J. Aust. Math. Soc. (First published online 2012), page 1 of 13*
doi:10.1017/S1446788711001741
*Provisional—final page numbers to be inserted when paper edition is published

ORIGAMI RINGS

JOE BUHLER, STEVE BUTLER ✉, WARWICK DE LAUNEY and RON GRAHAM

(Received 12 November 2010; accepted 21 August 2011)

Communicated by L. M. Batten

Abstract

Motivated by mathematical aspects of origami, Erik Demaine asked which points in the plane can be constructed by using lines whose angles are multiples of π/n for some fixed n. This has been answered for some specific small values of n including $n = 3, 4, 5, 6, 8, 10, 12, 24$. We answer this question for arbitrary n. The set of points is a subring of the complex plane $\mathbf{C}$, lying inside the cyclotomic field of nth roots of unity; the precise description of the ring depends on whether n is prime or composite. The techniques apply in more general situations, for example, infinite sets of angles, or more general constructions of subsets of the plane.

2010 *Mathematics subject classification*: primary 11R04.
Keywords and phrases: origami, rings, cyclotomic fields, binary hybridization.

1. Introduction

Origami constructions start with a flat sheet of paper and end with a three-dimensional figure through a series of folds. Some of the folds produce creases or pleats, whereas others produce reference points needed for further folds. Information about practical origami design, including amazing origami creations, can be found in [5]; various mathematical aspects of origami can be found, for example, in [1, 2, 4].

The sets of reference points that can be constructed under various assumptions have been studied for theoretical reasons—for example, solving quartic equations [3, pp. 285–291]—or for more practical reasons—for example, approximating desired reference points [6].

We will consider an idealized form of paper folding and determine the set of reference points that can be constructed by folds chosen from a fixed set of directions (that is, angles), where new points are intersections of folds through points that have already been constructed. As observed in [7], this is a more limited set of assumptions (axioms) than is sometimes used in mathematical origami. As a basic example,

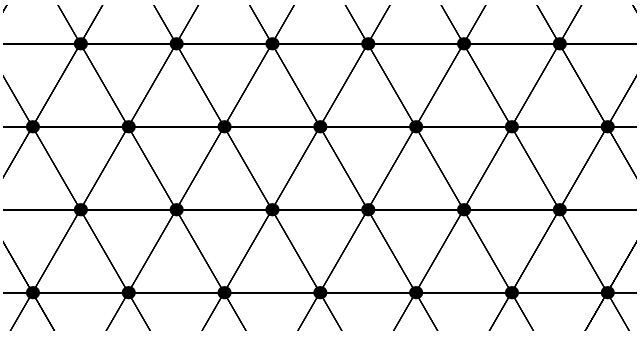


FIGURE 1. The hexagonal lattice $\mathbf{Z}[\zeta_3]$.

the set of all points constructible from the points 0 and 1 with angles chosen from $\{0, \pi/3, 2\pi/3\}$ is the hexagonal lattice $\mathbf{Z}[\zeta_3]$ in the complex plane $\mathbf{C}$ (see Figure 1), as the reader may enjoy verifying.

Erik Demaine raised the general version of this question: given an integer $n \geq 3$, what is the smallest set S of points of the complex plane that contains 0 and 1 and is closed under the operation of taking intersections of lines, through two points in S, of distinct slopes which are multiples of π/n? The case $n = 8$ was answered in [7], and the cases $n = 3, 4, 5, 6, 8, 10, 12, 24$ were found by Butler, Demaine, Graham and Tachi (work in preparation).

Our first goal here is to show that if U is a group of angles, finite or infinite, then the set of points constructed in this way (starting with just the two points 0 and 1) is a subring $R(U)$ of the complex plane. The techniques, and explicit description of $R(U)$, then enable us to answer Demaine's question for all n.

In order to state these results precisely, we now introduce some notation that will be used throughout the paper.

For us, an origami fold is a line in the complex plane. A line is determined by a point p on the line and a direction. A direction is determined by a nonzero complex number u, and the line through p with direction u is

$$L_u(p) := \{p + ru : r \in \mathbf{R}\}.$$

Two nonzero complex numbers determine the same direction if they are real scalar multiples of each other, so we will assume that direction vectors are complex numbers of absolute value 1, where the horizontal line has direction 1. Moreover, u and $-u$ determine the same direction. Thus direction vectors will be understood to lie in the circle group $\mathbf{T}$ of complex numbers of absolute value 1 (under multiplication), and the direction of a fold or line will be taken to be an element of the quotient group $\mathbf{T}/\{\pm 1\}$ of $\mathbf{T}$ by its subgroup $\{\pm 1\}$ of order two. We will assume throughout that a set U of direction vectors is closed under negation, and let $V = U/\{\pm 1\}$ be the corresponding set of folds. Note if a set of folds V has n elements, then the corresponding set of unit

direction vectors U has $2n$ elements. The reader could, alternatively, choose to identify $\mathbf{T}/\{\pm\}$ with the group $\mathbf{R}/\pi\mathbf{Z}$ of real numbers in $[0, \pi)$ under addition modulo π, where θ would correspond to $e^{i\theta}$ in the formulas to follow. In this setting, the horizontal line has angle 0. Note that addition of angles, in the usual geometric sense, corresponds to multiplication in the groups V and U.

It is natural to restrict attention to U and V that are subgroups of $\mathbf{T}$ (that is, closed under multiplication) since this holds in Demaine's context, is pleasant from the point of view of symmetry, and turns out to allow for a natural proof that the set $R(U)$ of constructed points is closed under multiplication. However, some of what we do (for example, the closure of $R(U)$ under addition) does not require that U be a group, and it would be interesting to consider arbitrary sets of angles.

If V_n is the cyclic group of order n generated by (the class of) $e^{i\pi/n} \bmod \{\pm 1\}$ then the corresponding group of direction vectors U_n is the cyclic group of order $2n$ generated by $e^{i\pi/n}$. The reader can check that if U is a group of directions and V is the corresponding group of folds then V is isomorphic to the group U^2 of squares in U.

If directions u and v determine distinct folds (that is, $u \neq \pm v$), let

$$I_{u,v}(p, q) := L_u(p) \cap L_v(q)$$

be the unique point on the intersection of the lines $L_u(p)$ and $L_v(q)$.

If $U \subset \mathbf{T}$ is a group of directions then let $R(U)$ be the set of points that can be obtained by repeatedly forming intersections $I_{u,v}(p, q)$, where u and v are arbitrary distinct elements of U, and p and q are known points; initially the only known points are 0 and 1. It is easy to check that $R(U)$ could also be defined to be the smallest subset of the complex plane that contains 0 and 1, and contains $I_{u,v}(p, q)$ whenever it contains p and q, and u, v are distinct elements of U.

THEOREM 1.1. *With the above notation, if the group V of folds has at least three elements (so that U has at least six elements) then $R(U)$ is a subring of $\mathbf{C}$, consisting of all integral linear combinations of arbitrary finite products of complex numbers of the form*

$$\frac{1 - u^2}{1 - v^2}$$

where u and v are in U. (Note that $u^2 \in \mathbf{T}$ is independent of the choice of representative of the class of $u \in \mathbf{T}/\{\pm 1\}$.)

Our other main result uses this theorem, together with results about cyclotomic fields, to answer Demaine's original question about V_n and describe $R(U)$ explicitly when U is finite. The key fact is that the quotients above are cyclotomic units when n is prime, and units outside the primes lying over n if n is not a prime.

THEOREM 1.2. *Let $n \geq 3$. If n is prime, then $R(U_n) = \mathbf{Z}[\zeta_n]$ is the cyclotomic integer ring. If n is not prime then $R(U_n) = \mathbf{Z}[\zeta_n, 1/n]$ is obtained from the ring of integers by inverting n (that is, localizing the ring away from the primes dividing n).*

This generalizes the $n = 3$ result depicted in Figure 1. However, that case is a bit of an outlier; later we will see that the theorem implies that for all $n > 3$, $R(U_n)$ is a dense subset of the complex plane. Finally, we note that the theorem implies that even though elements of $R(U_n)$ are found by intersecting lines whose directions are powers of ζ_{2n}, their coordinates lie in $\mathbf{Q}(\zeta_n)$.

2. Plane intersections

In order to investigate the points that are constructible from a given set of folds we will need to understand intersections in detail. The goal of this section is to give explicit formulas for $I_{u,v}(p, q)$ and then investigate the properties of this operation, from both algebraic and geometric perspectives.

Let u, v be distinct directions, and consider the lines $L_u(p)$ and $L_v(q)$. The intersection of these lines is the point $I_{u,v}(p, q)$ that is the unique solution z to

$$z = p + ru = q + sv,$$

for real numbers r and s. Since $s = v^{-1}(p - q + ru)$ is real, we can take the imaginary part to get an equation that can be solved for r:

$$r = \frac{\mathrm{Im}((q - p)/v)}{\mathrm{Im}(u/v)}.$$

It is convenient to introduce the notation

$$s_{x,y} = xy^* - x^*y = 2i|y|^2 \,\mathrm{Im}(x/y)$$

where x^* denotes the complex conjugate of x, and $|y|^2 = y^*y$. Note that $s_{\cdot,\cdot}$ is antisymmetric, and real-linear in each component. We can rewrite the equation for r in the form

$$r = \frac{s_{q-p,v}}{s_{u,v}}.$$

This gives

$$I_{u,v}(p, q) = p + \frac{s_{q-p,v}}{s_{u,v}}u = \frac{s_{u,v}p + s_{q,v}u - s_{p,v}u}{s_{u,v}}.$$

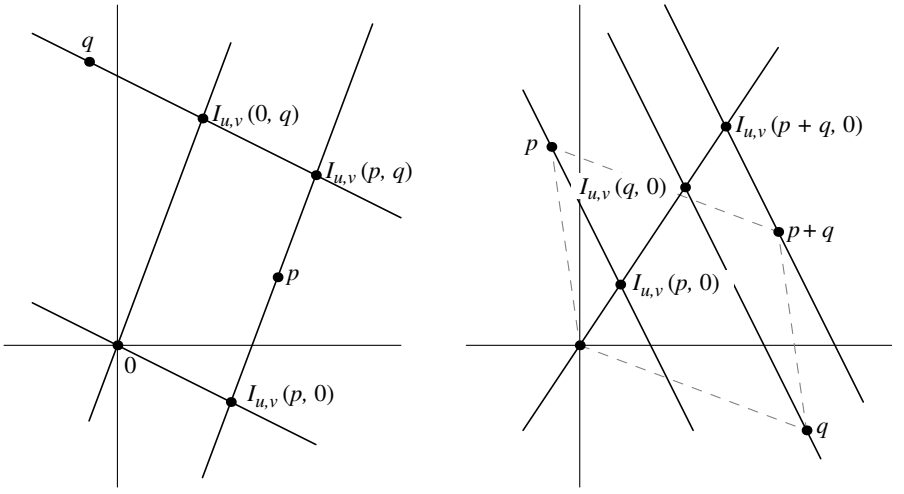
Substituting the definition and doing some algebraic juggling leads to a fundamental formula:

$$I_{u,v}(p, q) = \frac{up^*v - u^*pv - vq^*u + v^*qu}{s_{u,v}} = \frac{s_{u,p}}{s_{u,v}}v + \frac{s_{v,q}}{s_{v,u}}u. \tag{2.1}$$

A number of basic facts follow from these formulas.

Proposition 2.1. *Let p, q be points in the plane, and u, v be pairwise distinct directions.*

- *(Symmetry) $I_{u,v}(p, q) = I_{v,u}(q, p)$.*
- *(Reduction) $I_{u,v}(p, q) = I_{u,v}(p, 0) + I_{u,v}(0, q)$.*



(a) Law of parallelograms (b) Projection

FIGURE 2. Properties of $I_{u,v}(p, q)$.

- *(Projection)* $I_{u,v}(p, 0)$ *is a projection of* p *onto the line* $\{rv : r \in \mathbf{R}\}$ *in the direction* u.
- *(Linearity)* $I_{u,v}(p + q, 0) = I_{u,v}(p, 0) + I_{u,v}(q, 0)$ *and, for real* r, $I_{u,v}(rp, 0) = r\, I_{u,v}(p, 0)$.
- *(Convexity)* $I_{u,v}(p, q)$ *has the form* $Ap + Bq$ *where* A *and* B *are real-linear maps of the complex plane that satisfy* $A + B = 1_{\mathbf{C}}$, *where* $1_{\mathbf{C}}$ *is the identity map on the plane.*
- *(Rotation) For* $w \in \mathbf{T}$, $wI_{u,v}(p, q) = I_{wu,wv}(wp, wq)$.

The projection of p onto a line L in the direction u is the point of the form $p + ru$ that lies on the line L.

Using identity (2.1) to verify the facts in the proposition is a straightforward algebraic exercise which we leave to the reader. However, these facts can also be verified geometrically, as we now briefly sketch.

Symmetry follows from the fact that both sides of the equation solve the same intersection problem. Reduction is the law of parallelograms (see Figure 2(a)). Projection follows from a straightforward diagram. Linearity follows from projection and the fact that projections are linear (see Figure 2(b)). Convexity follows from reduction, the fact that each term in the reduction formula is a projection, and the fact that if $p = q$ then $I_{u,v}(p, q) = p$. (Note that the linear maps A, B have rank one, since they are projections.) Rotation expresses the fact that if the points and directions of an intersection problem are all rotated by multiplying by $w \in \mathbf{T}$ then the result is also rotated by w.

Real-linear maps of the complex plane can be written as

$$p \to p' = ap + bp^*$$

for complex constants a, b, or as maps taking $p = x + iy$ to $p' = x' + iy'$ written in terms of two by two matrices:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

where a, b, c, d are real. The intersection $I_{u,v}(p, q)$ can be given a purely trigonometric formula. Indeed, if $u = e^{i\alpha}$ and $v = e^{i\beta}$ are directions with angles α and β, let

$$A_{\alpha,\beta} = \begin{pmatrix} \dfrac{\sin(\alpha)\cos(\beta)}{\sin(\alpha-\beta)} & \dfrac{-\cos(\alpha)\cos(\beta)}{\sin(\alpha-\beta)} \\ \dfrac{\sin(\alpha)\sin(\beta)}{\sin(\alpha-\beta)} & \dfrac{-\cos(\alpha)\sin(\beta)}{\sin(\alpha-\beta)} \end{pmatrix}.$$

Then if $p = p_1 + ip_2$, $q = q_1 + iq_2$ then

$$I_{u,v}(p, q) = A_{\alpha,\beta} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} + A_{\beta,\alpha} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}.$$

It is easy to check that $A_{\alpha,\beta}$ has rank one, and that $A_{\alpha,\beta} + A_{\beta,\alpha}$ is the identity.

The intersection map, thought of as a binary operator on points p, q, has the form

$$I_{u,v}(p, q) = Ap + Bq$$

where $A + B = 1_{\mathbf{C}}$. We call this 'convexity' by analogy with convex combinations in real vector spaces, where x, y are mapped to $tx + (1 - t)y$, with $t \in [0, 1]$. Many of the ideas and results of this paper can be generalized by replacing 'intersection of lines of angles chosen from a fixed set' by considering binary operators

$$p, q \to Ap + Bq$$

(dubbed 'binary hybridization' operators by de Launey) where A, B range over a fixed set of functions from the plane to itself such that $A + B$ is the identity map. These arguments are somewhat more elaborate, and require additional hypotheses on the set of A, B. For the sake of expository simplicity we stick to the concrete case of intersections of lines described above.

3. Closure under addition and multiplication

Recall, for a fixed group U of directions, that $R(U)$ denotes the smallest set of complex numbers that contains 0 and 1 and has the property that if u, v are distinct elements of U, and p, q are elements of $R(U)$, then $I_{u,v}(p, q)$ is in $R(U)$. We now want to prove that if U determines at least three folds then $R(U)$ is a subring of $\mathbf{C}$, that is, that $R(U)$ is closed under addition, negation, and multiplication. We consider each of these operations separately.

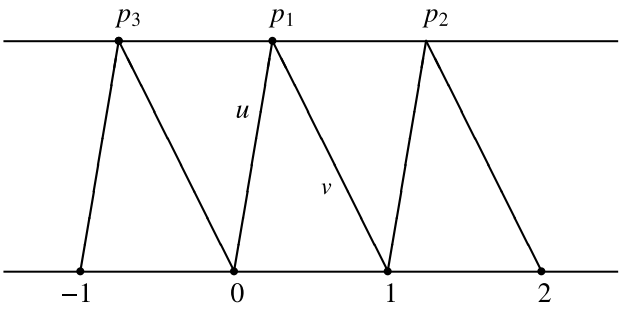


FIGURE 3. -1 and 2.

THEOREM 3.1. *If U is a subgroup of $\mathbf{T}$ that contains ± 1 and has at least six elements, then $R(U)$ is a group under addition.*

PROOF. First, we prove that 2 and -1 are in $R(U)$. Since there are at least three lines determined by the directions in U, there are directions u and v such that the six numbers $\pm 1, \pm u, \pm v$ are all distinct. Use u and v to construct a point $p_1 = I_{u,v}(0, 1)$ lying off the horizontal axis (see Figure 3). Then construct $p_2 = I_{u,1}(1, p_1)$ on a horizontal line through p_1. It is then easy to verify algebraically (and obvious geometrically) that

$$2 = I_{1,v}(0, p_2).$$

Similarly, if $p_3 := I_{v,1}(0, p_1)$ then one can check that

$$-1 = I_{1,u}(0, p_3).$$

Next, we show that if p is in $R(U)$ then so is $p + 1$. Indeed, apply the steps that were used to construct p starting from 0 and 1, but instead starting at the points 1 and 2; the result is $p + 1$.

Similarly, if p and q are in $R(U)$ then so is their sum: repeating the steps used to construct q, starting from p and $p + 1$, gives $p + q$.

Finally, by linearity we see that if p is in $R(U)$ then the same steps that lead to p from 0 and 1 will lead to $-p$ from 0 and -1. □

Now we turn to multiplication. A point p is said to be a *primitive monomial* if it can be constructed in one step from 0 and 1, that is,

$$p = I_{u,v}(0, 1)$$

for some u, v in U. More generally, a point p in $R(U)$ is said to be a *monomial* (or, if the emphasis is needed, a U-monomial) if it can be produced starting at 1 using only intersections of the form $I_{u,v}(*, 0)$, that is, intersections in which the second line is required to go through the origin. Thus a monomial lies in a sequence of the form

$$p_1 = I_{u_1,v_1}(1, 0), \quad p_2 = I_{u_2,v_2}(p_1, 0), \quad p_3 = I_{u_3,v_3}(p_2, 0), \ldots .$$

If $p = p_k = I_{u_k,v_k}(p_{k-1}, 0)$ occurs at the kth step, then p is said to be a monomial of length at most k. In terms of the linear operators A in the convexity property, this could be written

$$p = A_k A_{k-1} \cdots A_2 A_1 1$$

where A_i is the linear operator occurring in the ith step.

LEMMA 3.2. *The product of two monomials is a monomial. Any monomial is a product of elementary monomials.*

PROOF. Given u and v in U, let $r = [u, 1]/[u, v] \in \mathbf{R}$. Then $I_{u,v}(0, 1) = rv$ from our earlier formulas. Using rotation and linearity gives

$$\begin{aligned} I_{u,v}(1, 0)I_{u',v'}(1, 0) &= rv\, I_{u',v'}(1, 0) = r\, I_{vu',vv'}(v, 0) = I_{vu',vv'}(rv, 0) \\ &= I_{vu',vv'}(I_{u,v}(1, 0), 0). \end{aligned}$$

This shows that the product of two elementary monomials is a monomial, and (read in reverse) that a monomial of length two is a product of elementary monomials. The claims in the lemma follow by easy induction arguments on the length of the monomials. □

Note that this lemma was the first use of the rotation property, and the first use of the fact that U is a group under multiplication.

THEOREM 3.3. *If U is a group of directions that determine at least three folds, then $R(U)$ is the set of integral linear combinations of U-monomials and is therefore a subring of the complex numbers.*

PROOF. Let S be the set of all such linear combinations. Since the product of monomials is a monomial, S is obviously a ring.

Since $R(U)$ contains all monomials and is a group under addition, $R(U)$ contains S. Conversely, if r is an element of $R(U)$ then it has the form $r = I_{u,v}(p, q) = I_{u,v}(p, 0) + I_{u,v}(0, q)$. If p and q can be written as integral linear combinations of monomials of lengths at most k then, by linearity, r is an integral linear combination of monomials of length at most $k + 1$. The implicit induction argument shows that $R(U)$ is contained in S, finishing the proof. □

With a bit more work, these results can be extended to suitable binary hybridization operators described above, with similar proofs. For instance, if (A_i, B_i) are a collection of (pairs of) linear operators on the plane, satisfying $A_i + B_i = I$ for all i, then the set of points S that they generate, starting from 0 and 1, is an additive group if 2 lies in S. If the set of operators is (in a suitable sense) rotationally invariant and reversible, then the set of monomials is a subgroup of the multiplicative group $\mathbf{C}^\times$ of nonzero complex numbers, and the set S of points is closed under multiplication.

4. Finite groups of folds

Throughout this section let U be a group of directions that determine at least three folds, and let U_n denote the cyclic group of order $2n$ of directions generated by $e^{i\pi/n}$, for $n \geq 3$.

Monomials are products of elementary monomials. Elementary U-monomials have the form $I_{u,v}(1,0) = ([u,1]/[u,v])v$, which is a real number

$$\frac{[u,1]}{[u,v]} = \frac{\sin(\alpha)}{\sin(\alpha-\beta)}, \quad u = e^{i\alpha}, v = e^{i\beta},$$

multiplied by an element of U. In addition, we note that

$$I_{u,v}(1,0) = \frac{s_{u,1}}{s_{u,v}}v = \frac{u-u^*}{u(v^*)^2-u^*} = \frac{1-u^2}{1-(u/v)^2}$$

so that as u and v range over all elements of U, elementary monomials range over all complex numbers of the form $(1-a)/(1-b)$ where a and b range over all nontrivial distinct elements of the square group U^2. By reversing a and b we see that these quotients are obviously invertible in the ring $R(U)$, and therefore any monomial is a unit in $R(U)$.

This proves the following result.

THEOREM 4.1. *Let U determine at least three folds (that is, have order at least six). Then $R(U)$ is the smallest subring of $\mathbf{C}$ that contains all elements of the form*

$$\frac{1-a}{1-b}$$

for distinct nontrivial elements a and b of U^2. Moreover, these monomials are units in $R(U)$.

Now we turn to the case of finite groups U for which we will use cyclotomic fields (see [8]). Recall that the cyclotomic field $\mathbf{Q}(\zeta_n)$ is the smallest subfield of $\mathbf{C}$ that contains the primitive nth root of unity $\zeta_n := e^{2\pi i/n}$, and that it consists of the polynomials in ζ_n with rational coefficients,

$$\mathbf{Q}(\zeta_n) = \{f(\zeta_n) : f[X] \in \mathbf{Q}[X]\}.$$

The group U_n is generated by $\zeta_{2n} = e^{i\pi/n}$, the corresponding group V_n of folds is of order n, and the group U_n^2 of squares is generated by ζ_n. Thus the preceding theorem implies the following corollary.

COROLLARY 4.2. *The ring $R(U_n)$ is a subring in $\mathbf{Q}(\zeta_n)$.*

Note that this is slightly curious: the points in $R(U_n)$ result from intersections with lines whose direction vectors are powers of ζ_{2n} and yet the intersections lie in $\mathbf{Q}(\zeta_n)$. (Of course, this is only surprising if n is even, since if n is odd then $\mathbf{Q}(\zeta_{2n}) = \mathbf{Q}(\zeta_n)$.)

For prime n, the quotients

$$m_{a,b} := (1 - \zeta_n^a)/(1 - \zeta_n^b)$$

are familiar from algebraic number theory—they are examples of so-called cyclotomic units in $\mathbf{Q}(\zeta_n)$. In any case they lie in the ring $\mathbf{Z}[\zeta_n]$ of algebraic integers (polynomials in ζ_n with integer coefficients) in that field. Thus $R(U)$ is contained in $\mathbf{Z}[\zeta_n]$ and it is not hard to see that $R(U)$ is equal to that ring. For nonprime n, the $m_{a,b}$ do not necessarily lie in the ring of integers (when b is not prime to n), but it turns out that they lie in the ring $\mathbf{Z}[\zeta_n, 1/n]$, that is, the subring of the cyclotomic field of elements of the form $\sum a_k \zeta_n^k$ where the a_k are rational numbers such that all primes dividing their denominators are divisors of n. Moreover, the $m_{a,b}$ generate that ring.

Our remaining goal in this section is to prove all of these statements, by investigating the underlying cyclotomic fields. For later use, we recall that

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^k)$$

where $\zeta = \zeta_n$. Dividing by $X - 1$ and letting X go to 1 gives

$$n = \prod_{k=1}^{n-1} (1 - \zeta^k). \tag{4.1}$$

THEOREM 4.3. *Fix $n \geq 3$, let $U = U_n$, and $\zeta = \zeta_n$.*

(a) *The ring $R(U)$ contains ζ.*
(b) *Any element of the ring $R(U)$ is in the ring $\mathbf{Z}[\zeta, 1/n]$.*
(c) *If n is prime, then $R(U) = \mathbf{Z}[\zeta]$.*
(d) *If n is not a prime, then $R(U) = \mathbf{Z}[\zeta, 1/n]$.*

PROOF. The ring $R(U)$ contains -1 and

$$\frac{1 - \zeta}{1 - \zeta^{-1}} = -\zeta.$$

This proves (a) and shows that

$$\mathbf{Z}[\zeta_n] \subset R(U).$$

From (4.1) we see that for any n, and a that is nonzero modulo n, $1 - \zeta^a$ is a divisor of n. It follows that any elementary monomial $m_{a,b}$ can be written as an element of the ring of integers $\mathbf{Z}[\zeta]$ divided by n, and therefore that any element of $R(U)$ is an element of $\mathbf{Z}[\zeta]$ divided by a power of n. This finishes (b).

Assume that n is a prime, and consider an elementary monomial $m_{a,b}$ where a and b are coprime to n. By coprimality, we can solve the equation $a = rb - sn$ in integers r, s. Then

$$\frac{1 - \zeta^a}{1 - \zeta^b} = \frac{1 - \zeta^{a+sn}}{1 - \zeta^b} = \frac{1 - \zeta^{rb}}{1 - \zeta^b}$$

is obviously a polynomial in ζ and hence an algebraic integer. This proves (c).

To prove (d) it suffices to show that $1/p \in R(U)$ for every prime p dividing n. Since n is nonprime, either p^2 divides n or else there is another prime q such that pq divides n.

In the first case, it suffices to let $n = p^2$. Indeed, $\zeta_{p^2} = \zeta_n^{n/p^2}$ and any monomials that can be constructed in $\mathbf{Q}(\zeta_{p^2})$ can also be constructed in $\mathbf{Q}(\zeta_n)$. In the relation (4.1) for $n = p^2$,

$$p^2 = \prod_{k=1}^{p^2} (1 - \zeta^k),$$

there are $p(p-1)$ terms where k is coprime to p, and $p-1$ terms where k is divisible by p. The product of the latter is equal to p (by (4.1)) for $n = p$, so the product of the former is equal to p. It follows that the monomial

$$\prod_{k \text{ coprime to } p} \frac{1 - \zeta^k}{1 - \zeta^{pk}}$$

is equal to $p/p^p = 1/p^{p-1}$. Multiplying by p^{p-2} shows that $1/p$ is in $R(U)$ as claimed.

Now consider the case in which n is divisible by (at least) two primes, p and q. As above, it suffices to consider the case $n = pq$. In the expression

$$pq = \prod_{k=1}^{pq-1} (1 - \zeta^k)$$

there are three disjoint kinds of terms: k coprime to both p and q, k divisible by p, and k divisible by q. The products of the last two kinds of terms are equal to q and p, respectively. Therefore the product of the first kind is equal to 1, and $1 - \zeta$ is a unit. This implies that the monomial

$$\prod_{k=1}^{p-1} \frac{1 - \zeta}{1 - \zeta^{qk}} = \frac{u}{p}$$

is a unit divided by p. Multiplying by the inverse of u shows that $1/p$ is in $R(U)$ as claimed. □

Corollary 4.4. *If $n > 3$ then $R(U_n)$ is dense in the complex plane.*

Proof. If n is nonprime (so that $1/n$ is in the ring) then the ring has points arbitrarily close to zero and is therefore dense; for prime n it is well known in algebraic number theory that the image of the ring of integers under a complex embedding is dense if there is more than one pair of conjugate embeddings, and that this happens for prime n when $n > 3$.

However, this denseness result can also be proved directly: denseness of the ring $R(U_n)$ is equivalent to showing that 0 is a cluster point of $R(U_n)$, which in turn is equivalent to finding a nonzero element of $R(U_n)$ inside the unit circle (since powers

of such an element converge to 0). This is obvious for nonprime n, so we need only consider primes $n \geq 5$. In this case

$$\frac{1-\zeta}{1-\zeta^2} = \frac{1}{1+\zeta}$$

is easily verified to be a unit lying inside the unit circle. □

We conclude with a series of remarks. First, in any real-world context, the folds required to reach a specific element of the cyclotomic ring might be rather unwieldy. Second, we suspect that the proofs here can be turned into 'efficient' constructions in the sense of computational complexity; as is the case for the constructions in [7], the number of folds is likely to be linear in the complexity of a suitable description of the desired coordinates.

Also, the results here raise several interesting questions. We mention three.

(a) Is it possible to describe which subrings of the complex plane are of the form $R(U)$? For example, the ring $\mathbf{Z} + i\mathbf{Z}$ corresponds to the points which can be constructed by using the angles $\{0, \pi/4, \pi/2\}$.

(b) Is there a subgroup U of the unit circle whose Hausdorff dimension is zero and for which $R(U)$ is the entire complex plane? (Motivated by conservations with Dan Mauldin, see forthcoming work on this by Dan Mauldin, Warwick de Launey, and Dan Goldstein.)

(c) What subsets of the complex plane can be produced by the more general binary hybridization schemes $Ap + Bq$, and are there other contexts where this idea might be useful?

Acknowledgements

We thank Erik Demaine for describing this problem to us, and Roger Alperin for discussions and references. Steve Butler was supported by an NSF Mathematical Sciences Postdoctoral Fellowship. Our coauthor, Warwick de Launey, passed away while this paper was in press. We dedicate this paper to his memory, and are deeply grateful for the energy and distinctive insight that he brought to this project, and many others.

References

[1] R. C. Alperin, 'A mathematical theory of origami constructions and numbers', *New York J. Math.* **6** (2000), 119–133.

[2] R. C. Alperin and R. J. Lang, 'One-, two-, and multi-fold origami axioms', in: *Origami*^{4} (A K Peters, Natick, MA, 2009), pp. 371–393.

[3] E. D. Demaine and J. O'Rourke, *Geometric Folding Algorithms: Linkages, Origami, Polyhedra* (Cambridge University Press, Cambridge, 2007).

[4] *Origami*^{5}*: Fifth International Meeting of Origami Science, Mathematics, and Education* (A K Peters/CRC Press, Natick, MA, 2011).

[5] R. J. Lang, *Origami Design Secrets* (A K Peters, Natick, MA, 2003).

[6] R. J. Lang, ReferenceFinder, available online at http://www.langorigami.com/science/reffinder/reffinder.php4.
[7] T. Tachi and E. Demaine, 'Degenerative coordinates in 22.5° grid system', in: *Origami*^{5}*: Fifth International Meeting of Origami Science, Mathematics, and Education* (A K Peters/CRC Press, Natick, MA, 2011).
[8] L. Washington, *Introduction to Cyclotomic Fields*, 2nd edn (Springer, New York, 1997).

JOE BUHLER, Center for Communications Research,
La Jolla, CA 92121, USA
e-mail: buhler@ccrwest.org

STEVE BUTLER, Department of Mathematics, Iowa State University,
Ames, IA, 50011, USA
e-mail: butler@iastate.edu

WARWICK DE LAUNEY, Center for Communications Research,
La Jolla, CA 92121, USA

RON GRAHAM, Department of Computer Science and Engineering,
University of California, San Diego, La Jolla, CA 92093, USA
e-mail: graham@ucsd.edu