Open Mathematics

Research Article

Nadir Murru*, Marco Abrate, Stefano Barbero, and Umberto Cerruti

Groups and monoids of Pythagorean triples connected to conics

Abstract: We define operations that give the set of all Pythagorean triples a structure of commutative monoid. In particular, we define these operations by using injections between integer triples and 3×3 matrices. Firstly, we completely characterize these injections that yield commutative monoids of integer triples. Secondly, we determine commutative monoids of Pythagorean triples characterizing some Pythagorean triple preserving matrices. Moreover, this study offers unexpectedly an original connection with groups over conics. Using this connection, we determine groups composed by Pythagorean triples with the studied operations.

Keywords: Conics, Pythagorean groups, Pythagorean monoids, Pythagorean triples, Pythagorean triple preserving matrices

MSC: 11A99

1 Introduction

Algebraic structures, like groups and monoids, are widely studied in mathematics for their importance. It is very interesting to give particular sets an algebraic structure, in order to deepen their study. The set of Pythagorean triples and their properties have been extensively studied for several years and aroused the interests of many mathematicians. In spite of these studies, it is a hard work to give Pythagorean triples algebraic structures. In [1] and [2], an operation over Pythagorean triples has been studied, showing a group of primitive Pythagorean triples. In [3] and [4], a monoid structure has been provided.

In this paper, we show an original approach that allows to characterize a family of operations which determine commutative monoids of Pythagorean triples. In section 2, we define injections, which we call *natural*, between integer triples and 3×3 matrices. We use these injections to define products between integer triples, focusing on Pythagorean ones. In section 3, we characterize matrices generating natural injections that determine commutative monoids over $\mathbb{Z}^3$. Similarly, in section 4, we characterize a subset of Pythagorean triple preserving matrices, such that the set of all Pythagorean triples has a commutative monoid structure. Finally, in section 5, we find a surprising connection between Pythagorean triples and conics. In this way, we determine a group composed by Pythagorean triples by means of a morphism between points over conics and Pythagorean triples. Section 6 is devoted to conclusions.

***Corresponding Author: Nadir Murru:** Department of Mathematics, University of Turin, Torino, 10123, Italy,
E-mail: nadir.murru@unito.it
Marco Abrate: Department of Mathematics, University of Turin, Torino, 10123, Italy, E-mail: marco.abrate@unito.it
Stefano Barbero: Department of Mathematics, University of Turin, Torino, 10123, Italy, E-mail: stefano.barbero@unito.it
Umberto Cerruti: Department of Mathematics, University of Turin, Torino, 10123, Italy, E-mail: umberto.cerruti@unito.it

2 Commutative monoids of Pythagorean triples

Let $\mathcal{P}$ be the set of Pythagorean triples

$$\mathcal{P} = \{(x, y, z) \in \mathbb{Z}^3 : x^2 + y^2 = z^2\}.$$

Several operations can be defined over this set. In particular, Taussky [1] and Eckert [2] studied the following operation

$$(x_1, y_1, z_1) \cdot (x_2, y_2, z_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + y_1 x_2, z_1 z_2)$$

which defines a structure of free abelian group over primitive Pythagorean triples. In [5], this result has been generalized from $\mathbb{Z}$ to any ring of integers of an algebraic number field. In [3] and [4], the following operation has been studied

$$(x_1, y_1, z_1) \cdot (x_2, y_2, z_2) = (x_1 x_2, y_1 z_2 + y_2 z_1, y_1 y_2 + z_1 z_2),$$

determining a commutative monoid (i.e., a commutative semigroup with identity) over $\mathcal{P}$.

Here, we study new operations on Pythagorean triples starting from an injection between triples and matrices. These operations provide new commutative monoid structures over $\mathcal{P}$. Let ν be an injective function

$$\nu : \mathbb{Z}^3 \to M_3,$$

where M_3 is the set of 3×3 matrices whose entries belong to $\mathbb{Z}$. Clearly, ν can be used to induce products over $\mathbb{Z}^3$. Let us denote with ”.” the usual matrix product. One natural way to induce a product over $\mathbb{Z}^3$ is given by

$$\mathbf{a} \bullet_1 \mathbf{b} = \nu^{-1}(\nu(\mathbf{a}).\nu(\mathbf{b})), \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{Z}^3,$$

whenever ν is invertible. A second natural way is given by

$$\mathbf{a} \bullet_2 \mathbf{b} = \nu(\mathbf{a}).\mathbf{b}, \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{Z}^3.$$

Let us consider the following definition.

Definition 2.1. *We say that injection ν is* natural *when*
1. *$\nu(\nu(\boldsymbol{a}).\boldsymbol{b}) = \nu(\boldsymbol{a}).\nu(\boldsymbol{b})$, $\forall \boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^3$*
2. *$\nu(\boldsymbol{a}).\boldsymbol{b} = \nu(\boldsymbol{b}).\boldsymbol{a}$, $\forall \boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^3$*
3. *$\nu(1, 0, 1) = I_3$ (identity matrix)*

Remark 2.2. *We consider an element $\boldsymbol{a} \in \mathbb{Z}^3$ like a column vector or a row vector in order that products between $\boldsymbol{a}$ and matrices are consistent.*

In the following, we are interested in natural ν. Thus, we will consider the induced product $\bullet = \bullet_1 = \bullet_2$, i.e.,

$$\mathbf{a} \bullet \mathbf{b} = \nu(\mathbf{a}).\mathbf{b} = \nu^{-1}(\nu(\mathbf{a}).\nu(\mathbf{b})), \quad \forall \mathbf{a}, \mathbf{b} \in \mathbb{Z}^3.$$

If ν is natural, then $(\mathbb{Z}^3, \bullet)$ is a commutative monoid, whose identity is $(1, 0, 1)$.

We also want to determine when the product $\bullet$ preserves Pythagorean triples, i.e.,

$$\forall \mathbf{a}, \mathbf{b} \in \mathcal{P}, \quad \nu(\mathbf{a}).\mathbf{b} \in \mathcal{P}.$$

This study is clearly related to research Pythagorean triple preserving matrices.

Definition 2.3. *A matrix A is called a* Pythagorean triple preserving matrix *(PTPM) if given a Pythagorean triple $\boldsymbol{a}$, then A.$\boldsymbol{a}$ is still a Pythagorean triple.*

In [6] and [7], the authors characterized PTPMs. Precisely, they are of the form

$$\begin{pmatrix} \frac{1}{2}(r^2 - t^2 - s^2 + u^2) & rs - tu & \frac{1}{2}(r^2 - t^2 + s^2 - u^2) \\ rt - su & ru + st & rt + su \\ \frac{1}{2}(r^2 + t^2 - s^2 - u^2) & rs + tu & \frac{1}{2}(r^2 + t^2 + s^2 + u^2) \end{pmatrix}$$

for some values of r, s, t, u. Further results can be found in [8]. Moreover, Tikoo [9] studied special cases of PTPMs provided by matrices

$$B_1 = \begin{pmatrix} x & 0 & 0 \\ 0 & z & y \\ 0 & y & z \end{pmatrix} \quad B_2 = \begin{pmatrix} y & 0 & 0 \\ 0 & z & x \\ 0 & x & z \end{pmatrix} \quad B_3 = \begin{pmatrix} z & 0 & x \\ 0 & y & 0 \\ x & 0 & z \end{pmatrix}$$

$$B_4 = \begin{pmatrix} z & 0 & y \\ 0 & x & 0 \\ y & 0 & z \end{pmatrix} \quad B_5 = \begin{pmatrix} -x & y & 0 \\ y & x & 0 \\ 0 & 0 & z \end{pmatrix}$$

for (x, y, z) a given Pythagorean triple. All these matrices induce products that preserve Pythagorean triples. In other words, we can consider, e.g., the injection

$$\nu_{B_1} : \mathbb{Z}^3 \to M_3, \quad \nu_{B_1}(x, y, z) = B_1.$$

Thus, the induced product $\bullet_{B_1}$ preserves Pythagorean triples, i.e.,

$$\forall \mathbf{a}, \mathbf{b} \in \mathcal{P}, \quad \mathbf{a} \bullet_{B_1} \mathbf{b} \in \mathcal{P}.$$

Moreover, with a bit of calculation, it is possible to check that $(\mathcal{P}, \bullet_{B_1})$ is a commutative monoid or equivalently ν_{B_1} is natural. Similarly, we can consider the injection ν_{B_2} and the product $\bullet_{B_2}$. Clearly, $\bullet_{B_2}$ preserves Pythagorean triples. However, $\bullet_{B_2}$ is not commutative nor associative and there is not the identity. In this case $(\mathcal{P}, \bullet_{B_2})$ is not a commutative monoid or equivalently ν_{B_2} is not natural.

Thus, it is natural to ask when PTPMs determine commutative and associative products with identity. In the following we answer to this question finding a characterization for these matrices.

3 Matrices yielding commutative monoids of triples

In this section we determine all matrices that yield natural injections ν. In other words, we determine all matrices such that $(\mathbb{Z}^3, \bullet)$ is a commutative monoid whose identity is (1,0,1). Using previous notation, we have that $\nu(x, y, z) \in M_3$ has entries depending on triple (x, y, z).

We consider generic 3×3 matrices whose entries are functions of (x, y, z):

$$\nu(x, y, z) = \begin{pmatrix} a(x, y, z) & b(x, y, z) & c(x, y, z) \\ d(x, y, z) & e(x, y, z) & f(x, y, z) \\ g(x, y, z) & h(x, y, z) & i(x, y, z) \end{pmatrix}.$$

Triple $(1, 0, 1)$ is the identity with respect to $\bullet$ if and only if

$$(x, y, z) \bullet (1, 0, 1) = (1, 0, 1) \bullet (x, y, z) = (x, y, z), \quad \forall (x, y, z) \in \mathbb{Z}^3$$

i.e., if and only if

$$\nu(x, y, z).(1, 0, 1) = \nu(1, 0, 1).(x, y, z) = (x, y, z).$$

Direct calculations show that these equalities are satisfied if and only if

$$\nu(x, y, z) = \begin{pmatrix} a(x, y, z) & b(x, y, z) & x - a(x, y, z) \\ d(x, y, z) & e(x, y, z) & y - d(x, y, z) \\ g(x, y, z) & h(x, y, z) & z - g(x, y, z) \end{pmatrix}.$$

Moreover, $\bullet$ is commutative if and only if

$$(x, y, z) \bullet (r, s, t) = (r, s, t) \bullet (x, y, z), \quad \forall (x, y, z), (r, s, t) \in \mathbb{Z}^3.$$

From this condition, we obtain the following relations:

$$
\begin{aligned}
a(x, y, z)r + b(x, y, z)s + (x - a(x, y, z))t &= a(r, s, t)x + b(r, s, t)y + (r - a(r, s, t))z \\
d(x, y, z)r + e(x, y, z)s + (y - d(x, y, z))t &= d(r, s, t)x + e(r, s, t)y + (s - d(r, s, t))z \\
g(x, y, z)r + h(x, y, z)s + (z - g(x, y, z))t &= g(r, s, t)x + h(r, s, t)y + (t - g(r, s, t))z
\end{aligned}
$$

In particular, if $(r, s, t) = (1, 0, 0)$ we obtain

$$
\begin{aligned}
a(x, y, z) &= a(1, 0, 0)x + b(1, 0, 0)y + (1 - a(1, 0, 0))z \\
d(x, y, z) &= d(1, 0, 0)x + e(1, 0, 0)y - d(1, 0, 0)z \\
g(x, y, z) &= g(1, 0, 0)x + h(1, 0, 0)y - g(1, 0, 0)z
\end{aligned}
\tag{1}
$$

On the other hand, when $(r, s, t) = (0, 1, 0)$ we have

$$
\begin{aligned}
b(x, y, z) &= a(0, 1, 0)x + b(0, 1, 0)y - a(0, 1, 0)z \\
e(x, y, z) &= d(0, 1, 0)x + e(0, 1, 0)y + (1 - d(0, 1, 0))z \\
h(x, y, z) &= g(0, 1, 0)x + h(0, 1, 0)y - g(0, 1, 0)z
\end{aligned}
\tag{2}
$$

From (1), when $(x, y, z) = (0, 1, 0)$, we get

$$
\begin{aligned}
a(0, 1, 0) &= b(1, 0, 0) \\
d(0, 1, 0) &= e(1, 0, 0) \\
g(0, 1, 0) &= h(1, 0, 0)
\end{aligned}
$$

These relations allow to rewrite equations (1) and (2) introducing the parameters

$$
\begin{aligned}
\alpha &= a(1, 0, 0) \; \beta = a(0, 1, 0) = b(1, 0, 0) \; \phi = b(0, 1, 0) \\
\delta &= d(1, 0, 0) \; \gamma = d(0, 1, 0) = e(1, 0, 0) \; \rho = e(0, 1, 0) \\
\sigma &= g(1, 0, 0) \; \theta = g(0, 1, 0) = h(1, 0, 0) \; \lambda = h(0, 1, 0)
\end{aligned}
$$

and to finally find

$$
\begin{pmatrix}
\alpha(x - z) + \beta y + z & \beta(x - z) + \phi y & (1 - \alpha)(x - z) - \beta y \\
\delta(x - z) + \gamma y & \gamma(x - z) + \rho y + z & -\delta(x - z) + (1 - \gamma)y \\
\sigma(x - z) + \theta y & \theta(x - z) + \lambda y & -\sigma(x - z) - \theta y + z
\end{pmatrix}
$$

Elements of $\nu(x, y, z)$ are all linear functions of (x, y, z) depending on the introduced parameters. This fact is very useful in order to verify also condition 1 in Definition 2.1. Indeed, we may only consider such a condition for triples $(1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$. A (not so) little bit of calculation shows that parameters must satisfy the following system

$$
\begin{cases}
\alpha\gamma + (\rho + \theta - \beta)\delta + (1 - \gamma)\sigma = \gamma^2 \\
-(\phi - \lambda)\alpha + \phi\gamma - \lambda = \beta(\rho + \theta - \beta) \\
-\sigma(\phi - \lambda) + \lambda\gamma = \theta(\rho + \theta - \beta) \\
\alpha\theta + \delta\lambda - \beta\sigma = \theta\gamma \\
\delta(\phi - \lambda) = \beta\gamma - \theta\gamma + \theta
\end{cases}
$$

We consider two cases: $\phi = \lambda$ and $\phi \neq \lambda$. When $\phi = \lambda$, we have

$$
\begin{cases}
\alpha\gamma + (\rho + \theta - \beta)\delta + (1 - \gamma)\sigma = \gamma^2 \\
\phi\gamma - \lambda = \beta(\rho + \theta - \beta) \\
\phi\gamma = \theta(\rho + \theta - \beta) \\
\alpha\theta + \delta\phi - \beta\sigma = \theta\gamma \\
\beta\gamma = \theta(\gamma - 1)
\end{cases}
$$

In this case, when $\gamma \neq 0$ we find the solution $\alpha = \frac{\gamma^3 + \gamma^2\sigma - \gamma\sigma - \delta(\rho\gamma + \theta)}{\gamma^2}$, $\beta = \frac{\theta(\gamma - 1)}{\gamma}$, $\phi = \frac{\theta(\rho\gamma + \theta)}{\gamma^2}$, corresponding to matrices

$$
\mathcal{A} = \begin{bmatrix}
\frac{\gamma^3 + \sigma\gamma^2 - \sigma\gamma - \delta(\rho\gamma + \theta)}{\gamma^2}(x - z) + \frac{\theta(\gamma - 1)}{\gamma}y + z & \frac{\theta(\gamma - 1)}{\gamma}(x - z) + \frac{\theta(\rho\gamma + \theta)}{\gamma^2}y & \left(\frac{\gamma^2 - \gamma^3 - \sigma\gamma^2 + \sigma\gamma + \delta(\rho\gamma + \theta)}{\gamma^2}\right)(x - z) - \frac{\theta(\gamma - 1)}{\gamma}y \\
\delta(x - z) + \gamma y & \gamma(x - z) + \rho y + z & -\delta(x - z) + (1 - \gamma)y \\
\sigma(x - z) + \theta y & \theta(x - z) + \frac{\theta(\rho\gamma + \theta)}{\gamma^2}y & -\sigma(x - z) - \theta y + z
\end{bmatrix}
$$

On the other hand, if $\gamma = 0$ we find solution $\theta = \gamma = 0$, $\phi = \lambda = -\beta(\rho - \beta)$, $\sigma = -\delta(\rho - \beta)$ and corresponding matrices are

$$
\mathcal{B} = \begin{bmatrix}
\alpha(x - z) + \beta y + z & \beta(x - z) - \beta(\rho - \beta)y & (1 - \alpha)(x - z) - \beta y \\
\delta(x - z) & \rho y + z & -\delta(x - z) + y \\
-\delta(\rho - \beta)(x - z) & -\beta(\rho - \beta)y & \delta(\rho - \beta)(x - z) + z
\end{bmatrix}
$$

When $\phi \neq \lambda$ solution is $\alpha = \frac{\phi\gamma - \lambda - \beta(\rho + \theta - \beta)}{\phi - \lambda}$, $\delta = \frac{\beta\gamma - \theta\gamma + \theta}{\phi - \lambda}$, $\sigma = \frac{\lambda\gamma - \theta(\rho + \theta - \beta)}{\phi - \lambda}$, giving matrices

$$
\mathcal{C} = \begin{bmatrix}
\frac{\phi\gamma - \lambda - \beta(\rho + \theta - \beta)}{\phi - \lambda}(x - z) + \beta y + z & \beta(x - z) + \phi y & \left(\frac{\phi(1 - \gamma) + \beta(\rho + \theta - \beta)}{\phi - \lambda}\right)(x - z) - \beta y \\
\frac{\beta\gamma - \theta\gamma + \theta}{\phi - \lambda}(x - z) + \gamma y & \gamma(x - z) + \rho y + z & -\frac{\beta\gamma - \theta\gamma + \theta}{\phi - \lambda}(x - z) + (1 - \gamma)y \\
\frac{\lambda\gamma - \theta(\rho + \theta - \beta)}{\phi - \lambda}(x - z) + \theta y & \theta(x - z) + \lambda y & -\frac{\lambda\gamma - \theta(\rho + \theta - \beta)}{\phi - \lambda}(x - z) - \theta y + z
\end{bmatrix}
$$

4 Matrices yielding commutative monoids of Pythagorean triples

In the previous section, we have found all matrices $\nu(x, y, z)$ such that injection ν is natural and consequently $(\mathbb{Z}^3, \bullet)$ is a commutative monoid. Now we want to show that a particular subset of PTPMs lies in one of families $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$.

Let us consider the set $\mathcal{P} = \{(x, y, z) \in \mathbb{Z}^3 : x^2 + y^2 = z^2\}$ and matrices $\nu(x, y, z)$, where $(x, y, z) \in \mathcal{P}$. We recall that generic form of $\nu(x, y, z)$, with $(x, y, z) \in \mathcal{P}$, belonging to one of families $\mathcal{A}, \mathcal{B}, \mathcal{C}$, is

$$
\nu(x, y, z) = \begin{pmatrix}
A_1(x - z) + B_1 y + z & A_2(x - z) + B_2 y & A_3(x - z) + B_3 y \\
A_4(x - z) + B_4 y & A_5(x - z) + B_5 y + z & A_6(x - z) + B_6 y \\
A_7(x - z) + B_7 y & A_8(x - z) + B_8 y & A_9(x - z) + B_9 y + z
\end{pmatrix}. \tag{3}
$$

Lemma 4.1. *Necessary conditions for (3) to be a PTPM are*

$$
B_1 = B_5 = B_9, \quad B_7 = B_3, \quad B_8 = B_6, \quad B_4 = -B_2. \tag{4}
$$

Proof. Using the well–known parametrization $x = m^2 - n^2$, $y = 2mn$ and $z = m^2 + n^2$, matrix (3) becomes

$$
\begin{pmatrix}
-2A_1 n^2 + 2B_1 mn + m^2 + n^2 & -2A_2 n^2 + 2B_2 mn & -2A_3 n^2 + 2B_3 mn \\
-2A_4 n^2 + 2B_4 mn & -2A_5 n^2 + 2B_5 mn + m^2 + n^2 & -2A_6 n^2 + 2B_6 mn \\
-2A_7 n^2 + 2B_7 mn & -2A_8 n^2 + 2B_8 mn & -2A_9 n^2 + 2B_9 mn + m^2 + n^2
\end{pmatrix}.
$$

We find, with a little bit of calculation, that condition

$$
\nu(m^2 - n^2, 2mn, m^2 + n^2) . (u^2 - v^2, 2uv, u^2 + v^2) \in \mathcal{P}
$$

is valid for all Pythagorean triples $(m^2 - n^2, 2mn, m^2 + n^2)$ and $(u^2 - v^2, 2uv, u^2 + v^2)$ if the following equality holds

$$
\begin{aligned}
&[M_1^2 + M_2^2 - M_3^2 - M_1(u^2 - v^2) - 2M_2 uv + M_3(u^2 + v^2)]n^4 + \\
&+[N_1(u^2 - v^2) + 2N_2 uv - N_3(u^2 + v^2) - 2M_1 N_1 - 2M_2 N_2 + 2M_3 N_3]n^3 m + \\
&+[N_1^2 + N_2^2 - N_3^2 - M_1(u^2 - v^2) - 2M_2 uv + M_3(u^2 + v^2)]m^2 n^2 + \\
&[N_1(u^2 - v^2) + 2N_2 uv - N_3(u^2 + v^2)]nm^3 = 0
\end{aligned} \tag{5}
$$

where, for $j = 0, 1, 2$, we have

$$
\begin{cases}
M_{j+1} = A_{3j+1}(u^2 - v^2) + 2A_{3j+2}uv + A_{3j+3}(u^2 + v^2) \\
N_{j+1} = B_{3j+1}(u^2 - v^2) + 2B_{3j+2}uv + B_{3j+3}(u^2 + v^2)
\end{cases}. \tag{6}
$$

Equality (5) is independent by the choice of involved triples. Thus, all coefficients within square brackets must be equal to 0. In particular, if we consider the equality

$$N_1(u^2 - v^2) + 2N_2 uv - N_3(u^2 + v^2) = 0 \tag{7}$$

and we substitute the second relations of (6) into (7) we find

$$(B_1 + B_3 - B_7 - B_9)u^4 + 2(B_2 + B_4 + 2B_6 - 2B_8)u^3 v - 2(B_1 - 2B_5 + B_9)u^2 v^2 +$$
$$-2(B_2 + B_4 - B_6 + B_8)uv^3 + (B_1 - B_3 + B_7 - B_9)v^4 = 0$$

Since this equality must hold for all u and v, coefficients within round brackets must be 0, leading to the system of equations

$$\begin{cases} B_1 + B_3 - B_7 - B_9 = 0 \\ B_2 + B_4 + 2B_6 - 2B_8 = 0 \\ B_1 - 2B_5 + B_9 = 0 \\ B_2 + B_4 - B_6 + B_8 = 0 \\ B_1 - B_3 + B_7 - B_9 = 0. \end{cases}$$

which easily gives necessary conditions (4). □

Now, using previous lemma, we prove that PTPMs belong to family $\mathcal{C}$.

Theorem 4.2. *The PTPMs* $v(x, y, z) = M_{\beta,\gamma}(x, y, z)$, *with* $(x, y, z) \in \mathcal{P}$, *are subset of the family* $\mathcal{C}$ *and they have the following form*

$$\begin{pmatrix} (\gamma^2 - \gamma + 1 - \beta^2)(x - z) + \beta y + z & \beta(x - z) - \gamma y & (\beta^2 - \gamma^2 + \gamma)(x - z) - \beta y \\ -\beta(2\gamma - 1)(x - z) + \gamma y & \gamma(x - z) + \beta y + z & \beta(2\gamma - 1)(x - z) + (1 - \gamma)y \\ (\beta^2 + \gamma^2 - \gamma)(x - z) - \beta y & -\beta(x - z) + (1 - \gamma)y & -(\beta^2 + \gamma^2 - \gamma)(x - z) + \beta y + z \end{pmatrix} \tag{8}$$

Proof. First we show that conditions (4) are satisfied only by a subset of $\mathcal{C}$. Let us consider a matrix of the form $\mathcal{A}$. Conditions (4) correspond to relations

$$\frac{\theta(\gamma - 1)}{\gamma} = \rho = -\theta, \quad \theta = -\frac{\theta(\gamma - 1)}{\gamma^2}, \quad \frac{\theta(\rho\gamma + \theta)}{\gamma^2} = 1 - \gamma, \quad \gamma = \frac{\theta(\rho\gamma + \theta)}{\gamma^2},$$

which are clearly inconsistent.

If we examine a matrix belonging to family $\mathcal{B}$, we have that conditions (4) lead to equalities

$$\beta = \rho = 0, \quad \beta = 0, \quad -\beta(\rho - \beta) = 1, \quad -\beta(\rho - \beta) = 0,$$

and also in this case they are clearly inconsistent.

Finally, for matrices belonging to family $\mathcal{C}$, conditions (4) are equivalent to

$$\beta = \rho = -\theta, \quad \theta = -\beta, \quad \lambda = 1 - \gamma, \quad \phi = -\gamma.$$

They are compatible, providing matrices of the form (8). We can prove that these matrices are PTPMs considering two triples generated by m, n and u, v.

We have

$$(m^2 - n^2, 2mn, m^2 + n^2) \bullet (u^2 - v^2, 2uv, u^2 + v^2) = (A, B, C)$$

where

$$A = (mu + (1 - 2\gamma)nv)^2 - (mv + n(u + 2\beta v))^2,$$

$$B = 2(mu + (1 - 2\gamma)nv)(mv + n(u + 2\beta v)),$$

$$C = (mu + (1 - 2\gamma)nv)^2 + (mv + n(u + 2\beta v))^2,$$

which is clearly a Pythagorean triple.

On the other hand

$$(u^2 - v^2, 2uv, u^2 + v^2).v(m^2 - n^2, 2mn, m^2 + n^2) = (A', B', C')$$

where

$$A' = (mu + nv)^2 - (mv + n(u - 2\gamma u + 2\beta v))^2,$$
$$B' = 2(mu + nv)(mv + n(u - 2\gamma u + 2\beta v)),$$
$$C' = (mu + nv)^2 + (mv + n(u - 2\gamma u + 2\beta v))^2,$$

which is clearly another Pythagorean triple.   □

The previous theorem characterizes matrices $M_{\beta,\gamma}$, depending on two parameters β and γ, such that

$$\nu : \mathcal{P} \to M_3, \quad \nu(x, y, z) = M_{\beta,\gamma}(x, y, z)$$

is natural, i.e., said $\bullet_{\beta,\gamma}$ the induced product, $(\mathcal{P}, \bullet_{\beta,\gamma})$ is a commutative monoid.

5 Products over conics and groups of Pythagorean triples

Since we have the classical parametrization for the Pythagorean triples $(x, y, z) \in \mathcal{P}$ given by

$$\phi : \mathbb{Z}^2 \to \mathcal{P}, \quad \phi(u, v) = (u^2 - v^2, 2uv, u^2 + v^2),$$

matrices $M_{\beta,\gamma}(x, y, z)$ can be rewritten as

$$M_{\beta,\gamma}(u, v) = \begin{pmatrix} u^2 + 2\beta uv + (2\beta^2 - 2\gamma^2 + 2\gamma - 1)v^2 & -2v(\gamma u + \beta v) & 2(-\beta^2 v - \beta u + \gamma(\gamma - 1))v \\ -2(\beta v - \gamma(u + 2\beta v))v & u^2 + 2\beta uv + (-2\gamma + 1)v^2 & 2(-\gamma u + u + \beta v - 2\beta\gamma v)v \\ -2(\beta^2 v + \beta u + \gamma(\gamma - 1)v)v & 2(-\gamma u + u + \beta v)v & u^2 + 2\beta uv + (2\beta^2 + 2\gamma^2 - 2\gamma + 1)v^2 \end{pmatrix}.$$

Now, we define a product between points of $\mathbb{R}^2$ such that it is well–defined with respect to multiplication of matrices $M_{\beta,\gamma}(u, v)$.

Definition 5.1. *For any $(u, v), (s, t) \in \mathbb{R}^2$, we define*

$$(u, v) *_{\beta,\gamma} (s, t) = (su + tv(1 - 2\gamma), tu + sv + 2\beta tv). \tag{9}$$

The reader can easily prove that

$$M_{\beta,\gamma}(u, v).M_{\beta,\gamma}(s, t) = M_{\beta,\gamma}((u, v) *_{\beta,\gamma} (s, t)).$$

The determinant of $M_{\beta,\gamma}(u, v)$ is surprisingly $(u^2 + 2\beta uv - (1 - 2\gamma)v^2)^3$. Thus, function

$$\delta(M_{\beta,\gamma}(u, v)) = u^2 + 2\beta uv - (1 - 2\gamma)v^2$$

is multiplicative, i.e.,

$$\delta(M_{\beta,\gamma}(u, v).M_{\beta,\gamma}(u', v')) = \delta(M_{\beta,\gamma}(u, v)) \cdot \delta(M_{\beta,\gamma}(u', v')),$$

since it is the cubic root of the determinant.

In this way, study of commutative monoids of Pythagorean triples offers an unexpected connection with conics. Indeed, it is now natural to consider conics

$$\alpha_{\beta,\gamma}(z) = \{(x, y) \in \mathbb{R}^2 : x^2 + 2\beta xy - (1 - 2\gamma)y^2 = z\}.$$

From previous notation and remarks, it follows that

$$(u, v) *_{\beta,\gamma} (s, t) \in \alpha_{\beta,\gamma}(wz), \quad \forall (u, v) \in \alpha_{\beta,\gamma}(w), (s, t) \in \alpha_{\beta,\gamma}(z). \tag{10}$$

Proposition 5.2. *Let $(u, v)^{n *_{\beta,\gamma}}$ be the n–th power of (u, v) with respect to $*_{\beta,\gamma}$, then*

$$(M_{\beta,\gamma}(u, v))^n = M_{\beta,\gamma}((u, v)^{n *_{\beta,\gamma}}).$$

Consequently, power of matrices of the form (8) are still of this form.

Proof. The proof directly follows from previous observations. □

Conic $\alpha_{\beta,\gamma}(1)$ is especially interesting, due to equation (10). In [10], the authors studied the conic

$$x^2 + hxy - dy^2 = 1, \tag{11}$$

which is a group with the operation

$$(u, v) \cdot (s, t) = (tu + svd, tu + sv + tvh). \tag{12}$$

The identity is the point $(1, 0)$ and the inverse of a generic point (x, y) is $(x + hy, -y)$. This conic and this product clearly coincide with $\alpha_{\beta,\gamma}(1)$ and $*_{\beta,\gamma}$ for $h = 2\beta$ and $d = 1 - 2\gamma$. Thus, $(\alpha_{\beta,\gamma}(1), *_{\beta,\gamma})$ is a group.

Theorem 5.3. *If $\beta^2 - 2\gamma + 1$ is a positive square–free integer, then we have $(u_1 - \beta v_1, v_1) \in \alpha_{\beta,\gamma}(1)$, where (u_1, v_1) is the minimal solution of the Pell equation*

$$x^2 - (\beta^2 - 2\gamma + 1)y^2 = 1$$

Proof. The proof directly follows from the equality

$$x^2 + 2\beta xy - (1 - 2\gamma)y^2 = (x + \beta y)^2 - (\beta^2 - 2\gamma + 1)y^2. \qquad □$$

As a consequence, the set

$$N_{\beta,\gamma} = \{(u, v) \in \alpha_{\beta,\gamma}(1) : u, v \in \mathbb{Z}\}$$

includes infinite points and $(N_{\beta,\gamma}, *_{\beta,\gamma})$ is a group.

Let us consider $\bar{\phi} = \phi|_{\alpha_{\beta,\gamma}(1)}$, then $\bar{\phi}$ is a morphism, i.e.,

$$\bar{\phi}((u, v) *_{\beta,\gamma} (s, t)) = \bar{\phi}(u, v) \bullet_{\beta,\gamma} \bar{\phi}(s, t), \quad \forall (u, v), (s, t) \in \alpha_{\beta,\gamma}(1).$$

Moreover, $\ker \bar{\phi} = \{(\pm 1, 0)\}$ and

$$(Im(\bar{\phi}), \bullet_{\beta,\gamma}) \cong (N_{\beta,\gamma})/\{(\pm 1, 0)\}.$$

Thus we have the following theorem.

Theorem 5.4. *$(Im(\bar{\phi}), \bullet_{\beta,\gamma})$ is a group of Pythagorean triples and the inverse of the Pythagorean triple $\bar{\phi}(u, v)$ is*

$$\bar{\phi}(u + 2\beta v, -v) = (-v^2 + (u + 2\beta v)^2, -2v(u + 2\beta v), v^2(u + 2\beta v)^2).$$

Example. *Let us consider the Pythagorean triple $(3, 4, 5)$. Since we have $\phi(2, 1) = (3, 4, 5)$, we are interested in conics $\alpha_{\beta,\gamma}(1)$ containing the point $(2, 1)$. It is easy to see that $(2, 1) \in \alpha_{\beta,-2\beta-1}(1)$, $\forall \beta \in \mathbb{R}$. However, we only consider $\beta \in \mathbb{Z}$. By Theorem (5.4), inverse of $(2, 1)$ is $(2(\beta + 1), -1)$ and inverse of $(3, 4, 5)$ is*

$$\bar{\phi}(2(\beta + 1), -1) = (4\beta^2 + 8\beta + 3, -4(\beta + 1), 4(\beta + 1)^2 + 1).$$

Let us set, e.g., $\beta = 1$, the conic $\alpha_{1,-3}(1)$ is

$$x^2 + 2xy - 7y^2 = 1.$$

The inverse of $(2, 1)$ is $(4, -1)$ and inverse of $(3, 4, 5)$, with respect to $\bullet_{1,-3}$, is $(15, -8, 17)$. Indeed,

$$(3, 4, 5) \bullet_{1,-3} (15, -8, 17) = M_{1,-3}(3, 4, 5).(15, -8, 17) = \begin{pmatrix} -15 & 10 & 18 \\ -26 & 15 & 30 \\ -30 & 18 & 35 \end{pmatrix} \begin{pmatrix} 15 \\ -8 \\ 17 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Moreover, we can evaluate powers of Pythagorean triples:

$$(3,4,5)^{2\bullet_{1,-3}} = \begin{pmatrix} -15 & 10 & 18 \\ -26 & 15 & 30 \\ -30 & 18 & 35 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 85 \\ 132 \\ 157 \end{pmatrix}.$$

The Pythagorean triple $(85, 132, 157)$ *corresponds to the point* $(2, 1)^{2*_{1,-3}} = (11, 6) \in \alpha_{1,-3}(1)$. *Thus, the inverse of* $(11, 6)$ *is* $(23, -6)$ *and the inverse of* $(85, 132, 157)$ *is* $\phi(23, -6) = (493, -276, 565)$.

6 Conclusion

The paper provides new structures of commutative monoids and commutative groups over sets of Pythagorean triples, starting from *natural* injections between triples and 3×3 matrices. Moreover, this study has connection with groups over conics.

As future developments, we find interesting to study operations $*_{\beta,\gamma}$ and $\bullet_{\beta,\gamma}$ over finite fields $\mathbb{Z}_p$ for p prime. Moreover, this study offers the possibility to use Pythagorean triples in the approximation of quadratic irrationalities. Indeed, in [10], conic (11) and product (12) have been profitably used in Diophantine approximation for quadratic irrationalities. Thus, the above connections with Pythagorean triples show that they can be used in this context.

References

[1]   Taussky O., Sum of squares, American Mathematical Monthly, 1970, 77, 805-830

[2]   Eckert E., The group of primitive Pythagorean triangles, Mathematics Magazine, 1984, 54, 22-27

[3]   Beauregard R. A., Suryanarayan E. R., Pythagorean triples: the hyperbolic view, The College Mathematics Journal, 1996, 27(3), 170-181

[4]   Somboonkulavudi C., Harnchoowong A., Pythagorean triples over Gaussian integers, Int. J. of Algebra, 2012, 6(2), 55-64

[5]   Zanardo P., Zannier U., The group of Pythagorean triples in number fields, Annali di Matematica Pura ed Applicata, 1991, CLIX, 81-88

[6]   Palmer L., Ahuja M., Tikoo M., Finding Pythagorean triple preserving matrices, Missouri Journal of Mathematical Sciences, 1998, 10, 99-105

[7]   Palmer L., Ahuja M., Tikoo M., Constructing Pythagorean triple preserving matrices, Missouri Journal of Mathematical Sciences, 1998, 10, 159-168

[8]   Crasmareanu M., A new method to obtain Pythagorean triple preserving matrices, Missouri Journal of Mathematical Sciences, 2002, 14(3), 149-158

[9]   Tikoo M., A note on Pythagorean triple preserving matrices, Int. J. Math. Educ. Sci. Technol., 2002, 33(6), 893-894

[10]   Barbero S., Cerruti U., Murru N. , Generalized Rédei rational functions and rational approximations over conics, Int. J. of Pure and Applied Math., 2010, 64(2), 305-317