A GENERALIZATION OF WEDDERBURN'S THEOREM[1]

D. L. OUTCALT AND ADIL YAQUB

Wedderburn's Theorem, asserting that a finite division ring is necessarily commutative, has been generalized in several directions [2]. Our present object is to establish the following additional generalization.

THEOREM 1. *Suppose R is any associative ring with Jacobson radical J such that R/J is a finite ring with exactly q elements. Suppose also that* (i) *R/J is a division ring,* (ii) *$J^2=(0)$, and* (iii) *the number of distinct qth powers of all elements of R is at most q. Then R is commutative.*

PROOF. For any x in R, let $\bar{x}=x+J$. First, observe that $x^q \equiv y^q \pmod{J}$ if and only if $\bar{x}^q=\bar{y}^q$ which, in turn, is equivalent .to $\bar{x}=\bar{y}$, or $x\equiv y \pmod{J}$. Hence there are at least q *distinct* qth powers of elements of R. Thus, by (iii), there are exactly q distinct qth powers of elements of the ground ring R. It further follows that

$$x \equiv y (\text{mod } J) \text{ implies } x^q = y^q. \tag{1}$$

For, otherwise, there would be more than q distinct qth powers of elements of R, since $x\not\equiv y \pmod{J}$ implies $x^q\not\equiv y^q \pmod{J}$.

Now, let $a\in J$ and let $b\in R$. Then $\bar{b}^q=\bar{b}$ and hence $b^q-b\in J$. Therefore, by (ii), we have

$$a(b^q - b) = 0, \quad (b^q - b)a = 0 \quad (a \in J,\ b \text{ arbitrary}). \tag{2}$$

Again, let $a\in J$. Since $J^2=(0)$, by (ii), therefore

$$(ab + b)^q = ab^q + bab^{q-1} + b^2ab^{q-2} + \cdots + b^{q-1}ab + b^q, \tag{3}$$

$$(ba + b)^q = b^qa + bab^{q-1} + b^2ab^{q-2} + \cdots + b^{q-1}ab + b^q. \tag{4}$$

We have thus shown that

$$(ab + b)^q - (ba + b)^q = ab^q - b^qa \qquad (a \in J,\ b \text{ arbitrary}). \tag{5}$$

Moreover, $a\in J$ implies $ab+b\equiv ba+b \pmod{J}$, and hence, by (1),

$$(ab + b)^q = (ba + b)^q \qquad (a \in J,\ b \text{ arbitrary}). \tag{6}$$

Now, an easy combination of (2), (5), (6), shows that

Received by the editors April 22, 1966.

[1] The research of the first author was supported by Air Force Office of Scientific Research Grant AFOSR 698-65, and the research of the second author was supported by National Science Foundation Grant GP-4163.

$$(7) \qquad a \in J \quad \text{implies } a \text{ is in the center of } R.$$

To complete the proof of the theorem, let $x, y \in R$, and in view of (7), we may (and shall) assume $x \notin J$, $y \notin J$. Now, by hypothesis, R/J is a finite division ring and hence, by Wedderburn's Theorem, R/J is a finite commutative field. Therefore, the multiplicative group of nonzero elements of R/J is cyclic [1, p. 317]. Let $\bar{\xi}$ be a generator for R/J. Then, for some integers i, j and some $a, a' \in J$, we have

$$(8) \qquad x = \xi^i + a, \quad y = \xi^j + a' \qquad (a \in J,\ a' \in J).$$

Hence, by (7), (8), $xy = yx$, and the theorem is proved.

Note that the case $J = (0)$ of Theorem 1 yields Wedderburn's Theorem.

Next, we prove that, in the presence of (i) and (ii), condition (iii) is indeed equivalent to commutativity.

THEOREM 2. *Suppose R, J, and R/J are as in Theorem* 1, *and suppose that* (i) *and* (ii) *of Theorem* 1 *hold. Then R is commutative if and only if* (iii) *of Theorem* 1 *holds.*

PROOF. Suppose R is a *commutative* ring with Jacobson radical J such that R/J has exactly q elements. Suppose also that (i) and (ii) hold. In view of Theorem 1, we will be through if we can show that (iii) holds. Now, it is well known that the number q of elements in the finite field R/J satisfies: $q = p^k$, p the characteristic of R/J, p prime. Suppose $x \equiv y \pmod{J}$, and suppose for the moment $x \not\equiv 0 \pmod{J}$. Then $x = \xi^i + a$, $y = \xi^i + a'$, for some a, a' in J, and where $\bar{\xi}$ is a generator for R/J. Hence, $x^q = (\xi^i + a)^{p^k} = \xi^{ip^k}$ and $y^q = (\xi^i + a')^{p^k} = \xi^{ip^k}$. This follows since R is commutative, $J^2 = (0)$, and $p\xi \in J$ (since $p\bar{\xi} = \bar{0}$). We have thus shown that $x \equiv y \not\equiv 0 \pmod{J}$ implies $x^q = y^q$. As this holds trivially if $x \equiv y \equiv 0 \pmod{J}$ (since $J^2 = (0)$), we have $x \equiv y \pmod{J}$ implies $x^q = y^q$, and thus (iii) is verified. This proves the theorem.

We now show that Theorem 1 is not necessarily true if any one of the hypotheses (i), (ii), or (iii) is deleted. To this end, consider the following examples.

EXAMPLE 1. Any complete matrix ring R over $\mathrm{GF}(p^k)$ satisfies (ii) and (iii) but does not satisfy (i). Since R is not commutative, the hypothesis (i) in Theorem 1 cannot be deleted.

EXAMPLE 2. The direct sum of $\mathrm{GF}(2^2)$ with the subring R of 3×3 matrices consisting of the strictly upper triangular matrices with entries in $\mathrm{GF}(2)$ satisfies (i) and (iii) but does not satisfy (ii). Since R is not commutative, the hypothesis (ii) in Theorem 1 cannot be deleted.

EXAMPLE 3. The subring R of 2×2 matrices over GF(2) defined by

$$R=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix}\right\}$$

satisfies (i) and (ii) but does not satisfy (iii). Since R is not commutative, the hypothesis (iii) in Theorem 1 cannot be deleted.

Moreover, we remark that the hypothesis "$J^2=(0)$" in Theorem 1 cannot in general be replaced by the weaker hypothesis "$J^n=(0)$ for some $n>2$". Indeed, observe that for the ring given in Example 2 above, we have $J^n=(0)$ for every $n>2$.

Finally, note that Theorems 1 and 2 apply to infinite rings and to rings without identity. An example is furnished by taking the direct sum of the ring of integers mod p^2 (p prime) with an infinite number of copies of R_0, where R_0 is any ring of characteristic p which, in addition, is a zero ring. This ring, of course, is of characteristic p^2 and has no identity.

REFERENCES

1. I. N. Herstein, *Topics in algebra*, Blaisdell, New York, 1964.

2. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. 37, American Mathematical Society, Providence, R. I., 1964.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA