Gröbner-Shirshov Basis for HNN Extensions of Groups and for the Alternating Group
Yuqun Chen *
Chanyan Zhong *
* School of Mathematical Sciences, South China Normal University, Guangzhou, China

Online Publication Date: 01 January 2008

To cite this Article Chen, Yuqun and Zhong, Chanyan(2008)'Gröbner-Shirshov Basis for HNN Extensions of Groups and for the Alternating Group',Communications in Algebra,36:1,94 — 103
To link to this Article: DOI: 10.1080/00927870701665180
URL: http://dx.doi.org/10.1080/00927870701665180
GRÖBNER–SHIRSHOV BASIS FOR HNN EXTENSIONS OF GROUPS AND FOR THE ALTERNATING GROUP

Yuqun Chen and Chanyan Zhong
School of Mathematical Sciences, South China Normal University, Guangzhou, China

In this article, we generalize the Shirshov's Composition Lemma by replacing the monomial order for others. By using Gröbner–Shirshov bases, the normal forms of HNN extension of a group and the alternating group are obtained.

Key Words: Alternating group; Gröbner–Shirshov basis; HNN extension; Normal form.

2000 Mathematics Subject Classification: 20E06; 16S15; 13P10.

1. PRELIMINARIES

It is known that in the Gröbner–Shirshov basis theory, the Shirshov’s Composition–Diamond Lemma (Shirshov, 1962/1999) plays an important role. In the Composition–Diamond Lemma, the order is asked to be monomial. In this article, we generalize the Composition–Diamond Lemma by replacing the monomial order for others. From this result, we show by direct calculations of compositions that the presentation of the HNN extension is a Gröbner–Shirshov basis under an appropriate ordering of group words, in which the order is not monomial order. By the generalized composition lemma, we immediately obtain the Normal Form Theorem for HNN extensions. In fact, this is the first time to find a Gröbner–Shirshov basis by using a nonmonomial order.

HNN extensions of groups were first invented by Higman et al. (1949) and independently by Novikov in 1952 (see Novikov, 1952, 1954, 1955). The Normal Form Theorem for certain HNN extensions of groups was first established by Bokut (see Bokut, 1966/1967, 1967, 1968 and see also Kalorkoti, 1982). In general, the Normal Form Theorem for HNN extensions of groups was proved in the text of Lyndon and Schupp (1977).

For the alternating group \( A_n \), a presentation was given in the monograph of Jacobson (1985, p. 71). However, we still do not know what is the normal form for \( A_n \). In this article, we give the normal form theorem of \( A_n \) with respect to the above presentation.

Received August 30, 2006; Revised December 31, 2006. Communicated by V. A. Artamonov.
Address correspondence to Yuqun Chen, School of Mathematical Sciences, South China Normal University, Guangzhou 510631, China; Fax: +86-20-85216705; E-mail: yqchen@scnu@edu.cn
We first cite some concepts and results from the literature. Let $k$ be a field, $k\langle X \rangle$ the free associative algebra over $k$ generated by $X$ and $X^*$ the free monoid generated by $X$, where the empty word is the identity which is denoted by 1. For a word $w \in X^*$, we denote the length of $w$ by $\deg(w)$. Let $X^*$ be a well-ordered set. Let $f = \sum_{a \in X^*} f(a) a \in k\langle X \rangle$ with the leading word $\bar{f}$, where $f(a) \in k$. We say that $f$ is monic if $\bar{f}$ has coefficient 1. We denote $\text{supp} f = \{a \in X^* \mid f(a) \neq 0\}$.

**Definition 1.1** (Shirshov, 1962/1999, see also Bokut, 1972, 1976; Bokut and Shum 2005). Let $f$ and $g$ be two monic polynomials in $k\langle X \rangle$. Then, there are two kinds of compositions:

1. If $w$ is a word such that $w = \bar{f}b = a\bar{g}$ for some $a, b \in X^*$ with $\deg(\bar{f}) + \deg(\bar{g}) > \deg(w)$, then the polynomial $(f,g)_w = fb - ag$ is called the **intersection composition of $f$ and $g$ with respect to $w$**.

2. If $w = \bar{f} = a\bar{g}b$ for some $a, b \in X^*$, then the polynomial $(f,g)_w = f - agb$ is called the **inclusion composition of $f$ and $g$ with respect to $w$**.

In the above case, the transformation $f \mapsto (f,g)_w = f - agb$ is called the elimination of the leading word (ELW) of $g$ in $f$.

**Definition 1.2** (Bokut, 1972, 1976, cf. Shirshov, 1962/1999). Let $S \subseteq k\langle X \rangle$ and $< \in \mathcal{X}^*$ a well order on $X^*$. Then the composition $(f,g)_w$ is called trivial modulo $S$ if $(f,g)_w = \sum \alpha a_i s_i b_i$, where each $\alpha \in k$, $a_i, b_i \in X^*$ and $a_i s_i b_i < w$. If this is the case, then we write

$$(f,g)_w \equiv 0 \mod(S, w)$$

In general, for $p, q \in k\langle X \rangle$, we write

$p \equiv q \mod(S, w)$

which means that $p - q = \sum \alpha a_i s_i b_i$, where each $\alpha \in k$, $a_i, b_i \in X^*$ and $a_i s_i b_i < w$.

**Definition 1.3** (Bokut, 1972, 1976, cf. Shirshov, 1962/1999). We call the set $S$ with respect to the well order “<” a Gröbner–Shirshov set (basis) in $k\langle X \rangle$ if any composition of polynomials in $S$ is trivial modulo $S$.

**Remark.** Usually, in the definition of the Gröbner–Shirshov basis, the order is asked to be monomial.

A well order “<” on $X^*$ is monomial if it is compatible with the multiplication of words, that is, for $u, v \in X^*$, we have

$u > v \implies w_1 u w_2 > w_1 v w_2$, for all $w_1, w_2 \in X^*$.

The following lemma was proved by Shirshov (1962/1999) for the free Lie algebras (with deg–lex ordering) in 1962 (see also Bokut, 1972). Bokut (1976) specialized the approach of Shirshov to associative algebras (see also Bergman,
1978). For commutative polynomials, this lemma is known as the Buchberger’s Theorem (see Buchberger, 1965), published in Buchberger (1970).

**Lemma 1.4** (Composition–Diamond Lemma). Let \( A = k\langle X \mid S \rangle \) and “\(<\)” a monomial order on \( X^* \). Then the following statements are equivalent:

(i) \( S \) is a Gröbner–Shirshov basis;
(ii) For any \( f \in k\langle X \rangle, \ 0 \neq f \in \text{Ideal}(S) \Rightarrow \tilde{f} = a\tilde{s}b \) for some \( s \in S, \ a, b \in X^* \);
(iii) The set

\[
\text{Red}(S) = \{ u \in X^* \mid u \neq a\tilde{s}b, \ s \in S, \ a, b \in X^* \}
\]

is a linear basis of the algebra \( A \).

If a subset \( S \) of \( k\langle X \rangle \) is not a Gröbner–Shirshov basis, then we can add to \( S \) all nontrivial compositions of polynomials of \( S \), and by continuing this process (maybe infinitely) many times, we eventually obtain a Gröbner–Shirshov basis \( S^{\text{comp}} \). Such a process is called the Shirshov algorithm.

If \( S \) is a set of “semigroup relations” (that is, the polynomials of the form \( u - v \), where \( u, v \in X^* \)), then any nontrivial composition will have the same form. As a result, the set \( S^{\text{comp}} \) also consists of semigroup relations.

Let \( A = \text{sgp}\langle X \mid S \rangle \) be a semigroup presentation. Then \( S \) is a subset of \( k\langle X \rangle \) and hence one can find a Gröbner–Shirshov basis \( S^{\text{comp}} \). The last set does not depend on \( k \), and as mentioned before, it consists of semigroup relations. We will call \( S^{\text{comp}} \) a Gröbner–Shirshov basis of \( A \). This is the same as a Gröbner–Shirshov basis of the semigroup algebra \( kA = k\langle X \mid S \rangle \).

### 2. GENERALIZED COMPOSITION–DIAMOND LEMMA

In this section, we generalize the Composition–Diamond Lemma which is useful in the sequel, by replacing the monomial order for others. The proof of the following lemma is essentially the same as in Bokut et al. (2000). For the sake of convenience, we give the details.

**Lemma 2.1** (Generalized Composition–Diamond Lemma). Let \( S \subseteq k\langle X \rangle, \ A = k\langle X \mid S \rangle \) and “\(<\)” a well order on \( X^* \) such that:

(A) \( \overline{a\tilde{s}b} = a\tilde{s}b \) for any \( a, b \in X^*, \ s \in S \);
(B) for each composition \((s_1, s_2)_w\) in \( S \), there exists a presentation

\[
(s_1, s_2)_w = \sum_i x_i a_i t_i b_i, \ a_i \tilde{t}_i b_i < w, \quad \text{where } t_i \in S, \ a_i, b_i \in X^*, \ x_i \in k
\]

such that for any \( c, d \in X^* \), we have

\[
ca_i \tilde{t}_i b_i d <cwd.
\]
Then, the following statements hold.

(i) $S$ is a Gröbner–Shirshov basis;
(ii) For any $f \in k\langle X \rangle$, $0 \neq f \in \text{Ideal}(S) \Rightarrow \tilde{f} = a\tilde{s}b$ for some $s \in S$, $a, b \in X^*$;
(iii) The set

$$\text{Red}(S) = \{ u \in X^* \mid u \neq a\tilde{s}b, s \in S, a, b \in X^* \}$$

is a linear basis of the algebra $A$.

**Proof.** (i) is clear. Now, we prove (ii). Let

$$f = \sum_{i=1}^{n} \alpha_i a_i s_i b_i, \quad \alpha_i \in k, \quad s_i \in S, \quad a_i, b_i \in X^*.$$  

Assume that

$$w_i = a_i \tilde{s}_i b_i, \quad w_1 = w_2 = \ldots = w_l > w_{l+1} \ldots$$

We will use the induction on $l$ and $w_1$ to prove that $\tilde{f} = a\tilde{s}b$, for some $s \in S$ and $a, b \in X^*$.

If $l = 1$, then by (A), $\tilde{f} = a_i \tilde{s}_i b_1$ and hence the result holds. Assume that $l \geq 2$.

Then

$$f = (\alpha_1 + \alpha_2) a_1 s_1 b_1 + \alpha_2 (a_2 s_2 b_2 - a_1 s_1 b_1) + \cdots$$

For $w_1 = w_2$, there are three cases to consider.

**Case 1.** Assume that $b_1 = b \tilde{s}_2 b_2$ and $a_2 = a_1 \tilde{s}_1 b$. Then we have

$$a_2 s_2 b_2 - a_1 s_1 b_1 = a_1 s_1 b(s_2 - \tilde{s}_2)b_2 - a_1 (s_1 - \tilde{s}_1)b_2 b_2.$$  

For any $t \in \text{supp}(s_2 - \tilde{s}_2)$, by (A), $a_1 s_1 b t b_2 = a_1 \tilde{s}_1 b t b_2 < a_1 \tilde{s}_1 b_2 b_2 = w_1$ and similarly, we have $a_1 t_1 b_2 b_2 < w_1$, for any $t_1 \in \text{supp}(s_1 - \tilde{s}_1)$.

**Case 2.** Assume that $b_1 = b b_2$, $a_2 = a_1 a$, $\tilde{s}_1 b = a \tilde{s}_2$ and $\deg \tilde{s}_1 + \deg \tilde{s}_2 > \deg(a \tilde{s}_1)$. Then

$$a_2 s_2 b_2 - a_1 s_1 b_1 = a_1 (a s_2 - s_1 b) b_2.$$  

By (B), there exist $\beta_j \in k$, $u_j, v_j \in X^*$, $t_j \in S$ such that $u_j \tilde{t}_j v_j < w = \tilde{s}_1 b, s_1 b - a s_2 = \sum_j \beta_j u_j t_j v_j$ and $a_1 u_j t_j v_j b_2 < a_1 \tilde{s}_1 b_2 b_2$. Now, by (A), for any $j$, we have $a_1 u_j t_j v_j b_2 = a_1 u_j t_j v_j b_2 < a_1 \tilde{s}_1 b b_2 = w_1$.

**Case 3.** Assume that $b_2 = b b_1$, $a_2 = a_1 a$, and $\tilde{s}_1 = a \tilde{s}_2 b$. Then

$$a_2 s_2 b_2 - a_1 s_1 b_1 = a_1 (a s_2 b - s_1 b) b_1.$$  

by (A) and (B), there exist $\beta_j \in k$, $u_j, v_j \in X^*$, $t_j \in S$ such that $u_j \tilde{t}_j v_j < w = \tilde{s}_1$, $s_1 - a s_2 b = \sum_j \beta_j u_j t_j v_j$ and for any $j$, we have $a_1 u_j t_j v_j b_1 = a_1 u_j t_j v_j b_1 < a_1 \tilde{s}_1 b_1 = w_1$.

(iii) follows from (ii).
3. NORMAL FORM FOR HNN EXTENSION OF GROUP

In this section, by using the Gröbner–Shirshov basis, we provide a new proof of the normal form theorem of HNN extension of a group.

**Definition 3.1** (Higman et al., 1949; Novikov, 1952, 1954, 1955). Let $G$ be a group and let $A$ and $B$ be subgroups of $G$ with $\phi : A \to B$ an isomorphism. Then the HNN extension of $G$ relative to $A, B$ and $\phi$ is the group

$$ \mathcal{G} = \text{gp}(G, t; t^{-1}at = \phi(a), a \in A). $$

Let $G = G_1 \cup \{1\}$, where $G_1 = G \setminus \{1\} = \{g_\alpha; \alpha \in \Lambda\}$, and let

$$ G/A = \{gA; i \in I\}, \quad G/B = \{h_B; j \in J\}, $$

where $\{g_\alpha; i \in I\}$ and $\{h_B; j \in J\}$ are the coset representatives of $A$ and $B$ in $G$, respectively. We assume that all sets $\Lambda$, $I$, $J$ are well ordered and so are the sets $\{g_\alpha; \alpha \in \Lambda\}$, $\{g_\alpha; i \in I\}$, $\{h_B; j \in J\}$. Then we get a new presentation of the group $\mathcal{G}$ as a semigroup:

$$ \mathcal{G} = \text{sgp}(G_1, t, t^{-1}; gg' = [gg'], gt = g_A t \phi(a_\alpha), gt^{-1} = g_B t^{-1} \phi^{-1}(b_\beta), $$

$$ t^0 = 1, g, g' \in G_1, \varepsilon = \pm 1), $$

where $[gg'] \in G; g = g_A a_\alpha, g' = g'_A a'_\alpha$. Then $g >_A g'$ if and only if $(g_A, a_\alpha)$ is ordered lexicographically (elements $g_A, g'_A$ by $I$, elements $a_\alpha, a'_\alpha$ by (1)). We denote this order by $(G, >_A)$ and call it the A-order. In particular, if $g \neq g_A$, then $g >_A g_A$, for $(g_A, a_\alpha) > (g_A, 1), a_\alpha \neq 1$.

(3) For any $g, g' \in G$, suppose that $g = g_B b_\beta, g' = g'_B b'_\beta$. Then $g >_B g'$ if and only if $(g_B, b_\beta) > (g'_B, b'_\beta)$ is ordered lexicographically (elements $g_B, g'_B$ by $J$, elements $b_\beta, b'_\beta$ by (1)). We denote this order by $(G, >_B)$ and call it the B-order.

Then we order the set $G_1^*$ in three different ways:

(1) Let $1 < g_\alpha < g_\beta < \cdots (\alpha < \beta)$ be a well order of $G$. Then we denote this order by $(G, >)$ and call it an absolute order;

(2) For any $g, g' \in G$, suppose that $g = g_A a_\alpha, g' = g'_A a'_\alpha$. Then $g >_A g'$ if and only if $(g_A, a_\alpha)$ is ordered lexicographically (elements $g_A, g'_A$ by $I$, elements $a_\alpha, a'_\alpha$ by (1)). We denote this order by $(G, >_A)$ and call it the A-order. In particular, if $g \neq g_A$, then $g >_A g_A$, for $(g_A, a_\alpha) > (g_A, 1), a_\alpha \neq 1$.

(3) For any $g, g' \in G$, suppose that $g = g_B b_\beta, g' = g'_B b'_\beta$. Then $g >_B g'$ if and only if $(g_B, b_\beta) > (g'_B, b'_\beta)$ is ordered lexicographically (elements $g_B, g'_B$ by $J$, elements $b_\beta, b'_\beta$ by (1)). We denote this order by $(G, >_B)$ and call it the B-order.

Then we order the set $G_1^*$ in three different ways too:

(1) The absolute order $(G_1^*, \leq)$ is deg–lex order, to compare words $g_1 \cdots g_n (n \geq 0)$ first by length and then lexicographically using absolute order of $G_1$;

(2) The A-order $(G_1^*, \leq_A)$ is deg–lex_A order, firstly to compare words $g_1 \cdots g_n (n \geq 0)$ by length, secondly for $n \geq 1$, $g_1, \ldots, g_{n-1}$ lexicographically by absolute order, and finally the last elements $g_n$ by A-order;

(3) The B-order $(G_1^*, \leq_B)$ is similar to (2) replacing $>_A$ by $>_B$.

Each element in $(G_1 \cup \{t, t^{-1}\})^*$ has a unique form $u = u_1 t^{\varepsilon_1} u_2 t^{\varepsilon_2} \cdots u_k t^{\varepsilon_k} u_{k+1}$, where each $u_i \in G_1^*, \varepsilon_i = \pm 1, k \geq 0$. Suppose that $v = v_1 t^{\delta_1} v_2 \cdots v_l t^{\delta_l} v_{l+1} \in (G_1 \cup \{t, t^{-1}\})^*$.
Then
\[
\text{wt}(u) = (k, t^{e_1}, \ldots, t^{e_k}, u_1, \ldots, u_k, u_{k+1})
\]
\[
\text{wt}(v) = (l, t^{h_1}, \ldots, t^{h_l}, v_1, \ldots, v_l, v_{l+1}).
\]

We define \( u \succ v \) if \( \text{wt}(u) \succ \text{wt}(v) \) lexicographically, using the order of natural numbers and the following orders:

(a) \( t > t^{-1} \);
(b) \( u_i >_A v_i \) if \( e_i = 1, 1 \leq i \leq k \);
(c) \( u_i >_B v_i \) if \( e_i = -1, 1 \leq i \leq k \);
(d) \( u_{k+1} > v_{l+1} \) (\( k = l \)), the absolute order of \( G^*_1 \).

Now, we can easily verify the following lemma.

**Lemma 3.2.** Let the order \( \succ \) on \( \{ G^*_1 \cup \{ t, t^{-1} \} \}^* \) be defined as above. Then the order \( \succ \) is a well order but not monomial, for example, \( g \succ g' \) does not necessarily imply that \( gt \succ g't \).

Equipping with the above notation, we have the following lemma.

**Lemma 3.3.** Let \( X = G^*_1 \cup \{ t, t^{-1} \} \). Suppose that the order \( \succ \) on \( X^* \) is defined as above and \( S = \{ gg' - [gg'], gt - g_A \phi(a_g), gt^{-1} - g_A t^{-1} \phi^{-1}(b_g), t^e t^{-e} - 1 \mid g, g' \in G^*_1, \epsilon = \pm 1 \} \) is as above too. Then \( S \) satisfies conditions (A)–(B) in Lemma 2.1.

**Proof.** For any \( c, d \in X^* \), suppose that \( c = c_1 t^{e_1} \cdots c_n t^{e_n} c_{n+1}, d = d_1 t^{h_1} \cdots d_m t^{h_m} d_{m+1}, c_i, d_j \in G^*_1, e_i, h_j = \pm 1 \). We firstly check (A). Then there are four cases to consider. For example, the second case is for polynomials \( gt - g_A t \phi(a_g) \), \( g \neq g_A \). We need to prove that \( cgtd \succ cg_A t \phi(a_g) d \) for any \( c, d \).

Since
\[
\text{wt}(cgtd) = (n + m + 1, t^{e_1}, \ldots, t^{e_n}, t, t^{h_1}, \ldots, t^{h_m}, c_1, \ldots, c_n, c_{n+1} g, d_1, \ldots, d_m, d_{m+1}),
\]
\[
\text{wt}(cg_A t \phi(a_g) d) = (n + m + 1, t^{e_1}, \ldots, t^{e_n}, t, t^{h_1}, \ldots, t^{h_m}, c_1, \ldots, c_n, c_{n+1} g_A, \phi(a_g) d_1, \ldots, d_m, d_{m+1}),
\]
and \( c_{n+1} g >_A c_{n+1} g_A \) (since \( g >_A g_A \)), we have \( cgtd \succ cg_A t \phi(a_g) d \).

Secondly, we check that (B) holds in Lemma 2.1. By noting that there is no inclusion compositions in \( S \), we need only to consider the cases of intersection compositions. For any \( a, b \in X^*, s_1, s_2 \in S \), suppose that \( a \tilde{s}_1 = \tilde{s}_2 b \) with \( \deg \tilde{s}_1 + \deg \tilde{s}_2 = \deg(a \tilde{s}_1) \). Then, we consider the following cases:

\[ w = gg'g'', \quad gg't \ (g' \neq g''), \quad gg't^{-1} \ (g' \neq g''), \quad gt^e t^{-e}, \quad t^e t^{-e} t^e \ (\epsilon = \pm 1). \]

For example, the second case is as follows.

Let \( \tilde{s}_1 = gg', \tilde{s}_2 = gt \), \( w = gg't \). Then, by noting that \( gg' = [gg']_A a_{[gg']} = [gg']_A a_{[gg']} a_g \) implies that \( [gg']_A = [gg']_A \) and \( a_{[gg']} = a_{[gg']} a_g \), we know that
unique representation respectively.

Theorem 3.4. (The Normal Form Theorem for HNN Extension, Lyndon and Schupp, 1977, Theorem 4.2.1). Let \( \mathcal{G} = \langle G, t; t^{-1} at = \phi(a), a \in A \rangle \) be an HNN extension of group \( G \). If \( \{g_i; i \in I\} \) and \( \{h_j; j \in J\} \) are the sets of representatives of the left cosets of \( A \) and \( B = \phi(A) \) in \( G \), respectively, then every element \( w \) of \( \mathcal{G} \) has a unique representation \( w = g_1t^{e_1} \cdots g_nt^{e_n}g_{n+1} \) \( (n \geq 0, e_i = \pm 1) \), where, for \( 1 \leq l \leq n \), the following conditions are satisfied:

1. If \( e_i = 1 \), then \( g_i \in \{g_i; i \in I\} \);
2. If \( e_i = -1 \), then \( g_i \in \{h_j; j \in J\} \);
(3) There does not exist subwords $t t^{-1}$ and $t^{-1} t$;

(4) $g_{n+1}$ is an arbitrary element of $G$.

**Remark.** In Theorem 4.2.1 of Lyndon and Schupp (1977), the right cosets were considered. We notice that the above Theorem 3.5 is essentially the same as Theorem 4.2.1 in Lyndon and Schupp (1977).

## 4. NORMAL FORM FOR ALTERNATING GROUP

In this section, we first find a Gr"{o}bner–Shirshov basis for the alternating group $A_n$ and then we give the normal form theorem of $A_n$.

Let $S_n$ be the group of the permutations of $\{1, 2, \ldots, n\}$. Then the subset $A_n$ of all even permutations in $S_n$ is a normal subgroup of $S_n$. We call $A_n$ the alternating group of degree $n$. The following presentation of $A_n$ was given in the monograph of Jacobson (1985, p. 71):

$$A_n = gp(x_i (1 \leq i \leq n - 2); x_1^3 = 1, \ (x_{i-1} x_i)^3 = x_i^2 = 1 \ (2 \leq i \leq n - 2),$$

$$\ (x_i x_j)^2 = 1 \ (1 \leq i < j - 1, j \leq n - 2))$$

where $x_i = (12)((i + 1)(i + 2)), \ i = 1, 2, \ldots, n - 2, \ (ij)$ the transposition. Thus, we give a presentation of the group $A_n$ as a semigroup:

$$A_n = sgp(x_1^{-1}, \ x_i (1 \leq i \leq n - 2); \ x_i x_i^{-1} = x_i^{-1} x_i = x_1^3 = 1, \ (x_{i-1} x_i)^3 = x_i^2 = 1$$

$$\ (2 \leq i \leq n - 2), \ (x_i x_j)^2 = 1 \ (1 \leq i < j - 1, j \leq n - 2)).$$

We now order the generators in the following way:

$$x_1^{-1} < x_1 < x_2 < \cdots < x_{n-2}.$$ 

Let $X = \{x_1^{-1}, x_1, x_2, \ldots, x_{n-2}\}$. Then, with the above notations, we can order the words of $X^*$ by the deg–lex order, i.e., compare two words first by their degrees, then order them lexicographically when the degrees are equal. Clearly, this order is a monomial order. Now we define the words

$$x_{ji} = x_j x_{j-1} \cdots x_i,$$

where $j > i > 1$ and $x_{je} = x_j x_{j-1} \cdots x_i e, \ e = \pm 1$.

The proof of the following lemma is straightforward. We omit the detail.

**Lemma 4.1.** For $e = \pm 1$, the following relations hold in the alternating group $A_n$:

(4.1) $x_i^{2e} = x_i^{-e}$;

(4.2) $x_i^2 = 1, \ (i > 1)$;

(4.3) $x_j x_i = x_i x_j, \ (j - 1 > i \geq 2)$;

(4.4) $x_j x_i^2 = x_i^2 x_j, \ (j > 2)$;

(4.5) $x_j x_i = x_{j-1} x_{ji}, \ (j > i \geq 2)$;

(4.6) $x_{ji} x_j = x_{j-1} x_{ji-e}, \ (j > 2)$;
(4.7) $x_2 x_1^e x_2 = x_1^{-e} x_2 x_1^{-e};$
(4.8) $x_1^e x_1^{-e} = 1.$

Now, we can state the normal form theorem for the group $A_n$.

**Theorem 4.2.** Let

$$A_n = gp \langle x_i \mid 1 \leq i \leq n - 2 \rangle; \quad x_1^3 = 1, \quad (x_{i-1} x_i)^3 = x_i^2 = 1 \quad (2 \leq i \leq n - 2),$$

$$(x_i x_j)^2 = 1 \quad (1 \leq i < j - 1, j \leq n - 2)$$

be the alternating group of degree $n$. Let $S = \{x_1^{\pm e} - x_1^{-e}, \quad x_i^2 - 1 \quad (i > 1), \quad x_j x_i - x_i x_j \quad (j - 1 > i \geq 2), \quad x_j x_i^e - x_i^e x_j \quad (j > 2), \quad x_j x_{j-1} x_{j+1} \quad (j > i \geq 2), \quad x_j x_{j-1} x_{j+1} \quad (j > 2), \quad x_2 x_1^e x_2 - x_1^{e} x_2 x_1^{-e}, \quad x_1^2 x_1^{-e} - 1, \quad e = \pm 1\}$, where $x_i = x_j x_{j-1} \cdots x_i, \quad j > i > 1, \quad x_{i-1} = x_i x_{i-1} \cdots x_1^e, \quad e = \pm 1$. Then:

(i) $S$ is a Gröbner–Shirshov basis of the alternating group $A_n$;
(ii) Every element $w$ of $A_n$ has a unique representation $w = x_{i_1} x_{i_2} \cdots x_{n-2} x_{n-1}$, where $x_{i_1} = x_1, \quad (t > 1), \quad x_{i_{t+1}} = 1, \quad x_{i_{t+2}} = x_{i_{t+1}} \cdots x_1^e, \quad 1 \leq j \leq i + 1, \quad 1 \leq i \leq n - 2, \quad e = \pm 1$ (here we use $x_1$ instead of $x_1^{\epsilon}$).

**Proof.** By Lemma 4.1, it is easy to see that every element $w$ of $A_n$ has a representation $w = x_{i_1} x_{i_2} \cdots x_{n-2} x_{n-1}$ (if $i \leq i + 1$). Here $x_{i_1}$ may have 3 possibilities $1, x_1, x_1^{\epsilon}; \quad x_{i_2}$ 4 possibilities, and generally, $x_{i_j} 2 + 2$ possibilities, $1 \leq i \leq n - 2$. So there are $n!2$ words. From this it follows that each representation is unique since $|A_n| = n!/2$. On the other hand, it is clear that $Red(S)$ consists of the same words $w$. Hence, by Composition–Diamond Lemma, $S$ is a Gröbner–Shirshov basis of the alternating group $A_n$. \hfill \Box

**Remark.** According to Bokut and Shiao (2001), normal form in $S_{n-1}$ is $x_{i_1} x_{i_2} \cdots x_{n-2} x_{n-1}$, but here $x_{i_1} = x_1 x_{i-1} \cdots x_1$.

**ACKNOWLEDGMENT**

The authors would like to express their deepest gratitude to Professor L. A. Bokut for his kind guidance, useful discussions, and enthusiastic encouragement during his visit to the South China Normal University.

The research is supported by the National Natural Science Foundation of China (Grant No. 10771077) and the Natural Science Foundation of Guangdong Province (Grant No. 021073; 06025062).

**REFERENCES**


