Journal of Physical Sciences, Vol. 14, 2010, 125-131
ISSN: 0972-8791, www.vidyasagar.ac.in/journal
Published on December 24, 2010

Another Proof of Lyndon's Simple Identity Theorem and a Generalization of Steinberg's Theorem on Roots

Subrata Majumdar[1] and Quazi Selina Sultana

Department of Mathematics, Rajshahi University,
Rajshahi -6205, Bangladesh.
E-mail: prof.subrata.majumdar@gmail.com

Received August 26, 2010; accepted October 20, 2010

ABSTRACT

In this paper we have given a new proof of Lyndon's Simple Identity Theorem - a theorem which is crucial in his determination of the cohomology of a single-relator groups. We have also generalized a theorem of Steinberg on determination of roots of a word in a free group.

MSC (2000): 18G, 20J
Keywords: Free Resolution, Fox Derivatives, Identity Theorem, Roots, Primitives.

1. Introduction

The paper has two parts. In the first part we have given a new proof of Lyndon's Simple Identity Theorem and in the second part we have generalized a theorem of Steinberg about the roots of a word in a free group.

(A) Lyndon [5] proved an important theorem called the Identity Theorem in connection with his complete determination of the cohomology of groups with a single defining relation. Also Huebschmann [3] used this theorem for determination of cohomology of another important class of groups, viz, the small cancellation groups. We state this theorem below.

We recall that a word w in a free group on generators x_i is said to be *reduced* if it does not contain adjacent symbols x_i^{ei} and x_i^{-ei}, and it is said to be *cyclically reduced* if its first and last symbols are not x_i^{ei} and x_i^{-ei}, $e_i = \pm 1$.

Identity Theorem 1 ([5], P.658)

Let F be the free group on generators $x_1,\ldots, x_{n+s}$ (*and possibly other generators* y_i); *let* $r_1,\ldots,r_n$ *be cyclically reduced words in F such that, for each t,* x_t *and* x_{t+s} *are the first and last* (*in order of subscript*) *of the* x_i *that occur in* r_t. *Let each* $r_t = w_i^{f_t}$, *for* f_t *maximal*; *and let R be the smallest normal subgroup of F containing* $r_1,\ldots,r_n$. *If*

$$\prod_{i=1}^{m} s_i^{-1} r_{t_i}^{e_i} s_i = 1 \; (s_i \in F;\ e_i = \pm 1,\ t_i = 1, \ldots, n),$$

then the indices 1,...,*m can be grouped into pairs* (*i*, *j*) *such that* $t_i = t_j$, $e_i = -e_j$, *and, for certain integers* c_i, $s_i \equiv s_j q_{t_i}^{c_i}$ (*mod R*).

The following is an equivalent form of the Identity theorem [5].

Theorem 2 ([5], P.659)

The Identity Theorem is equivalent to the theorem obtained by replacing the condition $\prod_{i=1}^{m}(s_i^{-1} r_i^{e_i} s_i) = 1$ *by the condition that this product lies in the commutator subgroup* [*R*, *R*].

In case of a single relation *r*, the condition that *r* be cyclically reduced is supperflous and we obtain:

Theorem 3 (The Simply Identity Theorem). *Let* $r = q^f$, *for f maximal*, be *a word in the free group F*, *and R the normal closure of r*, *then*

$$\prod_{i=1}^{m}(s_i^{-1} r^{e_i} s_i) = 1$$

implies that the indices can be grouped into pairs (*i*, *j*) *such* that $e_i = -e_j$, *and*, *for certain integers* c_i, $s_i \equiv s_j q^{c_i}$ (*mod R*)

(B) In this paper we have used the derivatives of Fox's free differential calculus [1] to determine the roots of a word $w = x_1^{p_1} \ldots x_k^{p_k}$ where p_i is a prime, thus generalizing Steinberg's Theorem for $k = 2$.

Let *F* be a free group with a basis $\{x_1, x_2, \ldots, x_n\}$. Let $r \in F$. An element *r* in *F* is called *a root of w* (in *F*) if *w* is contained in the normal closure of *r*.
There is another definition of a root [6] which we do not consider here.

The word problem for a single-relator group solved by Magnus [7] is the algorithmic problem of determining whether r is a root of w. However the problem of determining all roots r of a given word w is difficult and has been solved only in simple cases. Steinberg [8] determined all roots of $x^k y^l$.

2. Let F be a field with basis X and R a normal subgroup of F with basis Y and let $G = \frac{F}{R}$ .Let $\mathcal{F}$ and $\mathcal{R}$ be the kernel of the ring homomorphisms $\varepsilon : ZF \to \mathrm{Z}$ and $\pi : ZG \to \mathrm{Z}$, given by $\varepsilon(w) = 1$ and $\pi(g) = 1$, for each $w \in F$, $g \in G$. Then $\mathcal{F}$ and $\mathcal{R}$ are free on $\{x - 1 \mid x \in X\}$ and $\{y - 1 \mid y \in Y\}$ as left ZF- modules. (see Gruenberg [4], p.33)

Theorem 4 ([4], P.37). If F is a free group with basis X and R is a normal subgroup of F with basis Y, Then $\frac{R}{R'}$ is a left ZG-module isomorphic to $\frac{\mathcal{R}}{\mathcal{RF}}$, where $\mathcal{F}$ and $\mathcal{R}$ are defined as above, and $\frac{R}{R'} \to \frac{\mathcal{R}}{\mathcal{RF}}$ given by f(r R') = (r-1) + $\mathcal{RF}$ is a ZG-isomorphism.

We shall now state The Simple Identity Theorem in the form of Theorem 2 and prove it by using Fox's free derivatives and Theorem 4. Since for a free group F with a basis X, $\mathcal{F}$ is a free left ZF- module on $\{(x - 1) \mid x \in X\}$, for each $w \in F$, $w - 1 = \sum_X \frac{\partial w}{\partial x}$ defines $\frac{\partial w}{\partial x}$ uniquely as an element of ZF. $\frac{\partial w}{\partial x}$'s are called Fox's free derivatives (left).

Theorem 5 (The Simply Identity Theorem). *Let* $G = \frac{F}{R}$ *be a torsion free–group with a single defining relation, where F is a free group with the basis X and R is the normal closure of r. If*

$$w = \prod_{i=1}^{n} (s_i^{-1} r^{ei} s_i),\ (s_i \in F,\ e_i = \pm 1)$$

is an element of $[R, R]$, *then the indices i's can be grouped into pairs* (j, k) *such that* $e_j = -e_k$ *and* $s_j \equiv s_k$ *(mod R).*

Proof of Theorem 5. Let $w = \prod_{i=1}^{n} (s_i^{-1} r^{e_i} s_i) \in R'$, then by Theorem 4, $w - 1 \in \mathcal{RF}$. Since

$w - 1 = \sum_{x \in X} \frac{\partial w}{\partial x}(x-1)$ by Lemma 4(ii) of Gruenberg [4], p.33,

Theorem 4 implies that, for each $x \in X$, $\frac{\partial w}{\partial x} \in \mathcal{R}$.

Now

$$\frac{\partial w}{\partial x} = [-s_1^{-1}\frac{\partial s_1}{\partial x} + s_1^{-1} e_1 r^{\frac{e_1-1}{2}} \frac{\partial r}{\partial x} + s_1^{-1} r^{e_1} \frac{\partial s_1}{\partial x}]$$

$$+ \sum_{j=2}^{n} \prod_{k=2}^{j-1} (s_k^{-1} r^{e_k} s_k)\, [-s_j^{-1}\frac{\partial s_j}{\partial x} + s_j^{-1} e_j r^{\frac{e_j-1}{2}} \frac{\partial r}{\partial x} + s_j^{-1} r^{e_j} \frac{\partial s_j}{\partial x}]$$

$$= [s_1^{-1}(r^{e_1}-1)\frac{\partial s_1}{\partial x} + s_1^{-1} e_1 r^{\frac{e_1-1}{2}} \frac{\partial r}{\partial x}]$$

$$+ \sum_{j=2}^{n} \prod_{k=2}^{j-1} (s_k^{-1} r^{e_k} s_k)\, [-s_j^{-1}\frac{\partial s_j}{\partial x} + s_j^{-1} e_j r^{\frac{e_j-1}{2}} \frac{\partial r}{\partial x} + s_j^{-1} r^{e_j} \frac{\partial s_j}{\partial x}] \qquad (1)$$

For each $\varphi \in ZF$, we denote $\pi(\varphi)$ by $\overline{\varphi}$ where, $\pi : ZF \to ZG$ is the ring homomorphism induced by the canonical homomorphism $F \to G$. Since

$$\frac{\partial w}{\partial x} \in \mathcal{R},\ \overline{\frac{\partial w}{\partial x}} = 0.$$

Hence from (1) we obtain $\left(\sum_{i=1}^{n} e_i \overline{s_i}^{-1}\right)\overline{\frac{\partial r}{\partial x}} = 0$, (2), in ZG.

Now $\overline{\frac{\partial r}{\partial x}} \neq 0$; for otherwise, $\frac{\partial w}{\partial x} \in \mathcal{R}$, for each x, and so, $r - 1 \in \mathcal{RF}$, and so by Theorem 5, $r \in R'$, $\frac{R}{R'} = 0$. Since $\frac{R}{R'}$ is a free abelian group with basis $\{(y-1) \mid y \in Y\}$, we thus have a contradiction to the definition of R. By the Theorem of Brown [1] QG and hence ZG has no zero divisors. Therefore from (2) we obtain

$$\left(\sum_{i=1}^{n} e_i \overline{s_i}^{-1}\right) = 0. \qquad (3)$$

Thus the indices are grouped into pairs (j, k) such that $e_j = -e_k$ and $\overline{s_j} \equiv \overline{s_k}$ i.e., $s_j \equiv s_k (\text{mod } R)$.

3. Steinberg [8] proved the following theorem on roots:
Let F be a free group with a basis $x_1, x_2, \ldots, x_n$. Then, for k and l both prime, the only cyclically reduced roots of $x_1^k x_2^l$ other than $x_1^k x_2^l$ itself are $P(x_1, x_2) \neq 1$, where $P(x_1, x_2)$ is a primitive in the free group on x_1 and x_2. Here w in F is called a primitive if it is a member of some basis.

Here we generalize this theorem and prove

Theorem 8. *Let F be a free group with a basis $X = \{x_1, x_2, \ldots, x_k, \ldots\}$, and $w = x_1^{p_1}, \ldots, x_k^{p_k}$, where $p_1, p_2, \ldots, p_k$ are primes. Then the roots of w are w and the primitives in F.*
Proof. Let r be a root of w. Then

$$w = \prod_{i=1}^{u} (s_i^{-1} r^{ei} s_i) \tag{4}$$

Then

$$\frac{\partial w}{\partial x} = [-s_1^{-1}\frac{\partial s_1}{\partial x} + s_1^{-1} e_1 r^{\frac{e_1-1}{2}} \frac{\partial r}{\partial x} + s_1^{-1} r^{e1}\frac{\partial s_1}{\partial x}] + \sum_{j=2}^{u}\prod_{k=2}^{j-1}(s_k^{-1} r^{ek} s_k)[-s_j^{-1}\frac{\partial s_j}{\partial x} + s_j^{-1} e_j r^{\frac{e_j-1}{2}} \frac{\partial r}{\partial x} + s_j^{-1} r^{ej}\frac{\partial s_j}{\partial x}]$$

$$= [s_1^{-1}(r^{e}{}_1^{-1})\frac{\partial s_1}{\partial x} + s_1^{-1} e_1 r^{\frac{e_1-1}{2}}\frac{\partial r}{\partial x}] + \sum_{j=2}^{n}\prod_{k=2}^{j-1}(s_k^{-1} r^{ek} s_k)[-s_j^{-1}\frac{\partial s_j}{\partial x} + s_j^{-1} e_j r^{\frac{e_j-1}{2}}\frac{\partial r}{\partial x} + s_j^{-1} r^{ej}\frac{\partial s_j}{\partial x}]$$

$$\therefore \frac{\overline{\partial} w}{\partial x} = \sum_{i=1}^{n} (e_i \overline{s}_i{}^{-1}) \frac{\overline{\partial} r}{\partial x} .$$

Here, for each $f \in ZF$, $\bar{f} = \pi(f)$.

Now

$$\frac{\partial w}{\partial x_1} = x_1^{p_1-1} + \ldots\ldots + x_1 + 1$$

$$\frac{\partial w}{\partial x_2} = x_1^{p_1}[x_2^{p_2-1} + \ldots\ldots + x_2 + 1]$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \tag{5}$$

$$\frac{\partial w}{\partial x_k} = x_1^{p_1} \ldots . x_{k-1}^{p_{k-1}} [x_k^{p_k-1} + \ldots\ldots + x_k + 1]$$

$$\frac{\partial w}{\partial x_1} = 0, l > k$$

From (5) $\frac{\partial r}{\partial x_l} = 0$, $l > k$, by the Freiheitssatz. Thus

$$\left.\begin{array}{l} \bar{x}_1^{p_1-1} + \ldots\ldots. + \bar{x}_1 + 1 = \sum_{i=1}^{u} (e_i \bar{s}_i{}^{-1}) \frac{\bar{\partial} r}{\partial x_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \bar{x}_1^{p_1} \ldots \bar{x}_{\alpha-1}^{p_{\alpha-1}} [\bar{x}_\alpha^{p_\alpha-1} + \ldots\ldots + \bar{x}_\alpha + 1] = \sum_{i=1}^{u} (e_i \bar{s}_i{}^{-1}) \frac{\bar{\partial} r}{\partial x_\alpha}, 2 \le \alpha \le k \end{array}\right\} \quad (6)$$

Since $\bar{x}_{\beta-1}^{p_\beta-1} + \ldots\ldots + \bar{x}_\beta + 1$ is irreducible in ZG for $(1 \le \beta \le k)$, (6) implies that either $\sum_{i=1}^{n} (e_i \bar{s}_i{}^{-1})$ or $\frac{\bar{\partial} r}{\partial x_\alpha}$ is a unit in ZG. The first equation in (6) shows that, if $\sum_{i=1}^{n} (e_i \bar{s}_i{}^{-1})$ is a unit, then $\sum_{i=1}^{n} (e_i \bar{s}_i{}^{-1}) = 1$,

and

$$\frac{\bar{\partial} r}{\partial x_1} = x_1^{p_1-1} + \ldots\ldots. + x_1 + 1.$$

So, $\frac{\bar{\partial} r}{\partial x_\alpha} = \bar{x}_1^{p_1} \ldots \bar{x}_{\alpha_1}^{p_\alpha-1} [\bar{x}_\alpha^{\alpha_1-1} + \ldots\ldots + \bar{x}_\alpha + 1]$, $2 \le \alpha \le k$;

Thus, for each β, $\frac{\bar{\partial} r}{\partial x_\beta} = \frac{\bar{\partial} w}{\partial x_\beta}$.

The nature of derivatives imply that $r = w$. On the other hand, $\sum_{i=1}^{n} (e_i \bar{s}_i{}^{-1})$ is not a unit, then $\frac{\bar{\partial} r}{\partial x_\beta}$ is a unit for each β. In this case $\frac{\partial r}{\partial x_\beta} \neq 0$ in ZF, and so, r is a primitive in ZF.

REFERENCES

1. K. A. Brown, On zero divisors in a group ring, *Bull. Lond. Math. Soc.* **8(3)**(1976),251-256.
2. R. H. Fox, Free differential calculus I (Derivation in the free group ring), *Ann. Math.* **57-3** (1953), 547-560.
3. J.Huebschmann, Cohomological theory of aspherical groups and of small cancellation groups, *J. Pure Appl. Algebra,* **14**, (1993) 137-143.
4. K. W. Gruenberg, Cohomological topics in Group Theory, *Springer-Verlag*, *Berlin* (1970).
5. R. C. Lyndon, Cohomology theory of groups with a single defining relation, *Ann. of Math.* **52**, 3, (1950), 656-665.
6. R.C. Lyndon and P.Schupp, Combinatorial group theory, *Springer- Verlag*, *Berlin* (1997)
7. W. Magnus, Das Identitas problem fur Grouppen mit einer difinierenden Relation, *Math. Ann.* **106** (1932), 295-307.
8. Stienberg, On equations in free groups, *Z. Math.* **18** (1971), 87-95.