Riv. Mat. Univ. Parma (3) 2 (1973), 83-89

GHIRDARI LAL FOTEDAR (*)

On one sided quasi-inverses. (**)

1. – It is well known [1] that if an element of a ring has more than one right quasi-inverse (r.q.i.) then, it has infinitely many r.q.i.'s. The object of this paper is to derive this result by a simple set theoretic argument and to find a formula giving all the r.q.i.'s of an element when one of them is known. We also obtain some properties of a ring with an element having more than one r.q.i.. In particular we shall show that such a ring admits an isomorphism into itself. We also obtain an infinite set of orthogonal idempotents constructed by JACOBSON as a particular case of our method. Incidently we also show that the ring contains an infinite set of elements whose squares vanish.

2. – Let a, b be two elements of a ring R such that $a \circ b = 0 \neq b \circ a$ so that b is a r.q.i. of a but not a left quasi-inverse, where $x \circ y = x + y - xy$ for all x, y in R. Let, $S = \{t \in R / a \circ t = 0\}$. Then S is obviously non-empty. Let φ be the mapping of R into itself defined by

(2.1) $$\varphi(z) = b - z \circ a \, .$$

Then we have,

Theorem (2.1). *φ is a one to one map of R into a subset of itself such that S is mapped into a proper subset of itself.*

(*) Indirizzo: U.G.C. Junior Research Fellow, Faculty of Mathematics, University of Delhi, Delhi - 7, India.

(**) Ricevuto: 21-III-1972.

Proof.

$$\varphi(z) = \varphi(z') \Rightarrow z \circ a = z' \circ a$$

circling both sides on the right by b, we get $z = z'$.

Let $z \in S$. Then,

$$a \circ (b - (z \circ a)) = a \circ b - a \circ (z \circ a) + a = -(a \circ z) \circ a + a = 0$$

so that $\varphi(z) \in S$. Obviously $b \notin \varphi(S)$, since there is no $z \in R$ such that, $z \circ a = 0$.

Corollary. *The set S is infinite.*

3. – We shall now obtain all the r.q.i.'s of a, given one of them, say b.

Lemma (3.1). *If u is any element of a ring R, then the general solution of the equation*

$$u \circ x = uy \tag{3.1}$$

is given by

$$x = uz - u\,, \qquad y = u \circ z\,, \tag{3.2}$$

where z is arbitrary in R, and distinct values of z give rise to distinct solutions.

Proof. Writing the equation $u \circ x = uy$ in the form $u + x = u(x + y)$ and denoting $x + y$ by z, it follows that any solution must be of the form (3.2).
Conversely, if x and y are given by (3.2), then

$$u \circ x = u \circ (uz - u) = u + uz - u - u^2 z + u^2 =$$

$$= u(z + u - uz) = u(u \circ z) = uy\,.$$

Now suppose that for some $z, z' \in R$, $uz - u = uz' - u$ and $u \circ z = u \circ z'$. Adding the corresponding sides of the two equations we get $z = z'$.

Theorem (3.1). *If b is a solution of the equation,*

$$a \circ w = 0\,, \tag{3.3}$$

for a given $a \in R$ *then,* $w = by + x$*, where* x *and* y *are given by* (3.2) *for any* $z \in R$ *and* $u = a$*. We observe that* w *may also be written in the form,*

$$w = z + b - (b \circ a \circ z)\,. \tag{3.4}$$

Proof. If $w = by + x$, where x and y are given by (3.2) for any z in R and $u = a$ then,

$$a \circ w = a \circ (by + x) = a + by + x - aby - ax =$$

$$= (a \circ x) + by - aby = (a + b - ab)\,y = (a \circ b)\,y = 0\,.$$

Moreover,

$$w = by + x = b(a \circ z) + (az - a) =$$

$$= b + (a \circ z) - b \circ (a \circ z) + (az - a - z) + z = b + z - (b \circ a \circ z)\,.$$

We now show that if w is any solution of (3.3), then w can be put in the form (3.4). In fact we have only to take $z = w$ so that

$$b + w - (b \circ a \circ w) = b + w - b = w\,.$$

We shall now give some deductions from Theorem (3.1).

1) If the equation (3.3) has a unique solution $b \in R$, then b is also a solution of $t \circ a = 0$, so that a is q.r.i.

Proof. By hypothesis $w = b$ for all $z \in R$, so that $z = b \circ a \circ z$. In particular taking $z = 0$, we get $b \circ a = 0$.

2) Conversely we have, if $b \circ a = 0$, then $w = z + b - z = b$ for all $z \in R$, so that b is the only r.q.i. of a.

3) The infinite number of r.q.i. of a of the form, $b - b \circ a^{\circ k} + a^{\circ k-1}$, $k = 1, 2, \ldots$ where for any $x \in R$, $x^{\circ n} = x \circ x^{\circ n-1}$, for $n \geqslant 1$ and $x^{\circ 0} = 0$ obtained by Jacobson [**1**] can be obtained from (3.4) by putting $z = a^{\circ k-1}$.

Lemma (3.2). *If* w *is any solution of* (3.3) *of which* b *is a given solution then,*

$$w \circ a = (b \circ a)(z \circ a)\,, \tag{3.5}$$

for some $z \in R$*; and conversely,* (3.5) *gives a solution* w *of* (3.3) *for any* $z \in R$*.*

Proof. Circling both sides of (3.4) by a on the right we get

$$w \circ a = b \circ a + z \circ a - (b \circ a \circ z \circ a) = (b \circ a)(z \circ a) .$$

Conversely circling both sides of (3.5) by b on the right we get

$$\{(b \circ a)(z \circ a)\} \circ b = \{(b \circ a) + (z \circ a) - (b \circ a) \circ (z \circ a)\} \circ b =$$

$$= \{(b + z - b \circ a \circ z) \circ a\} \circ b = (b + z - b \circ a \circ z) = w .$$

Lemma (3.3). *If* $u, z, z' \in R$, *then*

$$(z \circ u)(z' \circ u) = (z'' \circ u) , \tag{3.6}$$

where,

$$z'' = z + z' - (z \circ u \circ z') . \tag{3.7}$$

Proof.

$$(z \circ u)(z' \circ u) = (z \circ u) + (z' \circ u) - (z \circ u) \circ (z' \circ u) =$$

$$= \{z + z' - (z \circ u \circ z')\} \circ u = z'' \circ u .$$

Lemma (3.4). *If* w *is a solution of* (3.3) *for some* $z \in R$ *then, for any* $u \in R$

$$(u \circ a)(w \circ a) = (w \circ a) . \tag{3.8}$$

Proof. Taking $z' = w$, $z = u$ in (3.6) and (3.7) and $u = a$ we get

$$(z \circ a)(w \circ a) = \{u + w - (u \circ a \circ w)\} \circ a = (w \circ a) .$$

Corollary 1. $(w \circ a)^2 = (w \circ a)$, *for all solutions* w *of* (3.3).

Proof. Take $u = w$ in (3.8).

Corollary 2. *If* w *and* w' *are any two solutions of* (3.3) *and*

$$x = (w \circ a) - (w' \circ a) , \tag{3.9}$$

then $x^2 = 0$.

Proof.

$$x^2 = \{(w \circ a) - (w' \circ a)\}^2 = (w \circ a)^2 - (w \circ a)(w' \circ a) - (w' \circ a)(w \circ a) + (w' \circ a)^2$$
$$= (w \circ a) - (w' \circ a) - (w \circ a) + (w' \circ a) \quad \text{(by (3.8), Cor. 1)}$$
$$= 0 .$$

Lemma (3.5). *If $w' = (z')$ corresponding to $z' \in R$ and $w'' = (z'')$ corresponding to $z'' \in R$ are two solutions of* (3.3) *then*

$$w' - w'' = (b \circ a)(z' - z'') . \tag{3.10}$$

Proof. From (3.4) we have

$$w' - w'' = (z' - z'') - \{(b \circ a \circ z') - (b \circ a \circ z'')\} =$$
$$= (z' - z'') - \{- (b \circ a) z' + (b \circ a) z'' + (z' - z'')\} = (b \circ a)(z' - z'') .$$

Corollary. *If N is the right ideal in R defined by $N = R(b \circ a)$ then the elements in the same coset of N in R give rise to same solution of* (3.3) *and elements in the distinct cosets of N in R give rise to distinct solutions of* (3.3). *Also he index of N in R is infinite.*

Proof. This follows from Lemma (3.5) and Theorem (2.1).

4. – Theorem (4.1). *The mapping χ_{ij}: RR, $i, j = 1, 2, \ldots$ defined by*

$$\chi_{ij}(z) = b^{\circ i} \circ z \circ a^{\circ j} - b^{\circ i} \circ a^{\circ j} \tag{4.1}$$

is an isomorphism of $(R, +)$ into $(R, +)$.

For $i = j$, $\chi_{ii}(z)$ is an isomorphism of $(R, ., +)$ into $(R, ., +)$.
If R has identity 1 then, $1 - b^{\circ i} \circ a^{\circ i}$ is the identity for $\chi_{ii}(R)$.

Proof. We observe that

$$(1 - b)^i z (1 - a)^j = (1 - b)^i (1 - (1 - z))(1 - a)^j =$$
$$= (1 - b)^j (1 - a)^i - (1 - b)^i (1 - z)(1 - a)^j = (1 - b^{\circ i} \circ a^{\circ j}) -$$
$$- (1 - b^{\circ i} \circ z \circ a^{\circ j}) = b^{\circ i} \circ z \circ a^{\circ j} - b^{\circ i} \circ a^{\circ j} = \chi_{ij}(z) .$$

Hence

$$\chi_{ij}(z+z') = (1-b)^i(z+z')(1-a)^j =$$

$$= (1-b)^i z(1-a)^j + (1-b)^i z'(1-a)^j = \chi_{ij}(z) + \chi_{ij}(z') .$$

Obviously $\chi_{ij}(z) = 0$ for $z = 0$. Conversely if $\chi_{ij}(z) = 0$ then

$$0 = (1-a)^i \chi_{ij}(z)(1-b)^j = z .$$

Thus χ_{ij} is an isomorphism of $(R, +)$ into $(R, +)$. Since $\chi_{ij}(R)$ does not obviously contain the element $b^{\circ i} \circ a^{\circ j}$, it follows that χ_{ij} maps R into a proper subset.

For $i = j$, we have

$$\chi_{ii}(zz') = (1-b)^i(zz')(1-a)^i = (1-b)^i \big(z(1-a)^i\,(1-b)^i z'\big)(1-a)^i =$$

$$= \big((1-b)^i z(1-a)^i\big)\big((1-b)^i z'\,(1-a)^i\big) = \chi_{ii}(z)\,\chi_{ii}(z') .$$

Thus χ_{ii} is an isomorphism of $(R, ., +)$ into $(R, ., +)$. Finally if $1 \in R$, then $1 - b^{\circ i} \circ a^{\circ i} = (1-b)^i(1-a)^i$ is the identity for $\chi_{ii}(R)$, since

$$(1-b)^i z(1-a)^i(1-b)^i(1-a)^i = (1-b)^i z(1-a)^i = (1-b)^i\,(1-a)^i\,(1-b)^i z(1-a)^i$$

Remark 1.

$$\chi_{ij}(z)\,\chi_{kl}(z') = \chi_{il}\big(z(1-a)^{j-k}z'\big) , \qquad \text{if } j \geqslant k ,$$
$$= \chi_{il}\big(z(1-b)^{k-j}z'\big) , \qquad \text{if } j \leqslant k .$$

Hence,

$$\chi_{ij}(z)\,\chi_{kl}\big((b\circ a)\,z'\big) = 0 , \qquad \text{if } j > k ,$$
$$\chi_{ij}\big(z(b\circ a)\big)\,\chi_{kl}(z') = 0 , \qquad \text{if } j < k ,$$
$$\chi_{ij}(z)\,\chi_{jk}\big((b\circ a)\,z'\big) = \chi_{ij}\big(z(b\circ a)\big)\,\chi_{jk}(z') ,$$
$$= \chi_{ik}\big(z(b\circ a)\,z'\big) ,$$
$$\chi_{ij}\big(z(b\circ a)\big)\,\chi_{kl}\big((b\circ a)^{ik}z'\big) = 0 , \qquad \text{if } j \neq k ,$$
$$= \chi_{il}\big(z(b\circ a)\,z'\big) , \qquad \text{if } j = k .$$

In particular, taking $z = z' = w \circ a$ with $w \in S$, we get

$$\chi_{ij}(b \circ a)\chi_{kl}(w \circ a) = 0 \qquad \text{if} \quad j \neq k\,,$$
$$= \chi_{il}(w \circ a) \qquad \text{for } j = k\,.$$

which reduces to JACOBSON's result [**1**] for $w = b$.

Remerk 2. If R is a ring and $a, b \in R$ such that $ab = 1 \neq ba$. Then by KAPLANSKY's result a has an infinity of righ inverses. The general formula for all the right inverses of a will be, $w = z + b - baz$ where z is arbitrary in R and $aw = 1$. Here again we observe that $\chi_{ij}\colon R \to R$ such that $\chi_{ij}(z) = b^i z a^j$ is an isomorphism of $(R, +)$ into $(R, +)$ since $1 \notin \chi_{ij}(R)$ and for $i = j$, it is also true that χ_{ii} is an isomorphism of $(R, ., +)$ into $(R, ., +)$ and that $b^i a^i$ serves as the identity for $\chi_{ii}(R)$.

5. – Let $a \circ b = 0 \neq b \circ a$, for $a, b \in R$. Let $S = \{w \in R \mid a \circ w = 0\}$. Let $K = \{z \circ a \mid z \in R\}$. Then by Lemma (3.3) K is a semigroup. Let R' be the subring of R generated by the set K. Then

$$R' = \Big\{\alpha = \big(\sum_{z \in R} n(\alpha, z)(z \circ a)\big) \in R \mid n(\alpha, z) = 0$$
$$\text{for all but a finite number of } z \in R,\ n(\alpha, z) \text{ being an integer}\Big\}.$$

Let,

$$T = \{\beta = (w \circ a) - (w' \circ a) \mid w, w' \in S\}\,.$$

Then the subring D generated by T consists of linear combinations of the element $\beta \in T$. It is clear from (3.8), (3.9) and (3.10) that D is an ideal in R' and that $D^2 = 0$.

I am highly indebted to Dr. P. KESAVA MENON, Director, JOINT CIPHER BUREAU, Ministry of Defence, for his kind guidance and encouragement during the preparation of this manuscript. I also wish to express my thanks to OM KUMAR for typing out the manuscript.

References.

[**1**] N. JACOBSON, *Some remarks on one sided inverses*, Proc. Amer. Math. Soc. (1950), 352-355.

* * *