ALGEBRAIC STRUCTURES OF SOME SETS OF PYTHAGOREAN TRIPLES II

Marek Wójtowicz

Abstract. A natural bijection from $\mathbb{Z}^2$ onto the set of all Pythagorean triples $\mathcal{P} = \{(a,b,c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2\}$ is given (Theorem 6). Consequently, all algebraic structures of $\mathbb{Z}^2$ are carried in a natural way onto $\mathcal{P}$ (Theorems 7, 8, and 9). This solves the open problem of defining ring operations under which $\mathcal{P}$ is essentially a different ring than the one constructed by B. Dawson (Example, Section 5). This article and the enumeration of its sections and theorems is a continuation of the author's paper [3].

4. Elements of $\mathcal{P}$. Corollary 1 given in Section 2 yields the useful base for a description of all sets $\mathcal{P}_n$, $n \neq 0$ (the case $n = 0$ is obvious), and their elements by giving the apparent form of natural numbers $x_n \geq 2$ with $\psi_n(\mathcal{P}_n) = x_n\mathbb{Z}$ (Proposition 1 below). To this end we define two functions $\mathbb{Z} \to \mathbb{Z}$: quasi–square root $\sqrt[*]{\ }$, and degree of evenness d_{ev}, respectively, as follows.

If $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ is the prime factorization of $|n| \geq 1$, then $\sqrt[*]{n} := p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$, where $\beta_j = [(\alpha_j + 1)/2]$, $j = 1, \ldots, k$, and $[x]$ denotes the integer part of x, and $\sqrt[*]{0} := 0$.

If $n = 2^r n_0$, where $r, n_0 \in \mathbb{Z}$, $r \geq 0$ and $(2, n_0) = 1$, then

$$d_{\text{ev}}(n) = \begin{cases} 1, & \text{for } r \text{ odd,} \\ 2, & \text{for } r \text{ even and } r \geq 0. \end{cases}$$

(A function similar to quasi–square root was used by Dawson in [1].) In the proofs of Propositions 1 and 2 we shall use the following properties of $\sqrt[*]{\ }$ and d_{ev} (recall that if $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ is the prime factorization of $n \in \mathbb{N}$, then the square–free kernel of n is defined as $t(n) = p_1 \cdot \ldots \cdot p_k$, and n is called a square–free number provided that $t(n) = n$).

(1) $0 \leq (\sqrt[*]{n})^2 \leq |n| t(|n|)$.

(2) If $n \mid a^2$, for some $a \in \mathbb{Z}$, then $\sqrt[*]{n} \mid a$.

(3) For every integer n, l, p with $l \geq 0$ and p prime we have $\sqrt[*]{n^2} = |n|$ and $\sqrt[*]{p^{2l+1}} = p^{l+1}$.
(4) $n/\sqrt[*]{n}$ and $(\sqrt[*]{n})^2/n$ are integers for all $n \neq 0$.
(5) We have $\sqrt[*]{nm} \leq \sqrt[*]{n}\sqrt[*]{m}$ for all $n, m \in \mathbb{Z}$, and $\sqrt[*]{nm} = \sqrt[*]{n}\sqrt[*]{m}$ whenever $(n, m) = 1$.
(6) If $n \neq 0$, then $(\sqrt[*]{n})^2/n$ is even if and only if $d_{\mathrm{ev}}(n) = 1$ (and so $(\sqrt[*]{n})^2/n$ is odd if and only if $d_{\mathrm{ev}}(n) = 2$).
(7) For all $s \in \mathbb{Z}$ we have $d_{\mathrm{ev}}(2s+1) = 2$, and $d_{\mathrm{ev}}(4s+2) = 1$.
(8) $\sqrt[*]{n} = |n|$ if and only if $|n|$ is square–free.
(9) If $n, r \in \mathbb{N}$ with r odd and $(n, r) = 1$, then $d_{\mathrm{ev}}(nr) = d_{\mathrm{ev}}(n)$.

Proposition 1. Let ψ_n be the ring isomorphism defined in Theorem 1 and acting from $\mathcal{P}_n$ onto the ring ideal $G_n = x_n\mathbb{Z}$, where x_n is some integer greater than or equal to 2 and $n \neq 0$. Then $x_n = d_{\mathrm{ev}}(n)\sqrt[*]{n}$. In particular, $x_n = x_{2n} = 2\sqrt[*]{n}$ for n odd, and hence, $x_r = x_{2r} = 2r$ for every odd and square–free number $r \in \mathbb{N}$.

Proof. We shall consider the case $n \geq 1$ only; for $n \leq -1$ the proof is similar. We have $\psi_n(\mathcal{P}_n) = \{a_k^{(n)} - n : a_k^{(n)} = kx_n + n$ and $(a_k^{(n)}, b_k^{(n)}, c_k^{(n)}) \in \mathcal{P}_n, k \in \mathbb{Z}\}$, where $b_k^{(n)}$ and $c_k^{(n)}$ are defined in Section 1. Hence,
(10) $a_1^{(n)} = x_n + n$.
Since $(a_1^{(n)})^2 - n^2)/2n = b_1^{(n)} \in \mathbb{N}$, we have $n \mid (a_1^{(n)})^2$; hence, by property (2),
(11) $a_1^{(n)} = t\sqrt[*]{n}$ for some $t \in \mathbb{N}$.
By (4), (10), and (11), we obtain
(12) $x_n = l\sqrt[*]{n}$, where $l = t - n/\sqrt[*]{n} \in \mathbb{N}$,
and so, by (10), $a_1^{(n)} = l\sqrt[*]{n} + n$; putting this value into the formula defining $b_1^{(n)}$ we obtain
$$b_1^{(n)}(l) = ((\sqrt[*]{n})^2/n) \cdot (l/2) + l\sqrt[*]{n}.$$
It follows that l equals the least natural number with $b_1^{(n)}(l) \in \mathbb{N}$. By properties (4) and (6) we have that $l = 1 = d_{\mathrm{ev}}(n)$ provided that $(\sqrt[*]{n})^2/n$ is even, and $l = 2 = d_{\mathrm{ev}}(n)$ for $(\sqrt[*]{n})^2/n$ odd. Finally, by (12), we get $x_n = d_{\mathrm{ev}}(n)\sqrt[*]{n}$. The particular case follows from properties (5), (7) and (8).

The main result of this section reads as follows.

Theorem 6. For every $(a,b,c) \in \mathcal{P}^* := \mathcal{P} \backslash \mathcal{P}_0$ there exists exactly one pair $(k,n) \in \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$ with

$$a = a(k,n) = k \cdot d_{\mathrm{ev}}(n) \cdot \sqrt[*]{n} + n,$$

$$b = b(k,n) = k^2 \cdot \frac{(d_{\mathrm{ev}}(n) \cdot \sqrt[*]{n})^2}{2n} + k \cdot d_{\mathrm{ev}}(n) \cdot \sqrt[*]{n},$$

$$c = c(k,n) = b(k,n) + n.$$

Conversely, for every $(k,n) \in \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$, the triple (a,b,c), where the numbers a, b, c are defined as above, is an element of $\mathcal{P}^*$. Consequently, the function $\alpha \colon \mathbb{Z}^2 \to \mathcal{P}$, given by the rule

$$\alpha(k,n) = \begin{cases} (a(k,n), b(k,n), c(k,n)) & \text{for } n \neq 0 \\ (0,k,k) & \text{for } n = 0 \end{cases}$$

maps both $\mathbb{Z}^2$ onto $\mathcal{P}$ and $\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$ onto $\mathcal{P}^*$ bijectively. The inverse function $\alpha^{-1} \colon \mathcal{P} \to \mathbb{Z}^2$ is of the form: $(a,b,c) \to (k,n)$, where

$$k = k(a,b,c) = \frac{a+b-c}{d_{\mathrm{ev}}(c-b) \cdot \sqrt[*]{c-b}} \text{ and } n = n(a,b,c) = c - b \text{ for } c - b \neq 0,$$

and $k(0,j,j) = j$ and $n(0,j,j) = 0$.

Proof. Since $\mathcal{P} = \cup_{n \in \mathbb{Z}} \mathcal{P}_n$, and since the sets $\mathcal{P}_n$, $n \in \mathbb{Z}$, are pairwise disjoint, by Proposition 1 and the presence of elements of $\mathcal{P}$ given in Section 1, the first part of the theorem is clear. To prove the second part we must show that $b(k,n)$ and $c(k,n)$ are integers for all $k, n \in \mathbb{Z}$. Assume that $n \neq 0$ (the case $n = 0$ is trivial), and observe that the number $d_{\mathrm{ev}}(n) \sqrt[*]{n}$ is even, whence, by property (4), $s(n) := (d_{\mathrm{ev}}(n) \sqrt[*]{n})^2/2n$ is an integer. It follows that for every $k \in \mathbb{Z}$ we have $b(k,n) = k^2 s(n) + k d_{\mathrm{ev}}(n) \sqrt[*]{n} \in \mathbb{Z}$, and hence, $c(k,n) = b(k,n) + n \in \mathbb{Z}$ also. If

$(a,b,c) \in \mathcal{P}^*$, then $c-b=n \neq 0$, hence, by the formula defining $a(k,n)$, we have $k = k(a,b,c) = (a+b-c)/(d_{\mathrm{ev}}(c-b) \cdot \sqrt[*]{c-b})$; hence, we get the form of α^{-1}.

5. The Ring and the Lattice Structures on $\mathcal{P}$. Now we are in position to transfer two ring structures from $\mathbb{Z}^2$ onto $\mathcal{P}$: the "coordinatewise" one, where the additive zero is $(0,0)$ and the multiplicative unit is $(1,1)$, and the complex one, with the additive zero defined as above and the multiplicative unit equals $(1,0)$. The reader should note that the ring operations presented below are different from those constructed by B. Dawson (see Example below), and this solves affirmatively the open problem stated in [1], to define other operations in a natural way (cf. the remark after Lemma in Section 1) under which $\mathcal{P}$ is essentially a different ring than Dawson's. Moreover, the operations given in Theorem 7 do not extend Grytczuk's operations (i.e., when restricted to $\mathcal{P}_n$, $n \neq 0$, these operations take values outside of $\mathcal{P}_n$, in general, and the present author could not find any satisfactory extensions of Grytczuk's operations). Nevertheless, Dawson's multiplicative unit of $\mathcal{P}$ and the unit given in Theorem 7 (i) are identical; we denote this particular triple $(3,4,5)$ as $1_{\mathcal{P}}$.

The two theorems given below are now immediate consequences of Theorem 6 and the Lemma.

Theorem 7. The set $\mathcal{P}$ is a commutative ring with unit under the following pairs of addition and multiplication:

(i) $(a_1,b_1,c_1) \oplus (a_1,b_1,c_1) := \alpha(k_1+k_2, n_1+n_2)$, and $(a_1,b_1,c_1) \odot (a_1,b_1,c_1) := \alpha(k_1k_2, n_1n_2)$, with the additive zero $(0,0,0) = \alpha(0,0)$ and the multiplicative unit $1_{\mathcal{P}} = \alpha(1,1)$;

(ii) $(a_1,b_1,c_1) \oplus (a_1,b_1,c_1) := \alpha(k_1+k_2, n_1+n_2)$, and $(a_1,b_1,c_1) \odot (a_1,b_1,c_1) := \alpha(k_1k_2 - n_1n_2, k_1n_2 + k_2n_1)$, with the additive zero $(0,0,0)$ and the multiplicative unit $(0,1,1) = \alpha(1,0)$, where the numbers $k_j = k(a_j,b_j,c_j)$ and $n_j = n(a_j,b_j,c_j)$, $j=1,2$, and the function α are defined in Theorem 6.

Theorem 8. The set $\mathcal{P}$ is a distributive lattice under the following partial ordering:

$$
\begin{aligned}
&(a_1,b_1,c_1) \leq (a_2,b_2,c_2) \text{ if and only if}\\
&k(a_1,b_1,c_1) \leq k(a_2,b_2,c_2) \text{ and } n(a_1,b_1,c_1) \leq n(a_1,b_1,c_1),
\end{aligned}
$$

where the numbers $k(a_j, b_j, c_j)$ and $n(a_j, b_j, c_j)$, for $j = 1, 2$, are defined in Theorem 6.

Example. We shall show that Dawson's operations denoted here by $\oplus_D$ and $\odot_D$, differ from those given in Theorem 7. In case (i), we have $1_{\mathcal{P}} \oplus 1_{\mathcal{P}} = \alpha(1,1) \oplus \alpha(1,1) = \alpha(2,2) = (6,8,10) = 2 \cdot 1_{\mathcal{P}}$, and $(4,3,5) \odot (4,3,5) = \alpha(1,2) \odot \alpha(1,2) = \alpha(1,4) = (8,6,10) = 2 \cdot (4,3,5)$. On the other hand, from [1] it follows that $1_{\mathcal{P}} \oplus_D 1_{\mathcal{P}} = (4,3,5)$, and that $(4,3,5) \odot_D (4,3,5) = (16,30,32) = 2 \cdot (8,15,16)$.

In case (ii), the addition is identical as in case (i), and we have $(4,3,5) \odot (4,3,5) = \alpha(1,2) \odot \alpha(1,2) = \alpha(-3,4) = (-8,6,10) = 2 \cdot (-4,3,5)$.

6. The Field Structure on $\mathcal{P}^*$. The following observation leads to the construction of the field structure on some classes of subsets of $\mathcal{P}$. Theorem 6 and properties (7) and (8) yield

Proposition 2. For every odd and square–free number $r \geq 1$ we have $\alpha(1,r) = r1_{\mathcal{P}}$. In particular, for each pair of different odd prime numbers p, q we have $\alpha(1,pq) = pq1_{\mathcal{P}}$.

This result suggests to find a multiplication $\circ$ on $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ with $(1,p) \circ (1,q) = (1,pq)$ for all odd prime numbers p, q and to carry it onto $\mathcal{P}^*$, with the help of the function α, to obtain the equation $\alpha((1,p) \circ (1,q)) = \alpha(1,p) \odot \alpha(1,q)$. There exist two multiplications which fulfill that requirement: the coordinatewise multiplication, just used in Theorem 7 (i), and the multiplication connected with fractions, where the pair $(1,n)$ corresponds to the fraction $1/n$. Let R denote the equivalence relation on $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ of the form

$$(k_1, n_1)R(k_2, n_2) \text{ if and only if } k_1 n_2 = k_2 n_1,$$

and let $R(\alpha)$ be carried from $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ onto $\mathcal{P}^*$, by means of α, relation R, i.e.

$$\begin{aligned}
&(a_1, b_1, c_1)R(\alpha)(a_2, b_2, c_2) \text{ if and only if} \\
&(a_1 + b_1 - c_1)(c_2 - b_2)d_{\mathrm{ev}}(c_2 - b_2)\sqrt[*]{c_2 - b_2} \\
&= (a_2 + b_2 - c_2)(c_1 - b_1)d_{\mathrm{ev}}(c_1 - b_1)\sqrt[*]{c_1 - b_1}.
\end{aligned}$$

(The form of $R(\alpha)$ obtained from R, where $k_j = k(a_j, b_j, c_j)$ and $n_j = n(a_j, b_j, c_j)$, for $j = 1, 2$, are defined in Theorem 6.) The equivalence classes determined by R and

$R(\alpha)$, respectively, we denote by $[\,]_R$ and $[\,]_{R(\alpha)}$, respectively. From Theorem 6 it follows that the function $\hat{\alpha}\colon \mathbb{Z}\times(\mathbb{Z}\backslash\{0\})\to\mathcal{P}^*$ of the form $\hat{\alpha}([(k,n)]_R)=[\alpha(k,n)]_{R(n)}$ is bijective. Since $(\mathbb{Z}\times(\mathbb{Z}\backslash\{0\}))/R$ possesses the field structure (of fractions), $\hat{\alpha}$ transfers this structure onto $\mathcal{P}^*$ automatically. We also have the (additive zero) element $[0,1]_R$ going to $[(0,0,0)]_{R(\alpha)}$ and the (multiplicative unit) element $[(1,1)]_R$ going to $[1_{\mathcal{P}}]_{R(\alpha)}$. It is easy to check that $(a,b,c)R(\alpha)(0,0,0)$ provided that $a+b=c$, and that $(a,b,c)R(\alpha)1_{\mathcal{P}}$ whenever $a+b-c=(c-b)d_{\mathrm{ev}}(c-b)\sqrt[*]{c-b}$ (for example, $[1_{\mathcal{P}}]_{R(\alpha)}=[(6,8,10)]_{R(\alpha)}(=[\alpha(2,2)]_{R(\alpha)}=[(21,72,75)]_{R(\alpha)}(=[\alpha(3,3)]_{R(\alpha)})))$. This proves the following theorem.

Theorem 9. The set $\mathcal{P}^*/R(\alpha)$ is a commutative field under the following operations of addition $\oplus$ and multiplication $\odot$

$$[(a_1,b_1,c_1)]_{R(\alpha)}\oplus[(a_2,b_2,c_2)]_{R(\alpha)}:=[\alpha(k_1n_2+k_2n_1,n_1n_2)]_{R(\alpha)},$$
$$[(a_1,b_1,c_1)]_{R(\alpha)}\odot[(a_2,b_2,c_2)]_{R(\alpha)}:=[\alpha(k_1k_2,n_1n_2)]_{R(\alpha)},$$

where for the given representatives (a_j',b_j',c_j') of $[(a_j,b_j,c_j)]_{R(\alpha)}$, the integers $k_j=k(a_j',b_j',c_j')$ and $n_j=n(a_j',b_j',c_j')$, for $j=1,2$, are defined as in Theorem 6. The additive zero is $[(0,0,0)]_{R(\alpha)}$, and the multiplicative unit is $[(3,4,5)]_{R(\alpha)}$. The additive inverse of the element $[(a,b,c)]_{R(\alpha)}$ is

$$\ominus[(a,b,c)]_{R(\alpha)}=[(A,B,C)]_{R(\alpha)},\ \text{where}$$

$$A=-\frac{a+b-c}{d_{\mathrm{ev}}(c-b)}+c-b,\ B=(A^2-(c-b)^2)/2(c-b),\ C=B+c-b$$

(equivalently, $\ominus[\alpha(k,n)]_{R(\alpha)}=[\alpha(-k,n)]_{R(\alpha)}$). The multiplicative inverse of the element $[(a,b,c)]_{R(\alpha)}$ for $a+b\neq c$ is

$$[(a,b,c)]_{R(\alpha)}^{-1}=[(E,F,G)]_{R(\alpha)},\ \text{where}$$

$$E=(c-b)\cdot d_{\mathrm{ev}}\left(\frac{a+b-c}{d_{\mathrm{ev}}(c-b)\cdot\sqrt[*]{c-b}}\right)\cdot\sqrt[*]{\frac{a+b-c}{d_{\mathrm{ev}}(c-b)\cdot\sqrt[*]{c-b}}},$$

$$F=(E^2-(c-b)^2)/2(c-b),\ G=F+c-b$$

(equivalently, for $k \neq 0$, we have $[\alpha(k,n)]^{-1}_{R(\alpha)} = [\alpha(n,k)]_{R(\alpha)}$].

By way of example, we have $\ominus[(4,3,5)]_{R(\alpha)} = \ominus[\alpha(1,2)]_{R(\alpha)} = [\alpha(-1,2)]_{R(\alpha)} = [(0,-1,1)]_{R(\alpha)}$, and $[(4,3,5)]^{-1}_{R(\alpha)} = [\alpha(1,2)]^{-1}_{R(\alpha)} = [\alpha(2,1)]_{R(\alpha)} = [(5,12,13)]_{R(\alpha)}$.

References

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

2. A. Grytczuk, "Note on a Pythagorean Ring," *Missouri Journal of Mathematical Sciences*, 9 (1997), 83–89.

3. M. Wójtowicz, "Algebraic Structures of Some Sets of Pythagorean Triples I," *Missouri Journal of Mathematical Sciences*, 12 (2000), 31–35.

Marek Wójtowicz
T. Kotarbinski Pedagogical University
Institute of Mathematics
65-069 Zielona Góra, Poland
email: mwojt@lord.wsp.zgora.pl