Interdisciplinary Journal of Research and Development
ISSN 2410-3411 (online) / ISSN 2313-058X (print)
Vol 10 No 2 / July 2023

Cyber Security in the Maritime Transport

Osman Metalla[1]
Alma Golgota[2]
Kapiten Shpëtim Pupa[3]
Eduart Ndokaj[4]
Pranvera Beqiraj[5]
Elson Thana[6]
Artion Beqiraj[6]
Uendi Çerma[7]

[1]Prof. Dr., Lecturer, Faculty of Political Studies,
"Aleksandër Moisiu" University, Durrës, Albania
[2]Dr. Ing., Lecturer, Faculty of Professional Studies,
Aleksandër Moisiu University, Durrës, Albania
[3]Msc., Lecturer, Faculty of Professional Studies,
Aleksandër Moisiu University, Durrës, Albania
[4]Dok. Cand., Lecturer, Faculty of Professional Studies,
Aleksandër Moisiu University, Durrës, Albania
[5]Dr., Lecturer, Faculty of Political Sciences and Law,
University "Aleksandër Moisiu", Durrës, Albania
[6]Msc., Lawyer
[7]Msc., Lecturer, Faculty of Information Technology,
Aleksandër Moisiu University, Durrës, Albania

Received: 05 May 2022 / Accepted: 20 June 2023 / Published: 23 July 2023

Doi: 10.56345/ijrdv10n210

Abstract

Maritime transport is an essential element for the economic sustainability of many regions around the world, including Albania. Especially for the countries that have access to the sea, maritime transport is the backbone of domestic and international trade. One of the challenges faced by this sector is the protection from threats and cyber-attacks. Cyber-attacks can lead to major environmental or economic disaster, even being able to cause loss of human life. Also, technological changes are being implemented by shipping companies more slowly compared to other manufacturing sectors. Therefore, this sector is easily attacked in this direction. The purpose of this study is to present the consequences of cyber-attacks on maritime transport through a map of current cyber security provisions on ships and in ports. Regarding this, the purpose of the research in this study is related to the conference topics regarding technology and information and navigation sciences. The methodology used in this scientific research is based on published literature that enables a mapping of modern methods and analysis, interpretation, and implications of cyber security within the maritime industry. Major results and implications of the study regards suggestions on raising cyber security capacities against cyber threats for the realization of safe and modern port activities.

Keywords: *cyber security, maritime transport, legislation, logistics*

1. Introduction

Maritime transport is an essential element for the economic sustainability of many regions around the world, including Albania. Development of the maritime industry relies on different factors, such as: global growth and improvement of its standards, investments, elimination of trade barriers, etc., that also encourage an ever-increasing dependence on the maritime industry. Especially for the countries that have access to the sea, maritime transport is the backbone of domestic and international trade.

Furthermore, in markets that require sustainable development, low costs, efficiency and, of recent growing importance, environmentally friendly operations, the maritime sector is responsible for 90% of the transport of all goods.

Recent developments in the Internet of Things (IoT), Big Data and Artificial Intelligence have enabled the migration to more digitized maritime infrastructures and, therefore, required an urgent re-evaluation of cyber security provisions. Additionally, connectivity and reliance on smart devices play a key role in motivating cybercrime such as social engineering, identity theft and spam. Protecting the integrity of next-generation maritime infrastructures is an urgent need.[70]

The maritime sector, as a vital part of the global economy, must be protected from cyber threats and attacks. A cyber incident can lead to a major environmental or economic disaster, even being capable of causing the loss of human life.

Technological changes are being implemented by shipping companies more slowly than other manufacturing sectors. As a result, the maritime sector is mainly suffering the risks of cyber-attacks related to this way of conceiving and managing the business.

2. Methodology

The methodology used in this scientific research is based on published literature and documents issued by the International Maritime Organization (hereinafter IMO), that enables a mapping of modern methods and analysis, interpretation and implications of cyber security within maritime transport. The purpose of the desk-based research is to collect data on: the predictions set by the IMO on cyber security in maritime transport, the role of protection from cyber risks in maritime transport, legal predictions at the national level or their absence in cybersecurity in maritime transport. The purpose of the desk-based research is to highlight the predictions and standards that must be respected in the protection from cyber risks in maritime transport.

3. Results

Cyber security in the maritime sector is the great obsession of shipping companies, as nowadays almost everything is managed through the Internet, which is the medium of relationship and transition between a company, its suppliers and its customers, prompting hackers to hack and access the data of a transport company very easily. These attacks do not only refer to economic damages, but also affect reputation and credibility when it affects the trust that the environment has in the company. Since plans are focused on reducing risks related to security, port disruption, and environmental concerns, a traditional cybersecurity assessment may not be enough.

Currently there have been several attacks on the security systems of both ports and shipping companies or businesses that import/export their goods via sea transport. Even though the use of the Internet has been significantly introduced in almost all port operations, the seaports of the Republic of Albania have a significant lack of protection against cyber-attacks and therefore become very vulnerable to cyber-attacks or cyber terrorism.

On the other hand, IMO's response to this is issued in some guidelines, which, although they have a recommendatory character, are of particular value to be implemented by stakeholders in maritime transport. In the following, we are presenting some of them in a descriptive way.

Regarding the growing threat on cyber security in the maritime transport, IMO adopted on 16 June 2017 Resolution MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems"[71] which came into force on January 1,

[70] Kapalidis, P. "Cybersecurity at Sea. In Global Challenges in Maritime Security", Springer: Berlin/Heidelberg, Germany, 2020; pp. 127–143.

[71] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

2021.[72] Subject to this resolution are all vessels and it requires that in their safety management systems is included cyber risk management, in accordance with the International Safety Management (ISM) Code.

This resolution takes into account the MSC-FAL.1-Circ.3-Rev.2 "Guidelines on maritime cyber risk management"[73] (Guidelines hereinafter). The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.[74]

According to the Guidelines definition, maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.[75]

Cyber risk management means the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.[76]

According to the Guidelines, vulnerable systems could include, but are not limited to:

1. Bridge systems;
2. Cargo handling and management systems;
3. Propulsion and machinery management and power control systems;
4. Access control systems;
5. Passenger servicing and management systems;
6. Passenger facing public networks;
7. Administrative and crew welfare systems; and
8. Communication systems.[77]

The overall goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

The Resolution includes further recommendations as well, which can be summarized as following:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber event in a timely manner.

Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.[78]

Resolution MSC.428(98) *"Maritime Cyber Risk Management in Safety Management Systems"* has since been complemented by other guidelines, notably those developed by the Baltic and International Maritime Council (BIMCO) for cyber risk management.

In particular, we mention here "The Guidelines on Cyber Security onboard Ships" - Version 4, according to which vessels and shipping are vulnerable to cyber-attacks and which is based on high-level principles, such as:

- establishment of awareness of the safety, security and commercial risks that present themselves due to a lack of cyber security measures;
- protection of shipboard IT infrastructure and connected equipment;
- system for authentication and authorization of users, to ensure appropriate access to necessary information;

---

[72] *This resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.*

[73] *It was approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017).*

[74] *https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.*

[75] *MSC-FAL.1-Circ.3-Rev.2 "Guidelines on maritime cyber risk management", available on https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.*

[76] *Ibid..*

[77] *Ibid.*

[78] *Ibid.*

- protection of data that is used in the ship environment, ensuring it has adequate protection based on the sensitivity of the information;
- management of IT users, to make sure they only have access and rights to the information for which they are authorized;
- management of communication between the ship and the shore side, and
- develop and implement a cyber incident response plan based on a risk assessment.[79]

These guidelines lay out high-level recommendations for incorporating cyber risk management into existing safety management system (SMS) processes, enabling ship owners to protect their vessels. As of January 1, 2021, all ship owners must comply with IMO Resolution MSC.428(98) in order to continue sailing worldwide.[80]

4. Discussion

There are more than 50,000 merchant ships operating internationally, carrying all types of cargo. These vessels must dock at Critical Infrastructures (CI) to carry out their usual operations (ports, platforms, refineries, pipelines, power plants, etc.). Ports are one of the most important links in the logistics chain, especially in recent years, due to the tremendous growth of container shipping.

In the Republic of Albania, there are four state-owned ports open for international transport, such as the Port of Durrës, which covers about 80% of the import/export of goods in Albania, the Port of Vlora, the second port in terms of size and importance, the Port of Saranda which has mainly turned into a port for processing passengers and the Port of Shëngjin as the most northern port of Albania, which is mainly used by companies that have their activity in the north of the country.

Three terminals for the processing of hydrocarbon materials which have been built and operate under concession contracts between state institutions and private companies. These ports are Romano Port sha. and MBM Port which are in the bay of Porto Romano, Durrës and the Vlora-1 Petrolifera Italo-Albanese (PIA) terminal which operates in the bay of Vlora.

In the above ports, the possible illegal activities of cyber-crime or cyber terrorism can condition the Albanian economic and institutional activity and always cause losses for many economic actors, because of the collapse of processes and services.

5. Conclusions

Based on the above results and discussions, conclusions of this paper are as following:

- Safe and secure shipping, which is operationally resilient to cyber risks, should be supported by the increase of human capacities that cover this field and the adoption of the relevant legal rules.
- To safeguard shipping from current and emerging threats related to cyber security of processes and systems in shipping, all the actors involved should take the necessary measures based on international and national standards and best practices.
- Adoption of effective feedback mechanisms is required for effective cyber risk management.
- Adoption of new measures at domestic level (Albanian law) are required to fulfill the IMO guidelines.

References

MSC-FAL.1-Circ.3-Rev.2 “Guidelines on maritime cyber risk management.”, available on https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

“The Guidelines on Cyber Security onboard Ships - Version 4”, available on https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Resolution MSC.428(98) “Maritime Cyber Risk Management in Safety Management Systems”, available on https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Kapalidis, P. “Cybersecurity at Sea. In Global Challenges in Maritime Security”; Springer: Berlin/Heidelberg, Germany, 2020; pp. 127–143.

79 https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
80 https://marine-offshore.bureauveritas.com/marine/cybersecurity.

Homomorphism in Weakly Γ-Ring

Orgest Beqiri

Department of Mathematics,
Faculty of Information Technology,
University 'Aleksandër Moisiu',
Durrës, Albania

Received: 05 May 2022 / Accepted: 10 June 2023 / Published: 23 July 2023

Doi: 10.56345/ijrdv10n211

Abstract

Many algebraic structures have been defined so far. One of them, is that of Γ-ring, which is a generalization of ring. Weakening some of the conditions of the definition of Γ-ring, it has also been defined the concept of weakly Γ-ring. An important and well-known concept for every algebraic structure is homomorphism. In this paper, the concept of homomorphism in weakly Γ-ring is introduced. Further, some simple results analogous to the theory of rings, related to this concept are extended.

Keywords: *Γ-semigroup, Γ-ring, weakly Γ-ring, homomorphism*

1. Introduction

The concept of Γ ring, which is a generalization of the concept of ring, was first defined by Nobusawa in [1].

Barnes, in [2], weakened some of the conditions of the definition of Nobusawa, and defined those that he called Γ-rings, naming Γ-rings defined in [1], as Γ-rings of Nobusawa.

Based to the definition of Nobusawa's Γ-ring, Sen in [3], defined Γ-semigroup that is called Γ-semigroup of Sen. Sen and Saha in [4], defined a generalization of Γ-semigroup of Sen, which is called a Γ-semigroup. The concept of Γ-semigroup may be obtained by that of Γ-ring, by extracting addition.

Petro and Sema, in [5], weakened further the conditions of the definition of Barnes and defined those that they called weakly Γ-rings.

An important concept for every algebraic structure is homomorphism. Thus, it is eligible extending this concept to weakly Γ-rings.

In this paper, homomrphism to weakly Γ-rings is introduced and some simple results of rings to Γ-rings, which are related to this concept, are extended.

2. Materials and Methods

Here we give some notions and present some auxiliary results that will be used throughout the paper.

Let M and Γ be two nonempty sets. Any map from $M \times \Gamma \times M$ to M is called a Γ-*multiplication* on M and is denoted by $(\cdot)_\Gamma$. The result of this Γ-multiplication for each $a, b \in M$ and each $\gamma \in \Gamma$, is denoted by $a\gamma b$.

The concept of Γ-ring, which is a generalization of the concept of ring, was first defined by Nobusawa in [1], as follows:

Definition 2.1. [1] *Let M be an additive group with elements $a, b, c, \ldots$ and Γ another additive group with elements $\alpha, \beta, \gamma, \ldots$. Assume that $a\alpha b$ is defined as an element of M and $\alpha a \beta$ is defined as an element of Γ for each a, b, α and β. If the products satisfy the following conditions*:

1. $(a_1+a_2)\alpha b=a_1\alpha b+a_2\alpha b$, $a(\alpha_1+\alpha_2)b=a\alpha_1 b+a\alpha_2 b$, $a\alpha(b_1+b_2)=a\alpha b_1+a\alpha b_2$,
2. $(a\alpha b)\beta c = a\alpha(b\beta c) = a(\alpha b\beta)c$,
3. *if* $a\alpha b = 0$ *for each* a *and* b *in* M, *then* $\alpha = 0$,

then M is called a Γ-ring.

An ordinary ring $(A, +, \cdot)$ may turn into a Γ-ring, if we get M and Γ to be equal to A.

Barnes, in [2], weakened some of the conditions of Nobusawa, by calling Γ-rings of Nobusawa the ones defined as above and simply Γ-rings those that he defined himself.

Definition 2.2. [2] Every ordered five-tuple $(M, \Gamma, +, \oplus, (\cdot)_\Gamma)$, where M, Γ are sets, + is an addition on M, $\oplus$ addition on Γ, $(\cdot)_\Gamma$ is a Γ-multiplication on M, such that:

1. $(M, +)$ *is an abelian group.*
2. $(\Gamma, \oplus)$ *is an abelian group.*
3. $\forall(a, b, c, \alpha, \beta) \in M^3 \times \Gamma^2, (a\alpha b)\beta c = a\alpha(b\beta c)$.
4. $\forall(a, b, c, \gamma) \in M^3 \times \Gamma, (a + b)\gamma c = a\gamma c + b\gamma c$.
5. $\forall(a, b, c, \gamma) \in M^3 \times \Gamma, a\gamma(b + c) = a\gamma b + a\gamma c$.
6. $\forall(a, b, \alpha, \beta) \in M^2 \times \Gamma^2, a(\alpha \oplus \beta)b = a\alpha b + a\beta b$,

is called Γ-ring (of Barnes).

Sen and Saha in [4], defined Γ-semigroups, which may be obtained by the definition of Γ-rings, by avoiding the additions:

Definition 2.3. [4] Every ordered pair $(M, (\cdot)_\Gamma)$, where M and Γ are two nonempty sets and $(\cdot)_\Gamma$ is a Γ-multiplication on M, which satisfies the following condition:

$\forall(a, b, c, \alpha, \beta) \in M^3 \times \Gamma^2, (a\alpha b)\beta c = a\alpha(b\beta c)$,

is called Γ-semigroup.

The element $0 \in M$, such that:

$\forall(a, \gamma) \in M \times \Gamma, a\gamma 0 = 0 = 0\gamma a$,

is called zero of the Γ-semigroup $(M, (\cdot)_\Gamma)$.

Petro and Sema in [5], weakened further the conditions of the definition of Γ-rings (of Barnes), by defining weakly Γ-rings, as follows:

Definition 2.4. [5] Every ordered triple $(M, +, (\cdot)_\Gamma)$, where M, Γ are two nonempty sets, $+$ is an addition on M and $(\cdot)_\Gamma$ is a Γ-multiplication on M, such that:

1) $(M, +)$ *is an abelian group*,
2) $(M, (\cdot)_\Gamma)$ *is a* Γ*-semigroup*,
3) $\forall(a, b, c, \gamma) \in M^3 \times \Gamma, [(a + b)\gamma c = a\gamma c + b\gamma c] \wedge [a\gamma(b + c) = a\gamma b + a\gamma c]$,

is called weakly Γ-ring.

We notice that plain rings, Γ-rings of Nobusawa and Γ-rings of Barnes, are weakly Γ-rings, but the converse is not true.

Saha and Seth in [6] have introduced the concept of homomrphism between two Γ-semigroups, as follows:

Definition 2.5. [6] Let $(M, (\cdot)_\Gamma)$ be a Γ-semigroup and $(M_1, (\cdot)_{\Gamma_1})$ a Γ_1-semigroup. A pair of mappings (h_1, h_2), where $h_1 : M \to M_1$ and $h_2 : \Gamma \to \Gamma_1$, such that

$h_1(a\gamma b) = h_1(a)h_2(\gamma)h_1(b)$,

for each $a, b \in M$ and $\gamma \in \Gamma$, is called a homomorphism of (M, Γ) to (M_1, Γ_1).

Let $(M, +, (\cdot)_\Gamma)$ be a weakly Γ-ring. Every nonempty subset T of M, such that $(T, +)$ is a subgroup of $(M, +)$ and $a\gamma b \in T$, for each $(a, b) \in T^2$ and $\gamma \in \Gamma$, is called subΓ-ring of M.

Let M be a weakly Γ-ring and A, B two nonempty subsets of M. Define:

$A\Gamma B = \{\sum_{i=1}^{n} a_i\gamma_i b_i \in M : a_i \in A, b_i \in B, \gamma_i \in \Gamma \text{ for each } i = 1,2, \ldots, n; n \in \mathbb{N}\}$.

Every subgroup R $[L]$ of the group $(M, +)$, such that:

$R\Gamma M \subseteq R$ $[M\Gamma L \subseteq L]$,

is called right [left] ideal of the weakly Γ-ring $(M, +, (\cdot)_\Gamma)$.

Every subgroup I of the group $(M, +)$, such that:

$I\Gamma M \subseteq I$ and $M\Gamma I \subseteq I$, is called *ideal* of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$.

Thus, I is an ideal of the weakly Γ-ring M, only if it is a left ideal and a right ideal of M simultaneously.

3. Conclusions

In this section, basing on what is given above, mixing them, some new results are given.

Definition 3.1. *Let $(M,+,(\cdot)_\Gamma)$ be a weakly Γ-ring and $(M',+,(\cdot)_{\Gamma'})$ be a weakly Γ'-ring. Every ordered pair of mappings $H=(h_1,h_2)$, where $h_1: M \to M'$ and $h_2: \Gamma \to \Gamma'$, such that*:

1) $\forall(a,b) \in M^2, h_1(a+b)=h_1(a)+h_1(b)$.
2) $\forall(a,\alpha,b) \in M\times\Gamma\times M, h_1(a\alpha b)=h_1(a)h_2(\alpha)h_1(b)$,

is called a homomorphism of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ'-ring $(M',+,(\cdot)_{\Gamma'})$.

It is obvious that every homomorphism of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$, is an ordered pair of mappings (h_1,h_2), where h_1 is a homomorphism of the additive group $(M,+)$ of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the additive group $(M',+)$ of the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$, whereas (h_1,h_2) is a homomorphism of the Γ-semigroup $(M,(\cdot)_\Gamma)$ of the Γ-multiplication of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the Γ′-semigroup $(M',(\cdot)_{\Gamma'})$ of the Γ′-multiplication of the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$.

If both mappings h_1,h_2 are injective (one-to-one), the homomorphism H=(h_1, h_2) is called monomorphism and (M,Γ) is called monomorph to (M',Γ'). If these mappings are both surjective (onto), H is called epiomorphism and (M,Γ) is called epiomorph to (M',Γ'), whereas when both h_1, h_2 are bijective, H is called isomorphism, and (M,Γ) is called isomorph to (M',Γ').

Definition 3.2. Let $H=(h_1,h_2)$ be a homomorphism of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ'-ring $(M',+,(\cdot)_{\Gamma'})$. The kernel of the homomorphism h_1 of the additive group $(M,+)$ to the additive group $(M',+)$, is called kernel of the homomorphism $H=(h_1,h_2)$, and will be denoted by $KerH$. Thus:

$KerH=\{x\in M: h(x)=0_{M'}\}$.

The image of the homomorphism h_1, is called *image* of the homomorphism $H=(h_1,h_2)$, and will be denoted by ImH. Thus:

$ImH=\{h_1(x)\in M': x\in M\}=\{x'\in M': \exists x\in M, h_1(x)=x'\}$.

Proposition 3.3. *For every homomorphism $H=(h_1,h_2)$ of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ'-ring $(M',+,(\cdot)_{\Gamma'})$, the kernel $KerH$ is an ideal of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$, whereas, when h_2 is a surjective mapping, ImH is a subΓ'-ring of the weakly Γ'-ring $(M',+,(\cdot)_{\Gamma'})$.*

Proof. $KerH$ is a subgroup of the additive group of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$. For each element a of M, for each element b of $KerH$ and for each element γ of Γ, the following hold

$h_1(a\gamma b)=h_1(a)h_2(\gamma)h_1(b)=0h_2(\gamma)h_1(b)=0,$

$h_1(b\gamma a)=h_1(b)h_2(\gamma)h_1(a)=h_1(b)h_2(\gamma)0=0,$

which show that $KerH$ is an ideal of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$.

Let a',b' be two elements of ImH and γ' an arbitrary element of Γ′. Then, there exist the elements $a,b\in M$ and the element $\gamma\in\Gamma$, such that:

$a'=h_1(a),\ \ b'=h_1(b),\ \ \gamma'=h_2(\gamma)$.

The following equalities hold:

$a'\gamma'b'=h_1(a)h_2(\gamma)h_1(b)=h_1(a\gamma b),$

which show that ImH is a subΓ′-ring of the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$, since ImH is a subgroup of the group $(M',+)$. ■

Let $H=(h_1,h_2)$ be a homomorphism of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$, and B′ a subset of M'. Denote

$H^{-1}(\mathrm{B}')=\{x\in M: h_1(x)\in \mathrm{B}'\}$.

The subset $H^{-1}(\mathrm{B}')$ of M, will be called *inverse image* of B′.

Proposition 3.4 *Let $H=(h_1,h_2)$ be an epiomorphism of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ to the weakly Γ'-ring $(M',+,(\cdot)_{\Gamma'})$ with kernel, the ideal I of $(M,+,(\cdot)_\Gamma)$. Then, a nonempty subset B' of M' is an ideal of $(M',+,(\cdot)_{\Gamma'})$ if and only if*

$H^{-1}(B')=B$

is an ideal of the weakly Γ-ring $(M,+,(\cdot)_\Gamma)$ that contains the ideal I.

Proof. Assume that the nonempty subset B′ of M' is an ideal of the weakly Γ′-ring $(M',+,(\cdot)_{\Gamma'})$. Let a be an ordinary element of M, b an ordinary element of $B = H^{-1}(\mathrm{B}')$ and γ an ordinary element of Γ. Since:

$h_1(a\gamma b) = h_1(a)h_2(\gamma)h_1(b) \in M'\Gamma'B' \subseteq B'$,

$h_1(b\gamma a) = h_1(b)h_2(\gamma)h_1(a) \in B'\Gamma'M' \subseteq B'$,

the elements $a\gamma b, b\gamma a$ belong to the subset B and consequently $H^{-1}(\mathrm{B}') = B$ is an ideal of the weakly Γ-ring $(M, +, (\cdot)_\Gamma)$, since $H^{-1}(\mathrm{B}')$ is a subgroup of the additive group $(M, +)$ of the weakly Γ-ring $(M, +, (\cdot)_\Gamma)$.

The ideal $H^{-1}(\mathrm{B}') = B$ contains the ideal I of the epiomorphism H,:since we have

$\forall x \in M, x \in I \Rightarrow h_1(x) = 0 \in B'$.

Conversely, suppose that $H^{-1}(\mathrm{B}') = B$ is an ideal of the weakly Γ-ring $(M, +, (\cdot)_\Gamma)$, that contains the ideal I. Let a' be an element of M', b' an element of B' and γ' an element of Γ'. There exist the elements $a \in M, b \in H^{-1}(\mathrm{B}') = B$ and $\gamma \in \Gamma$, such that:

$a' = h_1(a),\ \ b' = h_1(b),\ \ \gamma' = h_2(\gamma)$.

The following equalities hold:

$a' - b' = h_1(a) - h_1(b) = h_1(a - b)$,

$a'\gamma'b' = h_1(a)h_2(\gamma)h_1(b) = h_1(a\gamma b)$,

$b'\gamma'a' = h_1(b)h_2(\gamma)h_1(a) = h_1(b\gamma a)$,

that show that B' is an ideal of the weakly Γ'-ring $(M', +, (\cdot)_{\Gamma'})$, since $B' \neq \emptyset$, because $I \subseteq H^{-1}(B') = B$, and $H^{-1}(\mathrm{B}') = B$ is an ideal of $(M, +, (\cdot)_\Gamma)$, that guarantees us that a-b, aγb, bγa are elements of $H^{-1}(\mathrm{B}') = B$. ■

References

Barnes, W.. E., (1966), “On the Γ-rings of Nobusawa”, *Pacific Journal of Mathematics*, 18, No. 3, p. 411-422.

Nobusawa, N. (1964), “On a generalization of ring theory”, *Osaka J. Math* , 1, p. 81-89.

Petro, P. and Sema, R., (2010), “Weakly Γ-rings and Γ-fields”, *AJNTS,* 28, Vol. 2, p. 157-168.

Saha, N.K. and Seth, (1987-1988), “Inverse Γ-semigroup”, *Journal of Pure Math*., Vol. 6, p. 0-8.

Sen, M.K. and Saha, N.K., (1986), “On Γ-semigroups I”, *Bull. Cal. Math. Soc.* 78, p. 81-89.

Sen, M.K., (1981), “On Γ-semigroups”, *Procedings of International Conference on Algebra and its Applications, Decker Publications*, New York, 301.