TAMKANG JOURNAL OF MATHEMATICS
Volume 21, Number 2, Summer 1990

ON A THEOREM OF HERSTEIN
DEDICATED TO PROFESSOR SHIH-TONG TU ON HIS 60TH BIRTHDAY

CHEN-TE YEN

Abstract. Let R be an associative ring with identity such that for some fixed integer $m > 1$, $(x+y)^m = x^m + y^m$ for all x, y in R. If $m \equiv 2 \pmod 4$, or $p-1|m-1$ for each prime factor p of m, then R is commutative. The restriction on m is essential. Moreover, in case of $m \equiv 2 \pmod 4$ and $m > 2$, then R is isomorphic to a subdirect sum of subdirectly irreducible rings R_i each of which, as homomorphic images of R, satisfies the same polynomial identity $(x+y)^m = x^m + y^m$; and for each x in R_i, either $x^2 = 0$ or $x^{2q} = 1$, where $(q, m) = 1$.

1. Introduction.

In [3], Johnsen, Outcalt, and Yaqub proved that $m = 2$ is the unique integer such that the following is true: if R is an associative ring with identity in which for some fixed integer $m > 1$, $(xy)^m = x^m y^m$ for all x, y in R, then R is commutative. When the multiplicative equality is replaced by additive one, then we ask that for what integers m that can force R to be commutative? In this paper, we find all such integers m that can imply the commutativity of R.

From now on, R will be an associative ring. In [1], Herstein proved.

Theorem A. *Let R be a ring in which for some fixed integer $m > 1$, $(x+y)^m = x^m + y^m$ for all x, y in R. Then every commutator in R is nilpotent, and the nilpotent elements of R form an ideal.*

In general, R is not necessarily commutative in Theorem A; if R has no identity or the mapping $x \to x^m$ in R is not onto, then for each such integer $m > 1$, we can easily find an example which shows that R is not commutative. Let R be a ring with identity 1. We shall denote the commutator $xy - yx$ in R by $[x, y]$, the center of R by z, the Jacobson radical of R by J, the group of units of R by R^*, and the set of all positive integers by N. For all n, m in N, we denote the greatest common divisor of n and m by (n, m).

To obtain our results, we need the following lemma which can be found for example in [5].

Received December 20, 1988; revised June 26, 1989.
1980 *Mathematics Subject Classification* (1985 Revision). Primary 16A70.
Key words and phrases. Subdirect sums, subdirectly irreducible rings.

Lemma A. *Let R be a ring with identity 1, and let $f : R \to R$ be a function such that $f(x+1) = f(x)$ holds for all $x \in R$. If for all $x \in R$, there exists a positive integer n such that $x^n f(x) = 0$, then necessarily $f(x) = 0$ for all $x \in R$.*

2. Main Results

We have our first main.

Theorem 1. *Let R be a ring with identity 1 such that for some fixed integer $m > 1$, $(x+y)^m = x^m + y^m$ for all x, y in R. If $m \equiv 2 \pmod 4$; or $m = p^i n$, where p is any odd prime divisor of m, and i and n are in N, and $n > 1$ is odd, and the multiplicative order of j does not divide $n-1$ for some $j \neq 0, 1$, and $j \in GF(p)$, the Galois field with p elements, then R is commutative.*

To prove Theorem 1, we need the following lemmas.

Lemma 1. *If $m \equiv 2 \pmod 4$, then R is commutative.*

Proof. Note that $2 = 1^m + (-1)^m = (1-1)^m = 0$, Hence, char $R = 2$. If $m = 2$, then $(x+y)^2 = x^2 + y^2$ for all x, y in R, and so $xy = -yx = yx$. Thus, let $m = 2k$, where $k \in N$ is odd and $k > 1$.

By hypotheses, we get $1 + x^m = (1+m)^m = \{(1+x)^2\}^k = \{(1+x^2)\}^k$ for all x in R. This implies that

$$x^2 + \sum_{i=2}^{k-1} \binom{k}{i} (x^2)^i = x^2 f(x) = 0 \text{ for all } x \text{ in } R, \tag{1}$$

$$\text{where } f(x) = 1 + \sum_{i=1}^{k-2} \binom{k}{i+1} (x^2)^i.$$

Note that for $x \in R$, $f(x) = 0$ implies that x is invertible. By Theorem A, every commutator $[x, y]$ in R is nilpotent. Let $[x, y]^j = 0$. If $j > 2$, then replacing x by $[x, y]$ in (1) and left-multiplying by $[x, y]^{j-3}$, we have that $[x, y]^{j-1} = 0$. Hence, continuing in this manner, we finally obtain that

$$[x, y]^2 = 0 \text{ for all } x, y \text{ in } R. \tag{2}$$

Thus, by (2) we get

$$(xy)^m - (yx)^m = [x, y]^m = 0 \text{ for all } x, y \text{ in } R. \tag{3}$$

Let $u = [x, y]$. Then by (2) and (3) we get $\{(1+u)z(1+u)\}^m = \{(1+u)^2 z\}^m = z^m$, and so $uz^m = z^m u$ for all z in R. Hence, we get

$$[x, y] z^m = z^m [x, y] \text{ for all } x, y, z \text{ in } R. \tag{4}$$

Claim 1. For $x, y \in R$, $xy = 0$ implies $yx = 0$.

Assume that $xy = 0$. Then replacing z by x in (4), we have $-yx^{m+1} = 0$. Thus, using (1) repeatedly, we finally obtain that $yx^2 = 0$. Similarly, we get $y^2x = 0$. By induction and using $xy = yx^2 = y^2x = 0$, we can easily show that $(x+y)^{2i} = x^{2i} + y^{2i}$ for all integers $i \geq 2$. Hence, using this equality and (1) we have

$$\begin{aligned} 0 &= (x+y)^2 + \sum_{i=2}^{k-1} \binom{k}{i} (x+y)^{2i} \\ &= yx + \sum_{i=1}^{k-1} \binom{k}{i} x^{2i} + \sum_{i=1}^{k-1} \binom{k}{i} y^{2i} \\ &= yx. \end{aligned}$$

By Birkhoff's Theorem [4, p. 55], every ring is isomorphic to a subdirect sum of subdirectly irreducible rings. Thus, we may assume that R is a subdirectly irreducible ring. Henceforth, R is a subdirectly irreducible ring. Let H be the heart of R, i.e., the smallest nonzero ideal of R. Let A denote the set of all zero divisors of R (together with 0). Then A is a proper subset of R.

Claim 2. A is an ideal of R, and $A = Ann(H) = \{x \mid x \in R, xH = 0\}$.

By Claim 1 there is no distinction between left and right zero divisors in R, and for any nonempty subset S of R, the left and right annihilator of S coincide and form a two sided ideal of R, which we denote by $Ann(S)$. Clearly, $Ann(H) \subseteq A$. Conversely, let a be any element in A. Since $Ann(a)$ is a nonzero dieal of R, it contains H. This means that $a \in Ann(H)$. Thus, $A = Ann(H)$ and so A is an ideal of R.

Claim 3. For each $x \in R$, either $x^2 = 0$ or $f(x) = 0$, where $f(x)$ is as in (1); in the latter case $x \in R^\star$.

If $f(x) \in A$, then by (1) and Claim 2 we see that $x^2 \notin A$. Thus by the definition of A and by (1) again, we get $f(x) = 0$ and so $x \in R^\star$.

If $f(x) \notin A$, then we have $x^2 = 0$ by (1) and so $x \in A$.

Since char $R = 2$, we get $x = (x+1) + 1$ for all x in R. If $x^2 = 0$, then $x + 1$ is invertible. Hence, by (2), Claim 2 and Claim 3 we have

Claim 4. R is generated by invertible elements, and $A = J = \{x \mid x \in R, x^2 = 0\}$, and R/J is a field.

Claim 5. For all $x \in R, x^m \in Z$.

Let $x, y \in R$. By Claim 3, either $y^2 = 0$ or y is invertible. If y is invertible, then by (3) we get $(yxy^{-1})^m = (y^{-1}yx)^m = x^m$ and so $yx^m = x^m y$. If $y^2 = 0$, then $(1+y)^2 = 1$ and by the result above we have $(1+y)x^m = x^m(1+y)$. Hence, $yx^m = x^m y$ and so $x^m \in Z$.

Claim 6. For all $x \in R, x^2 \in Z$.

By Claim 3, either $x^2 = 0$ or x is invertible for all x in R. If $x^2 = 0$, then $x^2 \in Z$ and we are done. Let x be invertible in R. By Claim 3 again, $f(x) = 0$. Then $GF(2)[x]$ is a finite ring. Thus, $x^i = x^j$ for some positive integers $i < j$, and so $x^n = 1$, where $n = j - 1$. Let $(m, n) = t, n/t = r$ and $m/t = s$. Then we get $(1 + x^r)^m = 1 + x^{mr} = 1 + x^{ns} = 0$ and so $(1 + x^r)^2 = 0$ by Claim 3. Hence, $x^{2r} = 1$. Continuing in this manner, we finally obtain $x^{2q} = 1$ for some $g \in N$ and $(g, m) = 1$. Since $(2q, m) = 2$, and by Claim 5, $x^m \in Z$, we conclude that $x^2 \in Z$.

Using Claim 6 and (2), and recalling char $R = 2$, we can easily show that $(xy)^2 = (yx)^2, (xy)^3 = y^3x^3$ and $(xy)^4 = x^4y^4$ for all x, y in R. Thus, using these equalities we can prove that $(x + y)^4 = x^4 + y^4$ for all x, y in R.

Using the above results, we have that

$$\begin{aligned}(xy + x)^m &= (xy)^m + x^m \\ &= x^{m-2}y^{m-2}(xy)^2 + x^m \\ &= x^{m-1}(y^{m-1}xy + x)\end{aligned}$$

and

$$\begin{aligned}(xy + x)^m &= \{x(y + 1)\}^{m-2}\{x(y + 1)\}^2 \\ &= x^{m-2}(y + 1)^{m-2}\{x(y + 1)\}^2 \\ &= x^{m-1}\{(y + 1)^{m-1}xy + (y + 1)^{m-1}x\}, \text{ for all } x, y \text{ in } R.\end{aligned}$$

These two equalities are equal, and thus we get

$$x^{m-1}\{y^{m-1}xy + x + (y + 1)^{m-1}xy + (y + 1)^{m-1}x\} = 0 \text{ for all } x, y \text{ in } R. \tag{7}$$

Since $y^{m-1}y + 1 + (y + 1)^{m-1}y + (y + 1)^{m-1} = y^m + 1 + (y + 1)^m = 0$, by Lemma A, (7) implies that

$$y^{m-1}xy + x + (y + 1)^{m-1}xy + (y + 1)^{m-1}x = 0 \text{ for all } x, y \text{ in } R. \tag{8}$$

Replacing x by $(y + 1)x$ in (8), we have that

$$\begin{aligned}0 &= y^{m-1}(y + 1)xy + (y + 1)x + (y + 1)^m xy + (y + 1)^m x \\ &= y^m xy + y^{m-1}xy + yx + x + (y^m + 1)xy + (y^m + 1)x \\ &= y^{m-1}xy + yx + xy + y^m x.\end{aligned}$$

Hence, we get

$$(1 + y^{m-1})[x, y] = 0 \text{ for all } x, y \text{ in} = R. \tag{9}$$

Claim 7. $A \subseteq Z$.

For all $y \in A$, we get $y^{m-1} \in A$ by Claim 2. Since A is a proper ideal of R, we have $1 + y^{m-1} \notin A$. Thus, (9) implies that $[x, y] = 0$ for all x in R and so $y \in Z$.

Finally, for all y in R, we consider the following two cases:

Case 1. $1 + y^{m-1} \notin A$.

Then using (9), we have [x,y]=0 for all x in R.

Case 2. $1 + y^{m-1} \in A$.

Then $1+y^{m-1} \in Z$ by Claim 7. Hence for all x in R, we get $x(1+y^{m-1}) = (1+y^{m-1})x$ and so $xy^{m-1} = y^{m-1}x$. Thus, $y^{m-2}[x, y] = 0$ by Clsim 6. Since $1 + y^{m-1} \in A$, and $A = J$, we must have that $y \notin A$. Therefore, by Claim 3, $y^{m-2}[x, y] = 0$ implies that $[x, y] = 0$ for all x in R. This completes the proof Lemma 1.

Since $(1 + [x, y])^m = 1 + [x, y]^m$ for all x, y in R, by using Theorem A repeatedly we have for some positive integer $j = j(x, y)$, depending on x and y,

$$m^j [x, y] = 0 \text{ for all } x, y \text{ in } R. \tag{10}$$

In order to prove the Theorem 1, it is sufficient to do it for subdirectly irreducible rings. We henceforth assume that R is a subdirectly irreducible ring. Let $S \neq (0)$ be the intersection of the nonzero ideals of R. Of course, S is the unique minimal ideal of R. The argument of [2, p. 84] shows the following

Lemma 2. *There exists a prime p such that the characteristic of R is p.*

Proof. By hypothesis, we have $2 = 1^m + 1^m = (1+1)^m = 2^m$. Thus, every element of R is of finite additive order. Let p be a prime and $pa = 0$, for some $a \in R$ and $a \neq 0$. Let $R_p = \{x \in R \mid px = 0\}$. Then $R_p \neq (0)$ is clearly an ideal of R, and hence $R_p \supset S$. If $R_q \neq (0)$ for some prime $q \neq p$, then $R_q \supset S$. Since $S \subset R_q \cap R_p = (0)$, we would have a contradiction.

Now by hypothesis again, $p^m = p$ and so $p(p^{m-1} - 1) = 0$. Since $(p, p^{m-1} - 1) = 1$, by the result above we conclude that $R_p = R$.

Lemma 3. *If R is not commutative, then p divides m.*

Proof. Suppose the contrary. Then by (10) and Lemma 2, we have $[x, y] = 0$ for all x, y in R, a contradiction. Hence, p divides m.

We are now ready to prove Theorem 1.

Proof of Theorem 1. Suppose that R is not commutative. Using Lemma 1, we see that m is the latter case stated in Theorem 1. Then by Lemmas 2 and 3, $charR = p$ and p divides m for some odd prime p. Let $k \neq 0, 1$, and $k \in GF(p)$. By hypothesis, we have $k^m = k$. Since $(k, p) = 1$, applying Fermat's Little Theorem repeatedly, we get $k = k^m = (k^{p^i})^n = k^n$ and so $k^{n-1} = 1$. Thus, the multiplicative order of k divides $n - 1$, a contradiction. Hence, R is commutative. This completes the proof of Theorem 1.

In Theorem A, if we add the assumption that the mapping $x \to x^m$ in R is onto then R is commutative. This result shows that in Herstein's another theorem [1, Theorem 3], the multiplicative homomorphism can be eliminated. We have our second main

Theorem 2. *If R is a ring, not necessarily with identity, in which the mapping $x \to x^m$ for a fixed integer $m > 1$ is an additive homomorphism onto, then R is commutative.*

To prove Theorem 2, we need the following lemmas. Assume that all the hypotheses as in Theorem 2 are satisfied.

Lemma 4. *If $a \in R$ is nilpotent, and all $a^2, a^3, \ldots \in Z$, then*

$$(11) \quad ax^m - x^m a - ax^m a + a^2 x^m = (ax)^m - (xa)^m - (axa)^m + (a^2 x)^m \text{ for all } x \text{ in } R.$$

Proof. See [1, pp. 31-32].

Lemma 5. *If $a \in R$ and $a^2 = 0$, then $a \in Z$.*

Proof. Let $a \in R$ and $a^2 = 0$.

Replacing x by ax in (11), and using $a^2 = 0$, we have $-(ax)^m a = -(axa)^m = 0$ for all x in R. Thus, left-multiplying by a in (11) we get $-ax^m a = -a(xa)^m = -(ax)^m a = 0$ for all x in R. Since the mapping $x \to x^m$ in R is onto, we have

$$(12) \qquad axa = 0 \text{ for all } x \text{ in } R.$$

Hence by (12), $x^m + a^m = (x+a)^m$ implies that

$$x^{m-1}a + x^{m-2}ax + \cdots + xax^{m-2} + ax^{m-1} = 0,$$

and so

$$x\{x^{m-1}a + x^{m-2}ax + \cdots + xax^{m-2} + ax^{m-1}\} = \\ \{x^{m-1}a + x^{m-2}ax + \cdots + xax^{m-2} + ax^{m-1}\}x \text{ for all } x \text{ in } R.$$

Thus, we get $x^m a = ax^m$ for all x in R. Since the mapping $x \to x^m$ in R is onto, $a \in R$ results.

By Theorem A, every commutator $[x, y]$ in R is nilpotent. Applying Lemma 5, it is easy to show that the nilpotency index of $[x, y]$ is at most 3.

If $m = 2$, then $(x+y)^2 = x^2 + y^2$ implies that $xy = -yx$ and so $xy^2 = (-yx)y = (-y)xy = y^2 x$ for all x, y in R. Since the mapping $x \to x^2$ in R is onto, the commutativity of R results.

Henceforth, we assume that $m > 2$. By the result above, we have $[x, y]^m = 0$ for all x, y in R.

Lemma 6. *If $b \in R$ and $b^3 = 0$, then $b \in Z$.*

Proof. Let $b \in R$ and $b^3 = 0$.

Since $(b^2)^2 = 0, b^2 \in Z$ by Lemma 5. Replacing a by b in (11), and using the result above, we have that

$$\begin{aligned} bx^m - x^m b - bx^m b + b^2 x^m &= (bx)^m - (xb)^m - (bxb)^m + (b^2 x)^m \\ &= (bx - xb)^m - bxb^2xb(bxb)^{m-2} + b^4x^2(b^2x)^{m-2} \\ &= 0 \qquad \text{for all } x \text{ in } R. \end{aligned}$$

Thus, we get

$$\begin{aligned} 0 &= b(bx^m - x^m b - bx^m b + b^2 x^m) \\ &= b^2 x^m - bx^m b \end{aligned}$$

and so

$$bx^m = x^m b \qquad \text{for all } x \text{ in} R.$$

Since the mapping $x \to x^m$ in R is onto, $b \in Z$ results.

We are now ready to prove Theorem 2.

Proof of Theorem 2. Since $[x,y]^3 = 0$, by Lemma 6 $[x,y] \in Z$ for all x, y in R. The equality $[x,y]^m = 0$ implies that

$$0 = (xy)^m - (yx)^m = mx^{m-1}y^{m-1}[x,y] \qquad \text{for all } x, y \text{ in } R.$$

Hence, we have

$$x^m y^m - y^m x^m = m^2 x^{m-1} y^{m-1}[x,y] = 0 \qquad \text{for all } x, y \text{ in } R.$$

Since the mapping $x \to x^m$ in R is onto, so R is commutative. This completes the proof of Theorem 2.

3. Remark and example.

We end this paper with

Remark. In Herstein's Theorem 3 of [1], we do not know whether the additive endomorphism can be eliminated. It is easy to prove that in Theorem 1, all the stated values of m are essential as Examples 1 and 2 of [6] show. From those examples, we see that in Theorem 1 the equality can not be replaced by the weaker condition "$(x+y)^m - x^m - y^m \in Z$ for all x, y in R". Finally, because of the proof of Lemma 1, we ask in Lemma 1, when $m > 2$, whether R is a subdirect sum of R_0's, where R_0 is described in the following.

Example. Let R_0 be a ring with identity 1 and of characteristic 2 such that for all $x \in R_0$, either $x^2 = 0$ or $x^2 = 1$. Then R_0 is generated by invertible elements, and thus R_0 is commutative. It is easy to verify that $(x+y)^{2n} = x^{2n} + y^{2n}$ for all $x, y \in R_0$ and all $n \in N$.

Acknowledgement. The author thanks the referee for pointing out the error of the original proof of Claim 6 of Lemma 1.

Added in Proof. Theorem 2 is included in H. Tominaga's paper "Some commutativity conditions" Math. J. Okayama Univ. 29(1987), 191-192. The proof of Theorem 2 is different. The author thanks Professor Hisao Tominaga for pointing out an error $(2r, m) = 2$, which is in the proof of Lemma 1, Claim 6.

References

[1] I. N. Herstein, "Power maps in rings," *Michigan Math. J.*,8(1961), 29-32.

[2] I. N. Herstein, *Noncommutative rings,* Carus Math. Monographs, No. 15, Math. Assoc. of Amer., 1968.

[3] E. C. Johnsen, D. L. Outcalt and Adil Yaqub, "An elementary commutativity theorem for rings," *Amer. Math. Monthly,* 75(1968), 288-289.

[4] N. H. McCoy, *The theory of rings,* The Macmillan Company, New York, 1964.

[5] W. K. Nicholson and A. Yaqub, "A commutativity theorem for rings and groups," *Canad. Math. Bull.,* 22(1979), 419-423.

[6] C. T. Yen, "On the commutativity of primary rings," *Math. Japonica,* 25(1980), 449-452.

Department of Mathematics, Chung Yuan Christian University, Chung Li, Taiwan, 32023, Republic of China.