Simultaneous Existence of right Inverses for $1 - ab$ and $1 - ba$

W.Herfort

Institut für Angewandte und Numerische Mathematik, Technische Universität, A-1040 Wien, Email: herfort @ uranus.tuwien.ac.at

G.Landsmann

Research Institute for Symbolic Computation (RISC-Linz), Johannes Kepler University, A-4040 Linz, Austria, Email: landsmann@risc.uni-linz.ac.at

Abstract

A well known fact in any associative ring with an identity element ensures the existence of a right-inverse for $1 - ba$ provided the one for $1 - ab$ exists. We present a *natural* proof by employing a suitable term rewriting procedure (see, e.g., [1]). AMS subject classification 16S15, 16U60

Key words: Inversion, term rewriting

1 Introduction

Throughout this note R denotes a unitary associative ring.

Lemma 1 *Let a, $b \in R$ such that exists $x \in R$ with*

$$(1 - ab)x = 1$$

then, for $y := 1 + bxa$,

$$(1 - ba)y = 1,$$

i.e., if $1 - ab$ has a right inverse, so has $1 - ba$.

[1] Partially supported by the Austrian Science Foundation

PROOF. Knowing the precise form of y the proof reduces to a routine check.

This proof certainly ignores the question of how to *find* the form of y. A standard method for doing this consists of first solving the problem in the non-commutative ring of formal power series $\mathbb{Z}\langle\langle a, b\rangle\rangle$, where one identifies x with $(1-ab)^{-1}$, i.e.,

$$x = \frac{1}{1-ab} = 1 + ab + (ab)^2 + \cdots$$

Multiplying by b from the left and by a from the right gives

$$bxa = ba + (ba)^2 + (ba)^3 + \cdots$$

so $y = 1 + bxa = \frac{1}{1-ba}$ follows.

2 A constructive proof of Lemma 1

In order to give a proof that exhibits the element y of the Lemma in a more constructive way we employ the following steps.

First consider the free monoid generated by the elements a, b and x:

$$MON := \langle a, b, x\rangle.$$

Note that MON consists of all *words* in the letters a, b and x. Every $\mu \in MON$ will be called a *monomial.* The word length of such a monomial will be referred to as the *total degree* of μ.

Next consider the free $\mathbb{Z}$ – algebra generated by MON, i.e.,

$$F := \mathbb{Z}\langle a, b, x\rangle$$

and the two sided ideal

$$I := \langle (1-ab)x - 1\rangle_F.$$

Put $A := F/I$. Our main idea consists of first to construct y for this particular $\mathbb{Z}$ – algebra and to consider in R the subalgebra $L := \langle a, b, x\rangle$ (we used by abuse of notation the same letters for the homomorphic images of a, b and x

in L). The homomorphic image of y in L serves as a right inverse of $1-ba$ in R.

Since F is a free algebra every element $f \in F$ has a unique presentation

$$f = \sum_{l=0}^{k} f_l$$

where each f_l is a homogeneous polynomial in the variables a, b and x of degree l and k is a suitable natural number. If $f_k \neq 0$ then f is said to have *total degree* k.

We introduce a notion of term reduction in F. Assume that μ is an element of MON. Assume that the word abx occurs in μ, i.e., there are $\nu, \kappa \in MON$ with

$$\mu = \nu abx\kappa,$$

then a $term - reduction$ we define to be a replacement of μ by the polynomial

$$\nu(x-1)\kappa.$$

In order to express this result of term – reduction we shall employ the notation

$$\mu \leftarrow \nu(x-1)\kappa.$$

This notion of term – reduction easily extends to all elements in F. Note that every element only permits a finite number of term – reductions since, after reduction, every monomial turns into a polynomial of lower total degree.

One observes that I is a principal ideal in F and that $f \in I$ if and only if either $f = 0$ or f can be reduced to 0 by performing a finite number of term – reductions.

Next one observes that $\mu \in MON$ cannot be reduced if there exists an element $w(a,b)$ in the submonoid generated by a, b in MON and $m, n \in \mathbb{N}$ so that μ equals one of the following:

$\mu_1 := w(a,b),$
$\mu_2 := w(a,b)ax^m, m \in \mathbb{N}, m > 0$
$\mu_3 := w(a,b)b^m x^n, m, n \in \mathbb{N}, m > 1, n > 0$
$\mu_4 := b^m x^n, m, n \in \mathbb{N}, n > 0.$

Any $\mu \in MON$ that cannot be reduced evidently is a product of elements of the form μ_1, μ_2, μ_3 and μ_4 such that μ_1 may appear only as the last factor (if

μ_1 ends with ab and the next factor begins with x) and μ_4 only occurs as the first factor (if $m = 1$).

Suppose now that one wants to find $y \in F$ with

$$u := (1 - ba)y - 1 \in I$$

then one may assume that there exists $n \in \mathbb{N}$, integers $z_l \in \mathbb{Z}$ and $\nu_l \in MON$, so that none of the ν_l can be reduced if $z_l \neq 0$ ($l = 1, ..., n$), with

$$y = \sum_{l=0}^{n} z_l \nu_l.$$

Next observe that $ba\nu_l$ can be reduced only if ν_l has the form

$$\nu_l = bx^m \nu_l', m \in \mathbb{N}, m > 0, \nu_l' \in MON.$$

Then the result of reduction amounts to

$$(1 - ba)\nu_l \leftarrow bx^{m-1}\nu_l',$$

and the element on the right hand side cannot be reduced further.

Note that y can be written in the form

$$y = y_0 + bxy_1 + bx^2 y_2,$$

where

- y_0 consists only of terms $z_l \nu_l$ where ν_l does not begin with bx,
- y_1 consists only of terms $z_l \nu_l$ where ν_l cannot be reduced and does not begin with x.
- y_2 consists only of terms $z_l \nu_l$ where ν_l cannot be reduced.

In the light of the previous point of discussion one finds that $(1 - ba)y - 1$ reduces to

$$u' := y_0 - bay_0 + by_1 + bxy_2 - 1.$$

Since $u' \in I$ and none of the terms in u' can be reduced one concludes

$$y_0 - bay_0 + by_1 + bxy_2 - 1 = 0 \qquad (1)$$

Since in u' none of the terms in $y_0, bay_0, by_1, -1$ begins with bx one concludes $y_2 = 0$. Therefore, and because none of the terms in y_0 begins with bx, one finds y_0' consisting only of terms $z_l \nu_l$ with ν_l not beginning with x such that

$$y_0 = 1 + by_0'.$$

Introducing this expression into equation 1 and left-cancellation of b (in the free $\mathbb{Z}$ – algebra F) yields the equation

$$y_0' - a - aby_0' + y_1 = 0.$$

Choose y_0' arbitrary to consist of terms not beginning with x, put $y_1 := a + (ab-1)y_0'$ then the equation is satisfied. Therefore one finds that y necessarily must have the form

$$y := 1 + bxa + b(1 - x + xab)y_0'.$$

Obviously y is a right inverse for $1 - ba$. Since y_0' was arbitrary (no term beginning with x) one may choose $y_0' := 0$. This yields the form of y as stated in Lemma 1. By using essentially the same method one can show that the

existence of a right inverse for $1 + ab + cd$ does not necessarily imply the existence of a right inverse for $1 + ba + dc$.

References

[1] F. Winkler, *Polynomial algorithms in computer algebra.* Texts and Monographs in Symbolic Computation. Wien: Springer 1991