ALGEBRAIC STRUCTURES OF SOME SETS OF PYTHAGOREAN TRIPLES I

Marek Wójtowicz

Abstract. Let $\mathcal{P}$ denote the set of all Pythagorean triples $\{(a,b,c) \in \mathbb{Z}^3 : a^2+b^2=c^2\}$, and let $\mathcal{P}_n = \{(a,b,c) \in \mathcal{P} : c-b=n\}$, for $n \neq 0$, and $\mathcal{P}_0 = \{(0,j,j) : j \in \mathbb{Z}\}$. It is shown that the ring operations defined by A. Grytczuk on $\mathcal{P}_n$'s are determined by shifts and an injection acting from suitable subsets of $\mathbb{Z}+i\mathbb{Z}$ into $\mathbb{Z}^3$ (Section 2), and that all $\mathcal{P}_n$'s are distributive lattices (Theorem 2). The ring and the lattice structures of $\Pi = \{(a,b,c) \in \mathcal{P} : a=2xy,\ b=x^2-y^2,\ c=x^2+y^2\}$ and some of its subsets are discussed in Theorems 3, 4, and 5.

1. Introduction. In 1994 B. Dawson [1] defined the operations $\oplus$ and $\odot$ on $\mathcal{P}$ in such a way that $(\mathcal{P};\oplus,\odot)$ is a commutative ring with unit. The operations are constructed on the sets $\mathcal{P}_n$, $n \in \mathbb{Z}$, and next extended to $\mathcal{P}$, but both the addition and the multiplication are given in inconvenient form. Therefore Dawson stated the open problem to define different "natural" ring operations on $\mathcal{P}$. In 1997 A. Grytczuk [2] gave the construction of new operations on $\mathcal{P}_n$, namely ([2], Theorem):

(a) We have $\alpha = (a,b,c) \in \mathcal{P}_n$ if and only if $\alpha = (a, (a^2-n^2)/(2n), (a^2+n^2)/(2n))$, where a and $n \neq 0$ are the same parity.

(b) Under the following well defined operations $\bigoplus_n$ and $\bigodot_n$ on $\mathcal{P}_n$:

$$\alpha \bigoplus\nolimits_n \beta = \left(a, \frac{a^2-n^2}{2n}, \frac{a^2+n^2}{2n}\right) \bigoplus\nolimits_n \left(b, \frac{b^2-n^2}{2n}, \frac{b^2+n^2}{2n}\right)$$

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

$$\alpha \bigodot\nolimits_n \beta := \Bigg((a-n)(b-n)+n,$$

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

for $n \neq 0$, and coordinatewise for $n=0$, the sets $\mathcal{P}_n$ are commutative rings (without multiplicative units for $n \neq 0$).

The purpose of this paper is to show that the above defined additions and multiplications are quite natural in the category of rings (Theorem 1), and to construct other natural algebraic operations on some subsets of $\mathcal{P}$ (Section 3).

We use standard notations. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, and $\mathbb{N}$ stand for the sets of all real, complex, whole, and natural numbers, respectively, endowed with their classical algebraic ring and order structures, and $i \in \mathbb{C}$ denotes the imaginary unit.

A general and known procedure constructing ring (or group, field, etc.) operations on arbitrary sets, which will be applied in this paper, is presented below.

Lemma. Let X and Y be nonempty sets with card $X =$ card Y, let $\triangle$ be a binary operation on X, and let ξ be a bijection $Y \to X$. The binary operation $\triangle_\xi$, defined by the rule $y_1 \triangle_\xi y_2 := \xi^{-1}(\xi y_1 \triangle \xi y_2)$, is well defined and the mapping ξ is an $\triangle_\xi - \triangle$ isomorphism of the sets Y and X. In particular, if $X = (X; +, \cdot)$ is a ring and ξ denotes the shift function $x \to x - t$, then we obtain the new ring operations on X: $x_1 \oplus_t x_2 := x_1 + x_2 - t$, and $x_1 \odot_t x_2 := (x_1 - t) \cdot (x_2 - t) + t$, and this shift establishes also a ring isomorphism from $(X; \oplus_t, \odot_t)$ onto X.

(In this way any countable and infinite set can be endowed with the ring structure carried from $\mathbb{Z}$. For example, there exist formally many different ring structures both on $\mathcal{P}$ and on $\mathcal{P}_n$'s, but most of them have nothing to do with the Pythagorean equation.)

The particular case holds for the ring $\mathbb{Z}$ and its complex copies $\mathbb{W}_n = \mathbb{Z} + in$, $n = \pm 1, \pm 2, \ldots$, where the addition $\#_n$ and the multiplication $*_n$ are those carried from $\mathbb{Z}$ and acting on the real coordinate only, i.e. $(a_1 + in)\#_n(a_2 + in) = a_1 + a_2 + in$, and similarly for $*_n$. As we shall see in the next section, shifts on $\mathbb{W}_n$'s are determined by the number n, the knowledge of which allows us to construct adequate ring operations on $\mathcal{P}_n$.

2. Grytczuk's Operations. Let $\oplus_n$ and $\odot_n$, $n = \pm 1, \pm 2, \ldots$, denote the operations on $\mathbb{W}_n$ obtained from $(\mathbb{W}_n; \#_n, *_n)$ by means of the shifts $w \to w - n$, i.e.,

$$(a_1 + in) \oplus_n (a_2 + in) = a_1 + a_2 - n + in,$$
$$(a_1 + in) \odot_n (a_2 + in) = (a_1 - n)(a_2 - n) + n + in.$$

The formulas defining $\bigoplus_n$ and $\bigodot_n$ become more clear if we shall use the rings $(\mathbb{W}_n; \oplus_n, \odot_n)$ and the functions $A: \mathbb{C} \to \mathbb{R}^3$ defined by the rules $A(z) = (\mathrm{Im}(z^2), \mathrm{Re}(z^2), |z|^2)$, and $A_n = (1/2n)A$, $n = \pm 1, \pm 2, \ldots$. These functions are injective on each nonempty subset H of $\mathbb{C}$ with $H \cap (-H) = \emptyset$ or $H \cap (-H) = \{0\}$, hence on $\mathbb{W}_n$, on the halfplane $\mathrm{Im}(z) > 0$, on each quarter of $\mathbb{C}$, etc. For any $\alpha = (a, b, c) \in \mathcal{P}_n$, where $n = c - b \neq 0$, we can determine uniquely the complex number $\tilde{\alpha} = a + in$ such that, by (a), we have $\alpha = A_n(\tilde{\alpha})$. Hence, Grytczuk's operations take the form

$$\alpha \bigoplus_n \beta = A_n(\tilde{\alpha} \oplus_n \tilde{\beta}),$$

$$\alpha \bigodot_n \beta = A_n(\tilde{\alpha} \odot_n \tilde{\beta}).$$

It is now obvious that $\bigoplus_n$ and $\bigodot_n$ are both associative and commutative, and that they fulfill the distributive law; however, the fact that $\bigoplus_n$ and $\bigodot_n$ are well defined is nontrivial and is proved in [2].

By the above observations, and since for every $n = \pm 1, \pm 2, \ldots$, the rings $(\mathbb{W}_n; \oplus_n, \odot_n)$ and $\mathbb{Z}$ are isomorphic via the mapping $\phi_n(w) = \mathrm{Re}(w) - n$, the main result of [2] can be presented in the following way.

Theorem 1. For every integer $n \neq 0$, $(\mathcal{P}_n; \bigoplus_n, \bigodot_n)$ is a commutative ring isomorphic, via the mapping $\psi_n(\alpha) = \phi_n(\tilde{\alpha}) = a + b - c$ (where $\alpha = (a, b, c)$ and $n = c - b$) with a subring of $\mathbb{Z}$ without multiplicative unit.

The last part of the above theorem follows also from the form of ψ_n: if $1 = \psi_n(\alpha) = a + b - c$, then $(a + b)^2 = (c + 1)^2$. Hence, $2ab = 2c + 1$, a contradiction.

Corollary 1. For every integer $n \neq 0$, the set

$$\mathcal{G}_n := \psi_n(\mathcal{P}_n) = \{a + b - c : a^2 + b^2 = c^2 \text{ and } c - b = n\}$$

is a proper ring ideal of $\mathbb{Z}$.

From the categorical point of view, the Grytczuk's operations seem to be "proper" (i.e., they fulfill Dawson's requirement to be natural) because they are generated by shifts, and the isomorphisms ψ_n defined in Theorem 1 are of the simplest ring nature.

3. Other Algebraic Operations on Subsets of $\mathcal{P}$. The possibility of unique transferring, by means of the function A_n, natural operations from a subset of $\mathbb{W}_n$ onto the set $\mathcal{P}_n$ suggests the constructing of new algebraic operations on subsets of $\mathcal{P}$ using suitable operations defined on some subsets of $\mathbb{Z} + i\mathbb{Z}$. In the first theorem of this section we discuss the lattice structure of $\mathcal{P}_n$, and the next ones are devoted to the connections between algebraic structures of the sets $\mathbb{W} = (\mathbb{Z} + i\mathbb{N}) \cup \{0\}$ and $\mathbb{W}_n$, respectively, and the set $\Pi := A(\mathbb{W}) \subset \mathcal{P}$ and $\Pi_n := A(\mathbb{W}_n)$, respectively. Similar results can be obtained when $\mathbb{W}$ and $\mathbb{W}_n$ are replaced by other subsets of $\mathbb{Z}+i\mathbb{Z}$ on which the function A is injective (here we have $\mathbb{W}\cap(-\mathbb{W}) = \{0\}$ and $\mathbb{W}_n \cap (-\mathbb{W}_n) = \emptyset$ which implies injectivity of A both on $\mathbb{W}$ and on $\mathbb{W}_n$).

The fact that the $\mathcal{P}_n$'s have the lattice structure follows from the observation that if $(a_k + in) \in D_n := A_n^{-1}(\mathcal{P}_n)$, $n = 1, 2, \ldots$, $k = 1, 2$, then $\max\{a_1, a_2\} + in$, $\min\{a_1, a_2\} + in \in D_n$. It follows that two natural functions map $\mathcal{P}_n$ (lattice) isomorphically onto a sublattice of $\mathbb{Z}$: the first one, universal for all $\mathcal{P}_n$'s, is of the form $(a, b, c) \to a$, and the second one is ψ_n, defined in Theorem 1 (since for all $x, y, t \in \mathbb{R}$ we have: $\max\{x-t, y-t\} = \max\{x, y\} - t$, and $\min\{x-t, y-t\} = \min\{x, y\} - t$). Hence we obtain the following theorem.

<u>Theorem 2</u>. Endowed with the ordering $\alpha_1 = (a_1, b_1, c_1) \leq (a_2, b_2, c_2) = \alpha_2$ if and only if $a_1 \leq a_2$, the sets $\mathcal{P}_n$, $n = \pm 1, \pm 2, \ldots$, are distributive lattices isomorphic with sublattices of $\mathbb{Z}$, and we have

$$\begin{aligned} &\sup(\alpha_1, \alpha_2) = A_n(\max\{a_1, a_2\} + in), \text{ and} \\ &\inf(\alpha_1, \alpha_2) = A_n(\min\{a_1, a_2\} + in), \end{aligned}$$

where $n = c_1 - b_1 = c_2 - b_2$.

<u>Corollary 2</u>. With the above notations, for every $n = \pm 1, \pm 2, \ldots$, we have:
(i) the mapping ψ_n is both a ring and lattice isomorphism;
(ii) the sets $\mathcal{G}_n$ and $\mathcal{G}'_n := \mathcal{G}_n + n = \{a \in \mathbb{Z} : a^2 + b^2 = c^2 \text{ and } c - b = n\}$ are sublattices of the lattice $\mathbb{Z}$.

From the Lemma given in Section 1 it follows that A carries in a natural way all algebraic structures of $\mathbb{W}$ to the set Π, and the same procedure takes place in the case $\mathbb{W}_n$ and Π_n; hence, the following three theorems are now immediate consequences of this fact.

<u>Theorem 3</u>. The set Π is a semiring with unit under the following pairs of addition and multiplication.
(i) $Az \oplus Au := A(z+u)$, and $Az \odot Au := A(z \cdot u)$;
(ii) $Az \oplus Au := A(z+u)$, and $Az \odot Au := A(z * u)$, where $+$ and $\cdot$ denote the classical operations, and $*$ denotes the coordinatewise multiplication in $\mathbb{C}$.

<u>Theorem 4</u>. For every $n \in \mathbb{N}$, the set Π_n is a commutative ring with unit under the following pairs of addition and multiplication.
(i) $Az[+]_n Au := A(z \#_n u)$, and $Az[\cdot]_n Au := A(z *_n u)$;
(ii) $Az\langle + \rangle_n Au := A(z \oplus_n u)$, and $Az\langle \cdot \rangle_n Au := A(z \odot_n u)$,

where $\oplus_n$, $\odot_n$, $\#_n$, and $*_n$ are defined in Section 2.

Theorem 5. Endowed with the ordering $Az \leq Au$ if and only if $z \leq u$ in $\mathbb{W}$, the set Π is a distributive lattice and Π_n, $n = \pm 1, \pm 2, \ldots$, is its distributive sublattice, and we have

$$\sup\{A(n_1 + im_1), A(n_2 + im_2)\} = A(\max\{n_1, n_2\} + i \max\{m_1, m_2\}), \text{ and}$$
$$\inf\{A(n_1 + im_1), A(n_2 + im_2)\} = A(\min\{n_1, n_2\} + i \min\{m_1, m_2\}).$$

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.

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