#A5 INTEGERS 24 (2024)

GROUPS AND MONOID IN THE SET OF PYTHAGOREAN TRIPLES

Roberto Amato
Department of Engineering, University of Messina, Italy
ramato@unime.it

Received: 6/6/23, Revised: 10/24/23, Accepted: 12/15/23, Published: 1/2/24

Abstract

The primary objective of this paper is to find suitable binary operations on the set of Pythagorean triples, obtaining two commutative infinite groups, one with elements in $\mathbb{Q}$ and the other with elements in $\mathbb{Z}$. Additionally, we aim to get a commutative infinite monoid with elements in $\mathbb{N}$ or in $\mathbb{Z}$. In particular, on the set of primitive Pythagorean triples, we establish a commutative infinite group with elements in $\mathbb{Z}$.

1. Introduction

Let x, y, and z be positive integers satisfying

$$x^2 + y^2 = z^2.$$

Such a triple (x, y, z) is called a *Pythagorean triple*. In particular, if x, y, and z are coprime, the triple is termed a *primitive Pythagorean triple*, while if $x, y, z \in \mathbb{Q}$, then it is described as a *rational Pythagorean triple*.

The main aim of this paper is to find some suitable binary operations on the set of Pythagorean triples to obtain some commutative infinite groups having elements in $\mathbb{Q}$ or in $\mathbb{Z}$. Moreover, we get a commutative infinite monoid having elements in $\mathbb{N}$ or in $\mathbb{Z}$. To achieve this, it is necessary to initially establish relations among Pythagorean triples. Let us review previous results concerning some relations among Pythagorean triples that have already been established. The primary tool utilized in those works was the fundamental characterization of Pythagorean triples through a cathetus. This reads as follows.

Theorem 1 ([1]). *The triple (x, y, z) is a Pythagorean triple if and only if there exists $d \in C(x)$ such that*

$$x = x, \qquad y = \frac{x^2}{2d} - \frac{d}{2}, \qquad z = \frac{x^2}{2d} + \frac{d}{2} \tag{1}$$

DOI: 10.5281/zenodo.10450948

with x positive integer, and where

$$C(x) = \begin{cases} D(x), & \text{if } x \text{ is odd,} \\ \\ D(x) \cap P(x), & \text{if } x \text{ is even,} \end{cases}$$

with

$$D(x) = \{d \in \mathbb{N} : d \leq x \text{ with } d \text{ divisor of } x^2\},$$

and if x is even with $x = 2^n k$, $n \in \mathbb{N}$ and $k \geq 1$ odd fixed, with

$$P(x) = \{d \in \mathbb{N} : d = 2^s l \text{ with } l \text{ divisor of } x^2 \text{ and } s \in \{1, 2, ..., n-1\}\}.$$

In Theorem 1 x is a predetermined integer, which means finding all right triangles whose sides have integer measures and one cathetus is predetermined. Moreover in [4], an analytic result was found that characterizes primitive Pythagorean triples through a cathetus. This method, which differs from Euler's formulas, offers the advantage of easily identifying all primitive Pythagorean triples $x, y, z \in \mathbb{N}$, where x is a predetermined integer.

In [2], relations were established between the primitive Pythagorean triple (x, y, z) generated by any predetermined positive odd integer x using formulas (1) and the primitive Pythagorean triple generated by x^m with $m \in \mathbb{N}$ and $m \geq 2$. In the same study, relations were found for the specific case in which the primitive triple (x, y, z) is generated by $d \in C(x)$ for $d = 1$ and the primitive triple (x^m, y', z') is generated by $d_m \in C(x^m)$ for $d_m = 1$. Consequently. formulas were obtained that give y' and z' directly from x, y, z.

Subsequently, additional relations among Pythagorean triples were established in [3]. The primary tool that serves as the foundation of our analysis is Theorem 1 in [1], enabling the determination of relationships between two Pythagorean triples with assigned catheti a and b, and the Pythagorean triple with cathetus $a \cdot b$. To summarize, the above statements can be encapsulated as follows.

Theorem 2 ([1],[3]). *Let $(a, a_1, a_2), (b, b_1, b_2)$, and $(a \cdot b, y, z)$ be the Pythagorean triples generated by a, b, and $a \cdot b$, respectively, using* (1) *with $a_2 - a_1 = d_1 \in C(a)$, $b_2 - b_1 = d_2 \in C(b)$, and $z - y = d_3 \in C(a \cdot b)$. Then*

$$y = a_1 b_2 + a_2 b_1, \qquad z = a_1 b_2 + a_2 b_1 + d_1 d_2 \tag{2}$$

and moreover,

$$y = a_1 b_1 + a_2 b_2 - d_1 d_2, \qquad z = a_1 b_1 + a_2 b_2 \tag{3}$$

with $d_3 = d_1 \cdot d_2 \in C(a \cdot b)$.

In Section 2 we will prove the existence of some suitable binary operations on the set of Pythagorean triples. The goal is to establish some commutative infinite groups having elements in $\mathbb{Q}$ or in $\mathbb{Z}$, and a commutative infinite monoid having elements in $\mathbb{N}$ or in $\mathbb{Z}$.

2. Results

We consider the set

$$G = \{(a,b) : a, b \in \mathbb{Z} \text{ with } |a| \text{ and } |b| \text{ coprime}\}$$

and for all (a,b), (c,d), and (e,f) in G, we define the set

$$E = \left\{ \left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) \text{ with } \frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q} \text{ and } a, b, d, f \neq 0 \text{ such that } \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2 = \left(\frac{e}{f}\right)^2 \right\}.$$

In order to find a binary operation on E, we need to prove the following lemma.

Lemma 1. *For any* $\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)$ *and* $\left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) \in E$ *the operation, defined as*

$$\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) \cdot \left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) = \left(\frac{ag}{bh}, \frac{cm}{dn} + \frac{ei}{fl}, \frac{cm}{dn} + \frac{ei}{fl} + d_1 d_2\right), \tag{4}$$

with $d_1 = \frac{e}{f} - \frac{c}{d}$ *and* $d_2 = \frac{m}{n} - \frac{i}{l}$, *is a binary operation on* E.

Proof. To prove that $\left(\frac{ag}{bh}, \frac{cm}{dn} + \frac{ei}{fl}, \frac{cm}{dn} + \frac{ei}{fl} + d_1 d_2\right) \in E$, we verify that

$$\left(\frac{ag}{bh}\right)^2 + \left(\frac{cm}{dn} + \frac{ei}{fl}\right)^2 = \left(\frac{cm}{dn} + \frac{ei}{fl} + d_1 d_2\right)^2, \tag{5}$$

that is,

$$\left(\frac{a^2}{b^2}\right) \cdot \left(\frac{g^2}{h^2}\right) = d_1^2 d_2^2 + 2\left(\frac{cm}{dn} + \frac{ei}{fl}\right) d_1 d_2 \,.$$

Taking into account that

$$\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right), \left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) \in E,$$

we obtain

$$\left(\frac{e^2}{f^2} - \frac{c^2}{d^2}\right) \cdot \left(\frac{m^2}{n^2} - \frac{i^2}{l^2}\right) = \left(\frac{e}{f} - \frac{c}{d}\right) \cdot \left(\frac{m}{n} - \frac{i}{l}\right) \cdot \left[\left(\frac{e}{f} - \frac{c}{d}\right) \cdot \left(\frac{m}{n} - \frac{i}{l}\right) + 2\left(\frac{cm}{dn} + \frac{ei}{fl}\right)\right].$$

From this, we get

$$\left(\frac{e}{f} + \frac{c}{d}\right) \cdot \left(\frac{m}{n} + \frac{i}{l}\right) = \left(\frac{e}{f} - \frac{c}{d}\right) \cdot \left(\frac{m}{n} - \frac{i}{l}\right) + 2\left(\frac{cm}{dn} + \frac{ei}{fl}\right)$$

from which it is easy to see that $2edin + 2fcml = 2cmfl + 2eidn$. As a result, the Pythagorean triple (5) is an identity in $\mathbb{Q}$. Therefore,

$$\left(\frac{ag}{bh}, \frac{cm}{dn} + \frac{ei}{fl}, \frac{cm}{dn} + \frac{ei}{fl} + d_1d_2\right) \in E$$

and the operation (4) is a binary operation on E. □

It is noteworthy that the binary operation (4) is defined in the same manner as the relation among Pythagorean triples (2) found in [3], specifically in the case of positive integers.

The following theorem holds.

Theorem 3. *The set E, together with the binary operation* (4) *defined on E, is a commutative infinite group with elements in $\mathbb{Q}$.*

Proof. We prove that in E, together with the binary operation (4) defined on E, the three group axioms hold, and the binary operation is commutative.

In order to prove the first axiom, considering for all $\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)$, $\left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right)$, and $\left(\frac{o}{p}, \frac{q}{r}, \frac{s}{t}\right) \in E$ with $d_1 = \frac{e}{f} - \frac{c}{d}$, $d_2 = \frac{m}{n} - \frac{i}{l}$, and $d_3 = \frac{s}{t} - \frac{q}{r}$ we verify that

$$\left[\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)\cdot\left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right)\right]\cdot\left(\frac{o}{p}, \frac{q}{r}, \frac{s}{t}\right) = \left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)\cdot\left[\left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right)\cdot\left(\frac{o}{p}, \frac{q}{r}, \frac{s}{t}\right)\right]. \quad (6)$$

Using the operation (4) within the square brackets, we get

$$\left(\frac{ag}{bh}, \frac{cm}{dn} + \frac{ei}{fl}, \frac{cm}{dn} + \frac{ei}{fl} + d_1d_2\right)\cdot\left(\frac{o}{p}, \frac{q}{r}, \frac{s}{t}\right)$$

$$= \left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)\cdot\left(\frac{go}{hp}, \frac{is}{tl} + \frac{mq}{nr}, \frac{is}{tl} + \frac{mq}{nr} + d_2d_3\right)$$

and re-applying it, we obtain

$$\left(\frac{ago}{bhp}, \left(\frac{cm}{dn} + \frac{ei}{fl}\right)\cdot\frac{s}{t} + \left(\frac{cm}{dn} + \frac{ei}{fl} + d_1d_2\right)\cdot\frac{q}{r}, \left(\frac{cm}{dn} + \frac{ei}{fl}\right)\cdot\frac{s}{t} \right.$$
$$\left. + \left(\frac{cm}{dn} + \frac{ei}{fl} + d_1d_2\right)\cdot\frac{q}{r} + d_1d_2d_3\right)$$

$$= \left(\frac{ago}{bhp}, \frac{c}{d}\cdot\left(\frac{is}{tl} + \frac{mq}{nr} + d_2d_3\right) + \frac{e}{f}\cdot\left(\frac{is}{tl} + \frac{mq}{nr}\right), \frac{c}{d}\cdot\left(\frac{is}{tl} + \frac{mq}{nr} + d_2d_3\right)\right.$$
$$\left. + \frac{e}{f}\cdot\left(\frac{is}{tl} + \frac{mq}{nr}\right) + d_1d_2d_3\right).$$

To prove that the latter equation is an identity, it suffices to verify that

$$\left(\frac{cm}{dn}+\frac{ei}{fl}\right)\cdot\frac{s}{t}+\left(\frac{cm}{dn}+\frac{ei}{fl}+d_1d_2\right)\cdot\frac{q}{r}=\frac{c}{d}\cdot\left(\frac{is}{tl}+\frac{mq}{nr}+d_2d_3\right)+\frac{e}{f}\cdot\left(\frac{is}{tl}+\frac{mq}{nr}\right).$$

To this aim, by replacing d_1, d_2, d_3, we have

$$\left(\frac{cm}{dn}+\frac{ei}{fl}\right)\cdot\frac{s}{t}+\left(\frac{cm}{dn}+\frac{ei}{fl}+\frac{(ed-cf)\cdot(ml-ni)}{fdnl}\right)\cdot\frac{q}{r}$$
$$=\frac{c}{d}\cdot\left(\frac{is}{tl}+\frac{mq}{nr}+\frac{(ml-ni)\cdot(sr-qt)}{nltr}\right)+\frac{e}{f}\cdot\left(\frac{is}{tl}+\frac{mq}{nr}\right),$$

from which

$$\frac{cmfl+eidn}{df}\cdot\frac{s}{t}+\frac{edml+cfin}{fd}\cdot\frac{q}{r}=\frac{c}{d}\cdot\frac{mlsr+inqt}{tr}+\frac{e}{f}\cdot\frac{isnr+mqlt}{tr}$$

that can be easily proved to be an identity in $\mathbb{Q}$. As a result, the requirement of associativity (6) holds. Therefore, the first axiom is proved.

To prove the second axiom, we define the identity element as

$$\left(\frac{1}{1},\frac{0}{1},\frac{1}{1}\right)=(1,0,1)\ ; \tag{7}$$

obviously $(1,0,1)\in E$. We also verify that, for all $\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)\in E$, we have

$$\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)\cdot(1,0,1)=(1,0,1)\cdot\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)=\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right). \tag{8}$$

Using the operation (4) on both sides of equation (8), we obtain

$$\left(\frac{a}{b}\cdot 1,\ \frac{c}{d}\cdot 1+\frac{e}{f}\cdot 0,\ \frac{c}{d}\cdot 1+\frac{e}{f}\cdot 0+\left(\frac{e}{f}-\frac{c}{d}\right)\cdot 1\right)=\left(1\cdot\frac{a}{b},0\cdot\frac{e}{f}+\cdot 1\cdot\frac{c}{d},0\cdot\frac{e}{f}+1\cdot\frac{c}{d}+1\left(\frac{e}{f}-\frac{c}{d}\right)\right),$$

that is,

$$\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)=\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)$$

and consequently, the second axiom is proved.

To prove the third axiom, for all $\left(\frac{a}{b},\frac{c}{d},\frac{e}{f}\right)\in E$, we define the inverse element as

$$\left(\frac{b}{a},-\frac{c}{d}\cdot\frac{b^2}{a^2},\frac{e}{f}\cdot\frac{b^2}{a^2}\right). \tag{9}$$

Obviously $\left(\frac{b}{a}, -\frac{c}{d} \cdot \frac{b^2}{a^2}, \frac{e}{f} \cdot \frac{b^2}{a^2}\right) \in E$. We also verify that, for all $\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) \in E$, we have

$$\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) \cdot \left(\frac{b}{a}, -\frac{c}{d} \cdot \frac{b^2}{a^2}, \frac{e}{f} \cdot \frac{b^2}{a^2}\right) = \left(\frac{b}{a}, -\frac{c}{d} \cdot \frac{b^2}{a^2}, \frac{e}{f} \cdot \frac{b^2}{a^2}\right) \cdot \left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) = \left(1, 0, 1\right). \tag{10}$$

Using the operation (4) on both sides of the equation (10), we obtain

$$\left(\frac{a}{b}\frac{b}{a}, \frac{c}{d}\frac{e}{f}\frac{b^2}{a^2} - \frac{e}{f}\frac{c}{d}\frac{b^2}{a^2}, \frac{c}{d}\frac{e}{f}\frac{b^2}{a^2} - \frac{e}{f}\frac{c}{d}\frac{b^2}{a^2} + \left(\frac{e}{f} - \frac{c}{d}\right)\frac{b^2}{a^2}\left(\frac{e}{f} + \frac{c}{d}\right)\right)$$

$$= \left(\frac{b}{a}\frac{a}{b}, -\frac{c}{d}\frac{b^2}{a^2}\frac{e}{f} + \frac{e}{f}\frac{b^2}{a^2}\frac{c}{d}, \frac{c}{d}\frac{b^2}{a^2}\frac{e}{f} - \frac{e}{f}\frac{b^2}{a^2}\frac{c}{d} + \frac{b^2}{a^2}\left(\frac{e}{f} + \frac{c}{d}\right)\left(\frac{e}{f} - \frac{c}{d}\right)\right).$$

From this, we get

$$\left(1, 0, \left(\frac{e^2}{f^2} - \frac{c^2}{d^2}\right)\frac{b^2}{a^2}\right) = \left(1, 0, \frac{b^2}{a^2}\left(\frac{e^2}{f^2} - \frac{c^2}{d^2}\right)\right)$$

from which

$$(1, 0, 1) = (1, 0, 1).$$

Therefore, the third axiom is proved.

To prove that the group is commutative for all $\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)$ and $\left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) \in E$ with $d_1 = \frac{e}{f} - \frac{c}{d}$ and $d_2 = \frac{m}{n} - \frac{i}{l}$, we verify that

$$\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right) \cdot \left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) = \left(\frac{g}{h}, \frac{i}{l}, \frac{m}{n}\right) \cdot \left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right). \tag{11}$$

Using the operation (4) on both sides of equation (11), we obtain that

$$\left(\frac{ag}{bh}, \frac{cm}{dn} + \frac{ei}{fl}, \frac{cm}{dn} + \frac{ei}{fl} + d_1 d_2\right) = \left(\frac{ga}{hb}, \frac{ie}{lf} + \frac{mc}{nd}, \frac{ie}{lf} + \frac{mc}{nd} + d_2 d_1\right)$$

is an identity in $\mathbb{Q}$ and therefore the fourth axiom is proved. Consequently, Theorem 3 is fully proved. □

Now, taking into account the relation among Pythagorean triples (2) found in [3], if we consider the set

$$M = \{(a, b, c) \text{ with } a, b, c \in \mathbb{Z} \text{ such that } a^2 + b^2 = c^2\},$$

it is easily to note that, for all (a, b, c) and $(d, e, f) \in M$ with $d_1 = c - b$ and $d_2 = f - e$, the operation defined as

$$(a, b, c) \cdot (e, f, g) = (ae, bf + ce, bf + ce + d_1 d_2) \tag{12}$$

is still a binary operation on M. Furthermore, it is straightforward to confirm that the first and second axioms hold true. The binary operation is commutative being a particular case of operation (4), with the same identity element $(1, 0, 1)$. The inverse element can be defined as in definition (9), for all $(a, b, c) \in M$, as

$$\text{if } a \neq 0, \ \left(\frac{1}{a}, -\frac{b}{a^2}, \frac{c}{a^2}\right). \tag{13}$$

Consequently, this element does not belong to M because $\frac{1}{a}, -\frac{b}{a^2}$, and $\frac{c}{a^2}$ do not belong to $\mathbb{Z}$.

Therefore, since the third axiom is not verified, the following corollary holds.

Corollary 1. *The set M, together with the binary operation* (12) *defined on M, is a commutative infinite monoid with elements in $\mathbb{Z}$, and with elements in $\mathbb{N}$ if $a, b, c \in \mathbb{N}$.*

Moreover, it is worth noticing that the previously obtained results can be also retrieved through the relations among Pythagorean triples (3) found in [3].

Now, we aim to study if the set of all primitive Pythagorean triples forms a commutative infinite group. To this goal, let us define the set

$$P = \left\{ \left(\frac{a}{c}, \frac{b}{c}\right) \text{ with } a, b, c \in \mathbb{Z} \text{ and } a, c \neq 0, \text{ with } |a|, |b|, \text{and } |c| \text{ coprime}, \right.$$
$$\left. \text{such that } a^2 + b^2 = c^2 \right\}$$

and prove the following theorem.

Theorem 4. *The set P together with the binary operation on P, defined for all $\left(\frac{a}{c}, \frac{b}{c}\right)$ and $\left(\frac{d}{f}, \frac{e}{f}\right) \in P$ as $l : P \times P \to P$, such that*

$$\begin{cases} \left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left(\frac{d}{f}, \frac{e}{f}\right) = \left(\frac{ad}{cf + eb}, \frac{bf + ec}{cf + eb}\right) & \textit{(I)} \\ \left(\frac{a^2}{a^2}, \frac{0}{a^2}\right) = \left(\frac{1}{1}, \frac{0}{1}\right) & \textit{(II)} \\ \left(\frac{a^{2n} ad}{a^{2n}(cf + eb)}, \frac{a^{2n}(bf + ec)}{a^{2n}(cf + eb)}\right) = \left(\frac{ad}{cf + eb}, \frac{bf + ec}{cf + eb}\right), \quad \textit{for all } n \in \mathbb{N}, & \textit{(III)} \end{cases} \tag{14}$$

is a commutative infinite group with elements in Q.

Proof. Firstly, we verify that the operation (14) is a binary operation on P, that is,

$$(ad)^2 + (bf + ec)^2 = (cf + eb)^2. \tag{15}$$

From this, we obtain

$$a^2 d^2 + e^2(c^2 - b^2) = f^2(c^2 - b^2)$$

and

$$d^2 + e^2 = f^2.$$

Moreover, we need to verify that, for all $\left(\frac{a}{c}, \frac{b}{c}\right)$ and $\left(\frac{d}{f}, \frac{e}{f}\right) \in P$, it also follows that $|ad|, |bf + ec|$, and $|cf + eb|$ are coprime. Since the Pythagorean triple (15) must be satisfied, it is sufficient to verify that $|bf + ec|$ and $|cf + eb|$ are coprime. In fact, if there exists $k \in \mathbb{Z} - \{0\}$ such that $cf + eb = k(bf + ec)$, we obtain $f(c - kb) = e(kc - b)$. Since $|f|$ and $|e|$ are coprime, it follows that $f = kc - b$ and $e = c - kb$, that is,

$$k = \frac{f + b}{c} \quad \text{and} \quad k = \frac{c - e}{b}$$

from which

$$b(f + b) = c(c - e).$$

From the previous equation, given that $|b|$ and $|c|$ are coprime, it follows that $b = c - e$ and $c = f + b$. Consequently, $f = e$, which is an absurdity. As a result, $\left(\frac{ad}{cf + eb}, \frac{bf + ec}{cf + eb}\right) \in P$ and therefore the operation (14) is a binary one on P.

To prove the second axiom, we define the identity element as $\left(\frac{1}{1}, \frac{0}{1}\right)$. Obviously, $\left(\frac{1}{1}, \frac{0}{1}\right) \in P$. Let us now verify that, for all $\left(\frac{a}{c}, \frac{b}{c}\right) \in P$, the equation

$$\left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left(\frac{1}{1}, \frac{0}{1}\right) = \left(\frac{1}{1}, \frac{0}{1}\right) \cdot \left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{a}{c}, \frac{b}{c}\right) \tag{16}$$

holds true. By using the condition (I) in the operation (14) on the first two members of equation (16), we obtain

$$\left(\frac{a1}{c1 + 0b}, \frac{b1 + 0c}{c1 + 0b}\right) = \left(\frac{1a}{1c + b0}, \frac{0c + b1}{1c + b0}\right),$$

that is,

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{a}{c}, \frac{b}{c}\right).$$

Therefore, the second axiom is proved.

To check the validity of the third axiom for all $\left(\frac{a}{c}, \frac{b}{c}\right) \in P$, we define the inverse element as $\left(\frac{a}{c}, -\frac{b}{c}\right)$. Obviously, $\left(\frac{a}{c}, -\frac{b}{c}\right) \in P$. Let us now verify that, for all $\left(\frac{a}{c}, \frac{b}{c}\right) \in P$, the equation

$$\left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left(\frac{a}{c}, -\frac{b}{c}\right) = \left(\frac{a}{c}, -\frac{b}{c}\right) \cdot \left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{1}{1}, \frac{0}{1}\right) \tag{17}$$

holds true. By using the condition (I) in the operation (14) on the first two members of equation (17), we obtain

$$\left(\frac{aa}{cc + (-b)b}, \frac{bc + (-b)c}{cc + (-b)b}\right) = \left(\frac{aa}{cc + b(-b)}, \frac{bc + c(-b)}{cc + b(-b)}\right),$$

that is,

$$\left(\frac{a^2}{c^2 - b^2}, \frac{0}{c^2 - b^2}\right) = \left(\frac{a^2}{c^2 - b^2}, \frac{0}{c^2 - b^2}\right).$$

Moreover, since $c^2 - b^2 = a^2$, according to the condition (II) in the operation (14), we obtain

$$\left(\frac{1}{1}, \frac{0}{1}\right) = \left(\frac{1}{1}, \frac{0}{1}\right)$$

and consequently, the third axiom is proved.

We observe that the inclusion of condition (II) in the operation (14) eliminates the possibility of getting all trivial elements $\left(\frac{a^2}{a^2}, \frac{0}{a^2}\right)$ such that $a^2 + 0^2 = a^2$, which do not belong to P. For this same reason, whenever we have a product of elements in P that includes both $\left(\frac{a}{c}, \frac{b}{c}\right)$ and $\left(\frac{a}{c}, -\frac{b}{c}\right)$, it is necessary to divide both the numerator and denominator of the fractions in the final result of the product by a^2. This ensures that we still obtain elements belonging to P. Otherwise, we would end up with elements $\left(\frac{a^2ad}{a^2(cf + eb)}\right), \left(\frac{a^2(bf + ec)}{a^2(cf + eb)}\right)$ such that $(a^2ad)^2 + (a^2(bf + ec))^2 = (a^2(cf + eb))^2$, which do not belong to P. Obviously, if both elements $\left(\frac{a}{c}, \frac{b}{c}\right)$ and $\left(\frac{a}{c}, -\frac{b}{c}\right)$ appear n times, then it is necessary to divide by a^{2n}. Now, the conditions (II) and (III) in operation (14) have been fully justified.

To prove the first axiom, let us now verify that the condition

$$\left[\left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left(\frac{d}{f}, \frac{e}{f}\right)\right] \cdot \left(\frac{g}{i}, \frac{h}{i}\right) = \left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left[\left(\frac{d}{f}, \frac{e}{f}\right) \cdot \left(\frac{g}{i}, \frac{h}{i}\right)\right] \tag{18}$$

holds true for all $\left(\frac{a}{c}, \frac{b}{c}\right), \left(\frac{d}{f}, \frac{e}{f}\right)$ and $\left(\frac{g}{i}, \frac{h}{i}\right) \in P$ with $\left(\frac{d}{f}, \frac{e}{f}\right) \neq \left(\frac{a}{c}, -\frac{b}{c}\right)$ and

$\left(\frac{d}{f},\frac{e}{f}\right)\neq\left(\frac{g}{i},-\frac{h}{i}\right)$. To this aim, by applying first the condition (I) in the operation (14) to the terms within the square brackets in (18), we get

$$\left(\frac{ad}{cf+eb},\frac{bf+ec}{cf+eb}\right)\cdot\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a}{c},\frac{b}{c}\right)\cdot\left(\frac{dg}{fi+hl},\frac{ei+hf}{fi+hl}\right),$$

and by re-applying it to the obtained result, we end up with

$$\left(\frac{adg}{(cf+eb)i+h(bf+ec)},\frac{(bf+ec)i+h(cf+eb)}{(cf+eb)i+h(bf+ec)}\right)$$

$$=\left(\frac{adg}{c(fi+hl)+(ei+hf)b},\frac{b(fi+he)+(ei+hf)c}{c(fi+hl)+(ei+hf)b}\right),$$

which is easily verified to be an identity in $\mathbb{Q}$. As a result, the requirement of associativity (18) holds. On the other hand, if the condition

$$\left(\frac{d}{f},\frac{e}{f}\right)=\left(\frac{a}{c},-\frac{b}{c}\right)$$

holds true, we have

$$\left[\left(\frac{a}{c},\frac{b}{c}\right)\cdot\left(\frac{a}{c},-\frac{b}{c}\right)\right]\cdot\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a}{c},\frac{b}{c}\right)\cdot\left[\left(\frac{a}{c},-\frac{b}{c}\right)\cdot\left(\frac{g}{i},\frac{h}{i}\right)\right];$$

that is,

$$\left(\frac{1}{1},\frac{0}{1}\right)\cdot\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a}{c},\frac{b}{c}\right)\cdot\left(\frac{ag}{ci-hb},\frac{-bi+hc}{ci-hb}\right).$$

Consequently, we obtain

$$\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a^2g}{c(ci-hb)+(-bi+hc)b},\frac{b(ci-hb)+(-bi+hc)c}{c(ci-hb)+(-bi+hc)b}\right)$$

from which

$$\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a^2g}{i(c^2-b^2)},\frac{h(c^2-b^2)}{i(c^2-b^2)}\right).$$

Moreover, since $c^2-b^2=a^2$, we have

$$\left(\frac{g}{i},\frac{h}{i}\right)=\left(\frac{a^2g}{ia^2},\frac{ha^2}{ia^2}\right)$$

and, for the condition (III) in the operation (14), we obtain an identity even in the case $\left(\frac{d}{f},\frac{e}{f}\right)=\left(\frac{a}{c},-\frac{b}{c}\right)$. Analogously, the same conclusion can be achieved if $\left(\frac{d}{f},\frac{e}{f}\right)=\left(\frac{g}{i},-\frac{h}{i}\right)$. Therefore, the first axiom is proved.

To prove that the group is commutative for all $\left(\frac{a}{b}, \frac{b}{c}\right)$ and $\left(\frac{d}{f}, \frac{e}{f}\right) \in P$, we verify that

$$\left(\frac{a}{b}, \frac{b}{c}\right) \cdot \left(\frac{d}{f}, \frac{e}{f}\right) = \left(\frac{d}{f}, \frac{e}{f}\right) \cdot \left(\frac{a}{b}, \frac{b}{c}\right). \tag{19}$$

Using the condition (I) in the operation (14) on both sides of equation (19), we obtain

$$\left(\frac{ad}{cf+eb}, \frac{bf+ec}{cf+eb}\right) = \left(\frac{da}{fc+be}, \frac{ec+bf}{fc+be}\right),$$

which is an identity in $\mathbb{Q}$. Therefore, the group is commutative. Consequently, Theorem 4 is proved. □

Now, let us introduce the following theorem.

Theorem 5. *The set of all primitive Pythagorean triples is a commutative infinite group with elements in* $\mathbb{Z}$*.*

Proof. We define the set

$$S = \left\{ (a,b,c) \text{ with } a,b,c \in \mathbb{Z} \text{ such that} \left(\frac{a}{c}, \frac{b}{c}\right) \in P \right\},$$

that is, the set of Pythagorean triples. We also consider the function $f : S \to P$ such that

$$\begin{cases} f(a,b,c) = \left(\frac{a}{c}, \frac{b}{c}\right) \\ f[(a,b,c)\cdot(d,e,f)] = \left(\frac{a}{c}, \frac{b}{c}\right) \cdot \left(\frac{d}{f}, \frac{e}{f}\right) = \left(\frac{ad}{cf+eb}, \frac{bf+ec}{cf+eb}\right). \end{cases} \tag{20}$$

Additionally, we introduce the function $g : P \to S$ such that

$$g\left[\left(\frac{ad}{cf+eb}, \frac{bf+ec}{cf+eb}\right)\right] = (ad, bf+ec, cf+eb).$$

Now, we can define the composite function

$$h = g \circ f : S \to S$$

such that

$$h[(a,b,c)\cdot(d,e,f)] = \begin{cases} (ad, bf+ec, cf+eb), & \text{if } (d,e,f) \neq (a,-b,c) \\ (1,0,1), & \text{if } (d,e,f) = (a,-b,c) \\ \big(a^{2n}ad, a^{2n}(bf+ec), a^{2n}(cf+eb)\big) & \\ \quad = \big(ad, bf+ec, cf+eb\big), & \text{for all } n \in \mathbb{N}, \end{cases} \tag{21}$$

which is a binary operation on S.

We note that for $(d,e,f)=(a,-b,c)$, if we first apply the function f

$$f[(a,b,c)\cdot(a,-b,c)]=\left(\frac{a}{c},\frac{b}{c}\right)\cdot\left(\frac{a}{c},-\frac{b}{c}\right)=\left(\frac{1}{1},\frac{0}{1}\right)$$

and then the function g

$$g\left[\left(\frac{1}{1},\frac{0}{1}\right)\right]=(1,0,1),$$

we effectively obtain

$$h[(a,b,c)\cdot(a,-b,c)]=(1,0,1).$$

Obviously, the binary operation is commutative with the identity element $(1,0,1)$ and the inverse element $(a,-b,c)$.

On the other hand, if we apply the composite function h directly, for $(d,e,f)=(a,-b,c)$, we obtain $(a^2,0,a^2)\notin S$. Therefore, to avoid ambiguity, in operation (21) we use $(1,0,1)$ if $(d,e,f)=(a,-b,c)$. For the same reason, if the triples (a,b,c) and $(a,-b,c)$ appear n times, we set $(a^{2n}ad,a^{2n}(bf+ec),a^{2n}(cf+eb))=(ad,bf+ec,cf+eb)$ in the operation (21), for all $n\in\mathbb{N}$. Consequently, Theorem 5 is proved. □

At last, more generally, it is possible to obtain a commutative infinite group for the set M of all Pythagorean triples. To this aim, let us introduce the following operation i, for all (a,b,c) and $(d,e,f)\in M$, defined as follows:

$$i: M\to M$$

and

$$i[(a,b,c)\cdot(d,e,f)]=\begin{cases}(ad,bf+ec,cf+eb), & \text{if }(d,e,f)\neq(a,-b,c)\\ (1,0,1), & \text{if }(d,e,f)=(a,-b,c)\\ \big(a^{2n}ad,a^{2n}(bf+ec),a^{2n}(cf+eb)\big) & \\ \quad =\big(ad,bf+ec,cf+eb\big), & \text{for all } n\in\mathbb{N},\end{cases} \tag{22}$$

which is a binary operation on M. Obviously, the above binary operation is commutative, with the identity element $(1,0,1)$ and the inverse element $(a,-b,c)$. As a consequence of that, let us state the following corollary.

Corollary 2. *The set M, together with the binary operation* (22) *defined on M, is a commutative infinite group with elements in $\mathbb{Z}$.*

We have not used the composite function h to define the binary operation on M, for all (a,b,c) and $(d,e,f)\in M$. In fact, by using the definition of f given in (20), the quantities $|ad|, |bf+ec|$ and $|cf+eb|$ are not always coprime. For this reason, the fractions in

$$\left(\frac{ad}{cf+eb}, \frac{bf+ec}{cf+eb}\right)$$

may or may not be simplified, and in turn, the uniqueness of result in the binary operation may be not guaranteed.

As a consequence of Corollary 2, we obtain that the group (P, h) is a subgroup of (M, i).

3. Conclusion and Remarks

In this manuscript, we reinforced the results obtained in previous work by emphasizing that the parametrizations and relationships among Pythagorean triples depend on $d \in C(x)$, which plays a fundamental role in characterizing the results. This approach could be employed to study further relationships among Pythagorean triples. For instance, it might be used to find a scalar multiplication which could allow us, in turn, to define a vector space of Pythagorean triples.

Acknowledgements. The author is grateful to the managing editor Bruce Landman and anonymous reviewers, who read my manuscript with great care and offered useful suggestions.

References

[1] R. Amato, A characterization of pythagorean triples, *JP J. Algebra, Number Theory and Applic.* **39** (2017), 221-230.

[2] R. Amato, A note on Pythagorean triples, *Intern. J. Math. and Comp. Sci.* **15** (2) (2020), 485-490.

[3] R. Amato, Some relations among Pythagorean triples, *Intern. J. Math. and Comp. Sci.* **16** (1) (2021), 143-147.

[4] R. Amato, A characterization of primitive pythagorean triples, *Palestine J. Math.* **12** (2) (2023), 524-529.

[5] Jerzy Kocik, Clifford algebras and Euclid's parametrization of Pythagorean triples, *Adv. in Appl. Clifford Algebras* **17** (2007), 71-93.

[6] W.Sierpinski, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, Warszawa, 1988.