On A Mathematical Theory of Origami Constructions and Numbers

Noah Dear

June 11, 2013

Abstract

This is work based on the paper "A Mathematical Theory of Origami Constructions and Numbers" by Roger C. Alperin. This paper investigates the fields of Thalian, Pythagorean, Euclidean and Origami numbers described in Alperin's paper. I will discuss the history of the rules of origami which allow for the hierarchical constructions of these fields along with some connections to classical geometric constructions. Going through Alperin's paper, I will fill in many details of his proofs for the purpose of adding clarity and pull in some arguments found in the papers "Totally Real Origami and Impossible Paper Folding" by David Auckly and John Cleveland and "Trisections and Totally Real Origami" by Roger C. Alperin.

In partial fulfillment of the Masters in Science degree at Portland State University
Advisor: Sean Larsen
Second Reader: John Caughman

Contents

0 Prerequisites and Preliminaries

Before we begin investigating the classification of the Origami Numbers, let's review some fundamental abstract algebra which are crucial in the understanding of many of the later discussions.

Definition 0.1. *[4, Definition 4.1] A* ***group*** $\langle G, \star \rangle$ *is a set G, closed under a binary operation $\star$, such that the following axioms are satisfied:*

$\mathcal{G}_1$: *For all $a, b, c \in G$, we have*

$$(a \star b) \star c = a \star (b \star c). \text{ (associativity of } \star\text{)}$$

$\mathcal{G}_2$: *There is an element e in G such that for all $x \in G$,*

$$e \star x = x \star e = x. \text{ (identity element } e \text{ for } \star\text{)}$$

$\mathcal{G}_3$: *Corresponding to each $a \in G$, there is an element a' in G such that*

$$a \star a' = a' \star a = e. \text{ (inverse } a' \text{ of } a\text{)}$$

Definition 0.2. *[4, Definition 4.3] A group G is* ***abelian*** *if its binary operation is commutative.*

Definition 0.3. *[4, Definition 18.1] A* ***ring*** $\langle R, +, \cdot \rangle$ *is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied:*

$\mathcal{R}_1$: $\langle R, + \rangle$ *is an abelian group.*

$\mathcal{R}_2$: *Multiplication is associative.*

$\mathcal{R}_3$: *For all $a, b, c \in R$, the* ***left distributive law****, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the* ***right distributive law*** *$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.*

Definition 0.4. *[4, Definition 18.16] Let R be a ring with unity (multiplicative identity) $1 \neq 0$. An element u in R is a* ***unit*** *of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a* ***division ring*** *(or* ***skew field****). A* ***field*** *is a commutative division ring. A noncommutative division ring is called a "****strictly skew field.****"*

Definition 0.5. *[4, Definition 29.1] A field E is an* ***extension field of a field*** *F if F is a subfield of E.*

Definition 0.6. *[4] Suppose E is an extension field of a field F and $\alpha \in E$. Then the field $F(\alpha)$ is the smallest subfield of E containing F and α and is called a* ***simple extension****.*

Definition 0.7. *[4, Definition 22.1] Let R be a ring. A* ***polynomial*** *$f(x)$* ***with coefficients in*** *R is an infinite formal sum*

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + ... + a_n x^n + ...,$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The a_i are ***coefficients of*** *$f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, the largest such value of i is the* ***degree of*** *$f(x)$. If all $a_i = 0$, then the degree of $f(x)$ is undefined.*

Definition 0.8. *[4] $R[x]$ is the ring of all polynomials with coefficients in R.*

Definition 0.9. *[9, Definition IV§7.1] Let K be a commutative ring with identity. A* ***K-algebra*** *(or* ***algebra over*** *K) A is a ring A such that:*

(i) $(A,+)$ *is a unitary (left)* K*-module;*

(ii) $k(ab) = (ka)b = a(kb)$ *for all* $k \in K$ *and* $a, b \in A$.

A K*-algebra* A *which, as a ring, is a division ring, is called a* ***division algebra****.*

Definition 0.10. *[4, Definition 23.7] Let* F *be a field. A nonconstant polynomial* $f(x) \in F[x]$ *is* ***irreducible over*** F *or is an* ***irreducible polynomial in*** $F[x]$ *if* $f(x)$ *cannot be expressed as a product* $g(x)h(x)$ *of two polynomials* $g(x)$ *and* $h(x)$ *in* $F[x]$ *both of lower degree than the degree of* $f(x)$*. If* $f(x) \in F[x]$ *is a nonconstant polynomial that is not irreducible over* F*, then* $f(x)$ *is* ***reducible over*** F*.*

Definition 0.11. *[4, Definition 29.6] An element* α *of an extension field* E *of a field* F *is* ***algebraic over*** F *if* $f(\alpha) = 0$ *for some nonzero* $f(x) \in F[x]$*. If* α *is not algebraic over* F*, then* α *is* ***transcendental over*** F*.*

Theorem 0.12. *[4, Theorem 29.13] Let* E *be an extension field of* F*, and let* $\alpha \in E$*, where* α *is algebraic over* F*. Then there is an irreducible polynomial* $p(x) \in F[x]$ *such that* $p(\alpha) = 0$*. This irreducible polynomial* $p(x)$ *is uniquely determined up to a constant factor in* F *and is a polynomial of minimal degree* ≥ 1 *in* $F[x]$ *having* α *as a zero. If* $f(\alpha) = 0$ *for* $f(x) \in F[x]$*, with* $f(x) \neq 0$*, then* $p(x)$ *divides* $f(x)$*.*

Definition 0.13. *[4, Definition 29.14] Let* E *be an extension field of a field* F*, and let* $\alpha \in E$ *be algebraic over* F*. The unique polynomial* $p(x)$ *with 1 as the coefficient of the highest power of* x *appearing and having the property described in Theorem 0.12 is the* ***irreducible polynomial for*** α ***over*** F *and will be denoted* $irr(\alpha, F)$*. The degree of* $irr(\alpha, F)$ *is the* ***degree of*** α ***over*** F*, denoted by* $deg(\alpha, F)$*.*

Theorem 0.14. *[4, Theorem 31.12] Let* E *be an extension of* F*. Then*

$$\bar{F}_E = \{\alpha \in E | \alpha \text{ is algebraic over } F\}$$

is a subfield of E*, the* ***algebraic closure of*** F ***in*** E*.*

Definition 0.15. *[4, Definition 31.14] A field* F *is* ***algebraically closed*** *if every nonconstant polynomial in* $F[x]$ *has a zero in* F*.*

Definition 0.16. *[9, Definition IV§1.1] Let* R *be a ring. A (left)* ***R-module*** *is an abelian group* A *together with a function* $R \times A \to A$ *(the image of* (r, a) *being denoted* ra*) such that for all* $r, s \in R$ *and* $a, b \in A$*:*

(i) $r(a + b) = ra + rb$.

(ii) $(r + s)a = ra + sa$.

(iii) $r(sa) = (rs)a$.

If R *has an identity element* 1_R *and*

(iv) $1_R a = a$ *for all* $a \in A$,

then A *is said to be a* ***unitary R-module.*** *If* R *is a division ring, then a unitary* R*-module is called a (left)* ***vector space****.*

Definition 0.17. *[4, Definition 48.1] Let* E *be an extension field of a field* F*. Two elements* $\alpha, \beta \in E$ *are called* ***conjugates*** *over* F *if* $irr(\alpha, F) = irr(\beta, F)$*, that is, if* α *and* β *are zeros of the same irreducible polynomial over* F*.*

Theorem 0.18. ***The Conjugation Isomorphisms*** *[4, Theorem 48.3] Let* F *be a field, and let* α *and* β *be algebraic over* F *with* $deg(\alpha, F) = n$*. The map* $\phi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ *defined by*

$$\phi_{\alpha,\beta}(c_0 + c_1\alpha + \cdots + c_n\alpha^{n-1}) = c_0 + c_1\beta + \cdots + c_n\beta^{n-1}.$$

for $c_i \in F$ is an isomorphism of $F(\alpha)$ onto $F(\beta)$ if and only if α and β are conjugate over F.

Corollary 0.19. *[4, Corollary 48.5] Let α be algebraic over a field F. Every isomorphism ϕ mapping $F(\alpha)$ onto a subfield of $\bar{F}$ such that $\phi(a) = a$ for $a \in F$ maps α onto a conjugate β of α over F. Conversely, for each conjugate β of α over F, there exists exactly one isomorphism $\phi_{\alpha,\beta}$ of $F(\alpha)$ onto a subfield of $\bar{F}$ mapping α onto β and mapping each $a \in F$ onto itself.*

Theorem 0.20. *[4, Theorem 31.4] If a field N is a finite extension of a field M which is in turn a finite extension of a field L, then N is a finite extension of L and*

$$[N : L] = [N : M][M : L]$$

The above theorem will be used extensively in this paper. For example, in Proposition 2.12 I state that $[\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}] = [\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$ which is a direct application of the above theorem.

Throughout this paper I will be referring to subfields X and Y of the real numbers $\mathbb{R}$ and then interchangeably referring to $X \bigoplus Yi$ and the subfield of the complex numbers $\mathbb{C}$ with real and imaginary parts lying in X and Y respectively. Note that these are not technically equivalent fields but they are isomorphic when you define multiplication in $X \bigoplus Yi$ by $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. For this reason we will consider the two fields equivalent and I will alternate between the two notations fluidly as is deemed convenient during the discussion.

There are many theorems, lemmas, corollaries and propositions throughout this paper, most of which are attributed to Alperin. However, some detail is left out of Alperin's paper and I have added a significant amount of explanation to his work. To differentiate my work from Alperin's I have labeled my results as propositions while all of his work is labeled as either a theorem, lemma or corollary.

1 Introduction

In 1989 Jacques Justin and Humiaki Huzita independently introduced the foundation for Origami Constructions based on seven rules or "axioms." [2, 10] Both Justin and Huzita presented their work in the same proceedings, although Huzita only showed the first six of these. Independently Koshiro Hatori discovered the seventh axiom in 2001 [3]. Also independently, David Auckly and John Cleveland discovered the first four of these axioms in 1995 [6]. The complete list of seven axioms is referred to as the Huzita-Hatori or Huzita-Justin Axioms. It is important to note these are not "axioms" in the classical sense of the word but actually just rules for what constructions you are allowed to make. For historical reasons I have left Huzita's Axioms in their original wording. We will soon see the reason for Huzita claiming "origami geometry superior," which comes from being able to perform constructions that are impossible using a compass and straightedge. The seventh axiom is written using Lang and Alperin's wording from their 2006 paper "One-, Two-, and Multi-Fold Origami Axioms."

Huzita-Hatori Axioms [2][3]:

1. given two distinct points, you can fold making the crease pass through both points, ——— ruler operation

2. given two distinct points, you can fold superposing one point onto the other point, ——— perpendicular bisector

3. given two distinct (straight)lines, you can fold superposing one line onto another. ——— bisector of the angle

4. given one line and one point, you can fold making the crease perpendicular to the line and passing through the point, ——— perpendicular footing

5. given one line and two distinct points not on this line, you can fold superposing one point onto the line and making the crease pass through the other point, ——— tangent from a point to a parabola

6. given two distinct points and two distinct lines, you can fold superposing the first point onto the first line and the second point onto the second line at the same time. ——— non existing in the geometry so far known thus making origami geometry superior

7. Given a point p_1 and two lines l_1 and l_2, we can make a fold perpendicular to l_2 that places p_1 onto line l_1.

We will begin with the first four of these axioms and determine which points in the complex plane are constructible using them. We will then continue to expand this set of numbers by consecutively adding axioms. We will find that the sets of numbers constructible via these axioms make up different fields of numbers under complex multiplication and addition. Thus, the goal of this paper is to hierarchically classify the fields formed as we add axioms to constuction allowance. Once this goal is achieved we will find that using the first five of these axioms we end up with exactly the field of numbers constructible using a compass and straightedge - the Euclidean Numbers $\mathbb{E}$. Then adding the sixth axiom we will find that the Origami Numbers properly contain the Euclidean Numbers, thus showing that there are constructions obtainable using origami folds that are impossible using classical geometric constructions. A famous example of this is that the trisection of an angle is not necessarily constructible using a compass and straightedge. We will show that this is possible using origami folds.

Definition 1.1. *Origami Numbers: The smallest subset of numbers in $\mathbb{C}$, starting with 0 and 1, constructible using the Huzita-Hatori Axioms given above.*

From Alperin's paper which this paper is based upon we will be using a slightly different list of axioms. The axioms to be used, which I will call *Alperin Axioms* are as follows:

Alperin Axioms:

1. The line connecting two constructible points is a constructible line.

2. The point of coincidence of two constructible lines is a constructible point.

3. The perpendicular bisector of the segment connecting two constructible points is a constructible line.

4. The line bisecting any given constructed angle can be constructed.

5. Given a constructed line l and constructed points P, Q, then whenever possible, the line through Q, which reflects P onto l, can be constructed.

6. Given constructed lines l, m and constructed points P, Q, then whenever possible, any line which simultaneously reflects P onto l and Q onto m, can be constructed.

Note that in this list, the 4th and 7th Huzita-Hatori Axioms are missing. Lang and Alperin claim that the 7th Huzita-Hatori Axiom does not actually expand the set of Origami Numbers [3] and we will show in the following pages that using the first 3 Alperin Axioms we can construct the 4th Huzita-Hatori Axiom, showing it is also unnecessary for our purposes. Further Alperin added his new Axiom stating that the point of coincidence of two lines is a constructible point. This is simply so that we may talk about constructible points as opposed to constructible lines. From here on out I will refer to the Alperin Axioms simply by axiom and the accompanying number.

2 Geometrical Axioms and Algebraic Consequences

2.1 Thalian Constructions

Thalian Axioms:

0. The set contains 3 points A, B, C, of the complex numbers, not all on a line.
1. The line connecting two points in Π is constructible.
2. The point of coincidence of two contructible lines is in Π.
3. The perpendicular bisector of the segment connecting two constructible points is constructible.

Definition 2.1. *Thalian Constructible Numbers, denoted* $\Pi = \Pi\{A, B, C\}$*, is the smallest subset of points in* $\mathbb{C}$ *which is closed under the Thalian Axioms.*

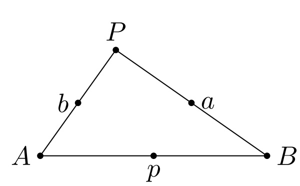
In this definition, note that the Thalian Constructible Numbers are defined dependent on three initial points A, B and C as opposed to just the two points 0 and 1 for the Origami Numbers. This will become handy as we extend the Thalian Constructible Numbers to the Pythagorean Numbers, Euclidean Numbers and eventually the Origami Numbers. We will call (0) above a new axiom for this purpose. We will soon assume A and B to be 0 and 1 respectively. Once this is done, Π becomes dependent only on C which we will call $z = a + bi \in \mathbb{C}$. We will also eventually assume $b \neq 0$ so $z \notin \mathbb{R}$. Hence we will be describing $\Pi = \Pi[z]$ as a set of numbers dependent only on the third chosen point z. We will show that, depending on our initial choice of z, either $\Pi[z] = \mathbb{Q}(z, \bar{z})$ or $\Pi[z] = \mathbb{Q}(z, \bar{z}, i) = \mathbb{Q}(a, b, i)$. The fact that $\mathbb{Q}(z, \bar{z}, i) = \mathbb{Q}(a, b, i)$ is proven in the appendix under Proposition A.1.

The preliminary to showing that $\Pi[z]$ is a subfield of $\mathbb{Q}(a, b, i)$ is to note that $\Pi[z]$ is made up of points in the complex plane which have both a real and imaginary part. From this we may let $X[z] = X \subset \mathbb{R}$ be the set of real numbers which appear as the real part of some Thalian Constructible Number and $Y[z] = Y \subset \mathbb{R}$ be the set of real numbers which appear as the coefficient of the imaginary part of some Thalian Constructible Number. This then implies that given any $x \in X$ and $y \in Y$, $z = x + yi \in \Pi[z]$ so $\Pi[z] = X \oplus Yi$ and $\Pi[z]$ may be determined by X and Y.

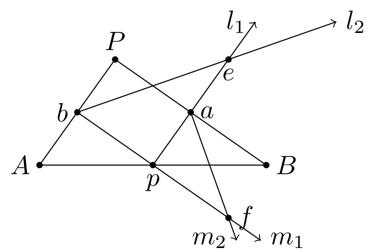
We need to find a way to realize how X and Y are related to each other. We begin by building some simple constructions which allow us to determine what elements are in X and Y respectively.

Lemma 2.2. *[1, Lemma 2.1] Given a point* P *and a line segment* AB*, we can construct the parallel segment of the same length and direction as* AB*, beginning or ending at* P*.*

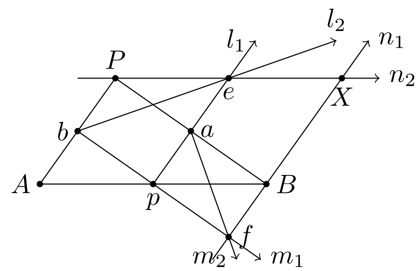
Proof. Note that midpoints of segments can be constructed using perpendicular bisectors. First suppose P is not on AB. Construct AP, BP and the midpoints of $AB = p$, $AP = b$ and $BP = a$.



Construct the midpoints of $pB = c$ and $aP = d$ and the lines l_1, l_2, m_1 and m_2 through pa, bd, bp and ac respectively. Construct the point of intersection e between l_1 and l_2 and the point of intersection f between m_1 and m_2



Construct the lines n_1 and n_2 through fB and Pe respectively and then construct X as the point of intersection of n_1 and n_2.

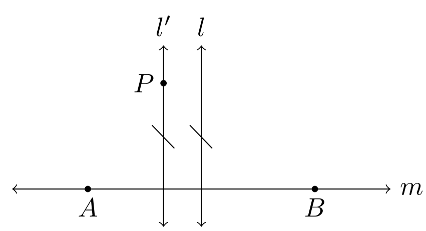


It can be seen that PX is parallel to AB and is of the same length by construction.
In the case where P lies on AB, first take any constructible point Q not on AB, construct the segment QX' parallel to AB as above and then transfer QX' to the end of P by the same construction.
The proof of constructing the segment ending at P which is of the same length as AB and parallel to AB can be performed symmetrically.

□

Corollary 2.3. *[1, Corollary 2.2] We can construct a perpendicular to a line m from a given point P.*

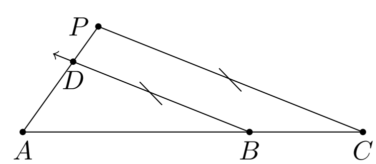
Proof. Take any two constructible points on m, say A and B and construct the perpendicular bisector l of AB. If l passes through P, we're done, else construct the line parallel to l which passes through P as in Lemma 2.2.



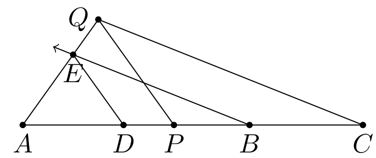
□

Corollary 2.4. *[1, Corollary 2.3] Given a point P and a segment ABC we can construct the segment ADP so that triangle ABD is directly similar to ACP.*

Proof. First, assume P is not on ABC. Construct AP, CP and the parallel to CP through B. Let D be the point of intersection of AP with the parallel to CP through B. Then ABD is directly similar to ACP.



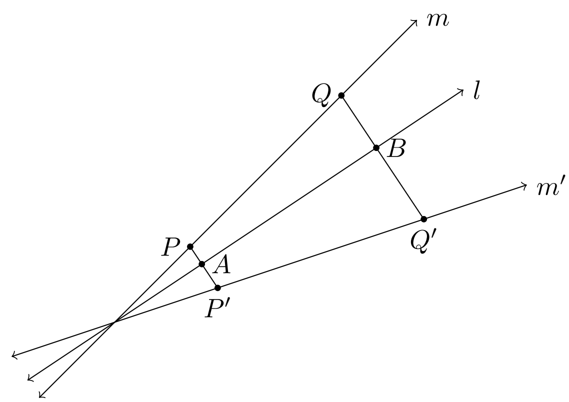
If P is on ABC, take any constructible point Q not on the line containing ABC and construct the point E on AQ just as D was constructed above. Then construct the line parallel to PQ through E. Let D be the point of intersection of the line passing through ABC and the line parallel to PQ through E. Then ABD is directly similar to ACP.



□

Corollary 2.5. *[1, Corollary 2.4] Given a point P and a line l we can reflect P across L. Given lines l and m we can reflect M across l.*

Proof. The proof of the first part is included in the proof of the second. Take two constructible points P and Q on m. By Corollary 2.3, we can construct a perpendicular to l through both P and Q. Let A and B respectively be the intersections of these perpendiculars with l. By Lemma 2.2, we can translate PA and QB to A and B respectively and name the new endpoints P' and Q'. The line m' containing P' and Q' is the line we desire.



□

To recap, we now have:

(a) The set Π of Thalian Constructible Numbers contains 3 points A, B, C, of the complex numbers, not all on a line.

(b) The line connecting two points in Π is constructible.

(c) The point of coincidence of two constructible lines is in Π.

(d) The perpendicular bisector of the segment connecting two constructible points is constructible.

(e) Given a segment AB and a point P, The segments PQ and $Q'P$ of length $|AB|$ and parallel to AB are constructible.

(f) Given a point P and a line l, the perpendicular to l through P is constructible.

(g) Given a point P and three points A, B and C on a line, The point D making ΔABD directly similar to ΔACP is constructible.

(h) Given a line l a point P and a line m, the reflections of P and m in l are constructible.

Corollary 2.6. *[1, Corollary 2.5] The subset Π is closed under segment addition in $\mathbb{C}$. If we take $A = 0$, then Π is an abelian group.*

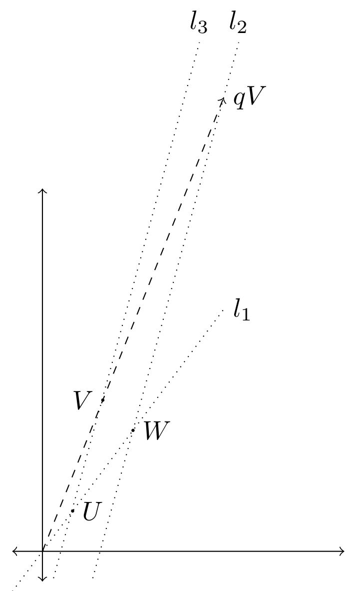
Proof. Given any two constructed segments, AB and CD, we can translate CD to the end of AB with C attached to B and construct $AD = AB + CD$ by Lemma 2.3. Similarly, we can translate CD to the end of AB with D attached to B and construct $AC = AB - CD$.
Note AA serves as the identity segment. Clearly association of segment addition holds. Given any segment BC, using Lemma 2.3 we can construct $C' \neq C$ on the line passing through BC such that $|BC| = |C'B|$. Then $B'A + AB = AA$. Clearly, given any segments BC and DE, $BC + DE = DE + BC$.
With $A = 0$ we can think of this segment addition as addition of complex numbers by translating any given segment so that it originates from the origin and terminates at a complex number. Thus Π is an abelian group under addition.

□

As mentioned before, in $\Pi\{A, B, C\}$ we will now assume that $A = 0$, $B = 1$ and $C = z \in \mathbb{C}$ so that $\Pi = \Pi[z]$. Again, let $X[z] = X \subset \mathbb{R}$ be the set of real numbers which appear as the real part of some Thalian Constructible Number and $Y[z] = Y \subset \mathbb{R}$ be the set of real numbers which appear as the coefficient of the imaginary part of some Thalian Constructible Number. By constructing the line through 0 and 1 we may construct the Real-axis. By constructing the perpendicular to the Real-axis through 0 we have now constructed the Imaginary-axis. Then, through any point in Π, we may project it onto both the Real and Imaginary axes. Thus X and Yi are subsets of Π. Conversely, given any $x \in X$ and $y \in Y$ we may construct the perpendiculars to the Real and Imaginary axes through x and y respectively to get $x + yi$ so $\Pi = X \bigoplus Yi$.
We want to show that $\Pi[z]$ is a field so it will suffice to show X and Y are fields. We've already shown $\Pi[z]$ is an abelian group under addition. We will now show that $\Pi[z]$ is a $\mathbb{Q}$-vector space with subspaces $X[z]$ and $Y[z]i$ and then use this to show that X is in fact a $\mathbb{Q}$-algebra and then a field.

Corollary 2.7. *[1, Corollary 2.6] For z a non-real complex number, $\Pi[z]$ is a $\mathbb{Q}$-vector space closed under complex conjugation with subspaces $X[z]$ and $Y[z]i$.*

Proof. Since we already know $\Pi[z]$ is an abelian group under addition, it suffices to show that scalar multiplication holds over $\mathbb{Q}$. Note multiples of any constructible point may be constructed by Lemma 2.2. Given any reduced fraction $p/q \in \mathbb{Q}$ and any point $W \in \Pi[z]$, construct the line l_1 through W and 0, and then construct qV for any constructible point V not on l_1. Then construct the line l_2 through qV and W. Lastly, construct l_3 parallel to l_2 through V by Lemma 2.3. Let U be the point of coincidence of l_1 and l_3. Then $qU = W$ and $pU = p/qW$. Associativity, distribution and identity hold since $\Pi[z] \subset \mathbb{C}$. This is really just an application of Corollary 2.4 with $A = 0$, $B = V$, $C = nV$ and $P = W$.
Given any $x_1, x_2 \in X[z]$ and $c \in \mathbb{Q}$, clearly $x_1 + x_2 \in X[z]$ and $cx_1 \in X[z]$ so $X[z]$ is a subspace. Similarly, $Y[z]$ is a subspace. $\Pi[z]$ is closed under complex conjugation since $\Pi[z] = X \bigoplus Yi$ as discussed above and for any $w = w_1 + w_2 i \in \Pi[z]$, $w_2 \in Y[z] \to -w_2 \in Y[z]$ and hence $\bar{w} = w_1 - w_2 i \in \Pi[z]$.

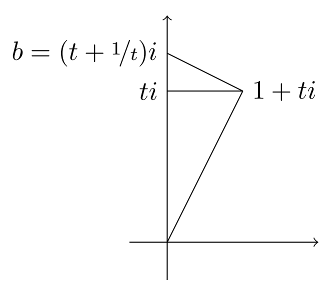


∎

In order to show X and Y are fields, we are going to need a number of building blocks. We will start with a lemma and then condense a number of other findings, including that X is a field, into a single corollary.

Lemma 2.8. *[1, Lemma 2.7] If $t \in Y$ is non-zero, then $1/t \in Y$.*

Proof. Assume for the moment that $t > 0$. Construct the points ti and $1 + ti$. Construct the line l_1 through 0 and $1 + ti$, the line l_2 throught $1 + ti$, perpendicular to l_1 and the line l_3 through ti and $1 + ti$. Let b be the intersection of l_2 with the Imaginary-axis. Then the triangle through 0, $1 + ti$ and ti is directly similar to the triangle through $1 + ti$, b and t. Hence $b - t = 1/t$ so $1/t \in Y$. If $t < 0$, $-1/t \in Y$ by the same construction, so $1/t \in Y$.



∎

Corollary 2.9. *[1, Corollary 2.8] Let $x \in X$, $t, v, y \in Y$:*

i) $vy \in X$, $xy \in Y$ and consequently, $tvy \in Y$.

ii) $x^2 \in X$ if $Y \neq \{0\}$, hence X is a $\mathbb{Q}$-algebra.

iii) For non-zero $y \in Y$, $Y = Xy$.

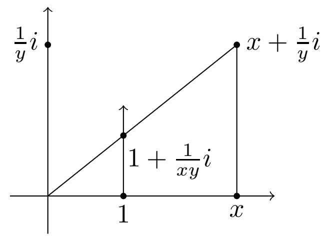
iv) For non-zero $x \in X$, if $Y \neq \{0\}$, then $1/x \in X$, and hence X is a field.

v) If $Y \bigcap X \neq \{0\}$, then $X = Y$.

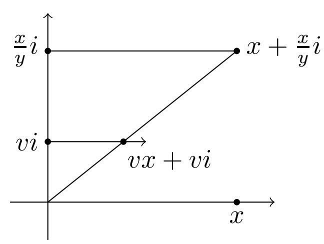
vi) If $X = Y$, then $\Pi[z]$ is the field $X(i)$.

vii) A real number μ is the slope of a constructed line if and only if $\mu \in Y$.

Proof. i) Construct x, $\frac{1}{y}i$, $x + \frac{1}{y}i$ and the line l_1 through 0 and $x + \frac{1}{y}i$. Construct the line l_2 perpendicular to the Real-axis and through 1. The point of coincidence of l_1 and l_2 is $1 + ki$ with $k = \frac{\frac{1}{y}}{x} = \frac{1}{xy}$ by similar triangles. Hence $\frac{1}{xy} \in Y$ and by Lemma 2.8, $xy \in Y$ as well.

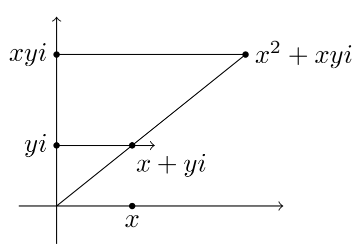


Using this and the fact that $\frac{1}{y} \in Y$, we get that $\frac{x}{y} \in Y$. We then construct x, $\frac{x}{y}i$, vi, $x + \frac{x}{y}i$ and the line l_3 through 0 and $x + \frac{x}{y}i$. Construct then, the line l_4 perpendicular to the Imaginary-axis through v. The point of coincidence of l_3 and l_4 is $vy + vi$ by similar triangles. Hence $vy \in X$.



The last statement follows from $vy \in X$ and $t \in Y$ implies $tvy \in Y$.

ii) Assuming $Y \neq \{0\}$ (which it shouldn't since we are supposing $z \notin \mathbb{R}$), choose $0 \neq y \in Y$. Construct x, yi, xyi (by part (i)) and $x + yi$. Construct then the line l_1 through 0 and $x + yi$ and the line l_2 perpendicular to the Imaginary-axis through xy. The point of coincidence of l_1 and l_2 is $x^2 + xyi$ so $x^2 \in X$.



We already know X is a $\mathbb{Q}$-vector space made up of real numbers so we take multiplication of elements of X to be a second operation. Given any two points $x_1, x_2 \in X$, take $0 \neq y \in Y$ and note $x_1 y \in Y$ and $\frac{x_2}{y} \in Y$ by (i) and Lemma 2.8. Thus $x_1 x_2 = x_1 y \cdot \frac{x_2}{y} \in X$ by (i). Since we are working with real numbers, bilinearity over $\mathbb{Q}$ is a given. Therefore X is a $\mathbb{Q}$-algebra.

iii) Given any $x \in X$ and any $v, y \in Y \backslash \{0\}$, we know $\frac{1}{y} \in Y$ by Lemma 2.8 so $\frac{v}{y} \in X$ by (i) and $v = \frac{v}{y} \cdot y \in Xy$. Thus $Y \subset Xy$. Since $xy \in Y$ it is also the case that $Xy \subset Y$ and hence, $Xy = Y$.

iv) Given any $x \in X\backslash\{0\}$ and any $y \in Y\backslash\{0\}$, then $\frac{1}{xy} \in Y$ by (i) and Lemma 2.8. Also by (i) we get $y^2 \in X$ so $\frac{y}{x} = \frac{y^2}{xy} \in Y$. Therefore $\frac{1}{x} = \frac{1}{y} \cdot \frac{y}{x} \in X$, again by (i). It immediately follows that X is a field since we now have multiplicative inverses and we've already shown that X is a $\mathbb{Q}$-algebra.

v) Choose any $y \in Y \bigcap X\backslash\{0\}$ so $\frac{1}{y} \in Y$ and $y \in X$. Thus $1 = y \cdot \frac{1}{y} \in Y$ by (i) and $Y = X \cdot 1 = X$ by (iii).

vi) Clearly, if $X = Y$, $\Pi = X \bigoplus Yi = X \bigoplus Xi = X(i)$.

vii) ($\rightarrow$) If μ is the slope of a constructed line, then we can transpose that line to go through the origin to get the line $y = \mu x$. Since $1 \in X$, $\mu = \mu \cdot 1 = y \in Y$. ($\leftarrow$) If $\mu \in Y$, then we may construct the line through $1 + \mu i$ which clearly has a slope of μ.

□

Corollary 2.10. *[1, Corollary 2.9] For any non-real complex $z = a + bi$, $\Pi[z]$ is a field over $\mathbb{Q}$ containing z, closed under complex conjugation and contained in the field $\mathbb{Q}(a, b, i)$.*

Proof. Using induction on the constructible points and the constructible lines via the Thalian Axiom, we can show that $\Pi[z] \subseteq \mathbb{Q}(a, b, i)$. A complete proof of this is included in the appendix as Proposition A.2. Given constructed point $v = v_1 + v_2 i$, note $v^2 = v_1^2 - v_2^2 + 2v_1v_2 i$ is constructible. This follows from $v_1^2 - v_2^2 \in X$ since X is a field, $v_1v_2 \in Y$ by Corollary 2.9 (i) and $2v_1v_2 \in Y$ since $\Pi[z]$ is a $\mathbb{Q}$-vectorspace (Corollary 2.7). Similarly, given constructed point $w = w_1 + w_2 i$, w^2 is constructible. Hence $vw = \frac{1}{2}\left((v + w)^2 - v^2 - w^2\right)$ is constructible since $\Pi[z]$ is a $\mathbb{Q}$-vectorspace. By Corollary 2.9 (i), $w_2^2 \in X$ and by Corollary 2.9 (ii), $w_1^2 \in X$. Thus $r^2 = w_1^2 + w_2^2 \in X$ and $\frac{1}{r^2} \in X$ since X is a field. Further, $\bar{w} = w_1 - w_2 i$ is constructible since $-1 \in X$ implies $-w_2 = -1 \cdot w_2 \in Y$ by Corollary 2.9 (i). Hence $\frac{1}{w} = \frac{\bar{w}}{r^2}$ is constructible since we've shown $\Pi[z]$ is closed under complex multiplication. Therefore, $\Pi[z]$ is a field. □

We have now accomplished the primary goal for this section which was to show $\Pi[z]$ is a field contained in $\mathbb{Q}(a, b, i)$. Remember that if $X = Y$, then $\Pi[z] = X(i)$. We continue by stating a condition on z for which X will equal Y.

Corollary 2.11. *[1, Corollary 2.10] Suppose that $z = a + bi$, with b (real) algebraic. If the irreducible integer polynomial $q(t)$ satisfied by b is not a polynomial in t^2 then $X = Y$. Hence, if b has odd degree or z is a non-real algebraic number of odd degree, then $X = Y$.*

Proof. Let $q(t) = q_0 + q_1 t + \cdots q_n t^n$ with n even so deg($q(t)$)=n or $q_n = 0$ and deg($q(t)$)=$n - 1$. Collecting together the even terms and evaluating at b we get $0 = q_0 + q_2 b^2 + \cdots + q_n b^n + q_1 b + q_3 b^3 + \cdots q_{n-1} b^{n-1}$ which implies

$$q_0 + q_2 b^2 + \cdots q_n b^n = -(q_1 b + q_3 b^3 + \cdots q_{n-1} b^{n-1}).$$

Note $q_0 \neq 0$ or $q(t)$ would not be irreducible. Since we are assuming $q(t)$ is not a polynomial in t^2 we see both the left and right hand sides of the above equation are not zero. Now $b^2 = b \cdot b \in X$ by Corollary 2.9 (i) so the left hand side of the above equation is in X since X is a $\mathbb{Q}$-vectorspace. For the right hand side, we factor out a b so that $-(q_1 + q_3 b^2 + \cdots q_{n-1} b^{n-2}) \in X$ and $-(q_1 + q_3 b^2 + \cdots q_{n-1} b^{n-2})b \in Xb = Y$. Since we are assuming $q(t)$ is not a polynomial in t^2, we see that the left and right hand sides do not equal zero so $X \bigcap Y \neq \{0\}$ and $X = Y$ by Corollary 2.9 (v).

□

I have not proven the second assertion of the previous corollary. In Alperin's paper, he claims that z being a non-real algebraic number of odd degree implies that $\mathbb{Q}(z, \bar{z})$ is of odd degree and hence not equal to $\mathbb{Q}(z, \bar{z}, i)$ since it can easily be shown that $\mathbb{Q}(z, \bar{z}, i)$ is of even degree. If this were true, it would then imply, with a little work, that b is also of odd degree and hence $X = Y$ by the first part of the corollary. However, the following counterexample shows this to be incorrect:

Let $z = \sqrt[3]{2}e^{i\frac{4\pi}{3}} = -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}i$ so $\bar{z} = \sqrt[3]{2}e^{i\frac{8\pi}{3}} = -\frac{\sqrt[3]{2}}{2} - \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}i$. Clearly $x^3 - 2$ is the irreducible polynomial for z over $\mathbb{Q}$ so z is of degree 3. Now, b in this case is $\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}$, which is a zero to $x^6 - \frac{27}{16}$ so b is of degree at most 6. Note that in $\mathbb{Q}$ there does not exist α_i satisfying

$$\alpha_5(\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2})^5 + \alpha_4(\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2})^4 + \alpha)_3(\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2})^3 + \alpha_2(\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2})^2 + \alpha_1(\frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}) + \alpha_0 =$$
$$\alpha_5\frac{9}{16}\sqrt[3]{2^2} + \alpha_4\frac{9}{8}\sqrt[3]{2} + \alpha_3\frac{3}{4}\sqrt{3} + \alpha_2\frac{3}{4}\sqrt[3]{2^2} + \alpha_1\sqrt[3]{2}\sqrt{3} + \alpha_0 = 0$$

since $\sqrt[3]{2^2}\sqrt{3}$, $\sqrt[3]{2}$, $\sqrt{3}$, $\sqrt[3]{2^2}$, $\sqrt[3]{2}\sqrt{3}$ and 1 are linearly independent over $\mathbb{Q}$. Thus b is of degree 6. That is, we've found a counterexample to Alperin's claim that z having odd degree over $\mathbb{Q}$ implies that b is of odd degree over $\mathbb{Q}$.
Keep in mind that this does not discount Alperin's original claim in the corollary, which is that z being of odd degree over $\mathbb{Q}$ implies that $X = Y$, only that his proof is incorrect. Despite attempt, I have not been able to prove this claim. However, the actual disconnect in the proof is that z being of odd degree implies that $\mathbb{Q}(z, \bar{z})$ is of odd degree. This being the case, I can still make the following proposition:

Proposition 2.12. *If $[\mathbb{Q}(z, \bar{z}) : \mathbb{Q}]$ is odd, then $X = Y$.*

Proof. Let $m = [\mathbb{Q}(z, \bar{z}) : \mathbb{Q}]$. Since $[\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}] = [\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$ and $[\mathbb{Q}(i) : \mathbb{Q}] = \deg(i, \mathbb{Q}) = 2$ it follows that $\mathbb{Q}(z, \bar{z}, i)$ is of even degree. By hypothesis we now have $\mathbb{Q}(z, \bar{z}) \neq \mathbb{Q}(z, \bar{z}, i)$. This then implies that $i \notin \mathbb{Q}(z, \bar{z})$ so $x^2 + 1$ is irreducible over $\mathbb{Q}(z, \bar{z})$ and thus $\deg(i)$ over $\mathbb{Q}(z, \bar{z})$ is 2. Similary $x^2 + 1$ is irreducible over $\mathbb{Q}(a, b)$ since a and b are real so $\deg(i)$ over $\mathbb{Q}(a, b)$ is also 2. Putting this together we have

$$\begin{aligned}
2 \cdot [\mathbb{Q}(a, b) : \mathbb{Q}] &= [(\mathbb{Q}(a, b))(i) : \mathbb{Q}(a, b)][\mathbb{Q}(a, b) : \mathbb{Q}] \\
&= [\mathbb{Q}(a, b, i) : \mathbb{Q}(a, b)][\mathbb{Q}(a, b) : \mathbb{Q}] \\
&= [\mathbb{Q}(a, b, i) : \mathbb{Q}] \\
&= [\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}] \\
&= [\mathbb{Q}(z, \bar{z}, i) : \mathbb{Q}(z, \bar{z})][\mathbb{Q}(z, \bar{z}) : \mathbb{Q}] \\
&= [(\mathbb{Q}(z, \bar{z}))(i) : \mathbb{Q}(z, \bar{z})][\mathbb{Q}(z, \bar{z}), \mathbb{Q}] \\
&= 2m.
\end{aligned}$$

This then implies $m = [\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a, b) : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}]$ so both $[\mathbb{Q}(b, a) : \mathbb{Q}(b)]$ and $[\mathbb{Q}(b) : \mathbb{Q}]$ are odd. Now, $[\mathbb{Q}(b) : \mathbb{Q}]$ being odd implies that the degree of b over $\mathbb{Q}$ is odd so therefore $X = Y$ by the previous part of this corollary. $\square$

2.2 Thalian Numbers

In this section we will show that $\Pi[z]$ is either $\mathbb{Q}(z, \bar{z})$ or $\mathbb{Q}(z, \bar{z}, i)$ and give some conditions on z that will help us determine which field $\Pi[z]$ is equivalent to. We will specifically find some conditions on z which will not only tell us which field $\Pi[z]$ is equivalent to, but which will also help us in determining the fields we get as we begin adding axioms to the Thalian Axioms.

Proposition 2.13. *For any non-real complex number $z = a + bi$, the field $X[z]$ contains $\mathbb{Q}(a, b^2)$ and is contained in $\mathbb{Q}(a, b)$.*

Proof. $X[z]$ containing $\mathbb{Q}(a, b^2)$ follows immediately from Corollary 2.9 parts (i) and (ii). The fact that $\mathbb{Q}(a, b)$ contains $X[z]$ is a result of $X[z]$ being a real subfield of $\Pi[z]$ which is contained in $\mathbb{Q}(a, b, i)$ by Corollary 2.10. $\square$

Definition 2.14. *If $\Pi[z]$ contains i, then we call the non-real complex number z Thalian.*

Theorem 2.15. *[1, Theorem 2.11] The non-real complex number z is Thalian if and only if $b \in \mathbb{Q}(a, b^2)$. Consequently, the field $X = \Pi[z] \bigcap \mathbb{R}$ is eiher $\mathbb{Q}(a, b)$ or $\mathbb{Q}(a, b^2)$, depending on whether or not z is Thalian. For any non-Thalian z, $\Pi[z]$ is the field $\mathbb{Q}(z, \bar{z})$, whereas for a Thalian z, $\Pi[z] = \mathbb{Q}(z, \bar{z}, i)$.*

Proof. Let $X_1 = \mathbb{Q}(a, b^2)$. If z is Thalian, then $\Pi[z]$ contains i so $1 \in Y$ and hence $X = Y$ by Corollary 2.9 (v). Thus $b \in X$ so $X = \mathbb{Q}(a, b)$. On the other hand, if $X = \mathbb{Q}(a, b)$ then $b \in X$ so $X \bigcap Y \neq \{0\}$, $X = Y$, $\Pi[z] = X(i)$ and z is Thalian. Hence, if z is non-Thalian, then $b \notin X$ so $b \notin X_1$ since $X \supseteq X_1$. The contrapositive then gives our assertion that $b \in X_1$ implies z is Thalian.
Suppose now $b \notin X_1$. Since $b^2 \in X_1$, we have $x^2 - b^2$ as the irreducible polynomial for both b and $-b$ so they are conjugates and by Corollary 0.19 there is a unique isomorphism $\phi : X_1(b) \to X_1(-b)$ which fixes X_1 and maps b onto $-b$.
Now, by induction, given any $w = w_1 + w_2 i \in \Pi[z]$, it can be shown that $w_1 \in X_1$, $w_2 \in X_1 b$, $\phi(w_1) = w_1$ and $\phi(w_2) = -w_2$. I give a complete proof of this in the appendix as Proposition A.3. Consider then $i = 0 + 1i$. For i to be constructible we would need $\phi(1) = -1$. However $1 \in X_1$ so $\phi(1) = 1 \neq -1$ and therefore i is not constructible. Thus, if $b \notin X_1$ then z is non-Thalian. The contrapositive here shows that if z is Thalian, then $b \in X_1$.
If z is Thalian we now have $b \in \mathbb{Q}(a, b^2)$ so $\mathbb{Q}(a, b^2) = \mathbb{Q}(a, b)$ and thus $X = \mathbb{Q}(a, b)$. If z is non-Thalian, then $b \notin \mathbb{Q}(a, b^2)$ so $x^2 - b^2$ is the irreducible polynomial for b over $\mathbb{Q}(a, b^2)$ and thus $[\mathbb{Q}(a, b) : \mathbb{Q}(a, b^2)] = [(\mathbb{Q}(a, b^2))(b) : \mathbb{Q}(a, b^2)] = 2$. Now, since X is properly contained in $\mathbb{Q}(a, b)$ and X contains $\mathbb{Q}(a, b^2)$ it must be that $X = \mathbb{Q}(a, b^2)$ by Proposition A.4.
If z is Thalian, then $Y = X = \mathbb{Q}(a, b)$ and $\Pi[z] \ni i$ so $\Pi[z] = \mathbb{Q}(a, b, i) = \mathbb{Q}(z, \bar{z}, i)$ by Proposition A.1. By Corollary 2.10 $\Pi[z] \subseteq \mathbb{Q}(a, b, i) = \mathbb{Q}(z, \bar{z}, i)$ and $\mathbb{Q}(z, \bar{z}) \subseteq \Pi[z]$. Thus, if z is non-Thalian so $i \notin \Pi[z]$, then $\mathbb{Q}(z, \bar{z}) \neq \mathbb{Q}(z, \bar{z}, i)$ so the degree of i over $\mathbb{Q}(z, \bar{z})$ is 2. Hence, by Proposition A.4, $\Pi[z]$ is a trivial extension of $\mathbb{Q}(z, \bar{z})$, that is $\Pi[z] = \mathbb{Q}(z, \bar{z})$ when z is non-Thalian. □

We should notice that $X = \mathbb{Q}(a, b)$ implies that $\Pi[z]$ contains i, yet not all $\mathbb{Q}(a, b)$ are equal. For example, if $a, b \in \mathbb{Q}$ then $X = \mathbb{Q}$ and $\Pi[z] = \mathbb{Q} + \mathbb{Q}i$. Yet, if we let b be non-rational but still algebraic with irreducible polynomial $q(t)$ not a polynomial in t^2, then $X = \mathbb{Q}(a, b) \supset \mathbb{Q}$ (proper) and $\Pi[z] = X + Xi \supset \mathbb{Q} + \mathbb{Q}i$ (proper).

Corollary 2.16. *[1, Corollary 2.12] The non-real complex number $z = a + bi$ with b algebraic over $\mathbb{Q}(a)$ is non-Thalian if and only if b satisfies a non-constant irreducible polynomial $q(t^2)$ with coefficients in $\mathbb{Q}(a)$.*

Proof. Suppose z is non-Thalian so $X = \mathbb{Q}(a, b^2)$, $Y = \mathbb{Q}(a, b^2)b$ and $X \bigcap Y = \{0\}$. Since b is algebraic over $\mathbb{Q}(a)$, b satisfies a polynomial $q(t)$ over $\mathbb{Q}(a)$. If $q(t)$ has no odd terms, we're finished. Otherwise, let $q(t) = q_0 + q_1 t + \cdots + q_n t^n$ and without loss of generality, let n be odd. Then

$$
\begin{aligned}
& & 0 &= q_0 + q_1 b + \cdots + q_n b^n \\
&\Rightarrow & -q_0 - q_2 b^2 - \cdots - q_{n-1} b^{n-1} &= (q_1 + q_3 b^2 + \cdots + q_n b^{n-1}) b
\end{aligned}
$$

But since the $q_i \in \mathbb{Q}(a)$ it follows that the left hand side is in $\mathbb{Q}(a, b^2) = X$ and the right hand side is in $\mathbb{Q}(a, b^2)b = Y$. Since $X \bigcap Y = \{0\}$ it follows that both the left and right hand sides equal zero. That is b satisfies $f(t) = -q_0 - q_2 t^2 - \cdots - q_{n-1} t^{n-1}$ which has no odd terms.
Conversely, if b satisfies a non-constant irreducible polynomial $q(t^2)$ with coefficients in $\mathbb{Q}(a)$ then $-b$ is a conjugate to b and the degree of b over $\mathbb{Q}(a)$ isn't 1 so $b \notin \mathbb{Q}(a)$ and we may extend $\mathbb{Q}(a)$ by b. Let $\sigma : (\mathbb{Q}(a))(b) \to (\mathbb{Q}(a))(-b)$ be the unique isomorphism which fixes $\mathbb{Q}(a)$ and takes $b \mapsto -b$ as in Corollary 0.19. Then $b^2 \mapsto b^2$ so σ fixes $\mathbb{Q}(a, b^2) = X_1$. By the proof of Theorem 2.15, given any $w = w_1 + w_2 i \in \Pi[z]$, $\sigma(w_1) = w_1$ and $\sigma(w_2) = -w_2$. Thus, if $1 \cdot i$ were constructible then $\sigma(1) = -1$. However $1 \in \mathbb{Q}(a, b^2)$ implies $\sigma(1) = 1 \neq -1$ so $1 \notin Y$ and hence $1 \cdot i = i \notin \Pi[z]$ so z is non-Thalian. □

Corollary 2.17. *[1, Corollary 2.13] If $D < 1$ is a square-free integer, $z = \sqrt{D}$ is non-Thalian.*

Proof. $D < 1$ and $z = \sqrt{D}$ implies $z = \sqrt{|D|}i$ so $a = 0$ and $b = \sqrt{|D|}$. Thus b satisfies $x^2 - |D|$ which is irreducible since D is square-free and $\mathbb{Q}(a) = \mathbb{Q}$. Hence z is non-Thalian by the previous corollary. $\square$

Here we can make a slightly stronger statement:

Proposition 2.18. *If $D < 1$ is a not a perfect square, $z = \sqrt{D}$ is non-Thalian.*

Proof. $D < 1$ and $z = \sqrt{D}$ implies $z = \sqrt{|D|}i$ so $a = 0$ and $b = \sqrt{|D|}$. Thus b satisfies $x^2 - |D|$ which is irreducible since D is not a perfect square and $\mathbb{Q}(a) = \mathbb{Q}$. Hence z is non-Thalian by Corollary 2.16. $\square$

Corollary 2.19. *[1, Corollary 2.14] For $m > 2$, the root of unity $e^{i2\pi/m}$ is Thalian if and only if m is divisible by 4.*

Proof. Let $z = e^{i2\pi/m}$. If 4 divides m so $m = 4 \cdot n$, then $i = e^{i\pi/4} = \left(e^{i2\pi/m}\right)^{m/4} = z^{m/4} = z^n \in \Pi[z]$ since $\Pi[z]$ is a field. Hence, z is Thalian.
Conversely consider $(m, 4) < 4$ so 4 does not divide m. In this case, Lehmer [5] shows that $\mathbb{Q}(\sin(^{2\pi}/_{m}))$ has degree $\phi(m)$, where $\phi(m)$ is the number of positive integers less than m which are relatively prime to m. Since $\mathbb{Q}(a, b) = \mathbb{Q}(\cos(2\pi/m), \sin(2\pi/m))$ this shows that the degree of $\mathbb{Q}(a, b)$ is at least $\phi(m)$. Lehmer [5] also showed that $\mathbb{Q}(\cos(^{2\pi}/_{m}))$ has degree $^{\phi(m)}/_{2}$. Since $\sin^2(2\pi/m) = 1 - \cos^2(2\pi/m) \in \mathbb{Q}(\cos(2\pi/m))$ it follows that $\mathbb{Q}(a, b^2) = \mathbb{Q}(\cos(2\pi/m), \sin^2(2\pi/m)) = \mathbb{Q}(\cos(2\pi/m)$ has degree $^{\phi(m)}/_{2} < \phi(m)$ so $b \notin \mathbb{Q}(a, b^2)$ and z is non-Thalian by Theorem 2.15. $\square$

3 Pythagorean Constructions and Numbers

We now add Alperin's 4th axiom and continue by still assuming we begin with the points 0 and 1 in $\mathbb{C}$.

Pythagorean Axioms:

0. The set contains 3 points A, B, C, of the complex numbers, not all on a line.
1. The line connecting two constructible points is a constructible line.
2. The point of coincidence of two constructible lines is a constructible point.
3. The perpendicular bisector of the segment connecting two constructible points is a constructible line.
4. The line bisecting any given constructed angle can be constructed.

Definition 3.1. *Pythagorean Numbers, denoted $\mathbb{P}$ is the smallest subset of numbers in $\mathbb{C}$, closed under the Pythagorean Axioms, where we let $A = 0$, $B = 1$ and $C = i$.*

Definition 3.2. *Let $X_{\mathbb{P}}$ and $Y_{\mathbb{P}}$ to be the set of constructible real and imaginary parts of $\mathbb{P}$.*

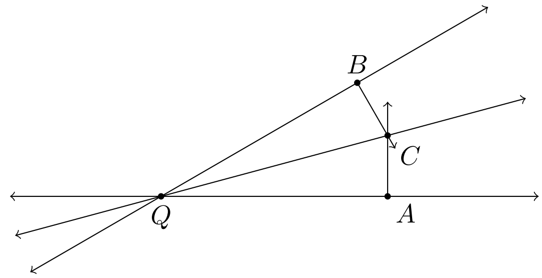
Theorem 3.3. *[1, Theorem 3.1] Given axioms (0) - (3), the following are equivalent:*

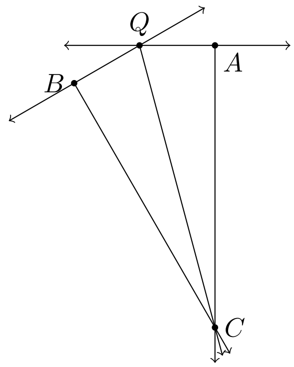
i) a unit length segment can be marked on any constructed ray;

ii) the angle bisector axiom (4);

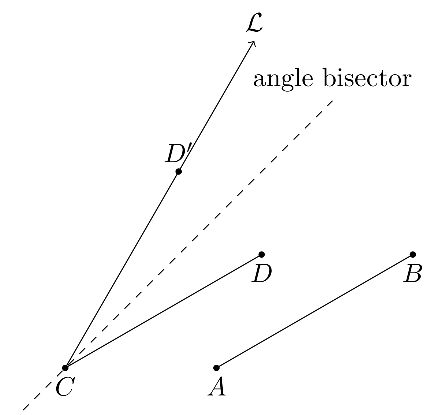
iii) a constructed segment's length can be marked on any other constructed ray.

Proof. iii) $\rightarrow$ i) is trivial since a unit length is the initial constructed segment's length.
i) $\rightarrow$ ii) Given two constructed lines intersecting at the point Q, construct the unit length on each ray of the angle to be bisected, letting the new points be A and B. We may then construct perpendiculars to the rays at each point. Let C be the intersection of these two perpendiculars. Then the triangles ΔQCB and ΔQCA are right triangles with $1 = |QA| = |QB|$ and that share the common side QC. Thus, they are congruent and the line through Q and C is the angle bisector of angle AQB. The figures below show both the acute and oblique cases.





ii) $\to$ iii) Given a constructed segment AB and a ray L originating from C, we may translate AB to originate from C to give segment CD by Lemma 2.2. Then construct line m as the angle bisector of CD and ray L. By Corollary 2.5 we may now reflect D in m to acquire point D' on L where CD' is of length $|AB|$.



□

The next corollary is to show a distinction between Thalian Numbers and Pythagorean Numbers. Above, we showed that with the angle bisector axiom (4), the Pythagorean constructions allow us to mark a unit length segment on any constructed ray. Now we will show an example of where this is not possible using only Thalian constructions.

Corollary 3.4. *[1, Corollary 3.2] The angle at the origin formed by* 1, *0 and* $z = e^{i\pi/k}$, *k an odd integer not equal to 1, can be bisected by Thalian constructions in* $\Pi[z]$ *but a unit length on that ray is not in* $\Pi[z]$.

Proof. Since $|z| = 1$ we may bisect the angle at the origin formed by 1, 0 and z by the proof of Theorem 3.3 i) $\rightarrow$ ii). That is, replace Q with 0, A with 1 and B with z in the figure above. Thus, the angle at the origin formed by 1, 0 and $z = e^{i\pi/k}$, may be bisected by Thalian constructions. For the sake of contradiction, suppose $w = e^{i\pi/2k}$, which has unit length on the constructed bisection, can be constructed. Then $w^k = e^{i\pi/2} = i$ is constructible, but this contradicts Corollary 2.19 which states that z is Thalian only if k is divisible by 4. Thus, the unit length on the constructed bisection may not be constructed. $\square$

In his proof, Alperin also explains that the constructed bisector from the above corollary "has a length which does not belong to X." This is just to say that, using only Thalian constructions, we may construct segments of lengths which are not in X. I have proven this claim in the appendix as Proposition A.5. Note this is an important distinguishing factor between Thalian and Pythagorean Numbers since Theorem 3.3 (iii) says that using Pythagorean constructions, every constructed length is in X.

Definition 3.5. *Let $\mathcal{P}$ be the smallest subfield of the real numbers containing $\mathbb{Q}$ which is closed under the operation $x \mapsto \sqrt{1+x^2}$.*

Theorem 3.6. *[1, Theorem 3.3] $\mathbb{P} = \mathcal{P} \bigoplus \mathcal{P}i$.*

Proof. Given any $x \in X_{\mathbb{P}}$, we may construct the point $x + i$ which has magnitude $\sqrt{1+x^2}$. By Theorem 3.3 we may then construct $\sqrt{1+x^2}$ and hence $\mathcal{P} \subseteq X_{\mathbb{P}}$.
By Proposition A.6, $X_{\mathbb{P}} \subseteq \mathcal{P}$ and hence $X_{\mathbb{P}} = \mathcal{P}$.
Since $\mathbb{P}$ contains i, Corollary 2.9 tells us that $X_{\mathbb{P}} = Y_{\mathbb{P}}$ and our result immediately follows. $\square$

Note I used my own Proposition A.6 in the appendix so that Theorem 3.6 became a corollary. In his paper, Alperin neglects to show the containment of $X_{\mathbb{P}}$ in $\mathcal{P}$ and states the theorem without a thorough proof. Alperin's neglect is simply because the induction proof used is tedious and when you begin thinking about it, the conclusion seems natural.
Alperin concludes this section by noting that $\mathcal{P}$ is equal to "the set of all real algebraic numbers which are obtained by extraction of (positive) square roots, and which are totally real, meaning that any of its algebraic conjugates are also real numbers." Let $\mathbb{A}$ be this described set. He gives a brief explanation for why $\mathcal{P}$ is contained in $\mathbb{A}$ and then refers us to Auckly and Cleveland's work [6] for the proof of containment in the other direction. For the sake of space and because this paper is not as concerned with totally real numbers, I too will leave out this proof and suffice it to quote Alperin: "It is easy to see that the positive Pythagorean reals are totally real since they are obtained from $\mathbb{Q}$, using only field operations, and the operation $\sqrt{1+x^2}$, which is a totally real number for any totally real number x." It is quite impressive that Auckly and Cleveland made this connection with totally real numbers back in 2000 as undergraduates. Alperin's paper "Trisections and Totally Real Origami" takes this connection to an even higher level, using the fact to show some interesting examples, such as the regular heptagon, of what new constructions may be made using origami folds. We shall discuss some of these interesting connections and constructions in the summary.

Note here that Theorem 3.3 tells us that $\mathcal{P}$ is really the set of all possible constructed lengths in $\mathbb{P}$. Thus $\sqrt{4+2\sqrt{2}} = \sqrt{1+(1+\sqrt{2})^2}$ is a constructible length since $\sqrt{2} = \sqrt{1+1} \in \mathcal{P}$. On the other hand, while we can construct both lengths $\sqrt{2}$ and $\sqrt{4+2\sqrt{2}}$, we may not construct a right triangle with a leg of length $\sqrt{2}$ and hypotenuse of length $\sqrt{4+2\sqrt{2}}$ since that would give the second leg a length of $\sqrt{2+2\sqrt{2}}$. This is a problem because the irreducible polynomial in $\mathbb{Q}$ for $\sqrt{2+2\sqrt{2}}$ is $x^4 - 4x^2 - 4$ which is also satisfied by $\sqrt{2-2\sqrt{2}}$ and this is not a real number. This shows us that while the field of real Pythagorean numbers is closed under $a\sqrt{1+(a/b)^2} = \sqrt{a^2+b^2}$ it is not closed under $\sqrt{a^2-b^2}$ since we just had $\sqrt{\sqrt{4+2\sqrt{2}}^2 - \sqrt{2}^2} = \sqrt{2+2\sqrt{2}} \notin \mathcal{P}$.

4 Euclidean Constructions and Numbers

Next we add Alperin's 5th axiom and continue by still assuming we begin with the points 0 and 1 in $\mathbb{C}$.

Euclidean Origami Axioms:

1. The line connecting two constructible points is a constructible line.
2. The point of coincidence of two constructible lines is a constructible point.
3. The perpendicular bisector of the segment connecting two constructible points is a constructible line.
4. The line bisecting any given constructed angle can be constructed.
5. Given a constructed line l and constructed points P, Q, then whenever possible, the line through Q, which reflects P onto l, can be constructed.

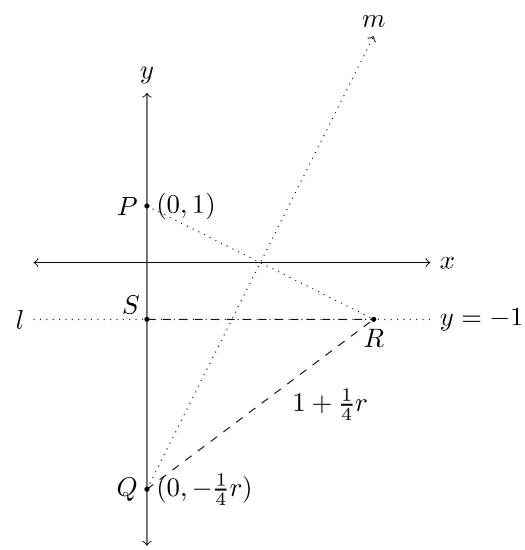
Definition 4.1. *Euclidean Origami Numbers, denoted $\mathcal{E}$ is the smallest subset of numbers in $\mathbb{C}$, closed under the Euclidean Origami Axioms, beginning with just 0 and 1.*

Definition 4.2. *Let $X_{\mathcal{E}}$ and $Y_{\mathcal{E}}$ to be the set of constructible real and imaginary parts of $\mathcal{E}$.*

Note that the Euclidean Origami Axioms do not include Alperin's Axiom (0) since the Euclidean Origami Numbers are an extension of the Pythagorean Numbers which we already know contain i. This also implies $X_{\mathcal{E}} = Y_{\mathcal{E}}$ just as $X_{\mathbb{P}} = Y_{\mathbb{P}}$. The very interesting thing about the Euclidean Origami Numbers is that they are exactly the Euclidean Numbers, $\mathbb{E}$, obtainable using a compass and straightedge. The Euclidean Numbers have long been known to be the smallest field containing $\mathbb{Q}$ and closed under taking square roots. To see that $\mathcal{E} = \mathbb{E}$, Alperin first claimed that given a point P and line l, that we may construct the parabola with focus P and directrix l. However, this is a falsity since it would imply that we could construct every real number and hence all of $\mathbb{C}$ - not at all what we are about to prove. What Alperin meant was that we could construct some subset of the parabola defined by focus P and directrix l. In part due to this and in part because I've simplified the proof, I will circumvent his entire parabola discussion. In order to prove that $\mathcal{E} = \mathbb{E}$, I will need to show that given $z = re^{i\theta}$, I may construct $\sqrt{r}e^{i\theta/2}$. To do this, I begin with the following proposition.

Proposition 4.3. *Given any $r \in \mathcal{E} \bigcap \mathbb{R} > 0$, we may construct $\sqrt{r}$.*

Proof. As in axiom (5), take $P = (0, 1)$, l given by $y = -1$ and $Q = (0, -\frac{1}{4}r)$. Note Q is constructible since $Y_{\mathcal{E}}$ is a field and $X_{\mathcal{E}} = Y_{\mathcal{E}}$. Construct the line m through Q which reflects P onto l with the reflection point having $x > 0$. Construct the perpendicular m' to m through P. Let the intersection of m' and l be R, the reflection of P in m. Now, ΔPQR is isosceles with m being the angle bisector [resp. perpendicular bisector] of $\angle PQR$ [resp. segment PR]. Thus $|QR| = |QP| = 1 + \frac{1}{4}r$. Let $S = (0, -1)$ so S, R and Q form a right triangle with vertical leg of length $\frac{1}{4}r - 1$ and hypotensue $|QR| = 1 + \frac{1}{4}r$. Thus $|SR| = \sqrt{\left(1 + \frac{1}{4}r\right)^2 - \left(-1 + \frac{1}{4}r\right)^2} = \sqrt{r}$.



∎

Theorem 4.4. *[1, Theorem 4.1] The constructible points in $\mathbb{C}$, obtained by using axioms (1) - (5), starting with the numbers 0 and 1, the field of Euclidean Origami Numbers $\mathcal{E}$, is the smallest subfield of $\mathbb{C}$ closed under square roots, the Euclidean Numbers $\mathbb{E}$.*

Proof. Suppose that after taking either a field operation or square root n times, you come up with an element $z = re^{i\theta} \in \mathbb{E}$ which is still in $\mathcal{E}$. Then $\sqrt{z} = \sqrt{r}e^{i\frac{\theta}{2}}$ is in $\mathcal{E}$ since $\sqrt{r} \in \mathcal{E}$ by the previous proposition and $e^{i\frac{\theta}{2}}$ is in $\mathcal{E}$ since this is simply angle bisection. Thus $\mathbb{E} \subseteq \mathcal{E}$ by induction.
On the other hand, given any $z = x + iy \in \mathcal{E}$, I have shown in Proposition A.7 that $x, y \in \mathbb{E}$ and thus $z \in \mathbb{E}$. This shows $\mathcal{E} \subseteq \mathbb{E}$ and therefore $\mathcal{E} = \mathbb{E}$. ∎

Of interest is how to minimize the number of axioms necessary to construct $\mathcal{E}$. We will show that we can actually discard axioms (1) and (4) and still maintain $\mathcal{E}$ with the remaining axioms (2), (3) and (5). We state this as a theorem.

Theorem 4.5. *[1, Theorem 4.2] The field of Euclidean Origami Numbers $\mathcal{E}$ is the smallest subset of constructible points in the complex numbers $\mathbb{C}$, which contains the numbers 0 and 1 and is closed under the axioms:*

(α) *The point of coincidence of two constructible lines is a constructible point.*

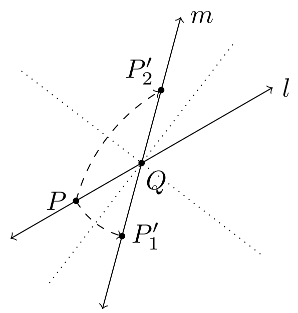
(β) *The perpendicular bisector of the segment connecting two constructible points is a constructible line.*

(γ) *Given a constructed line l and constructed points P, Q, then whenever possible, the line through Q, which reflects P onto l, can be constructed.*

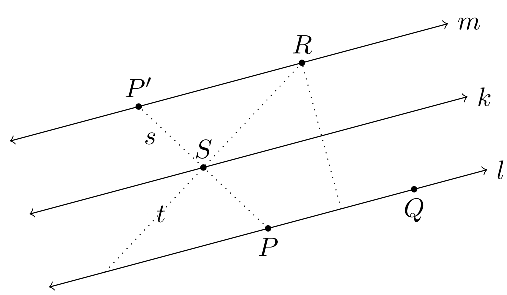
Here I consider two cases, one of which is the angle bisector of an angle formed at a point in $\mathbb{C}$ and the other is where the angle is formed at a point at infinity (so the lines which form the angle are parallel).

Proof. To obtain axiom (1) which states "The line connecting two constructible points is a constructible line," take any constructible points P and Q. Then (β) allows us to construct the line l as the perpendicular bisector of P and Q. (γ) allows us to construct the line m through Q which reflects P onto l. Again by (γ), we may now construct the line through P wich reflects Q onto m. Since Q is already on m, this line goes through P and Q.
Next we obtain axiom (4) which states "the line bisecting any given constructed angle can be constructed," in the following manner: Given two lines l and m we consider first the case where l and m intersect. Let Q

be the intersection of l and m and take any other constructible point P on l. Then axiom (5) allows us to construct either line through Q which reflects P onto m. This line is the angle bisector.



If l and m are parallel then we take any 2 constructed points P and Q on l and by (β) construct their perpendicular bisector and let its intersection with m be R. Then use (γ) to construct the line s through P which reflects R onto l. Let P' be the intersection of s with m. By (β), construct the line t as the perpendicular bisector of PP' letting S be the intersection of s and t. Then S is halfway between l and m. Note there are two lines through S which reflect P onto m (see note after Proposition A.7), one of which is t since s and t cross at right angles and S is halfway between l and m, and the other of which is parallel to l and m. We then use (γ) one last time to construct the line k through S which reflects P onto m and is parallel to m and l. k is then our angle bisector.



□

5 Conic Constructions and Origami Numbers

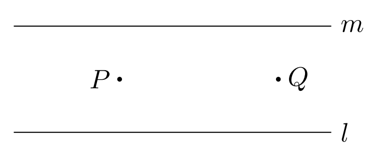
Finally we add Alperin's 6th axiom to complete the description of Origami Numbers. We continue by still assuming we begin with the points 0 and 1 in $\mathbb{C}$.

Origami Axioms:

1. The line connecting two constructible points is a constructible line.
2. The point of coincidence of two constructible lines is a constructible point.
3. The perpendicular bisector of the segment connecting two constructible points is a constructible line.
4. The line bisecting any given constructed angle can be constructed.
5. Given a constructed line l and constructed points P, Q, then whenever possible, the line through Q, which reflects P onto l, can be constructed.

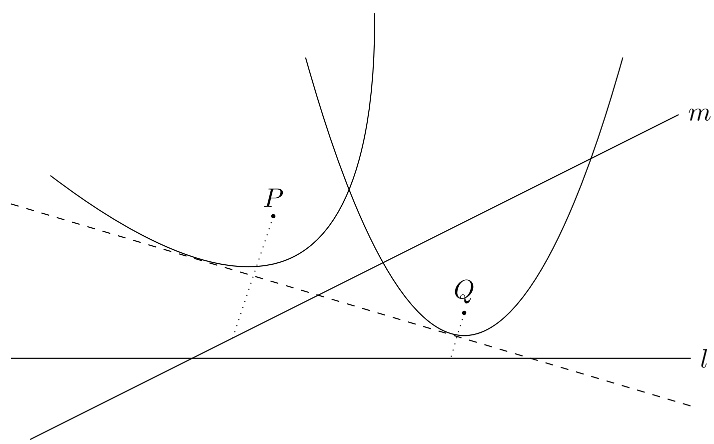
6. Given constructed lines l, m and constructed points P, Q, then whenever possible, any line which simultaneously reflects P onto l and Q onto m, can be constructed.

In Axiom (6) it is of interest to note a situation in which P and Q cannot simultaneously be reflected onto l and m. An easy example is when m and l are parallel with P and Q both lying halfway between l and m.



Definition 5.1. *Origami Numbers, denoted $\mathcal{O}$, is the smallest subset of numbers in $\mathbb{C}$, closed under the Origami Axioms, beginning with just 0 and 1.*

This idea of folding a line which simultaneously takes two separate points to two different lines is actually synonymous with constructing a common tangent to the two parabolas with foci P and Q and respective directrices l and m.



Lemma 5.2. *[1, Lemma 5.1] The intersection points and common tangents of two distinct non-degenerate conics with equations defined over $\mathcal{O}$ can be constructed by origami methods defined by axioms (1)-(6).*

For this reason, the Origami Axioms are also Conic Constructions and Origami Numbers are exactly the Conic Constructible Points. The next two theorems allow us to complete our classification of Origami Numbers.

Definition 5.3. *Let $\mathcal{O}_{\mathbb{R}}$ be the real subfield of the origami complex numbers $\mathcal{O}$.*

Theorem 5.4. *[1, Theorem 5.2] The constructible points in $\mathbb{C}$, obtained by using axioms (1)-(6), starting with the numbers 0 and 1, is the field of origami constructible numbers, $\mathcal{O}$; it is the smallest subfield of $\mathbb{C}$ closed under square roots, cube roots and complex conjugation. This field $\mathcal{O} = \mathcal{O}_{\mathbb{R}} \bigoplus i\mathcal{O}_{\mathbb{R}}$ is also the set of conic constructible points. The field $\mathcal{O}_{\mathbb{R}}$ is the smallest subfield of the reals closed under arbitrary (real) cube roots and square roots of its positive elements.*

Theorem 5.5. *[1, Theorem 5.3] The field of origami constructible numbers $\mathcal{O}$ is the smallest subset of constructible points in the complex numbers $\mathbb{C}$, which contains the numbers 0 and 1, and is closed under the axioms:*

(α) *The point of coincidence of two constructible lines is a constructible point.*

(β) *The perpendicular bisector of the segment connecting two constructible points is a constructible line.*

(γ) *Given a constructed line l and constructed points P, Q, then whenever possible, the line through Q, which reflects P onto l, can be constructed.*

(δ) *Given constructed lines l, m and constructed points P, Q, then whenever possible, any line which simultaneously reflects P onto l and Q onto m, can be constructed.*

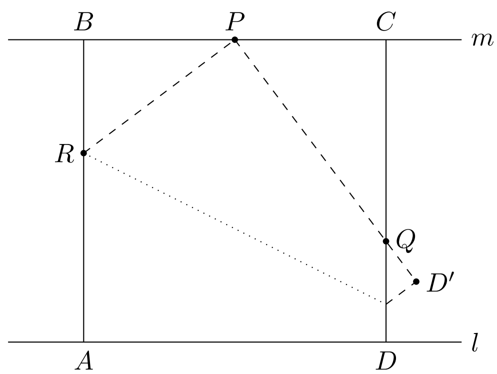
6 Trisecting an Angle

We now use Origami for the application of trisecting an angle, a feat which is impossible using only a straightedge and compass.

Theorem 6.1. *It is possible to trisect an angle using the Origami Axioms.*

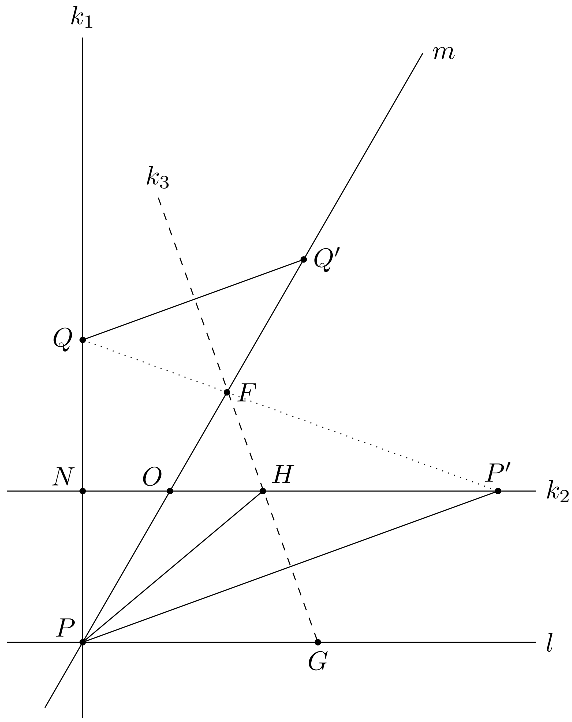
Here I consider two cases, one of which is the angle trisector of an angle formed at a point in $\mathbb{C}$ and the other is where the angle is formed at a point at infinity (so the lines forming the angle are parallel).

Proof. First let's look at the case where we start with two lines l and m which are parallel. Take any constructible point A on l and construct the line k_1 perpendicular to l through A. Let the intersection of k and m be B. Construct the angle bisector of the angle formed at B by k_1 and m and let the its intersection with l be D. Construct a line k_2 perpendicular to l through D and let its intersection with m be C. You now have square $ABCD$. Construct the perpendicular bisector of BC and let its intersection with m be P. Construct the perpendicular bisector of AP as line k_3 and let its intersection with k_1 be R. Reflect D in k_3 to obtain D' and then construct the line through P and D' to obtain the point Q as the intersection of PD' and k_2.



Assume $|AB| = 1$ so $|BP| = |PC| = 1/2$. Let $|RB| = x$ and $CQ = y$. Note that RP is the reflection of RA and PD' is the reflection of AD so $\angle RPD = 90°$. Also, this tells us that $|RP| = 1 - x$. Thus $1 - x = \sqrt{1/4 + x^2}$ implying that $x = 3/8$. Since $\angle RPD = 90°$ we have $\triangle RBP \sim \triangle PCQ$ and thus $\frac{y}{.5} = \frac{.5}{x}$ implying $y = 2/3$. Therefore the line perpendicular to k_2 through Q and the perpendicular bisector of QC trisect l and m. [8]

Now for the case where l and m are not parallel. Let P be their point of intersection. First construct the line k_1 perpendicular to l through P and choose any point Q on k_2. Construct the perpendicular bisector of PQ as line k_2. Let the intersection of k_1 and k_2 be N and the intersection of k_2 and m be O. Using (6), construct the line k_3 which simultaneously reflects Q onto m and P onto k_2. Let F be the intersection of k_3 with m, H the intersection of k_3 with k_2 and G the intersection of k_3 with l.



Let $\angle NP'Q = \alpha$. Since NP' is the perpendicular bisector of PQ, we have $PP'Q$ isosceles so $\angle NP'P = \alpha$. Since l is parallel to k_2 we have $\angle GPP' = \alpha$. Since P' is the reflection of P over k_3 with H on k_3 we have PHP' isosceles so $\angle P'PH = \alpha$. Since F is on k_3 we have PFP' isosceles so $2\alpha = \angle PP'F = \angle P'PF$ implying $\angle HPF = \alpha$. Therefore PP' and PH trisect l and m. [7]

□

There is also the degenerative case where l and m are at right angles. The above proof still works, however we will have $m = k_1$ so $Q = Q'$ and instead of needing axiom (6) we only need to use axiom (5) which allows us to construct the line through Q which reflects P onto k_2. From this we see that right angles may be trisected using only Euclidean Origami Axioms or a compass and straight edge.

7 Summary

As I was going through the paper there was one thing that jumped out at me where further research may be done. In Corollary 2.11, we discuss the consequences to the Thalian Numbers $\Pi[z]$ when $z = a + bi$ with b (real) algebraic. What happens if we choose z with b transcendental? It seems to be of some value to know for exactly which b we end up with X equaling Y - which is why Corollary 2.11 was even laid down, so why not discuss all possibilities for b?

This concludes the classification of numbers constructible using the Huzita-Hitori Axioms. It is interesting to note that Alperin also proved that, given axioms (1), (2) and (4), that axiom (6) holds if and only if any arbitrary angle may be constructed [7]. While this is a very new field of study in mathematics, it has its roots in an art that has been around for centuries and the mathematics has quickly blossomed over the last 24 years. While the solid ground work was laid out in the Proceedings of the First International Meeting of Origami Science and Technology in only 1989, the meetings have become more regular and the proceedings take up larger and larger volumes - the latest of which is *Origami^5: Fifth International Meeting of Origami Science, Mathematics, and Education* [11] . Alperin himself has taken the classification of Origami Numbers further in his paper "Trisections and Totally Real Origami" where he re-identifies the real subfield of the Pythagorean Numbers as the totally real subfield of the Euclidean numbers and the real subfield of Origami Numbers as the totally real subfield of the Vie´ten Numbers [7]. Alperin and Lang then took this work even further in their paper “One-, Two-, and Multi-Fold Origami Axioms” where they explore the classification of the subfields of $\mathbb{C}$ you may obtain by allowing more than one fold to occur at a time [3]! What is amazing is how this field is not only applied to folding small animals or trumping Euclidean Constructions, but how it is applied to modern science. There are many examples of origami being used to innovate new technology, one of which would be Lawrence Livermore National Laboratory’s Eyeglass Telescope which is being designed to be the largest space telescope at a size about that of the Island of Manhattan! They are utilizing origami to find a way to fold the telescope to a size that may be deployed from earth and then unfolded automatically in space [12]. In all, origami is a fascinating science for reasons of art, mathematics and technology and one that may be appreciated by everybody.

Appendix

A

Proposition A.1. *Let $z = a + bi \in \mathbb{C}$. Then $\mathbb{Q}(z, \bar{z}, i) = \mathbb{Q}(a, b, i)$.*

Proof. Since $z = a + bi$ and $\bar{z} = a - bi$ are both in $\mathbb{Q}(a, b, i)$, we have $\mathbb{Q}(z, \bar{z}, i) \leq \mathbb{Q}(a, b, i)$. On the other hand $a = \frac{1}{2}(z + \bar{z}) \in \mathbb{Q}(z, \bar{z}, i)$ and $b = \frac{1}{2}(z - \bar{z}) \in \mathbb{Q}(z, \bar{z}, i)$ so $\mathbb{Q}(a, b, i) \leq \mathbb{Q}(z, \bar{z}, i)$ Thus
$\mathbb{Q}(z, \bar{z}, i) = \mathbb{Q}(a, b, i)$. □

Proposition A.2. *For a given $z = a + bi \notin \mathbb{R}$, $\Pi[z] \subseteq \mathbb{Q}(a, b, i)$.*

Proof. Suppose $v = v_1 + v_2 i, w = w_1 + w_2 i \in \mathbb{Q}(a, b, i)$. Then $v_1, v_2, w_1, w_2 \in \mathbb{Q}(a, b)$.
I will proceed in $\mathbb{R}^2$ for the ease of writing equations of lines and finding their intersections. Thus we look at the lines obtainable via the points $v = (v_1, v_2)$ and $w = (w_1, w_2)$.
The line through v and w is given by $y = \frac{w_2 - v_2}{w_1 - v_1}(x - w_1) + w_2$. Note $\frac{w_2 - v_2}{w_1 - v_1}, w_1, w_2 \in \mathbb{Q}(a, b)$ since $\mathbb{Q}(a, b)$ is a field.
The perpendicular bisector of the segment from v to w is given by $y = \frac{w_1 - v_1}{v_2 - w_2}\left(x - \frac{v_1 + w_1}{2}\right) + \frac{v_2 + w_2}{2}$. Again, note $\frac{w_1 - v_1}{v_2 - w_2}, \frac{v_1 + w_1}{2}, \frac{v_2 + w_2}{2} \in \mathbb{Q}(a, b)$ since $\mathbb{Q}(a, b)$ is a field.
Thus, given 2 constructible points in $\mathbb{Q}(a, b, i)$, the constructible lines via these 2 points are of the form $y = m(x - c) + d$ where $m, c, d \in \mathbb{Q}(a, b)$. Given 2 such lines, $y = m_1(x - c_1) + d_1$ and $y = m_2(x - c_2) + d_2$, their intersection is $\left(\frac{-m_2c_2 + d_2 + m_1c_1 - d_1}{m_1 - m_2}, \frac{m_1m_2(c_1 - c_2) + d_2m_1 - d_1m_2}{m_1 - m_2}\right)$. Note $\frac{-m_2c_2 + d_2 + m_1c_1 - d_1}{m_1 - m_2}, \frac{m_1m_2(c_1 - c_2) + d_2m_1 - d_1m_2}{m_1 - m_2} \in \mathbb{Q}(a, b)$ since $\mathbb{Q}(a, b)$ is a field. Hence $\frac{-m_2c_2 + d_2 + m_1c_1 - d_1}{m_1 - m_2} + \frac{m_1m_2(c_1 - c_2) + d_2m_1 - d_1m_2}{m_1 - m_2} i \in \mathbb{Q}(a, b, i)$. Since the first three points, 0,1 and z with which we start with are in $\mathbb{Q}(a, b, i)$ and every point in $\Pi[z]$ is build up from these using the Thalian Axioms, it follows that $\Pi[z] \subseteq \mathbb{Q}(a, b, i)$. □

Proposition A.3. *Suppose $z = a + bi$ with $b \notin X_1 = \mathbb{Q}(a, b^2)$. Then given any $w = w_1 + w_2 i \in \Pi[z]$ we will have $w_1 \in X_1$, $w_2 \in X_1 b$, $\phi(w_1) = w_1$ and $\phi(w_2) = -w_2$.*

Proof. Suppose $u = u_1 + u_2 i, v = v_1 + v_2 i \in \Pi[z]$ with $u_1, v_1 \in X_1$, $u_2, v_2 \in X_1 b$, $\phi(u_1) = u_1$, $\phi(v_1) = v_1$, $\phi(u_2) = -u_2$ and $\phi(v_2) = -v_2$. Then the line of through u and v is given by $y = \frac{v_2 - u_2}{v_1 - u_1}(x - v_1) + v_2$ and the perpendicular bisector of the segment through u and v is given by $y = \frac{v_1 - u_1}{u_2 - v_2}\left(x - \frac{u_1 + v_1}{2}\right) + \frac{u_2 + v_2}{2}$. Note $\frac{v_1 - u_1}{u_2 - v_2} \in X_1 b$, $\frac{v_2 - u_2}{v_1 - u_1} \in X_1 b$, $\frac{u_1 + v_1}{2} \in X_1$ and $\frac{u_2 + v_2}{2} \in X_1 b$ since X_1 is a field. Thus, from two points with the given conditions we may only construct lines of the form $y = m(x - c) + d$ with $m, d \in X_1 b$ and $c \in X_1$. Suppose $y = m_1(x - c_1) + d_1$ and $y = m_2(x - c_2) + d_2$ are two such lines. Then their intersection is at the point $\left(\frac{-m_2c_2 + d_2 + m_1c_1 - d_1}{m_1 - m_2}, \frac{m_1m_2(c_1 - c_2) + d_2m_1 - d_1m_2}{m_1 - m_2}\right) = (w_1', w_2')$. Note that $\frac{-m_2c_2 + d_2 + m_1c_1 - d_1}{m_1 - m_2} \in X_1$ and $\frac{m_1m_2(c_1 - c_2) + d_2m_1 - d_1m_2}{m_1 - m_2} \in X_1 b$. Since 0, 1 and z all satisfy the conditions, by induction we have shown that for any $w = w_1 + w_2 i \in \Pi[z]$ we will have $w_1 \in X_1$ and $w_2 \in X_1 b$.
Since ϕ fixes X_1 and $w_1' \in X_1$ we have $\phi(w_1') = w_1'$. Since $w_2' \in X_1 b$ it follows that $w_2' = x \cdot b$ for some $x \in X_1$ and thus $\phi(w_2') = \phi(x \cdot b) = \phi(x)\phi(b) = x(-b) = -x \cdot b = -w_2'$. □

Proposition A.4. *Suppose a field N is a finite extension of a field M which is in turn a finite extension of a field L. Further suppose $[N : L] = 2$. Then $M = N$ or $M = L$.*

Proof. By Theorem 0.20, $2 = [N : L] = [N : M][M : L]$ so either $[N : M] = 1$ or $[M : L] = 1$. But, if the degree of the extension is 1 then it is a trivial extension, so $M = N$ or $M = L$. □

Proposition A.5. *Let $z = e^{i\pi/k}$ with $k > 1$ an odd integer. Let l be the angle bisector of angle formbed by 1 and z about the origin. Then the length $\frac{1}{1+\mu^2}$, where μ is the slope of l, can be constructed on l and is not in X.*

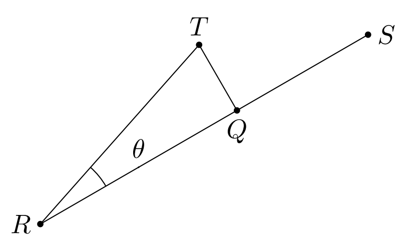
Proof. Construct the perpendicular m to l through 1 and let the intersection of m and l be the point P so that we have created a right triangle with vertices 0, 1 and P. Let the opposite side from the angle at the origin have length c and the adjacent side have length d. Then $c = d\mu$ so $d^2 + (d\mu)^2 = 1$ which leads to $d = \frac{1}{\sqrt{1+\mu^2}}$ as a constructible length on l. On the other hand, if this length were in X then we could construct the perpendicular m' to the real-axis through $\frac{1}{\sqrt{1+\mu^2}}$ and let the intersection of m' and l be Q so that we have created a right triangle with vertices 0, $\frac{1}{\sqrt{1+\mu^2}}$ and Q. Then the length of the side opposite from the angle at the origin is $\frac{\mu}{\sqrt{1+\mu^2}}$ giving a hypotenuse of length 1 which contradicts the previous corollary so $\frac{1}{\sqrt{1+\mu^2}} \notin X$. □

Clearly $\mathcal{P}$ is a subfield of $\mathbb{E}$ since it is the smallest field containing $\mathbb{Q}$ closed under certain square roots while $\mathbb{E}$ is the smallest field containing $\mathbb{Q}$ closed under any square root. We use this to prove the following.

Proposition A.6. $X_{\mathbb{P}} \subseteq \mathcal{P}$.

In this proof I will work in $\mathbb{R}^2$ to make working with equations of lines more fluid.

Proof. We proceed by induction. Suppose after n constructions every point has coordinates which are both in $\mathcal{P}$. Take any 2 such constructed points $S = (s_1, s_2)$ and $T = (t_1, t_2)$. Then the line through S and T is given by $y = \frac{t_2 - s_2}{t_1 - s_1}(x - s_1) + s_2$ and the perpendicular bisector of S and T is given by $y = \frac{s_1 - t_1}{t_2 - s_2}\left(x - \frac{s_1 + t_1}{2}\right) + \frac{s_2 + t_2}{2}$. In both of these cases the lines are of the form $y = mx + d$ where m and d are both in $\mathcal{P}$ since they are constructed using only field operations.
Take a third previously constructed point $R = (r_1, r_2)$ and let $\theta = \angle TRS$. Then the angle bisector is given by $y = \tan(\theta/2)(x - r_1) + r_2$. Let Q be the projection of T onto $\overrightarrow{ST}$.



Then

$$|RQ| = |RT|cos\theta = \frac{\overrightarrow{RT} \cdot \overrightarrow{RS}}{|RS|}$$
$$= \frac{(t_1 - r_1)(s_1 - r_1) + (t_2 - r_2)(s_2 - r_2)}{\sqrt{(s_2 - r_2)^2 + (s_1 - r_1)^2}}$$

and

$$|RT| = \sqrt{(t_2 - r_2)^2 + (t_1 - r_1)^2}$$

so

$$|QT| = \frac{(t_2 - r_2)(s_1 - r_1) - (t_1 - r_1)(s_2 - r_2)}{\sqrt{(s_2 - r_2)^2 + (s_1 - r_1)^2}}$$

Putting this together we get

$$
\begin{aligned}
\tan(\theta/2) &= \csc\theta - \cot\theta \\
&= \frac{\sqrt{(s_2-r_2)^2+(s_1-r_1)^2}}{(t_2-r_2)(s_1-r_1)-(t_1-r_1)(s_2-r_2)} - \frac{t_1-r_1)(s_1-r_1)+(t_2-r_2)(s_2-r_2)}{(t_2-r_2)(s_1-r_1)-(t_1-r_1)(s_2-r_2)} \\
&= \frac{(s_2-r_2)\sqrt{1+\left(\frac{s_1-r_1}{s_2-r_2}\right)^2}}{(t_2-r_2)(s_1-r_1)-(t_1-r_1)(s_2-r_2)} - \frac{t_1-r_1)(s_1-r_1)+(t_2-r_2)(s_2-r_2)}{(t_2-r_2)(s_1-r_1)-(t_1-r_1)(s_2-r_2)}.
\end{aligned}
$$

Thus $\tan(\theta/2) \in \mathcal{P}$ since it is built using only field operations and $\sqrt{1+\left(\frac{s_1-r_1}{s_2-r_2}\right)^2}$ and the angle bisector of $\angle TRS$ is of the form $y = mx + d$ with m and d in $\mathcal{P}$.

Given two lines $y = m_1x + d_1$ and $y = m_2x + d_2$ their point of intersection is $\left(\frac{d_2-d_1}{m_1-m_2}, m_1\frac{d_2-d_1}{m_1-m_2} + d_1\right)$. Now both the x and y coordinates are in $\mathcal{P}$ since they are built using elements of $\mathcal{P}$ and field operations. Since our original points have coordinates in $\mathcal{P}$ it follows by induction that $(x, y) \in \mathcal{P} \bigoplus \mathcal{P}$ for all $(x, y) \in \mathbb{P}$ so $X_{\mathbb{P}} \subseteq \mathcal{P}$. ☐

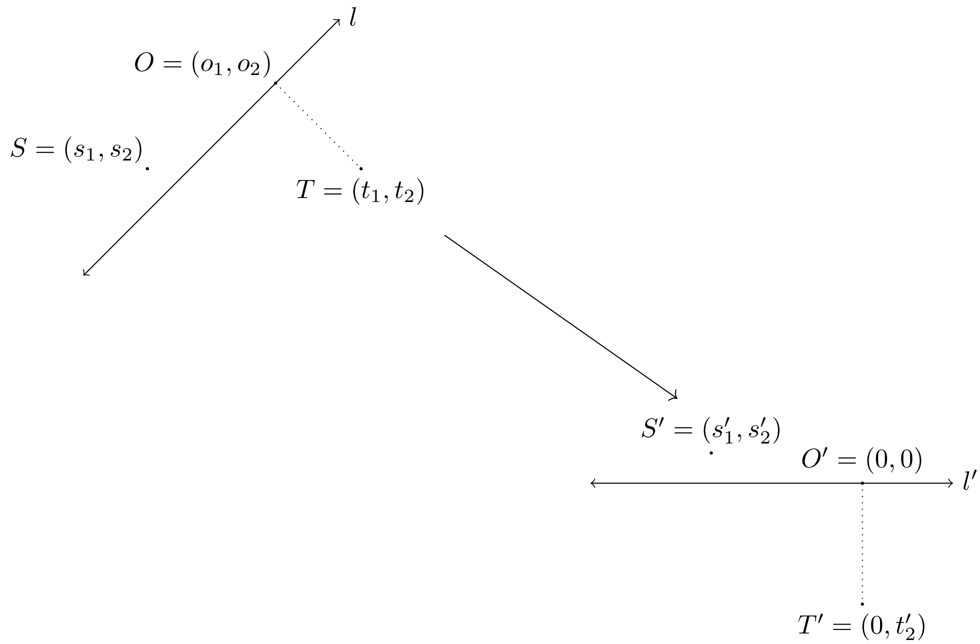
Proposition A.7. *Every $x \in X_{\mathcal{E}}$ and $y \in Y_{\mathcal{E}}$ may be written using nothing but field operations and square roots, thus showing $\mathcal{E} \subseteq \mathbb{E}$.*

In this proof I will work in $\mathbb{R}^2$ to make working with equations of lines more fluid.

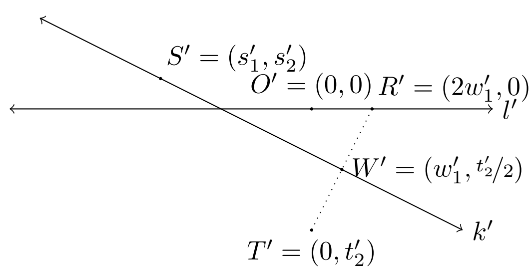
Proof. Suppose after n constructions using the Euclidean Origami Axioms, every line is of the form $y = mx + d$ where m and d are both in $\mathbb{E}$ and every point has coordinates which are both in $\mathcal{E}$. Take any 2 such constructed points $S = (s_1, s_2)$ and $T = (t_1, t_2)$. By Proposition A.6 we know that both the perpendicular bisector and the line going through these two points are of the form $y = mx + d$ where m and d are both in $\mathcal{E}$. Take a third previously constructed point $R = (r_1, r_2)$. Again by Proposition A.6 the angle bisector of $\theta = \angle TRS$ is of the form $y = mx + d$ where m and d are both in $\mathcal{P} \subset \mathbb{E}$.
Now take any previously constructed line l and drop a perpendicular from T to l, letting the intersection be $O = (o_1, o_2)$. Let $u = |T - O|$ and let

$$
\mathcal{L}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{u}{(t_1-o_1)^2+(t_2-o_2)^2}\begin{pmatrix} t_2-o_2 & -(t_1-o_1) \\ t_1-0_1 & t_2-o_2 \end{pmatrix}\begin{pmatrix} x_1-o_1 \\ x_2-o_2 \end{pmatrix}
$$

which is the translation and rotation of a vector $X = (x_1, x_2)$ which takes T to the negative $y - axis$ since $\mathcal{L}\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = \begin{pmatrix} 0 \\ u \end{pmatrix}$. Then, for each of O, T and S apply $\mathcal{L}$ to obtain $O' = (0, 0)$, $T' = (0, t'_2)$ and $S' = (s'_1, s'_2)$.



Now, use axiom (5) to construct a line k' through S' which reflects T' to R' on l' and then construct $T'R'$, letting the intersection of k' and $T'R'$ be $W' = (w'_1, w'_2)$. Then basic geometry tells us that $w'_2 = t'_2/2$ and $r'_1 = 2w'_1$.



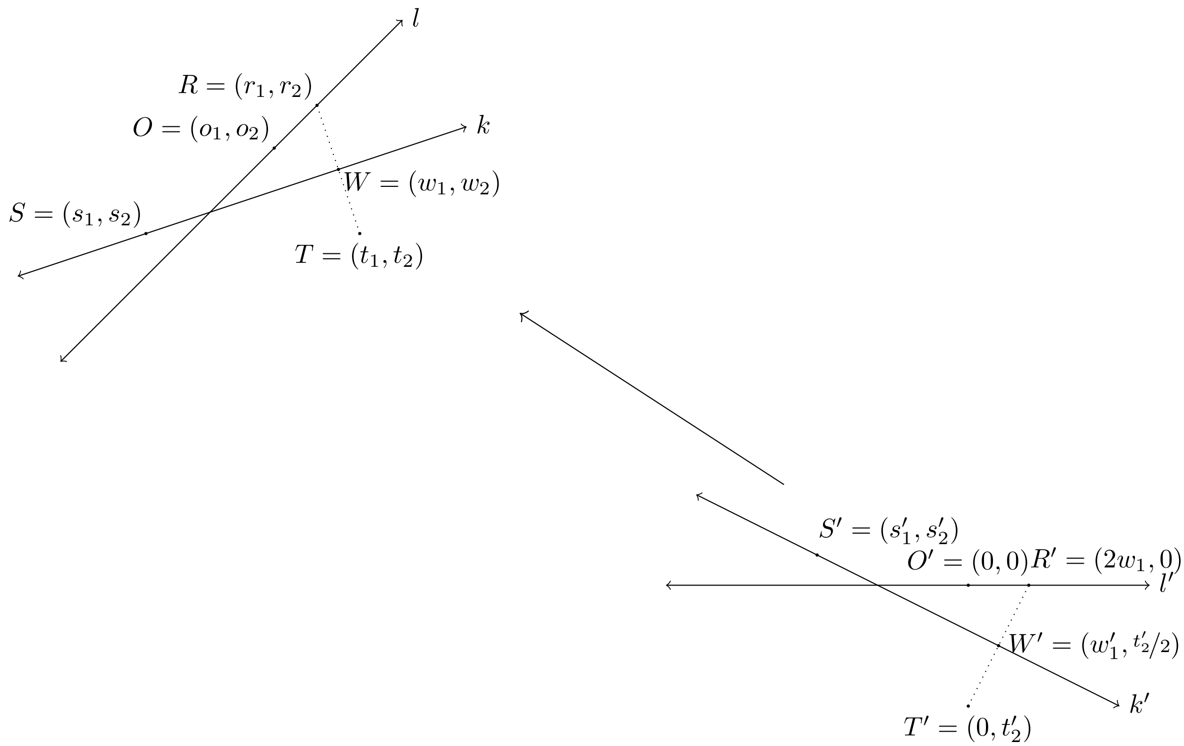
Since $T'R'$ is perpendicular to k', k' must have a slope of $\frac{2w'_1}{t'_2}$ and thus k' has equation $y = \frac{2w'_1}{t'_2}(x - w'_1) + \frac{t'_2}{2}$. Since (s'_1, s'_2) falls on k', we get the following:

$$\begin{aligned} s'_2 &= \frac{2w'_1}{t'_2}(s'_1 - w'_1) + \frac{t'_2}{2} \\ 4(w'_1)^2 - 4s'_1 w'_1 + 2t'_2 s'_2 - (t'_2)^2 &= 0 \\ w'_1 &= \frac{4s'_1 \pm \sqrt{16(s'_1)^2 - 16(2t'_2 s'_2 - (t'_2)^2)}}{8} \\ &= \frac{1}{2}(s'_1 \pm \sqrt{(s'_1)^2 - 2t'_2 s'_2 + (t'_2)^2}) \end{aligned}$$

Now, $\mathcal{L}$ transforms S and T so that s'_1, s'_2 and t'_2 are made up of only field operations and square roots so w'_1 is only made up only of field operations and square roots. Since $R' = (2w'_1, 0)$, its coordinates are also only made up of field operations and square roots. And since $w'_2 = \frac{t'_2}{2}$, it too is only made up of field operations and square roots.
Next note that

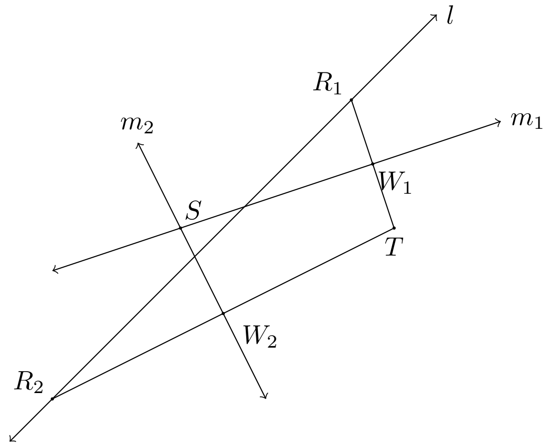
$$\mathcal{L}^{-1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\frac{1}{u}\begin{pmatrix}t_2-o_2 & t_1-o_1\\-(t_1-0_1 & t_2-o_2)\end{pmatrix}+\begin{pmatrix}o_1\\o_2\end{pmatrix}$$

which is the rotation and translation that takes S', T' and O' back to S, T and O respcetively. Then apply $\mathcal{L}^{-1}$ to W' and R' to obtain W and R as shown below.



Since $\mathcal{L}^{-1}$ is a linear transformation of elements which are made up of square roots and field operations and then a translation which is only a field operation, it follows that w_1, w_2, r_1 and r_2 are all made up only of square roots and field operations.
Therefore k has equation $y=mx+d$ where $m=\frac{w_2-s_2}{w_1-s_1}$ and $d=s_1\frac{s_2-w_2}{w_1-s_1}+s_2$, which are both clearly made up only of field operations and square roots, so y is of the form we desire.
Then, if we take any two lines $y=m_1x+d_1$ and $y=m_2x+d_2$ with $m_1,m_2,d_1,d_2\in\mathbb{E}$, their intersection is $\left(\frac{d_2-d_1}{m_1-m_2}, m_1\frac{d_2-d_1}{m_1-m_2}+d_1\right)$ which clearly has coordinates in $\mathbb{E}$ since they are made up using only field operations and elements of $\mathbb{E}$.
Since we are starting with 0 and 1, by induction given any $x\in X_{\mathcal{E}}$ or $y\in Y_{\mathcal{E}}$, it may be written with only field operations and square roots. $\square$

Of interest is that in the above proof there are two solutions for w_1'. This is due to the fact that you may reflect T onto l via a line through S in two different ways. Here we can see both:


l
R_1
m_1
m_2
W_1
S
T
W_2
R_2

References

[1] Roger C. Alperin, *A Mathematical Thoery of Origami Constructions and Numbers*, New York Journal of Mathematics, **6** (2000) 119 - 133.

[2] Humiaki Huzita, *Axiomatic Development of Origami Geometry*, Proceedings of the First International Meeting of Origami Science and Technology , Humiaki Huzita, ed., 1989, pp 143-158

[3] Roger C. Alperin and Robert J. Lang, *One-, Two-, and Multi-Fold Origami Axioms*, 4OSME (A K Peters), 2006.

[4] John B. Fraleigh, *A First Course in Abstract Algebra*, Pearson Education Inc., 2003.

[5] D.H. Lehmer, *A Note on Trigonometric Algebraic Numbers*, American Mathematical Monthly, 1933, 165 - 166.

[6] D. Auckly and J. Cleveland, *Totally real origami and impossible paper folding*, American Mathematical Monthly, 1995, 215 - 226, MR 95m:12001

[7] Roger C. Alperin, *Trisections and Totally Real Origami*, American Mathematical Monthly, 2005, 200-211.

[8] Kishiro, *How to Divide the Side of a Square Paper*, Japan Origami Academic Society, *http://origami.gr.jp/Archives/People/CAGE_/divide/02-e.html*, last visited 6/2/2013.

[9] Thomas W. Hungerford, *Algebra*, Springer Science+ Business Media, LLC, 1974.

[10] Jacques Justin, *RSOLUTION PAR LE PLIAGE DE L'QUATION DU TROISIME DEGR ET APPLICATIONS GOMTRIQUES*, *http://irem.u-strasbg.fr/php/publi/ouvert/articles/42_Justin.pdf*, 1989, last visited 6/2/2013.

[11] P. Wang-Iverson, Robert James Lang, M. Yim, *Origami^5: Fifth International Meeting of Origami Science, Mathematics, and Education*, CRC Press, 2011.

[12] Robert James Lang *Eyeglass Telescope*, Robert J. Lang Origami, *http://www.langorigami.com/science/technology/eyeglass/eyeglass.php*, last visited 6/2/2013.