NOTE ON A PYTHAGOREAN RING

Aleksander Grytczuk

Abstract. In this note we give a construction of a Pythagorean ring

$$P_n = \{ <x, y, z> \in \mathbb{Z}^3 \ : \ x^2 + y^2 = z^2, \ z - y = n \},$$

where n is a fixed integer.

1. Introduction. B. Dawson in [1] gave a construction of a Pythagorean ring

$$P = \{ <x, y, z> \in \mathbb{Z}^3 \ : \ x^2 + y^2 = z^2 \}.$$

He defined the operations "$\oplus$" and "$\circ$" by an isomorphism $\Phi: P \to \mathbb{Z} \times \mathbb{Z}$ and utilized the elements of P_n. The fact that P is partitioned into sets P_n leaves an interesting avenue for further exploration. Dawson remarked that it may be possible to define other operations in a natural way under which P is essentially a different ring and this is an open problem. In this connection we prove the following theorem.

Theorem. Let

$$P_n = \{ <x, y, z> \in \mathbb{Z}^3 \ : \ x^2 + y^2 = z^2, \ z - y = n \}.$$

Then, the integers x, y, z are given by the formulas

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

where x and $n \neq 0$ are the same parity. Moreover, let

$$\alpha = < a, \frac{a^2 - n^2}{2n}, \frac{a^2 + n^2}{2n} >, \ \beta = < b, \frac{b^2 - n^2}{2n}, \frac{b^2 + n^2}{2n} >,$$

and

$$\alpha \oplus \beta = < a + b - n, \frac{(a + b - n)^2 - n^2}{2n}, \frac{(a + b - n)^2 + n^2}{2n} > \tag{2}$$

(3)

$$\alpha\circ\beta =< (a-n)(b-n)+n, \frac{((a-n)(b-n)+n)^2-n^2}{2n}, \frac{((a-n)(b-n)+n)^2+n^2}{2n} >$$

and for $n=0$,

$$< 0,a,a > \oplus < 0,b,b > = < 0,a+b,a+b > \tag{4}$$

and

$$< 0,a,a > \circ < 0,b,b > = < 0,ab,ab > . \tag{5}$$

Then the set $< P_n, \oplus, \circ >$ is a commutative ring for any fixed integer n.

Proof. First we prove by another way than in [1] that if $< x,y,z > \in P_n$, where $n \neq 0$ is a fixed integer then the integer elements x, y, z are given by (1). It is well–known that all solutions of the Pythagorean equation $x^2+y^2=z^2$ are given by the formulas

$$x=(M^2-N^2)R, \quad y=2MNR, \quad z=(M^2+N^2)R \tag{6}$$

or

$$x=2MNR, \quad y=(M^2-N^2)R, \quad z=(M^2+N^2)R \tag{7}$$

where M, N, R are integers such that $(M,N)=1$. Suppose that (6) is satisfied. Since $< x,y,z > \in P_n$, $n \neq 0$, then

$$n=z-y=R(M-N)^2. \tag{8}$$

By (6) and (8), it follows that

$$x^2-n^2=R^2(M-N)^2((M+N)^2-(M-N)^2)=4nMNR=2ny. \tag{9}$$

From (9), we have

$$y=\frac{x^2-n^2}{2n}. \tag{10}$$

In a similar way, we obtain

$$x^2 + n^2 = 2nR(M^2 + N^2) = 2nz \tag{11}$$

and by (11) it follows that

$$z = \frac{x^2 + n^2}{2n}. \tag{12}$$

On the other hand, it is easy to see that by (9) and (11), it follows that x, n are of the same parity and that y and z are integers. We also note that if x, y, z are given by (1), then

$$x^2 + \left(\frac{x^2 - n^2}{2n}\right)^2 = \left(\frac{x^2 + n^2}{2n}\right)^2.$$

Now, we can assume that (7) is satisfied. Then we obtain

$$n = z - y = 2N^2R. \tag{13}$$

From (13) and (7), we get

$$x^2 - n^2 = 2nR(M^2 - N^2) = 2ny \tag{14}$$

and by (14), it follows that

$$y = \frac{x^2 - n^2}{2n}. \tag{15}$$

Similarly, we obtain

$$x^2 + n^2 = 4N^2R^2(M^2 + N^2) = 2nR(M^2 + N^2) = 2nz. \tag{16}$$

From (16), we have

$$z = \frac{x^2 + n^2}{2n}. \tag{17}$$

By (14) and (16), it follows that x, n are the same parity and x, y, z given by (15) and (17) satisfy the Pythagorean equation. Hence, the first part of our theorem is proved.

We also note that if $n = 0$, then $x = 0$ and $y = z$ and therefore the operations (4) and (5) are well–defined. Moreover, the set $< P_0; \oplus >$ is a commutative group with identity $e_0 =< 0, 0, 0 >$. It is easy to see that if α, β, $\gamma \in P_0$ then we have $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ and $\alpha \circ \beta = \beta \circ \alpha$. The distributive law is also satisfied. Moreover, the set P_0 has multiplicative identity $1_0 =< 0, 1, 1 >$. Therefore, the set $< P_0; \oplus, \circ >$ is a commutative ring. It remains to prove that the set P_n, for $n \neq 0$ with the operations (2) and (3) is a commutative ring. First, we prove that the operations (2) and (3) are well–defined. By the assumptions that α, $\beta \in P_n$ we have

$$2n \mid a^2 - n^2, \quad 2n \mid a^2 + n^2, \quad 2n \mid b^2 - n^2, \quad 2n \mid b^2 + n^2. \tag{18}$$

By well–known properties of the divisibility relation and (18), it follows that

$$2n \mid a^2 + b^2, \quad n \mid ab. \tag{19}$$

We prove that the numbers

$$\frac{(a + b - n)^2 - n^2}{2n} \quad \text{and} \quad \frac{(a + b - n)^2 + n^2}{2n}$$

are integer numbers. By (19), it follows that $2n \mid a^2 + b^2 + 2ab = (a + b)^2$. Since $(a + b - n)^2 - n^2 = (a + b)^2 - 2n(a + b)$, then

$$2n \mid (a + b - n)^2 - n^2.$$

In a similar way, we obtain that $2n \mid (a + b - n)^2 + n^2$. On the other hand, it is easy to see that

$$(a + b - n)^2 + \left(\frac{(a + b - n)^2 - n^2}{2n}\right)^2 = \left(\frac{(a + b - n)^2 + n^2}{2n}\right)^2$$

and
$$\frac{(a+b-n)^2+n^2}{2n}-\frac{(a+b-n)^2-n^2}{2n}=\frac{2n^2}{2n}=n.$$
So denote that $\alpha\oplus\beta\in P_n$. In a similar way, we prove that $\alpha\circ\beta\in P_n$. Indeed, since

$$((a-n)(b-n)+n)^2-n^2=(a-n)^2(b-n)^2+2n(a-n)(b-n)$$

and $(a-n)^2=a^2+n^2-2na$, $(b-n)^2=b^2+n^2-2nb$, then by (18), it follows that

$$2n\mid((a-n)(b-n)+n)^2-n^2.$$

Similarly, we obtain that $2n\mid((a-n)(b-n)+n)^2+n^2$. Therefore, the numbers

$$\frac{((a-n)(b-n)+n)^2-n^2}{2n},\quad\frac{((a-n)(b-n)+n)^2+n^2}{2n}$$

are integers and together with $(a-n)(b-n)+n$, satisfy the Pythagorean equation. For further process of the proof, we note that the second and third coordinates in (2) and (3) are generated by the first coordinate, therefore it suffices to check all the conditions of the ring with respect to the first coordinate. Denote by $[\alpha]_1$ the first coordinate of $\alpha\in P_n$.

Now, we prove that the set $<P_n;\oplus>$ is a commutative group. Let α, β, $\gamma\in P_n$. Then by (1) we obtain

$$\alpha=<a,\frac{a^2-n^2}{2n},\frac{a^2+n^2}{2n}>,$$

$$\beta=<b,\frac{b^2-n^2}{2n},\frac{b^2+n^2}{2n}>,$$

$$\gamma=<c,\frac{c^2-n^2}{2n},\frac{c^2+n^2}{2n}>.$$

Then, by (2) we obtain

(20) $$[(\alpha\oplus\beta)\oplus\gamma]_1=((a+b-n)+c)-n=a+b+c-2n$$

and

$$(21) \qquad [\alpha \oplus (\beta \oplus \gamma)]_1 = a + (b + c - n) - n = a + b + c - 2n.$$

From (20) and (21), we have $(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma)$. Similarly, we obtain

$$[\alpha \oplus \beta]_1 = a + b - n = b + a - n = [\beta \oplus \alpha]_1,$$

so denote that $\alpha \oplus \beta = \beta \oplus \alpha$. On the other hand, we see that $e_{\oplus} =< n, 0, n >$ is the identity element in $< P_n; \oplus >$. We have

$$[\alpha \oplus e_{\oplus}]_1 = (a + n) - n = a = (n + a) - n = [e_{\oplus}\alpha]_1 = [\alpha]_1,$$

and therefore, $\alpha \oplus e_{\oplus} = e_{\oplus} \oplus \alpha = \alpha$.

The inverse element to $\alpha \in P_n$ is the element $\alpha' \in P_n$ given by

$$(22) \qquad \alpha' =< -a + 2n, \frac{(-a + 2n)^2 - n^2}{2n}, \frac{(-a + 2n)^2 + n^2}{2n} > .$$

Indeed by (22), it follows that $[\alpha \oplus \alpha']_1 = a + (-a + 2n) - n = n = [e_{\oplus}]_1$ and

$$[\alpha' \oplus \alpha]_1 = (-a + 2n + a) - n = n = [e_{\oplus}]_1,$$

and consequently $\alpha \oplus \alpha' = \alpha' \oplus \alpha = e_{\oplus}$, and we see that the set $< P_n; \oplus >$ is a commutative group. Further by (3), it follows that $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$. We observe that

$$[(\alpha \circ \beta) \circ \gamma]_1 = ((a - n)(b - n) + n - n)(c - n) + n = (a - n)(b - n)(c - n) + n$$

and

$$[\alpha \circ (\beta \circ \gamma)]_1 = (a - n)((b - n)(c - n) + n - n) + n = (a - n)(b - n)(c - n) + n,$$

hence the associative law for (3) is proved.

Now, we prove the distributive law. By (2) and (3), it follows that

$$(23) \qquad [(\alpha \oplus \beta) \circ \gamma]_1 = (a + b - 2n)(c - n) + n$$

and

$$[(\alpha \circ \gamma) \oplus (\beta \circ \gamma)]_1$$
$$= (a-n)(c-n) + n + (b-n)(c-n) + n - n$$
$$= (c-n)(a+b-2n) + n. \tag{24}$$

and from (23) and (24), we obtain $(\alpha \oplus \beta) \circ \gamma = (\alpha \circ \gamma) \oplus (\beta \circ \gamma)$. On the other hand, we have

$$[\alpha \circ (\beta \oplus \gamma]_1 = (a-n)(b+c-n-n) + n = (a-n)(b+c-2n) + n) \tag{25}$$

and

$$[(\alpha \circ \beta) \oplus (\alpha \circ \gamma)]_1$$
$$= (a-n)(b-n) + n + (a-n)(c-n) + n - n$$
$$= (a-n)(b+c-2n) + n \tag{26}$$

and by (25) and (26), it follows that $\alpha \circ (\beta \oplus \gamma) = (\alpha \circ \beta) \oplus (\alpha \circ \gamma)$. The distributive law is proved.

Finally, we observe that

$$[\alpha \circ \beta]_1 = (a-n)(b-n) + n = (b-n)(a-n) + n = [\beta \circ \alpha]_1$$

and consequently, we obtain $\alpha \circ \beta = \beta \circ \alpha$. Summarizing, we obtain that the set $< P_n; \oplus, \circ >$ with the operations "$\oplus$" and "$\circ$" defined by (2) and (3) is a commutative ring for any fixed integer $n \neq 0$. The proof of the Theorem is complete.

Remark. The rings $< P_n; \oplus, \circ >$; $n \neq 0$ are the rings without multiplicative identity.

Acknowledgement. I would like to thank the referee for his valuable suggestions for the improvement of this paper.

Reference

1. B. Dawson, "A Ring of Pythagorean Triples," *Missouri Journal of Mathematical Sciences*, 6 (1994), 72–77.

Aleksander Grytczuk
Institute of Mathematics
Department of Algebra and Number Theory
T. Kotarbiński Pedagogical University
65–069 Zielona Góra, Poland