Rose-Hulman Undergraduate Mathematics Journal

Subrings of $\mathbb{C}$ Generated by Angles

Jackson Bahr[a] Arielle Roth[b]

Volume 17, No. 1, Spring 2016

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Carnegie Mellon University
[b]Elizabethtown College

Rose-Hulman Undergraduate Mathematics Journal
Volume 17, No. 1, Spring 2016

Subrings of $\mathbb{C}$ Generated by Angles

Jackson Bahr   Arielle Roth

Abstract. Consider the following inductively defined set. Given a collection U of unit magnitude complex numbers, and a set initially containing just 0 and 1, through each point in the set, draw lines whose angles with the real axis are in U. Add every intersection of such lines to the set. Upon taking the closure, we obtain $R(U)$. We investigate for which U the set $R(U)$ is a ring. Our main result holds for $1 \in U$ and $|U| \geq 4$. If P is the set of real numbers in $R(U)$ generated in the second step of the construction, then $R(U)$ equals the module over $\mathbb{Z}[P]$ generated by the set of points made in the first step of the construction. This lets us show that whenever the pairwise products of points made in the first step remain inside $R(U)$, it is closed under multiplication, and is thus a ring.

Acknowledgements: Thanks to Gregory Johnson for advising this research.

1 Introduction

When creating origami, sometimes one will fold the paper just to obtain the intersection point of two folds as a reference point. If we can fold only along certain angles through reference points, and only start with two points, what new reference points can be reached? To understand this, we'll consider the plane to be the complex plane, $\mathbb{C}$, and study an algebraic question about the reference points.

Suppose we are given a collection U of unit length elements of $\mathbb{C}$. If we have some collection of points in $\mathbb{C}$, we can draw lines through each of them with every angle in U (with respect to the real axis). In this way we can construct intersections of lines and repeat the process. Specifically, if we start with 0 and 1 in the complex plane and continue this construction indefinitely, when is the resulting collection of points, denoted $R(U)$, a subring of the complex numbers? Buhler et al. first introduced this question with a discussion of origami [1].

Note that even though we are drawing lines, only the intersection points, our reference points from before, are considered to be constructed. Throughout this paper, we assume that we can always draw a horizontal line, that is, $1 \in U$. Figure 1 illustrates the first two steps in the construction of $R(U)$ where $U = \{1, e^{i\pi/4}, e^{i\pi/2}\}$.

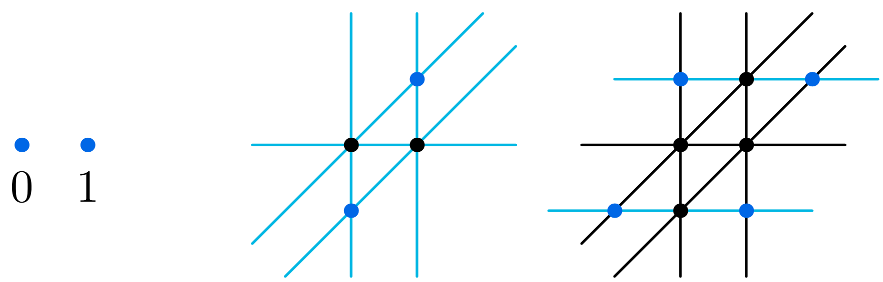

Figure 1: Construction of $R(U)$

It is known that $R(U)$ is a group. Specifically, it's a $\mathbb{Z}$-module generated by an infinite collection of points called monomials. We prove that $R(U)$ is also a module over $\mathbb{Z}[P]$, where we adjoin special points called projections. The generating set is the set of elementary monomials, which is finite whenever U is finite, unlike the set of all monomials. Effectively, the ring becomes more complicated, but the generating set is much simpler. This trade-off lets us compute and prove statements about $R(U)$ for specific sets of angles.

After some preliminary definitions in Section 2, we consider the case when $|U| = 3$ in Section 3. We prove that the set of reference points forms a lattice and use this fact to understand when the reference points form a ring. Next, in Section 4, we study the case when $|U| \geq 4$. In this case, the set of reference points are dense in the complex plane. We'll show three main results about the structure of $R(U)$. The first of these results states that $R(U) \cap \mathbb{R}$ is always a ring. In fact, this ring is generated by the real numbers formed in the second step of the construction of $R(U)$, called projections. We denote this ring $\mathbb{Z}[P]$ where

P is the set of projections. Next, we prove that $R(U)$ is exactly the $\mathbb{Z}[P]$-module generated by the set of points added in the first step of the construction. This leads us to our last result, that if every pairwise product of points from the first step of the construction lies in $R(U)$, then $R(U)$ is a ring. With this theorem, in Section 5 we consider certain sets of angles and prove that the corresponding sets of reference points are rings. Finally, in Section 6, we consider open questions that arose in our research.

2 Background and Definitions

We now formally define $R(U)$ and state some known results.

Definition 2.1. Let $p, q, \alpha, \beta \in \mathbb{C}$ with $|\alpha| = |\beta| = 1$. Define $L_\alpha(p)$ to be the line through p with angle α. In other words, $L_\alpha(p) \coloneqq p + \mathbb{R}\alpha$. Define $I_{\alpha,\beta}(p, q) \coloneqq L_\alpha(p) \cap L_\beta(q)$ when $\alpha \neq \pm\beta$ so that an intersection exists.

Definition 2.2. Let U be a set of unit magnitude complex numbers. Set $S_0 = \{0, 1\}$. For each $n \in \mathbb{N}$, set

$$S_{n+1} = \{I_{\alpha,\beta}(p, q) \mid \alpha, \beta \in U,\ p, q \in S_n, \text{ and } \alpha \neq \pm\beta\}.$$

We then define $R(U) = \bigcup_{n\in\mathbb{N}} S_n$.

Definition 2.3. Define $T \coloneqq \{z \in \mathbb{C} \mid |z| = 1\}$, which is viewed as a group under complex multiplication. We can use $T/\{\pm 1\}$ as the collection of angles, since α and β are considered equivalent if and only if $\alpha = \pm\beta$. Unless otherwise specified, $U \subseteq T/\{\pm 1\}$.

Definition 2.4. Given $U \subseteq T/\{\pm 1\}$, we define all elements $z \in R(U)$ of the form $I_{\alpha,\beta}(0, 1)$ to be elementary monomials, or length 1 monomials.

Next, if m is a length k monomial, then $I_{\alpha,\beta}(0, m) \in R(U)$ is a length $k + 1$ monomial. In this way we inductively define monomials.

Definition 2.5. Let $1 \in U$. The length 2 monomials on the real axis are called projections.

Proposition 2.6 (Buhler, Butler, de Launey, Graham [1])**.** *For $p, q \in \mathbb{C}$ and $\alpha \neq \beta \in T/\{\pm 1\}$,*

$$I_{\alpha,\beta}(p, q) = \frac{[\alpha, p]}{[\alpha, \beta]}\beta + \frac{[\beta, q]}{[\beta, \alpha]}\alpha,$$

where $[x, y] = x\bar{y} - y\bar{x}$ and $\bar{z}$ is the complex conjugate of z.

Proposition 2.7 (Buhler, Butler, de Launey, Graham [1])**.** *We list some properties of $I_{\alpha,\beta}(p, q)$ below for $w \in T/\{\pm 1\}$ and $r \in \mathbb{R}$.*

(Symmetry) $I_{u,v}(p, q) = I_{v,u}(q, p)$

(Reduction) $I_{u,v}(p, q) = I_{u,v}(p, 0) + I_{v,u}(q, 0)$

(Linearity) $I_{u,v}(rp+q,0) = rI_{u,v}(p,0) + I_{u,v}(q,0)$

(Rotation) *For* $w \in T/\{\pm 1\}$, $wI_{u,v}(p,q) = I_{wu,wv}(wp,wq)$

Lemma 2.8 (Buhler, Butler, de Launey, Graham [1]). *Let* $|U| \geq 3$ *with* $1 \in U$. *Then* $R(U)$ *is closed under addition and additive inverses.*

Theorem 2.9 (Buhler, Butler, de Launey, Graham [1]). *Let* $|U| \geq 3$. *Then* $R(U)$ *is the collection of integer linear combinations of monomials.*

Remark. Since $R(U)$ is a group under addition whenever $|U| \geq 3$, we need only check closure under multiplication to ensure that $R(U)$ is a ring.

Buhler et. al. then studied the case when U is a group [1]. Specifically, they took the set of unit magnitude complex numbers T, the unit circle, and considered it to be a group under complex multiplication. Then they took the quotient of T by $\{-1,+1\}$. The result can be viewed as the top half of the unit circle. By convention, whenever we use U, we will refer to $U \subseteq T/\{\pm 1\}$ where the elements are viewed as complex numbers.

Theorem 2.10 (Buhler, Butler, de Launey, Graham [1]). *Let* U *be a subgroup of* $T/\{\pm 1\}$ *with* $|U| \geq 3$. *Then,* $R(U)$ *is a ring.*

In their paper, Buhler et al. observed that $R(U)$ may be a ring even when U is not a group. They left the question of what properties U must satisfy exactly for $R(U)$ to be a group open.

3 Three Angles

In order to understand $R(U)$, first we look at $|U| = 3$ with $1 \in U$. We find that $R(U)$ has the structure of a lattice and can be understood in terms of one of the elementary monomials.

Lemma 3.1. *Let* $U = \{1, u, v\}$. *We claim that* $R(U)$ *is a lattice in* $\mathbb{C}$ *with the form* $R(U) = \mathbb{Z} + I_{u,v}(0,1)\mathbb{Z}$.

Proof. Set $x = I_{u,v}(0,1)$. From Lemma 2.8, we know that $R(U)$ is a subgroup of $\mathbb{C}$ with addition. Since $1 \in R(U)$ and $x \in R(U)$, we clearly see that $R(U) \supseteq \mathbb{Z} + x\mathbb{Z}$.

We will prove the other containment with induction. We know that $S_1 = \{x, 1-x, 0, 1\} \subseteq \mathbb{Z} + x\mathbb{Z}$. Let $p, q \in S_n$, which are assumed to be in $\mathbb{Z} + x\mathbb{Z}$. Let $\alpha, \beta \in U$.

We claim that $z = I_{\alpha,\beta}(p,q) \in \mathbb{Z} + x\mathbb{Z}$. Since $I_{\alpha,\beta}(p,q) = I_{\alpha,\beta}(p,0) + I_{\beta,\alpha}(q,0)$, it suffices to prove that $I_{\alpha,\beta}(a+bx,0) \in \mathbb{Z} + x\mathbb{Z}$. Further note that

$$\begin{aligned} I_{\alpha,\beta}(a+bx,0) &= I_{\alpha,\beta}(a,0) + I_{\alpha,\beta}(bx,0) \\ &= aI_{\alpha,\beta}(1,0) + I_{\alpha,\beta}(bx,0). \end{aligned}$$

by linearity.

$I_{\alpha,\beta}(1,0) \in S_1$, so $I_{\alpha,\beta}(1,0) = 1$, 0, x, or $1-x$. There are only four choices since if one of the angles is 0 radians, the resulting point is 0 or 1. If $\alpha, \beta \neq 1$, then there are two choices left, $\alpha = u, \beta = v$ or $\alpha = v, \beta = u$. One of these yields the point x and the other yields (by the parallelogram law) $1-x$. Thus $I_{\alpha,\beta}(a,0) \in \mathbb{Z} + x\mathbb{Z}$.

Next, note that $I_{\alpha,\beta}(bx,0) = bI_{\alpha,\beta}(x,0)$. Thus it suffices to prove that $I_{\alpha,\beta}(x,0) \in \mathbb{Z}+x\mathbb{Z}$. We have six cases.

(u,v) Since $x = ru$ for some $r \in \mathbb{R}$, $I_{u,v}(x,0) = rI_{u,v}(u,0) = 0 \in \mathbb{Z} + x\mathbb{Z}$.

(v,u) $I_{v,u}(x,0)$ is the projection of x onto the line ru in the direction of v, but $x \in \mathbb{R}u$, so $I_{v,u}(x,0) = x$.

$(u,1)$ $I_{u,1}(x,0)$ is the projection of x onto the real axis in the direction of u. It is easy to see that this must be 0, since the line from 0 (which is on the real axis) extending in the u direction intersects x.

$(v,1)$ $I_{v,1}(x,0) = 1$, for a similar reason. The line extending from 1 (which is on the real axis) in the v direction intersects x.

$(1,u)$ $I_{1,u}(x,0)$ is the line crossing through $x+s$ and ru for $s,r \in \mathbb{R}$, but since $x \in \mathbb{R}u$, this intersection is clearly at x.

$(1,v)$ $I_{1,v}(x,0)$ is at $x-1$ which is demonstrated by the fact that $I_{1,v}(x,0) + I_{v,1}(x,0) = x$ and $I_{v,1}(x,0) = 1$.

All of these points line in $\mathbb{Z}+x\mathbb{Z}$, so we have shown that $R(U)$ for $|U| = 3$ is of the form $\mathbb{Z}+x\mathbb{Z}$ where $x = I_{u,v}(0,1)$. □

Remark. Given $U = \{1,u,v\}$, if we find u', v' such that $I_{u',v'}(0,1) = m + I_{u,v}(0,1)$ for $m \in \mathbb{Z}$ and set $U' = \{1,u',v'\}$, by the above structural result, $R(U) = R(U')$.

Theorem 3.2 expands on this remark and shows when U and U' of size three generate the same lattice.

Theorem 3.2. *Let $I_{u,v}(0,1) = x$ and let $I_{u',v'}(0,1) = y$. Let $x = a+bi$ and $y = c+di$. Set $U = \{1,u,v\}$ and $U' = \{1,u',v'\}$. We claim that $R(U) = R(U')$ if and only if $b = \pm d$ and $a \mp c \in \mathbb{Z}$.*

Proof. If $\mathbb{Z}+x\mathbb{Z} = \mathbb{Z}+y\mathbb{Z}$ then $\{m+nx \mid m,n \in \mathbb{Z}\} = \{p+qy \mid p,q \in \mathbb{Z}\}$. For arbitrary $m,n \in \mathbb{Z}$, we have that $m+nx \in \{p+qy \mid p,q \in \mathbb{Z}\}$ holds if and only if $nx \in \mathbb{Z}+y\mathbb{Z}$, which is equivalent to $na+nbi = p+qc+qdi$ for some $p,q \in \mathbb{Z}$.

In order for this to hold, the imaginary parts must equal: $nbi = qdi$ (for any n, there is some q). Thus $d \mid b$ (using $n=1$). We can make the same argument swapping x and y, which tells us that $b \mid d$, so $b = \pm d$ and thus $n = \pm q$.

Also, the real parts must be equal: $na - qc = p$ (for any n there are such p,q). Above we determined that $n = \pm q$, so $n(a \mp c) = p$. Such a p exists for any n, so $a \mp c \in \mathbb{Z}$. We thus know that if $\mathbb{Z}+x\mathbb{Z} = \mathbb{Z}+y\mathbb{Z}$, then $b = \pm d$ and $a \mp c \in \mathbb{Z}$.

Now, if we assume that $b = \pm d$ and $a \mp c \in \mathbb{Z}$, then for any $\mathbb{Z} + x\mathbb{Z} = m + na + nbi$, we have

$$\begin{aligned} m + na + nbi &= m + n(k \pm c) + n(\pm d)i \\ &= (m + nk) \pm nc \pm ndi \in \mathbb{Z} + y\mathbb{Z}. \end{aligned}$$

This shows that $\mathbb{Z} + x\mathbb{Z} \subseteq \mathbb{Z} + y\mathbb{Z}$. Likewise, $\mathbb{Z} + y\mathbb{Z} \subseteq \mathbb{Z} + x\mathbb{Z}$.

Since $R(U) = \mathbb{Z} + x\mathbb{Z}$ and $R(U') = \mathbb{Z} + y\mathbb{Z}$, we have that $R(U) = R(U')$ if and only if $b = \pm d$ and $a \mp c \in \mathbb{Z}$, so $\mathbb{Z} + x\mathbb{Z} = \mathbb{Z} + y\mathbb{Z}$. □

Now that we understand what form $R(U)$ has for $|U| = 3$ with $1 \in U$, we can easily show exactly when $R(U)$ is a ring. The only point that gives any difficulty is x, one of the two elementary monomials off of the real line. If we can square this point and the result lies in $R(U)$, then $R(U) = \mathbb{Z} + x\mathbb{Z}$ must be closed under multiplication.

Now we characterize all U with $1 \in U$ and $|U| = 3$ such that $R(U)$ is a ring.

Theorem 3.3. *Let $U = \{1, u, v\}$ and let $I_{u,v}(0, 1) = x$. Then $R(U)$ is a ring if and only if x is a (non-real) quadratic integer, that is, x is the root of some monic integer quadratic polynomial.*

Proof. First we will prove that if x is a quadratic integer, then $R(U)$ is a ring. Note that $R(U) = \mathbb{Z} + x\mathbb{Z}$ where $x = I_{u,v}(0, 1)$. Since $R(U)$ is already a group, we need to show closure under multiplication. We write $(a + bx)(c + dx) = ac + (bc + ad)x + bdx^2$. Since x is a quadratic integer, $x^2 = \lambda x + \mu$ for some $\lambda, \mu \in \mathbb{Z}$. Then,

$$\begin{aligned} (a + bx)(c + dx) &= ac + (bc + ad)x + bd(\lambda x + \mu) \\ &= (ac + bd\mu) + (bc + ad + bd\lambda)x \end{aligned}$$

so in fact $R(U)$ is closed under multiplication.

Now assume that $R(U)$ is closed under multiplication and that $x \notin \mathbb{R}$, since otherwise $R(U)$ is degenerate. Then $(a + bx)(c + dx) \in \mathbb{Z} + x\mathbb{Z}$, but we can expand this:

$$(a + bx)(c + dx) = ac + (bc + ad)x + bdx^2 \in \mathbb{Z} + x\mathbb{Z}$$

Since $ac + (bc + ad)x \in \mathbb{Z} + x\mathbb{Z}$, we know that $bdx^2 \in \mathbb{Z} + x\mathbb{Z}$ for every $b, d \in \mathbb{Z}$. In particular, this holds for $b = d = 1$, so $x^2 \in \mathbb{Z} + x\mathbb{Z}$. In other words, x must be a quadratic integer. □

We can compute the intersection point x in terms of $\arg(u)$ and $\arg(v)$ and rephrase Theorem 3.3.

Corollary 3.4. *Let $\arg(U) = \{0, \theta, \phi\}$ with $\phi < \theta$. Then $R(U)$ is a ring if and only if*

$$\frac{\tan\theta}{\tan\theta - \tan\phi} + \frac{\tan\phi\tan\theta}{\tan\theta - \tan\phi}i$$

is a quadratic integer.

Proof. We can see from Figure 2 that

$$(1+w)\tan\phi = h = w\tan\theta,$$

so $w = \frac{\tan\phi}{\tan\theta - \tan\phi}$. Immediately, we see also that $h = \frac{\tan\phi\tan\theta}{\tan\theta-\tan\phi}$. Thus,

$$x = \frac{\tan\theta}{\tan\theta - \tan\phi} + \frac{\tan\phi\tan\theta}{\tan\theta - \tan\phi} i.$$

□

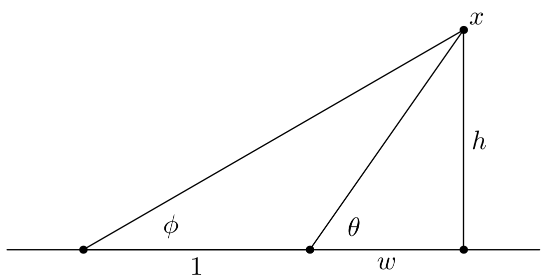

Figure 2: Relating angles when $\arg(U) = \{0, \theta, \phi\}$

Remark. Nedrenco independently characterized $R(U)$ where $|U| = 3$, describing $R(U) = \mathbb{Z} + x\mathbb{Z}$ and generalized to when $1 \notin U$ [2]. In the same paper, Nedrenco also noted that $R(U)$ is dense when $|U| = 4$. We present what we found independently.

4 Four or More Angles

Since we understood $R(U)$ for $|U| = 3$ in terms of an elementary monomial, we wish to understand $R(U)$ for $|U| \geq 4$ in terms of elementary monomials. Because $R(U)$ is now dense in the complex plane, we cannot hope for an integral basis. By linearity if we have some $p \in \mathbb{R} \cap R(U)$, then $I_{\alpha,\beta}(0,p) = pI_{\alpha,\beta}(0,1)$. This means we can scale points. This motivates our interest in "projections" onto the real axis.

Figure 3 depicts the construction of projections, each the intersection of a line through an elementary monomial and the horizontal line through 0.

Proposition 4.1. *Let $U = \{1, u, v, w\}$ with $\arg(u) < \arg(v) < \arg(w) < \pi$. There are at most eight length-two monomials on the real axis. Also, there are at most five length-two monomials constructed from elementary monomials of the form $I_{\alpha,\beta}(0,1)$ with $\arg(\alpha) < \arg(\beta)$. They are $0, 1, x, 1/x, x/(x-1)$ where $x = I_{v,1}(I_{u,w}(0,1), 0)$.*

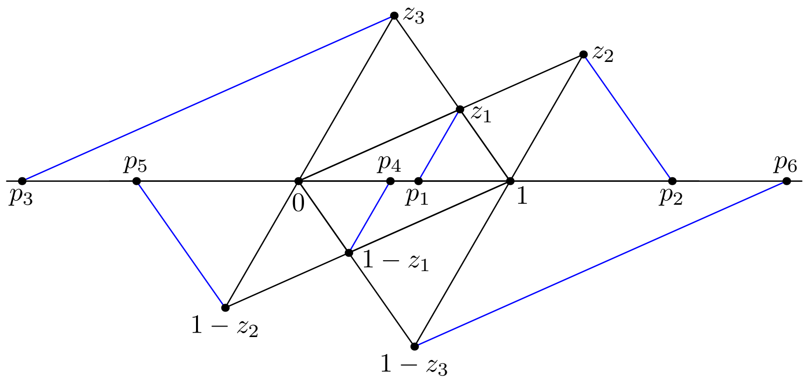

Figure 3: Construction of projections when $|U| = 4$

Proof. With the exception of 0 and 1, the only way to construct a length-two monomial on the real axis is to intersect a line through an elementary monomial and the line passing through 0 and 1. For any given elementary monomial, there are already two lines passing through the point: one passes through 0 and one passes through 1. Thus there can be at most six extra length-two monomials on the real axis, at most three of which are created from z_1, z_2, z_3 in the form described in the claim, and at most three of which are created from $1 - z_1, 1 - z_2, 1 - z_3$ which are of the opposite form.

Note that $p_1 = 1 - p_4$, $p_2 = 1 - p_5$, and $p_3 = 1 - p_6$. As proof, we calculate

$$\begin{aligned} I_{1,\alpha}(0, I_{\beta,\gamma}(0,1)) &= I_{1,\alpha}(0, 1 - I_{\gamma,\beta}(0,1)) \\ &= I_{1,\alpha}(0,1) - I_{1,\alpha}(0, I_{\gamma,\beta}(0,1)) \\ &= 1 - I_{1,\alpha}(0, I_{\gamma,\beta}(0,1)). \end{aligned}$$

Now we will show that the projections have the described form. Figure 4 depicts the various triangles referred to in this proof. Set $x = p_1$. Note that the triangle $(0, p_1, z_1)$ is similar to the triangle $(0, 1, z_2)$, so $\frac{p_1}{1} = \frac{z_1}{z_2}$. Also, the triangle $(0, 1, z_1)$ is similar to the triangle $(0, p_2, z_2)$, so $\frac{1}{p_2} = \frac{z_1}{z_2}$. Thus, $p_2 = 1/x$.

Next, the triangle $(0, p_1, z_1)$ is similar to the triangle $(p_3, 0, z_3)$, so $\frac{|z_1|}{|z_3 - p_3|} = \frac{|p_1|}{|p_3|}$. Also, the triangle $(0, 1, z_1)$ is similar to the triangle $(p_3, 1, z_3)$, so $\frac{|z_1|}{|z_3 - p_3|} = \frac{1}{|1 - p_3|}$. We conclude the following.

$$\begin{aligned} \frac{|x|}{|p_3|} &= \frac{1}{|1 - p_3|} \\ |p_3 - 1|\,|x| &= |p_3| \\ |p_3| &= \left|\frac{x}{x - 1}\right| \end{aligned}$$

To remove the absolute value signs, we note that since $\arg(z_3) > \arg(z_1)$, the line through

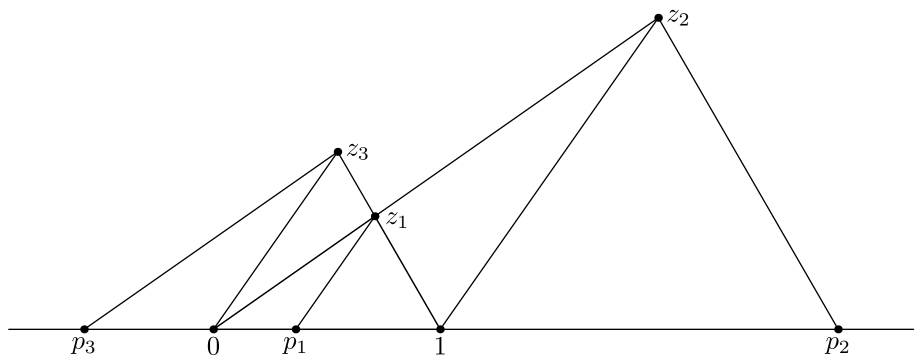

Figure 4: Similar triangles relating the projections when $|U| = 4$

z_3 with angle $\arg(z_1)$ must intersect the negative real axis, so $p_3 < 0$. Furthermore, since $x < 1$, $\frac{x}{x-1} < 0$, so we deduce that $p_3 = x/(x-1)$. □

Now that we understand a small amount of $\mathbb{R} \cap R(U)$, we can quickly construct an entire ring inside $\mathbb{R} \cap R(U)$ with the scaling mentioned earlier. Later we will show that what we construct next is exactly $\mathbb{R} \cap R(U)$

Proposition 4.2. *Let* $0 \in \arg(U)$ *with* $|U| \geq 4$. *Let* P *be the set of length-two monomials on the real axis. For any* $x \in R(U)$ *and any* $p \in P$, $px \in R(U)$. *As a result, the ring* $\mathbb{Z}[P]$ *is constructible, which is to say that* $\mathbb{Z}[P] \subseteq R(U)$.

Proof. Let p be a projection. Since $R(U)$ is the collection of finite linear combinations of monomials, it suffices to construct pm for a given monomial m, since if we have $x \in R(U)$, we can simply represent $x = \sum_{i=1}^{n} c_i m_i$ for $c_i \in \mathbb{Z}$ and then write $px = \sum_{i=1}^{n} c_i(pm_i)$.

The proof that $pm \in R(U)$ follows from linearity. Formally, we rely on induction.

Base Case: The length of m is one, so $m = I_{\alpha,\beta}(0, 1)$ for some $\alpha, \beta \in U$. Then, $pm = I_{\alpha,\beta}(0, p)$ by linearity, which is in $R(U)$ since $p \in R(U)$.

Inductive Step: Suppose every length $n-1$ monomial satisfies the claim. Let m be of length n. Then, $m = I_{\alpha,\beta}(0, q)$ for some length $n-1$ monomial q. By linearity, $pm = I_{\alpha,\beta}(0, pq)$ which is constructible since $pq \in R(U)$ by the inductive hypothesis.

Thus every monomial can be arbitrarily multiplied by projections, so in fact everything in $R(U)$ can be arbitrarily multiplied by projections. In particular, so can the projections themselves. This means that arbitrary powers of projections are in $R(U)$. Furthermore, since $R(U)$ is a group under addition, $\mathbb{Z}[P] \subseteq R(U)$. □

Remark. This holds even when $|U| > 4$.

Our current goal is to characterize all monomials in terms of $\mathbb{Z}[P]$ and elementary monomials. By Theorem 2.9, if the monomials have a nice enough form, we will be able to understand all of $R(U)$. Characterizing all monomials starts with the length two monomials. First, however, we need a quick lemma.

Lemma 4.3. *Let $0, \alpha, \beta \in \arg(U)$. Let $p, q \in R(U)$, and let $x = I_{\alpha,\beta}(p,q)$ and $y = I_{\beta,\alpha}(p,q)$. Then, $x = p + q - y$.*

Proof. Since the lines from x to q and from p to y are parallel, and also the lines from x to p and from q to y are parallel, this forms a parallelogram, as shown in Figure 5. It is clear that 0, $x - q$, $p - q$, and $y - q$ form a parallelogram and that $x - q + y - q = p - q$, so $x = p + q - y$. □

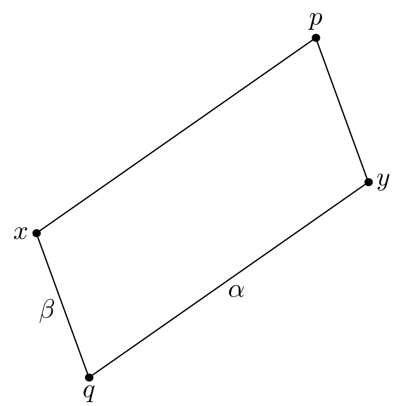

Figure 5: Relationship between $x = I_{\alpha,\beta}(p,q)$ and $y = I_{\beta,\alpha}(p,q)$

Lemma 4.4. *Let $|U| \geq 4$ and let $1 \in U$. Let P be the set of projections from the elementary monomials to the real axis along angles in U. Every length two monomial is a $\mathbb{Z}[P]$-linear combination of elementary monomials.*

Proof. Let $z = I_{\alpha,\beta}(0,1)$ for some $\alpha, \beta \in U$ and let our length two monomial $m = I_{\gamma,\delta}(0,z)$. We will prove that m is a $\mathbb{Z}[P]$-linear combination of elementary monomials by cases.

($\delta = 1$): Note that

$$I_{\gamma,0}(0,z) + I_{0,\gamma}(0,z) = z,$$

so $I_{\gamma,\delta}(0,z) = z - I_{0,\gamma}(0,z)$. Since $I_{0,\gamma}(0,z) \in P$, m is a $\mathbb{Z}[P]$-linear combination of elementary monomials.

($\delta = \alpha$): Since the line through $z = I_{\alpha,\beta}(0,1)$ with angle $\arg(\alpha)$ passes through the origin, $m = I_{\gamma,\alpha}(0,z) = 0$. This is trivially a $\mathbb{Z}[P]$-linear combination of elementary monomials.

($\delta = \beta$): Since the line through $z = I_{\alpha,\beta}(0,1)$ with angle $\arg(\beta)$ passes through 1, $m = I_{\gamma,\beta}(0,z) = I_{\gamma,\beta}(0,1)$, which is an elementary monomial.

($\delta \in U \setminus \{1, \alpha, \beta\}$): Let $p = I_{0,\gamma}(0,z)$ be the projection from z to the real axis in the direction of γ. Note that $I_{\gamma,\delta}(0,p) = pI_{\gamma,\delta}(0,1)$ by linearity.

Set $x = I_{\gamma,\delta}(0,p)$. We know that $x+z-p = m$, and since $x = pI_{\gamma,\delta}(0,1)$, this is enough to prove that m is a $\mathbb{Z}[P]$-linear combination of elementary monomials. Restated, the claim is that

$$I_{\gamma,\delta}(0, I_{0,\gamma}(0,z)) + z - I_{0,\gamma}(0,z) = I_{\gamma,\delta}(0,z).$$

To prove this, we will show that $I_{\gamma,\delta}(x,z) = m$. This follows by the fact that $x \in \mathbb{R}\gamma$, so the line through x with angle $\arg(\delta)$ also passes through 0 and thus $I_{\gamma,\delta}(x,z) = I_{\gamma,\delta}(0,z) = m$.

Furthermore, $I_{\delta,\gamma}(x,z) = p$. To see this, first note that $I_{\gamma,0}(z,0) = p$. Also, $I_{\delta,0}(x,0) = p$, because

$$I_{\delta,0}(x,0) = I_{\delta,0}(I_{\gamma,\delta}(0,p),0),$$

and both x and p lie along the same line through p with angle $\arg(\delta)$ by construction of x.

This means that x and z lie on opposite corners of a parallelogram which has a corner at p through the real axis and another corner through m. Thus, 0, $(x-p)$, $(z-p)$, and $(m-p)$ form the corners of a parallelogram and $(x-p)+(z-p)+p = m$ so $m = x+z-p$, concluding the proof.

Since in all cases m is a $\mathbb{Z}[P]$-linear combination of elementary monomials, we know that every length two monomial is of this form. □

Now that we understand length two monomials, we can apply induction to characterize all monomials, and thus all of $R(U)$.

Theorem 4.5. *Let $1 \in U$. Let P be the set of projections of elementary monomials along lines with angles from* $\arg(U)$ *onto the real axis. Then, every monomial in $R(U)$ is a $\mathbb{Z}[P]$-linear combination of elementary monomials. Indeed, $R(U)$ is the set of $\mathbb{Z}[P]$-linear combinations of elementary monomials.*

Proof. We will prove this by induction on the length of the monomial. Length one monomials are already elementary and length two monomials follow from the above theorem. Let m be length n and suppose that all length $n-1$ monomials are of this form. Then,

$$\begin{aligned} m &= I_{\alpha,\beta}(0,m') \\ &= I_{\alpha,\beta}(0, \sum_{i=1}^{k} c_i z_i) \\ &= \sum_{i=1}^{k} c_i I_{\alpha,\beta}(0,z_i) \\ &= \sum_{i=1}^{k} \left(c_i \sum_{j=1}^{\ell} d_i x_i \right) \end{aligned}$$

using linearity and the fact that all length two monomials are of this form. The c_i and d_i are in $\mathbb{Z}[P]$ and the x_i and z_i are elementary monomials. After simplification, it is easy to see that m is in fact a $\mathbb{Z}[P]$-linear combination of elementary monomials.

Since everything in $R(U)$ is an integer linear combination of monomials, everything in $R(U)$ is a $\mathbb{Z}[P]$-linear combination of elementary monomials.

Furthermore, since $\mathbb{Z}[P]$ is constructible by Proposition 4.2, and $pR(U) \subseteq R(U)$ for all $p \in P$, we can construct every $\mathbb{Z}[P]$-linear combination of elementary monomials. Thus, $R(U)$ equals the set of $\mathbb{Z}[P]$-linear combinations of elementary monomials. □

Remark. We can alternatively say that $R(U)$ is a $\mathbb{Z}[P]$-module in $\mathbb{C}$ generated by the elementary monomials.

As in the three angle case, understanding the structure of $R(U)$ leads us to understand when $R(U)$ is a ring in terms of products of elementary monomials. In fact Theorem 3.3 can be seen as a special case of the following theorem.

Theorem 4.6. *Let U with $|U| \geq 4$ and $0 \in \arg(U)$ and let P represent the collection of projections. $R(U)$ is a ring if and only if every pairwise product of elementary monomials is a $\mathbb{Z}[P]$-linear combination of elementary monomials.*

Proof. First note that $R(U)$ equals the collection of $\mathbb{Z}[P]$-linear combinations of elementary monomials. We know that the $\mathbb{Z}[P]$-linear combinations of elementary monomials are closed under multiplication if and only if every pairwise product of elementary monomials is a $\mathbb{Z}[P]$-linear combination of elementary monomials.

Assume that every pairwise product of elementary monomials is as above. Then, for any $x, y \in R(U)$, we write $x = \sum_{i=1}^{n} c_i x_i$ and $y = \sum_{j=1}^{m} d_j y_j$ for $c_i, d_j \in \mathbb{Z}[P]$ and x_i, y_j elementary monomials.

Then, $xy = \sum_{i,j} c_i d_j x_i y_j$. Since $x_i y_j$ is a $\mathbb{Z}[P]$-linear combination of elementary monomials, so is xy. Thus $R(U)$ is a ring.

Now, suppose that $R(U)$ is a ring. It must be closed under multiplication, so the pairwise product of elementary monomials must be in $R(U)$, but $R(U)$ is the $\mathbb{Z}[P]$-linear combinations of elementary monomials, so the claim holds. □

When we have four or more angles, we have at least one projection $p \in (0, 1)$, so we can construct points close to zero. Because elements of $R(U)$ scaled by p are still in $R(U)$ and $R(U)$ is a group, it is actually dense in $\mathbb{C}$ as we will prove below.

Theorem 4.7. *If $1 \in U$ and $|U| \geq 4$, then $R(U)$ is dense in $\mathbb{C}$.*

Proof. Since $R(U)$ is the set of $\mathbb{Z}[P]$-linear combinations of elementary monomials, if z is a non-real elementary monomial and $p \in \mathbb{Z}[P] \cap (0, 1)$, we can construct p^n and $p^n z$ which, informally, go to zero from two different directions.

Let $\varepsilon > 0$ and let $x \in \mathbb{C}$. Since $R(U)$ is a group under addition, we can construct $ap^{N_1} + bp^{N_2} z$ for all $N_1, N_2 \in \mathbb{N}$.

Since $p \in (0,1)$, we can find N_2 such that $\left|\operatorname{Im}(z)p^{N_2}\right| < \varepsilon/2$. To simplify the following expression, write $\theta = \operatorname{Im}(z)p^{N_2}$. Then there exists a unique $b \in \mathbb{Z}$ such that

$$b - 1 \leq \frac{\operatorname{Im}(x)}{\theta} \leq b.$$

So we can show that

$$\left|b \operatorname{Im}(z)p^{N_2} i - \operatorname{Im}(x)i\right| = |b\theta - \operatorname{Im}(x)| \leq \varepsilon/2.$$

Likewise we can find a, N_1 such that $\left|ap^{N_1} - \left(\operatorname{Re}(x) - bp^{N_2}\operatorname{Re}(p)\right)\right| < \varepsilon/2$. Once we have such $a \in \mathbb{Z}$ and $N_1 \in \mathbb{N}$, we have the following.

$$\begin{aligned}\left|ap^{N_1} + bp^{N_2}z - x\right| &= \left|ap^{N_1} + bp^{N_2}\operatorname{Re}(z) - \operatorname{Re}(x) + bp^{N_2}\operatorname{Im}(z)i - \operatorname{Im}(x)i\right| \\ &\leq \left|ap^{N_1} + bp^{N_2}\operatorname{Re}(z) - \operatorname{Re}(x)\right| + \left|bp^{N_2}\operatorname{Im}(z) - \operatorname{Im}(x)\right| \\ &< \varepsilon\end{aligned}$$

Since $ap^{N_1} + bp^{N_2}z \in R(U)$, and this holds for any $x \in \mathbb{C}$ and for every $\varepsilon > 0$, we can always find a point in $R(U)$ arbitrarily close to any point of $\mathbb{C}$. Thus, $R(U)$ is dense in $\mathbb{C}$.

□

5 Some U for Which $R(U)$ Is a Ring

Now we can use Theorem 4.6 to prove that $R(U)$ is a ring for a particular example of U.

Example 1. Let $U = \{1, e^{i\pi/6}, e^{i\pi/3}, e^{i\pi/2}\}$. Then $R(U)$ is a ring.

Proof. It suffices to show that all products of elementary monomials are $\mathbb{Z}[P]$-linear combinations of elementary monomials. Our elementary monomials are $0, 1, z_1, z_2, z_3, 1 - z_1, 1 - z_2, 1 - z_3$.

$$\begin{aligned} z_1 &= \frac{2\sqrt{3}}{3}e^{i\pi/6} \\ z_2 &= \sqrt{3}e^{i\pi/6} \\ z_3 &= 2e^{i\pi/3} \end{aligned}$$

First we calculate the projections and get $2/3, 3/2, -2$. Note that $\mathbb{Z}[2/3, 3/2, -2] = \mathbb{Z}[2/3, 3/2] = \mathbb{Z}[1/3, 1/2] = \mathbb{Z}[1/6]$.

We calculate all pairwise products of z_1, z_2, z_3, since calculating more would be redundant, as the others are either 0, 1, or an integer linear combination of $\{1, z_1, z_2, z_3\}$.

$$\begin{aligned} z_1^2 &= \frac{4}{3}e^{i\pi/3} = \frac{2}{3}z_3 \\ z_1z_2 &= 2e^{i\pi/3} = z_3 \\ z_1z_3 &= \frac{4}{\sqrt{3}}e^{i\pi/2} = \frac{4i}{\sqrt{3}} = 4(z_1 - 1) \\ z_2^2 &= z_1^2\frac{z_2^2}{z_1^2} = \frac{9}{4}\cdot\frac{2}{3}z_3 = \frac{3}{2}z_3 \\ z_2z_3 &= \frac{z_2}{z_1}z_1z_3 = 6(z_1 - 1) \\ z_3^2 &= z_1z_2z_3 = 6(z_1^2 - z_1) = 4z_3 - 6z_1 \end{aligned}$$

These are all in $R(U)$, so $R(U)$ is closed under multiplication and is a ring. □

Remark. We suspected that perhaps any subset U of a finite group containing a generator for that finite group would result in a ring. The following example shows that this cannot be necessary.

Example 2. Let $U = \{1, e^{i\pi/6}, e^{i\pi/4}, e^{i\pi/3}\}$. Then $R(U)$ is a ring.

Proof. As above, it suffices to show that the products of all elementary monomials are $\mathbb{Z}[P]$-linear combinations of elementary monomials. We go by the convention that $z_1 = I_{e^{i\pi/6},e^{i\pi/2}}(0,1)$, $z_2 = I_{e^{i\pi/6},e^{i\pi/3}}(0,1)$, and $z_3 = I_{e^{i\pi/3},e^{i\pi/2}}(0,1)$ and that p_1, p_2, p_3 are projections from z_1, z_2, z_3 to the real axis.

We calculate the following products.

$$\begin{aligned} z_1z_2 &= p_3(1 - z_3) \\ z_1z_3 &= -p_1z_2 - (p_2p_3)z_3 + 2p_3 \\ z_2z_3 &= -p_3z_2 - (p_2p_3)z_3 + 2p_2p_3 \\ z_1^2 &= p_1p_3(1 - z_3) \\ z_2^2 &= p_2p_3(1 - z_3) \\ z_3^2 &= -6z_2 - 3p_2p_3z_3 + 3p_3 \end{aligned}$$

□

Remark. We then suspected that any subset of a finite group might result in a ring. Our next result shows this too cannot be necessary.

Example 3. Let $U = \{1, e^i, e^{2i}, e^{3i}\}$. Then $R(U)$ is a ring.

This example is a special case of Theorem 5.1.

Remark. We strongly suspect that $R(\{1, e^{i\pi/5}, e^{i\pi/4}, e^{i\pi/3}\})$ is not a ring, so we suspect that it is not sufficient for U to just be a subset of a finite group.

Theorem 5.1. *Let $U = \{1, \alpha, \alpha^2, \alpha^3\}$. Then $R(U)$ is a ring.*

Proof. Set $z_1 = I_{\alpha,\alpha^3}(0,1)$, $z_2 = I_{\alpha,\alpha^2}(0,1)$, and $z_3 = I_{\alpha^2,\alpha^3}(0,1)$. Since the only elementary monomials are $0, 1, z_1, z_2, z_3, 1-z_1, 1-z_2, 1-z_3$, it suffices to check pairwise products of $\{z_1, z_2, z_3\}$.

Set $p_1 = I_{1,\alpha^2}(0, z_1)$, $p_2 = I_{1,\alpha^3}(0, z_2)$, and $p_3 = I_{1,\alpha}(0, z_3)$. Then $\mathbb{Z}[P] = \mathbb{Z}[p_1, p_2, p_3]$, since the other projections are 0, 1, $1 - p_1$, $1 - p_2$, and $1 - p_2$.

First we claim that $z_1 z_2 = z_3$. We will prove this by calculation.

$$\begin{aligned} z_1 z_2 &= \frac{[1,\alpha^3]}{[\alpha,\alpha^3]}\frac{[1,\alpha^2]}{[\alpha,\alpha^2]}\alpha^2 \\ &= \frac{e^{-3i\theta}-e^{3i\theta}}{e^{-2i\theta}-e^{2i\theta}}\frac{e^{-2i\theta}-e^{2i\theta}}{e^{-i\theta}-e^{i\theta}} \\ &= \frac{[1,\alpha^3]}{[\alpha,\alpha^2]}\alpha^2 = \frac{[1,\alpha^3]}{[\alpha^2,\alpha^3]}\alpha^2 \\ &= z_3 \end{aligned}$$

Next we claim that $z_1/z_2 = p_1$ and $z_2/z_1 = p_2$. These can also be calculated, but Figure 6 should make it clear.

The first claim follows from the fact that the triangles $0-p_1-z_1$ and $0-1-z_2$ are similar. The second claim follows from the similarity of the triangles $0-1-z_1$ and $0-p_2-z_2$.

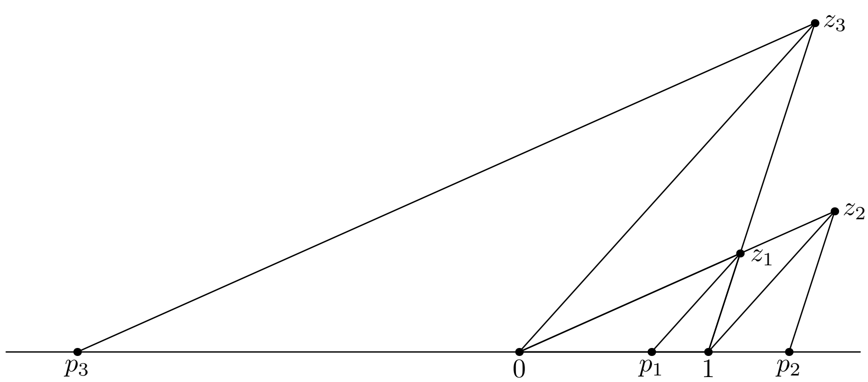

Figure 6: Similarity of triangles in $R(\{1, \alpha, \alpha^2, \alpha^3\})$

So far we can construct the following pairwise products of elementary monomials.

$$\begin{aligned} z_1^2 &= z_1 z_2 \frac{z_1}{z_2} = p_1 z_3 \\ z_1 z_2 &= z_3 \\ z_2^2 &= p_2^2 p_1 z_3 = p_2 z_3 \end{aligned}$$

We need only construct z_3^2 and $z_2 z_3$ since $z_1 z_3 = p_1 z_2 z_3$.

First we show $z_3^2 = p_3^2(z_3 - z_2)$ algebraically. We calculate z_3^2 using the formula given in Proposition 2.6 and obtain

$$z_3^2 = 1 + 2\alpha^2 + 3\alpha^4 + 2\alpha^6 + \alpha^8$$

which is exactly what we find by calculating $p_3^2(z_3 - z_2)$, so the two are equal.

Likewise, we calculate $z_2 z_3$ to be

$$z_2 z_3 = 1 + 2\alpha^2 + 2\alpha^4 + \alpha^6$$

which precisely equals $p_3(1 - z_3)$.

Thus all 6 pairwise products of $\{z_1, z_2, z_3\}$ are $\mathbb{Z}[P]$-linear combinations of elementary monomials, so $R(U)$ is a ring. □

6 Conclusion

Previously, it was known that $R(U)$ was a $\mathbb{Z}$ module generated by monomials. We have replaced the ring with $\mathbb{Z}[P]$ and the generating set by elementary monomials, so $R(U)$ is a $\mathbb{Z}[P]$-module generated by elementary monomials. This lets us understand $R(U)$ after only two steps of the construction and simplifies checking of examples.

We showed this by first showing that elements of $R(U)$ could be scaled by real numbers in $R(U)$, which implies that $\mathbb{Z}[P]$ is constructible. Next we showed that degree two monomials are $\mathbb{Z}[P]$-linear combinations of elementary monomials. This let us show by induction that all monomials are of this form. Since the monomials generate $R(U)$ over the ring $\mathbb{Z}$, we concluded that $R(U)$ is the set of $\mathbb{Z}[P]$-linear combinations of elementary monomials.

This characterization of $R(U)$ makes finding examples of rings $R(U)$ a matter of verifying that finitely many products are contained in $R(U)$. In some cases, this can be done quickly with computer aid. However, finding counter-examples is still difficult, as proving that products stay outside of $R(U)$ involves solving linear equations over an arbitrary ring, which can be non-trivial.

Some U that are very difficult to work with like $\{1, e^i, e^{2i}, e^{3i}\}$ yield rings, while other nicer sets like $\{1, e^{i\pi/5}, e^{i\pi/4}, e^{i\pi/3}\}$ are suspected to not yield rings. It is unknown how our current conditions on the elementary monomials translate into conditions on U. Some open questions are posed below.

1. How does $1 \notin U$ affect our current results? Can we still express $R(U)$ as a module over some ring generated by elementary monomials?

2. When exactly are the products of elementary monomials $\mathbb{Z}[P]$-linear combinations of elementary monomials in terms of the set U?

3. Is $R(\{1, e^{i\pi/5}, e^{i\pi/4}, e^{i\pi/3}\})$ a ring?

4. Are there non-rings for any $|U|$?

5. What subrings of $\mathbb{C}$ are of the form $R(U)$ for some U?

6. Given $p \in \mathbb{C}$, for which U is $p \in R(U)$?

7. We can write $I_{u,v}(p,q) = \frac{[u,p]}{[u,v]}v + \frac{[v,q]}{[v,u]}u$ where $[x,y] = x\bar{y} - y\bar{x}$. Note that $[x,y]$ is an alternating bilinear map. If V is some vector space equipped with $[\cdot,\cdot]$, an alternating bilinear map into $\mathbb{C}$ and we have some $S \subseteq V$ of allowable "angles", we can define $I : S^2 \times V^2 \to V$ via

$$I_{u,v}(p,q) = \frac{[u,p]}{[u,v]}v + \frac{[v,q]}{[v,u]}u$$

Do similar results hold for this generalization? Perhaps we could require V to be a complex normed vector space and say that S is the sphere of radius one.

References

[1] Joe Buhler, Steve Butler, Warwick de Launey and Ron Graham, 'Origami rings', *Journal of the Australian Mathematical Society* **92** (June 2012), 299–311.

[2] D. Nedrenco, 'On origami rings', *arXiv:1502.07995* (February 2015).