TAMKANG JOURNAL OF MATHEMATICS
Volume 28, Number 1, Spring 1997

ON A THEOREM OF YEN

THOMAS P. KEZLAN

Abstract. In [5] Yen showed that if R is an associative ring with unity and $m > 1$ is a fixed integer such that $m \equiv 2 (\mathrm{mod}\, 4)$ and $(x+y)^m = x^m + y^m$ for all x, y in R, then R must be commutative. In the present paper it is shown that commutativity is achieved even in the case where m is dependent on x and y.

In [1] Herstein showed that if R is a ring in which for some fixed integer $m > 1$, $(x+y)^m = x^m + y^m$ for all, x, y in R, then the commutator ideal of R is nil. In [5] Yen pursued this further and proved, under additional assumptions on m, that if R has a unity, then R has not only nil commutator ideal but is in fact commutative. More precisely, if R has a unity, then R is commutative if either $m \equiv 2 (\mathrm{mod}\, 4)$ or m is odd and satisfies a rather technical condition concerning its prime divisors. The purpose of this paper is to prove that if R has a unity, then R is commutative when $m \equiv 2 (\mathrm{mod}\, 4)$ even if m is allowed to depend on x and y. We do not investigate the case of odd m here.

All rings are assumed associative. The commutator ideal of R will be denoted $C(R)$ and the center $Z(R)$.

Theorem. *Let R be a ring with unity satisfying (*) given x, y in R there exists a positive integer $m = m(x,y) \equiv 2 (mod 4)$ such that $(x+y)^m = x^m + y^m$. Then R is commutative.*

Proof. We shall make use of the following well-known result of Streb [4]:

A noncommutative ring has a noncommutative factorsubring of one of the following types:

(a) $\begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} GF(p) & 0 \\ GF(p) & 0 \end{pmatrix}$ where p is a prime;

(b) $M_\sigma(GF(q^r)) = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix} | \alpha, \beta \text{ in } GF(q^r)\}$ where σ is a nontrivial automorphism of $GF(q^r)$ with fixed field $GF(q)$;

(c) a division ring;

(d) a simple radical domain;

(e) a finite nilpotent subdirectly irreducible ring S such that $C(S)$ is the heart of S and $SC(S) = C(S)S = (0)$;

Received April 19, 1996.
1991 *Mathematics Subject Classification.* Primary 16A70.
Key words and phrases. Commutativity, polynomial constraints.

(f) a subdirectly irreducible ring S generated by two elements of finite additive order such that $C(S)$ is the heart of S, $SC(S) = C(S)S = (0)$, and the nilpotent elements of S form a commutative nilpotent ideal.

Suppose that R is a ring with unity satisfying (*) and that R is not commutative. Then R has a noncommutative factorsubring of one of the types (a)-(f) and of course S inherits (*). The proof will be achieved by showing that each type leads to a contradiction.

First we note that if $m = m(1, -1)$, then $0 = (1-1)^m = 1 + (-1)^m = 2$ since m is even, and hence the characteristic of R, and therefore of S, is 2.

Now let $x \in R$ and $m = m(x, 1)$. Then $(x+1)^m = x^m + 1$ implies

$$\sum_{i=1}^{m-1} \binom{m}{i} x^i = 0. \tag{1}$$

Thus every element of R, and therefore of S, satisfies an equation of the form (1) with m depending on x. Writing $m = 2 + 4k$, we have $m = 0$ in S and $\binom{m}{2} = \frac{(2+4k)(1+4k)}{2} = (1+2k)(1+4k)$, an odd integer. Hence $\binom{m}{2} = 1$ in S and so (1) becomes

$$x^2 = x^3 f(x) \text{ for some polynomial } f \text{ with integer coefficients.} \tag{2}$$

We now eliminate types (a) and (c)-(f), leaving the more difficult type (b) for last.

Type (a): If $x = e_{11}$ and $y = e_{12}$, then $(x+y)^m = e_{11} + e_{12}$ whereas $x^m + y^m = e_{11}$. Thus S cannot be of type $\begin{pmatrix} GF(p) & GF(p) \\ 0 & 0 \end{pmatrix}$, and similarly it cannot be of type $\begin{pmatrix} GF(p) & 0 \\ GF(p) & 0 \end{pmatrix}$.

Type (c): If S is a division ring, then (2) shows that S is algebraic over the finite subfield $GF(2)$, whence S must be commutative by a theorem of Jacobson [3].

Type (d): Let $x \neq 0$ be in S. Since x is not nilpotent, we obtain from (2) a nonzero idempotent $e = x^2(f(x))^2$ in S as in [2, p.22], an impossibility in a simple radical ring.

Type (e): Let $x \neq 0$ be in S. Then $x^k = 0 \neq x^{k-1}$ for some $k \geq 2$. If $k > 2$, then from (2) we have $x^{k-1} = x^{k-3}(x^3 f(x)) = x^k f(x) = 0$; hence $k = 2$, that is, $x^2 = 0$ for all $x \in S$. Now for all x, y in S we have $0 = (x+y)^2 = x^2 + xy + yx + y^2 = xy + yx$ and hence $xy = -yx = yx$ since S has characteristic 2.

Type (f): If S is nil, then we are done, as in Type(e). Hence there is a nonnilpotent element in S, from which we obtain as in Type (d) a nonzero idempotent e. For all $x \in S$ we have $e(xe - ex) \in SC(S) = (0)$, so $exe = ex$. Similarly $exe = xe$ and hence $e \in Z(S)$. Thus the set $I = \{x \in S | ex = x\}$ is an ideal of S and is nonzero since it contains e. Hence $C(S) \subseteq I$. But now for all x, y in S we have $[x, y] = e[x, y] \in SC(S) = (0)$.

This leaves Type (b) and for this case we need the following

Lemma. *Let t and r be positive integers with $r > 1$ and let $q = 2^t$. Then there exists a prime which divides $q^r - 1$ but not $q - 1$.*

Proof. First we establish the result when $r = 2^n$ for $n \geq 1$ by induction on n. Suppose that $n = 1$ and that every prime dividing $q^2 - 1$ also divides $q - 1$. Let p be any prime dividing $q + 1$; p must be odd since q is even. But p divides $q^2 - 1$ and so by assumption p divides $q - 1$, whence p divides $(q + 1) - (q - 1) = 2$, a contradiction which proves the case $n = 1$. Now assume inductively that $n > 1$ and that there is a prime dividing $q^{2^{n-1}} - 1$ which does not divide $q - 1$. Clearly this prime divides $q^{2^n} - 1 = (q^{2^{n-1}} - 1)(q^{2^{n-1}} + 1)$, which completes the induction for the case in which r is a power of 2.

Now suppose r is divisible by an odd prime p. We first show that there is a prime which divides $q^p - 1$ but not $q - 1$. Suppose to the contrary that every prime which divides $q^p - 1$ also divides $q - 1$. Writing

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

we let p' be any prime dividing $q^{p-1} + q^{p-2} + \cdots + q + 1$. Then p' divides $q^p - 1$ and so by assumption $q - 1$. But now p' divides $q^{p-i} - 1$ for $i = 1, 2, \cdots, p - 1$ and since $q^{p-1} + q^{p-2} + \cdots + q + 1 = (q^{p-1} - 1) + (q^{p-2} - 1) + \cdots + (q - 1) + p$, we see that p' must divide p. Since p and p' are both prime, we must have $p = p'$ and hence p is the *only* prime dividing $q^{p-1} + q^{p-2} + \cdots + q + 1$. Moreover it is clear that $q^{p-1} + q^{p-2} + \cdots + q + 1 > p$, so we may write

$$q^{p-1} + q^{p-2} + \cdots + q + 1 = p^c \text{ for some } c \geq 2. \tag{4}$$

Let $q - 1 = p^d k$ where p does not divide k. From (3) and (4) we have $q^p - 1 = p^{c+d}k$. Since p^d divides $q^{p-i} - 1$ for $i = 1, 2, \cdots, p - 1$, letting $q^{p-i} - 1 = p^d s_i$, we have

$$p^c = (q^{p-1} - 1) + (q^{p-2} - 1) + \cdots + (q - 1) + p = p^d(s_1 + s_2 + \cdots + s_{p-1}) + p.$$

If $d > 1$, then $p^{c-1} = p^{d-1}(s_1 + s_2 + \cdots + s_{p-1}) + 1$ with $c - 1$ and $d - 1$ both positive, a contradiction. Thus $d = 1$, $q - 1 = pk$ and $q^p - 1 = p^{c+1}k$. Hence $1 + p^{c+1}k = q^p = (1 + pk)^p = \sum_{i=0}^{p} \binom{p}{i}(pk)^i$, whence $p^{c+1}k = p(pk) + \binom{p}{2}(pk)^2 + \cdots + \binom{p}{p-1}(pk)^{p-1} + (pk)^p$. Every term has p^2 as a factor, so dividing by p^2 yields $p^{c-1}k = k + \binom{p}{2}k^2 + \binom{p}{3}pk^3 + \cdots + \binom{p}{p-1}p^{p-3}k^{p-1} + p^{p-2}k^p$, a contradiction since all terms but k are divisible by p. This shows that there is a prime which divides $q^p - 1$ but not $q - 1$.

For the general case in which r is divisible by an odd prime p we let $r = pk$ and observe that since $q^r - 1 = (q^k)^p - 1$, the preceding argument yields a prime which divides $q^r - 1$ but not $q^k - 1$, and clearly this prime cannot divide $q - 1$. This proves the lemma.

Getting back to Type (b), we assume that $S = M_\sigma(GF(q^r))$ where σ has fixed field $GF(q)$ and that S satisfies (*). Since S has characteristic 2, q is a power of 2. By the lemma there exists a prime p which divides $q^r - 1$ but not $q - 1$. Since p divides $q^r - 1$, there is an element α of multiplicative order p in $GF(q^r)$, and since p does not divide $q - 1$, $\alpha^{q-1} \neq 1$ and hence $\alpha \notin GF(q)$, that is ,$\sigma(\alpha) \neq \alpha$. Let

$$x = \begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix}, y = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, m = m(x, y). \text{ Then}$$

$$(x+y)^m = \begin{pmatrix} (\alpha-1)^m & \frac{(\alpha-1)^m - \sigma((\alpha-1)^m)}{\alpha-\sigma(\alpha)} \\ 0 & \sigma((\alpha-1)^m) \end{pmatrix} \text{ and}$$

$$x^m + y^m = \begin{pmatrix} \alpha^m - 1 & -m \\ 0 & \sigma(\alpha^m - 1) \end{pmatrix} = \begin{pmatrix} \alpha^m - 1 & 0 \\ 0 & \sigma(\alpha^m - 1) \end{pmatrix}.$$

Equating these, we obtain $\alpha^m - 1 = (\alpha-1)^m = \sigma((\alpha-1)^m) = \sigma(\alpha^m - 1) = \sigma(\alpha^m) - 1$, where $\sigma(\alpha^m) = \alpha^m$. Thus α^m is in the fixed field $GF(q)$ and so $\alpha^{m(q-1)} = 1$. But now p, being the multiplicative order of α, must divide $m(q-1)$, and since p does not divide $q-1$, p must divide m. Therefore $(\alpha-1)^m = \alpha^m - 1 = 1 - 1 = 0$ and so $\alpha = 1$, a contradiction which completes the proof of the theorem.

In closing we point out that there are examples [6] of noncommutative rings with unity satisfying $(x+y)^{4k} = x^{4k} + y^{4k}$ for all x, y and any positive integer k, so for even m the condition $m \equiv 2 (\bmod 4)$ is essential in the above theorem. As for odd m, Yen also gave an example [6] of a noncommutative ring with unity of odd prime characteristic p satisfying $(x+y)^{p^k} = x^{p^k} + y^{p^k}$ for all x, y and any positive integer k and also showed in [5] that commutativity is achieved for fixed odd m provided that for every prime p dividing m we have $m = p^i n$ where $n > 1$, p does not divide n, and $p-1$ does not divide $n-1$. It is not clear at this point whether making this further assumption on variable odd $m(x,y)$ will yield commutativity, so this question remains open.

References

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

[2] I. N. Herstein, *Noncommutative Rings*, Carus Math. Monograph No.15, Math. Assoc. Amer., Wiley, 1968.

[3] N. Jacobson, "Structure theory for algebraic algebras of bounded degree," *Ann. Math.*, 46 (1947), 695-707.

[4] W. Streb, "Zur Struktur nichtcommutativer Ringe," *Math. J. Okayama Univ.*, 31 (1989), 135-140.

[5] C. T. Yen, "On a theorem of Herstein," *Tamkang J. Math.*, 21 (1990), 123-130.

[6] C. T. Yen, "A commutativity theorem for rings," *Tamkang J. Math.*, 13 (1982), 243-246.

Department of Mathematics and Statistics, University of Missouri-Kansas City, 5100 Rockhill Road, Kansas City, MO 64110, U.S.A.