A Note on the Gröbner-Shirshov Bases over Ad-hoc Extensions of Groups

Eylem G. Karpuz, Firat Ates, Nurten Urlu, A. Sinan Cevik, I. Naci Cangul

Abstract. The main goal of this paper is to obtain (non-commutative) Gröbner-Shirshov bases for monoid presentations of the knit product of cyclic groups and the iterated semidirect product of free groups. Each of the results here will give a new algorithm for getting normal forms of the elements of these groups, and hence a new algorithm for solving the word problem over them.

1. Introduction and Preliminaries

The Gröbner basis theory for commutative algebras was introduced by Buchberger [12] and provides a solution to the reduction problem for commutative algebras. In [6], Bergman generalized the Gröbner basis theory to associative algebras by proving the “Diamond Lemma”. On the other hand, the parallel theory of Gröbner bases was developed for Lie algebras by Shirshov [22]. In [7], Bokut noticed that Shirshov’s method works for also associative algebras. Hence, for this reason, Shirshov’s theory for Lie algebras and their universal enveloping algebras is called the Gröbner-Shirshov basis theory. There are some important studies on this subject related to the groups (see, for instance, [8, 14]). We may finally refer the papers [4, 9, 10, 18, 19] for some other recent studies over Gröbner-Shirshov bases.

Algorithmic problems such as the word, conjugacy and isomorphism problems have played an important role in group theory since the work of M. Dehn in early 1900’s. These problems are called decision problems which ask for a yes or no answer to a specific question. Among these decision problems especially the word problem has been studied widely in groups (see [1]). It is well known that the word problem for finitely presented groups is not solvable in general; that is, given any two words obtained by generators of the group, there may not be an algorithm to decide whether these words represent the same element in this group.
The method of Gröbner-Shirshov bases which is the main theme of this paper gives a new algorithm for getting normal forms of elements of groups, and hence a new algorithm for solving the word problem in these groups. By considering this fact, our aim in this paper is to find Gröbner-Shirshov bases of the knit product of cyclic groups and the iterated semidirect product of free groups.

This paper can be thought as a part of the classification of groups since it will classify solvable groups. In fact this problem has taken so much interest for decades. For instance, in [2], the authors have recently identified the related tensor degree of finite groups. On the other hand, some other part of the classification is based on the usage of automorphism groups (see, for example, [17]) and this would give an advantage of obtaining some new groups in the meaning of products of groups. As a consequence of that the constructions such as direct and semidirect product of groups are quite popular in mathematics. In fact the structure of semidirecct products is well known. Basically, the semidirect product of any two groups is a generalization of the direct product of these two groups which requires at least one of the factors must be normal in the product. In other words, if a group \( G \) is a product \( AB \) of two subgroups with \( A \) normal and \( A \cap B = 1 \), then the conjugation of \( A \) by the elements of \( B \) gives an action of \( B \) on \( A \) by automorphisms. Moreover, if \( A \) and \( B \) are groups not known to be subgroups of another group and if there exists an action of \( B \) on \( A \) by automorphisms, then a group structure, namely the semidirect product, on the set \( A \times B \) can be defined so that the conjugation of \( A \times 1 \) by elements of \( 1 \times B \) mirrors the given action. The next step along this path is the Zappa-Szep product of any two groups, which requires neither of the factors to be normal in the product. Note that the terminology Zappa-Szep product was developed and suggested by G. Zappa in [24]. Moreover, in [20], it is proved that if a Lie algebra is the direct sum of two sub Lie algebras then one can write the bracket in a way that mimics semidirect products on both sides. This construction is called the knit product of graded Lie algebras. Additionally, in [20], the behaviour of homomorphisms with respect to knit products was investigated. The integrated version of a knit product of Lie algebras will be called the knit product of groups which coincides with the Zappa-Szep product (see [23]).

In [16], by considering the iterated semidirect product of finitely generated free groups, the authors introduced a new class of groups and then gave some topological and geometric interpretations. In Section 3, we use the (monoid) presentation of iterated semidirect product of free groups defined in [16].

The organization of this paper is as follows: In Section 2, we find the Gröbner-Shirshov basis of a monoid presentation of the knit product of cyclic groups. At the final section, again by considering the monoid presentation version, we present the Gröbner-Shirshov basis for the iterated semidirect product of free groups. In each of the sections, by obtaining Gröbner-Shirshov basis of corresponding group extensions, we get the normal forms of the elements, and so we get the solvability of the word problem over them.

Throughout this paper, the order of words will be chosen in the given alphabet in the meaning of deg-lex way comparing two words first by their lengths and then lexicographically when the lengths are equal. Additionally, the notation \( (i) \land (j) \) and \( (i) \lor (j) \) will denote the intersection and inclusion compositions of relations \( (i) \) and \( (j) \), respectively. We finally note that all the background and historical material on Gröbner-Shirshov Bases can be found, for instance, in [4, 6–10, 12, 14, 18, 19, 22]. At this stage, we just recall the next lemma (that characterizes the leading terms of elements in the given ideal) which will be needed in the proofs of our main results. In fact this lemma is called the Composition-Diamond Lemma (or Buchberger’s Theorem in some sources) and different versions of the proof of it can be found in [6, 7, 12, 22].

**Lemma 1.1.** Let \( K \) be a field, \( A = K \langle X \mid S \rangle = K(X)/\text{Id}(S) \), where \( \text{Id}(S) \) is the ideal of \( K(X) \) generated by \( S \). Also let the ordering be monomial on \( X^* \). Then the following statements are equivalent:

1. \( S \) is a Gröbner-Shirshov basis.
2. \( f \in \text{Id}(S) \Rightarrow \overline{f} = asb \) for some \( s \in S \) and \( a, b \in X^* \).
3. \( \text{Irr}(S) = \{ u \in X^* \mid u \neq asb, s \in S, a, b \in X^* \} \) is a basis for the algebra \( A = K \langle X \mid S \rangle \).

If a subset \( S \) of \( K(X) \) 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.
2. The Gröbner-Shirshov Basis for the Knit Product of Cyclic Groups

Let $A$ and $K$ be two groups, and let $\alpha, \beta$ be homomorphisms defined by $\beta : A \rightarrow \text{Aut}(K)$, $a \mapsto \beta_a$; $\alpha : K \rightarrow \text{Aut}(A)$, $k \mapsto \alpha_k$, for all $a \in A$ and $k \in K$. Then the knit product $G = A \bowtie_{(\alpha,\beta)} K$ of $K$ by $A$ is defined by the operation $(a_1,k_1)(a_2,k_2) = (a_1\alpha_k(a_2),\beta_a(k_1)k_2)$. It is known that $(1,1)$ is the identity and the inverse of an element $(a,k)$ is $(a,k)^{-1} = (\alpha_k^{-1}(a^{-1}),\beta_a^{-1}(k^{-1}))$ (see [3]). The cases $a \equiv \text{Id}_A$ (or $\beta \equiv \text{Id}_B$) imply $G$ becomes the semidirect product. Now, if $P_A = \langle X;R \rangle$ and $P_K = \langle Y;S \rangle$ are presentations for the groups $A$ and $K$, respectively, under the maps $y \mapsto k_y(y \in Y)$ and $x \mapsto a_x(x \in X)$ with $X \cap Y = \emptyset$, then according to [11], a presentation for $G$ is $P = \langle X,Y;R,S,T \rangle$, where $T$ consist of all pairs $(yx, (y,x)(y'))$, $(y,x) \in K \times A$.

As a special case of this, by [3], let $P_A = \langle x;x^n \rangle$ and $P_K = \langle y;y^m \rangle$ be presentations for the cyclic groups $A$ and $K$, respectively. Suppose that $x^{n-1} = 1_A$ and $y^{m-1} = 1_B$ such that $1 \leq |y| < n$ and $1 \leq |y| < m$. Then $G = A \bowtie_{(\alpha,\beta)} K$ has a presentation $P_G = \langle x,y;x^n,y^m,xy = x'y \rangle$. In fact, the monoid presentation of $G$ is given by

$$\langle x,x^{-1},y,y^{-1},x^n = 1, y^m = 1, yx = x'y, xx^{-1} = x^{-1}x = 1, yy^{-1} = y^{-1}y = 1 \rangle.$$  \hspace{1cm} (1)

To obtain Gröbner-Shirshov basis for $G = A \bowtie_{(\alpha,\beta)} K$, let us order the generators as $x > x^{-1} > y > y^{-1}$. Therefore, we have the following result.

**Theorem 2.1.** A Gröbner-Shirshov basis for the presentation in (1) consists of the relations

$$\begin{align*}
(1) & \ x^n = 1, \quad (2) & \ y^m = 1, \quad (3) & \ x^iy' = yx, \quad (4) & \ xy^{-1} = 1, \\
(5) & \ x^{-1}x = 1, \quad (6) & \ yy^{-1} = 1, \quad (7) & \ y^{-1}y = 1 \quad (1 \leq |y| < n, 1 \leq |y| < m).
\end{align*}$$

**Proof.** We need to prove that all compositions of polynomials (1) – (7) are trivial. To do that, firstly, we consider the intersection compositions of these polynomials. Thus we have the following ambiguities:

$$\begin{align*}
(1) \land (1) : & \quad w = x^{n+1}, \quad (1) \land (3) : w = x^iy', \quad (1) \land (4) : w = x^ix^{-1}, \\
(2) \land (2) : & \quad w = y^{m+1}, \quad (2) \land (6) : w = y^my^{-1}, \quad (3) \land (2) : w = x^iy'^m, \\
(3) \land (6) : & \quad w = x^iy'y^{-1}, \quad (4) \land (5) : w = xx^{-1}x, \quad (5) \land (1) : w = x^{-1}x^n, \\
(5) \land (4) : & \quad w = x^{-1}xx^{-1}, \quad (6) \land (7) : w = yy^{-1}y, \quad (7) \land (6) : w = y^{-1}yy^{-1}.
\end{align*}$$

All these ambiguities are trivial. Let us show some of them.

$$\begin{align*}
(1) \land (3) : w & = x^iy', \\
(f,g)_w & = (x^i - 1)y' - x^{-1}(x^iy' - yx) \\
& = x^iy' - y' - x^{-1}x^iy' + x^{-1}y = x^{-1}yx - y' \equiv yx - xy \equiv 0. \\
(3) \land (6) : w & = x^iy'y^{-1}, \\
(f,g)_w & = (x^i - yx)y^{-1} - x^iy'y^{-1}(yy^{-1} - 1) \\
& = x^iy'y^{-1} - yxy^{-1} - x^iy'y^{-1}yy^{-1} + x^iy'y^{-1} = x^iy'y^{-1} - yxy^{-1} \equiv yx - xy \equiv 0.
\end{align*}$$

It is seen that there are no any other inclusion compositions among relations (1) – (7). This ends up the proof. \hspace{1cm} \square

As a consequence of Lemma 1.1 and Theorem 2.1, we have the following result.

**Corollary 2.2.** Let $C(u)$ be a normal form of a word $u \in A \bowtie_{(\alpha,\beta)} K$. Then $C(u)$ is of the form $y^{p_1}x^{q_1}y^{p_2}x^{q_2} \cdots y^{p_r}x^{q_r}$, where $0 \leq p_i \leq l - 1$ and $0 \leq q_i \leq t - 1$ ($1 \leq i \leq r$). Hence the knit product $G = A \bowtie_{(\alpha,\beta)} K$ with a as in (1) has a solvable word problem.
3. The Gröbner-Shirshov Basis for the Iterated Semidirect Product of Free Groups

Let \( G_1 \) and \( G_2 \) be any two groups, and let \( \alpha \) be a homomorphism \( \alpha : G_1 \to Aut(G_2) \) from \( G_1 \). The semidirect product \( G_2 \rtimes_G \alpha \) of \( G_1 \) and \( G_2 \) with respect to \( \alpha \) is defined on the group operation \((g_2, g_1)(g_2', g_1') = (\alpha(g_1')(g_2)g_2', g_1g_1')\). Of course, this construction can be iterated to finite number of groups. To do that, let \( G_1, G_2, \cdots, G_l \) be groups and \( \alpha_i' : G_i \to Aut(G_{i+1}) \) be homomorphisms satisfying the compatibility conditions

\[
a_i'((g_i)\alpha_i(g_i)) = \alpha_i'((g_i)(\alpha_i(g_i))), \quad \text{for each } i < j < k.
\]

Then, in [16], the authors defined the iterated semidirect product of groups \( G_1, G_2, \cdots, G_l \) with respect to the actions \( \alpha_i' \) as the group

\[
G = G_1 \rtimes_{\alpha_1} G_{l-1} \rtimes_{\alpha_{l-2}} \cdots \rtimes_{\alpha_2} G_2 \rtimes_{\alpha_1} G_1,
\]

where for each \( 1 < q < l \) the partial iteration, \( G^q = G_q \rtimes_{\alpha_q} G^{q-1} \) is defined by the homomorphism \( \alpha_q : G^{q-1} \to Aut(G_q) \). The restriction of each of the homomorphisms to \( G_p \) is \( \alpha_q^p \), where \( 1 \leq p < q \).

**Lemma 3.1.** [16] Let \( F_{d_i} \) (\( 1 \leq q \leq l \)) be free groups presented by \( \langle x_{i,q} (1 \leq i \leq d_i, 1 \leq q \leq l) \rangle \). Then the iterated semidirect product \( G = \sqcup_{q=1}^{l} F_{d_i} \) of free groups \( F_{d_i} \) has the presentation

\[
\mathcal{P}_G = \langle x_{i,q} (1 \leq i \leq d_q, 1 \leq q \leq l) ; x_{i,q}^{-1} x_{i,p} x_{i,p} = \alpha_q^{ip}(x_{i,q}) \quad (p < q) \rangle . \tag{2}
\]

Let us order the generators in presentation (2) as \( F_{d_1} > F_{d_2}^{-1} > F_{d_3} > F_{d_2}^{-1} > \cdots > F_1 > F_{d_1}^{-1} \). In detailed, the ordering among generators as

\[
x_{1,1} > x_{2,1} > \cdots > x_{d_1,1} > x_{1,1}^{-1} > \cdots > x_{d_1,1}^{-1} > x_{1,2} > x_{2,2} > \cdots > x_{d_1,2} > x_{2,2}^{-1} > \cdots > x_{d_2,2} > \cdots > x_{d_1,1} > x_{1,2}^{-1} > x_{2,2}^{-1} > \cdots > x_{d_1,1}^{-1} > x_{1,2}^{-1} > x_{2,2}^{-1} > \cdots > x_{d_2,2}^{-1}.
\]

In Theorem 3.2 below, we choose each homomorphism \( \alpha_q^{ip} (p < q) \) as trivial, and hence we obtain the related Gröbner-Shirshov basis on the base of this case. However, in the following result (see Theorem 3.3), we consider each homomorphism \( \alpha_q^{ip} (p < q) \) as sending each corresponding generator to its inverse, and then obtain the Gröbner-Shirshov basis over this case.

**Theorem 3.2.** Let us consider the free groups \( F_{d_i} = \{ x_{i,q}, x_{2,q}, x_{3,q}, \cdots, x_{d_i,q} \} \), for each \( 1 \leq q \leq l \). Then a Gröbner-Shirshov basis of the monoid presentation of the direct product of groups \( F_{d_i} \) consists of the relations

\[
(1) \ x_{j,p} x_{i,q} = x_{i,q} x_{j,p}, \quad (2) \ x_{f,q}^{-1} x_{f,q}^{-1} = 1, \quad (3) \ x_{f,q}^{-1} x_{f,q}^{-1} = 1,
\]

where \( x_{j,p} \in F_{d_j}, F_{d_j}, \cdots, F_{d_{j-1}}, \ x_{i,q} \in F_{d_i}, F_{d_i}, \cdots, F_{d_{i-1}} \) and \( x_{f,q}^{-1} \in F_{d_f}, \cdots, F_{d_f} \).

**Proof.** As previously, we need to prove that all compositions of polynomials (1) – (3) are trivial. To do that, firstly, consider the intersection compositions of these polynomials. Thus we have the ambiguities

\[
(1) \wedge (1) : \ w = x_{j,p} x_{i,q} x_{i,p}, \quad (1) \wedge (2) : \ w = x_{j,p} x_{i,p} x_{i,q}^{-1}, \quad (2) \wedge (3) : \ w = x_{f,q}^{-1} x_{f,q}^{-1} x_{f,q}^{-1}, \quad (3) \wedge (2) : \ w = x_{f,q}^{-1} x_{f,q}^{-1} x_{f,q}^{-1},
\]

where \( 1 \leq j \leq d_{j-2}, 1 \leq i \leq d_{j-1}, 1 \leq t \leq d_i, 1 \leq i' \leq d_i, 2 \leq p \leq l - 2, 2 \leq q \leq l - 1, 3 \leq x \leq l \) and \( 1 \leq g' \leq l \). All
these ambiguities are trivial. Let us show some of them.

\[(1) \land (1) : w = x_{1,1}x_{2,2}x_{3,3},\]
\[(f, g)_w = (x_{1,1}x_{2,2} - x_{2,2}x_{1,1})x_{3,3} - x_{1,1}(x_{2,2}x_{3,3} - x_{3,3}x_{2,2})\]
\[= x_{1,1}x_{2,2}x_{3,3} - x_{2,2}x_{1,1}x_{3,3} - x_{1,1}x_{2,2}x_{3,3} + x_{1,1}x_{3,3}x_{2,2}\]
\[= x_{1,1}x_{3,3}x_{2,2} - x_{2,2}x_{1,1}x_{3,3}\]
\[\equiv x_{3,3}x_{1,1}x_{2,2} - x_{2,2}x_{3,3}x_{1,1} \equiv x_{3,3}x_{2,2}x_{1,1} - x_{3,3}x_{2,2}x_{1,1} \equiv 0.\]

\[(1) \land (1) : w = x_{d_{a-2},m-2}x_{d_{a-1},m-1}x_{d_{a,m}},\]
\[(f, g)_w = (x_{d_{a-2},m-2}x_{d_{a-1},m-1} - x_{d_{a-2},m-2}x_{d_{a-1},m-1})x_{d_{a-3},m} - x_{d_{a-2},m-1}x_{d_{a-1},m}x_{d_{a-3},m} + x_{d_{a-2},m-2}x_{d_{a-1},m}x_{d_{a-3},m-1}\]
\[= x_{d_{a-2},m-2}x_{d_{a-1},m-1}x_{d_{a-3},m} - x_{d_{a-2},m-1}x_{d_{a-1},m}x_{d_{a-3},m} - x_{d_{a-2},m-2}x_{d_{a-1},m-1}x_{d_{a-3},m}\]
\[\equiv x_{d_{a-2},m}x_{d_{a-1},m-1}x_{d_{a-3},m} - x_{d_{a-2},m-1}x_{d_{a-1},m}x_{d_{a-3},m-2}\]
\[\equiv x_{d_{a,m}}x_{d_{a-1},m-1}x_{d_{a-2},m-2} - x_{d_{a,m}}x_{d_{a-1},m-1}x_{d_{a-2},m-2} \equiv 0.\]

\[(2) \land (3) : w = x_{d_{j,l}}x_{d_{j,l}}x_{d_{j,l}},\]
\[(f, g)_w = (x_{d_{j,l}}x_{d_{j,l}} - 1)x_{d_{j,l}} - x_{d_{j,l}}x_{d_{j,l}}x_{d_{j,l}} - 1\]
\[= x_{d_{j,l}}x_{d_{j,l}}x_{d_{j,l}} - x_{d_{j,l}}x_{d_{j,l}}x_{d_{j,l}}x_{d_{j,l}} + x_{d_{j,l}} \equiv 0.\]

We note that the number of ambiguities of types \((1) \land (1), (1) \land (2)\) \((for i < j), (2) \land (3), (3) \land (1)\) and \((3) \land (2)\) are the combination \(\binom{3}{3}\), the sum \(\sum_{1 \leq i < j \leq l} d_i d_j\), the sum \(d_1 + d_2 + \cdots + d_l\), the sum \(d_1 + d_2 + \cdots + d_{l-1}\) and the sum \(d_1 + d_2 + \cdots + d_l\), respectively. It remains to check including compositions of relations given in \((1) - (3)\).

Hence the result. \(\square\)

**Theorem 3.3.** Let us consider the free groups \(F_{d_i} = \langle x_{1,q}, x_{2,q}, x_{3,q}, \ldots, x_{d_{i}}, q \rangle\), for each \(1 \leq q \leq l\). Then a Gröbner-Shirshov basis of the monoid presentation of the iterated semidirect product of groups \(F_{d_i}\) consists of the following relations:

\[(1) x_{i,j} x_{i,j}^{-1} = x_{i,j} x_{i,j},\]
\[(2) x_{i,q} x_{j,q}^{-1} x_{i,q}^{-1} = 1,\]
\[(3) x_{i,q}^{-1} x_{i,q} = 1,\]

where \(x_{i,j} \in F_{d_{j}}, F_{d_{j}}, \ldots, F_{d_{i+1}}, x_{i,q} \in F_{d_{i}}, F_{d_{i}}, \ldots, F_{d_{i-1}}\) and \(x_{i,q}^{-1} \in F_{d_{i}}, \ldots, F_{d_{l}}\).

**Proof.** Let us show that all compositions of polynomials \((1) - (3)\) are trivial. Thus, let us consider the intersection compositions of them in which the following ambiguities are obtained:

\[(1) \land (3) : w = x_{i,j} x_{i,j}^{-1} x_{i,j}, (2) \land (3) : w = x_{i,q} x_{j,q}^{-1} x_{i,q}^{-1},\]
\[(3) \land (1) : w = x_{i,j}^{-1} x_{i,j} x_{i,j}^{-1}, (3) \land (2) : w = x_{i,q}^{-1} x_{i,q} x_{i,q}^{-1},\]

where \(1 \leq j \leq d_{i-2}, 1 \leq i \leq d_{i-1}, 1 \leq i' \leq d_{p}, 2 \leq p \leq l-2, 2 \leq q \leq l-1\) and \(1 \leq q' \leq l\). Let us show the triviality
just two of them.

\[(1 \land (3)) : w = x_{jp}x_{iq}^{-1}x_{ij},\]

\[(f, g)_w = (x_{jp}x_{iq}^{-1} - x_{ip}x_{jp})x_{ij} - x_{jp}(x_{iq}^{-1}x_{ij} - 1)\]

\[= x_{jp}x_{iq}^{-1}x_{ij} - x_{iq}x_{jp}x_{ij} - x_{jp}x_{iq}^{-1}x_{ij} + x_{ij} = x_{jp} - x_{ij} \iff 0.\]

\[\overset{\text{Corollary 3.4.}}\text{Corollary 3.5. Let } R \text{ be the set of relations given in Theorem 3.2 (and Theorem 3.3). Assume that } C(u) \text{ denotes the normal form of a word } u \in G = \bigwedge_{q=1}^{q} F_{d_q}. \text{ Therefore } C(u) \text{ has a form } W_{F_{d_1}}W_{F_{d_1-1}} \cdots W_{F_{d_q}}W_{F_{d_q}}, \text{ where } W_{F_{d_q}} (1 \leq q \leq l) \text{ is } R\text{-irreducible word.}\]

\ Andrei\, M. \ Alghamdi, \ F. \ G. \ Russo, \ Remarks \ on \ the \ Relative \ Tensor Degree \ of \ Finite \ Groups, \ Filomat \ 28-9 (2014) 1929-1933.

Acknowledgement. The authors would like to thank to the referees for their kind suggestions and valuable comments.

References


