Section 16 Supplement. The Group of Pythagorean Triples

Note. In this supplement to Section 16. Pythagorean Triangles, we create a group **P** out of the primitive Pythagorean triples. We define a binary operation and show that **P** is a free abelian group. The results of this supplement are from: Ernest Eckert, The Group of Primitive Pythagorean Triangles, *Mathematics Magazine*, **57**(1), 22–27 (January 1984).

Note. In January 1984, I was an undergraduate student in math at Auburn University at Montgomery. I was in the middle of completing an Analysis (MATH 321 and 322) sequence and a Numerical Analysis (MATH 460 and 461) sequence. I had taken Number Theory (MATH 330) and the Introduction to Modern Algebra (MATH 331 and 332) sequence during the previous academic year. I was mildly fascinated that one could take Pythagorean triples (from number theory) and make them elements of a group (from modern algebra). This supplement will assume a bit of knowledge of the structure and properties of groups, as covered in ETSU's Introduction to Modern Algebra (for introduction to the concept of a group; this is also briefly covered Mathematical Reasoning [MATH 3000] in Section 6.1. Operations) and Introduction to Modern Algebra 2 (especially Section VII.38. Free Abelian Groups).

Note/Definition. Recall that three positive integers a, b, c which are lengths of the sides of a right triangle determine a *Pythagorean triple* (a, b, c) when $a^2 + b^2 = c^2$. If a, b, c share no common divisor (that is, if a, b, c is a *fundamental solution* to the equation $x^2 + y^2 = z^2$), then we call (a, b, c) a *primitive Pythagorean triple* (or the lengths of the sides of a *primitive Pythagorean triangle*). Notice that we are treating Pythagorean triples as ordered triples so, for example, we distinguish between $(3, 4, 5)$ and $(4, 3, 5)$.

Definition. We define an equivalence relation on the set of all Pythagorean triples as

$$(a_1, b_1, c_1) \equiv (a_2, b_2, c_2) \text{ if and only if } a_1/a_2 = b_1/b_2 = c_1/c_2 \in \mathbb{N}$$

$$\text{or } a_2/a_1 = b_2/b_1 = c_2/c_1 \in \mathbb{N}.$$

That is, two Pythagorean triples are equivalent if and only if one is a positive integer multiple of the other. Notice that each equivalence class contains exactly one primitive Pythagorean triple. We denote an equivalence class as the unique primitive Pythagorean triple in the equivalence class. Let $\mathbf{P}$ denote the set of all equivalence classes of Pythagorean triples.

Note. We have, for example, that $(3, 4, 5) \equiv (6, 8, 10) \equiv (9, 12, 15)$, but $(3, 4, 5) \not\equiv (4, 3, 5)$. We should comment that Eckert in his paper does not discuss an equivalence relation or equivalence classes, but instead accomplishes this through a geometric argument.

Note. It is straightforward to confirm that the product of two integers, each of which is a sum of two squares, is again a sum of two squares:

$$(a^2+b^2)(A^2+B^2) = (aA-bB)^2+(aB+bA)^2. \quad (1)$$

Notice that if $a^2 + b^2 = c^2$ and $A^2 + B^2 = C^2$, that is, if (a, b, c) and (A, B, C) are Pythagorean triples, then this equation suggests a way to make a new Pythagorean triple. Based on this observation, we define a binary operation that produces a Pythagorean triple from two given Pythagorean triples. We'll put a geometric interpretation on this process below.

Definition. Define the binary operation (which we denote as "+") on the set of **P** of equivalence classes of Pythagorean triples as

$$(a, b, c) + (A, B, C) = \begin{cases} (aA - bB, bA + aB, cC) & \text{when } aA - bB > 0 \\ (bA + aB, bB - aA, cC) & \text{when} aA - bB \leq 0 \end{cases}$$

Note. If we consider (ka, kb, kc) and (KA, KB, KC) as non-primitive Pythagorean triples with $(ka, kb, kc) \equiv (a, b, c)$ and $(KA, KB, KC) \equiv (A, B, C)$, then we have $(ka, kb, kc) + (KA, KB, KC) \equiv (a, b, c) + (A, B, C)$. That is, + is well defined.

Note. In order to make a group, we need the binary operation to be associative, we need an identity, and each element must have an inverse. We add the equivalence class containing $(1, 0, 1)$ to **P** and notice that for $(a, b, c), (A, B, C) \in \mathbf{P}$ we have

$$(a, b, c) + (1, 0, 1) = (1a - 0b, 1b + 0a, 1c) = (a, b, c)$$

$$\text{and } (1,0,1)+(A,B,C)=(1A-0B,0B+1A,1C)=(A,B,C).$$

So $(1,0,1)$ is a left and right identity. Notice that *if* we included the equivalence class containing triple $(0,1,1)$, then we would have $(a,b,c)+(0,1,1)=(0b+1a,1b-0a,1c=(a,b,c)$ and $(0,1,1)+(A,B,C)=(1A+0B,1B-0A,1C)=(A,B,C)$ and this would also be an identity under $+$; but we do not include this triple and the identity is unique. We also have

$$(A,B,C)+(a,b,c) = \begin{cases} (Aa-Bb,Ba+Ab,Cc) & \text{when } Aa-Bb>0 \\ (Ba+Ab,Bb-Aa,Cc) & \text{when } Aa-Bb\leq 0 \end{cases}$$

$$= \begin{cases} (aA-bB,bA+aB,cC) & \text{when } aA-bB>0 \\ (bA+aB,bB-aA,cC) & \text{when } aA-bB\leq 0. \end{cases}$$

That is, $(a,b,c)+(A,B,C)=(A,B,C)+(a,b,c)$ and so the binary operation is commutative. Notice that for any $(a,b,c)\in\mathbf{P}$, we also have $(b,a,c)\in\mathbf{P}$ (as ordered triples, these are distinct), and

$(a,b,c)+(b,a,c)=(bb+aa,ba-ab,cc)=(a^2+b^2,0,c^2)\equiv(1,0,1)$, so that the inverse under $+$ of (a,b,c) is (b,a,c). We could establish associativity computationally (though it will be tedious), but instead we now make a geometric observation and argue associativity from this geometric interpretation (as Eckert does in his paper).

Note. Suppose (a,b,c) is a Pythagorean triple (or the triple $(1,0,1)$). Consider the complex number $z=a+ib$, where $a>0$ and $b\geq 0$ (notice that a and b play different roles here; this will ultimately be related to the fact that, in the associated Pythagorean triples, we distinguish between (a,b,c) and (b,a,c)). Then the modulus of z is $|z|=|a+ib|=\sqrt{a^2+c^2}=c$. Then z is in the (open) first quadrant of the complex plane $\mathbb{C}$, or $z=a$ is a positive real number. If we

"normalize" z and consider the complex number $z/|z|$ of modulus 1, then we get $z/|z| = (a/c) + i(b/c)$. Now every complex number of modulus 1 is of the form $e^{i\alpha}$, where α is an argument of the complex number. Since $z/|z|$ is in the open first quadrant of $\mathbb{C}$ or is a positive real number, then we can choose α to satisfy $0 \leq \alpha < \pi/2$. For material on the behavior of complex numbers, see my online notes for Complex Variables (MATH 4337/5337). So if (A, B, C) is a Pythagorean triple (or the triple $(1, 0, 1)$) then we can similarly consider the complex number $w = A + iB$ of modulus C, and write $w/|w| = (A/C) + i(B/C) = e^{i\beta}$ where $0 \leq \beta < \pi/2$. By properties of the complex exponential function, we then have:

$$\frac{z}{|z|}\frac{w}{|w|} = e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)} = \left(\frac{a}{c} + i\frac{b}{c}\right)\left(\frac{A}{C} + i\frac{B}{C}\right) = \frac{aA - bB}{cC} + i\frac{aB + bA}{cC}.$$

See Figure 1.

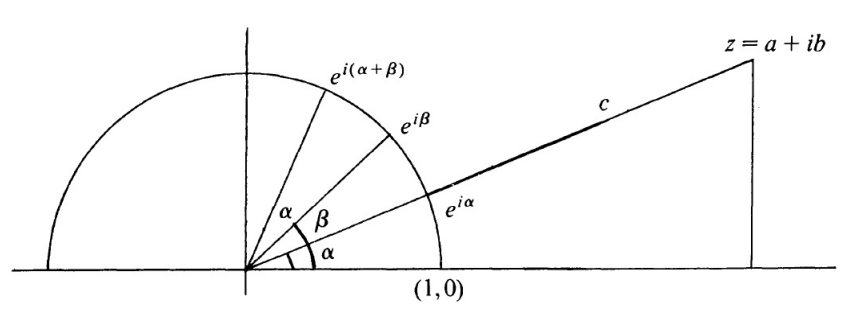

Figure 1. From Eckert's "The Group of Primitive Pythagorean Triangles"

Note. Notice that the complex number $Z = \dfrac{aA - bB}{cC} + i\dfrac{aB + bA}{cC}$ may have a 0 or negative real part and so may not lie in the open first quadrant or along the positive real axis. We do know that $(aA - bB)^2 + (aB + bA)^2 = (cC)^2$, either because the complex number Z is of modulus 1 or by equation (1) above. So we know that we can make a Pythagorean triple out of either $aA - bB, aB + bA, cC$

or $bB - aA, aB + bA, cC$. By our definition of $+$ we take the Pythagorean triple $(aA-bB, bA+aB, cC)$ if $aA-bB > 0$, and $(bA+aB, bB-aA, cC)$ if $aA-bB \leq 0$. But this means that when $aA - bB \leq 0$, we are modifying the complex number $Z = \dfrac{aA-bB}{cC} + i\dfrac{aB+bA}{cC}$ (which lies in the open second quadrant of along the positive imaginary axis) to the new complex number $\dfrac{aB+bA}{cC} + i\dfrac{bB-aA}{cC}$. That is, we are replacing Z with $-iZ$; notice that with $Z = \mathrm{Re}(Z) + i\mathrm{Im}(Z)$ we have

$$-iZ = -i(\mathrm{Re}(Z) + i\mathrm{Im}(Z)) = \mathrm{Im}(Z) - i\mathrm{Re}(Z)),$$

so that this new complex number lies in the open first quadrant or along the positive real axis. Geometrically, this corresponds to subtracting $\pi/2$ from the argument of Z. Notice that if an argument of Z is γ so that $Z = e^{i\gamma} = \cos\gamma + i\sin\gamma$, then we have

$$-iZ = -ie^{i\gamma} = -i(\cos(\gamma) + i\sin(\gamma))$$

$$= \sin\gamma - i\cos\gamma = \cos(\gamma - \pi/2) + i\sin(\gamma - \pi/2),$$

since by the the difference formulae $\cos(\alpha - \beta) = \cos\alpha\cos\beta + \sin\alpha\sin\beta$ and $\sin(\alpha - \beta) = \sin\alpha\cos\beta - \cos\alpha\sin\beta$ imply that $\cos(\gamma - \pi/2) = \cos\gamma\cos\pi/2 + \sin\gamma\sin\pi/2 = \sin\gamma$ and $\sin(\gamma - \pi/2) = \sin\gamma\cos\pi/2 - \cos\gamma\sin\pi/2 = -\cos\gamma$ (we can also justify this claim using the fact that an argument of $-i$ is $-\pi/2$).

Note. So we can interpret $(a, b, c)+(A, B, C)$ in $\mathbf{P}$ as multiplying the modulus-one complex numbers $(a/c)+i(b/c)$ and $(A/C)+i(B/C)$, reducing the argument of the resulting product modulo $\pi/2$, and converting back to a Pythagorean triple with third entry cC. As an example, consider $(3, 4, 5) + (5, 12, 13)$. We consider $\dfrac{3}{5} + i\dfrac{4}{5}$ and $\dfrac{5}{13} + i\dfrac{12}{13}$, which produce the product $-\dfrac{33}{65} + i\dfrac{56}{65}$. But the product is in the

second quadrant (that is, the argument of the product is greater than $\pi/2$). We next subtract $\pi/2$ from the argument of the product (or shuffle around the real and imaginary parts) to get $\frac{56}{65} + i\frac{33}{65}$. So $(3,4,5)+(5,12,13) = (56,33,65)$. See Figure 2.

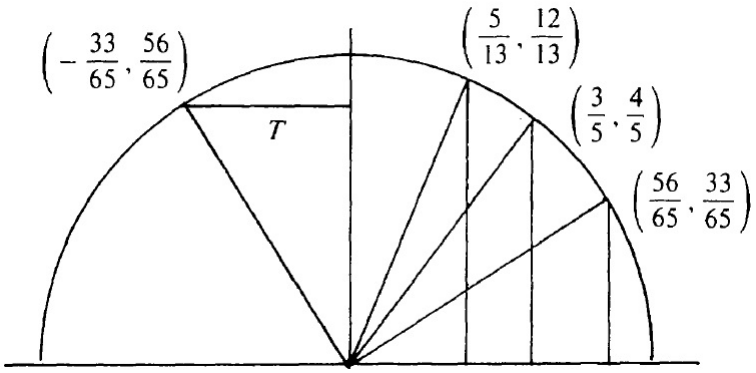

Figure 2. From Eckert's "The Group of Primitive Pythagorean Triangles"

Note. Notice that we can associate Pythagorean triple (a,b,c) with modulus-one complex number $e^{i\alpha}$ where $\alpha = \cos^{-1}(a/c)$. Conversely we can associate complex number $e^{i\alpha}$, where $\cos\alpha = a/c$ for some $a, c \in \mathbb{N} \cup \{0\}$ such that $c^2 - a^2$ is a perfect square, with the Pythagorean triple $(a, \sqrt{c^2-a^2}, c)$. So if (a_1,b_1,c_1), (a_2,b_2,c_2), and (a_3,b_3,c_3) are Pythagorean triples which under this association are associated with the modulus-one complex numbers $e^{i\alpha_1}$, $e^{i\alpha_2}$, and $e^{i\alpha_3}$, respectively, then $((a_1,b_1,c_1)+(a_2,b_2,c_2))+(a_3,b_3,c_3)$ is associated with $(e^{i\alpha_1}e^{i\alpha_2})(e^{i\alpha_3}) = e^{i(\alpha_1+\alpha_2+\alpha_3}$ and $(a_1,b_1,c_1)+((a_2,b_2,c_2)+(a_3,b_3,c_3))$ is associated with $e^{i\alpha_1}(e^{i\alpha_2}e^{i\alpha_3}) = e^{i(\alpha_1+\alpha_2+\alpha_3}$. It follows that

$$((a_1,b_1,c_1)+(a_2,b_2,c_2))+(a_3,b_3,c_3) = (a_1,b_1,c_1)+((a_2,b_2,c_2))+(a_3,b_3,c_3)),$$

so that we have associativity of $+$. Therefore, $\mathbf{P}$ is a commutative group under $+$.

Note. Consider the group of elements $[0, \pi/2)$ with the binary operation of addition modulo $\pi/2$. With the "association" of the previous note, we see that we can map the group $\mathbf{P}$ into the group $[0, \pi/2)$ under addition modulo $\pi/2$ (in the process, we go "through" the modulus-one complex numbers described above). So $\mathbf{P}$ is isomorphic to a subgroup of $[0, \pi/2)$.

Note. Since we treat $\mathbf{P}$ as an additive group, then we denote the sum of an element (a, b, c) with itself n times as $n(a, b, c)$:

$$n(a,b,c) = \underbrace{(a,b,c) + (a,b,c) + \cdots + (a,b,c)}_{n \text{ times}}.$$

This is not to be confused with the idea above involving the equivalence relation. Here, the coefficient represents repeated addition. For $-n$ a negative integer, we have:

$$-n(a,b,c) = \underbrace{(b,a,c) + (b,a,c) + \cdots + (b,a,c)}_{n \text{ times}}.$$

For $n = 0$, we take $n(a, b, c) = 0(a, b, c) = (1, 0, 1)$ (the identity in $\mathbf{P}$). We can now consider the subgroup of $\mathbf{P}$ generated by an element of $\mathbf{P}$:

$$\langle (a,b,c) \rangle = \{ n(a,b,c) \mid n \in \mathbb{Z} \}.$$

Notice that $\langle (a, b, c) \rangle = \langle (b, a, c) \rangle$. Eckert gives an argument that each element of $\mathbf{P}$, other than the identity $(1, 0, 1)$, generates an infinite cyclic subgroup (Eckert's argument is geometric and based on the irrationality of π).

Definition. In an additive group with identity e, the *order* of an element a is the smallest positive integer n such that $na =$. If no such n exists, then a is of *infinite order*. One can show that in a commutative group G, the set of elements of finite order form a subgroup of G (see Exercise II.11.39 in John B. Fraleigh's *A First Course In Abstract Algebra*, 7th Edition (Addison-Wesley (2003)). This group is the *torsion subgroup* of G. A commutative group is *torsion free* if the identity e is the only element of finite order.

Definition. For X a subset of commutative group G, if each nonidentity element a in G can be expressed uniquely (up to order of summands) in the form $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ for $n_i \neq 0$ in $\mathbb{Z}$ and distinct $x_i \in X$, then G is a *free abelian group* and X is a *basis* for the group. (See my online notes for Introduction to Modern Algebra 2 [MATH 4137/5137] on Section VII.38. Free Abelian Groups).

Note. Eckert proves that $\mathbf{P}$ is a free abelian group and gives a basis for the group in the following result.

Proposition of Eckert. The group $\mathbf{P}$ is a free abelian group which has as a basis

$$X = \{a, b, p) \mid p \text{ prime}, p \equiv 1 (\text{mod } 4), \text{ and } a > b\}.$$

Note. Using the representation of the elements of **P** in terms of the basis given in his proposition, Eckert is able to count the number of primitive Pythagorean triangles with the same hypotenuse, as follows.

Corollary of Eckert. The number of primitive Pythagorean triangles with the same hypotenuse $c = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ is 2^k. Equivalently, the number of primitive Pythagorean triples of the form (a, b, c) where $a^2 + b^2 = c^2$ and $c = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ is 2^k.

Revised: 2/18/2022