1-1-1976

# Multiplicatively Periodic Rings

Ted Chinburg
*University of Pennsylvania*

Melvin Henriksen
*Harvey Mudd College*

# MATHEMATICAL NOTES

EDITED BY RICHARD A. BRUALDI

*Material for this Department should be sent to Richard A. Brualdi, Laboratoire Calcul des Probabilités, Université de Paris, T.56, 4 Place Jussieu, 75–230 Paris, France.*

## MULTIPLICATIVELY PERIODIC RINGS

TED CHINBURG AND MELVIN HENRIKSEN

**1. Introduction.** A ring $R$ is called *periodic* if for each element $a$ of $R$ there is a positive integer $n(a)$ such that $a^{n(a)+1} = a$. If there is a positive integer $n$ such that $a^{n+1} = a$ for all $a$ in $R$, then the smallest such $n$ is called the *period* of $R$, and $R$ is called a *J-ring* (see [7]). It is well known that every periodic ring is commutative [**6**, Chapter X].

A ring $R$ is called a $p^k$*-ring* in [**8**] if there is a prime $p$ and a positive integer $k$ such that $pa = 0$ and $a^{p^k} = a$ for all $a$ in $R$. In [7], J. Luh uses Dirichlet's Theorem on primes in an arithmetic progression to show that $R$ is a $J$-ring if and only if it is the direct sum of finitely many $p^k$-rings. In this note we prove the following generalization of Luh's result without using Dirichlet's theorem:

THEOREM 1. *A ring $R$ is periodic if and only if it is the union of a countable ascending chain $\{R(n)\}$ of $J$-rings such that every $J$-ring contained in $R$ is contained in some $R(n)$. Moreover, each $R(n)$ is the direct sum of finitely many $p^k$-rings.*

We use Theorem 1 to show that the $J$-subrings of a periodic ring form a lattice with respect to join and intersection (the *join* of two subrings is the smallest subring containing both of them).

After noting that every $J$-ring has nonzero characteristic, we determine for which positive integers $n$ and $m$ there exist $J$-rings of period $n$ and characteristic $m$. This generalizes a problem posed by G. Wene in [**9**].

**2. A basic lemma.** If $R$ is a ring and $n$ is a positive integer, let $\mathcal{A}(R, n) = \{a \in R : na = 0\}$, and for any $a \in R$, let $S(a)$ denote the subring of $R$ generated by $a$. Some parts of the following lemma are well known but appear in the literature only in the middle of proofs.

LEMMA 1. *Suppose $a$ is a non-zero element of a periodic ring $R$, $p$ is a prime, $n$, $r$ and $s$ are positive integers, $a^{n+1} = a$, and $(2a)^{s+1} = 2a$.*

(a) *$a^n$ is the identity element of $S(a)$.*

(b) *There is a non-zero square-free integer $m$, dependent only on $n$ and $s$, such that $a \in \mathcal{A}(R, m)$.*

(c) *If $pa = 0$, there is a positive integer $k$, dependent only on $n$ and $p$, such that $a^{p^k} = a$.*

(d) *If $pa = 0$, then $S(a)$ is isomorphic to the direct sum of finitely many finite fields of characteristic $p$.*

(e) *If $m = \prod_{i=1}^r p_i$ is the product of finitely many distinct primes $p_i$, then $\mathcal{A}(R, m)$ is the direct sum $\sum_{i=1}^r \oplus \mathcal{A}(R, p_i)$ of the rings $\mathcal{A}(R, p_i)$.*

(f) *If $R = \sum_{i=1}^r \oplus R_i$, where each $R_i$ is a $J$-ring of period $n_i$, then $R$ is a $J$-ring whose period is the least common multiple of $\{n_i : i = 1, \ldots, r\}$.*

*Proof.* The proof of (a) is left as an exercise.

If $a^{n+1} = a$ and $(2a)^{s+1} = 2a$, then by (a), $2a = (2a)^{s+1} = (2a)^{ns+1} = 2^{ns+1}a^{ns+1} = 2^{ns+1}a$. Hence $a$ has non-zero characteristic $m$. Since the only nilpotent element of $R$ is 0, $m$ is square free, so (b) holds.

In (c), suppose $n = p^e d$ for some integers $e \geqq 0$ and $d \geqq 1$ and that $(d, p) = 1$. By the Euler-Fermat Theorem [**5**, Chapter 6] there is a positive integer $k$ such that $p^k \equiv 1 \pmod d$. Then $(p^k - 1)p^e \equiv 0$

(mod $n$) so $a^{p^{k+e}} = a^{p^e}$ from part (a). Since $pa = 0$ we have

$$(a^{p^k} - a)^{p^e} = a^{p^{k+e}} - a^{p^e} = 0.$$

But $R$ has no nonzero nilpotents, so $a^{p^k} - a = 0$ and (c) holds.

If $pa = 0 \neq a$, then by (a), $S(a)$ is an algebra over the ring $Z_p$ of integers mod $p$. Since $a^{n+1} - a = 0$, there is a monic polynomial $\phi(x) \in Z_p[x]$ such that $S(a)$ and $Z_p[x]/\phi(x)Z_p[x]$ are isomorphic. Since $S(a)$ has no nonzero nilpotents, $\phi(x) = \Pi_{i=1}^r \phi_i(x)$ is a product of distinct irreducible elements $\phi_i(x) \in Z_p[x]$ and

$$Z_p[x]/\phi(x)Z_p[x] = \sum_{i=1}^r \oplus Z_p[x]/\phi_i(x)Z_p[x].$$

But each of these latter direct summands is a finite field, so (d) follows.

Part (e) follows from the well-known fact that every torsion abelian group $G$ may be represented as a direct sum of $p$-groups [4, p. 21]. Part (f) follows from (a), so the lemma is proved.

**3. The proof of Theorem 1 and some consequences.** Clearly the union of a chain of periodic rings is periodic, so it suffices to show that every periodic ring has the structure described in Theorem 1.

Let $\{p(i)\}$ denote the sequence of primes in numerical order, and for any positive integers $k$ and $r$, let $m(k) = \Pi_{i=1}^k p(i)$ and $P(r,k) = \{a \in \mathscr{A}(R, p(r)) \colon a^{p(r)^{k!}} = a\}$. Since every periodic ring is commutative, each $P(r,k)$ is a $p(r)^{k!}$-ring. Let $R(k)$ denote the subring of $R$ generated by $\bigcup_{i=1}^k P(i,k)$. Now, $R(k) \subset \mathscr{A}(R, m(k))$, and by Lemma 1(e), $\mathscr{A}(R, m(k)) = \Sigma_{i=1}^k \oplus \mathscr{A}(R, p(i))$. Therefore $R(k)$ is isomorphic to $\Sigma_{i=1}^r \oplus P(i,k)$, and hence is the direct sum of finitely many $p_i^{k_i}$-rings. Thus, $R(k)$ is a $J$-ring by Lemma 1(f), and $R(k) \subset R(k+1)$ since $P(i,k) \subset P(i,k+1)$ if $1 \leqq i \leqq k$.

If $n$ and $s$ are positive integers, let $T(n,s) = \{a \in R \colon a^{n+1} = a \text{ and } (2a)^{s+1} = 2a\}$. Clearly $\bigcup_{n,s=1}^\infty T(n,s) = R$, and if $T$ is a $J$-subring of $R$ with period $n$, then $T \subset T(n,n)$. Hence to complete the proof of Theorem 1, it suffices to show that given $n$ and $s$, there is a positive integer $k$ for which $T(n,s) \subset R(k)$.

By Lemma 1(b, e), there is a positive integer $r$ such that

$$T(n,s) \subset \mathscr{A}(R, m(r)) = \sum_{i=1}^r \oplus \mathscr{A}(R, p(i)).$$

If $1 \leqq i \leqq r$, then by Lemma 1(c), there is a positive integer $k^*(i)$ dependent only on $p(i)$ and $n$ such that if $a \in T(n,s) \cap \mathscr{A}(R, p(i))$, then $a^{p(i)^{k^*(i)}} = a$. Hence if $k(i) = \max(i, k^*(i))$, then $T(n,s) \cap \mathscr{A}(R, p(i)) \subset R(k(i))$. We conclude that if $k = \max(k(1), \ldots, k(r))$ then $T(n,s) \subset R(k)$, so by our previous remarks Theorem 1 follows.

Clearly the intersection of any two $J$-subrings of a periodic ring is a $J$-ring. By Theorem 1, the union of any two $J$-subrings of $R$ is contained in a $J$-subring of $R$, and so their join is a $J$-subring of $R$. Hence we have proved

COROLLARY 1. *The $J$-subrings of a periodic ring $R$ form a lattice with respect to the operations of intersection and join.*

By Theorem 1, every $J$-ring has finite characteristic. The next theorem describes the relation between the period and the characteristic of a $J$-ring.

THEOREM 2. *If $n$ and $m$ are positive integers, then there is a $J$-ring of period $n$ and characteristic $m$ if and only if $m = n = 1$ or $m = \Pi_{i=1}^r p(i)$ is a product of distinct primes and $n$ is the least common multiple of $\{p(i)^{k(i,j)} - 1 \colon i = 1, \ldots, r \text{ and } j = 1, \ldots, l(i)\}$ for some set of positive integers $\{k(i,j)\}$ and $\{l(i)\}$.*

*Proof.* Clearly $R$ has characteristic 1 if and only if $R = \{0\}$, so we suppose $m > 1$.

If $k$ is a positive integer and $p$ is a prime, let GF$[p^k]$ denote the finite field with $p^k$ elements. It is well known (see [1, Chapter 5]) that GF$[p^k]$ has characteristic $p$ and a cyclic multiplicative group.

Hence $GF(p^k]$ is a $J$-ring of period $(p^k - 1)$. Thus if $n, m, \{k(i,j)\}$ and $\{l(i)\}$ are as above and $m > 1$, then $R = \Sigma \oplus \{GF[p(i)^{k(i,j)}]: i = 1, \ldots, r \text{ and } j = 1, \ldots, l(i)\}$ is a $J$-ring of period $n$ and characteristic $m$ by Lemma 1(f).

Conversely suppose $R \neq \{0\}$ is a $J$-ring of characteristic $m$ and period $n$. By Theorem 1, $R = \Sigma_{i=1}^{r} \oplus R(i)$ for some set of $p(i)^{k(i)}$-rings $R(i) \neq \{0\}$ having periods $n(i)$. Then $n =$ L.C.M.$\{n(i): i = 1, \ldots, r\}$ by Lemma 1(f) and $m = \Pi_{i=1}^{r} p(i)$. If $0 \neq a \in R(i)$ let $n_a$ denote the period of $S(a)$. Clearly $n(i) =$ L.C.M.$\{n_a : a \in R(i)\}$. By Lemma 1(d, f), $n_a =$ L.C.M.$\{p(i)^{k(i,j)} - 1: j = 1, \ldots, l_a\}$ for some set of positive integers $\{k(i,j): j = 1, \ldots, l_a\}$, so Theorem 2 follows.

Suppose $n$ is the period of a $J$-ring $R$. In [**9**], G. Wene calls $n+1$ the $\mu$-value of $R$, and asks for which positive integers $k$ there exist $J$-rings having $\mu$-value $k$. An answer to this question follows readily from Theorem 2. He also asks the reader to show that there are infinitely many $k$ that are not the $\mu$-value of any $J$-ring. The following corollary determines when an integer of the form $p^n + 1$ is the $\mu$-value of some $J$-ring.

COROLLARY 2. *Suppose $p$ is a prime and $n$ is a positive integer. Then $p^n$ is the period of some $J$-ring if and only if either*:
(a) *$p$ is odd, $n = 1$, and $p = 2^s - 1$ for some positive integer $s$, or*
(b) *$p = 2$, and $2^n + 1$ is a prime or $n = 3$.*

*Proof of* (a). It follows immediately from Theorem 2 that $p^n$ is a period of some $J$-ring if and only if $p^n = 2^s - 1$ for some positive integer $n$. In [**3**, Corollary 2], J. W. Cassells has shown that this equation has a solution if and only if $n = 1$, so (a) follows.

*Proof of* (b). By Theorem 2, $2^n$ is a period of some $J$-ring if and only if $2^n = p^s - 1$ for some odd prime $p$ and positive integer $s$. By [**3**, Theorem IV], this equation has a solution if and only if $s = 1$ or $n = 3$, so (b) holds.

Let $K$ denote the set of all positive integers $k$ for which there exist $J$-rings having $\mu$-value $k$. It follows from Corollary 2 that $p^n + 1 \in K$ if and only if $n = 1$ and $p = 2^s - 1$ is a Mersenne prime, $p^n + 1 = 9$, or $p^n + 1 = 2^n + 1$ is a Fermat prime. Consequently there are infinitely many integers of the form $p^n + 1$ that are not in $K$.

A more satisfactory solution of [**9**] would provide an efficient algorithm for deciding when a given positive integer is in $K$. It would also be interesting to determine the asymptotic density of $K$ if this density exists.

Theorem 1 reduces the problem of determining the structure of an arbitrary periodic ring to the study of $p^k$-rings. The structure of such rings is described by R. Arens and I. Kaplansky in [**2**, pp. 470–477].

**References**


1. A. A. Albert, Fundamental Concepts of Higher Algebra, University of Chicago Press, 1956.
2. R. F. Arens and I. Kaplansky, Topological representations of algebras, Trans. Amer. Math. Soc., 63 (1948) 457–481.
3. J. W. Cassells, On the equation $a^x - b^y = 1$, Amer. J. Math., 7 (1953) 159–162.
4. L. Fuchs, Abelian Groups, Hungarian Academy of Science, Budapest, 1958.
5. G. Hardy and E. Wright, An Introduction to the Theory of Numbers, Oxford University Press, Oxford, England, 1945.
6. N. Jacobson, Structure of Rings, Amer. Math. Soc. Colloq. Publ., XXXVII, 1956.
7. J. Luh, On the structure of $J$-rings, this MONTHLY, 74 (1967) 164–166.
8. N. H. McCoy and D. Montgomery, A representation of generalized Boolean rings, Duke Math. J., 3 (1937) 455–459.
9. G. Wene, Problem 5972, this MONTHLY 81 (1974) 524. (**Added in proof,** 6/10/76: A solution to Problem 5972 is given in this MONTHLY, 83 (1976) 66.)


DEPARTMENT OF MATHEMATICS, HARVEY MUDD COLLEGE, CLAREMONT, CA 91711.