Canad. Math. Bull. Vol. **19** (1), 1976

A PROOF OF JACOBSON'S THEOREM

BY
S. W. DOLAN

ABSTRACT. Let R be a ring such that, for each element a of R, there exists a positive integer $n(a)>1$, depending on a, such that $a^{n(a)}=a$. Jacobson proved that such a ring R is necessarily commutative and the purpose of this paper is to give a proof of Jacobson's Theorem that does not involve the use of the axiom of choice.

We take this opportunity to point out that all rings are assumed to be associative and that nothing beyond elementary ring theory is assumed in the proof to follow. Such ring theory can be found, for example, in [1].

1. **A preliminary lemma.** In [1] Jacobson's Theorem is proved for division rings and the following lemma is really just an observation that certain ideas in this proof in fact apply to the more general situation that we are about to consider.

LEMMA 1. *Let the finite field J be isomorphic to a subring of the ring R, henceforth we shall consider J and this subring to be identified. If a is an element of J but not of $Z(R)$ then there is an element b of R such that $ba-ab=sb\neq 0$, for some element s of J.*

Proof. Let J have order $q=p^m$ for some prime p. Define maps from R into itself by $T_a(x)=xa-ax$ and by $sI(x)=sx$, for any s in J.

Then each sI commutes with T_a and, by induction on k, we obtain $T_a^k(x)=xa^k-\binom{k}{1}axa^{k-1}+\cdots+(-1)^k a^k x$ for any positive integer k and any element x of R. In particular we obtain $T_a^q=T_a$. However, in $J[t]$, $t^q-t=\prod_{s\in J}(t-s)$ and so $\prod_{s\in J}(T_a-sI)=0$ on R.

Suppose the conclusion of Lemma 1 to be false i.e. for any elements s of J and c of R, $(T_a-sI)(c)=0$ only if $T_a(c)=0$. Then in the equation $\prod_{s\in J}(T_a-sI)=0$ we can successively replace each T_a-sI by T_a, obtaining $T_a^q=0$ and contradicting the fact that $T_a^q=T_a\neq 0$. This contradiction proves that the conclusion of Lemma 1 does indeed hold.

2. **Proof of main result.** R shall henceforth denote a *Jacobson ring* i.e. a ring such that for each element a of R there is an integer $n(a)>1$ such that $a^{n(a)}=a$.

Received by the editors November 23, 1973 and, in revised form, March 15, 1974.

https://doi.org/10.4153/CMB-1976-007-9 Published online by Cambridge University Press

Furthermore, for each element a of R, we shall denote $a^{n(a)-1}$ by $\bar{a}$ and $(n(a)-1)\times(n(2a)-1)+1$ by $m(a)$.

First we shall prove the following elementary result.

LEMMA 2. *For each element a of R, $\bar{a}$ is a central idempotent.*

Proof. $\bar{a}$ is trivially an idempotent and so, for any element b of R, $(\bar{a}b-\bar{a}b\bar{a})^2=0$ and hence $\bar{a}b=\bar{a}b\bar{a}$. Thus, by symmetry, $\bar{a}b=b\bar{a}$ for any element b of R and the result is proved.

For the remaining steps of the proof it will be convenient to introduce the following notation.

Suppose that k is a positive integer and that a is an element of R, then ka will denote $a+\cdots+a$, the sum having k terms.

If a is an element of R that is not in $Z(R)$ we define $X(a)$ to be $\{\sum_{i=1}^{n(a)-1} l_i a^i \mid 1\le l_i\le 2^{m(a)}-2\}$ and, if the elements a and b of R satisfy $ba=sb\neq ab$, for some element s of $X(a)$, we define $X(a, b)$ to be $\{\sum_{i=1}^{n(a)-1}\sum_{j=1}^{n(b)-1} l_{ij}a^ib^j \mid 1\le l_{ij}\le 2^{m(a)}-2\}$.

LEMMA 3. *Let a be any element of R that is not in $Z(R)$, then $X(a)$ is a finite commutative subring of R with identity element $\bar{a}$. Furthermore, for some element u of R, $X(u)$ is a field.*

Proof. First we observe that $a^{m(a)}=a$ and $(2a)^{m(a)}=2a$, and so $(2^{m(a)}-2)a=0$, with $m(a)>1$. Hence the finite subset $X(a)$ of R is closed under both multiplication and addition and is therefore a subring of R. Furthermore, $X(a)$ is clearly commutative with identity element $\bar{a}$.

Suppose that $x\neq 0$ is a non unit of $X(a)$ and let b be any element of R such that $ba-ab\neq 0$. We now have two cases to consider.

If $(\overline{ba-ab})x=0$, let $u=(\overline{ba-ab})a$ and $v=(\overline{ba-ab})b$, then $vu-uv=ba-ab\neq 0$. Whereas, if $(\overline{ba-ab})x\neq 0$, then $\bar{x}(ba-ab)\neq 0$ and so, letting $u=\bar{x}a$ and $v=\bar{x}b$, we have $vu-uv=\bar{x}(ba-ab)\neq 0$.

Thus, in either case, $X(u)$ exists and is $\{(\overline{ba-ab})r \mid r\in X(a)\}$ or $\{\bar{x}r \mid r\in X(a)\}$ respectively. Then in the natural map from $X(a)$ to $X(u)$, units map onto units, 0 onto 0 and x onto either 0 or a unit. Hence $X(u)$ has less non units than $X(a)$.

Repeating this procedure, if necessary, we eventually obtain a division ring of the desired form, completing the proof of Lemma 3.

The method of proof of Lemma 3 also yields the following result.

LEMMA 4. *If $X(a, b)$ exists, for some elements a and b of R, then it is a finite subring of R with identity element $\bar{a}\bar{b}$. Furthermore, for some elements u and v of R, there is a division ring of the form $X(u, v)$.*

Proof. If $X(a, b)$ exists, i.e. if $ba=sb\neq ab$ for some element s of $X(a)$, then it is a finite subset of R closed under both multiplication and addition and is therefore a subring of R. Furthermore, $\bar{a}\bar{b}$ is clearly an identity element.

Suppose that $x \neq 0$ is a non unit of $X(a, b)$. Let $u = (\overline{ba-ab})a$ and $v = (\overline{ba-ab})b$ or $u = \bar{x}a$ and $v = \bar{x}b$ depending upon whether $(\overline{ba-ab})x = 0$ or not, respectively. Then, as in Lemma 3, $X(u, v)$ exists and has less non units than $X(a, b)$.

Repeating this procedure, if necessary, we eventually obtain a division ring of the desired form, completing the proof of Lemma 4.

JACOBSONS THEOREM. *Any Jacobson ring is commutative.*

Proof. Let R be any Jacobson ring and suppose that R is not commutative. By Lemma 3 there is an element a of R such that $X(a)$ exists and is a finite field.

Then, by Lemma 1, there is an element b of R such that $X(a, b)$ exists. Hence, by Lemma 4, there are elements u and v of R such that $X(u, v)$ exists and is a division ring. Then, by Wedderburn's Theorem [1], $X(u, v)$ is a field, contradicting the fact that it is not commutative by definition.

Hence R is commutative and the result is proved.

REFERENCE

1. I. N. Herstein, *Topics in Algebra*, Ginn Blaisdell, 1964.

OXFORD UNIVERSITY,
OXFORD, ENGLAND.