Korean J. Math. **28** (2020), No. 3, pp. 483–488
http://dx.doi.org/10.11568/kjm.2020.28.3.483

THE IDENTICAL CHARACTERISTIC OF A RING

A. O. Atagün

Abstract. In this paper, a new characterization concept is introduced for rings with identity, called the identical characteristic. Some general results are obtained for various ring classes and illustrated by several examples.

1. Introduction

Throughout this study, all rings will be rings with identity, unless they cause any confusion, the identity of the ring will be indicated by 1 and the zero of the ring will be indicated by 0. The order of R will be denoted by $|R|$. $R[x]$ will denote the ring of polynomials in indeterminate x with coefficients in R.

The concept characteristic of a ring played a facilitating and effective role in the classification of the rings and the study of their algebraic properties.

In this study, we introduce the concept of identical characteristic(IC), which is a new characteristic concept for rings with identity, and its basic properties. We prove that IC is unchanged under an isomorphism. We obtain some results related to IC in various ring classes such as division rings, factor rings, Boolean rings, rings with zero-divisor, integer domains, polynomial rings, prime fields, finite and infinite fields.

Received March 5, 2020. Revised July 28, 2020. Accepted July 29, 2020.
2010 Mathematics Subject Classification: 16K20, 16K40, 13A35, 12E15, 12E20.
Key words and phrases: Characteristics of ring, Fields, Identical characteristic.

2. Preliminaries

Throughout this paper, all rings considered will be different from the zero ring. We refer to Hungerford [2] for all undefined concepts and notations. A commutative ring R with identity $1 \neq 0$ and no zero divisor is called an integral domain. A ring R with identity $1 \neq 0$ in which every non-zero element is a unit is called a division ring. A field is a commutative division ring. For a ring R if there is a positive integer n such that $n \cdot x = 0$ for all $x \in R$, then the least such positive integer is the characteristic of the ring R and denoted by $char(R)$. If no such positive integer exists, then R is of characteristic 0.

Proposition 2.1. [1] *Let R be a non-trivial ring with identity 1_R. Suppose S is a non-trivial subring of R with identity 1_S with $1_S \neq 1_R$. Then there exist proper divisors of zero in R.*

3. The identical characteristic

Identical characteristic has been chosen as the name because it is depending on the identity of a ring and is structurally parallel to the characteristic of rings.

Definition 3.1. Let R be a ring. If there exist a positive integer n such that $x^n = 1$ for all $0 \neq x \in R$, then the smallest of n is called *the identical characteristic* of R and denoted by $IC(R)$. If no such n exists, then $IC(R) = 0$.

Example 3.2. $IC(\mathbb{Z}) = IC(\mathbb{Q}) = IC(\mathbb{R}) = IC(\mathbb{C}) = 0$.
$IC(\mathbb{Z}_3) = 2$, since $\overline{1}^2 = \overline{2}^2 = \overline{1}$.

Proposition 3.3. *Let R be a ring with $IC(R) = n \neq 0$. Then, k is a positive integer such that $x^k = 1$ for all $0 \neq x \in R$ if and only if $n|k$.*

Proof. Assume $x^k = 1$ for all $0 \neq x \in R$. By division algorithm, there exist integers q, r such that $k = nq + r$ and $0 \leq r < n$. Since $IC(R) = n \neq 0$, then $x^n = 1$ and we have $1 = x^k = x^{nq+r} = (x^n)^q x^r = x^r$. Since $0 \leq r < n$ and $IC(R) = n$, we have $r = 0$ by Definition 3.1. Hence $n|k$. Conversely, we assume that $n|k$. Then there exists an integer $t \geq 1$ such that $k = nt$. Then $x^k = x^{nt} = (x^n)^t = 1$ for all $0 \neq x \in R$. □

From Definition 3.1, we immediately have;

THEOREM 3.4. *Let R be a ring. Then we have the following;*

a) *If $IC(R) = n \neq 0$, then R is a division ring.*
b) *If R is commutative and $IC(R) = n \neq 0$, then R is a field.*
c) *If R is commutative and has a zero-divisor, then $IC(R) = 0$.*

Proof. **a)** Let $0 \neq x \in R$. Since $IC(R) = n$, we have $x^n = 1$. Then $xx^{n-1} = x^{n-1}x = 1$, so x is a unit in R. As x is arbitrary, R is a division ring.
b) Clear.
c) Assume that R is commutative with a zero-divisor, say a. Then there exists a $0 \neq b \in R$ such that $ab = 0$. Assume that $IC(R) = n \neq 0$. By assumption, $0 = 0^n = (ab)^n = a^n b^n = 1 \cdot 1 = 1$ is a contradiction. Therefore $IC(R) = 0$. □

The converse of Theorem 3.4 (a) is not true, in general. We have the following example:

EXAMPLE 3.5. Let H be the ring of real quaternions, where $i^2 = j^2 = k^2 = ijk = -1$. It is known that H is a division ring. Since there is no positive integer n such that $(i + j)^n = 1$, $IC(H) = 0$.

THEOREM 3.6. *The identical characteristic of a ring is preserved under isomorphism.*

Proof. Let R and T be rings with $IC(R) = n \neq 0$, $IC(T) = m \neq 0$ and let $f : R \to T$ be an isomorphism of rings. Obviously, $f(1_R) = 1_T$. Since $IC(T) = m$, $t^m = 1_T$ for all $0 \neq t \in T$. Then $(f(r))^m = f(r^m) = 1_T = f(1_R)$ which implies $r^m = 1_R$ for all $0 \neq r \in R$. Then $n|m$, by Proposition 3.3. By symmetry $m|n$. Hence $m = n$, since $m, n > 0$.
If $n = 0$ or $m = 0$, the result can be obtained similarly. □

THEOREM 3.7. *Let R be a ring with identity 1_R and T be a ring with identity 1_T. If $IC(R) = 0 \neq IC(T)$, then there is no monomorphism $f : R \to T$ such that $f(1_R) = 1_T$.*

Proof. Assume that $f : R \to T$ is a monomorphism such that $f(1_R) = 1_T$ and let $IC(R) = 0 \neq IC(T) = m$. Since $IC(T) = m$, $(f(r))^m = f(r^m) = 1_T = f(1_R)$ for all $0 \neq r \in R$. Then $r^m = 1_R$ for all $0 \neq r \in R$ which is a contradiction of $IC(R) = 0$. □

Is the identical characteristic of a ring with identity the same as that's subrings with identity? The answer is no for a commutative case. We have the following:

THEOREM 3.8. *Let R be a commutative ring with identity 1_R. If there exists a non-trivial subring S of R with identity 1_S such that $1_S \neq 1_R$, then $IC(R) = 0$.*

Proof. R has a zero-divisor by Proposition 2.1 and assumptions, then $IC(R) = 0$ by Theorem 3.4 (c). □

EXAMPLE 3.9. Consider the ring $R = \mathbb{Z}_6$ and a subring $S = \{\bar{0}, \bar{3}\}$ of R. Then $1_S = \bar{3} \neq \bar{1} = 1_R$. We have $IC(R) = 0$ and $IC(S) = 1$. Another subring of R is $T = \{\bar{0}, \bar{2}, \bar{4}\}$ such that $1_T = \bar{4}$ and $IC(T) = 2$.

THEOREM 3.10. *Let R be a ring. Then we have the following;*

a) *If R has a nonzero idempotent element which is $\neq 1$, then $IC(R) = 0$.*
b) *If R has a non-zero nilpotent element, i.e. R is not a reduced ring, then $IC(R) = 0$.*
c) *If R is a Boolean ring such that $|R| \geq 3$, then $IC(R) = 0$.*
d) *If R is a direct product of non-zero rings, then $IC(R) = 0$.*

Proof. **a)** Suppose that there exist an $x \in R$ such that $x \neq 0$, $x \neq 1$ and $x^2 = x$. Then there is no positive integer n such that $x^n = 1$, i.e. $IC(R) = 0$.
b) If $0 \neq x \in R$ is a nilpotent element, then $x^k = 0$ for some positive integer k. Now assume that $x^n = 1$ for some integer $n \geq 1$. Then there is an integer $m \geq 1$ such that $nm \geq k$. Hence $1 = (x^n)^m = x^{nm-k}x^k = 0$, a contradiction.
c) Follows directly from (a).
d) Assume that $R = R_1 \times R_2$, $R_1 \neq \{0\}, R_2 \neq \{0\}$ and $IC(R) = n \neq 0$. There exist an element $(0,0) \neq (x,0) \in R$, such that $(x,0)^n = (x^n, 0) \neq 1 = (1_{R_1}, 1_{R_2})$ is a contradiction, hence $IC(R) = 0$. □

EXAMPLE 3.11. Consider the 2 by 2 full matrix ring $M_2(\mathbb{Z}_2)$ over $\mathbb{Z}_2$. Since $\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}^2 = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}$, there is an idempotent element which is different from zero and the identity. Thus $IC(M_2(\mathbb{Z}_2)) = 0$.

THEOREM 3.12. *If F is a finite field of order n, $IC(F) = n - 1$.*

Proof. Since the multiplicative group $F - \{0\}$ is a cyclic group of order $n - 1$, then $x^{n-1} = 1$ for all $0 \neq x \in F$. Moreover if x is a generator of $F - \{0\}$, then $x^k \neq 1$ for $1 \leq k < n - 1$. Thus $IC(F) = n - 1$. □

COROLLARY 3.13. *If p is a prime number, then $IC(\mathbb{Z}_p) = p - 1$.*

Proof. If p is a prime number and $0 \neq \bar{a} \in \mathbb{Z}_p$, then $gcd(a, p) = 1$. Then $a^{p-1} \equiv 1\ (modp)$ by Fermat's Little Theorem. Therefore $\bar{x}^{p-1} = \bar{1}$ for all $\bar{0} \neq \bar{x} \in \mathbb{Z}_p$, i.e. $IC(\mathbb{Z}_p) = p - 1$. □

EXAMPLE 3.14. Consider the field

$$F_4 = \left\{ \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\},$$

where the components of matrices are in $\mathbb{Z}_2$. Then it is easily checked that $IC(F_4) = 3$.

PROPOSITION 3.15. *Let F be a field. Then $IC(F[x]) = 0$.*

Proof. Assume that $IC(F[x]) = n \neq 0$. If $f(x)$ is a non-constant polynomial of $F[x]$, then $(f(x))^n = 1$. This implies $(f(x))^{n-1} = (f(x))^{-1} \in F[x]$, but this is a contradiction because the units of $F[x]$ is equal to units of F. Also $F[x]$ is not a field and then $(f(x))^{-1} \in F[x]$ is not true in general. Hence $IC(F[x]) = 0$. □

REMARK 3.16. Let F be a prime field. It is known that $F \cong \mathbb{Q}$, when $char(F) = 0$ and $F \cong \mathbb{Z}_p$, when $char(F) = p$. Since $IC(\mathbb{Q}) = 0$ and $IC(\mathbb{Z}_p) = p - 1$ by Theorem 3.6, we have, if $char(F) = 0$, then $IC(F) = 0$ and if $char(F) = p$, then $IC(F) = p - 1$.

THEOREM 3.17. *If F is a field with $char(F) = 0$, then $IC(F) = 0$.*

Proof. If $char(F) = 0$, then $\mathbb{Q} \subseteq F$, and for example, $2^n \neq 1$ for all integers $n \geq 1$. Hence $IC(F) = 0$. □

From the Theorem 3.17, we have the following question: If the characteristic of a field F is a prime number, $IC(F) \neq 0$? But the answer is no, we have the following example:

EXAMPLE 3.18. $\mathbb{Z}_p(x) = \{\frac{f}{g} | f, g \in \mathbb{Z}_p[x], g \neq 0\}$ is a field of rational functions in the indeterminate x with the coefficient in $\mathbb{Z}_p$. Since $\mathbb{Z}_p \subset \mathbb{Z}_p(x)$, then $char(\mathbb{Z}_p(x)) = p$. But there is no positive integer n such that $(\frac{x}{1})^n = 1$, i.e. $IC(\mathbb{Z}_p(x)) = 0$.

THEOREM 3.19. *If F is an infinite field, then $IC(F) = 0$.*

Proof. If $char(F) = 0$, then $\mathbb{Q} \subseteq F$ and hence $IC(F) = 0$. Now assume $char(F) = p \neq 0$. If F is transcendental over $\mathbb{Z}_p$, then there is an element $t \in F$ that is transcendental over $\mathbb{Z}_p$. But $t^n \neq 1$ for all integers $n \geq 1$. Hence F is algebraic over $\mathbb{Z}_p$. Since F is infinite, there is a chain of fields, say, $\mathbb{Z}_p \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F$ such that $[F_i : \mathbb{Z}_p] < \infty$

for all $i \geq 1$. Hence for each integer $n \geq 1$, there is an integer $k \geq n$ such that $[F_k : \mathbb{Z}_p] > n$. Then $|F_k| > p^n > n$ and hence $x^n \neq 1$ for some $0 \neq x \in F_k \subseteq F$. Thus $IC(F) = 0$. □

Acknowledgements
The author are highly grateful to the referees for their valuable comments and suggestions. Especially, the author would like to thank the referee who solved the open problem and brought out Theorem 3.19.

References

[1] P. J. Arpaia, *Rings, subrings, identities and homomorphisms*, The Two-Year College Math. J., **5** (1) (1974), 25–28.
[2] T. W. Hungerford, *Algebra*, Springer, New York, 2003.

A. O. Atagün
Department of Mathematics
Kırşehir Ahi Evran University
Kırşehir 40100, Turkey
E-mail: aosman.atagun@ahievran.edu.tr