

POWER-ASSOCIATIVE RINGS OF CHARACTERISTIC TWO

LOUIS A. KOKORIS

1. Introduction. Sufficient conditions for associativity of powers in commutative rings of characteristic prime to two have been given elsewhere.¹ We shall state the known results in the following theorems.

THEOREM 1. *Let \mathfrak{A} be a commutative ring whose characteristic is prime to 30 and let $x^2x^2 = x^3x$ for every x of \mathfrak{A} . Then \mathfrak{A} is power-associative.*

THEOREM 2. *Let \mathfrak{A} be a commutative ring whose characteristic is 3 and let $x^2x^2 = x^3x$ and $2[(xy)x]x^2 + (x^2y)x^2 + 2(xy)x^3 = x^4y + (x^3y)x + [(x^2y)x]x + 2\{[(xy)x]x\}x$ for every x in \mathfrak{A} and every y in \mathfrak{A} which is a power of x . Then \mathfrak{A} is power-associative.*

In case \mathfrak{A} is an algebra we have the following corollary to Theorem 2.

COROLLARY. *Let \mathfrak{A} be a commutative algebra over a field \mathfrak{F} whose characteristic is 3, \mathfrak{F} have more than three elements, and $x^2x^2 = x^3x$, $x^3x^2 = x^4x$ for every x in \mathfrak{A} . Then \mathfrak{A} is power-associative.*

THEOREM 3. *Let \mathfrak{A} be a commutative ring whose characteristic is 5 and let $x^2x^2 = x^3x$, $x^4x^2 = x^5x$ for every x in \mathfrak{A} . Then \mathfrak{A} is power-associative.*

These theorems are important tools in the study of power-associative rings and algebras, and it seems desirable to complete this set of conditions for power-associativity by obtaining the corresponding theorem for rings with characteristic two. The result may be stated as

THEOREM 4. *Let \mathfrak{A} be a commutative ring whose characteristic is 2 and let $(x^2y)y = (y^2x)x$ and $x^{2^{n-1}}x^{2^{n-1}} = x^{2^n}$ for every x, y in \mathfrak{A} and every positive integer n . Then $x^\lambda x^\mu = x^{\lambda+\mu}$ for every x in \mathfrak{A} and all positive integers λ, μ .*

When \mathfrak{A} is an algebra we have the following result.

COROLLARY. *Let \mathfrak{A} be a commutative algebra over a field \mathfrak{F} of characteristic 2 and let \mathfrak{F} contain at least four elements. Then \mathfrak{A} is power-*

Presented to the Society, April 30, 1955; received by the editors February 9, 1953 and, in revised form, November 18, 1954.

¹ For Theorem 1 see A. A. Albert, *On the power-associativity of rings*, Summa Brasiliensis Mathematicae vol. 2 (1948) pp. 21–33. Theorems 2 and 3 are given in *New results on power-associative algebras*, Trans. Amer. Math. Soc. vol. 77 (1954) pp. 363–373.

associative if $x^{2^n-1}x^{2^n-1} = x^{2^n}$ for every x in \mathfrak{A} and every positive integer n .

2. Associativity of fourth powers. Consider a commutative algebra \mathfrak{A} over a field \mathfrak{F} whose characteristic is 2 and suppose that $x^2x^2 = x^3x$ for every x in \mathfrak{A} . Then replace x by $x + \lambda y$ where λ is in \mathfrak{F} and obtain $(x + \lambda y)^2(x + \lambda y)^2 = x^2x^2 + \lambda^4y^2y^2 = [(x + \lambda y)^2(x + \lambda y)](x + \lambda y) = (x^3 + \lambda x^2y + \lambda^2xy^2 + \lambda^3y^3)(x + \lambda y) = x^4 + \lambda x^3y + \lambda(x^2y)x + \lambda^2(x^2y)y + \lambda^2(xy^2)x + \lambda^3(xy^2)y + \lambda^3xy^3 + \lambda^4y^4$. The result is a polynomial in λ which we write as $A\lambda^3 + B\lambda^2 + C\lambda = 0$ where $A = (xy^2)y + xy^3$, $B = (x^2y)y + (xy^2)x$, and $C = x^3y + (x^2y)x$. If \mathfrak{F} contains at least four elements it follows that $A = B = C = 0$ and we then have

$$(1) \quad (x^2y)x = x^3y$$

and

$$(2) \quad (x^2y)y = (y^2x)x.$$

Thus we see that once Theorem 4 is established the corollary will follow.

Now replace y in (2) by $y + z$ so that $(x^2y)y + (x^2z)y + (x^2y)z + (x^2z)z = (y^2x)x + (z^2x)x$. By (2) we conclude that

$$(3) \quad (x^2y)z = (x^2z)y.$$

As a consequence of relation (3) we have

LEMMA 1. *Let \mathfrak{A} be a commutative ring whose characteristic is 2, let $(x^2y)y = (y^2x)x$ and $x^\lambda x^\mu = x^{\lambda+\mu}$ for $\lambda + \mu < n$, $n \geq 5$. Then $x^{n-\alpha}x^\alpha = x^n$ for every positive odd integer $\alpha < n$ and $x^{n-\beta}x^\beta = x^{n-\gamma}x^\gamma$ for all positive even integers $\beta, \gamma < n$.*

For proof observe that if $y = x$, $z = x^{n-3}$ in (3) then $x^3x^{n-3} = (x^2x^{n-3})x = x^n$. If we assume $x^{n-\alpha}x^\alpha = x^n$ for α odd, then $y = x^\alpha$, $z = x^{n-(\alpha+2)}$ in (3) yield $x^{\alpha+2}x^{n-(\alpha+2)} = x^{n-\alpha}x^\alpha$ and we have proved the part of the lemma involving odd integers.

When $y = x^2$, $z = x^{n-4}$ in relation (3), $x^{n-4}x^4 = x^{n-2}x^2$. Assume $x^{n-\beta}x^\beta = x^{n-(\beta-2)}x^{(\beta-2)}$ and set $y = x^\beta$, $z = x^{n-(\beta+2)}$. Then $x^{n-(\beta+2)}x^{\beta+2} = x^{n-\beta}x^\beta$. This completes the proof of the lemma.

A corollary of Lemma 1 is

LEMMA 2. *Under the hypotheses of Lemma 1, if $x^\lambda x^\mu = x^{\lambda+\mu}$, $\lambda + \mu < n$, for n a positive odd integer, then $x^\lambda x^\mu = x^{\lambda+\mu}$ for $\lambda + \mu = n$.*

It is only necessary to show that $x^{n-\alpha}x^\alpha = x^{n-\beta}x^\beta$ for α odd and β even. This follows from the fact that n is odd, $n - \alpha$ is even. Then write $\beta = n - \alpha$.

If n is an even integer it has the form $n = 2^s k$ where k is an odd

integer. At this point we are able to obtain the following limited result.

LEMMA 3. *Under the hypotheses of Lemma 1, if $x^\lambda x^\mu = x^{\lambda+\mu}$, $\lambda + \mu < n$, and if $n = 2k$, k odd, then $x^\lambda x^\mu = x^{\lambda+\mu}$ for $\lambda + \mu = n$.*

The substitution $y = x^{k-1}$ in (2) yields $x^{k+1}x^{k-1} = x^{2k-1}x = x^{2k}$. Since $k - 1$ is an even integer, the result follows from Lemma 1.

It is seen that given relation (2) the assumption of associativity of fourth powers implies associativity of fifth powers by Lemma 2. Then Lemma 3 implies sixth power associativity and a second application of Lemma 2 gives the associativity of seventh powers. However, associativity of eighth powers does not follow.

3. Associativity of 2ⁿth powers. Let us now consider the hypothesis $x^{2^{n-1}}x^{2^{n-1}} = x^{2^n}$, $n > 1$, and that all powers with less than 2^n factors are associative. In order to eliminate a large number of parentheses we shall write $ab \cdots x$ instead of $aR_b \cdots R_x$ where R_n denotes right multiplication by n . Then the substitution of $x + \lambda y$ for x in the left side of the equality yields $x^{2^{n-1}}x^{2^{n-1}} + \lambda^{2^n}y^{2^{n-1}}y^{2^{n-1}}$. The quantity x^{2^n} may be written $x^{2^{n-1}}x^{2^{n-2}}x^{2^{n-3}} \cdots x^2xx$. Substitution of $x + \lambda y$ for x in $x^{2^{n-1}}x^{2^{n-1}} = x^{2^n}$ gives the polynomial identity $\sum_{i=1}^{2^n-1} \lambda^i A_i^n = 0$ where A_i^n is the sum of all terms obtained by replacing factors x^{2^n-k} by y^{2^n-k} in $x^{2^{n-1}}x^{2^{n-2}}x^{2^{n-3}} \cdots x^2xx$ so that there are i factors y . There are precisely two ways of making this substitution and thus each A_i^n is the sum of two terms.

Preliminary to showing that each $A_i^n = 0$, we use (2) and (3) to see that $x^{4r}y^{2s} = x^{2r}x^{2r}y^{2s} = x^{2r}y^{2s}x^{2r} = x^{4r}y^s y^s = x^{2r}y^s x^{2r}y^s = (x^{2r}y^s)^2$ for $2r + 4s < 2^n$. The result is stated as relation

$$(4) \quad x^{4r}y^{2s} = (x^{2r}y^s)^2.$$

The study of the coefficients A_i^n is divided into two parts depending on whether i is odd or even. If i is odd, $A_i^n = z_1^{2^{n-1}}z_2^{2^{n-2}} \cdots z_{n-1}^2yx + z_1^{2^{n-1}}z_2^{2^{n-2}} \cdots z_{n-1}^2xy$ where z_j is either x or y . By (3), $A_i^n = x^{2^{n-i-1}} \cdot y^{i-1}yx + x^{2^{n-i-1}}y^{i-1}xy$. Since i is an odd integer, it follows that $2^n - i - 1 = 2p$ and $i - 1 = 2q$ for integers p and q . Also $2p + 2q = 2^n - 2$ and so $p + q = 2^{n-1} - 1$. Therefore, either p or q is even and we may use (4) to write $A_i^n = (x^p y^q)^2 yx + (x^p y^q)^2 xy$. Relation (3) then implies $A_i^n = 0$.

When i is an even integer it is necessary to consider only the case where the last two factors of one term of A_i^n are x and the last two factors of the other term are y and we may then use (3) to write $A_i^n = x^{2^n-i-2}y^i x x + x^{2^n-i}y^{i-2}y y$. The integer i is even and therefore we may write $2p = 2^n - i$ and $2q = i$. It follows that $p + q = 2^{n-1}$ and p and

q are both even or both odd. An application of (4) gives $A_i^n = (x^{p-1}y^q)^2 \cdot xx + (x^p y^{q-1})^2 yy$.

Let us suppose that p and q are both odd. Then $(x^{p-1}y^q)^2 xx = x^2(x^{p-1}y^q)(x^{p-1}y^q) = (x^{p+1}y^q)(x^{p-1}y^q) = x^{p+1}(x^{p-1}y^q)y^q = x^{2p}y^q y^q$ where we have used (2), (3), and the fact that $p-1$ and $p+1$ are even. Similarly, $(x^p y^{q-1})^2 yy = y^{2q} x^p x^p$ and (2) implies $A_i^n = 0$. Thus we have shown that $A_i^n = 0$ unless i and $2^n - i$ are multiples of four.

We now proceed to show simultaneously that the remaining A_i^n are equal to zero and that the relation

$$(5) \quad x^{2k-1}y^{2k-1-1}y = y^{2k-1}x^{2k-1-1}x$$

holds for every $k > 1$. The proof is by induction and we note that when $k = 2$, (5) reduces to (2). At this point we also have (5) for $k = 3$, since then $\sum_{i=1}^7 A_i^3 = 0$ and thus $A_4^3 = 0$. The statement $A_4^3 = 0$ is exactly (5) for $k = 3$.

Assume now that $A_i^n = 0$ for all n , and every i not a multiple of 2^{k-2} . Since $\sum_{i=1}^{2^{k-1}-1} A_i^{k-1} = 0$, $A_{2^{k-2}}^{k-1} = 0$ and (5) holds for $k-1$. Then consider the case $i = 2^{k-2}r$ where r is odd. It follows that $2^n - i = 2^{k-2}s$ with s odd, and $x^{2^{k-2}r}y^{2^{k-2}r-2}yy = x^{2^{k-2}s}y^{2^{k-2}(r-1)}y^{2^{k-2}-2}yy = (x^s y^{r-1})^{2^{k-2}} \cdot y^{2^{k-2}-1}y = z^{2^{k-2}}y^{2^{k-2}-1}y$ where we have used (3), (4), and $z = x^s y^{r-1}$. By the hypothesis of our induction $(z^{2^{k-2}}y^{2^{k-2}-1})y = y^{2^{k-2}}z^{2^{k-2}-1}z$ and then (3) and (4) may be used to show that this expression is equivalent to $y^{2^{k-2}r}x^{2^{k-2}s-2}xx$, the second term of A_i^n . Thus $A_i^n = 0$ for i a multiple of 2^{k-2} and therefore we have (5) for all values of k .

Using (5) it is possible to prove

LEMMA 4. *Under the hypotheses of Lemma 1, if $x^\lambda x^\mu = x^{\lambda+\mu}$, $\lambda + \mu < m$, $m \geq 6$ and $m = 2^t k$, k odd, then $x^\lambda x^\mu = x^{\lambda+\mu}$ for $\lambda + \mu = m$.*

For if $k = t + 1$ and $y = x^{k-1}$ in (5), it follows that $x^{2^t}x^{(k-1)(2^t-1)}x^{k-1} = x^{(k-1)2^t}x^{2^t-1}x$. Consequently, $x^{[2^t k - (k-1)]}x^{k-1} = x^{2^t k}$. Since k is odd, $k-1$ is even and the conclusion follows from Lemma 1 and the proof of Lemma 2. Note that Lemma 3 is the case $t = 1$ of Lemma 4.

The results of the lemmas combine to give Theorem 4 and we have already shown that the corollary follows. We now proceed to show that the hypotheses of our theorem are actually necessary.

4. Necessity of the hypotheses. In order to show that the assumption of the associativity of 2^n th powers is necessary, we shall construct an algebra in which all powers are associative except powers with 2^n factors. Moreover, this construction is valid for every $n > 1$.

Let \mathfrak{A} be the algebra over a field \mathfrak{F} whose characteristic is 2 and let \mathfrak{F} contain at least four elements. Also let \mathfrak{A} have the basis

$a, a^2, a^3, \dots, a^{2^n}$ and $a^{2^{n-1}}a^{2^{n-1}}$. The multiplication table is given by $a^\lambda a^\mu = a^{\lambda+\mu}$ for $\lambda + \mu < 2^n$, $a^\lambda a^\mu = 0$ for $\lambda + \mu > 2^n$, $a^{2^n-\alpha}a^\alpha = a^{2^n}$ for α odd, $a^{2^n-\beta}a^\beta = a^{2^{n-1}}a^{2^{n-1}}$ for β even, and $a^{2^n-1}a^{2^n-1}a^\lambda = 0$ for every λ . The general element x of \mathfrak{A} may be written $x = \sum_{i=1}^{2^n} \gamma_i a^i + \delta a^{2^{n-1}} a^{2^{n-1}}$. We compute $x^2 = \sum_{i=1}^{2^{n-1}-1} \gamma_i^2 a^{2i} + \gamma_{2^{n-1}}^2 a^{2^{n-1}} a^{2^{n-1}}$ and then

$$x^3 = \sum_{i=1}^{2^{n-1}-1} \sum_{j=1}^{2^{n-1}} \gamma_i^2 \gamma_j a^{2i+j}$$

It follows that

$$x^4 = \sum_{i=1}^{2^{n-1}-1} \sum_{j=1}^{2^{n-1}} \sum_{k=1}^{2^{n-1}} \gamma_i^2 \gamma_j \gamma_k a^{2i+j+k}$$

Since \mathfrak{A} has characteristic 2 and because of the symmetry in j and k of the expression x^4 we have $x^4 = \sum_{i=1}^{2^{n-1}-1} \sum_{j=1}^{2^{n-1}-1} \gamma_i^2 \gamma_j^2 a^{2i+2j}$. Due to symmetry we again have two like terms whenever $i \neq j$, so that $x^4 = \sum_{i=1}^{2^{n-1}-1} \gamma_i^4 a^{4i} + \gamma_{2^{n-2}}^4 a^{2^{n-1}} a^{2^{n-1}}$. On the other hand

$$x^2 x^2 = \sum_{i=1}^{2^{n-1}-1} \gamma_i^2 a^{2i} \sum_{j=1}^{2^{n-1}-1} \gamma_j^2 a^{2j} = \sum_{i=1}^{2^{n-1}-1} \sum_{j=1}^{2^{n-1}-1} \gamma_i^2 \gamma_j^2 a^{2i+2j} = x^4$$

Having the associativity of fourth powers and the hypothesis on the number of elements in \mathfrak{F} , we use Lemmas 2 and 3 to see that powers with five, six, and seven factors are associative. Furthermore, Lemma 1 implies that if $x^4 x^4 = x^8$, then all eighth powers are associative.

Computing, we have

$$x^4 x^4 = \sum_{i=1}^{2^{n-2}-1} \sum_{j=1}^{2^{n-1}-1} \gamma_i^4 \gamma_j^4 a^{4i+4j} = \sum_{i=1}^{2^{n-2}-1} \gamma_i^8 a^{8i} + \gamma_{2^{n-2}}^8 a^{2^{n-1}} a^{2^{n-1}}$$

and $x^7 x = \sum_{i_1, \dots, i_8=1}^{2^{n-1}} \gamma_{i_1} \dots \gamma_{i_8} a^{i_1} \dots a^{i_8}$. Due to symmetry $i_1 = i_2 = \dots = i_8 = i$ and so $x^4 x^4 = x^7 x = x^8$.

Assume now that we have the associativity of 2^{q-1} st powers for $q < n$ and therefore

$$\begin{aligned} x^{2^{q-1}} &= \sum_{i_1, \dots, i_{2^{q-1}}=1}^{2^{n-1}} \gamma_{i_1} \dots \gamma_{i_{2^{q-1}}} a^{i_1} \dots a^{i_{2^{q-1}}} \\ &= \sum_{i=1}^{2^{n-q+1}-1} \gamma_i^{2^{q-1}} a^{2^{q-1}i} + \gamma_{2^{n-q+1}}^{2^{q-1}} a^{2^{n-1}} a^{2^{n-1}} \end{aligned}$$

Then Lemmas 2 and 4 give the associativity of powers with less than 2^q factors. It follows that

$$x^{2^{q-1}} x^{2^{q-1}} = x^{2^q} = \sum_{i=1}^{2^{n-q}} \gamma_i a^{2^q} + \gamma_{2^{n-q}} a^{2^{n-1}} a^{2^{n-1}}.$$

Thus all powers involving less than 2^n factors are associative, but 2^n th powers are not associative.

The hypothesis $(x^2y)y = (y^2x)x$ is also necessary. Albert has given an example² of a commutative algebra over the field of two elements in which fourth powers associate but no higher powers associate. This is an example in which relation (2) does not hold. But then the conclusions of Lemmas 1 and 2 do not follow.

5. Jordan algebras of characteristic 2. As an application of our theorem we prove the power-associativity of a Jordan algebra over a field containing at least four elements and with characteristic 2. A Jordan algebra is a commutative algebra whose elements satisfy the identity $(x^2y)x = x^2(yx)$. This identity may be linearized to give

$$(6) \quad (x^2y)z = x^2(yz).$$

The value $z=y$ in (6) yields $(x^2y)y = x^2y^2$ and by symmetry $(y^2x)x = x^2y^2$ so relation (2) holds. Assume $x^\lambda x^\mu = x^{\lambda+\mu}$ for $\lambda+\mu < 2^n$ and let $y = x^{2^n-3}$, $z=x$ in (6) to obtain $x^{2^n} = x^2x^{2^n-2}$. Lemma 1 implies $x^{2^{n-1}}x^{2^{n-1}} = x^2x^{2^n-2}$ and then Theorem 4 implies power-associativity.

UNIVERSITY OF WASHINGTON

² See the first paper of footnote one.