ISSN: 2822-4566 Journal of Balkan Science and Technology 2024: 3(3): 77-79

Journal of Balkan Science and Technology

journal homepage: www.jbst.nku.edu.tr/

The Commutativity Condition of the Ring

Nuray Eroğlu*[1]

[1] *Department of Mathematics, Tekirdağ Namık Kemal University, Tekirdağ, Türkiye*

Research Article

Keywords:
commutativity axiom
ring
group

Received: 30.12.2024
Accepted: 04.03.2025
Published: 14.03.2025

DOI: 10.55848/jbst.2025.03

ABSTRACT

As it is well known, modules are a common generalization of vector spaces, abelian groups, and rings. The definition of a module is obtained by replacing the term 'field' in the set of conditions defining a vector space with an arbitrary ring. In this paper, we prove that the abelianity (commutativity) property of the group structure of a unitary module over an arbitrary ring with identity can be recovered from the remaining conditions.

1. Introduction

A *ring* is a set equipped with two binary operations satisfying certain conditions, one of which is called *addition* and the other *multiplication*. Mostly, the additive binary operation is written symbolically as "+", whereas the multiplicative binary operation is denoted by "·". The theory of rings originated from the algebraic integers and, more generally, polynomials. Several mathematicians have attempted to give a solid foundation to algebraic systems known today as a ring today, including R. Dedekind [1], D. Hilbert [2], and A. Fraenkel [3]; eventually, E. Noether [4] accomplished this task of giving the modern definition of a ring, now called a *commutative ring*. Although Noether did not require a multiplicative identity in the definition, most mathematicians define rings in a way that they necessarily have one. As far as we have seen in all books, the definition of a ring presupposes it to be abelian with respect to the addition. Following the arguments of [5], however, one can show, among other things, that the condition of being "abelian" in the definition of a ring follows from the other axioms. We believe that this observation is of independent interest, let alone a good exercise.

In order to make the paper self-contained and educational, we provide below some well-established algebraic concepts.

A *binary operation* (shortly, an *operation*) on a non-empty set is a function from the cartesian product of this set with itself into the set. An operation $*$ on a set G, where we write $*(x, y)$ as $x * y$, is called a *group operation* if

(i) $(x * y) * z = x * (y * z)$ for all $x, y, z \in G$.

(ii) There exists $e \in G$ such that $x * e = e * x = x$ for all $x \in G$.

(iii) For each $x \in G$ there exists $x^{-1} \in G$ satisfying $x * x^{-1} = x^{-1} * x = e$.

Note that (i) allows one to define any finite string of elements $a_1 * \cdots * a_n$ by induction whenever the elements a_i belong to G, and the elements e and x^{-1} (called respectively, the *identity* and the *inverse* of x) provided by (ii) and (iii) are unique. In the latter case, the pair $(G, *)$ is called a *group*. A group G is called *abelian* if $a * b = b * a$ for all $a, b \in G$.

Throughout the note $(G, +)$ denotes a group with identity 0, unless otherwise stated. For each $x \in G$ we will write $-x$ instead of x^{-1}. For $x, y \in G$, the symbolism $x - y$ instead of $x + (-y)$ is preferred; similar notational facilities are invoked for $-x + y = (-x) + y$ and $-x - y = (-x) + (-y)$. It is useful to note that $-(x+y) = (-x)+(-y)$ holds. A subset S of a group G is called a *subgroup* if for each $x, y \in S$, the element $x + y$ is in S and the element $-x$ belongs to S. It is obvious that every subgroup is a group.

It can be clearly seen that a group $(G, +)$ is commutative if and only if $-(a + b) = -a - b$ for all $a, b \in G$. If R is a non-empty set and $\cdot : R \times G \to G$ is a function, we write $\cdot(r, x) = rx$. For $x \in R$, we denote $xG := \{xa : a \in G\}$, where Gx is defined similarly. Instead of $(xa) + (xb)$ for $x \in R$, $a, b \in G$, we will use the notation $xa + xb$.

2. Main Results

One of the main results of the paper can be stated as it follows.

Theorem 2.1. *Let $(G, +)$ be a group, R be a non-empty set, and $\cdot : R \times G \to G$ be a function. Suppose that $x(a + b) = xa + xb$ for all $x \in R$, $a, b \in G$. Then for each $x \in R$, the set xG is a subgroup of G. Moreover, the following are equivalent:*

(i) *xG is commutative.*

(ii) *For each $x \in R$, $a, b \in G$, one has $-(x(a+b)) = x(-a-b)$.*

In particular, the equality $x(a + b) = x(b + a)$ holds.

Proof. Let $x \in R$ be given. Since $x0 = x(0 + 0) = x0 + x0$, we have $x0 = 0$. Also for given $y \in G$ we have

$$0 = x(y + (-y)) = xy + x(-y) \text{ and}$$
$$0 = x((-y) + y) = x(-y) + xy.$$

This shows $-(xy) = x(-y)$. Now it is obvious that for each $x \in R$, the set xG is a subgroup of G.

*Corresponding author: *Department of Mathematics, Tekirdağ Namık Kemal University, Tekirdağ, Türkiye*
E-mail address: **neroglu@nku.edu.tr**

Suppose now that (i) holds and that $x \in R$ and $a,\, b \in G$ are given. Then

$$\begin{aligned} x(-a-b)+x(a+b) &= x(-a)+x(-b)+xa+xb \\ &= x(-a)+xa+x(-b)+xb \\ &= -(xa)+xa-(xb)+xb \\ &= 0 \end{aligned}$$

whence we have

$$-(x(a+b)) = x(-a-b).$$

Now suppose that (ii) holds and $x \in R$ is fixed. Let $a,\, b \in G$ be given. Since

$$0 = x0 = x((a+b)+(-b-a)) = x(a+b)+x(-b-a)$$

we have

$$xa+xb = x(a+b) = -(x(-b-a)) = x(b+a) = xb+xa.$$

Thus, xG is commutative, which completes the proof. □

We note that if the condition $x(a+b) = xa+xb$ is replaced by $(a+b)x = ax+bx$ in the above theorem, then the result turns out to be that for each $x \in R$ the set Gx is abelian if and only if $-(a+b)x = (-a-b)x$ for all $x \in R$ and $a,\, b \in G$.

As a corollary, we have the following.

Corollary 2.2. *Let R and G be as in Theorem 2.1. Suppose that $R = G$ and $(a+b)c = ac+bc$ for all $a,\, b,\, c \in G$. Then for each $x \in R$, the group xG is commutative. In particular, if $xG = G$ for some $x \in G$, then G is commutative.*

Proof. Let x and $a \in R$ be given. From the equality,

$$0 = (a+(-a))x = ax+(-a)x$$

we get

$$(-a)x = -(ax) = a(-x).$$

Also, for $b \in R$ we have

$$\begin{aligned} -(x(a+b)) &= (-x)(a+b) = (-x)a+(-x)b \\ &= x(-a)+x(-b) = x(-a-b) \end{aligned}$$

Now from Theorem 2.1, it follows that xG is commutative. □

A *$\star$-ring* is a triple $(R, +, .)$, where $+$ and $\cdot$ are binary operations on R satisfying the following conditions:

(i) $(R, +)$ is a group.

(ii) For each $x,\, y,\, z \in R$, one has $x(y+z) = xy+xz$ and $(x+y)z = xz+yz$.

(iii) For each $x,\, y,\, z \in R$, one has $x(yz) = (xy)z$.

Similar to the case of a ring, the operation $+$ is called *addition* and $\cdot$ is called *multiplication*, generally. If there exists an element $1 \in R$ (called the *identity* of R) with $1x = x1 = x$, then we shall call a *$\star$-ring with unit*. A $\star$-ring $(R, +, .)$ is called a *ring* if $(R, +)$ is abelian.

An example of a $\star$-ring without identity is $2\mathbb{Z} = \{2x : x \in \mathbb{Z}\}$ with usual algebraic operations. In particular, let A be a set with more than two elements and R be the set of all one-to-one and onto functions from A into A. Define the algebraic operations,

$$f+g := f \circ g \text{ and } f.g := I$$

where, $f \circ g$ is the composition of f and g, I is the identity function on A. Then $(R, +, .)$ is a $\star$-ring but not a ring since the group $(R, +)$ is non-commutative.

The following theorem, whose proof results directly from the above results which are taken into consideration, establishes the fact that in the definition of a ring with unit, the condition of commutativity of the addition can be omitted. In other words, every $\star$-ring with identity is a ring. To the best of our knowledge, this fact is absent in every standard book of algebra.

Theorem 2.3. *Every $\star$-ring with unit is a ring.*

Proof. Let $(R, +, .)$ be a $\star$-ring with unit 1. As $G = R$, the set R satisfies the conditions of Theorem 2.1; since $1R = R$, from Theorem 2.1, it immediately follows that $(R, +)$ is abelian. □

One expected question to be answered is the relation between $\star$-rings and rings in the lack of a unit element. We will answer this question by giving a frame as in the following theorem. Recall that a *$\star$-ring homomorphism* from a $\star$-ring R into another one R' is a function f satisfying

$$f(a+b) = f(a)+f(b) \text{ and } f(ab) = f(a)f(b)$$

where algebraic operations are denoted by the same symbols. If f is also one-to-one then one says that f is a *$\star$-embedding* and that in this R is said to be *embedded* into R'. We note that if a $\star$-ring is embedded into a ring, then it is also a ring, as the subgroup of an abelian group is abelian.

Theorem 2.4. *Let R be a $\star$-ring. The following assertions are equivalent:*

(i) *R is a ring.*

(ii) *R can be embedded into a ring with unit.*

(iii) *R can be embedded into a $\star$-ring with unit.*

Proof. It is well-known that every ring can be embedded into a ring with unit. More precisely, let $R' = R \times \mathbb{Z}$, where $\mathbb{Z}$ is the ring of integers. Then, under the binary operations

$$\begin{gathered} (x,m)+(y,n) = (x+y, m+n) \\ (x,m)(y,n) = (xy+nx+my, mn) \end{gathered}$$

R' is a ring with unit element $(0,1)$ and $r \mapsto (r,0)$ is an embedding. So we have the fact that (i) implies (ii). That (ii) implies (iii) follows from the definition. Now suppose that (iii) holds, that is R is embedded into a $\star$-ring R' with unit. By Theorem 2.3 R' is abelian with respect to the addition operation. Hence R is abelian as well with respect to the same operation, whence it is a ring. □

Let R be a ring and A be a group. Let $\cdot : R \times A \to A$ be a map satisfying for each $r,\, s \in R$ and $a,\, b \in A$ the following conditions:

(i) $r(a+b) = ra+rb$.

(ii) $(r+s)a = ra+sa$.

(iii) $(rs)a = r(sa)$.

One can easily show that $-(r(a+b)) = (-r)(a+b) = r(-a-b)$, so from Theorem 2.1 we have for each $r \in R$ that rA is an abelian subgroup of A.

Let R and A be as above with the given conditions. If A is abelian, then A is said to be a *left R-module*. In particular, if R has a unit 1 and $1a = a$ for all $a \in R$, then A is said to be a *left R-module with unit*. Now we can state the following theorem, which says that in the definition of left R-module A with unit, it is not necessary to suppose the "abelianness" of A.

Theorem 2.5. *Let R and A be defined as above. If R has unit 1 and $1a = a$ for all $a \in A$, then A abelian, so it is a left R-module with unit.*

Finally, let us note that the proofs of the given results do not use the associativity property "$x(yz) = (xy)z$."

3. Conclusion

In the literature, various studies have been conducted to reduce the number of axioms that constitute algebraic structures. One notable example in this field was carried out by Bryant [5]. Similarly, the aim of this study is to ensure that some algebraic structures can be obtained with fewer axioms. The results obtained indicate that some concepts can be restructured in a way that increases the efficiency of their investigation processes. Future research may focus on further reducing axioms or exploring the potential effects of these results in other areas of algebra.

Decleration

Author Contribution: Conceive-N.E.; Design-N.E.; Supervision-N.E.; Computational Performance, Data Collection and/or Processing-N.E.; Analysis and/or Interpretation Literature Review-N.E. ; Writer-N.E.; Critical Reviews–N.E.;

Acknowledgment: I would like to thank the reviewers for their remarks and improvement of the paper. The author declare that this study has received no financial support.

Conflict of Interest: The author declares no conflicts of interest.

Orcid ID:

Nuray Eroğlu 0000-0002-0780-2247

References

[1] R. Dedekind. "Sur la théorie des nombres entiers algébriques". *Bulletin des Sciences Mathématiques et Astronomiques* 1 (1877), pp. 207–248.

[2] D. Hilbert. "Die Theorie der algebraischen Zahlkörper." *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 (1894/95), pp. 175–535.

[3] A. Fraenkel. "Über die Teiler der Null und die Zerlegung von Ringen." *Journal für die reine und angewandte Mathematik* 145 (1915), pp. 139–176.

[4] E. Noether. "Idealtheorie in Ringbereichen". *Mathematische Annalen* 83 (1921), pp. 24–66.

[5] V. Bryant. "Reducing classical axioms". *The Mathematical Gazette* 55 (1971), pp. 38–40.