



Pseudo-Inverses in Associative Rings and Semigroups

Author(s): M. P. Drazin

Source: *The American Mathematical Monthly*, Vol. 65, No. 7 (Aug. - Sep., 1958), pp. 506-514

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2308576>

Accessed: 21/09/2008 19:44

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact support@jstor.org.



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

display to them what McShane has called the “two legs” on which mathematics stands—its “innate beauty and austere elegance” as well as its “usefulness to scientists and technicians of all kinds.”*

* E. J. McShane, Maintaining communication, this MONTHLY, vol. 64, 1957, pp. 309–317.

PSEUDO-INVERSES IN ASSOCIATIVE RINGS AND SEMIGROUPS

M. P. DRAZIN, Northwestern University

1. Introduction. E. H. Moore ([5], and *cf.* also Penrose [6], Rado [8]) has shown how, given any square matrix x with elements in the complex field, it is possible to define another matrix, coinciding with x^{-1} whenever x^{-1} happens to exist, and having (even for singular x) properties leading to simple proofs of several theorems which yield to other methods only with difficulty (if at all). More precisely, Moore's result (stated in Penrose's form) is that, given any square* complex matrix x , then there is always exactly one complex matrix c satisfying

$$cxc = c \quad \text{and} \quad xcx = x,$$

$$cx \text{ and } xc \text{ are both hermitian.}$$

Following Penrose, we denote this unique matrix c by x^\dagger , and call it *the generalized inverse of x* ; for evidence of the value of this concept, we refer the reader to the work of Moore and Penrose ([5], [6], [7]).

It is clear from Penrose's arguments that the function x^\dagger thus defined for square complex matrices can be extended to the elements of any finite-dimensional algebra R over the complex field by the standard device of mapping R isomorphically into the algebra M_n of all $n \times n$ complex matrices (*e.g.* with $n = 1 + \dim R$), *provided* that the image of R in M_n admits the operation of forming transposed complex conjugate matrices. However, there seems to be no prospect of extending Moore's generalized inverse concept so as to apply to finite-dimensional algebras over a given division ring F unless F at any rate admits an involutory anti-automorphism $\lambda \rightarrow \bar{\lambda}$ such that $\lambda_1 \bar{\lambda}_1 + \dots + \lambda_m \bar{\lambda}_m = 0$ implies $\lambda_1 = \dots = \lambda_m = 0$. (This, of course, would restrict F to having zero characteristic.)

In this note we show how to define a function, somewhat analogous to the generalized inverse function, over the elements of *arbitrary* finite-dimensional algebras, and even of an extensive class of associative rings. Indeed, all of our

* In fact, Moore and Penrose considered rectangular matrices, but this aspect of the result is not relevant here.

theorems in Section 2 below apply equally well to arbitrary semigroups; however, we shall for brevity, generally use the language of ring theory.

Given any associative ring R , and any element x of R , we shall call c *pseudo-invertible (in R)* if an element c of R exists satisfying

$$(i) \quad cx = xc,$$

$$(ii) \quad x^m = x^{m+1}c \text{ for some positive integer } m,$$

and

$$(iii) \quad c = c^2x.$$

By Theorem 1 below, these three conditions determine c uniquely when it exists, so we may refer to c as *the* pseudo-inverse of x . We show also (*inter alia*) that the existence of such a c in fact follows from the apparently much weaker hypothesis that elements a, b of R exist such that

$$x^p = x^{p+1}a, \quad x^q = bx^{q+1}$$

(for some positive integers p, q); in other words, pseudo-invertibility (as applied to a given element x of a given ring) coincides with Azumaya's property [2] of *strong π -regularity*. Since it is known that every element of any algebraic ring (as defined in [3]), or of any ring with minimal condition on left or right ideals, is strongly π -regular, it follows that our pseudo-inverse function is applicable to all such rings (and, in particular, to matrices and all finite-dimensional algebras). The specialization of pseudo-invertibility in which (ii) above holds with $m=1$ was discussed by Azumaya, and indeed some of our arguments below are, formally, only slight generalizations of his: the essence of our present contribution is that (i), (ii) and (iii) determine c uniquely even when m is unrestricted (and indeed variable). The case $m=1$ of pseudo-invertibility, but with (iii) omitted, was discussed by A. H. Clifford [10], who called the corresponding property "relative invertibility"; in view of our Theorem 4 below, this property of relative invertibility is, in fact, precisely equivalent to pseudo-invertibility with $m=1$.

In our third section, we use pseudo-inverses to obtain a simple proof of another result of Azumaya ([2] Theorem 4). At the suggestion of a referee, we describe, in a concluding section, another way of looking at pseudo-inverses in any semigroup S : it turns out that our definition can be equivalently expressed, in a natural and simple way, in terms of certain idempotents and maximal subgroups of S . After Moore's and Penrose's work, it seems not unreasonable to hope that the pseudo-inverse may prove to be a useful tool in dealing with those rings in which it is everywhere defined, and that the publication here of the basic properties of pseudo-inverses may perhaps serve as a starting-point for other applications.

2. General results on pseudo-inverses. In this section we establish a number of facts about pseudo-inverses in rings (or semigroups) not subjected to any global conditions. First and most fundamentally, we have

THEOREM 1. *Let R be any given associative ring (or semigroup), and x any element of R . Then x has at most one pseudo-inverse in R , and, if a pseudo-inverse for x does exist, it commutes with every element of R which commutes with x .*

Proof. Let c_1, c_2 satisfy conditions corresponding to those imposed on c by (i), (ii) and (iii) of our definition of pseudo-invertibility, say with integers m_1, m_2 in (ii). Then, on writing $m = \max(m_1, m_2)$, the conditions on c_1, c_2 arising from (i), (ii) certainly imply

$$(A) \quad c_1 x^{m+1} = x^m = x^{m+1} c_2,$$

while those arising from (i), (iii) certainly imply

$$(B) \quad c_1 = c_1^2 x, \quad c_2 = x c_2^2.$$

And in fact (A), (B) together imply that $c_1 = c_2$. For, by induction from (B), we have $c_1 = c_1^{k+1} x^k, c_2 = x^k c_2^{k+1}$ ($k = 1, 2, \dots$), and in particular $c_1 = c_1^{m+1} x^m, c_2 = x^m c_2^{m+1}$, whence, by (A),

$$c_1 = c_1^{m+1} x^m = c_1^{m+1} x^{m+1} c_2 = c_1 x c_2 = \dots = c_2.$$

Thus x has at most one pseudo-inverse c . Also, if y is any element of R satisfying $xy = yx$, then, by (ii) and (i), we find

$$c x^m y = c y x^m = c y x^{m+1} c = c x^{m+1} y c = x^m y c,$$

whence $c^{m+1} x^m y = x^m y c^{m+1}$; but, as above, (iii) gives $c = c^{m+1} x^m$, and so, using (i) again, we conclude that

$$c y = c^{m+1} x^m y = x^m y c^{m+1} = y c^{m+1} x^m = y c,$$

as required.

In view of Theorem 1, we may denote the unique pseudo-inverse of a given pseudo-invertible element x by x' ; obviously, whenever x^{-1} exists in the ordinary sense, then x' exists and $x' = x^{-1}$. It should be noted that, when it is defined at all, x' is independent of what ring we think of x as lying in (in the sense that, if R_1, R_2 are subrings of a given ring R and x lies in $R_1 \cap R_2$, having pseudo-inverses c_1, c_2 in R_1, R_2 respectively, then c_1, c_2 , being pseudo-inverses for x in R , must coincide).

COROLLARY 1. *If x_1, \dots, x_j are given pseudo-invertible elements (of some ring) with $x_s x_t = 0$ ($s, t = 1, \dots, j; s \neq t$), then $x_1 + \dots + x_j$ is also pseudo-invertible, with $(x_1 + \dots + x_j)' = x_1' + \dots + x_j'$.*

Proof. There will clearly be no loss of generality in supposing from the outset that $j = 2$; and it will also be convenient to write u, v in place of x_1, x_2 . By (i), the hypothesis $uv = vu (= 0)$, and a double application of the last part of Theorem 1, we see that u, v, u', v' all commute with one another; further, by (iii),

any product of these which simultaneously involves u or u' and also v or v' can be expressed as a product involving both u and v , and must consequently vanish. Hence

$$(u' + v')(u + v) = (u + v)(u' + v'),$$

$$(u' + v')^2(u + v) = u'^2u + v'^2v = u + v,$$

and, choosing m so large that $u^m = u^{m+1}u'$, $v^m = v^{m+1}v'$, we have

$$(u + v)^{m+1}(u' + v') = u^{m+1}u' + v^{m+1}v' = u^m + v^m = (u + v)^m;$$

by the first part of Theorem 1, the result now follows.

Given any pseudo-invertible element x of a ring, then, by (ii), there will be a unique (positive) integer $i(x)$ such that $x^m = x^{m+1}x'$ for every $m \geq i(x)$ but for no $m < i(x)$. We shall refer to $i(x)$ as *the index of x* ; again, provided that it does indeed exist, this integer $i(x)$ does not depend on what ring we regard x as lying in. If x is not pseudo-invertible, then we take $i(x) = \infty$ conventionally.

The special case of Theorem 1 in which $m_1 = m_2 = 1$ is, apart from differences in terminology, just Azumaya's ([2] Lemma 1) with the existence clause omitted;* our next result, however, is of interest chiefly when $i(x) > 1$.

THEOREM 2. *Let x be any pseudo-invertible element (of some given ring) and k any positive integer. Then x^k is pseudo-invertible, with $(x^k)' = (x')^k$, and $i(x^k)$ is the unique (positive) integer q satisfying $0 \leq kq - i(x) < k$.*

Proof. By (i), $x^k(x')^k = (x')^kx^k$. Also, by induction from (ii), (iii) respectively, we have $x^{i(x)} = x^{i(x)+j}(x')^j$, $x^j = (x')^{j+1}x^j$ ($j = 1, 2, \dots$), so that, since $kq \geq i(x)$,

$$(x^k)^q = x^{kq-i(x)}x^{i(x)} = x^{kq-i(x)}x^{i(x)+k}(x')^k = (x^k)^{q+1}(x')^k,$$

$$(x')^k = (x')^{k-1}(x')^{k+1}x^k = ((x')^k)^2x^k.$$

Thus $(x')^k$ satisfies the conditions for $(x^k)'$, and $i(x^k) \leq q$.

Finally, $i(x^k) < q$ would mean that $(x^k)^{q-1} = (x^k)^q(x')^k$, and, since $x' = x^{k-1}(x')^k$, this in turn implies that $x^{k(q-1)} = x^{kq-(k-1)}x' = x^{k(q-1)+1}x'$, whence, by the definition of $i(x)$, we should have $k(q-1) \geq i(x)$, contrary to our definition of q .

THEOREM 3. *Given any element x of a ring, then if x is pseudo-invertible so is x' ; in fact x' has index 1 whenever it exists, and then $x'' = x^2x'$.*

To prove this, one has merely to verify that, if c satisfies (i), (ii) and (iii), then $d = x^2c$ satisfies $cd = dc$, $c = c^2d$, $d = d^2c$. We omit the details, and also leave to the reader the proofs of the following equally trivial joint corollaries of Theorems 1, 2 and 3:

* The last clause of Theorem 1 in this special case has also been set as a problem by T. Skolem [9].

COROLLARY 2. *Given any element x of a ring R , then $x'' = x$ if and only if x is pseudo-invertible with index 1; and, when this is the case, for any given element y of R , x commutes with y if and only if x' does.*

COROLLARY 3. *Given any pseudo-invertible element x of a ring, then $(x^k)'' = x^k$ for every integer $k \geq i(x)$.*

COROLLARY 4. *For any pseudo-invertible element of a ring, $x''' = x'$.*

We have already noted that an element x of a ring R is called *strongly π -regular* in R if elements a, b of R and positive integers p, q exist such that

$$(1) \quad x^p = x^{p+1}a, \quad x^q = bx^{q+1}.$$

We now prove

THEOREM 4. *Given any element x of a ring R , then x is pseudo-invertible in R if and only if it is strongly π -regular in R .*

Proof. That pseudo-invertibility implies strong π -regularity is obvious (even without using (iii)). Conversely, we shall show that (1) implies (i), (ii) and (iii) with $m = \max(p, q)$ and $c = x^m a^{m+1}$.

We note first that (1) gives

$$x^{m+1}a = x^m = bx^{m+1},$$

so that $x^m a = bx^{m+1} \cdot a = b \cdot x^{m+1}a = bx^m$, whence, by induction, $x^m a^k = b^k x^m$ ($k = 1, 2, \dots$). Thus our choice $c = x^m a^{m+1}$ can equivalently be written $c = b^{m+1} x^m$, and we have:

(i) $xc = x \cdot x^m a^{m+1} = x^{m+1} a \cdot a^m = x^m a^m = b^m x^m = \dots = cx$ by symmetry;

(ii) By another induction, $x^m = x^{m+k} a^k$ ($k = 1, 2, \dots$), and so

$$x^{m+1}c = x^{m+1} \cdot x^m a^{m+1} = x^{m+(m+1)} a^{m+1} = x^m;$$

(iii) By (i) and (ii) which we have just proved,

$$c^2x = c \cdot xc = c \cdot x^{m+1} a^{m+1} = x^{m+1} c \cdot a^{m+1} = x^m a^{m+1} = c.$$

It is clear from this proof that (1) ensures that $i(x) \leq \max(p, q)$, and (cf. [2] Lemma 3) indeed it is easy to see that in fact $i(x) \leq \min(p, q)$: for if, say, $p < q$, then (1) gives $x^p = x^{p+(q-p)} a^{q-p} = x^q a^{q-p}$, so that $bx^{p+1} = bx \cdot x^q a^{q-p} = bx^{q+1} \cdot a^{q-p} = x^q a^{q-p} = x^p$. In view of this, our Theorem 4 includes Azumaya's Theorem 3, in which he proved that strong π -regularity implies the *existence* of c satisfying (i) and (ii); we can arrange for uniqueness only by introducing some additional restriction such as (iii). For a discussion of the implications subsisting between strong π -regularity (*i.e.*, pseudo-invertibility), right π -regularity, left π -regularity and π -regularity, we refer the reader to Azumaya's paper.

COROLLARY 5. *Let R be any finite-dimensional algebra. Then, for any given $x \in R$, x' exists and lies in the subalgebra generated by x .*

Proof. If R has dimension k , then x, x^2, \dots, x^{k+1} are linearly dependent, and so, for some $j \leq k+1$, x^j is a linear combination of x^{j+1}, x^{j+2}, \dots , hence even of x^{j+2} and higher powers. Thus x is strongly π -regular, with $a = b$ in (1) expressible as polynomials in x (without constant terms); the corollary now follows from the form of c in the proof of Theorem 4 above. More generally, the result clearly holds even for all "algebraic rings" (in which, by definition, there corresponds to each element x an integer $j(x)$ such that $x^{j(x)}$ is a linear combination of $x^{j(x)+1}$ and higher powers).*

We remark that, immediately from the definition and uniqueness property, the operation of taking the pseudo-inverse (when such exists) of a given element commutes with all homomorphisms and antihomomorphisms of the containing ring. In particular, for any matrix algebra over the complex field, the pseudo-inverse of the complex conjugate (or transpose) of a given matrix is the same as the complex conjugate (or transpose) of the pseudo-inverse. Thus the pseudo-inverse of a given complex matrix x is real (symmetric, hermitian, etc.) whenever x is; and, even for arbitrary square complex matrices, it can be shown (e.g., by using (iii) and Corollary 5) that the property of having all eigenvalues real and nonnegative is also preserved.

3. Sufficient conditions for pseudo-invertibility in rings.

Following Azumaya, we call an element x of a ring R *right π -regular* in R if a positive integer p and an element a of R exist such that $x^p = x^{p+1}a$. In these circumstances we shall define the *right index* of x in R , denoted by $r(x)$ (or more precisely $r_R(x)$), as the smallest integer p occurring in any such representation; and we take $r(x) = \infty$ whenever x is not right π -regular. Thus $r(x)$ is defined for all elements of R ; and we define the *left index* $l(x) = l_R(x)$ of x in R similarly. Then, for any given x , we know from Theorem 4 that $i(x)$ is finite (i.e., x is pseudo-invertible) if and only if $r(x), l(x)$ are both finite, while our remark following Theorem 4 shows that then in fact $r(x) = l(x) = i(x)$.

This "local" result (i.e., concerning only the single element x) is new, but a still more striking "global" result has been known for some time ([4] p. 74). Given any subset T of a ring R , let us write

$$i(T) = \sup i(x), \quad r(T) = \sup r(x), \quad l(T) = \sup l(x),$$

where each upper bound is taken over all $x \in T$ (with the natural convention for infinite values \ddagger). Obviously $r(T) \leq i(T)$, and Kaplansky's result (or rather

* In the case of a square matrix x over an algebraically closed field F , we could alternatively prove the existence of x' by combining Corollary 1 (for $j=2$) with the well-known fact that x is similar over F to diagonal (u, v) , where u, v are square matrices over F with u (if occurring) nilpotent and v (if occurring) nonsingular.

§ For a pseudo-invertible element x , the common value of $r(x), l(x)$ and $i(x)$ coincides with the value of the "index of x " as defined by Azumaya (whose definition concerned only pseudo-invertible elements); but it is important in what follows that $r(x), l(x)$ and $i(x)$ are meaningful for arbitrary x , and that $r(x), l(x)$ (separately) can be finite even for nonpseudo-invertible x .

‡ More precisely, we take $i(T) = \infty$ whenever the $i(x)$ with $x \in T$ are finite but unbounded, and also whenever $i(x) = \infty$ for some $x \in T$; and similarly for $r(T), l(T)$.

a slightly-strengthened form of it) is that, if $r(R)$ is finite, then so is $i(R)$ and in fact $i(R) = r(R)$; moreover, by our final remark in the previous paragraph, we even have $i(x) = r(x) = l(x) < \infty$ for each $x \in R$.

To motivate the next theorem (which was discovered by Azumaya, and does not seem readily extensible to semigroups), we note first that our definitions of $i(x), r(x), l(x)$ are of course consistent with the accepted meaning of the "index" of a given nilpotent element of a ring. More precisely, every nilpotent element x is clearly pseudo-invertible (with $x' = 0$), so that $i(x) = r(x) = l(x) < \infty$, and satisfies $x^{i(x)} = 0, x^{i(x)-1} \neq 0$ (since $x^{i(x)} = x^{i(x)+k}(x')^k$ for arbitrarily high k , while $x^{i(x)-1} = 0$ would contradict the definition of $i(x)$). Thus, if $N = N(R)$ denotes the set of all nilpotent elements of the ring R , then we always have $i(N) = r(N) = l(N)$ (possibly all infinite), and $i(N) < \infty$ expresses the condition that the nilpotent elements of R have bounded index.

In ([2] Theorem 4), Azumaya generalized Kaplansky's result that the finiteness of $r(R)$ implies that of $i(R)$; replacing the finiteness of $r(R)$ by that of $i(N)$, he showed that this obviously weaker hypothesis in fact implies that $i(x) \leq i(N)$ whenever $r(x)$ (or $l(x)$) is finite. We present now a new and very simple proof, bearing only a slight resemblance to Azumaya's (and none to Kaplansky's), of this result.

THEOREM 5. *Let R be any associative ring whose nilpotent elements have bounded index (i.e., with finite bound $i(N)$). Then every right π -regular element x of R is pseudo-invertible, with $i(x) = r(x) = l(x) \leq i(N)$.*

Proof. Given any right π -regular element x of R , say with $x^p = x^{p+1}a$, we shall first show that x is necessarily pseudo-invertible; by Theorem 4, it will be enough to find $b \in R$ and a positive integer q such that $x^q = bx^{q+1}$.

Now, by induction, we have $x^p = x^{p+k}a^k$, and so

$$x^{p+k}(x^p - a^k x^{p+k}) = (x^p - x^{p+k}a^k)x^{p+k} = 0 \quad (k = 1, 2, \dots).$$

Also each of the 2^t monomials in the expansion of $(x^p - a^k x^{p+k})^t$ has x^{p+k} as a right-hand factor provided only that $pt \geq p+k$, and so, for each k , we have $(x^p - a^k x^{p+k})^{t+1} = 0$ for large enough t . Hence, by our hypothesis that $i(N)$ is finite, it follows that $(x^p - a^k x^{p+k})^{i(N)} = 0$, so that $x^{i(N)p} \in Rx^{p+k}$ ($k = 1, 2, \dots$). Choosing $k = (i(N) - 1)p + 1$, we deduce that an element b of R exists such that $x^q = bx^{q+1}$, where $q = i(N)p$.

Thus x is pseudo-invertible, so that (i) and (ii) clearly give $(x - x^2x')^m = 0$ for some m , whence $(x - x^2x')^{i(N)} = 0$; hence, by (i), $x^{i(N)} = x^{i(N)+1}y$ for a suitable polynomial y in x, x' (with integer coefficients and no constant term), and so, finally, by (i) and the proof of Theorem 4, we can conclude that $i(x) \leq i(N)$. (Also, incidentally, we have the explicit representation $x' = x^p a^{p+1}$).

COROLLARY 6. *Let R be any associative ring whose nilpotent elements have bounded index. Then, if every element of R is right π -regular, R must in fact be boundedly right π -regular, i.e. $r(R)$ is finite, and indeed $r(R) = i(R) = i(N) < \infty$.*

To deduce this from the theorem, we have only to note that $r(R) \leq i(R) \leq i(N) = r(N) \leq r(R)$ (the inequality $i(R) \leq i(N)$ following from Theorem 5 and the hypothesis of the corollary, while the other relations are obviously true in any ring); and of course Kaplansky's result is included in Corollary 6. We remark also that, by Azumaya's ([2] Theorem 5), one may, in the hypothesis of Corollary 6, replace "right π -regular" by " π -regular."

Some familiar examples of rings satisfying the hypotheses of Corollary 6 are (a) rings with minimal condition on (say) right ideals, and (b) algebraic rings of bounded degree (or, more generally, of bounded index); but it is already known (see [1] Theorem 3.1 and [4] p. 74) that rings of type (a) have $r(R), l(R)$ finite, and this is obvious in case (b). However, Arens and Kaplansky's proof that $r(R)$ is finite in case (a), though brief enough, depends on the Wedderburn-Artin structure theory, and it would be gratifying to find a direct proof. We mention in this connection that, since every element x of any ring of type (a) is (from consideration of the descending chain of principal right ideals generated by the powers of x) clearly right π -regular, it would, in view of Corollary 6, suffice to prove (directly) the finiteness of $i(N)$; and, for this, since the rings in question have nilpotent (Jacobson) radicals, only the semisimple case need be considered.

4. Concluding remarks. The author is grateful to a referee for pointing out that, even in the context of arbitrary semigroups, the definition of pseudo-invertibility can be rephrased in a way that may perhaps make it more immediately available as a tool for tackling certain problems. To do this, given any element e of a semigroup S , let G_e denote the set of all elements $a \in S$ such that

$$(\alpha) ae = ea = a, \quad \text{and} \quad (\beta) ab = ba = e \text{ for some } b \in S.$$

Clearly, if G_e is nonempty, then e is necessarily idempotent, and, conversely, we have (this being, essentially, Lemma 1.3 of Clifford's paper [10]).

THEOREM 6. *If e is idempotent, then G_e is a group with e as identity element, and moreover every subgroup G of S containing e is in fact a subgroup of G_e .*

Proof. To prove the first assertion, it clearly suffices to show that, given any $a \in G_e$, we can find an inverse for a in G_e ; and (e being idempotent) this is immediate, since $(\alpha), (\beta)$ for a and any corresponding b imply that $ebe \in G_e$, so that ebe is the inverse of a in G_e .

For the second assertion, we have only to note that e must be the identity of any subgroup G in which it lies, so that $(\alpha), (\beta)$ are immediate for all $a \in G$, as required.

COROLLARY 7. *The maximal subgroups of S are precisely the subgroups G_e with e idempotent.*

We next have

THEOREM 7. *Given any element x of a semigroup S and any positive integer m , then the statement*

(1) x is a pseudo-invertible element of S with index at most m is equivalent to

(2) there is an idempotent $e \in S$ such that $ex = xe \in G_e$ and $x^m \in G_e$.

Proof. To see that (1) implies (2), we mention first that (i) and (iii) of the definition of pseudo-invertibility imply that $e = xc = cx$ is idempotent. Also, by (i), $ex = xe$ and $(ex)e = e(ex) = ex$, while (iii) gives $(ex)c = c(ex) = e$; hence $ex = xe \in G_e$. Similarly, (ii) becomes $x^m = x^m e$, so that $x^m e = ex^m = x^m$, while (i) and (iii) give $x^m c^m = c^m x^m = e$, whence $x^m \in G_e$ and (2) follows.

Conversely, given (2), let c denote the inverse of $ex = xe$ in the group G_e . Then $ce = ec = c$ and $cex = xec = e$, whence $cx = xc = e$ and $c = ce = c^2 x$, which are (i) and (iii). Finally, if $x^m \in G_e$, then we have $x^m = x^m e = x^{m+1} c$, which is (ii).

COROLLARY 8. *An element x of S is pseudo-invertible with $i(x) = 1$ if and only if x belongs to some maximal subgroup of S .*

References

1. R. Arens and I. Kaplansky, Topological representation of algebras, *Trans. Amer. Math. Soc.*, vol. 63, 1948, pp. 457–481.
2. G. Azumaya, Strongly π -regular rings, *J. Fac. Sci. Hokkaido Univ.*, vol. 13, 1954, pp. 34–39.
3. M. P. Drazin, Algebraic and diagonal rings, *Canad. J. Math.*, vol. 8, 1956, pp. 341–354.
4. I. Kaplansky, Topological representation of algebras II, *Trans. Amer. Math. Soc.*, vol. 68, 1950, pp. 62–75.
5. E. H. Moore, *General Analysis* (Mem. Amer. Philos. Soc., vol. 1, Philadelphia, 1935); especially p. 8 and Chapter 3, Section 29 of Part 1.
6. R. Penrose, A generalized inverse for matrices, *Proc. Cambridge Philos. Soc.*, vol. 51, 1955, pp. 406–413.
7. ———, On best approximate solutions of matrix equations, *Proc. Cambridge Philos. Soc.*, vol. 52, 1956, pp. 17–19.
8. R. Rado, Note on generalized inverses of matrices, *Proc. Cambridge Philos. Soc.*, vol. 52, 1956, pp. 600–601.
9. T. Skolem, *Nordisk Mat. Tidskr.*, vol. 5, 1957, pp. 113–114.
10. A. H. Clifford, Semigroups admitting relative inverses, *Ann. of Math.*, vol. 42, 1941, pp. 1037–1049.

ACKNOWLEDGMENT

At the time of publication, the author of *Solution of a ranking problem from binary comparisons*, this MONTHLY, vol. 64, No. 8, Part II, October, 1957, was unaware of the work of R. A. Bradley and M. E. Terry along similar lines. Had he known of this, he would have made reference to their paper, *The rank analysis of incomplete block designs I; The method of paired comparisons*, *Biometrika*, vol. 39, Parts 3 and 4, December, 1952, both in the body of the text and in the bibliography.