RELATIVE GRÖBNER–SHIRSHOV BASES FOR ALGEBRAS AND GROUPS

L. A. BOKUT AND K. P. SHUM

ABSTRACT. The notion of a relative Gröbner–Shirshov basis for algebras and groups is introduced. The relative composition lemma and relative (composition-)diamond lemma are established. In particular, it is shown that the relative normal forms of certain groups arising from Malcev’s embedding problem are the irreducible normal forms of these groups with respect to their relative Gröbner–Shirshov bases. Other examples of such groups are given by showing that any group \( G \) in a Tits system \((G, B, N, S)\) has a relative \((B-)\)Gröbner–Shirshov basis such that the irreducible words are the Bruhat words of \( G \).

§1. INTRODUCTION

In this paper we define the notion of a relative Gröbner–Shirshov basis and prove the relative Shirshov lemma and a relative composition-diamond lemma for \( \Gamma \)-algebras (\( \Gamma \)-semigroups, \( \Gamma \)-groups) presented by generators and defining relations. Here \( \Gamma \) is a fixed subgroup of the algebra (semigroup, group).

As illustrations, in subsequent sections we consider a number of examples of \( \Gamma \)-semigroups and \( \Gamma \)-groups for a nontrivial \( \Gamma \), calculate relative Gröbner–Shirshov bases for them, and indicate some applications. Here are these examples.

1) Let \( Q_4 \) (see [4]) be the following semigroup:

\[
Q_4 = \langle a_i, b_i, c_i, s_i, t_i \mid 1 \leq i \leq 4, v_0, v_1, a_is_i = c_ivi, b_is_{i+1} = c_iv_{i+1}, b_it_{i+1} = a_it_i, 1 \leq i \leq 4 \rangle,
\]

where \( s_5 = s_1, t_5 = t_1 \).

Let \( R \) be the algebra of formal power series over \( Q_4 \) with coefficients in \( GF(2) \). In other words, the algebra \( R \) is the completion of the semigroup algebra \( GF(2)(Q_4) \) relative to the norm \( 2^{-\deg(f)} \), where \( \deg(f) \) is the natural degree of an element \( f \in GF(2)(Q_4) \).

We fix the presentation of the multiplicative semigroup \( R^* \) of \( R \) that was found in [5]. Then \( R^* \) is a \( \Gamma \)-semigroup, where \( \Gamma \) is the group of units of \( R \) (\( \Gamma \) consists of series with nonzero constant terms).

By definition, to be a \( \Gamma \)-semigroup means that for any element \( q \) among the selected generators for \( R^* \) there are two isomorphic subgroups \( \Gamma_q \) and \( \Gamma_q' \) of \( \Gamma \) with

\[
\gamma q = q \gamma',
\]

where \( \gamma \in \Gamma_q \) and \( \gamma' \in \Gamma_q' \). In our case,

\[
\Gamma_q = \{1 + qA \mid A \in R\}, \quad \Gamma_q' = \{1 + Aq \mid A \in R\}.
\]
It should be noted that the above Γ-semigroup structure of $R^*$ was absolutely crucial in proving that $R^*$ is embeddable into a group (see [6,8,9]), though $R$ is not embeddable into any skew field (see §3). The relative composition-diamond lemma allows us to say that the main technical result of [6,8,9] consists in finding a relative Gröbner–Shirshov basis of the universal group $G(R^*)$ in an explicit form (see §3).

Recall that a universal group $G(P)$ of some semigroup presentation $P$ is the group with the same generators and defining relations as $P$.

2) Let $Q$ be any SNA-semigroup presentation in the sense of [8]. This is a semigroup with defining relations of the form $wh = uf$, where $w,h,u,f$ are generators with some additional properties. One of the crucial properties of $Q$ is that $Q$ has no left (right) cycles of order not exceeding 3 in the sense of Adyan [1]; in particular, no relations of the form $w_1h_1 = uf_1$, $w_1h_2 = w_2f_2$ may be fulfilled in $Q$ simultaneously. This is not the case for the above semigroup $Q_4$.

However, obviously, there are many examples of SNA-semigroups (cf. [8]).

Let $k$ be a field, and let $kQ$ be the algebra of formal power series over $Q$ with coefficients in $k$. Again, the semigroup $kQ^*$ is a Γ-semigroup, where $Γ$ is the group of units of $kQ$. The universal group $G(kQ^*)$ is also a Γ-group. Again, the relative composition-diamond lemma makes it possible to state the main technical result of [8] about SNA-semigroups as follows: a relative Gröbner–Shirshov basis of the universal group $G(kQ^*)$ can be found explicitly (see §3).

As a result, any semigroup $kQ^*$ is embeddable into a group (see [8]).

3) Let $(G, B, N, S)$ be a Tits system (see, e.g., [2]). Then $G$ can be viewed as a Γ-group for $Γ = B$ (see §4). From this point of view, the Bruhat normal form for $G$ is the irreducible normal form for $G$ with respect to a relative Gröbner–Shirshov basis of $G$ (see §5).

It should be noted that in the papers [4,5,6,8,9] cited above (see also [12]) the main goal was to solve the following Malcev embedding problem (cf. [23]) in the class of semigroup algebras:

*Does there exist a semigroup algebra that is not embeddable into any skew field, but with the multiplicative semigroup embeddable into a group?*

In §4 we discuss an analog of the Malcev problem for group algebras, as well as some other problems for them.

---

**§2. Relative composition lemma**

Let $X = \{x_i, i \in I\}$ be a well-ordered set (we transfer this order to $I$, that is, $x_i < x_j$ if $i < j$), and let $Γ$ be a group, the elements of which will be denoted by small greek letters $γ, δ, ...$ with indices. Consider the multiplication table

\[ γδ = μ \]

for $Γ$.

Suppose that for any $x \in X$ two isomorphic subgroups $Γ_x$ and $Γ'_x$ of $Γ$ are fixed, together with an isomorphism

\[ \partial_x : Γ_x \rightarrow Γ'_x. \]

Then we consider $k\langle X; Γ \rangle$, the Γ-free algebra over a field $k$ and the set $X$ (see [14]). In fact, this is an associative algebra with 1, generated by $X$ and $Γ$, with the defining
Thus, this is the length $u, v, a, b$ for any $\Gamma$-words there are several leading monomials of $f$ in $\Gamma$. If $\Gamma = 1$, then this algebra is simply the free algebra over $k$ and $X$.

By definition, the $\Gamma$-words have the form

$$u = \gamma_0 x_1 \cdots x_k \gamma_k,$$

where $k \geq 0$, $\gamma_j \in \Gamma$, $x_i \in X$. We denote the projection of $u$ to $X$ by $[u]$, that is,

$$[u] = x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Also, we define

$$|u| = |[u]| = k;$$

this is the length or the degree of $u$.

It is easily seen that two $\Gamma$-words $u = \gamma_0 x_{i_1} \cdots x_{i_k} \gamma_k$ and $v = \delta_0 x_{j_1} \delta_1 \cdots x_{j_l} \delta_l$ are equal in the $\Gamma$-free algebra $k\langle X; \Gamma \rangle$ if and only if

$$k = l, \quad x_{i_s} = x_{j_s}, \quad 1 \leq s \leq k,$$

and

$$\gamma_0 = \delta_0 \gamma_{x_{i_1}}, \quad \gamma'_1 \gamma_1 = \delta_1 \gamma_{x_{i_2}}, \quad \ldots, \quad \gamma'_{i_k} \gamma_k = \delta_k.$$ 

If $u = u_1 v u_2$ for some $\Gamma$-words, then $v$ is called a $\Gamma$-subword of $u$. The relation $uv = wt$ implies immediately that $u = wa$ and $t = aw$, or $w = ua$ and $v = at$, for some $\Gamma$-word $a$.

We fix a monomial order of $X$-words (5), such that $u < v$ implies $aub < avb$ for any $X$-words $u, v, a, b$, assuming that this order agrees with the order of $X$ (clearly, this is possible). Then, it gives rise to a quasi-order of $\Gamma$-words:

$$u \preceq v \quad \text{if} \quad [u] \leq [v].$$

Thus,

$$u \preceq v \quad \text{implies} \quad aub \preceq avb$$

for any $\Gamma$-words $u, v, a, b$.

Let $f \in k\langle X; \Gamma \rangle$. We assume that $f$ is presented in the form

$$f = \sum \alpha_i u_i,$$

where $\alpha_i \in k$ and the $u_i$ are pairwise distinct $\Gamma$-words.

For the above polynomial $f$, we use $\bar{f}$ to denote a leading monomial of $f$. In general, there are several leading monomials of $f$. In other words, $\bar{f}$ is a maximal $\Gamma$-word occurring in $f$ with a nonzero coefficient. If $\bar{f}$ is unique, then we call $f$ a strong polynomial and $\bar{f}$ the strong leading monomial of $f$.

We say that $f$ is monic strong if $f$ is strong with leading coefficient 1 (i.e., the coefficient of $\bar{f}$ is 1).

Let $S \subset k\langle X; \Gamma \rangle$. Then we call $S$ a monic strong set if any $s \in S$ is a monic strong polynomial. From now on, we use $S$ to denote some set of monic strong polynomials.

The composition of two monic strong polynomials $f, g$ can be defined, in essence, in the same way as in the case where $\Gamma = 1$ (see, e.g., [14]). Namely, we define

$$(f, g)_w = \begin{cases} 
fv - ug & \text{if} \quad w = \bar{f}v = u\bar{g}, \quad |\bar{f}| > |u|, \\
fv - ug & \text{if} \quad w = \bar{f} = u\bar{g},
\end{cases}$$

where $w, v, u$ are $\Gamma$-words. In the second case of (8), the transformation

$$f \mapsto f - ugv$$

in the $\Gamma$-free algebra $k\langle X; \Gamma \rangle$ is given by

$$\bar{f} \mapsto \bar{f} - u\bar{g},$$

where $\bar{f}$ is a leading monomial of $f$.
is called elimination of the leading word (briefly, ELW) of \( g \) in \( f \). In both cases of (8), for any leading word \((f, g)_w\) we have

\[
(f, g)_w < w,
\]

though \((f, g)_w\) may fail to be a strong polynomial.

Let \( f \) be a polynomial (not necessarily strong) such that a leading monomial \( \bar{f} \) of \( f \) is of the form

\[
\bar{f} = u\bar{g}v,
\]

where \( g \) is a monic strong polynomial. Suppose that \( f \) is \( \bar{f} \)-monic, that is, \( \bar{f} \) occurs in \( f \) with coefficient 1. Then the transformation (9) (elimination of the leading word of \( g \) in \( f \)) is applicable. In this case, for the polynomial \( f - ug v \) the number of occurrences of leading words that are quasi-equal to \( \bar{f} \) is smaller than that for \( f \). By using this crucial observation, we obtain the following important property: any sequence of ELW’s of strong monic polynomials is finite; i.e., any sequence

\[
f_1 \rightarrow f_2 \rightarrow \cdots \rightarrow f_n \rightarrow \cdots
\]

is finite, where the leading word of a strong monic polynomial is eliminated at each step.

A composition of the form (8) is said to be trivial relative to \( S \) (more precisely, relative to \( S \) and \( w \)), and we write \((f, g)_w \equiv \mod (S, w)\) if

\[
(f, g)_w = \sum \alpha_i u_i s_i v_i,
\]

where \( \alpha_i \in k, u_i, v_i \) are \( \Gamma \)-words, and

\[
u_i s_i v_i < w.
\]

In particular, if \((f, g)_w\) goes to zero under the action of ELW’s of \( S \), then \((f, g)_w\) is trivial relative to \( S, w \) (see the proof of the “if” part in the next theorem).

A monic strong set \( S \) is called a relative \( \Gamma \)-Gröbner–Shirshov basis (in \( k\langle X; \Gamma \rangle \)) if any composition \((f, g)_w\) of elements \( f, g \) of \( S \) is trivial mod \((S, w)\).

**Remark 2.1.** For the first time, condition (11) (for \( \Gamma = 1 \)) was stated in [10] for the case of Lie algebras; then it was used in [11] for associative algebras, and also in [22] for commutative algebras. In fact, condition (11) is easier to check, as compared to a stronger condition involving ELW’s, though the latter condition is algorithmic (for a recursive \( S \)). For the definition of a (relative) Gröbner–Shirshov basis, any of these two conditions can be used (see below).

With the above concepts at hand, now we can formulate the relative composition lemma. This is an analog (even a generalization) of Shirshov’s composition lemma [25] (see, e.g., [15]). In what follows, \( \text{id}(S) \) stands for the two-sided ideal of the algebra \( k\langle X; \Gamma \rangle \) generated by \( S \).

**Theorem 2.1** (Relative composition lemma). Let \( S \subset k\langle X; \Gamma \rangle \) be a strong monic set of the \( \Gamma \)-free algebra \( k\langle X; \Gamma \rangle \). Then \( S \) is a relative Gröbner–Shirshov basis if and only if for any \( f \in \text{id}(S) \) we have \( f = asb \) for some leading monomial \( f \) of \( f \) and \( s \in S \).

**Proof.** The “only if” part. Let \( S \) be a relative Gröbner–Shirshov basis, and let \( f \in \text{id}(S) \). Then

\[
f = \sum_{i=1}^{n} \alpha_i \alpha_i s_i b_i,
\]

where \( \alpha_i \in k \), the \( \alpha_i \), \( b_i \) are \( \Gamma \)-words, and \( s_i \in S \). It is easily seen that each \( a_i s_i b_i \) is a monic strong polynomial with the leading word \( a_i s_i b_i \). Now, we arrange these leading
words in nonincreasing order by
\[ w = a_1s_1b_1 = a_2s_2b_2 = \cdots = a_k\bar{s}_k \geq a_{k+1}\bar{s}_{k+1} \geq \cdots \geq a_n\bar{s}_n b_n \]
and \( w \neq a_{k+i}s_{k+i}b_{k+i}, \ i \geq 1. \) If \( k = 1, \) then on the right-hand side of (13) there are no \( \Gamma \)-words equal to \( a_1\bar{s}_1b_1. \) This shows that \( f = a_1\bar{s}_1b_1 \) is a leading word of \( f. \) Let \( k \geq 2, \) and let
\[ (14) \quad a_1\bar{s}_1b_1 = a_2\bar{s}_2b_2, \quad [a_1]\bar{s}_1[b_1] = [a_2]\bar{s}_2[b_2]. \]
The following three cases arise.

1) The subwords \([\bar{s}_1]\) and \([\bar{s}_2]\) do not intersect. For example, let
\[ [a_2] = [a_1][s_1][d], \quad [b_1] = [d][s_2][b_2], \]
where \([d]\) is an \( X \)-word. Then (14) implies that
\[ a_2 = a_1\bar{s}_1d, \quad b_1 = d\bar{s}_2b_2 \]
for some \( \Gamma \)-word \( d. \)

Consequently,
\[ \alpha_1a_1\bar{s}_1b_1 + \alpha_2a_2\bar{s}_2b_2 = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(a_1s_1b_1 - a_2s_2b_2) \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(a_1s_1d\bar{s}_2b_2 - a_1\bar{s}_1ds_2b_2) \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(a_1s_1d(\bar{s}_2 - s_2)b_2 + a_1(s_1 - \bar{s}_1))ds_2b_2), \]
where
\[ a_1s_1d(\bar{s}_2 - s_2)b_2 = \sum \gamma_jc_j s_j d_j, \quad c_j s_j d_j < w, \]
and
\[ a_1(s_1 - \bar{s}_1)ds_2b_2 = \sum \delta_jc_j' s_j d_j', \quad c_j' s_j d_j' < w. \]

The above identities allow us to rewrite (13) with a smaller \( k. \)

2) The subwords \([\bar{s}_1]\) and \([\bar{s}_2]\) in (14) have nonempty intersection, but none of them includes the other. For example, let
\[ [\bar{s}_1] = [a][c], \quad [\bar{s}_2] = [c][b], \quad [c] \neq 1. \]
Then (14) implies that
\[ a_2 = a_1a, \quad b_1 = bb_2, \quad \bar{s}_1b = a\bar{s}_2 = w_1, \quad |\bar{s}_1| > |a|, \]
where \( a, b \) are some \( \Gamma \)-words. Indeed,
\[ \bar{s}_1 = a'c', \quad \bar{s}_2 = c'b', \quad a_1a'c'b_1 = a_2c'b_2b_2 \]
for some \( \Gamma \)-words \( a', c', b'. \) Then
\[ a_2 = a_1a' \gamma, \quad \gamma c' = c' \delta, \quad b_1 = \delta b' b_2 \]
for some \( \gamma, \delta \) in \( \Gamma. \) It remains to put \( a = a' \gamma, b = \delta b'. \)

Now we can deduce the formula
\[ \alpha_1a_1s_1b_1 + \alpha_2a_2s_2b_2 = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(a_1s_1b_1 - a_2s_2b_2) \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(a_1s_1bb_2 - a_1as_2b_2) \]
\[ = (\alpha + \alpha_2)a_1s_1b_1 - \alpha_2a_1(s_1b - as_2)b_2 \]
\[ = (\alpha + \alpha_2)a_1s_1b_1 - \alpha_2a_1(s_1, s_2)w_1b_2. \]

Since \( S \) is a Gröbner–Shirshov basis, the composition \((s_1, s_2)w_1\) is trivial \( \text{mod}(S, w_1) \),
and we obtain
\[ a_1(s_1, s_2)w_1b_2 = \sum \gamma_ja_1c_j s_j d_j b_2, \]
where \( s_j \in S \) and
\[ c_j s_j d_j < w_1. \]
Then
\[ a_1c_j\bar{s}_jd_jb_2 \prec a_1w_1b_2 = w. \]

By using the above relations, we can rewrite (13) with a smaller \( k \).

3) One of the subwords \([\bar{s}_1], [\bar{s}_2]\) is a subword of the other.

For example, let
\[ [\bar{s}_1] = [a][\bar{s}_2][b]. \]

Arguing as in the preceding case, we deduce from (14) that
\[ a_2 = a_1a^\prime \gamma, \quad \gamma\bar{s}_2 = \bar{s}_2\beta, \quad \delta b_2 = b'b_1 \]
for some \( \Gamma \)-words \( a^\prime, b' \) and some elements \( \gamma, \delta \in \Gamma \). Putting \( a = a^\prime \gamma, b = \delta^{-1}b' \), we see that
\[ w_1 = \bar{s}_1 = a\bar{s}_2b, \quad a_2 = a_1a, \quad b_2 = bb_1 \]
for some \( \Gamma \)-words \( a, b \). Now, we can deduce the formula
\[ \alpha_1a_1s_1b_1 + \alpha_2a_2s_2b_2 = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(\alpha_1s_1b_1 - a_2s_2b_2) \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2(\alpha_1s_1b_1 - a_1as_2bb_1) \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2a_1(s_1 - as_2b)b_1 \]
\[ = (\alpha_1 + \alpha_2)a_1s_1b_1 - \alpha_2a_2(s_1, s_2)_w, b_1. \]

As before,
\[ a_1(s_1, s_2)_w = 1, \]
where \( s_j \in S \) and
\[ c_j\bar{s}_jd_j \succ w_1, \quad a_1c_j\bar{s}_jd_jb_1 \prec a_1w_1b_1 = w. \]

After this, we can use the above relations to rewrite (13) with a smaller \( k \).

Thus, by induction on \( k \), we can easily complete the proof of the “only if” part.

The “if” part. First, we let \((f, g)_w\) be a composition of elements of \( S \) relative to \( w \). Then
\[ (f, g)_w = \sum \beta_ju_j, \quad u_j \prec w. \]

By using ELW’s of \( S \) in \((f, g)_w\), we can present \((f, g)_w\) in a form \( h \) such that any leading monomial \( h \) of \( h \) contains no subwords \( \bar{s}, s \in S \). Clearly, we have \( h = 0 \), because \( h \in \text{id}(S) \). By the construction of \( h \),
\[ (f, g)_w = \sum \alpha_i\alpha_1s_i, \quad s_i \in S, \quad a_1\bar{s}_ib_i \prec w, \]
i.e., \((f, g)_w = 0 (\text{mod}(S, w))\), and precisely this is required for \( S \) to be a relative Gröbner–Shirshov basis. To clarify the last formula, let \( u_j \) be a leading monomial in the initial presentation of \((f, g)_w, u_j \prec w\). We know that \( u_j < w \). Suppose that \( u_j = a\bar{s}b \) for some \( s \in S \). Then
\[ (f, g)_w - \beta_jasb \]
has a smaller number of leading monomials than \((f, g)_w\), and \( a\bar{s}b \prec w \). After a finite number of such steps, we can obtain the zero polynomial and, with it, the required presentation of \((f, g)_w\). \( \Box \)

Theorem 2.2 implies the following useful proposition. This is an analog (again, a generalization) of the composition-diamond lemma (see, e.g., [15]). We say that a \( \Gamma \)-word \( u \) is irreducible relative to some \( S \) (Irr-word for short) if \( u \not\prec asb, s \in S \). The set of all Irr-words relative to \( S \) is denoted by Irr(\( S \)) (this set was denoted by PBW(\( S \)) in [15]).
Theorem 2.2 (Relative composition-diamond lemma). Let $S \subset k\langle X; \Gamma \rangle$ be a monic strong set. Then $S$ forms a relative Gröbner–Shirshov basis in $k\langle X; \Gamma \rangle$ if and only if $\text{Irr}(S)$ is a basis over $k$ of the algebra $k\langle X; \Gamma | S \rangle$, that is, the $\Gamma$-algebra with generators $X$ and defining relations $S$.

Proof. The “only if” part. Using ELW’s of $S$, we can easily check that every $f \in k\langle X; \Gamma \rangle$ can be presented modulo $\text{id}(S)$ as a linear combination of Irr-words. On the other hand, all the Irr-words are linearly independent modulo $\text{id}(S)$.

The “if” part. Suppose that a composition $(f, g)_w$, where $f, g \in S$, is nontrivial. Then we can use ELW’s of $S$ to present $(f, g)_w$ as a nontrivial linear combination of Irr-words plus some element of $\text{id}(S)$. This contradicts the linear independence of the Irr-words. \hfill $\square$

The following corollary also characterizes the relative Gröbner–Shirshov bases in $k\langle X; \Gamma \rangle$. This statement is well known for the case where $\Gamma = 1$ (it dates back to [25] and [10]).

Corollary 2.3. Let $S \subset k\langle X; \Gamma \rangle$ be a monic strong subset of $k\langle X; \Gamma \rangle$. Then $S$ is a relative Gröbner–Shirshov basis in $k\langle X; \Gamma \rangle$ if and only if any composition of elements of $S$ can be reduced to zero by ELW’s of $S$.

Proof. The “only if” part. By using ELW’s of $S$, we can represent a composition $(f, g)_w$, $f, g \in S$, as a linear combination of Irr-words. By the relative composition lemma, this linear combination must be trivial.

The “if” part. This part is clear: see the text after (12) and the proof of the “if” part of Theorem 2.3. \hfill $\square$

Recall that

$$k\langle X; \Gamma | S \rangle = k\langle X; \Gamma \rangle / \text{id}(S)$$

is the $\Gamma$-algebra generated by $X$ with the set of defining relations $S$. We define the $\Gamma$-semigroups and $\Gamma$-groups in a similar way.

Let $X = \{ x_i, i \in I \}$, $\Gamma$, $\Gamma_x$, $\Gamma_x^\prime$, $x \in X$, be as above. By a $\Gamma$-free semigroup $\text{sgr}(X; \Gamma)$ we mean a semigroup with 1 that is generated by $X$ and $\Gamma$, with the defining relations (1) and (3). The elements of $\text{sgr}(X; \Gamma)$ are the $\Gamma$-words (4) with the equality relation (6).

Let $S = \{(u_j, v_j), j \in J\}$ be a set of pairs of $\Gamma$-words. As usual, we introduce the $\Gamma$-semigroup with defining relations $S$ by

$$P = \text{sgr}(X; \Gamma | u_j = v_j), \ j \in J = \text{sgr}(X; \Gamma | S)$$

(we identify the relation $u = v$ with the pair $(u, v)$). Then the semigroup algebra $k(P)$ is the $\Gamma$-algebra

$$k(P) = \langle X; \Gamma | u_j - v_j = 0, \ j \in J \rangle = \langle X; \Gamma | S \rangle$$

(again we identify the relation $u - v = 0$ with the pair $(u, v)$). Clearly, a relative Gröbner–Shirshov basis of the semigroup algebra (16) does not depend on $k$ and is simply a set of semigroup relations, say $S_{\text{comp}}$. This set $S_{\text{comp}}$ is called a relative Gröbner–Shirshov basis of the semigroup (15).

The $\Gamma$-free group $\text{gr}(X; \Gamma)$ is defined as the group generated by $X$ and $\Gamma$ with the defining relations (1) and (3). In fact, this is the free $\Gamma$-semigroup generated by $X \cup X^{-1}$, with defining relations

$$x_i x_i^{-1} = 1 \quad \text{and} \quad x_i^{-1} x_i = 1, \ \text{where} \ x_i \in X.$$ 

Now, we can easily define the $\Gamma$-group

$$G = \text{gr}(X; \Gamma | S)$$

generated by $X$ with defining relations $S$. The group algebra $k(G)$ has the following presentation:
\begin{equation}
  k(G) = (X \cup X^{-1}; \Gamma \mid x_i x_i^{-1} = 1, x_i^{-1} x_i = 1, S).
\end{equation}

A relative Gröbner–Shirshov basis of the algebra (17) will be called a relative Gröbner–Shirshov basis of $G$ with respect to the set of generators $X$ and the order of the group of $X$-words.

§3. Groups like $G(GF(2)(Q_0))$, $Q_0 = \text{sgr}(w, h, u, f \mid wh = uf)$

We denote by $GF(2)(Q_0)$ the semigroup algebra of $Q_0$ over $GF(2)$. Then $GF(2)(Q_0)$ is the completion of $GF(2)(Q_0)$ up to the algebra of formal infinite power series. It is a domain (see [23]). Let $GF(2)(Q_0)$ denote the multiplicative semigroup of nonzero elements. In [5], a certain representation of this semigroup was found in terms of generators and relations; we fix this presentation of $GF(2)(Q_0)$. We use $G_0 = G(GF(2)(Q_0))$ to denote the universal group of fractions of the semigroup in question (recall that this is the group with the same generators and defining relations as $GF(2)(Q_0)$). An abstract definition of groups “like” $G_0$ was given in [14]. Explicit examples of such groups can be found in [8]. These are groups of the form $G(GF(2)(Q))$, where $Q$ is the so-called SNA-semigroup with defining relations $w_i h_i = u_i f_i$, where $w_i$, $h_i$, $u_i$, $f_i \in X$, under some conditions. Here are some properties of these groups.

1) They are $\Gamma$-groups, where $\Gamma$ is the group of invertible series (units) of $GF(2)(Q)$.

For any $p$ in the fixed system of generators of the semigroup $GF(2)(Q)$, we have
\[ \Gamma_p = \{1 + pA\}, \quad \Gamma'_p = \{1 + Ap\}, \]
where $A \in GF(2)(Q)$.

2) In [8], for any $G = G(GF(2)(Q))$, where $Q$ is an SNA-semigroup, we constructed a rewriting system (semi-Thue-system)
\[ \vdash = \{\Sigma; \Gamma \mid A_j \rightarrow B_j, j \in J\} \]
such that the set of canonical words (that contain no $A_j$, $j \in J$) is a $\Gamma$-basis of $G$ (i.e., any $\Gamma$-word is equal to a unique canonical $\Gamma$-word). Actually, for any $j \in J$ we have
\[ A_j > B_j, \]
in the “tower” order of the $\Sigma$-words.

Now we briefly describe the tower order of words. First, we let $X = Y \cup Z$ be a well-ordered set such that $z > y$ for any $z \in Z$, $y \in Y$. Suppose that the set $Y^*$ of $Y$-words can be well ordered in agreement with the order of all $Y$ and with concatenation of words. Any $X$-word has the form
\[ u = u_0 z_1 u_1 \cdots u_k z_k u_{k+1}, \]
where $k \geq 0$, $u_i \in Y^*$, $s_i \in Z$. We define
\[ \text{wt}(u) = (k, u_0, z_1, u_1, \ldots, u_k, z_k, u_{k+1}) \]
and order all the $\text{wt}$’s lexicographically. Then the tower order of the $X$-words is defined as follows:
\[ u > v \iff \text{wt}(u) > \text{wt}(v). \]
Clearly, this is a well-ordering compatible with concatenation of words.

Property 2) above and Theorem 2.3 (the relative composition-diamond lemma) imply the following statement.
Theorem 3.1. Let

\[ \square = [\Sigma; \Gamma \mid A_i \rightarrow B_j, j \in J] \]

be the rewriting system for \( G = G(GF(2)(Q))\), where \( Q \) is an SNA-semigroup \([8]\). Then the set

\[ S = \{A_j - B_j, j \in J\} \subset GF(2)(\Sigma; \Gamma) \]

is the relative \( \Gamma \)-Gröbner–Shirshov basis of \( G \) with respect to the tower order of words.

Corollary 3.2 \([\mathbf{8}]\). Any semigroup \( GF(2)(Q) \), where \( Q \) is an SNA-semigroup, is embeddable in a group.

Now, we return to SNA-semigroups \( Q \) \([\mathbf{8}]\). A crucial property of \( Q \) is that \( Q \) has no left (right) cycles of order not exceeding 3 in the sense of Adyan \([\mathbf{1}]\); in particular, \( Q \) admits no relations of the form

\[ w_h = u_f, \quad w_1h_1 = u_{f_1}, \quad w_1h_2 = w_{f_2}. \]  

On the contrary, the semigroup \( Q_4 \) (see \([\mathbf{8}, \mathbf{9}]\)) is defined by the same relations as in the Introduction:

\[ a_is_i = c_iv_0, \quad b_is_{i+1} = c_iv_1, \quad b_idx_{i+1} = a_ih_i, \]

where \( 1 \leq i \leq 4 \), \( s_5 = s_1 \), \( t_5 = t_1 \). This system of relations is similar to (18). Consequently, \( Q_4 \) is not an SNA-semigroup.

Here we note that the algebra \( GF(2)(Q_4) \) is not embeddable into a division algebra; it is not even invertible. (A domain \( D \) is said to be invertible if \( D \subset D_1 \), where \( D_1 \) is a domain such that any nonzero element of \( D \) is invertible in \( D_1 \)). Indeed, suppose that \( D = GF(2)(Q_4) \) is contained in \( D_1 \) with the above property. Then in \( D_1 \) we have

\[ v_0^{-1}v_1 = s_i^{-1}a_i^{-1}b_is_{i+1} = t_it_{i+1}s_i^{-1}t_{i+1}s_{i+1}, \quad 1 \leq i \leq 4, \]

whence

\[ (v_0^{-1}v_1)^4 = 1. \]

This means that

\[ (v_0^{-1}v_1 - 1)^4 = 0 \]

in \( D_1 \), and \( v_0^{-1}v_1 = 1 \), so that \( v_0 = v_1 \) in \( D \), a contradiction.

Remark 3.3. The above argument shows that the algebra \( GF(2)(Q_4) \) cannot be embedded in any domain \( D_1 \) with \( Q_4 \subset U(D_1) \), where \( U(D_1) \) is the group of units of \( D_1 \).

Let \( GF(2)(Q_4) \) be the completion of \( GF(2)(Q_4) \). Then the main results of \([\mathbf{6}, \mathbf{8}, \mathbf{9}]\) take the following form.

Main Theorem. The semigroup \( GF(2)(Q_4) \) is embeddable in a group.

For the proof of this theorem, the concept of an “almost” \( \Gamma \)-normal form was constructed for the group \( G_4 = G(GF(2)(Q_4)) \). Here, as before, \( \Gamma \) is the group of units of \( GF(2)(Q_4) \), and

\[ \Gamma_q = \{1 + qA\}, \quad \Gamma'_q = \{1 + A_q\}, \]

where \( q \) is among the fixed generators of \( GF(2)(Q_4) \), and \( A \in GF(2)(Q_4) \). The only problem (“almost”) is that we changed the generator \( v_1 \) of \( G \) to

\[ p = v_0^{-1}v_1. \]

But all arguments of \([\mathbf{8}]\) and \([\mathbf{9}]\) are still valid for \( v_1 \) in place of \( p \). This can be checked directly. We only need to change the presentation of the first \( \Gamma \)-group \( G_1 \) in \([\mathbf{9}]\):

\[ G_1 = \langle v_0; v_1; \Gamma \mid (v_0^{-1}v_1)^4 = 1 \rangle. \]
Thus, the relative Gröbner–Shirshov basis of this new Γ-group $G_1$ consists only of trivial relations and the relations
\begin{align}
&v_0^{-1}v_1v_0^{-1}v_1 = v_1^{-1}v_0v_1^{-1}v_0, \\
v_0v_1^{-1}v_0v_1^{-1} = v_1v_0^{-1}v_1v_0^{-1},
\end{align}
where the left-hand sides are maximal words in the tower order relative to \( \{v_0^{-1}, v_0\} \cup \{v_1^{-1}, v_1\} \), and $v_0^{-1} < v_0 < v_1^{-1} < v_1$.

So, the results of \cite{8} and \cite{9} lead to the following statement.

**Theorem 3.4.** Let
\[ \mathcal{R}_d = [\Sigma, \Gamma | A_j \rightarrow B_j, \ j \in J] \]
be the rewriting (semi-Thue) system constructed for $G(GF(2)(Q_4)^*)$ in \cite{9}, with (20) in place of the transformations $p^4 \rightarrow 1$, $p^{-1} \rightarrow p^3$. Then the relations
\begin{align}
S_4 = \{A_j - B_j, j \in J\}
\end{align}
constitute a relative (Γ)-Gröbner–Shirshov basis for the group $G(GF(2)(Q_4)^*)$ with respect to the tower order of group words.

The main theorem mentioned above follows immediately from Theorem 3.4. On the other hand, we could use the relative composition-diamond lemma (Theorem 2.3) to prove Theorem 3.4 by checking that all possible compositions of the polynomials (21) are trivial. In principle, this approach would be easier than the rather complicated arguments used in \cite{8} and \cite{9}, based on the notion of a "group with a relative standard basis" \cite{7}.

§4. Digression to some open problems for semigroup and group algebras

The following are some classes of domains (i.e., associative rings without divisors of zero, see \cite{13}):
- $D_0$ — all domains;
- $D_1$ — all domains with multiplicative semigroups embeddable into groups;
- $D_2$ — all invertible domains (see §3);
- $D_3$ — all domains embeddable into fields; then
\begin{align}
D_0 \supseteq D_1 \supseteq D_2 \supseteq D_3.
\end{align}

Malcev’s famous example \cite{23} shows that $D_0 \neq D_1$. In particular, it follows that $D_0 \neq D_3$, which solves the problem of Van der Waerden (see \cite{20}).

The example given by Bokut in \cite{6} \cite{8} \cite{9} shows that $D_1 \neq D_2$. The examples given by Bowtell \cite{3} and Klein \cite{20}, together with the result of Gerasimov in \cite{18}, show that $D_2 \neq D_3$ (see also \cite{17}). In fact, these three examples give a complete solution to the Malcev problem.

**Remark 4.1.** A. I. Malcev formulated his problem ($D_1 \neq D_3$) around 1937 (see \cite{24}, p. 5). At the Moscow ICM, 1966, the solution of the Malcev problem was announced by L. A. Bokut, by P. M. Cohn on behalf of his student A. Bowtell, and by S. Amitsur on behalf of his student A. A. Klein. Next year, three papers on this subject were published (see \cite{8} \cite{9} \cite{20}). The paper \cite{6} was submitted by A. I. Malcev to the Russian Academy of Sciences Doklady. A full proof of Bokut’s example appeared in \cite{8} \cite{9}, as has already been mentioned.
In fact, the Malcev and Bokut examples are semigroup algebras. Note that, up to now, the Bokut example is the only known example of a semigroup algebra in $D_1 \setminus D_2$.

To present the situation for semigroup algebras, we let $S_i$ be the intersection of $D_i$ with the class of semigroup algebras, $0 \leq i \leq 3$. Then

$$S_0 \supset S_1 \supset S_2 \supseteq S_3.$$  

However, so far there are no examples of semigroup algebras in $D_2 \setminus D_3$.

Very interesting open problems arise if the domains in (23) are group algebras over a field. Consider the following classes of algebras:

- $K$ — all group algebras of torsion free groups;
- $K_0$ — all group algebras without zero divisors (i.e., domains);
- $K_1$ — all group algebras that are domains with multiplicative semigroups embeddable into groups;
- $K_2$ — all invertible group algebras;
- $K_3$ — all group algebras embeddable into fields.

Then

$$K \supseteq K_0 \supseteq K_1 \supseteq K_2 \supseteq K_3.$$  

The question as to whether $K \neq K_0$ becomes the famous Kaplansky zero-divisor problem \cite{19}.

The question as to whether $K_0 \neq K_3$ is a problem similar to the Van der Waerden problem in the class of group algebras.

The question as to whether $K_1 \neq K_3$ is a problem similar to the Malcev problem in the class of group algebras.

So far, all the proper embedding questions in (24) remain open and difficult problems.

§ 5. Tits systems

In this section, we shall show that the well-known Bruhat decompositions of elements of a group $G$ involved in a Tits system $(G, B, N, S)$ are Irr-words with respect to a relative $(B)$-Gröbner–Shirshov basis of $G$ (see, e.g., \cite{2}). The definition of a Tits system $(G, B, N, S)$ is as follows. First, let $G$ be a group, and let $B$ and $N$ be subgroups of $G$. Suppose $T = B \cap N$ is a normal subgroup of $N$ and $S \subset W = N/B \cap N$.

Then, we present $B$, $N$, and $T$ by the following multiplication tables:

$$B = \langle \{b\} | bb' = b'' \rangle,$$

$$N = \langle \{n\} | nn' = n'' \rangle,$$

$$T = \langle \{t\} = B \cap N | tt' = t'' \rangle.$$  

A system $(G, B, N, S)$ is called a Tits system if the following axioms are fulfilled (see \cite{2}).

(T1) The set $B \cup N$ generates $G$, i.e.,

$$\forall g \in G \quad g = b_0n_1 \cdots b_{k-1}n_kb_k,$$

where $k \leq 0$, $b_i \in B$, $n_i \in N$.

(T2) $S$ generates $W$ and all elements of $S$ are of order 2.

(T3) $(\forall s \in \{s\})$, $sBw \subset BwB \cup BswB$.

(T4) $(\forall s \in \{s\})$ $sBs \not\subset B$.

Since $\{w\}$ is a system of representatives of the cosets $nT$, $n \in N$, we have

$$\forall n \in N \quad n = wt,$$

$$\forall w, w' \in \{w\} \quad ww' = w''t,$$

$$\forall t \in T, w \in \{w\} \quad tw = wt',$$

where $k \leq 0$, $b_i \in B$, $n_i \in N$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
where all \(w\)'s belong to \(\{w\}\) and all \(t\)'s belong to \(T\). The third identity in (27) shows that, for a fixed \(w\), the map

\[
t \rightarrow t'
\]

is an automorphism of \(T\).

By (26) and (27), we have

\[
(\forall g \in G) \quad g = b_0w_1b_1 \cdots w_kb_k,
\]

where \(k \geq 0, b_i \in B, w_i \in \{w\}\). Thus, \(G\) is generated by \(B\) and \(\{w\}\).

Next, axiom (T2) implies that

\[
(\forall w \in \{w\}) \quad w = s_1 \cdots s_n t, \quad s_i \in S, \quad t \in T,
\]

and (31) implies

\[
(\forall s \in \{s\}) \quad s^2 = t, t \in T.
\]

Indeed,

\[
w = s_1t_1s_2t_2s_3t_3 \cdots s_n t_n
\]

\[
= s_1s_2t_1t_2s_3t_3 \cdots s_n t_n
\]

\[
= s_1s_2s_3t_1t_2t_3 \cdots s_n t_n
\]

\[
= \cdots
\]

\[
= s_1 \cdots s_n t.
\]

Axiom (T3) shows that

\[
(\forall s \in \{s\}, b \in B, w \in \{w\}) \quad sbw = b_1s^\delta w b_2,
\]

where \(\delta = 0, 1; b_1, b_2 \in B\).

Moreover,

\[
(\forall w_1, w_2 \in \{w\}, b \in B) \quad w_1bw_2 = b_1w_2b_2,
\]

for some \(b_1, b_2 \in B, w \in \{w\}\). Indeed, by (29), \(w_1\) is representable in the form \(w_1 = s_1, \ldots, s_n t\); next, \(b_0 = tb \in B\), and (31) implies

\[
w_1bw_2 = s_1 \cdots s_n tbw_2 = s_1 \cdots s_n b_0w_2 = b_1 s_1^\delta \cdots s_n^\delta w_2 b_2 = b_1bw_2 = b_1wb_2
\]

where \(\delta_i = 0, 1\).

Finally, (T4) means that

\[
(\forall s \in \{s\} \exists b \in B) \quad sbs \notin B.
\]

The above axioms (more precisely, T1–T3) imply that \(G\) is generated by \(B\) and \(\{w\}\), with the defining relations (25), (27), and (31). For any \(w \in \{w\}\), we define

\[
\Gamma_w = \{ \gamma \in B \mid (\exists \gamma' \in B) \gamma w = w\gamma' \},
\]

\[
\Gamma'_w = \{ \gamma' \in B \mid (\exists \gamma \in B) w\gamma' = \gamma w \}.
\]

Then \(\Gamma_w, \Gamma'_w\) are two isomorphic subgroups of \(B\) that contain \(T\). Also, the isomorphism \(\Gamma_w \rightarrow \Gamma'_w, \gamma \mapsto \gamma'\), extends the automorphism \(T \rightarrow T, t \mapsto t'\).

Now we see that \(G\) is indeed a \(B\)-group with the following defining \(B\)-group relations:

\[
w_1bw_2 = b_1wb_2,
\]

\[
w_1w_2 = wt.
\]

By using (35), we can show that any element \(g\) of \(G\) can be presented in the form \(g = b_1wb_2\).

Clearly, this is the Bruhat decomposition of \(g\). It is well known that a Bruhat decomposition is unique:

\[
(36) \quad b_1wb_2 = b'_1w'b'_2 \Rightarrow w = w'
\]
(see, e.g., [2]). Then we have
\[ \gamma = b_1^{-1}b_1 \in \Gamma_w, \quad \gamma' = b_2b_2^{-1} \in \Gamma'_w. \]
This shows the uniqueness of the Bruhat decomposition (36) in the sense of \( B \)-words.

Now, using Theorem 2.3 (the relative composition-diamond lemma) and assuming that \( \{ w \} \) is well ordered and the set of \( B \)-words on \( \{ w \} \) is ordered in the deg-lex order, we obtain the following result.

**Theorem 5.1.** Let \( (G, B, N, S) \) be a Tits system. The relations
\[ w_1bw_2 = b_1wb_2, \quad w_1w_2 = wt, \]
where \( w, w_i \in \{ w \}, b, b_i \in B, t \in T, \) form a relative \((B)\)-Gröbner–Shirshov basis of \( G \) as a \( B \)-group in the generators \( \{ w \} \). Next, the Irr-words of \( G \) with respect to the above relative Gröbner–Shirshov basis are the Bruhat decompositions (words) of \( G \).

We illustrate Theorem 5.1 by \( G = SL_2(k) \). We follow the notation of [21].

Suppose \( k \) is a field, \( b \in k, a \in k \setminus \{ 0 \} \). Write
\[ u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad t(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \text{and} \quad w = s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \]

Then \( T = \{ t(a), a \in k \setminus \{ 0 \} \} \) is a maximal torus subgroup of \( G \), \( U = \{ u(b), b \in k \} \) is a unipotent subgroup of \( G \),
\[ B = UT = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in k \setminus \{ 0 \}, b \in k \right\} \]
is a Borel subgroup of \( G \), and
\[ N = T \cup wT = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & a^{-1} \\ a & 0 \end{pmatrix}, a \in k \setminus \{ 0 \} \right\}. \]

Clearly, \( N \) is a subgroup of \( G \) and \( N \cap B = T \cap N \) is a normal subgroup of \( N \). Then \( (G, B, N, S = \{ wT \}) \) is a Tits system and the following relations are valid:
\[ wu(a)w = u(a)wt(-a)u(a), \]
\[ w^2 = t(-1), \]
\[ u(b_1)u(b_2) = u(b_1 + b_2), \]
\[ t(a_1)t(a_2) = t(a_1a_2), \]
\[ t(a)u(b) = u(ba^2)t(a), \]
\[ t(a)w = wt(a). \]

Moreover,
\[ sBs = \left\{ \begin{pmatrix} a^{-1} & 0 \\ b & a \end{pmatrix} \right\} \notin B. \]

In this case \( \Gamma_w = \Gamma'_w = \Gamma \). System (37) is a \( B \)-relative Gröbner–Shirshov basis of \( G \) in the deg order of \( B \)-words in \( \{ w \} \). Moreover, in this case, (37) may be regarded as an (absolute) Gröbner–Shirshov basis if \( U \) is well ordered, \( T \) is ordered arbitrarily, and then the words in \( U \cup T \) are ordered by using deg-lex order, assuming \( u(b) > t(a) \). Then, we order the words in \( (U \cup T) \cup \{ w \} \) in the tower order. Now, by direct computation of compositions, it is easy to show that (37) is complete under compositions not only as a \( B \)-set, but in the absolute sense.

Using the usual composition-diamond lemma (\( \Gamma = 1 \)), we obtain the following statement.
Theorem 5.2. Any element of $SL_2(k)$ has a unique presentation in the form
\[ u(b)t(a) \text{ or } u(b)wu(c)t(a). \]

Results such as Theorems 5.1 and 5.2 can be checked not only for $SL_2(k)$, but also for any Chevalley group (see [16, Theorem 8.4.3]), by applying the composition-diamond lemma with $\Gamma = 1$.

REFERENCES


RELATIVE GRÖBNER–SHIRSHOV BASES FOR ALGEBRAS AND GROUPS


Sobolev Institute of Mathematics, Russian Academy of Sciences, Siberian Branch, Novosibirsk, 630090, Russia
E-mail address: bokut@math.nsc.ru

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong, China (SAR)
E-mail address: kpshum@maths.hku.hk

Received 6/AUG/2007
Translated by THE AUTHORS