International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 /doi:10.14445/22315373/IJMTT-V67I1P510
Volume 67 Issue 1, 66-69, January, 2021

A Study on Characteristic of Rings

Laxman Saha
Assistant professor, Department of Mathematics, Balurghat College, Balurghat 733101, India

Abstract -- *The characteristic of a ring R, denoted by $\Psi(R)$, is the smallest positive integer n such that $nr = 0$ for all $r \in R$. If no such integer exists, we say that R has characteristic 0. In this article, the characteristic of a ring $(R, +, .)$ is presented in terms of the order of the elements in the commutative group $(R, +)$. Also it has been shown that the prime generators of $O(R)$ and $\Psi(R)$ are same. This article also gives a relationship among $\Psi(R), \Psi(I)$ and $\Psi(R/I)$ for any ring R and any ideal I of R.*

Keywords -- *Group, Ring, Characteristic.*

I. INTRODUCTION

For a given ring $(R, +, .)$ and $n \in \mathbb{N}$, an important task is to find some subrings which are isomorphic to a factor ring $\mathbb{Z}/n\mathbb{Z}$. The characteristic of a ring determines the number n for which the ring contains a subring isomorphic to Z=nZ. If there exist a positive integer n such that $nr = 0$ for each element r of a ring R, the smallest such positive integer is called the *characteristic* of R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\Psi(R)$. A *ring R with finite characteristic* we mean that $\Psi(R) \neq 0$. In this article, the characteristic of a ring $(R, +, .)$ is presented in terms of the order of the elements in the commutative group $(R, +)$. Also it has been shown that the prime generators of $O(R)$ and characteristic of R are same. This article also gives a relationship among $\Psi(R), \Psi(I) and\ \Psi(R/I)$ for any ring R and any ideal I of R.

II. PRELIMINARIES

In this section we give some preliminary results, definitions and lemmas on group theory and ring theory.

Theorem 2.1. *(Lagrange Theorem)[1]. Let G be a finite group and H be a subgroup of G. Then $O(H)$ divides $O(G)$.*
Corollary 2.1. *If G be a finite group and $a \in G$, then $O(a)|O(G)$. Moreover, $a^{O(G)} = e_G$ for all $\in G$, where e_G denotes the identity elements of G.*
Theorem 2.2. *(Cauchy's Theorem) [1]. If G is a finite group and p is a prime dividing $O(G)$, then G has an element of order p.*

Definition 2.1. The *additive order* of an element$a$, denoted by $O^+(a)$, in the ring $(R, +, .)$, we mean the order of the element a in the group $(R, +)$. An element $a \in R$ is said to be *maximal additive order element* if $O^+(a) \geq O^+(b)$ for all $b \in R$.

The following two lemmas follow from the definition of the characteristic of a ring R.

Lemma 2.1. *A ring have finite characteristic if and only if the additive order of maximal elements are finite.*

Lemma 2.2. *Let R be a ring with unity* 1. *If $\Psi(R) \neq 0$, then $O^+(a)|O^+(1)$ for all $a \in R$.*

Corollary 2.2. *The identity element of a ring ring with unity* 1 *is a maximal additive order element.*

From here to onwards, we denote the least common multiple of $n_1, n_2, n_3, , \ldots, n_r$ by $lcm\ \{n_1, n_2, n_3, \ldots, n_r\}$.

III. RESULTS ON CHARACTERISTIC OF A RING

In this section first we present some results on characteristic of a ring R in terms of the order of the elements in the commutative group $(R, +)$. Then we show that the prime generators of $O(R)$ and characteristic of R are same.
Lemma 3.1. *Let G be commutative group and a and b be two elements of G of order m and n, respectively. Then there exists an element c in G such that the order of c is the least common multiple of m and n.*

Theorem 3.1. *For a finite ring R, $\Psi(R)|O(R)$, where $\Psi(R)$ denotes the characteristic of R.*

Proof: Let $O(R) = m$. Applying Corollary 2.1 to every element x of the additive group $(R, +)$, we have $m.x = 0$ for any $x \in R$. In particular, this tells us that $\Psi(R)$ is finite and hence $\Psi(R) \neq 0$. Let $\Psi(R) = n > 0$. Then by the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $m = nq + r$. For any $x \in R$, we have that

$$0 = m.x = (nq + r).x = (nq).x + r.x = q.(n.x) + r.x = q.0 + r.x = r.x$$

Thus, $r.x = 0$ for all $x \in R$. But n is the smallest positive integer with this property, and $r < n$, so it follows that $r = 0$. Hence, $m = nq = \Psi(R)q$, so $\Psi(R)$ divides $O(R)$.

Remark 3.1. Finite ring always have finite characteristic. But the ring having finite characteristic may not be finite. As an example, we may consider the polynomial ring $\mathbb{Z}_p[x]$.

Definition 3.1. For a positive integer n, by the *prime generators*, denoted by $PG(n)$, of n we mean set of all primes that are used to represent n as prime factors. For examples, if $n = 20$, then the prime generators
of n are 2,5 as $20 = 2^2.5$.

Theorem 3.2. Let R be a ring with an unit a. If $O^+(a)$ is infinite, then the characteristic of R is 0; *otherwise* $\Psi(R) = O^+(a)$.

Proof : If $O^+(a)$ is infinite, then there exists no positive integer n such that $n.a = 0$. So the characteristic of R is 0. Now we consider $O^+(a)$ is finite and say, $O^+(a) = n$. Then $n.a = 0$ and this implies $(n.a)a^{-1} = 0.a^{-1} = 0$. Then from this $n.x = 0.x = 0$ for all $x \in R$. Since $O^+(a)|\Psi(R)$, last equality gives $\Psi(R) = n = O^+(1)$.

Corollary 3.1. Let R be a ring with unity 1. If $O^+(1)$ is infinite, then the characteristic of R is 0; otherwise $\Psi(R) = O^+(1)$.

Corollary 3.2. Let R be a ring consisting at least two units. Then for any two units $a, b \in R$ with finite additive orders, $O^+(a) = O^+(b)$.

Definition 3.2. A relation ρ between two elements of R is defined as follows: for any two elements $a, b \in R$ $a\rho b$ if and only if $O^+(a) = O^+(b)$.

It is not difficult to proof the following lemma.

Lemma 3.2. *ρ is an is an equivalence relation on R.*

Lemma 3.3. *For every element a in a ring R with finite characteristic $\Psi(R)$, $O^+(a)$ $|\Psi(R)$.*

Proof : Since R is a ring with finite characteristic, there exists a positive integer n such that $n.a = 0$ for all $a \in R$. Thus $O^+(a)|n$ and hence $O^+(a)$ is finite. If the characteristic of a ring R is finite, then from Lemma 3.2 and Lemma 3.3 it is clear that the ρ have finite numbers of equivalence classes and each class contains elements of same additive order.

Lemma 3.4. An element *a in a ring R* with *finite characteristic* is *maximal additive order element if and only if* $O^+(a) = lcm\{m_1, m_2, . . . m_r\}$ *where* r denotes the total number of classes of *R under ρ and m_l* denotes *the additive order of an element of the class l.*

Theorem 3.3. Let R be a ring with finite characteristic. Then the following are hold
(a) there exists an element $a \in R$ such that $O^+(a) = \Psi(R)$
(b) $O^+(a) = \Psi(R)$ if and only if a is a maximal additive order element.

Proof: (a). Let $a_1, a_2, . . . , a_r$be elements from distinct classes with additive orders $m_1, m_2, . . . , m_r$, respectively. Let $lcm\{m_1, m_2, . . . , m_r\} = L$. Then $L.x = 0$for all $x \in R$ and this implies that $\Psi(R)|L$. Again from Lemma 3.1 there exists an element a such that $O^+(a) = L$. So using Lemma 3.3 , $L|\Psi(R)$ and consequently $\Psi(R) = L = O^+(a)$. Thus there exists an element $a \in R$ such that $O^+(a) = \Psi(R)$.

(b) If a is a maximal order element then from Lemma 3.4 and part (a) of this theorem, we have $O^+(a) = \Psi(R)$. Now converse part follows from the fact that $O^+(a)| \Psi(R)$.

A general questions comes : Is there any finite ring with a given characteristic ? As an example, for distinct p and : Is there any ring R with $O(R) = pq$ and $\Psi(R) = p$ or q? The answer of this question is negative. In the theorem below we give a relationship between prime generators of $O(R)$and $\Psi(R)$ and from this relationship readers may get some preliminary idea about the existence of a finite ring with a given characteristic.

Theorem 3.4. *For a finite ring R, the prime generators of $O(R)$ and $\Psi(R)$ are same.*

Proof: From Remark 3.1, $\Psi(R)$is finite. Let $\Psi(R) = m$ and $O(R) = n$. Then by Theorem $m|n$ and hence $PG(m) \subseteq PG(n)$. Now we show that $PG(n)\backslash PG(m)$ is empty. If possible, let $p \in PG(n)$ but $p \notin PG(m)$. Then from Theorem 3.3, there exists a maximal additive order element a such that $O^+(a) = \Psi(R)$=m. Since $p \in PG(n)$, by Cauchy's Theorem (Theorem 2.2) there exists an element b in R such that $O^+(b) = p$. Since $p \notin PG(m)$, so the $\gcd(O^+(a), O^+(b)) = 1$. Thus there exists an element c

in the group $(R,+)$ such that $O^+(c) = O^+(a).O^+(b)$, which contradicts the fact that a have maximal additive order. Hence $PG(n)\backslash PG(m)$ is empty and consequently, $PG(m) = PG(n)$.

Corollary 3.3. For a *finite integral domain* D, $O(D) = p^n$ for some *positive integer* n *and prime* p.

Proof : Since the characteristic of a finite integral domain is prime, applying Theorem 3.4 we get the result.

Remark 3.2. From above theorem we may conclude that there exists no integral domain D with $|PG(n)| > 1$, where n denotes the order of D.

Remark 3.3. From above theorem we may conclude that there exists no ring with pq numbers of elements and characteristic p or q, where p and q are distinct primes. More generally, if $O(R)$ is $p_1^{\alpha_1} p_2^{\alpha_2} . . . p_r^{\alpha_r}$ then the characteristic of R must be of the form $p_1^{\beta_1} p_2^{\beta_2} . . . p_r^{\beta_r}$ where p_i are primes and α_i's, β_i's are integers satisfies $1 \leq \beta_i \leq \alpha_i$ and vise versa.

In Theorem 3.4 it has been shown that for a finite ring R the prime generators of $O(R) and\ \Psi(R)$ are same. The next theorem gives the existence of a finite ring R with any finite characteristic having same prime generators as of $O(R)$.

Theorem 3.5. *There exists always a ring R with* $O(R) = p_1^{\alpha_1} p_2^{\alpha_2} . . . p_r^{\alpha_r}$ and $\Psi(R) = p_1^{\beta_1} p_2^{\beta_2} . . . p_r^{\beta_r}$ where p_i are primes and α_i's, β_i's are integers satisfies $1 \leq \beta_i \leq \alpha_i$.

Proof: If $O(R) = \Psi(R)$ then we consider the ring $\mathbb{Z}_n$. Now let $\Psi(R) < O(R)$. Also let $s_i = \alpha_i - \beta_i$, $1 \leq i \leq r$. Clearly $s_i \geq 0$. Define an index set I as $I = \{i : 1 \leq s_i \leq r\}$. Now we consider $R = \mathbb{Z}_{p_1^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \times . . . \times \mathbb{Z}_{p_r^{\beta_r}} \times \prod_{i\in I} S_i$, where $S_i = \prod_{i=1}^{s_i} \mathbb{Z}_{p_i}$. It is clear that $O(R) = p_1^{\alpha_1} p_2^{\alpha_2} . . . p_r^{\alpha_r}$ and from corollary 4.1, we have $\Psi(R) = p_1^{\beta_1} p_2^{\beta_2} . . . p_r^{\beta_r}$.

IV. CHARACTERISTIC OF OPERATIONAL RINGS

In this section first we give a relationship among $\Psi(R), \Psi(S)$ and $\Psi(R \times S)$ for any two rings R and S. After that we try to find out a relationship among $\Psi(R)$, $\Psi(I)$ and $\Psi(R/I)$ for any ring R and any ideal I of R. The proof of Theorem 4.1 may be found in literature but here the proof is presented by another arguments.

Theorem 4.1. *Let R and S be rings with characteristics* $\Psi(R)$ *and* $\Psi(S)$*, respectively. If both* $\Psi(R)$ *and* $\Psi(R)$ *are finite then* $\Psi(R \times S) = lcm\{\Psi(R), \Psi(S)\}$*, otherwise* $\Psi(R \times S) = 0$.

Proof : First we consider both $\Psi(R)$ and $\Psi(S)$ are finite. Let $\Psi(R) = m$ and $\Psi(S) = n$. Then $m.x = 0_R$ for all $x \in R$ and $n.y = 0_S$ for all $y \in R$ where 0_R and 0_S denote the additive identity of R and S, respectively. Therefore, $lcm\{m,n\}.(x,y) = 0$ for all $x \in R$ and all $y \in S$ and this implies that $\Psi(R \times S) \leq lcm\{m,n\}$. Again from Theorem 3.3, there exist maximal additive order elements $r \in R$ and $s \in S$ such that $O^+(r) = m$ and $O^+(a) = n$ and then $(r, 0_S), (0_R, s) \in R \times S$ with $O^+((r, 0_S)) = m$ and $O^+(0_R, s) = n$. Then applying Lemma 3.1, there exists an element $u \in R \times S$ such that $O^+(u) = lcm\{m,n\}$ and this implies that $lcm\{m,n\}|\Psi(R \times S)$. Since $\Psi(R \times S) \leq lcm\{m,n\}$ and $lcm\{m,n\}|\Psi(R \times S)$., we get the result $\Psi(R \times S) = lcm\{m,n\}$.

Corollary 4.1. *For the rings* $R_1, R_2, . . . , R_m$, $\Psi(\prod_{i=1}^m R_i) = lcm\{\Psi(R_1), \Psi(R_2), . . . , \Psi(R_m)\}$ if each $\Psi(R_i)$ is finite ; otherwise $\Psi(\prod_{i=1}^m R_i) = 0$

Theorem 4.2. *For a ring R with finite characteristic and an ideal I of R,* $\Psi(R/I) = k.\frac{\Psi(R)}{\Psi(I)}$ *where k is positive integer satisfies* $1 \leq k \leq \gcd(\Psi(I), \Psi(R/I))$.

Proof : Since $\Psi(R)$ is finite and I is an ideal, $\Psi(I)$ is also finite and $\Psi(I)|\Psi(R)$. Again we know that for every $r \in R$, $O^+(r + I)|O^+(r)$ and so $\Psi(R/I)$is finite and $\Psi(R/I)|\Psi(R)$. Let $\Psi(R), \Psi(I), \Psi(R/I)$ be n, m, l, respectively. Then $m.a = 0$ for all $a \in I$ and $l.(x + I) = I$ for all $x \in I$. Again $l.(x + I) = I$ implies $l.x + I = I$ and this is true if $l.x \in I$. Thus we have for all $x \in R$, $m.(l.x) = (ml).x = 0$for all $x \in R$. Thus $n|m.l$ and hence $\frac{n}{m} \leq l$ Again since $\Psi(I)|\Psi(R)$ and $\Psi(R/I)|\Psi(R)$, $lcm\{m,l\}|n$ and hence $l \leq \gcd(l,m)\frac{n}{m}$. Replacing the values of n, m and l we get the result.

In the next example we show that there are rings and ideals for which $\Psi(R/I) = k.\frac{\Psi(R)}{\Psi(I)}$ with $k = \gcd(\Psi(I), \Psi(R/I))$.

Example 4.1. Let us consider the ring $R = \mathbb{Z}_m \times \mathbb{Z}_n$ with $m > n$ and an ideal of R as $I = \langle(1,0)\rangle$. Since $\Psi(\mathbb{Z}_m) = m$ and $\Psi(\mathbb{Z}_n) = n$, $\Psi(R) = lcm\{m,n\}$. Also $\Psi(I) = m$ and $\Psi(R/I) = n$. Therefore,$\Psi(R/I) = \gcd(m,n)\frac{\Psi(R)}{\Psi(I)}$.

In the next theorem we show that there are rings and ideals for which $\Psi(R/I) = \frac{\Psi(R)}{\Psi(I)}$.

Theorem 4.3. *For any ring R with finite characteristic, there exists an ideal J such that* $\Psi(R/J) = \frac{\Psi(R)}{\Psi(J)}$.

Proof: If $\Psi(R) = \Psi(I)$for every ideal I of R then the theorem is true for $J = R$ Now we consider $\Psi(R) \neq \Psi(I)$ for some ideal I. Let $\Psi(R) = n$ and $\Psi(I) = m$. It is clear that $m \mid n$. Let $n = mk$. Let us define $J = \{r \in R: mr = 0\}$. We show that J is an ideal of R. If $\alpha, \beta \in J$ then $m\alpha = 0 = m\beta\_$. Hence $m(\alpha - \beta) = 0$ and $m(\alpha\beta) = 0$ so J is closed under subtraction and under multiplication, so J is a subring of R. Similarly, for any $r \in R$ we have $m(\alpha r) = (m\alpha)r = 0$, and also $m(r\alpha) = r(m\alpha) = 0$ by the distributive laws, so $\alpha r, r\alpha \in I_m$. Thus I_m is an ideal of R. Now we show that $\Psi(\mathrm{I_m}) = \mathrm{k} = \frac{\mathrm{n}}{\mathrm{m}}$. For any $r \in R$ as $m(kr) = nr = 0$, $kr \in I_m$, so $k(r + I_m) = kr + I_m = I_m$. Therefore $\Psi(\mathrm{I_m}) \leq \mathrm{k}$. If possible let $\Psi(\mathrm{I_m}) = l < k$. Since $\Psi(\mathrm{R}) = \mathrm{n}$, applying Theorem 3.3 there exists an element $a \in R$ such that $O^+(a) = n$ i.e., n is the least positive integer such that $na = 0$. Again $\Psi(\mathrm{I_m}) = l$ implies that $l(a + I_m) = I_m$ and this is true only if $la \in I_m$ i.e., only when $m(la) = 0 = (ml)a$. Now $l < k$ implies that $ml < mk = n$ which is contradicts the fact that n is the least positive integer such that $na = 0$. So $\Psi(\mathrm{I_m}) = \mathrm{k} = \frac{\mathrm{n}}{\mathrm{m}} = \frac{\Psi(\mathrm{R})}{\Psi(\mathrm{J})}$.

Remark 4.1. From Example 4.1 and Theorem 4.3 we can say that the multiplicity k in the Theorem 4.2 can not be determined uniquely over rings.

Theorem 4.4. *Let R be a ring with finite characteristic and I be an ideal of R. If R/I is an integral domain then* $\Psi(\mathrm{R/I}) = \frac{\Psi(\mathrm{R})}{\Psi(\mathrm{I})}$ or $\Psi(\mathrm{R}) = \Psi(\mathrm{I})$.

Proof : Since R/I is an integral domain and $\Psi(\mathrm{R})$is finite, $\Psi(\mathrm{R/I})$ is a prime number, say it is p. By similar argument as in the proof of Theorem 4.2, we have $\Psi(\mathrm{I})|\Psi(\mathrm{R})$ and $\Psi(\mathrm{R})|\mathrm{p}\Psi(\mathrm{I})$and so $\Psi(\mathrm{R}) = \mathrm{k_1}\Psi(\mathrm{I})$, $\mathrm{p}\Psi(\mathrm{I}) = \mathrm{k_2}\Psi(\mathrm{R})$ for some positive integers k_1 and k_2. Combining these two equations we have $p\Psi(\mathrm{I}) = \mathrm{k_1 k_2}\Psi(\mathrm{I})$ and so $p = \mathrm{k_1 k_2}$. Since p is prime exactly one of $\mathrm{k_1}$ and $\mathrm{k_2}$ must be 1. If $\mathrm{k_1} = 1$, then $\Psi(\mathrm{R}) = \Psi(\mathrm{I})$ and if $\mathrm{k_2} = 1$ then $\frac{\Psi(\mathrm{R})}{\Psi(\mathrm{I})} = \mathrm{p} = \Psi(\mathrm{R/I})$. Hence the theorem.

Corollary 4.2. *For a prime or maximal ideal I of a ring R with finite characteristic* $\Psi(\mathrm{R/I}) = \frac{\Psi(\mathrm{R})}{\Psi(\mathrm{I})}$ or $\Psi(\mathrm{R}) = \Psi(\mathrm{I})$.

Remark 4.2. The result of Theorem 4.4 can be used to determine an ideal is prime or not.

V. REFERENCES

[1] D.S. Dummit, and R.M. Foote, Abstract Algebra, Wiley India Pvt. Ltd., 2017.
[2] Kleiner, The Genesis of the Abstract Ring Concept, American Mathematical Monthly. 103(1996) 417-424.
[3] G. Birkhoff, and S.M. Lane, A Survey of Modern Algebra, 5th 2d,(1996).