The Identity $(XY)^n = X^nY^n$: Does It Buy Commutativity?

HOWARD E. BELL
Brock University
St. Catharines, Ontario, Canada L2S 3A1

Let $(S, *)$ be a set with an associative binary operation, which we shall think of as multiplication; denote the product $x*y$ by xy. If the operation $*$ is also commutative, then S satisfies the identity

$$(xy)^n = x^n y^n \tag{1}$$

for each positive integer n. Conversely, suppose that S satisfies (1) for one or more $n>1$. Need $*$ be commutative? If not, under what additional hypotheses will $*$ be commutative? This problem is a natural one, and interesting answers can be obtained by using techniques covered in a first abstract algebra course. It is, therefore, somewhat surprising that the problem, at least in its ring-theory version, has only recently been investigated.

Let F be any field and consider the set of 3×3 matrices

$$M = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \middle| \, a, b, c \in F \right\}.$$

Ordinary matrix multiplication is a binary operation on M, and $xyz = 0$ for all $x, y, z \in M$; hence M satisfies (1) for every $n \geqslant 2$. Since matrix multiplication on M is clearly noncommutative, it is already evident that something more than (1) must be assumed in order to prove commutativity.

Some results for groups

The positive result which sparked recent interest in the problem is an easy and probably long-known result for groups, which I first encountered as an exercise in Herstein's textbook on algebra [**10**].

THEOREM 1. *Let G be a group, and suppose that there exist three consecutive positive integers n for which G satisfies* (1). *Then G is a commutative group.*

Proof. Suppose G satisfies (1) for $n = k, k+1, k+2$. Making use of (1) for $n = k$ and $n = k+1$, we obtain, for arbitrary $x, y \in G$,

$$x^{k+1}y^{k+1} = (xy)^{k+1} = (xy)^k(xy) = x^k y^k xy;$$

and cancelling x^k on the left and y on the right gives

$$xy^k = y^k x. \tag{2}$$

Repeating the argument with $k+1$ and $k+2$ gives

$$xy^{k+1} = y^{k+1}x; \tag{3}$$

substituting (2) into (3) we get

$$xy^{k+1} = yxy^k,$$

which implies $xy = yx$.

It is almost obvious that a group G satisfying (1) for $n = 2$ must be commutative; and while the analogous result for a single n greater than 2 does not hold, groups satisfying (1) for even one $n > 1$ are somewhat restricted in their behavior. (For details, see Alperin's paper [**2**], the major theorem of which is accessible to anyone with a little knowledge of free groups.)

A careful look at the proof of Theorem 1 yields information about groups satisfying (1) for *two* consecutive n: specifically, G is commutative if it satisfies (1) for $n = k$ and $n = k+1$ and if every element of G is of the form y^k for some $y \in G$. But satisfying (1) for two consecutive n does not by itself guarantee commutativity, as we see by considering the following example from [**22**].

EXAMPLE 1. Let Z_{10} denote the integers mod 10, with $+$ and $\cdot$ denoting the usual operations, and let $G = \{(a, b, c) \mid a, b, c \in Z_{10}\}$. If the operation $*$ is defined on G by $(a, b, c) * (a', b', c') = (a + a', b + b', c + c' + 2a \cdot b')$, then G is a noncommutative group under $*$; however it is easily verified that G satisfies (1) for $n = 5$ and $n = 6$.

The problem for rings

Since the essential mechanism in the proof of Theorem 1 is cancellation, it is immediate that there is a version of Theorem 1 for rings without zero divisors. However, since these constitute a relatively small class of rings, it is reasonable to ask what conditions in addition to (1) will yield commutativity in more general rings. The first authors to consider this question were Johnsen, Outcalt, and Yaqub [**13**], who proved in 1968 that a ring having a multiplicative identity element must be commutative if it satisfies (1) with $n = 2$. Luh [**17**] in 1971 established commutativity of certain rings having a multiplicative identity element and satisfying (1) for three consecutive n. Several years later Anthony Richoux, at that time an undergraduate, and Steve Ligh, one of Richoux's professors, succeeded in proving the following ring analogue of Theorem 1 [**16**].

THEOREM 2. *Let R be a ring with a multiplicative identity element, and suppose R satisfies the identity* (1) *for three consecutive positive integers n. Then R is commutative.*

In the discussion that follows we shall use the symbol 1 to denote the multiplicative identity element of the ring R, and use expressions such as "R has 1" or "a ring R with 1" to indicate that R has a multiplicative identity element. We shall also use the term "polynomial function of two variables on R" to denote a function such as $f(x, y) = x^2yx + yxyx + y^4x^4$, where the x and y range over elements of R. (Note that since R is not assumed to be commutative, this function f is distinct from the function $g(x, y) = x^3y + x^2y^2 + x^4y^4$.) Among the important polynomial functions is the **commutator function** or **bracket function**, defined by $[x, y] = xy - yx$. Clearly, $[x, y] = 0$ if and only if the elements x and y commute. Moreover, $[\ ,\ ]$ is linear in each component; hence if R has 1, it follows that $[x + 1, y] = [x, y + 1] = [x, y]$ for all $x, y \in R$.

The Ligh-Richoux proof of Theorem 2, which is astonishingly simple, depends on a limited cancellation property in rings with 1.

LEMMA. *Let R be a ring with* 1, *and suppose f is any polynomial function of two variables on R with the property that $f(x + 1, y) = f(x, y)$ for all $x, y \in R$. If there exists a positive integer n such that $x^n f(x, y) = 0$ for all $x, y \in R$, then $f(x, y) = 0$ for all $x, y \in R$.*

Proof. Given that $x^n f(x, y) = 0$, replace x by $x + 1$, obtaining

$$0 = (x+1)^n f(x+1, y) = \left(x^n + nx^{n-1} + \binom{n}{2}x^{n-2} + \cdots + nx + 1\right)f(x, y), \tag{4}$$

where the $\binom{n}{i}$ are the usual binomial coefficients. Left-multiplying (4) by x^{n-1} and using the fact that $x^n f(x, y) = 0$, we get $x^{n-1}f(x, y) = 0$; and simply repeating the argument finitely many times yields $f(x, y) = 0$.

Proof of Theorem 2. Suppose R satisfies (1) for $n = k$, $k + 1$, and $k + 2$. We begin as in the proof of Theorem 1, noting that the equation $x^{k+1}y^{k+1} = x^ky^kxy$ can be rewritten as $x^k[x, y^k]y = 0$. Repeat the argument, using $n = k + 1$ and $n = k + 2$ and apply the Lemma to obtain

$$[x, y^k]y = 0 \quad \text{and} \quad [x, y^{k+1}]y = 0 \quad \text{for all } x, y \in R. \tag{5}$$

Now left-multiply the first equation in (5) by y, obtaining $yxy^{k+1} = y^{k+1}xy$, and note that the second equation in (5) may be expressed as $xy^{k+2} = y^{k+1}xy$. Therefore, $xy^{k+2} = yxy^{k+1}$, which says

$$[x, y]y^{k+1} = 0 \quad \text{for all } x, y \in R. \tag{6}$$

A right-hand version of the Lemma now yields $[x, y] = 0$ for all $x, y \in R$.

As in the group case, we cannot get by in Theorem 2 with only two consecutive n.

EXAMPLE 2. Let R_1 be the set of all ordered 4-tuples with entries from the integers mod 10; define addition componentwise and define multiplication by

$$(a, b, c, d)(a', b', c', d') = (aa', ab' + ba', ac' + ca', ad' + da' + 2bc').$$

It is readily verified that R_1 is a noncommutative ring under these operations, and that the 4-tuple $(1,0,0,0)$ is a multiplicative identity element, which we denote as usual by 1. Let W be the set of 4-tuples with first component 0; note that for all $w_1, w_2, w_3 \in W$, we have $w_1w_2w_3 = 0$ and $5w_1w_2 = 0$. Observe also that every element of R_1 can be written as $k1 + w$ for some integer k and some $w \in W$. Now let $x = j1 + u$ and $y = k1 + v$ be arbitrary elements of R_1, where j and k are integers and $u, v \in W$. Then $xy = jk1 + jv + ku + uv = jk1 + w_0$, where $w_0 = jv + ku + uv$ belongs to W. Since 1 commutes multiplicatively with w_0, we can use the binomial theorem to obtain

$$(xy)^n = (jk)^n 1 + n(jk)^{n-1}w_0 + \frac{n(n-1)}{2}(jk)^{n-2}w_0^2$$

for any positive integer n. In particular, if $n(n-1)/2$ is divisible by 5, we have

$$(xy)^n = (jk)^n 1 + n(jk)^{n-1}w_0 = (jk)^n 1 + n(jk)^{n-1}(jv + ku + uv). \qquad (7)$$

Subject to the same restriction on n, we have

$$x^n y^n = (j^n 1 + nj^{n-1}u)(k^n 1 + nk^{n-1}v) = (jk)^n 1 + n(jk)^{n-1}(jv + ku + nuv). \qquad (8)$$

Since $n(n-1)/2$, and hence $n^2 - n$, was assumed to be divisible by 5, the right sides of (7) and (8) are equal; thus, R_1 satisfies the identity (1) for any n such that $n(n-1)/2$ is divisible by 5. In particular, for $n = 5$ and $n = 6$, identity (1) is satisfied by R_1.

Despite the existence of examples such as this, we need not give up on the case of two consecutive n; instead we can impose hypotheses which are incompatible with the "bad" behavior of R_1. The theorem below is due to Harmanci **[7]**; the proof is based on the proof of Theorem 1 of **[4]**.

THEOREM 3. *Let R be a ring with* 1. *Suppose that R satisfies* (1) *for $n = k, k + 1$, and that R contains no nonzero elements x for which $k!x = 0$. Then R is commutative.*

The basic strategy of the proof is to study a factor ring $\bar{R} = R/I$, where I is an ideal chosen so that $\bar{R}$ is more tractable than R, and then to transfer information about $\bar{R}$ back to R. In our case, we take I to be the set N of **nilpotent** elements of R, defined by

$$N = \{x \in R \mid x^j = 0 \quad \text{for some positive integer } j\}.$$

In our arguments, we shall also make use of the **center** C of R, defined by

$$C = \{x \in R \mid xy = yx \quad \text{for all } y \in R\},$$

and use the fact that the center of any ring is a subring. For arbitrary rings R, the set N need not be an ideal, nor even an additive subgroup; hence, the first step of the proof is to show that the hypotheses of Theorem 3 force the inclusion $N \subseteq C$. This inclusion implies that N is an ideal. Finally, we shall invoke yet another cancellation property, which we call Property **C**.

PROPERTY **C**. Let R be a ring with no nonzero nilpotent elements, and let f be a polynomial function in two variables on R such that every monomial term in $f(x, y)$ contains y. Then if R satisfies the identity $f(x, y)y = 0$, it also satisfies the identity $f(x, y) = 0$.

To establish property **C**, note first that if $ab = 0$, then $(ba)^2 = 0$, hence $ba = 0 = bax$ for every $x \in R$. Repeating the argument now yields $axb = 0$, so we have an **insertion-of-factors property** (IFP): in a ring with no nonzero nilpotent elements, if a product of finitely many elements is 0, then all products obtained by inserting additional factors in any positions are also 0. (Of course, all commutative rings have IFP, but noncommutative rings in general do not.) Suppose now that R satisfies the identity $f(x, y)y = 0$, where $f(x, y) = \Sigma_{i=1}^{n} p_i(x, y)$ for monomials $p_i(x, y)$ having y as a factor. Then, because of IFP, R satisfies each of the identities $f(x, y)p_i(x, y) = 0$, $i = 1,\ldots,n$; consequently R satisfies the identity $(f(x, y))^2 = 0$, which in the absence of nilpotent elements implies the identity $f(x, y) = 0$.

Proof of Theorem 3. Let R be any ring satisfying the hypotheses of the Theorem and C its center. Then, as in the proof of Theorem 2, we have $x^k[x, y^k]y = 0$, and applying the Lemma gives

$$[x, y^k]y = 0 \quad \text{for all } x, y \in R. \tag{9}$$

If y is not a zero divisor—in particular, if y is invertible (has a multiplicative inverse)—the obvious cancellation shows that $y^k \in C$. If $u \in N$, $u^n = 0$ implies that $(1+u)(1-u+u^2 - \cdots + (-1)^{n-1}u^{n-1}) = 1$, so that $1+u$ is invertible, and hence $(1+u)^k \in C$.

For arbitrary $u \in N$, let the **index** of u be the smallest n such that $u^n = 0$. We now proceed, by induction on the index of elements of N, to show that $N \subseteq C$. Expanding $(1+u)^k$ by the binomial theorem, we have

$$1 + ku + v \in C \tag{10}$$

for each $u \in N$, where

$$v = \binom{k}{2}u^2 + \binom{k}{3}u^3 + \cdots.$$

Thus, if u has index 2, $v = 0$ and $ku \in C$, so that $0 = [ku, x] = k[u, x] = k![u, x]$ for all $x \in R$. But recalling the hypotheses on R, we then get $[u, x] = 0$ for all $x \in R$, which says $u \in C$. Now suppose all nilpotent elements of index less than n are in C, and consider u of index n. It is easily seen that the corresponding v has index less than n, so (10) again yields $ku \in C$ and hence $u \in C$. Our induction is now complete.

Since $N \subseteq C$, the set N forms an ideal. (If $a, b \in N$, then $a^n = b^m = [a, b] = 0$; the fact that $a - b \in N$ follows by expanding $(a-b)^{n+m-1}$ by the binomial theorem and noting that each summand contains either a^n or b^m as a factor.) We consider the factor ring $\bar{R} = R/N$, which inherits all the original hypotheses and in addition has no nonzero nilpotent elements. Suppose, temporarily, that $\bar{R}$ can be shown to be commutative. Then for every $x, y \in R$, $[x, y] = xy - yx \in N$, hence $[x, y] \in C$. It now follows by an easy induction that $[x, y^n] = ny^{n-1}[x, y]$ for all $x, y \in R$ and all positive integers n; and recalling (9), we have $0 = [x, y^k]y = ky^k[x, y]$. It follows that $k!y^k[x, y] = 0$, and so, by hypothesis, $y^k[x, y] = 0$; hence, by the Lemma, R is commutative.

The proof of Theorem 3 is not yet complete; it is necessary to justify our temporary assumption concerning $\bar{R}$. We show, in fact, that any R satisfying the hypotheses of Theorem 3 and having $N = \{0\}$ must be commutative. Note first that Property **C** applied to (9) shows that $x^k \in C$ for *all* $x \in R$. Thus,

$$(1+x)^k - x^k - 1 = kx + \binom{k}{2}x^2 + \cdots + kx^{k-1} \in C,$$

so that

$$\left[kx + \binom{k}{2}x^2 + \cdots + kx^{k-1}, y\right] = 0 \quad \text{for all } x, y \in R. \tag{11}$$

Replacing x in (11) by $2x, 3x, \ldots, (k-1)x$ in turn, we see that

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 2 & 2^2 & \ldots & 2^{k-1} \\ 3 & 3^2 & \ldots & 3^{k-1} \\ & & \ldots & \\ k-1 & (k-1)^2 & \ldots & (k-1)^{k-1} \end{bmatrix} \begin{bmatrix} [kx, y] \\ \left[\binom{k}{2}x^2, y\right] \\ \vdots \\ [kx^{k-1}, y] \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{12}$$

for all $x, y \in R$. Now the $(k-1)\times(k-1)$ matrix A on the left side of (12) is a Vandermonde matrix with determinant Δ equal to $\pm\Pi(i-j)$, where the factors $i-j$ range over all pairs with $i, j \in \{2,3,\dots,k-1\}$ and $i<j$ (see [**18**, p. 15–16]); and since all these factors divide $k!$, it follows that Δ divides $(k!)^m$ for some positive integer m. Left-multiplying both sides of (12) by the matrix adj A [**15**, p. 36] and recalling that (adj $A)A$ is equal to Δ times the $(k-1)\times(k-1)$ identity matrix, we get

$$\Delta[kx, y] = \Delta\left[\binom{k}{2}x^2, y\right] = \cdots = \Delta\left[kx^{k-1}, y\right] = 0 \quad \text{for all } x, y \in R.$$

Consequently, $\Delta k[x, y] = 0 = \Delta k![x, y] = (k!)^{m+1}[x, y]$ for all $x, y \in R$. Repeatedly using the hypothesis that $k!z = 0$ implies $z = 0$, we obtain $[x, y] = 0$ for all $x, y \in R$; hence R is commutative.

Extensions and related results

Our choice of theorems has been influenced by a desire to keep the proofs elementary and reasonably self-contained. Not surprisingly, by using more elaborate methods, one can obtain somewhat better results.

An examination of the proof of Theorem 3 shows that only in the final stages did we use the full force of the hypothesis that $k!x = 0$ implies $x = 0$; usually we employed only the weaker hypothesis that $kx = 0$ implies $x = 0$. In fact, the conclusion of Theorem 3 remains true if we assume only the weaker hypothesis [**4**]. In this case, we omit the last paragraph of the proof of Theorem 3 and show that commutators in R are nilpotent by appealing to a deep theorem of Herstein [**3**], [**8**], [**9**]: if the ring R (not necessarily with 1) satisfies (1) for some $n > 1$, then all commutators in R are nilpotent, and the ideal generated by the commutators consists entirely of nilpotent elements.

Clearly Herstein's result implies that a ring with no nonzero nilpotent elements is commutative if it satisfies (1) for even one $n > 1$. There are other one-n theorems available as well, for example, the following recent result due to Abu-Khuzam [**1**]:

THEOREM 4. *Let $n > 1$ be a positive integer, and let R be a ring with* 1. *If R satisfies* (1) *and contains no nonzero x for which $n(n-1)x = 0$, then R is commutative.*

Incidentally, in this theorem the hypothesis that $n(n-1)x = 0$ implies $x = 0$ cannot be weakened to the hypothesis that $nx = 0$ implies $x = 0$. (Consider the ring R_1 of Example 2 with $n = 21$.)

So far we have always assumed the existence of one, two, or three n such that every pair x, y of elements satisfies (1) for those n. One possibility of generalization is to assume that the n varies with x and y; and it works—at least sometimes. Indeed, Richoux [**21**] has recently established commutativity of R with 1 under the hypothesis that for each $x, y \in R$ there exist three consecutive integers n, *depending on x and y*, for which (1) holds, and his result has been further generalized in [**12**], [**19**], and [**20**].

Other closely-related theorems assert commutativity of rings satisfying (1) together with other identities (see [**5**, Theorem 2] and [**11**]). We conclude with a sample of this kind of result.

THEOREM 5. *Let R be a ring with* 1, *and let n and m be relatively prime integers, greater than or equal to* 2. *If R satisfies the identities $(xy)^n = x^n y^n$, $(xy)^{n+1} = x^{n+1}y^{n+1}$, and $x^m y^m = y^m x^m$, then R is commutative.*

Supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. A 3961.

This paper had its genesis in a talk given for undergraduates at Mount Holyoke College, South Hadley, Massachusetts, during the spring semester of 1979. The author acknowledges with gratitude the encouragement given by the members of the Mathematics Department at Mount Holyoke.

References

[1] H. Abu-Khuzam, A commutativity theorem for rings, Math. Japon., 25 (1980) 593–595.
[2] J. Alperin, A classification of n-abelian groups, Canad. J. Math., 21 (1969) 1238–1244.
[3] H. E. Bell, On a commutativity theorem of Herstein, Arch. Math., 21 (1970) 265–267.
[4] ______, On the power map and ring commutativity, Canad. Math. Bull., 21 (1978) 399–404.
[5] ______, On rings with commuting powers, Math. Japon., 24 (1979) 473–478.
[6] L. O. Chung and J. Luh, Conditions for elements to be central in a ring, Acta Math. Acad. Sci. Hungar., 34 (1979) 261–265.
[7] A. Harmanci, Two elementary commutativity theorems for rings, Acta Math. Acad. Sci. Hungar., 29 (1977) 23–29.
[8] I. N. Herstein, Power maps in rings, Michigan Math. J., 8 (1961) 29–32.
[9] ______, A remark on rings and algebras, Michigan Math. J., 10 (1963) 269–272.
[10] ______, Topics in Algebra, Xerox College Publishing, Lexington, 1975.
[11] Y. Hirano, M. Hongan, and H. Tominaga, Supplements to the previous paper "Some commutativity theorems for rings," to appear.
[12] M. Hongan and I. Mogami, A commutativity theorem for rings, Math. Japon., 23 (1978) 131–132.
[13] E. C. Johnsen, D. L. Outcalt, and A. Yaqub, An elementary commutativity theorem for rings, Amer. Math. Monthly, 75 (1968) 288–289.
[14] A. Kaya, On a commutativity theorem of Luh, Acta Math. Acad. Sci. Hungar., 28 (1976) 33–36.
[15] P. Lancaster, Theory of Matrices, Academic Press, New York, 1969.
[16] S. Ligh and A. Richoux, A commutativity theorem for rings, Bull. Austral. Math. Soc., 16 (1977) 75–77.
[17] J. Luh, A commutativity theorem for primary rings, Acta Math. Acad. Sci. Hungar., 22 (1971) 211–213.
[18] M. Marcus and H. Minc, A Survey of Matrix Theory and Matrix Inequalities, Allyn & Bacon, Boston, 1964.
[19] I. Mogami and M. Hongan, Note on commutativity of rings, Math. J. Okayama Univ., 20 (1978) 21–24.
[20] I. Mogami, Note on commutativity of rings, II, Math. J. Okayama Univ., 22 (1980) 51–54.
[21] A. Richoux, On a commutativity theorem of Luh, Acta Math. Acad. Sci. Hungar., 34 (1979) 23–25.
[22] H. Trotter, Groups in which raising to a power is an automorphism, Canad. Math. Bull., 8 (1965) 825–827.

Races with Ties

Elliott Mendelson
Queens College
Flushing, NY 11367

When there are n runners in a race, the number of possible outcomes is $n!$ if we assume that there are no ties. If any number of the runners are allowed to tie for arbitrarily many positions, calculation of the number J_n of outcomes becomes much more complicated. The number J_n has other interesting interpretations. It is the number of possible election ballots when there are n candidates and the voters are allowed to express equal preference among some of the candidates. It is also the number of preferential arrangements of n objects, allowing indifference among some of the objects.

The first few values of J_n are easy to calculate: $J_0 = 1$ and $J_1 = 1$, while $J_2 = 3$ (either (A, B), (B, A) or a tie (AB)). When $n = 3$, we have the six standard permutations of A, B, C, plus (ABC) (all tied for first), (AB, C), (AC, B), (BC, A) (two tied for first), and (C, AB), (B, AC), (A, BC) (two tied for second). Thus, $J_3 = 13$. We shall derive recursion equations for J_n, several closed forms for J_n, and some other methods for calculating J_n.

Assume that there are $n+1$ runners. If the number of runners who do not finish first is j, then those j runners can finish in 2nd, 3rd,... places in J_j ways. Moreover, those j runners can be chosen from the $n+1$ runners in $\binom{n+1}{j}$ ways. Hence, the number of possible outcomes is $\binom{n+1}{j}J_j$. Since j can be any number between 0 and n, the value of J_{n+1} is