* (W, S) *and* (W, S') *are non-isomorphic Coxeter systems, one of which is irreducible, the other reducible. Hence the notion of irreducibility depends on* S*, not just on the underlying group* W*. Bourbaki says: when* (W, S) *is a Coxeter system, and also says, by abuse of language, that* W *is a Coxeter group. However one can check that, in the example cited, the two systems do have distinct Artin groups, which may be distinguished by their centres (see §7).*]

The existence of the unique word $\overline{\Delta}$ of maximal length in $\overline{G}$ and its properties are well known (see [1], Bourbaki, Groupes et Algrìbres de Lie, IV, §1, ex. 22; V, §4, ex. 2 and 3; V, §6, ex. 2). For example we know that the length $l(\overline{\Delta})$ is equal to the number of reflections of $\overline{G}$ and thus

$$L(\Delta) \;=\; \frac{nh}{2}$$

where h is the Coxeter number and n the rank, i.e. the cardinality of the generating system I. Explicit representations of $\overline{\Delta}$ by suitable words are also known and from this we now obtain quite simple corresponding expressions for Δ.

Let M be an irreducible Coxeter system of finite type over I. A pair (I', I'') of subsets of I is a decomposition of I if I is the disjoint union of I' and I'' and $m_{ij} \leq 2$ for all $i, j \in I'$ and all $i, j \in I''$. Obviously there are exactly two decompositions of I which are mapped into each other by interchanging I' and I''.

[*Ed: Proof. By Bourbaki, V §4 number 8 corollary to proposition 8, or from the classification of finite Coxeter groups we know that if* (W, S) *is irreducible and*

finite then its graph is a tree. So the statement about decompositions boils down to the following statement about trees: if Γ *is a tree with a finite set* S *of vertices then there exists a unique partition* (S', S'') *(up to interchange of* S' *and* S''*), of* S *into two sets such that no two elements of* S' *and no two elements of* S'' *are joined by an edge.*

We prove this by induction on the number of vertices of Γ*. For a graph on one vertex* a *it is clear that the only suitable partitions are* $(\{a\}, \phi)$ *and* $(\phi, \{a\})$*. Now let* Γ *be an arbitrary tree with a finite set of vertices and let* a *be a terminal vertex. Then applying the assumption to the subgraph of* Γ *whose vertices are those vertices* $n \neq a$ *of* Γ *we see that there exists a unique partition* (S'_1, S''_l) *(up to interchange of* S'_1, S''_1*) of* $S \setminus \{a\}$ *such that no two elements of* S'_1 *and no two elements of* S''_1 *are joined by an edge of* Γ'*. Now, by definition of a tree,* a *is joined to exactly one vertex* b *of* Γ'*. Without loss of generality let* $b \in S'_1$*. Then it is easy to see that* $(S'_1, S''_1 \cup \{a\})$ *is a partition of* S *satisfying the above conditions and that it is unique up to interchanging* S'_1 *and* $S''_1 \cup \{a\}$*.* $\square$]

Definition. Let M be a Coxeter matrix over I and (I', I'') a decomposition of I. The following *products of generators* in G_M^+ are associated to the decomposition:

$$\Pi' \doteqdot \prod_{i \in I'} a_i, \qquad \Pi'' \doteqdot \prod_{i \in I''} a_i, \qquad \Pi \doteqdot \Pi' \Pi''.$$

Lemma 5.8. *Let* M *be a Coxeter-matrix over* I*, irreducible and of finite type. Let* Π', Π'' *and* Π *be the products of generators of* G_M^+ *defined by a decomposition of* I *and let* h *be the Coxeter number. Then:*

$$\begin{aligned} \Delta &\doteqdot \Pi^{h/2} && \text{if } h \text{ is even,} \\ \Delta &\doteqdot \Pi^{h-1/2}\Pi' \doteqdot \Pi''\Pi^{h-1/2} && \text{if } h \text{ is odd,} \\ \Delta^2 &\doteqdot \Pi^h && \text{always.} \end{aligned}$$

Proof. According to Bourbaki, V §6 ex 2 (6) the corresponding equations for $\overline{\Delta}, \overline{\Pi}, \overline{\Pi}', \overline{\Pi}''$ hold. Since, in addition, the elements on the right hand sides of the equations have length $nh/2$ the statement follows from Proposition 5.7 (ii).

Remark. The Coxeter number h is odd only for types A_{2k} and $I_2(2q+1)$. When h is even, it is by no means necessary for $\Delta \doteqdot P^{h/2}$ to hold where P is a product

of the generators in an arbitrary order. In any case, the following result show that this dependence on the order plays a role when Δ is not central in G^+, thus in the irreducible cases of types A_n for $n \geq 2$, D_{2k+1}, E_6 and $I_2(2q+1)$. [*See end of* §7.]

Proposition. *Let $a_1, \cdots, a_n$ be the generating letters for the Artin semigroup G_M^+ of finite type. Then:*

(i) *For the product $P \doteq a_{i_1} \cdots a_{i_n}$ of the generators in an arbitrary order $\Delta^2 \doteq P^h$.*

(ii) *If Δ is central in G_M^+ then in fact for the product P of the generators in an arbitrary order, $\Delta \doteq P^{h/2}$.*

(iii) *If Δ is not central and h is even, there is an ordering of the generators such that, for the product of the generators in this order $\Delta \neq P^{h/2}$.*

Proof. By [1] V §6.1 Lemma 1, all products P of generators in G_M are conjugate to one another. Thus P^h is conjugate to Π^h and $P^{h/2}$ is conjugate to $\Pi^{h/2}$ if h is even. If Δ is central and h is even then $\Delta = \Pi^{h/2}$ is central and hence $P^{h/2} = \Pi^{h/2}$ in G_M and thus $P^{h/2} \doteq \Pi^{h/2} \doteq \Delta$ in G_M^+. Likewise it follows immediately that $P^h \doteq \Pi^h \doteq \Delta^2$ since $\Delta^2 \doteq \Pi^h$ is always central. Hence (i) and (ii) are shown. [*Note: we are using the fact that $G_M^+ \longrightarrow G_M$ is injective here.*]

(iii) Suppose Δ is not central, i.e. $\sigma \neq \mathrm{id}$ and let h be even. If for all products $P \doteq a_{i_1} \cdots a_{i_n}$ we were to have the equation $P^{h/2} \doteq \Delta$ then this also would be true for the product $a_{i_n} P a_{i_n}^{-1}$ which arises from it by cyclic permutation of the factors. Now, if P were such a product with $\sigma(a_{i_n}) \neq a_{i_n}$ then we would have $a_{i_n} P^{h/2} a_{i_n}^{-1} \doteq \Delta$ and thus $a_{i_n} \Delta \doteq \Delta a_{i_n}$ in contradiction to $a_{i_n} \Delta \doteq \Delta \sigma(a_{i_n})$. □

§6. The Word Problem

In this section we solve the word problem first for Artin semigroups of finite type and then for Artin groups of finite type.

6.1. Let M be a Coxeter matrix on I. For each positive word W we define a subset $I(W)$ of I by

$$I(W) \;=\; \{i \in I \;\text{ such that }\; a_i | W\}\ .$$

For $W \doteqdot W'$ it follows naturally that $I(W) = I(W')$.

For each subset J of I for which a fundamental element exists, we choose to represent this by the fundamental word Δ_J as we did in 5.8. [*Ed: Implicitly we have chosen an ordering of the elements of J, and the words Π, Π', Π'' from (5.8) are products of letters in that order.*] Now we can define the normal form for positive words.

Definition. A positive word W is in *normal form* relative to M when

$$W \equiv \Delta_{I_1}\Delta_{I_2}\cdots\Delta_{I_k}$$

where $k \geq 0$ and the I_j are nonempty subsets of I such that, for $j = 1, 2, \ldots, k$, we have

$$I_j \;=\; I(\Delta_{I_j}\Delta_{I_{j+1}}\ldots\Delta_{I_k})\ .$$

Lemma 6.1. *For positive words in normal form we have*

$$\Delta_{I_1}\ldots\Delta_{I_k} \doteqdot \Delta_{J_1}\cdots\Delta_{J_l}$$

exactly when $k = l$ and $I_j = J_j$ for $j = 1, 2, \ldots k$.

Proof. The proof is by induction on the length of the words. For length 0 the statement is trivial.

Let $V \equiv \Delta_{I_1}\cdots\Delta_{I_k}$ and $W \equiv \Delta_{J_1}\cdots\Delta_{J_l}$ be of length less than or equal to λ and assume the statement of the lemma for words of length less than λ. It follows from $V \doteqdot W$ that $I(V) = I(W)$ and thus $I_1 = J_1$. From 2.3 it follows that $\Delta_{I_2}\cdots\Delta_{I_k} \doteqdot \Delta_{J_2}\cdots\Delta_{J_l}$ and hence that $l = k$ and $I_j = J_j$ by the induction assumption. □

6.2. We shall algorithmically rewrite each positive word W into a positive equivalent word $N^+(W)$ which is in normal form.

For the empty word W we define $N^+(W) \equiv W$. For words W of positive length $N^+(W)$ is recursively defined by

$$N^+(W) \equiv \Delta_{I(W)} N^+(W : \Delta_{I(W)}).$$

Lemma 6.2. *(i)* $N^+(W) \doteq W$.

(ii) $N^+(W)$ *is in normal form.*

Proof. (i) By induction on word length one proves that

$$W \doteq \Delta_{I(W)} \cdot (W : \Delta_{I(W)}) \doteq \Delta_{I(W)} N^+(W : \Delta_{I(W)})\,.$$

(ii) This statement is also proved by an easy induction. By the induction assumption $N^+(W : \Delta_{I(W)})$ is in normal form and since, by (i), $I(W) = I(N^+(W))$ it follows that $N^+(W)$ is in normal form.

□

Definition. $N^+(W)$ is the *positive normal form* of W.

6.3 The following theorem solves the word problem for all Artin semigroups such that the positive normal form is computable.

Theorem 6.3. $V \doteq W$ *if and only if* $N^+(V) \equiv N^+(W)$. *In other words: positive words represent exactly the same element of the Artin semigroup* G_M^+ *when they have the same normal form with respect to* M.

Proof. By 6.2 (i) $V \doteq W$ if and only if $N^+(V) \doteq N^+(W)$. By 6.1 and 6.2 (ii) this happens exactly when $N^+(V) \equiv N^+(W)$. □

6.4. Let M be a Coxeter matrix on I and suppose the Artin group G_M is of finite type.

Definition. A word in the free group F_I is in *normal* form if it is equal in the free group to a word

$$\Delta_I^m \Delta_{I_1} \cdots \Delta_{I_k}$$

where m is an integer, k is a natural number, $k \geq 0$, the I_j are subsets of I and the positive word $\Delta_{I_1} \cdots \Delta_{I_k}$ is in normal form. [*Ed: Here it is assumed that* $I_1 \neq I$.]

Lemma 6.4. *For words in normal form we have*

$$\Delta_I^m \Delta_{I_1} \cdots \Delta_{I_k} \;=\; \Delta_I^n \Delta_{J_1} \cdots \Delta_{J_l}$$

if and only if $m = n$ *and* $k = l$ *and* $I_j = J_j$ *for* $j = 1, \cdots, k$.

Proof. Let $m \geq n$. Then by 5.5

$$\Delta_I^{m-n} \Delta_{I_1} \cdots \Delta_{I_k} \doteqdot \Delta_{J_1} \cdots \Delta_{J_l}$$

and the result now follows from 6.1. □

6.5. Now we define a computable normal form $N(W)$ for each word W. By 5.5, for each W there exists an integer m and a positive word W' such that $W = \Delta_I^m W'$. We define the exponent of W to be the maximum $m(W)$ of all such m. The integer $m(W)$ is computable.

There is a positive word W^+ with

$$W \;=\; \Delta_I^{m(W)} W^+ \,.$$

Such a W^+ is computable by the division algorithm 3.6 and the method described in 5.5. We note that with this definition W^+ is defined only up to positive equivalence, but by 6.3 $N^+(W^+)$ is uniquely defined. Thus we can define

$$N(W) \;\equiv\; \Delta_I^{m(W)} N^+(W^+) \,.$$

Lemma 6.5. *(i)* $N(W) = W$ *in* G_M.

(ii) $N(W)$ *is in normal form.*

Proof. (i) This statement follows trivially from 6.2 (i).

(ii) To prove that (ii) is satisfied one observes that by 5.2 and 6.2 (ii) one need only show that $I(N^+(W^+)) \neq I$. This is clear from the maximality of $m(W)$. □

Definition. $N(W)$ is the *normal form* of W.

6.6. The following theorem solves the word problem for Artin groups of finite type.

Theorem 6.6. *In an Artin group of finite type two words* V *and* W *represent the same element precisely when their normal forms are such that* $N(V) \equiv N(W)$.

Proof. The theorem follows trivially from 6.4 and 6.5.

§7. The Centre

In this section we determine the centre of all the Artin semigroups and the centre of the Artin groups of finite type.

7.1. Let M be a Coxeter matrix over I and $I = \cup_\nu I_\nu$ the expression of I as a disjoint union corresponding to the decomposition of the Coxeter graph Γ_M into connected components. If M_ν is the restriction of M to a Coxeter matrix over I_ν, then G_M^+ (resp. G_M) is isomorphic to the direct sum of the $G_{M_\nu}^+$ (resp. G_{M_ν}), and the centre of each direct sum is isomorphic to the direct sum of the centres of the summands. It suffices therefore to restrict our attention to the case where M is irreducible, that is where Γ_M is connected. In what follows there shall arise the two distinct cases of whether M is of finite type, that is $\overline{G}_M$ is finite, or not.

Theorem 7.1. *Let M be an irreducible Coxeter matrix. Then we have:*

(i) *If M is of infinite type, the centre of the Artin semigroup G_M^+ is trivial.*

(ii) *If M is of finite type, the centre of G_M^+ is an infinite cyclic semigroup. It is generated by the fundamental element Δ, if the associated involution σ is trivial, and otherwise by Δ^2.*

Proof. An element Z in a semigroup (resp. group) with generators a_i, $i \in I$, shall be called *quasicentral* when there is, for each $i \in I$, a $j \in I$ such that $a_i Z = Z a_j$. The quasicentral elements form a semigroup (resp. group), the *quasicentre*, in which the centre is naturally embedded.

Now suppose that Z is a non-trivial element of the quasicentre of G_M^+, and a a letter which divides Z. Then for each letter b with $m_{ab} > 2$, it is true that $baZ \doteq Zb'a' \doteq a(Z:a)b'a'$ for appropriate letters a', b'. Hence, by 2.1, baZ is divisible by $\langle ba \rangle^{m_{ab}}$, and Z is therefore divisible by b. It follows by connectedness of Γ_M that Z is divisible by every letter, and hence by 4.1 that there exists a fundamental element Δ and it divides Z. By 5.2, $(Z:\Delta)$ is also quasicentral, and it has strictly smaller length than Z. By induction on the length, there exists a natural number r such that $Z \doteq \Delta^r$. This show that the quasicentre of G_M^+ is trivial for the infinite type, and for the finite type is infinite cyclic, generated by Δ. Thus we have proven (i) and part of (ii). The rest follows easily from 5.2, as $\sigma = id$ exactly when Δ is central, and Δ^2 is always central since $\sigma^2 = id$. □

7.2. From 7.1 we obtain the following description of the centres of the Artin groups of finite type.

Theorem 7.2. *Let M be an irreducible Coxeter matrix of finite type over I. Then the centre of the Artin group G_M is infinite cyclic. It is generated by the fundamental element Δ when the associated involution σ is the identity on I, and otherwise by Δ^2.*

For the generating element of the centre we have $\Delta = \Pi^{h/2}$, resp. $\Delta^2 = \Pi^h$, where h is the Coxeter number and Π is the product of the generating letters of G_M in any particular order.

Proof. Let $Z = \Delta^{m(z)} Z^+$ be quasicentral. As Δ is quasicentral, then Z^+ is also quasicentral in G_M, hence also in G_M^+. Therefore, by 7.1, the element Z^+ is trivial, and the quasicentre of G_M is infinite cyclic and generated by Δ. The rest of the argument follows from 5.2, 5.5 and 5.8. □

By explicitly calculating each case under the classification into types A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2, H_3, H_4 and $I_2(p)$ the following may be shown, either by 5.8 or by well-known results about the longest element in $\overline{G}_M$ (the Coxeter group).

Corollary. *In the irreducible case the involution σ is non-trivial only for the following types: A_n for $n \geq 2$, D_{2k+1}, E_6 and $I_2(2q+1)$.*

§8. The Conjugation Problem

In this section we solve the conjugation problem for all Artin groups G_M of finite type.

Two words V and W are called *conjugate* when there exists a word A such that $V = A^{-1}WA$ and we denote this by $V \sim W$. The conjugation problem consists of giving an algorithm for deciding whether any two given words are conjugate. In our case this problem can easily be reduced to the simpler problem of checking whether any two positive words are conjugate. Here we give a method with which one can calculate, for every positive word W, the finite set of all positive words which are conjugate to W. With this the conjugation problem is clearly solved.

8.1 When two positive words V and W are conjugate, there exists a word A such that $AV = WA$. Since by 5.5 there exist a positive word B and a central word C such that $A = BC^{-1}$, then also $BV \doteq WB$. This proves the following lemma.

Lemma 8.1. *Positive words V and W are conjugate precisely when there is a positive word A such that*

$$AV \doteq WA$$

8.2. Every positive word is positive equivalent to the product of square free words. This approaches the goal of creating the positive word $A^{-1}WA$ conjugate to the positive word W, in which one conjugates successively by the square-free factors of A, and in such a manner that one always obtains positive words. By considering 8.1 one arrives at the following construction.

For every finite set X of positive words define the set X' of positive words by

$$X' = \{V \mid AV \doteq WA \text{ with } W \in X \text{ and } A \text{ square free}\}.$$

Because this set is finite, one can iterate the construction and obtain the sets

$$X^{(k)} = (X^{(k-1)})'.$$

The sets $X^{(k)}$ of positive words are calculable. Since by 5.4, for G_M of finite type there are only finitely many square free words A, namely divisors of the fundamental word Δ, and these are calculable using the division algorithm. Furthermore the division algorithm decides for which square free words A the word WA is left divisible, and the division algorithm 3.6 gives us the quotient $(W \cdot A) : A$. Finally, by the solution to the word problem in 6.3, all positive words V such that $V \doteq (WA) : A$ are calculable, that is, all V such that $AV \doteq WA$. Hence X' is calculable, and so too are $X^{(k)}$.

Let $l(X)$ be the maximum of the lengths of words in X. Then it is clear that $l(X^{(k)}) = l(X)$. [*Ed: Clearly $X^{(i)} \subseteq X^{(i+1)}$, by putting $A \equiv 1$, and for $V \in X^{(i+1)}$, $l(V) = l(W)$ for some $W \in X^{(i)}$.*] If we let $k(l)$ be the number of positive words of length $\leq l$ then $X^{(k)}$ has at most $k(l(X))$ elements. Because $X^{(k)} \subseteq X^{(k+1)}$, then eventually, for $k = k(l(X))$, $X^{(k)} = X^{(k+1)}$. [*Ed: Note that once $X^{(i)} = X^{(i+1)}$ then $X^{(i)} = X^{(j)}$ for all $j > i$.*] Hence

$$X^{(k(l(X)))} = \cup_k X^{(k)}\,.$$

Definition. $X^{\sim} = X^{(k(l(X)))}$.

So $X^{\sim}$ is the smallest set of positive words containing both X and, for every element $W \in X^{\sim}$, all other positive words V of the form $V = A^{-1}WA$ for some square free word A. The set $X^{\sim}$ is calculable.

Lemma 8.2. *Let X be a finite set of positive words. Then the finite set $X^{\sim}$ is calculable and*

$$X^{\sim} \;=\; \{V \mid V \sim W \;\; \textit{with} \;\; W \in X\}$$

Proof. By 8.1 it suffices to show, by induction on the length of A, that for positive words V and A with $AV \doteq WA$ for some $W \in X$, that V is also an element of $X^{\sim}$. [*Ed: It is clear that $X^{\sim} \subseteq \{V \mid V \sim W \;\; \textit{with} \;\; W \in X\}$. One must establish the reverse inclusion.*]

Let $A \doteq BC$ where B is a square free divisor of A of maximal length. We claim that B is a left divisor of WB. When we have proved this we are finished because then $WB \doteq BU$ with $U \in X^{\sim}$ and $BCV \doteq WBC \doteq BUC$, so $CV \doteq UC$ and by induction hypothesis $V \in (X^{\sim})^{\sim} = X^{\sim}$.

To prove the left divisibility of WB by B:

For B square free, by 5.1 and 5.4 there exists a positive word D with $DB \doteq \Delta$. Then $DWBC \doteq DBCV \doteq \Delta CV$, so that $DWBC$ is divisible by Δ. We claim that indeed DWB is divisible on the right by every letter a and thus by Δ. Otherwise by 5.3 we have that C is left divisible by a and by 3.4 Ba is square free. Both together contradict the maximality of the length of B. So there exists a positive word U with $DWB \doteq \Delta U$, that is with $WB \doteq BU$, which is what was to be shown. □

8.3. The result of the previous section contains the solution to the conjugation problem.

Theorem 8.3. *Let G_M be an Artin group of finite type. Let Δ be the fundamental word for G_M. Then the following solves the conjugation problem.*

(i) *Let V and W be arbitrary words. For their exponents take $m(V) \geq m(W)$. Let $V = \Delta^{m(V)}V^+$ and $W = \Delta^{m(W)}W^+$ with V^+ and W^+ positive words.*

Then V and W are conjugate when

$$W^+ \sim \Delta^{m(V)-m(W)}V^+, \quad \textit{if } \Delta \textit{ is central or } m(W) \textit{ even,}$$
$$\Delta W^+ \sim \Delta^{m(V)-m(W)+1}V^+, \quad \textit{if } \Delta \textit{ is not central and } m(W) \textit{ odd.}$$

(ii) *If V and W are positive words, then V is conjugate to W when V is an element of the calculable set of positive words $W^\sim$.*

Proof. The statement (i) follows in a trivial way from the centrality of Δ^2, and (ii) follows trivially from 8.2. □

Note added in proof. In the work which was cited in the introduction, Deligne also determined the centre and solved the word and the conjugation problems for the Artin groups of finite type. As we have, he utilises the ideas of Garside but in a geometric formulation which goes back to Tits. We therefore after some consideration deem the publication of our simple purely combinatorial solution defensible.

Bibliography

1. Bourbaki,N.: Groupes et algèbres de Lie, Chapitres 4,5 et 6. Eléments de Mathématique XXXIV. Paris: Hermann 1968.
2. Brieskorn,E.: Die Fundamentalgruppe des Raumes der regulären Orbits einer endlichen komplexen Spiegelungsgruppe. Inventiones math. **12**, 57-61(1971).
3. Brieskorn,E.: Sur les groupes de tresses [d'après V.I.Arnol'd] Séminaire Bourbaki, 24e année, 1971/72, no. 401.
4. Deligne, P.: Les immeubles des groupes de tresses généralisés. Inventiones math. **17**, 273-302(1972).
5. Garside,F.A.: The braid group and other groups. Quart. J. Math. Oxford, 2 Ser. **20**, 235-254(1969).
6. Tits,J.: Le problème des mots dans les groupes de Coxeter. Istituto Nazionale di Alta Matematica, Symposia Mathematica, Vol.1 175-185(1968).