Gary Birkenmeier

Exponentiation without associativity

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 24 (1983), No. 2, 3--7

Persistent URL: `http://dml.cz/dmlcz/142511`

Exponentiation Without Associativity

GARY F. BIRKENMEIER
Department of Mathematics Southeast Missouri State University*)

Received 30 March 1983

In this note we give examples which show that there are many distinct types of exponentiation. A definition of exponentiation will be presented which encompasses these various types of exponentiation. Using this definition, several well known results on exponentiation in a semigroup, including the Euler-Fermat Theorem for finite semigroups, are generalized.

V této poznámce uvádíme příklady ukazující, že existuje mnoho různých typů exponenciace. Bude prezentována definice exponenciace, zahrnující tyto různé speciální typy. Užitím této definice jsou zobecněny některé známé výsledky o exponenciaci v pologrupě, včetně Euler-Fermatovy věty pro konečné pologrupy.

В этой заметке мы включаем примеры показывающие, что существуют многие различные типы образования степеней. Будет представлено определение образования степеней, включающее эти различные частные типы. Используя это определение, мы обобщаем некоторые известные результаты о степенях в полугруппе, включая теорему Эйлера-Ферматa для конечных полугрупп.

Throughout this note, G denotes a groupoid (i.e. a nonempty set with a binary operation); and N denotes the set of counting numbers.

Definition 1. Let P and S be nonempty sets with $x \in S$. A *P-exponentiation* of x is a mapping $E: \{x\} \times P \to S$. For $k \in P$, x^k denotes $E(x, k)$ and is called the k-th power of x.

Example 2. Let S be a set and M the set of all mappings from S into S.

(i) An M-exponentiation of $x \in S$ can be defined as $E(x,f) = x^f = (x)f$ for $f \in M$. This type of exponentiation is considered in Bruck's article on nonassociative integers [1, pp. 82–86].

(ii) An N-exponentiation of $x \in S$ can be defined as

$$E(x, i) = \begin{cases} x & \text{if } i = 1 \\ (x)f^{i-1} & \text{if } i > 1 \end{cases}$$

*) Cape Girardeau, Missouri 63701, U.S.A.

where $i \in N$, $f \in M$, and f^{i-1} denotes the $(i-1)$-th composition of f. If S is a semigroup and f is the inner right translation defined by $(s)f = sx$ for all $s \in S$, then E is the usual exponentiation of x in the semigroup S.

Example 3. Let $S = \{x, b, c\}$. An N-exponentiation of x can be defined as

$$E(x, i) = x^i = \begin{cases} x \text{ if } i = 1 \\ b \text{ if } i \text{ is even} \\ c \text{ if } i \text{ is odd} . \end{cases}$$

Usually exponentiation is defined in terms of an associative binary operation. The next three definitions of N-exponentiations in a groupoid will be used to exemplify the generality of our results.

Definition 4. For $x \in G$ and $n \in N$, $x^1 = x$ and $x^{n+1} = x^n x$.

Definition 5. For $x \in G$ and $n \in N$, $x^1 = x$ and

$$x^{n+1} = \begin{cases} xx & \text{if } n = 1 \\ x^2 x^{n-1} & \text{if } n > 1 . \end{cases}$$

Definition 6. For $x \in G$ and $n \in N$, $x^1 = x$ and

$$x^{n+1} = \begin{cases} x^n x & \text{if } n+1 \text{ is odd} \\ (x^{(n+1)/2})(x^{(n+1)/2}) & \text{if } n+1 \text{ is even} . \end{cases}$$

Using the following nonassociative operation table and considering a^5 in each of the last three definitions, we can see that these definitions are distinct.

Table I

•	*a*	*b*	*c*	*d*
a	*c*	*b*	*c*	*b*
b	*b*	*c*	*a*	*c*
c	*b*	*a*	*a*	*d*
d	*d*	*c*	*d*	*a*

Definition 7. Suppose S is a set and $x \in S$ with an N-exponentiation E and x has only finitely many distinct powers. Let r be the least positive integer such that $x^r = x^n$ [i.e. $E(x, r) = E(x, n)$] for some positive integer n where $n > r$. Let u be the least possible value for n. Call r the *index* of x and $m(= u - r)$ the *period* of x. In Example 3, x has index 2 and period 2. Using Table I, a has index 3 and period 1 under Definition 4; but, under Definitions 5 and 6, a has index 1 and period 3. Also, note that under Definition 6, b has index 1 and period 4 although $b^3 = b^4$.

Theorem 8. Let S be a set and $x \in S$ with an N-exponentiation E such that x has index r and period m under E. Then the following statements are equivalent:

(a) If $x^i = x^j$ then $x^{i+1} = x^{j+1}$.

(b) If $x^i = x^j$ then $x^{i+h} = x^{j+h}$ for all $h \in N$.

(c) Let $k, n \in N$. Then $k \geqq r$ and $m \mid n$ if and only if $x^{k+n} = x^k$.

Proof. (a $\Rightarrow$ b). By induction, a implies b.

(b $\Rightarrow$ c). Suppose $k \geqq r$, $m \mid n$, and whenever $x^i = x^j$ then $x^{i+h} = x^{j+h}$. There exists integers p and d such that $k = r + p$ and $n = dm$. By Definition 7, $x^r = x^{r+m}$. From part b, $x^{r+m} = x^{(r+m)+m} = x^{r+2m}$. By induction $x^r = x^{r+dm}$. Hence $x^{r+p} = = x^{(r+dm)+p}$. Therefore $x^k = x^{k+n}$.

Now assume $x^{k+n} = x^k$ and part b holds. By Definition 7, $k \geqq r$. Claim: there exists a positive integer $s \leqq m$ such that $x^k = x^{r+s}$. If $k = r$, let $s = m$. If $r < k \leqq \leqq r + m$, let $s = k - r$. Otherwise there exists $t > m$ such that $k = r + t$. There exists integers j and w such that $t = jm + w$ where $\emptyset \leqq w < m$. If $w = \emptyset$, then $x^k = x^r$. So, let $s = m$. For $w \neq \emptyset$, $x^k = x^{r+w+jm} = x^{r+w}$. So, let $s = w$. Hence the claim is proved. Now suppose $m \nmid n$. Either $n < m$ or $n > m$. If $n > m$, $n = hm + q$ where $1 \leqq q < m$. Thus $x^k = x^{k+hm+q} = x^{k+q}$. Hence in either case there exists a positive integer $v < m$ such that $x^k = x^{k+v}$. From the claim there exists an integer e such that $s + e = m$. Consider $x^r = x^{r+m} = x^{r+s+e} = x^{k+e} = x^{k+v+e} = x^{r+s+v+e} = = x^{(r+s+e)+v} = x^{(r+m)+v} = x^{r+v}$ where $v < m$. This contradicts Definition 7. Hence $m \mid n$.

(c $\Rightarrow$ a). Suppose part c holds and $x^i = x^j$. Without loss of generality, assume $i < j$. By part c, $j = i + qm$. Again by part c, $x^{i+1} = x^{(i+1)+qm}$. Thus $x^{i+1} = x^{j+1}$.

Definition 9. Let S be a set and $x \in S$ with an N-exponentiation E such that x has only finitely many distinct powers under E. We say E is a *cyclic N-exponentiation* if $x^i = x^j$ implies $x^{i+1} = x^{j+1}$.

Clearly, if S is a finite set then Example 2 (ii) is a cyclic N-exponentiation. Hence, if G is a finite groupoid then Definition 4 is a cyclic N-exponentiation for every element of G. Also, Example 3 is a cyclic N-exponentiation. Using Table I, Definition 5 is cyclic for d; but it is not cyclic for a, b, or c. Definition 6 is not cyclic for any element in the groupoid of Table I.

Table II.

$\cdot$	a	b	c	d	e
a	c	b	c	b	d
b	d	b	d	d	c
c	e	c	b	e	d
d	b		e	e	b
e	b	c	a	b	a

Definitions 4 and 5.

The following tables which are halfgroupoids [2, p. 1] were constructed so that every element has a cyclic N-exponentiation under the indicated definitions. The blanks can be arbitrarily filled with a, b, c, d (or e in Table II) to form a groupoid. Thus one can see that every element of a groupoid can have a cyclic N-exponentiation with definitions of exponentiation other than Definition 4.

Table III.

$\cdot$	a	b	c	d
a	b			
b	c	d		
c			d	
d	c	b	c	d

Definition 6.

Corollary 10. Let S be a set and $x \in S$ with a cyclic N-exponentiation E such that x has index r and period m under E. Then there exists a unique positive integer e such that $x^e = x^{2e}$ where $r \leqq e \leqq r + m - 1$. Furthermore $m \mid e$.

Proof. There exists a unique $e \in N$ such that $r \leqq e \leqq r + m - 1$ and $m \mid e$. From Theorem 8, $x^{2e} = x^{e+e} = x^e$.

Hence Corollary 10 generalizes the well known result that some power of every element of a finite semigroup is idempotent [3, p. 20]. The next corollary is a direct consequence of Theorem 8 and generalizes the Euler-Fermat Theorem for finite semigroups [4].

Corollary 11. Let S be a finite set such that every element s has a cyclic N-exponentiation E_s which may vary from element to element. Let $R = \max \{r_s \mid r_s$ is the index of s under $E_s\}$ and $M =$ l.c.m. $\{m_s \mid m_s$ is the period of s under $E_s\}$. Then R and M are the least positive integers such that $s^{R+M} = s^R$ under E_s for all $s \in S$.

If Definition 5 is used for every element in the halfgroupoid of Table II then $R = 4$ and $M = 12$. However if Definition 4 is used for a, b, and c and Definition 5 is used for d and e then $R = 4$ and $M = 30$.

Lemma 12. Let S be a set and $x \in S$ with a cyclic N-exponentiation E such that x has index r and period m under E. Let $C_x = \{r, r + 1, \ldots, r + m - 1\}$. Define two binary operations, $\oplus$ and $*$, on C_x by $a \oplus b = c$ where $x^{a+b} = x^c$ and $a * b = d$ where $x^{ab} = x^d$ for $a, b, c, d \in C_x$ with $+$ and juxtaposition denoting integer addition and multiplication, respectively. Then $(C_x, \oplus, *)$ is ring isomorphic to Z/m (i.e. integers modulo m).

Proof. There exists a positive integer j and $e \in C_x$ such that $e = jm$. Define e_n to be that element of C_x such that $x^{e_n} = x^{e+n}$ for $n \in \{0, 1, 2, \ldots, m - 1\}$. Define

$h: C_x \to Z/m$ by $(e_n)h = \bar{n}$ (i.e. the equivalence class of integers congruent to n mod m). It follows routinely that h is the desired isomorphism. Note $e_n \in \bar{n}$.

The final result generalizes the well known theorem that if X is a finite cyclic group generated by x then x^t is a generator if and only if t is relatively prime to m [6, p. 17].

Theorem 13. Let S be a set and $x \in S$ with a cyclic N-exponentiation E such that x has index r and period m under E. For a positive integer $t \geqq r$, then t is relatively prime to m if and only if for each $v \in N$, where $v \geqq r$, there exists a positive integer $n \leqq m$ (depending on v) such that $x^{tn} = x^v$.

Proof. Let $k \in N$, then k is a generator for the cyclic group Z/m if and only if $(k, m) = 1$. Hence, from Lemma 12, e_k is a generator for $(C_x, \oplus)$ if and only if $(e_k, m) = 1$. Consequently for $t \geqq r$, $(t, m) = 1$ if and only if there exists $e_k \in C_x$ such that $(e_k, m) = 1$ and $x^t = x^{e_k}$. Since $v \geqq r$ there exists $c \in C_x$ such that $x^v = x^c$. Thus, if $(t, m) = 1$ then there exists $n \in N$ such that $x^{ne_k} = x^c$. By repeated use of Theorem 8(b), $x^{ne_k} = x^{nt}$. Thus $x^{nt} = x^v$. The converse follows by a reverse argument.

Our final result characterizes a cyclic N-exponentiation in terms of a groupoid.

Proposition 14. Let S be a nonempty set and E is an N-exponentiation of $x \in S$. Let $P_x = \{x^n \mid n \in N\}$ and define a relation $*$ from $P_x \times P_x$ into P_x by $(x^k, x^j)* = x^{k+1}$. Then $(P_x, *)$ is a groupoid if and only if whenever $x^j = x^k$ then $x^{j+1} = x^{k+1}$ if and only if $(P_x, *)$ is a right cancellative left unar.

Proof. The proof is routine and uses Theorem 8.

Acknowledgement

The results in this paper grew out of joint work done by the author and S. J. Plackemeier. The original results were restricted to the exponentiation indicated in Definition 4 for a groupoid and appear in [5].

References

[1] Albert, A. A.: "Studies in Modern Algebra," II, Mathematical Association of America Prentice-Hall, Englewood Cliffs, N. J., 1963.

[2] Bruck R. H.: "A Survey of Binary Systems," Springer-Verlag, Berlin, 1958.

[3] Clifford, A. H. and Preston, G. B.: "The Algebraic Theory of Semigroups," I, American Mathematical Society, Providence, R.I., 1961.

[4] Ecker, A.: Comment on the note: "The congruence $a^{r+s} \equiv a^r$ (mod m)" by A. E. Livingston and M. L. Livingston, Amer. Math. Monthly, 87 (1980), 811—814.

[5] Plackemeier, S. J.: A semigroup of power functions acting on a finite grupoid, M. A. Thesis, directed by G. F. Birkenmeier, Southeast Missouri State University, December, 1981.

[6] Rotman, J. J.: "The Theory of Groups," Allyn and Bacon, Boston, MA, 1973.