A THEOREM ON RINGS

HISAO TOMINAGA

It is a well-known theorem of Jacobson that *if every element* x *of a ring* R *satisfies a relation* $x^{n(x)}-x=0$ *where* $n(x)>1$ *is an integer, then* R *is commutative.* Recently, in his paper [3], I. N. Herstein has generalized Jacobson's theorem as follows : *Let* R *be a ring in which* $[x, y]^{n(x,y)}-[x, y]=0$ *for each* $x, y\in R$ *where* $n(x, y)>1$ *is an integer and* $[x, y]=xy-yx$. *Then* R *is commutative.* On the other hand, in [2], he proved also that *if there exists an integer* $n>1$ *such that every* x^n-x $(x\in R)$ *is contained in the center of* R, *then* R *is commutative.* Corresponding to [3], we shall introduce here the notion of C-rings : A ring R is called a *C-ring* if there exists an integer $n>1$ for which every $[x, y]^n-[x, y]$ $(x, y\in R)$ is contained in the center of R.

As one can easily see, there exists a non-commutative ring R with $R^3=0$.[1] This fact will show that a C-ring is not always commutative. However, in what follows, one will see that if R is a C-ring then each commutator is a central nilpotent element.

We shall begin our study with the following lemma whose proof proceeds just as in that of [1, Theorem 2].[2]

Lemma 1. *If* R *is a semi-prime ring*[3] *satisfying a polynomial identity of degree* n *whose every coefficient is either* 1 *or* -1, *then* R *is a subring of the complete direct sum of central simple algebras of rank* $\leqq\left[\frac{n}{2}\right]^2$.

Corollary 1. *Let* R *be semi-prime. If every* $[x, y]$ $(x, y\in R)$ *is contained in the center of* R *then* R *is commutative.*

Proof. Since $[[x, y], w]=0$ for each $x, y, w\in R$, R satisfies a polynomial identity of degree 3 with coefficients ± 1. By Lemma 1, R is a subring of the complete direct sum of S_α's where S_α is a central simple algebra of rank $\leqq\left[\frac{3}{2}\right]^2=1$, that is a field. Hence R is commutative.

Lemma 2. *A division ring* R *which is a C-ring is commutative.*

Proof. Let Z be the center of R. If every $[x, y]$ is in Z then $R=Z$ by Corollary 1. Thus, we shall suppose that there exists some $u=[a, b]$

---

1) Let D be a non-commutative division ring. Then $R=\left\{\begin{pmatrix}0&0&0\\a&0&0\\b&c&0\end{pmatrix}\middle|\, a, b, c\in D\right\}$ is an example of this type.

2) Cf. [5, p. 215].

3) R is said to be semi-prime if the lower nil radical of R is 0 (cf. [4, p. 194]).

not contained in Z. Since $zu = [za, b]$ for each $z \in Z$, there holds $(zu)^n - zu \in Z$. Combining this with $u^n - u \in Z$, we obtain $(z^n - z)u \in Z$. And then, $u \notin Z$ implies that $z^n - z = 0$. Hence we see that Z is a finite field $GF(q)$. Now let $f(\alpha)$ be a minimal polynomial of u over Z. Then, noting that $z^q = z$ for all $z \in Z$, we have $0 = \{f(u)\}^q = f(u^q)$. Hence, by [4, p. 151], there exists an $r \in R$ such that $u^q = rur^{-1}$, that is, $u^q r = ru$. Consequently, $[r, u]u = u^q[r, u]$, and $u^q \neq u$ implies $v = [r, u] \neq 0$. Noting that $u^n - u \in Z$, $v^n - v \in Z$ and $vu = u^q v$, one will readily see that $\{\sum_{i,j=0}^{n-1} z_{ij} u^i v^j \mid z_{ij} \in Z\}$ is a finite field. Accordingly, we have $uv = vu$, but this contradicts $u^q \neq u$.

Lemma 3. *Let R be a prime C-ring. If $x^m = 0$ then $x = 0$, and if $e^2 = e$ then $e = 0$ or 1 (if exists).*

Proof. If $x^m = 0$, without loss of generality, we may restrict our proof to the case $m = 2$. Since $xrx = [xr, x]$ for every $r \in R$, $-xrx = (xrx)^n - xrx$ is contained in the center Z of R, whence it follows $xRx \subseteq Z$. Hence we have $(Rx)^3 = R(xRx)Rx = R^2 xRx^2 = 0$. And then, R being prime, x must be 0. Next, let $e^2 = e$. Then $(ere - er)^2 = 0 = (ere - re)^2$ for every $r \in R$, from which we have $ere - er = 0 = ere - re$ by the fact proved above. We obtain therefore $e \in Z$. Our second assertion will be readily seen from the fact $eR \cdot A = 0$ where $A = \{er - r \mid r \in R\}$.

The next will be almost trivial.

Lemma 4. *If R is a C-ring then so is each homomorphic image of a subring of R.*

Lemma 5. *A primitive C-ring R is commutative.*

Proof. In virtue of Lemma 2, it suffices to show that R is a division ring. In fact, if R is not a division ring then, by [4, Theorem 2. 4. 3], there exists an integer $m > 1$ and a division ring D such that the complete $m \times m$ matrix ring over D is a homomorphic image of a subring of R, which is a C-ring by Lemma 4. But this contradicts Lemma 3.

Corollary 2. *A semi-simple C-ring is commutative.*

Lemma 6. *Let R be a C-ring with the center Z. Then every $[x, y]$ is contained in Z.*

Proof. Evidently, by Corollary 2, $u = [x, y]$ is contained in the radical N of R. If $z \in N \cap Z$ then $(z^n - z)u$ is contained in Z (cf. the proof of Lemma 2), that is, $(z^n - z)[u, r] = 0$ for all $r \in R$. Since $z \in N$, we have $z[u, r] = 0$.[4] Setting here particularly $z = u^n - u$, we obtain $(u^n - u)[u, r] = 0$. Recalling again $u \in N$, we obtain $u[u, r] = 0$. Similarly we have $[u, r]u = 0$. From these, one will readily see that $u^2 r = ru^2$, that

4) $(z^{n-1} - 1)$ operates formally as a regular element.

is, $u^2 \in Z$. Then, in case n is even, $u^n - u \in Z$ yields at once $u \in Z$. On the other hand, in case n is odd, $u^{n-1}r - r = ru^{n-1} - r$ for every $r \in R$, whence we have $r(u^n - u) = (u^n - u)\, r = u(ru^{n-1} - r)$. Hence, $u^{n-1} - 1$ operating as a regular element, we have eventually $ur = ru$.

Now we can prove our principal theorem.

Theorem 1. *If R is a C-ring then every $[x, y]$ is a central nilpotent element.*

Proof. Let N_0 be the lower nil radical of R. Since every $[x, y]$ is contained in the center of R by Lemma 6, Corollary 1 shows that $[x, y]$ is contained in N_0 which is a nil ideal.

Let R be a ring with the center Z. R is called a *C'-ring* if for each $x, y \in R$ there exists an integer $n(x, y) > 1$ such that $[x, y]^{mn(x,y)} - [x, y]^m \in Z$ for all natural numbers m. If for every $x, y \in R$ there exists an integer $n(x, y)$ such that $[x, y]^{n(x,y)} - [x, y] = 0$, then R is a C'-ring of course. Theorem 1 is true also for C'-rings. To see this, we shall prove here two essential lemmas which correspond to Lemma 2 and Lemma 6 respectively.

Lemma 2′. *A division ring R which is a C'-ring is commutative.*

Proof. As in the proof of Lemma 2, we shall suppose that $u = [a, b]$ is not contained in the center Z. Since $zu = [za, b]$ for all $z \in Z$, there holds $(zu)^{nn(z)} - (zu)^n \in Z$ where $n = n(a, b)$ and $n(z) = n(za, b)$. Noting that $u^{n(z)n} - u^{n(z)} \in Z$, $u^n - u \in Z$ and $(zu)^{n(z)} - zu \in Z$, we can readily see $(z^{(n-1)(n(z)-1)} - 1)\, z^n u \in Z$. And then, $u \notin Z$ implies $(z^{(n-1)(n(z)-1)} - 1)\, z^n = 0$. Hence Z must be of characteristic $p \neq 0$, and algebraic over its prime field P. Now let $f(\alpha) = \alpha^t + z_1\alpha^{t-1} + \dots + z_t (z_i \in Z)$ be a minimal polynomial of u over Z. Evidently, $W = P(z_1, \dots, z_t)$ is a finite field, say, $GF(q)$. Hence, as in the proof of Lemma 2, we can find some non-zero $r \in R$ such that $v = [r, u] \neq 0$ and $vu = u^q v$. Now, recalling that $v^m = v + z'$ for some $m > 1$ and $z' \in Z$, one will easily see that the set $\{\sum_{i=0}^{t-1} \sum_{j=0}^{m-1} z_{ij}\, u^i v^j \mid z_{ij} \in W(z')\}$ is a finite field. Accordingly, $uv = vu$ of course, but this contradicts $u^q \neq u$.

Lemma 6′. *Let R be a C'-ring with the center Z. Then every $[x, y]$ is contained in Z.*

Proof. Evidently, $u = [x, y]$ is contained in the radical N of R by the fact corresponding to Corollary 2. If $z \in N \cap Z$, then $(z^{(n-1)(m-1)+1} - z)z^{n-1}u \in Z$ where $n = n(x, y)$ and $m = n(zx, y)$ (cf. the proof of Lemma 2′), that is, $(z^{(n-1)(m-1)+1} - z)z^{n-1}[u, r] = 0$ for all $r \in R$. Since $z \in N$, we have $z^n[u, r] = 0$. Setting here particularly $z = u^n - u (\in N \cap Z)$, we obtain $(u^n - u)^n[u, r] = 0$. Noting again $u \in N$, it follows $u^n[u, r] = 0$.

Similarly, we have $[u, r]u^n = 0$. From these, one will readily see that $u^{2n}r = u^n r u^n = r u^{2n}$, whence $u^{2n} \in Z$. Further $u^{2n} - u^2 \in Z$ yields $u^2 \in Z$. Hence, as in the proof of Lemma 6, we obtain eventually $u \in Z$.

We have proved therefore

Theorem 2. *The following conditions are equivalent to each other*:

(1) *R is a C-ring.*

(2) *R is a C'-ring.*

(3) *Every* $[x, y]$ $(x, y \in R)$ *is contained in the center of R* (*and nilpotent*).

Corollary 3 (Herstein). *If* $[x, y]^{n(x,y)} - [x, y] = 0$ *for each* $x, y \in R$ *where* $n(x, y) > 1$ *is an integer then R is commutative.*

Proof. Noting that $[x, y]^{n(x,y)-1}$ is an idempotent, our assertion is evident from Theorem 2.

REFERENCES

[1] S. A. AMITSUR, An embedding of PI-rings, Proc. Amer. Math. Soc., 3 (1952) 3—9.
[2] I. N. HERSTEIN, A generalization of a theorem of Jacobson, Amer. J. Math., 73 (1951) 756—762.
[3] I. N. HERSTEIN, A condition for the commutativity of a ring, Can. J. Math., 10 (1958) 583—586.
[4] N. JACOBSON, Structure of rings, Amer. Math. Soc. Colloq. Publ., 37 (1956)
[5] T. NAKAYAMA and G. AZUMAYA, Algebra II (Theory of Rings), Tokyo, lwanami (1954), (in Japanese).

DEPARTMENT OF MATHEMATICS,
HOKKAIDO UNIVERSITY

(*Received April 20, 1959*)