**S. Alberts**
s.alberts–93@hotmail.com

# Origami

**Bachelorscriptie**

**Scriptiebegeleider: M. Derickx**

**Datum Bachelorexamen: 26 juni 2015**


**Mathematisch Instituut, Universiteit Leiden**

**Samenvatting**

Al sinds de Grieken houdt men zich bezig met constructieproblemen: welke vergelijkingen kunnen we oplossen met welke constructie? In deze scriptie houden we ons bezig met origami-constructies. We zullen aantonen dat we met origami elke algebraïsche vergelijking kunnen oplossen.

# Inhoudsopgave

# 1 Tweedimensionale Origami

## 1.1 Axioma's in het vlak

Als we het complexe vlak als oneindig vel papier beschouwen, kunnen we door middel van origami getallen construeren. Hierbij moeten we weten wat we met origami kunnen vouwen. De vlakke constructies leggen we vast in de volgende zes axioma's. Deze expositie is gebaseerd op [AL], maar de originele axioma's komen van Humiaki Huzita in [HH].

**(O1)** Van twee gegeven punten $p \neq q$ kunnen we de verbindingslijn $L(p, q)$ vouwen.

**(O2)** Van twee gegeven punten $p \neq q$ kunnen we de middelloodlijn van $p$ en $q$ vouwen.

**(O3)** Van niet-parallelle lijnen $L, M$, kunnen we beide bisectrices tussen $L$ en $M$ vouwen.

**(O4)** Gegeven een lijn $L$ en een punt $p$, kunnen we de loodlijn op $L$ door $p$ vouwen.

**(O5)** Gegeven een lijn $L$ en punten $p \neq q$ kunnen we, als deze bestaat, een lijn door $q$ vouwen zo dat $p$ op $L$ terecht komt.

**(O6)** Gegeven twee punten $p, q$ en twee lijnen $L, M$, kunnen we, als deze bestaat, een lijn vouwen zo dat $p$ op $L$ en $q$ op $M$ terecht komen.

**Opmerking 1.1.** Het bestaan van een vouwlijn als in (O5) hangt af van het bestaan van een oplossing van een tweedegraadsvergelijking. In $\mathbb{R}$ heeft deze mogelijk geen oplossing. De lijn die we vouwen is de raaklijn door $q$ aan de parabool met brandpunt $p$ en richtlijn $L$. Het bestaan hiervan hangt af van de plaats van $q$ ten opzichte van de parabool.

**Opmerking 1.2.** Axioma (O6) beschrijft het vinden van een simultane raaklijn van twee parabolen. De punten en lijnen uit (O6) zijn de brandpunten en richtlijnen van de parabolen. Deze simultane raaklijn hoeft niet altijd te bestaan. Bekijk bijvoorbeeld de parabolen $P_1 := \{(x, y) \in \mathbb{R}^2 : y = x^2 + 1\}$ en $P_2 := \{(x, y) \in \mathbb{R}^2 : y = 2x^2 + 2\}$, dan zien we dat elke raaklijn aan $P_2$ twee snijpunten met $P_1$ heeft.

## 1.2 Construeerbare getallen

De meeste hiervoor beschreven constructies zijn redelijk eenvoudig uit te voeren met een stuk papier. Nu moeten we nog wel aangeven wat we verstaan onder construeerbare punten.

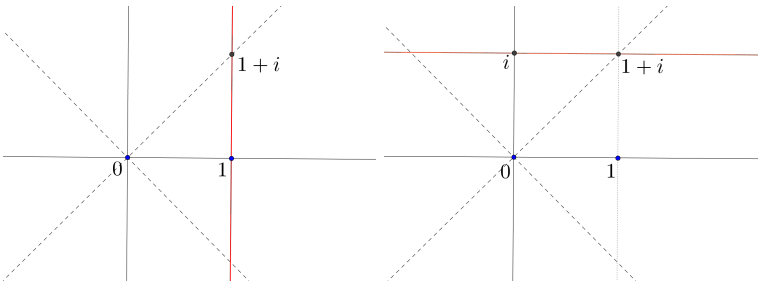
**Definitie 1.3** (Construeerbaar)**.** Laat $X \subset \mathbb{C}$ een deelverzameling zijn. We noemen $\alpha \in \mathbb{C}$ construeerbaar vanuit $X$ als $\alpha$ het snijpunt is van construeerbare lijnen vanuit punten in $X$. Hier zijn construeerbare lijnen precies de lijnen die na een eindig aantal keer vouwen verkregen kunnen worden.

**Definitie 1.4** (Origami getal)**.** Een $\alpha \in \mathbb{C}$ heet een origami getal als $\alpha$ construeerbaar is vanuit $\{0, 1\}$. We schrijven $\mathcal{O}$ voor de verzameling van origami getallen.

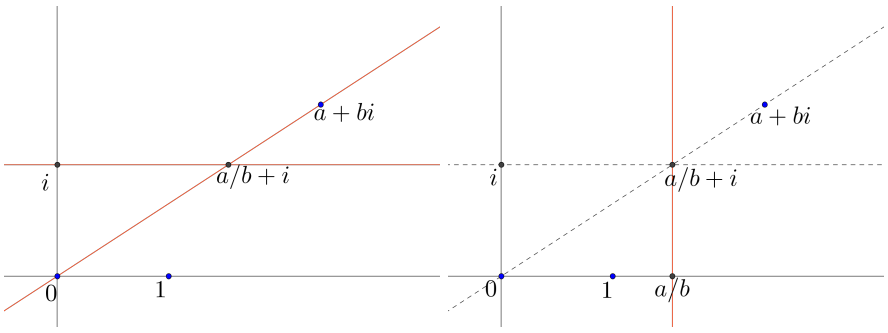
Tot nu toe lijkt het vouwen van papier erg op passer-en-lineaal constructies. Het blijkt dat we met origami alles kunnen maken wat we ook met passer en lineaal konden.

**Propositie 1.5.** Voor een nulpunt $i$ van $X^2 + 1 \in \mathbb{Z}[X]$ geldt $\mathbb{Z}[i] \subset \mathcal{O}$. Verder geldt dat $\mathbb{Q} \subset \mathcal{O}$.

*Bewijs.* De lijn $L(0, 1)$ en de loodlijn op deze lijn door 0 levert een assenstelsel op. Door een bissectrice te construeren levert een diagonaal op, het snijpunt met de loodlijn $L$ op $L(0, 1)$ door 1 levert het punt $1 \pm i$ op. De loodlijn door $1 + i$ op $L$, doorsneden met de imaginaire as levert het punt $\pm i$ op. We verkrijgen dus een vierkant met hoekpunten $0, 1, 1 \pm i$ en $\pm i$. Als we de voorgaande constructiestappen herhaaldelijk toepassen zien we dat elk roosterpunt construeerbaar is, oftewel $\mathbb{Z}(i) \subset \mathcal{O}$.




Om een breuk $\frac{a}{b} \in \mathbb{Q}$ te construeren, kunnen we de lijn door $a + bi$ en 0 construeren en deze doorsnijden met de loodlijn op de imaginaire as door $i$. Dit levert het punt $\frac{a}{b} + i$ op. Projectie op de reële as levert $\frac{a}{b}$ op.



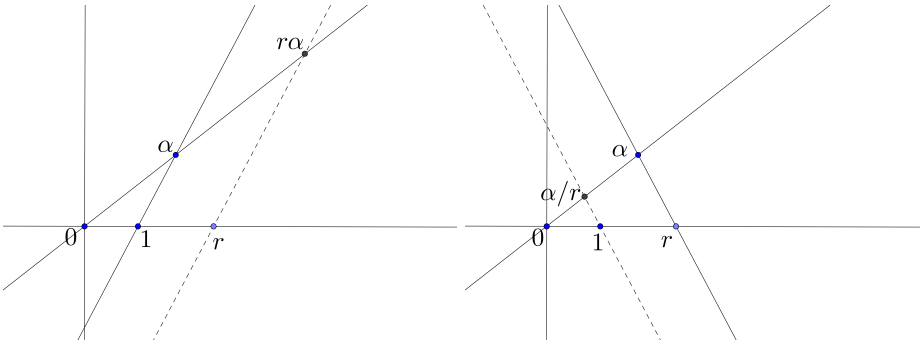

□

**Lemma 1.6.** Gegeven een lijn $L$ en een punt $p$ kunnen we een lijn door $p$ construeren die evenwijdig is aan $L$.

*Bewijs.* In het geval dat $p$ op $L$ ligt is hebben we deze lijn al, dus we nemen aan dat $p$ niet op $L$ ligt. Met (O4) kunnen we een loodlijn $M$ op $L$ vouwen die door $p$ gaat. De loodlijn op $M$ door $p$ is de lijn die we zoeken. □

**Lemma 1.7.** Gegeven een $\alpha \in \mathcal{O}$ en een reëel getal $r \in \mathcal{O} \cap \mathbb{R}$, geldt $r\alpha \in \mathcal{O}$ en $\frac{\alpha}{r} \in \mathcal{O}$ als $r \neq 0$.

*Bewijs.* [Ki] We gaan twee gevallen af: $\alpha \in \mathbb{R}$ en $\alpha \notin \mathbb{R}$. In het tweede geval construeren we lijnen $L(\alpha, 0), L(\alpha, 1)$ en een lijn $M$ door $r$ evenwijdig aan $L(\alpha, 1)$ met lemma 1.6. Als $p := L(\alpha, 0) \cap M$, zijn de driehoeken $\triangle(0, 1, \alpha)$ en $\triangle(0, r, p)$ hiermee gelijkvormig, en de afstand $d(0, p)$ is precies gelijk aan $d(r\alpha, 0)$. Er volgt dat $p = r\alpha$. Door de lijn $L(\alpha, r)$ te vouwen en een evenwijdige lijn door 1 te vouwen, krijgen we op soortgelijke manier dat $\frac{\alpha}{r}$ construeerbaar is.




In het geval dat $\alpha \in \mathbb{R}$, kunnen we $r(\alpha + i)$ construeren. Een loodlijn op de reële as door dit punt levert $r\alpha$ op.

□

**Propositie 1.8** (Optelling)**.** Als $\alpha, \beta \in \mathcal{O}$ dan geldt $\alpha + \beta \in \mathcal{O}$.

*Bewijs.* Omdat $\alpha$ en $\beta$ gegeven zijn, kunnen we de middelloodlijn van $\alpha$ en $\beta$ construeren. Deze snijdt de lijn $L(\alpha, \beta)$ in het punt $\frac{\alpha+\beta}{2}$. Met lemma 1.7 is hiermee $\alpha + \beta$ construeerbaar.

□

**Lemma 1.9.** Als $i$ een nulpunt is van $X^2 + 1 \in \mathbb{Q}[X]$ en $\alpha \in \mathcal{O}$, dan geldt $i\alpha \in \mathcal{O}$.

*Bewijs.* Dit bewijs gaat analoog aan de constructie van $i$ zelf. Vouw de lijn $L(0, \alpha)$, de loodlijn $L$ op $L(0, \alpha)$ door 0. Vouw vervolgens de juiste bissectrice $M$ en de loodlijn op het snijpunt van $L(0, \alpha)$ en $M$ op $L(0, \alpha)$. Het punt in $L \cap M$ is $i\alpha$.

□

**Propositie 1.10** (Vermenigvuldiging)**.** Als $\alpha, \beta \in \mathcal{O}$, dan geldt $\alpha \cdot \beta \in \mathcal{O}$.

*Bewijs.* Schrijf $\alpha = a + bi, \beta = c + di$ met $a, b, c, d \in \mathbb{R}$. Dan is

$$\alpha \cdot \beta = (a + bi)(c + di) = ac - bd + (bc + ad)i$$

Omdat $\alpha$ en $\beta$ construeerbaar zijn, zijn $a, bi, c, di$ construeerbaar met behulp van geschikte loodlijnen. Door vermenigvuldiging met $-i$ zijn daarmee $b$ en $d$ construeerbaar. Met lemma 1.7 zijn $ac, bd, bc, ad$ construeerbaar. Wegens propositie 1.8 zijn $ac - bd$ en $bc + ad$ construeerbaar. Uit lemma 1.9 volgt $(bc + ad)i \in \mathcal{O}$, en tenslotte geeft propositie 1.8 dat $\alpha \cdot \beta \in \mathcal{O}$. □

**Propositie 1.11** (Conjugatie)**.** De verzameling $\mathcal{O}$ is gesloten onder complexe conjugatie.

*Bewijs.* Laat $\alpha = a + bi \in \mathcal{O}$. Dan zijn $a$ en $bi$ construeerbaar met geschikte loodlijnen. Uit lemma 1.7 volgt dat $-bi$ construeerbaar is, en daarmee is $a - bi$ construeerbaar wegens propositie 1.8.

□

**Propositie 1.12** (Inversen)**.** Voor $\alpha \in \mathcal{O} \backslash \{0\}$ geldt $\alpha^{-1} \in \mathcal{O}$.

*Bewijs.* Voor $\alpha = a + bi$ geldt $\alpha^{-1} = \frac{a-bi}{a^2+b^2}$. Wegens propositie 1.11 is $a - bi$ construeerbaar en omdat $a$ en $b$ construeerbaar zijn, volgt uit proposities 1.7 en 1.8 dat $a^2 + b^2$ construeerbaar zijn. Uit lemma 1.7 volgt dat $\alpha^{-1}$ construeerbaar is.

□

Al deze informatie kunnen we samenvatten in de volgende stelling.

**Stelling 1.13.** $\mathcal{O}$ is een deellichaam van $\mathbb{C}$ dat gesloten is onder complexe conjugatie.

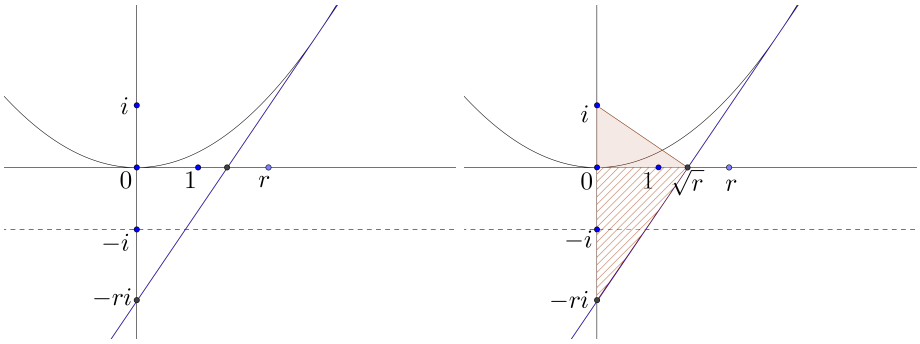
**Lemma 1.14** (Reële wortels)**.** Als $r \in \mathbb{R}_{>0}$ construeerbaar is, dan zijn de kwadratische wortels $\sqrt{r}$ construeerbaar.

*Bewijs.* [Ki]

Als $r$ construeerbaar is, dan is ook $-ri$ construeerbaar. Met (O5) kunnen we een lijn $L$ door $-ri$ construeren zo dat $i$ op de horizontale lijn door $-i$ terecht komt. Laat $M = i, P = -ri$ en $N = x$ het snijpunt van $L$ en de reële as. Laat $O$ de oorsprong. Dan zijn de construeerbare driehoeken $\triangle NOM$ en $\triangle PON$ gelijkvormig. Uit verhoudingen van zijden volgt

$$\frac{x}{1} = \frac{r}{x}$$

Hieruit volgt dat $x^2 = r$, oftewel $x = \sqrt{r}$, waarbij $\sqrt{r}$ de positieve reële wortel is. Hieruit volgt dat de beide wortels construeerbaar zijn.




□

**Stelling 1.15** (Complexe wortels)**.** Als $\alpha \in \mathcal{O}$, dan is elke kwadratische wortel $\sqrt{\alpha}$ een origami getal.

*Bewijs.* Het trekken van een vierkantswortel van een complex getal $\alpha$ komt neer op het halveren van het argument en de wortel trekken van de norm. Laat $r := |\alpha|$. Zonder verlies van algemeenheid kunnen we stellen dat $r > 0$, dus wegens het lemma 1.14 is $\sqrt{r} > 0$ construeerbaar. Laat $M$ een bissectrice tussen $L(\alpha, 0)$ en de reële as zijn. Kies een construeerbaar punt $z = a + bi$ op $M$, zo dat $a, b > 0$ (het zou kunnen dat zo'n punt niet op $M$ ligt, in dit geval kiezen we dit punt op de andere bisectrice). Dan is $\frac{\sqrt{r}z}{a^2+b^2}$ construeerbaar, en aangezien het een reëel veelvoud van $z$ is, ligt $z$ op $M$. De norm van deze breuk is $\sqrt{r}$, en we concluderen dat $\frac{\sqrt{r}z}{a^2+b^2}$ een wortel is van $\alpha$. De andere wortel is nu eenvoudig construeerbaar.

□

## 1.3 Derdegraadsvergelijkingen

We schrijven $\mathcal{C}$ voor de verzameling van complexe getallen die construeerbaar zijn met passer en lineaal. Een bekende stelling uit de algebra karakteriseert dit lichaam.

**Stelling 1.16.** $\mathcal{C}$ is het kleinste deellichaam van $\mathbb{C}$ dat gesloten is onder complexe conjugaties en worteltrekken.

Uit de eigenschappen van het vorige hoofdstuk, zien we dat elk getal dat construeerbaar is met passer en lineaal ook een origamigetal is.

**Stelling 1.17.** Er geldt $\mathcal{C} \subset \mathcal{O}$.

Tot nu toe hebben we echter niet gezien waarom het van belang is om naar vlakke origami te kijken. We hebben immers nog geen origamigetallen gezien die niet construeerbaar zijn met passer en lineaal. De volgende stelling brengt daar verandering in.

**Stelling 1.18** (Derdegraadsvergelijkingen [Al])**.** Laat $f \in \mathbb{Q}[X]$ een polynoom van graad 3. Dan is elk nulpunt van $f$ een origamigetal.

De reden dat we derdegraadsvergelijkingen op kunnen lossen met origami, is axioma (O6). Wat dit axioma zegt, is dat gegeven twee parabolen $P_1$ en $P_2$, we een lijn kunnen vouwen die zowel $P_1$ als $P_2$ raakt. Voor we het algebraïsche bewijs van 1.16 geven, volgt hier een meetkundige manier om te zien dat (O6) het oplossen van een derdegraadsvergelijking beschrijft met behulp van projectieve meetkunde. Laat $\mathbb{P}^2(\mathbb{C})$ een projectief vlak over $\mathbb{C}$.

**Definitie 1.19** (Kegelsnede)**.** Een kegelsnede is deelverzameling van een projectief vlak $\mathbb{P}^2(\mathbb{C})$ van de volgende vorm:

$$Q = \{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) : f(x, y, z) = 0\}$$

Hierbij is $f$ een kwadratisch homogeen polynoom over $\mathbb{C}$.

**Definitie 1.20** (Glad)**.** Een kegelsnede $Q$ heet glad als $Q$ gegeven kan worden door een polynoom $f$ met discriminant $\Delta(f) \neq 0$.

De parabolen $P_1$ en $P_2$ kunnen we zien als gladde kegelsneden in $\mathbb{P}^2(\mathbb{C})$.

Voor de volgende stelling hebben we nodig dat een projectieve lijn geschreven kan worden als de nulpuntsverzameling van een homogeen polynoom van graad 1. Oftewel, een projectieve lijn $L \subset \mathbb{P}^2(\mathbb{C})$ heeft de vorm

$$L = \{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) : ax + by + cz = 0\}$$

Hierbij kunnen $a, b, c$ niet alledrie 0 zijn.

**Notatie 1.21.** Schrijf $L_{a,b,c}$ voor de lijn gegeven door het polynoom $ax + by + cz = 0$.

**Stelling 1.22.** Laat $\mathcal{L}$ de verzameling lijnen in $\mathbb{P}^2(\mathbb{C})$ zijn. Dan is

$$\phi : \mathcal{L} \to \mathbb{P}^2(\mathbb{C}), L_{a,b,c} \mapsto (a : b : c)$$

een welgedefinieerde bijectieve afbeelding.

De $\mathcal{L}$ uit de vorige stelling wordt ook wel het duale projectieve vlak genoemd. Dit noteren we met $\mathbb{P}^2(\mathbb{C})^*$. Als we de verzameling van raaklijnen aan een gladde kegelsnede beschouwen, hoort bij deze verzameling lijnen een verzameling punten. Deze punten vormen opnieuw een gladde kegelsnede.

**Lemma 1.23.** Laat $Q$ een gladde kegelsnede in $\mathbb{P}^2(\mathbb{C})$. Voor $q \in Q$, laat $L_q$ de raaklijn aan $Q$ door $q$ zijn. Laat

$$\psi : Q \to \mathbb{P}^2(\mathbb{C})^*, q \mapsto L_q$$

Dan is $\psi(Q) =: Q^*$ een gladde kegelsnede in $\mathbb{P}^2(\mathbb{C})^*$.

De $Q^*$ uit het vorige lemma heet de duale kegelsnede. We zien dus dat (O6) de snijpunten van $P_1^*$ en $P_2^*$ bepaalt. De parabolen $P_1$ en $P_2$ hebben beiden precies 1 punt op de oneindig verre lijn, deze lijn is een gemeenschappelijke raaklijn. Dit is dus een reëel snijpunt van $P_1^*$ en $P_2^*$. In gunstige gevallen, wanneer $P_1$ en $P_2$ een gemeenschappelijke raaklijn in het reële affiene vlak hebben, komt het vinden van de overige reële snijpunten van $P_1^*$ en $P_2^*$ neer op het oplossen van een derdegraadsvergelijking.

Dit is het meetkundige idee achter het bewijs, hier komt een algebraïsche versie.

*Bewijs van stelling 1.18.* Gebruikmakend van standaard lichaamsoperaties, kunnen we elke derdegraadsvergelijking omschrijven tot een vorm $x^3 + ax + b = 0$. We beschouwen de parabolen $P$ en $Q$, met $P$ gegeven door de vergelijking $(y - \frac{1}{2}a)^2 = 2bx$ en $Q$ gegeven door de vergelijking $y = \frac{1}{2}x^2$. Hiervoor zien we de reële as als $x$-as en imaginaire as als $y$-as. De brandpunten en richtlijnen die deze parabolen definiëren, zijn punten en lijnen die construeerbaar zijn als $a$ en $b$ dat zijn, waardoor we met axioma (O6) een simultane raaklijn kunnen vouwen, als deze bestaat.

Als we $P$ en $Q$ als complexe parabolen beschouwen, weten we dat er wel een simultane raaklijn zal zijn. Laat deze complexe lijn $L$ gegeven worden door $y = \mu x + c$. We zullen laten zien dat we $\mu$ en $c$ reëel kunnen kiezen. Stel dat $\mu$ reëel is. De lijn $L$ raakt aan $Q$ in het punt $(\mu, \mu^2)$, dit punt is dan dus ook reëel. Omdat $(\mu, \mu^2)$ op $L$ moet liggen, kunnen we hier ook $c$ uit afleiden, dus is $c$ reëel. Het is dus voldoende om aan te tonen dat $\mu$ reëel gekozen kan worden. Claim: $\mu^3 + a\mu + b = 0$.

Merk allereerst op dat $\mu \neq 0$, aangezien $\mu$ in het bijzonder aan $P$ moet raken. Laat $x_0 + y_0 i$ het raakpunt van $L$ met $P$, en $x_1 + y_1 i$ het raakpunt van $L$ met $Q$. Aangezien $L$ de raaklijn in $x_0 + y_0 i$ aan $P$ is, is $L$ gegeven door een eerste orde Taylor-polynoom in dit punt. Dit geeft een uitdrukking voor $\mu$. $L$ wordt nu gegeven door

$$x = x_0 + \frac{y_0 - \frac{1}{2}a}{b}(y - y_0)$$

Omschrijven geeft dat $\mu = \frac{b}{y_0 - \frac{1}{2}a}$. We kunnen ook zien dat $\mu$ gelijk is aan de richtingscoefficient van $Q$ in $x_1$, dit geeft $\mu = x_1$. Hier volgt uit dat $y_1 = \frac{1}{2}\mu^2$. Vullen we $x_0$ in in de vergelijking voor $P$, dan geeft dit

$$x_0 = \frac{(y_0 - \frac{1}{2}a)^2}{2b} = \frac{1}{2}\frac{1}{\frac{b}{(y_0 - \frac{a}{2})^2}} = \frac{1}{2}\frac{b}{\frac{b^2}{(y_0 - \frac{a}{2})^2}} = \frac{b}{2\mu^2}$$

We krijgen ook $y_0 = \frac{b}{\mu} + \frac{a}{2}$. Nu hebben we uitdrukkingen voor $x_0, x_1, y_0, y_1$ in termen van $\mu, a, b$. Dit geeft de volgende relatie voor $\mu$:

$$\mu = \frac{y_1 - y_0}{x_1 - x_0} = \frac{\frac{\mu^2}{2} - \frac{a}{2} - \frac{b}{\mu}}{\mu - \frac{b}{2\mu^2}}$$

Oftewel:

$$\mu - \frac{\frac{\mu^2}{2} - \frac{a}{2} - \frac{b}{\mu}}{\mu - \frac{b}{2\mu^2}} = 0$$

Omschrijven geeft

$$\frac{\mu^4 + a\mu^2 + b\mu}{2\mu^3 - b} = 0$$

Aangezien $\mu \neq 0$ geeft dit

$$\mu^3 + a\mu + b = 0$$

De richtingscoëfficiënt van $L$ is dus een nulpunt van $X^3 + aX + b = 0$. Aangezien hier een reële oplossing voor bestaat, kunnen we $\mu$ reëel kiezen. We concluderen

dat er een construeerbare simultane raaklijn van $P$ en $Q$ bestaat. Construeerbaarheid van dit nulpunt is nu eenvoudig: snij de lijn $L$ met de verticale lijn door 1, dit geeft het punt $\mu + b$, en aangezien $b$ construeerbaar is, is $\mu$ dit ook.

□

**Gevolg 1.24.** Een willekeurige hoek is driedeelbaar met origami.

*Bewijs.* Voor een hoek $\theta \in [0, 2\pi)$, geldt de volgende verdubbelingsformule

$$\sin(\theta) = 3\sin\left(\frac{\theta}{3}\right) - 4\sin^3\left(\frac{\theta}{3}\right)$$

Gegeven een zo'n hoek kunnen we dus kijken naar het polynoom $f = X^3 - \frac{3X}{4} + \frac{\sin(\theta)}{4}$. De nulpunten van dit polynoom zijn wegens 1.18 construeerbaar als $\sin(\theta)$ dat is. Gegeven een hoek $\theta$, is de sinus construeerbaar. Een nulpunt van $f$ geeft oplossingen voor $\sin\left(\frac{\theta}{3}\right)$. Hier is $\cos\left(\frac{\theta}{3}\right)$ af te leiden door simpele goniometrie en een wortel trekken, en vervolgens is de lijn door 0 en $\cos\left(\frac{\theta}{3}\right) + i\sin\left(\frac{\theta}{3}\right)$ construeerbaar. Hiermee zijn we klaar.

□

# 2 3D Origami

Tot nu toe zagen we dat we met origami elke kwadratische en cubische uitbreiding van $\mathbb{Q}$ kunnen construeren. Al onze constructies tot nu toe gebruiken echter dat na elke keer vouwen het papier weer plat eindigt. Dit is een beperking die we met 3D origami willen wegnemen. Hiervoor hebben we nieuwe axioma's nodig.

## 2.1 Een voorbeeld van 3D-constructies

We willen deze sectie beginnen met een illustratie van hoe een 3D-constructie eruit zou kunnen zien. Het volgende axioma zijn we in het artikel [PT] tegengekomen.

**(Regular Polygon Axioms):** [PT] Voor alle $n \geq 2$: Gegeven de hoekpunten $A_1, \ldots, A_{n+1}$ van een regelmatige $n+1$-hoek, kunnen we de regelmatige $n$-hoek met hoekpunten $B_1, \ldots, B_n$ construeren, gedefinieerd door $B_1 = A_1$ en $B_2 = A_2$.

Dit axioma berust op het "dichtvouwen"van een van de zijdes van de $n+1$-hoek. Hierbij vouwen we de middelloodlijn van $A_2$ en $A_3$, en vouwen we $A_3$ via deze middelloodlijn op $A_3$. Om deze constructie te vertalen naar de taal van origami-getallen, hebben we dit axioma. We refereren hier vanaf nu aan met de afkorting RPA.

Dit axioma geeft een lichaam dat uitgebreider is dan $\mathcal{O}$. Dit uitgebreidere lichaam geven we aan met $\mathcal{O}_{RPA}$.

We schrijven $\zeta_n$ voor een primitieve $n$-degraads eenheidswortel.

**Lemma 2.1** ([PT])**.** Laat $\mathbb{Q} \subset K \subset \mathbb{C}$ een lichaam, zo dat $K$ de hoekpunten $A_1, \ldots, A_{n+1}$ van een regelmatige $n+1$-hoek bevat. Laat $B_i$ als in het RPA. Dan geldt

$$K(B_1, \ldots, B_n) = K(\zeta_n)$$

*Bewijs.* We kunnen aannemen dat $n > 2$. Laat $C$ het middelpunt van de $n$-hoek zijn. Dan geldt

$$B_i - C = \zeta_n^{i-1}(B_1 - C)$$

Dit geeft ook

$$B_2 - \zeta_n B_1 = (1 - \zeta_n)C$$

Hierdoor geldt $C \in K(\zeta_n)$, aangezien $B_1, B_2, \zeta_n \in K(\zeta_n)$. Er volgt dat $B_i \in K(\zeta_n)$ voor alle $i$, dus

$$K(B_1, \ldots, B_n) \subset K(\zeta_n)$$

Aangezien $C = \frac{B_1 + \cdots + B_n}{n}$ geldt dat $C \in K(B_1, \ldots, B_n)$ en omdat

$$\zeta_n = \frac{B_2 - C}{B_1 - C}$$

geldt ook $K(\zeta_n) \subset K(B_1, \ldots, B_n)$. De gelijkheid volgt.

□

**Stelling 2.2** ([PT])**.** Er geldt $\zeta_n \in \mathcal{O}_{RPA}$ voor alle $n$.

*Bewijs.* Laat $n > 2$ gegeven zijn, en kies $k$ zo dat $2^k > n + 1$. We kunnen het vierkant met hoekpunten $1 + i$, $-1 + i$, $-1 - i$ en $1 - i$ gebruiken om een regelmatige $2^k$-hoek te construeren. Hiervoor delen we het vierkant door middel van bissectrices op in $2 \cdot 2^k$ stukken, en door de snijpunten van deze bissectrices met het vierkant met elkaar te verbinden krijgen we een regelmatige $2^k$-hoek. Wegens RPA zijn de hoekpunten van een $2^k - 1$-hoek construeerbaar. Door deze constructie vaak genoeg toe te passen, zien we dat de hoekpunten van een $n + 1$-hoek construeerbaar zijn, waarmee wegens lemma 2.1 $\zeta_n$ construeerbaar is.

□

Deze constructie levert ons dus de maximale abelse uitbreiding van $\mathbb{Q}$ op. Een gegeneraliseerde versie van het RPA wordt vermeld in [PT] voor zogenaamde cyclische veelhoeken. Dit zijn veelhoeken waarvan de hoekpunten op een cirkel liggen. Deze constructie levert zelfs algebraïsche getallen op waarvan de Galoisgroep niet oplosbaar is. Dit roept de vraag op wat er nog meer mogelijk is. Voor we deze kunnen beantwoorden hebben we algemenere definities nodig die beschrijven wat 3D-origami constructies zijn.

## 2.2 Definities voor 3D-origami

Wat we hier willen geven is een manier om vast te leggen wat 3D-constructies zijn. We willen graag dat de constructie die we zojuist gezien hebben hierin past. Zodra we dit vastgelegd hebben, kunnen we gaan werken aan een constructie die ons alle algebraïsche getallen gaat geven. Allereerst moeten we weten wat het betekent om van een stuk papier een 3-dimensionale vorm te vouwen. Dit betekent dat we een verzameling van lijnstukken en punten die we al gevouwen hebben in $\mathbb{R}^3$ moeten inbedden op een manier die overeenkomt met het vouwen van papier.

**Definitie 2.3** (Vouwpatroon)**.** Een vouwpatroon $V$ is een verzameling punten en lijnstukken die construeerbaar zijn vanuit 0 en 1 met 2D-origami, ingebed in $[0, 1]^2$.

**Definitie 2.4** (3D-configuratie)**.** Een 3D-configuratie is een continue afbeelding

$$g : [0, 1]^2 \to \mathbb{R}^3$$

die een isometrie is op de samenhangscomponenten van

$$X := [0, 1]^2 \backslash \{\text{vouwlijnen in } V\}$$

Waar we nu naar streven is een manier om vast te leggen wanneer iets een constructie is en wanneer niet. Bij het voorbeeld van [PT] merken we op dat in de eindtoestand het object rigide is, mits we een vlak kiezen waar de hoekpunten van de pyramide in liggen. Intuïtief is rigide een duidelijk begrip, wat we nu willen doen is dit ook wiskundig definiëren. We zouden een 3D-configuratie rigide willen noemen als deze niet meer vervormbaar is, dus we gaan eerst bekijken wat een vervorming moet zijn.

**Definitie 2.5** (Vervorming)**.** Een vervorming van een 3D-configuratie $g$ is een homotopie

$$G : [0,1] \times [0,1]^2 \to \mathbb{R}^3$$

die begint in $g$, zodanig dat voor alle $t \in [0,1]$ de afbeelding $G(t,\cdot)$ een 3D-configuratie is.

Nu zijn er vervormingen die we ook kunnen toepassen op configuraties die we wel rigide willen noemen. De configuratie van [PT] kunnen we namelijk nog steeds verplaatsen door $\mathbb{R}^3$, wat gezien de definitie een vervorming is. De volgende definitie sluit deze flauwe vervormingen uit.

**Definitie 2.6** (Triviale vervormingen)**.** We noemen een vervorming $G$ triviaal als voor alle $t \in [0,1]$ en alle $p, q \in [0,1]^2$ geldt dat

$$d(G(0,p), G(0,q)) = d(G(t,p), G(t,q))$$

Hier is $d$ de Euclidische afstand in $\mathbb{R}^3$.

Nu kunnen we opschrijven wat een rigide configuratie is.

**Definitie 2.7** (Rigide)**.** Een 3D-configuratie heet rigide als elke vervorming triviaal is.

Eerder hadden we het over restricties die ervoor zorgden dat de configuratie van [PT] een rigide object werd.

**Definitie 2.8** (Restrictie)**.** Laat $a$ en $b$ punten of vouwlijnen in $V$, of samenhangscomponenten van $X$. Een restrictie op een 3D-configuratie is een eis van de vorm $g[a] \subset g[b]$.

Een restrictie is dus bijvoorbeeld een eis dat een bepaald punt op een bepaald lijnstuk terecht komt, of dat twee samenhangscomponenten op elkaar blijven liggen. In het RPA wat we eerder zagen, is het dichtvouwen van een zijde een restrictie dat een bepaald lijnstuk op een ander lijnstuk terecht komt.

Met al deze definities kunnen we vastleggen wat een 3D-constructie met origami moet zijn. Dit moet een 3D-configuratie zijn, waarop we met bepaalde restricties een rigide object te pakken hebben. Hiervoor moeten we onze eerdere definities van vervormingen en rigiditeit aanpassen zodat ze iets zeggen over configuraties met restricties.

**Definitie 2.9** (Rigide onder restricties)**.** We noemen een 3D-configuratie $g$ rigide onder een aantal restricties rigide als elke vervorming van $G$ waarvoor de 3D-configuratie $G(t,\cdot)$ aan de restricties voldoet triviaal is.

**Definitie 2.10** (3D-Constructie)**.** Een 3D-constructie is een 3D-configuratie die onder een eindig aantal restricties rigide is.

Het RPA die we eerder zagen, past in deze definities. Als we een regelmatige veelhoek met hoekpunten $A_1, \ldots, A_{n+1}$ hebben, en we vouwen deze dicht langs de zijde $A_2A_3$, verkrijgen we een open pyramide waar het grondvlak van ontbreekt. Door een vlak in $\mathbb{R}^3$ te kiezen waar de hoekpunten van het

grondvlak in liggen, krijgen we een gesloten pyramide. Dit soort objecten zijn wegens Cauchy's rigiditeitsstelling rigide [AZ]. Als we het middelpunt van $A_1, \ldots, A_{n+1}$ aangeven met $C$, zijn de restricties op deze constructie de restricties dat $g(A_1C) = g(A_2C)$ en $A_1, A_2, A_3, \ldots, A_{n+1} \in H$ voor een of ander vlak $H$ in $\mathbb{R}^3$. Ten slotte hebben we een restrictie nodig dat de dichtgevouwde driehoek $A_2CA_3$ op zijn plaats houdt, oftewel $g(A_2CA_3) \subset g(A_1CA_2)$.

# 3 De Derickx-constructie

De constructies die we tot nu toe hebben toegepast, stellen ons in staat om vanuit $\{0,1\}$ de maximale abelse uitbreiding van $\mathbb{Q}$ te construeren. We maakten al de opmerking dat een generalisatie van de RPA's ook oplossingen van polynomen met niet-oplosbare Galoisgroep kan geven. Gezien de forse hoeveelheid mogelijkheden die we met 3D-origami gekregen hebben, stellen we ons nu de vraag of het mogelijk is om een algebraïsche afsluiting van $\mathbb{Q}$ te construeren met origami.

We geven een beschrijving van een 3D-configuratie die ons een algebraïsche afsluiting van $\mathbb{Q}$ gaat geven. Deze configuratie is bedacht door Maarten Derickx. We noemen deze configuratie vanaf nu de Derickx-constructie. Hiervoor zullen we natuurlijk wel aan moeten tonen dat zijn configuratie een 3D-constructie is. De Derickx-constructie is niet voor elk algebraïsch getal geschikt, maar we zullen zien dat de constructie ons voldoende geeft om met de standaard lichaamsoperaties een oplossing voor elk polynoom te vinden.

## 3.1 Algebraïsche getallen tussen 0 en 1

We beginnen met $\overline{\mathbb{Q}} \subset \mathbb{C}$ een algebraïsche afsluiting van $\mathbb{Q}$, $\alpha \in \overline{\mathbb{Q}} \cap (0,1)$ en $f = \sum_{i=0}^{n} a_i X^i$ het minimumpolynoom van $\alpha$ over $\mathbb{Q}$ met $a_n = 1$.

De eis $\alpha \in (0,1)$ geeft ons dat er een unieke $\theta \in \left(0, \frac{\pi}{2}\right)$ bestaat die voldoet aan $\cos(\theta) = \alpha$. Omdat $f(\alpha) = 0$ geeft dit de relatie

$$\sum_{i=0}^{n} a_i \cos(\theta)^i = 0$$

We kunnen dit herschrijven door goniometrische identiteiten te gebruiken.

**Stelling 3.1** (Power Reduction Formulas [W2])**.** Voor een positief geheel getal $k$ geldt

$$\cos(\theta)^k = \begin{cases} \dfrac{2}{2^k} \displaystyle\sum_{j=0}^{\frac{k-1}{2}} \binom{k}{j} \cos((k-2j)\theta) & k \text{ oneven} \\ \dfrac{1}{2^k}\binom{k}{\frac{k}{2}} + \dfrac{2}{2^k} \displaystyle\sum_{j=0}^{\frac{k}{2}-1} \binom{k}{j} \cos((k-2j)\theta) & k \text{ even} \end{cases}$$

Deze uitdrukkingen geven ons een manier om $\sum_{i=0}^{n} a_i \cos(\theta)^i = 0$ om te schrijven naar iets van de vorm $\sum_{i=0}^{n} b_i \cos(i\theta) = 0$.

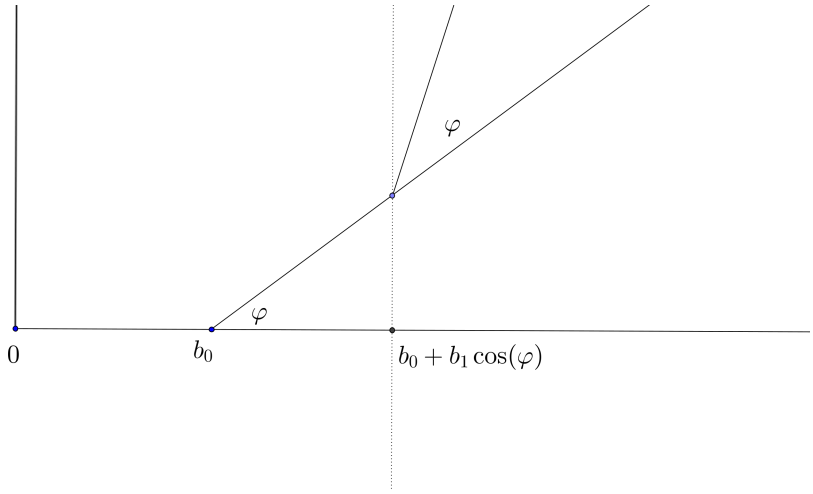
Bij elk algebraïsch getal tussen 0 en 1 hoort dus een rijtje $b_0, \ldots, b_n$. We zijn geïnteresseerd in die algebraïsche getallen waarvoor $b_i > 0$ voor alle $i$. Daarnaast willen we om het bewijs voor rigiditeit eleganter te maken, eisen dat $\theta$ zo is dat er geen zelfdoorsnijding plaats vindt.

## 3.2 De Derickx-constructie

We beschouwen nu een $\alpha \in \overline{\mathbb{Q}}$ die aan de eisen uit de vorige paragraaf voldoet, met minimumpolynoom $f$. We schrijven weer $\alpha = \cos(\theta)$ en

$$\sum_{i=0}^{n} b_i \cos(i\theta) = 0$$

De configuratie begint met een strook papier, voor het gemak één die willekeurig lang is. We buigen een rechte hoek af, waardoor we een reële en imaginaire as krijgen. We meten met origami een lengte $b_0$ af van de reële as; omdat de coëfficiënten van $f$ rationaal zijn, en $b_i$ een $\mathbb{Q}$-lineaire combinatie van die coëfficiënten is, kunnen we deze afstand met origami afmeten. Op deze lengte vouwen we een hoek $\varphi$ af. Deze hoek nemen we kleiner dan $\theta$. Hieronder een illustratie hiervan.




Van de diagonale lijn kunnen we een lengte $b_1$ afmeten. Het reële deel van het nieuwe punt is gelijk aan $b_0 + b_1\cos(\varphi)$. Als we weer afbuigen met de zelfde constructie en een lengte $b_2$ afmeten, krijgen we een punt met een reëel deel $b_0 + b_1\cos(\varphi) + b_2\cos(2\varphi)$. Als we dit $n$ keer doen, heeft het $j^{\text{de}}$ punt een reëel deel van

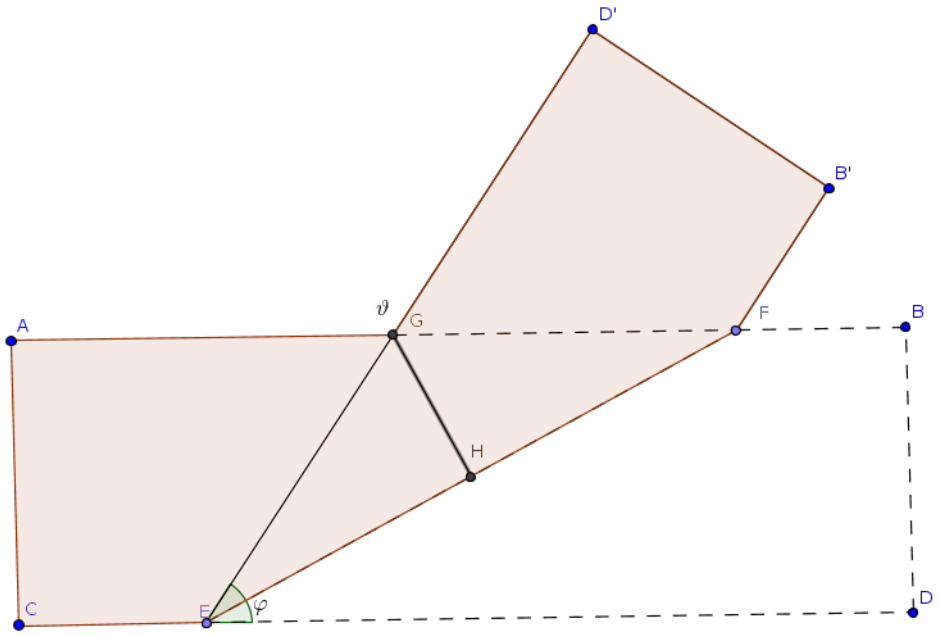
$$b_0 + b_1\cos(\varphi) + \cdots + b_j\cos(j\varphi)$$

Voor deze constructie willen we zelfdoorsnijding voorkomen. Dit is om het bewijzen van rigiditeit te vereenvoudigen en om de constructie elegant te houden. Omdat er geen zelfdoorsnijding plaats vindt als we op elke plek een hoek $\theta$ afbuigen en omdat $\varphi \leq \theta$, zal er hier ook geen zelfdoorsnijding plaats vinden.

Merk nu op dat het laatste punt reëel deel

$$b_0 + b_1\cos(\varphi) + \cdots + b_n\cos(n\varphi)$$

heeft. Mocht $\varphi$ gelijk zijn aan $\theta$, dan is dit dus gelijk aan 0. We willen nu de hoek $\varphi$ gaan veranderen met een 3D-constructie. Hiervoor laten we nog een illustratie zien.

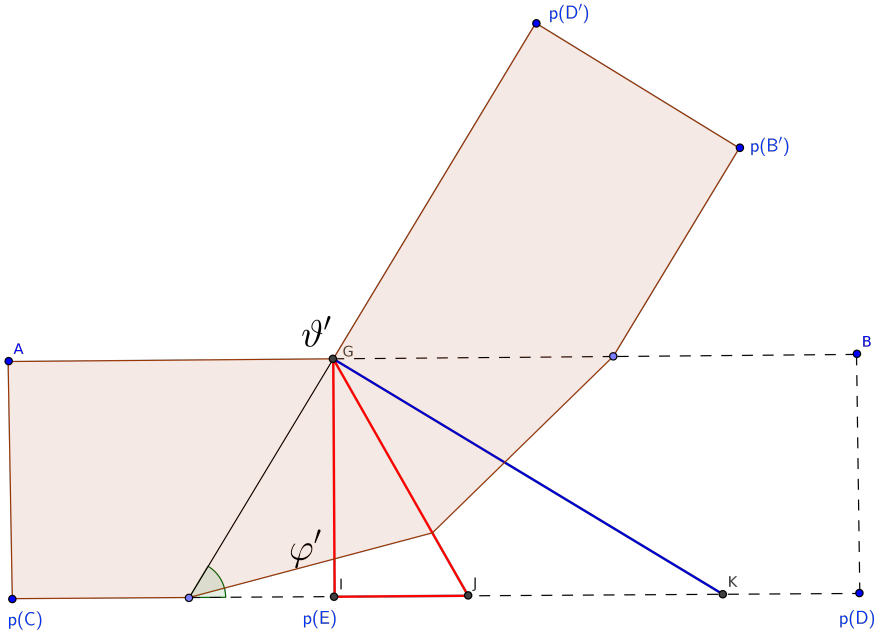



Deze illustratie geeft een enkel stuk van de configuratie weer; in de hele configuratie liggen er $n$ van deze figuren achter elkaar en is er een imaginaire as gevouwen. Voor de beschrijving van de configuratie nemen we aan dat dit het eerste stuk is. De afstand tussen $A$ en $G$ is dus $b_0$ en de afstand tussen $G$ en $D'$ is $b_1$. De vouwlijn tussen $G$ en $H$ gaat als scharnier dienen voor de constructie. We kunnen dit figuur als vouwpatroon $V$ beschouwen, dus als deelverzameling van $[0,1]^2$: we kunnen het vierkant immers altijd een aantal keer omvouwen om een rechthoek van de gewenste verhoudingen te krijgen. We kiezen nu de inbedding $i : [0,1]^2 \to \mathbb{R}^3$, die $p \in [0,1]^2$ naar het punt $(p,0) \in \mathbb{R}^2 \times \mathbb{R}$ stuurt. Dit levert ons ook gelijk een inbedding van $V$ in $\mathbb{R}^3$ op. Voor vereenvoudiging van notatie vatten we punten $x \in [0,1]^2$ op als punten in $\mathbb{R}^3$, en noteren we $i(x)$ als $x$. We beschrijven nu 3D-configuraties $g_\psi$ van $V$ voor $\psi \in [0, \frac{\pi}{2}]$. We willen allereerst dat $g_\psi(A) = A, g_\psi(G) = G$ en $g_\psi(D') \in \mathbb{R}^2 \times \{0\}$. Verder willen we dat

$$\angle C A g_\psi(C) = \psi$$

Door te spiegelen in het vlak door $GH$ dat loodrecht staat op $\mathbb{R}^2 \times \{0\}$, volgt dan ook dat $\angle B' g_\psi(D') g_\psi(B') = \psi$. In origami ziet dit eruit als het uit het vlak kantelen van $AGEC$ over de lijn $AG$ met een hoek $\psi$. Het rechtop zetten

van de figuur, levert geprojecteerd op $\mathbb{R}^2 \times \{0\}$ een configuratie $V'$ op, die bijna hetzelfde is als $V$. Alleen de hoeken $\vartheta$ en $\varphi$ en enkele afstanden zijn gewijzigd. Ons doel is aan te tonen dat er een $\psi$ bestaat zo dat de hoek op de plaats van $\varphi$ gelijk is aan $\theta$. Dit probleem heeft twee componenten. Allereerst moeten we weten dat $\varphi'$, de projectie van $\varphi$ op $\mathbb{R}^2 \times \{0\}$, alleen afhangt van $\psi$. Hierdoor weten we dan dat deze hoek op elke plaats in de geprojecteerde configuratie gelijk blijft.




Hierboven een illustratie van het geprojecteerde vouwpatroon. We beginnen dus met de strook die we eerder zagen, we zetten deze met een hoek $\psi$ omhoog en $p(C)$, $p(E)$ en $p(D)$ zijn de geprojecteerde punten. De nieuwe hoeken geven we aan met $\varphi'$ en $\vartheta'$. Eigenlijk is dit misbruik van notatie: we geven $A, G, B$ aan voor punten in $[0,1]^2$ die we ingebed hebben met $i$. We schrijven $p(C), p(E), p(D)$ voor de projecties van $g_\psi(C), g_\psi(E), g_\psi(D)$. De punten $I, J, K$ zijn ook projecties die horen bij de originele strook. Omdat de lijnstukken $IJ$ en $JK$ loodrecht geprojecteerd worden, liggen de lengtes hiervan vast door de originele strook papier.

**Lemma 3.2.** Laat $\gamma = \angle IGJ$. Laat $a$ de lengte van $AC$, $b$ de lengte van $IJ$ en $c$ de lengte van $GJ$. Laat $h$ de afstand van $p(C)$ naar $g_\psi(C)$ zijn. Laat ten slotte $d = \sqrt{c^2 + h^2}$. Dan geldt

$$\sin(\gamma) = \frac{b}{\sqrt{d^2 - a^2 \sin(\psi)^2}}$$

*Bewijs.* Er geldt $\sin(\gamma) = \frac{b}{c}$ dus het bewijs komt neer op het omschrijven van $c$. Uit de definitie van $d$ volgt dat $c = \sqrt{d^2 - h^2}$. De lengte $h$ voldoet wegens wat simpele goniometrie aan de relatie $\sin(\psi) = \frac{h}{a}$, waaruit de formule in het lemma volgt.

□

**Gevolg 3.3.** Er geldt

$$\sin\left(\frac{\varphi'}{2}\right) = \frac{b}{\sqrt{d^2 - a^2\sin(\psi)^2}}$$

*Bewijs.* Allereerst geldt $\vartheta' = \pi - \varphi'$, omdat $\varphi'$ gelijk is aan de hoek $\angle g_\psi(D')GB$. Nu geldt ook $\vartheta' + 2\cdot\frac{\pi}{2} + 2\gamma = 2\pi$. De hoeken $\angle AGI$ en $\angle g_\psi(D')GK$ zijn immers $\frac{\pi}{2}$ en omdat $GJ$ een symmetrieas is geldt dat $\gamma = \angle IGJ = \angle JGK$. We vinden $2\gamma = \pi - \vartheta$. Dus $2\gamma = \varphi$ en de formule volgt uit lemma 3.2.

□

Als we nu een strook papier hebben dan liggen de lengtes van $a$ en $b$ vast, ongeacht welke lengtes $AG$ en $Gg_\psi(D')$ hebben. Merk ook op dat $d$ de lengte is van het lijnstuk dat geprojecteerd wordt op $GJ$. Ook deze lengte ligt dus vast zodra we de lengtes van de strook papier weten. De enige variabele die verschil maakt voor $\varphi'$ is de hoek $\psi$. Hierdoor is de geprojecteerde configuratie dus een configuratie die we zouden krijgen als we met een dunnere strook begonnen waren en een hoek $\varphi'$ omgevouwen hadden.

We kunnen nu $\varphi$ als functie $[0, \frac{\pi}{2}] \to [0, \pi]$ beschouwen, die een $\psi$ naar de bijbehorende $\varphi(\psi)$ stuurt. Hierbij is $\varphi(0)$ onze beginhoek.

**Stelling 3.4.** De functie $\varphi$ is strikt stijgend en surjectief op het interval $[\varphi(0), \pi]$.

*Bewijs.* Gevolg 3.3 geeft ons dat

$$\varphi(\psi) = 2\arcsin\left(\frac{b}{\sqrt{d^2 - a^2\sin(\psi)^2}}\right)$$

Als $0 \leq \psi \leq \frac{\pi}{2}$ groter wordt, wordt $\sin(\psi)^2$ dit ook, dus wordt de noemer van de breuk kleiner. De term in de arcsinus groeit dus als $\psi$ groter wordt. Tenslotte is de arcsinus op het gedefinieerde domein een strikt stijgende functie, waarmee $\varphi$ stikt stijgend is. Uit Pythagoras volgt $d^2 - a^2 = b^2$, dus geldt

$$\varphi\left(\frac{\pi}{2}\right) = 2\arcsin\left(\frac{b}{\sqrt{d^2 - a^2}}\right) = 2\arcsin(1) = \pi$$

Omdat $\varphi$ continu is volgt uit de tussenwaardestelling dat elke waarde tussen $\varphi(0)$ en $\pi$ wordt aangenomen.

□

Wat we dus aangetoond hebben is dat er een $\psi$ bestaat waarvoor $\varphi(\psi) = \theta$. De Derickx-constructie is de configuratie $g_\psi$. Er rest ons te bewijzen dat de configuratie met de eis dat het laatste punt op het vlak door $A, C$ en $g_\psi(C)$ ligt rigide is.

## 3.3 Rigiditeit van de configuratie

De laatste stap is het bewijs dat de Derickx-constructie rigide is. Hiervoor laten we $b_0, \ldots, b_n > 0$ gegeven zijn en $\theta \in (0, \pi)$ zo dat er geen zelfdoorsnijding plaats kan vinden.

Allereerst wat notatie. Voor dit stuk beschouwen we 3D-configuraties als deelverzameling van $\mathbb{C}\times\mathbb{R} \cong \mathbb{R}^3$. We beginnen in 0 met de strook en buigen na lengte $b_0$ met een hoek $\varphi < \theta$ af. Dit buigpunt geven we aan met $B_0 \in \mathbb{C} \subset \mathbb{C} \times \mathbb{R}$. Soortgelijk geven we de opvolgende buigpunten aan met $B_1, \ldots, B_n$. We schrijven $\mathcal{D} : [0, 1]^2 \to \mathbb{C} \times \mathbb{R}$ voor de Derickx-constructie. Nu is $\mathrm{Re}(B_i)$ een functie in $\varphi$, namelijk

$$\mathrm{Re}(B_i)(\varphi) = \sum_{j=0}^{i} b_j \cos(j\varphi)$$

De restricties op $\mathcal{D}$ zijn de volgende. Allereerst willen we dat $\mathcal{D}(B_0), \ldots, \mathcal{D}(B_n) \in \mathbb{C} \times \{0\}$. Daarnaast willen we dat $\mathrm{Re}(B_n)(\varphi) = 0$. In de configuratie is dat dus de eis dat $B_n$ op de loodlijn door 0 op de lijn $L(0, B_0)$ ligt. Verder eisen we voor het gemak dat $\mathcal{D}(0) = 0$.

Voor we het bewijs van rigiditeit geven, hebben we nog een extra restrictie nodig. We willen dat er lokaal maar één oplossing is voor de vergelijking $\mathrm{Re}(B_n)(\varphi) = 0$, oftewel dat er een open omgeving van $\theta$ is waarin $\mathrm{Re}(B_n)(\varphi)$ niet 0 is. Dit is waar als de afgeleide in $\theta$ niet 0 is.

**Stelling 3.5.** Laat $\mathrm{Re}(B_n)' = \frac{d}{d\varphi}\mathrm{Re}(B_n)$. Als $\mathrm{Re}(B_n)'(\theta) \neq 0$, dan is $\mathcal{D}$ rigide onder de restricties $\mathcal{D}(B_0), \ldots, \mathcal{D}(B_n) \in \mathbb{R}^2 \times \{0\}$ en $\mathrm{Re}(B_n)(\varphi) = 0$.

*Bewijs.* Aangezien $\mathrm{Re}(B_n)'(\theta) \neq 0$, kan een vervorming van $\mathcal{D}$ de hoek $\psi$ niet meer veranderen. Immers, $\varphi$ was als functie in de variabele $\psi$ injectief, dus bij een wijziging van $\psi$ wijzigt $\varphi$ ook.

Aangezien $\mathcal{D}(0) = 0$, weten we dat $\mathcal{D}(B_0)$ op een cirkel met straal $b_0$ om 0 heen moet liggen. Dit is een cirkel, en geen bol, omdat we een vlak gekozen hebben. Zodra we $\mathcal{D}(B_0)$ gekozen hebben, weten we ook waar $B_1$ heen moet: de hoek $\angle 0\mathcal{D}(B_0)\mathcal{D}(B_1)$ moet gelijk zijn aan $\pi - \theta$ en de afstand tussen $\mathcal{D}(B_0)$ en $\mathcal{D}(B_1)$ moet gelijk zijn aan $b_1$. Zo liggen achtereenvolgend ook $\mathcal{D}(B_2), \ldots, \mathcal{D}(B_n)$ vast. Ook van de punten $A_i$ die "boven" de $B_i$ liggen, ligt het beeld vast, dit zijn de punten die we omhoog tillen om de hoek $\psi$ te krijgen. Interpolatie tussen deze hoekpunten legt de configuratie nu vast.

Een vervorming met restricties van $\mathcal{D}$ komt dus neer op het verplaatsen van $\mathcal{D}(B_0)$. Aangezien dit verplaatsen over de cirkel met een isometrie kan, volgt dat elke vervorming triviaal is.

□

Met het bewijs van rigiditeit hebben we een constructie gevonden die ons algebraïsche getallen $\alpha$ geeft die voldoen aan een aantal eisen. In de volgende sectie gaan we bewijzen dat de getallen die we hiermee kunnen krijgen genoeg zijn om een algebraïsche afsluiting van $\mathbb{Q}$ te construeren.

# 4 Elk algebraïsch getal is origami-construeerbaar

We hebben nu een constructie gevonden die vrij specifieke algebraïsche getallen construeert. Op het eerste oog is misschien niet duidelijk welke en hoeveel getallen we te pakken hebben. In dit hoofdstuk tonen we aan dat de algebraïsche getallen die construeerbaar zijn met de Derickx-constructie genoeg zijn om heel $\overline{\mathbb{Q}}$ te construeren.

Allereerst een algemene definitie.

**Definitie 4.1** (Signatuur)**.** Laat $\alpha \in \overline{\mathbb{Q}}$ met minimumpolynoom $f$. De signatuur van $\alpha$ is een paar $(r, s)$ waarbij $r$ het aantal reële nulpunten en $2s$ het aantal niet-reële nulpunten van $f$ is.

## 4.1 Tensorproduct van $\mathbb{Q}(\alpha)$ en $\mathbb{R}$

We laten nu $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ met signatuur $(r, s)$ en minimumpolynoom $f$. We bekijken allereerst een tensorproduct, namelijk het tensorproduct $\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R}$. Dit geeft ons de mogelijkheid om te werken met de reële topologie. Als $\mathbb{Q}$-vectorruimte is $\mathbb{Q}(\alpha)$ isomorf met $\mathbb{Q}^n$, waar $n$ de graad van $f$ is. Voor het tensorproduct met $\mathbb{R}$ geldt dan

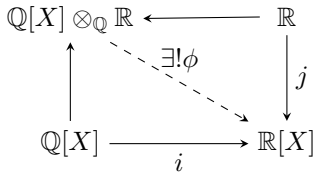
$$\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{Q}^n \otimes_{\mathbb{Q}} \mathbb{R} \cong \left( \bigoplus_{i=1}^{n} \mathbb{Q} \right) \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigoplus_{i=1}^{n} (\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{R}) \cong \mathbb{R}^n$$

Hiermee kunnen we het tensorproduct een topologie geven door transport van structuur. We weten dat $\mathbb{Q}(\alpha)$ hier dicht in ligt met de kanonieke inbeddeing $x \mapsto x \otimes 1$.

Nu willen we ook weten wat het tensorproduct als ring precies is, hiervoor bekijken we $\mathbb{Q}[X]/(f) \cong \mathbb{Q}(\alpha)$.

**Lemma 4.2.** Er geldt $\mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]$ en dat $(f) \otimes_{\mathbb{Q}} \mathbb{R} \cong f\mathbb{R}[X]$.

*Bewijs.* We beschouwen twee ringhomomorfismen, namelijk de inclusies $i : \mathbb{Q}[X] \to \mathbb{R}[X]$ en $j : \mathbb{R} \to \mathbb{R}[X]$. Aangezien het tensorproduct een som is in de categorie van commutatieve ringen, bestaat er een unieke afbeelding van ringen $\phi : \mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}[X]$ zo dat




commuteert. Hierbij zijn de afbeeldingen $\mathbb{R} \to \mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R}$ en $\mathbb{Q}[X] \to \mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R}$ de kanonieke afbeeldingen. Deze $\phi$ wordt gegeven door $g \otimes r \mapsto gr$. Als $gr = 0$, dan moet $g = 0$ of $r = 0$, dus moet $g \otimes r = 0$, dus $\phi$ is injectief. Verder kunnen we een polynoom $h \in \mathbb{R}[X]$ terugvinden door de som van $\phi(X \otimes h_i)$ te bekijken,

waarbij de $h_i$ de coëfficienten van $h$ zijn. We zien dat $\phi$ een isomorfisme is. Een restrictie van deze afbeelding tot $(f) \otimes_{\mathbb{Q}} \mathbb{R}$ levert een isomorfisme

$$(f) \otimes_{\mathbb{Q}} \mathbb{R} \cong f\mathbb{R}[X]$$

op. □

**Gevolg 4.3.** Er is een ringisomorfisme $\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(f)$.

*Bewijs.* We hebben een korte exacte rij van $\mathbb{Q}$-vectorruimtes

$$0 \to (f) \to \mathbb{Q}[X] \to \mathbb{Q}[X]/(f) \to 0$$

De eerste pijl is de inclusie van het ideaal $(f)$ in $\mathbb{Q}[X]$, de tweede pijl is de quotientafbeelding. Omdat het tensorproduct van vectorruimtes over het grondlichaam exact is, krijgen we een korte exacte rij

$$0 \to (f) \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R} \to (\mathbb{Q}[X]/(f)) \otimes_{\mathbb{Q}} \mathbb{R} \to 0$$

Hieruit volgt met lemma 4.2

$$(\mathbb{Q}[X]/(f)) \otimes_{\mathbb{Q}} \mathbb{R} \cong (\mathbb{Q}[X] \otimes_{\mathbb{Q}} \mathbb{R})/((f) \otimes_{\mathbb{Q}} \mathbb{R}) \cong \mathbb{R}[X]/(f)$$

□

Laat $f = (X - \alpha_1) \cdots (X - \alpha_n)$ de ontbinding van $f$ in $\mathbb{C}$ zijn, dan krijgen we een ontbinding in $\mathbb{R}$:

$$f = (X - x_1) \cdots (X - x_r)(X^2 - (z_1 + \overline{z_1})X + z_1\overline{z_1}) \cdots (X^2 - (z_s + \overline{z_s})X + z_s\overline{z_s})$$

Merk op dat $r \geq 1$ omdat $f(\alpha) = 0$.

**Stelling 4.4.** Er is een ringisomorfisme $\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$.

*Bewijs.* Omdat $f$ separabel is, zijn alle irreducibele factoren verschillend, en hebben ze verschillende nulpunten. We krijgen

$$\begin{aligned} \text{ggd}(X - x_i, X - x_j) &= \text{ggd}(X - x_i, X^2 - (z_j + \overline{z_j})X + z_j\overline{z_j}) \\ &= \text{ggd}(X^2 - (z_i + \overline{z_i})X + z_i\overline{z_i}, X^2 - (z_j + \overline{z_j})X + z_j\overline{z_j}) = 1 \end{aligned}$$

zodra $i \neq j$. Dit geeft gelegenheid de Chinese reststelling toe te passen:

$$\mathbb{R}[X]/(f) \cong \prod_{i=1}^{r} \mathbb{R}[X]/(X - x_i) \times \prod_{j=1}^{s} \mathbb{R}[X]/(X^2 - (z_j + \overline{z_j})X + z_j\overline{z_j})$$

Wegens irreducibiliteit zijn de ringen in het product lichaamsuitbreidingen van $\mathbb{R}$, de eerste $r$ zijn triviale uitbreidingen en de laatste $s$ zijn isomorf met de enige niet-triviale uitbreiding van $\mathbb{R}$. We krijgen $\mathbb{R}[X]/(f) \cong \mathbb{R}^r \times \mathbb{C}^s$. Uit gevolg 4.3 volgt de stelling. □

## 4.2 Een open deel in $\mathbb{R}^r \times \mathbb{C}^s$

We willen nu een niet-lege open verzameling in $\mathbb{R}^r \times \mathbb{C}^s$ vinden waarin aan de condities voor de Derickx-constructie wordt voldaan. We laten $(r, s)$ wederom de signatuur van een $\alpha \in \overline{\mathbb{Q}}$ met $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

**Notatie 4.5.** Laat $x := (x_0, \ldots, x_{n+1}) \in \mathbb{R}^{n+2}$. We definiëren

$$g_x(t) := x_0 + x_1 \cos(t) + \cdots + x_n \cos(t)$$

Deze $g_x$ maakt de notatie voor ons open deel iets gemakkelijker.

**Notatie 4.6.** We schrijven

$$U := \left\{ x = (x_0, \ldots, x_{n+1}) \in \mathbb{R}^{n+2} \;\middle|\; \begin{array}{c} x_0, \ldots, x_n > 0 \\ \exists \theta \in (0, \pi)\, x_{n+1} = \cos(\theta) \\ \frac{dg_x}{dt}(\theta) \neq 0 \\ \text{De bijbehorende Derickx-constructie} \\ \text{heeft geen zelfdoorsnijding.} \end{array} \right\}$$

De laatste twee eisen zorgen ervoor dat de configuratie rigide is.

**Propositie 4.7.** De verzameling $U$ is open in $\mathbb{R}^{n+2}$.

*Bewijs.* De eerste drie eisen beschrijven een open deel in $\mathbb{R}^{n+2}$, omdat die gaan over ongelijkheden, open intervallen en de open afbeelding cos. We bewijzen hier dat ook de laatste eis een open conditie is. De conditie dat er geen zelfdoorsnijdingen plaatsvinden is de conditie dat alle niet-aangrenzende lijnstukken niet snijden. We laten zien dat dit voor twee lijnstukken een open conditie is. Laat $A, B, C, D$ punten in $\mathbb{R}^2$ zijn. Laat $AB$ het lijnstuk tussen $A$ en $B$ zijn en $CD$ het lijnstuk tussen $C$ en $D$. Als we aannemen dat $AB \cap CD = \varnothing$, dan is

$$d(AB, CD) := \inf\{|x - y| : x \in AB, y \in CD\} > 0$$

Deze afstand is groter dan 0 omdat $AB$ en $CD$ compact zijn. De verzameling

$$\left\{ (x, y, z, w) \in \mathbb{R}^4 : |x - A|, |x - B|, |x - C|, |x - D| < \frac{d(AB, CD)}{2} \right\}$$

is een open omgeving van $(A, B, C, D)$ in $\mathbb{R}^4$, en binnen deze verzameling snijden de lijnstukken $xy$ en $zw$ elkaar niet. De conditie dat twee lijnstukken elkaar niet snijden is dus een open conditie, en er volgt dat $U$ open is.

□

Ons doel is nu om een continue afbeelding van $\mathbb{R}^r \times \mathbb{C}^s$ naar $\mathbb{R}^{n+2}$ te maken die niet meer afhangt van $\alpha$. Het inverse beeld van $U$ zal dan een voortbrenger van $\mathbb{Q}(\alpha)$ bevatten.

Laat $\mathbb{R}[X]_n$ de verzameling van monische polynomen in $\mathbb{R}[X]$ van graad $n$. Door coëfficiënten van polynomen in $\mathbb{R}[X]_n$ als coördinaten in $\mathbb{R}^n$ te beschouwen, krijgen we een natuurlijke bijectie tussen $\mathbb{R}[X]_n$ met $\mathbb{R}^n$:

$$h : \mathbb{R}[X]_n \to \mathbb{R}^n,\ X^n + a_{n-1}X^{n-1} + \cdots + a_0 \mapsto (a_{n-1}, \ldots, a_0)$$

Daarmee kunnen we een topologie op $\mathbb{R}[X]_n$ leggen door te eisen dat deze bijectie een homeomorfisme is.

**Notatie 4.8.** We schrijven $(x, z) := (x_1, \ldots, x_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$ en

$$f_{x,z} := \prod_{i=1}^{r}(X - x_i) \prod_{j=1}^{s}(X - z_i)(X - \overline{z_i})$$

We definiëren

$$\varphi : \mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}[X]_n \times \mathbb{R}, (x, z) \mapsto (f_{x,z}, x_1)$$

Deze afbeelding is continu. Wegens de topologie op $\mathbb{R}[X]_n$ is $\varphi$ namelijk continu precies als $(h, \mathrm{id}_{\mathbb{R}}) \circ \varphi$ dat is, en aangezien elk van de coëfficienten van $f_{x,z}$ een polynomiale uitdrukking in $x_1, \ldots, x_r, z_1, \ldots, z_s$ is, is deze afbeelding continu.

We definiëren de verzameling

$$Z := \{(f, x) \in \mathbb{R}[X]_n \times \mathbb{R} : f(x) = 0\}$$

dan kunnen we het codomein van $\varphi$ vervangen door $Z$. Gegeven een polynoom $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ krijgen we coëfficienten $b_0, \ldots, b_n$ door $\cos(\theta)$ in te vullen voor $X$ en de power reduction formulas toe te passen. Dit geeft een afbeelding

$$\psi : Z \to \mathbb{R}^{n+2}, (X^n + a_{n-1}X^{n-1} + \cdots + a_0, x) \mapsto (b_0, \ldots, b_n, x)$$

Deze afbeelding is continu, want het is de samenstelling van $(h, \mathrm{id}_{\mathbb{R}})$ met de $\mathbb{R}$-lineaire afbeelding

$$\mathbb{R}^n \to \mathbb{R}^{n+1}, (a_0, \ldots, a_{n-1}) \mapsto (b_0, \ldots, b_n)$$

Samengevat levert ons dit het volgende op.

**Gevolg 4.9.** De afbeelding

$$\Psi : \mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}^{n+2}, (x, z) \mapsto (b_0, \ldots, b_n, x_1)$$

waarbij $b_0, \ldots, b_n$ de coëfficiënten verkregen door de substitutie $X = \cos(\theta)$ in $f_{x,z}$ zijn, is continu.

Eerder hebben we een open deel $U$ in $\mathbb{R}^{n+2}$ gevonden waar de Derickx-constructie goed gaat. Met $\Psi$ levert dit een open deel $\Psi^{-1}(U)$ op in $\mathbb{R}^r \times \mathbb{C}^s$ waar de constructie goed gaat.

## 4.3 Voortbrengers van $\mathbb{Q}(\alpha)$

We hebben nu een continue afbeelding $\mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}^{n+2}$. Dit levert ons een open deel in $\mathbb{R}^r \times \mathbb{C}^s$ op. We weten dat $\mathbb{Q}(\alpha)$ dicht in $\mathbb{R}^r \times \mathbb{C}^s$ ligt, dus als dit open deel niet leeg is, wat later zal blijken, hebben we in dit open deel elementen van $\mathbb{Q}(\alpha)$ liggen. We hebben echter nog meer nodig. Wij willen namelijk dat er een voortbrenger van $\mathbb{Q}(\alpha)$ in ligt.

**Definitie 4.10** (Discriminantlocus)**.** De discriminantlocus $\Delta$ in $\mathbb{R}^r \times \mathbb{C}^s$ is de verzameling

$$\Delta := \{(x, z) \in \mathbb{R}^r \times \mathbb{C}^s : f_{x,z} \text{ is niet separabel}\}$$

De formele definitie van de discriminantlocus is dat $x_i = x_j$ voor zekere $i \neq j$, $z_i = z_j$ voor zekere $i \neq j$ of voor zekere $i, j$ geldt dat $\overline{z_i} = \overline{z_j}$. In onze context is dat precies wanneer $f_{x,z}$ niet separabel is. Om een voortbrenger van $\mathbb{Q}(\alpha)$ in $\mathbb{R}^r \times \mathbb{C}^s$ te vinden, zullen we buiten $\Delta$ moeten blijven. Een inseparabele $f_{x,z}$ gaat immers nooit het minimumpolynoom van een algebraïsch getal zijn. Het voordeel is dat $\Delta$ gesloten is, dus weten we dat $\Psi^{-1}(U) \cap ((\mathbb{R}^r \times \mathbb{C}^s) \backslash \Delta)$ nog steeds open is.

**Notatie 4.11.** We schrijven

$$V := \Psi^{-1}(U) \cap ((\mathbb{R}^r \times \mathbb{C}^s) \backslash \Delta)$$

Stel nu dat $\alpha' \in \mathbb{Q}(\alpha)$ is, zo dat de uitbreiding $\mathbb{Q}(\alpha') \subset \mathbb{Q}(\alpha)$ graad $d$ heeft. We definiëren

$$B : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha),\ x \mapsto \alpha' x$$

**Definitie 4.12** (Karakteristiek polynoom)**.** Het karakteristieke polynoom van een $\alpha' \in \mathbb{Q}(\alpha)$ is het karakteristieke polynoom dat hoort bij $B$ als $\mathbb{Q}$-lineair endomorfisme.

We kunnen nu ook de $\mathbb{Q}$-lineaire afbeelding

$$A : \mathbb{Q}(\alpha') \to \mathbb{Q}(\alpha'), x \mapsto \alpha' x$$

Bij $A$ hoort een karakteristiek polynoom, zeg $f_{\alpha'}$. Doordat $\mathbb{Q}(\alpha)$ als vectorruimte isomorf is met $\mathbb{Q}(\alpha')^d$, geldt dat het karakteristieke polynoom van $\alpha'$ gelijk is aan $(f_{\alpha'})^d$.

**Stelling 4.13.** Voor een $\alpha' \in \mathbb{Q}(\alpha)$ is het beeld onder de afbeelding $\mathbb{Q}(\alpha) \to \mathbb{R}[X]_n$ gelijk aan het karakteristieke polynoom van $\alpha'$.

*Bewijs.* Laat $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R}$ de kanonieke inbedding $x \mapsto x \otimes 1$ zijn. Dan krijgen we een afbeelding

$$\phi(A) : \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R}, x \mapsto \phi(\alpha') x$$

Nu beeldt een $\alpha' \in \mathbb{Q}(\alpha)$ onder de inbedding in $\mathbb{R}^r \times \mathbb{C}^s$ af op een element van de vorm $(\sigma_1(\alpha'), ..., \sigma_r(\alpha'), \tau_1(\alpha'), ..., \tau_s(\alpha'))$ waarbij $\sigma_i$ de verschillende inbeddingen in $\mathbb{R}$ zijn en $\tau_j, \overline{\tau_j}$ zijn de overige inbeddingen in $\mathbb{C}$. Hiervoor kiezen we dus één inbedding per paar geconjugeerde inbeddingen. Met een geschikte keuze van basis voor $\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{R}$ als $\mathbb{R}$-vectorruimte, namelijk die correspondeert met de basis van de eenheidsvectoren in $\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$, kunnen we $\phi(A)$ als blokmatrix schrijven:

$$\begin{pmatrix} \sigma_1(\alpha') & 0 & \cdots & 0 & 0 \\ 0 & \sigma_2(\alpha') & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \tau_{s-1}(\alpha') & 0 \\ 0 & 0 & \cdots & 0 & \tau_s(\alpha') \end{pmatrix}$$

Hierbij zijn $\sigma_i$ de $1 \times 1$-matrices die horen bij de reële inbeddingen van $\mathbb{Q}(\alpha')$ en $\tau_i$ de niet-diagonaliseerbare inbeddingen, die $2 \times 2$-matrices opleveren. Het

karakteristieke polynoom van $\phi(A)$ is nu precies het polynoom waar $\alpha'$ op afgebeeld wordt in $\mathbb{R}[X]_n$. Merk tenslotte op dat het karakteristieke polynoom gedefinieerd kan worden als het product van $X - \lambda_i$ als $\lambda_i$ de eigenwaarden van de afbeelding zijn. Wegens de definitie van $\phi(A)$ geldt dat de eigenwaarden van $\phi(A)$ precies de eigenwaarden van $A$ zijn, dus de karakteristieke polynomen zijn gelijk. Er volgt dat $\alpha'$ op $f_{\alpha'}$ wordt afgebeeld.

□

Aangezien het karakteristieke polynoom van $\alpha'$ separabel is precies als $\mathbb{Q}(\alpha') \subset \mathbb{Q}(\alpha)$ graad 1 heeft, kunnen we uit deze stelling het volgende afleiden.

**Gevolg 4.14.** Een $\alpha' \in \mathbb{Q}(\alpha)$ wordt afgebeeld op een separabel polynoom in $\mathbb{R}[X]_n$ dan en slechts dan als $\alpha'$ een voortbrenger van $\mathbb{Q}(\alpha)$ is.

In $V$ is nu wegens de laatste stelling elk element van $\mathbb{Q}(\alpha)$ een voortbrenger van $\mathbb{Q}(\alpha)$. Aangezien $\mathbb{Q}(\alpha)$ dicht in $\mathbb{R}^r \times \mathbb{C}^s$ ligt, weten we dat $V \neq \varnothing$ voldoende is om te concluderen dat we een voortbrenger van $\mathbb{Q}(\alpha)$ kunnen vinden die geschikt is voor de Derickx-constructie.

## 4.4 Een construeerbare voortbrenger

We bekijken de volgende uitdrukking:

$$c + \frac{1}{2} + \cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta)$$

voor een zekere $c$ en $\theta \in (0, \pi)$ zo dat er geen zelfdoorsnijding plaats vindt. We claimen dat er voor elke signatuur $(r, s)$ met $r > 0$ een geschikte $c$ is zo dat er een separabel polynoom $f_c$ met signatuur $(r, s)$ en een gegeven reëel nulpunt $x$ bestaat zo dat $(f_c, x)$ door de $\psi$ uit paragraaf 4.2 op $(c, 1, \ldots, 1, \cos(\theta)) \in \mathbb{R}^{n+2}$ wordt afgebeeld. Merk op dat deze combinatie geschikt is voor de Derickx-constructie.

### 4.4.1 Totaal reële getallen

Allereerst bekijken we zogenaamde totaal reële getallen.

**Definitie 4.15** (Totaal reëel)**.** Een $\alpha \in \overline{\mathbb{Q}}$ heet totaal reëel als de signatuur gelijk is aan $(n, 0)$, waarbij $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Hiervoor bekijken we de uitdrukking

$$\frac{1}{2} + \sum_{i=1}^{n} \cos(i\theta)$$

We gaan allereerst aantonen dat deze uitdrukking gelijk is aan $f(\cos(\theta))$ voor een of ander polynoom $f$. Hiervoor hebben we zogeheten Chebyshev polynomen nodig.

**Definitie 4.16** (Chebyshev polynomen [W1])**.** De Chebyshev polynomen worden gedefinieerd door $T_0(X) := 1$, $T_1(X) := X$ en $T_{n+1}(X) := 2XT_n(X) - T_{n-1}(X)$ als $n \geq 0$.

Het nut van deze polynomen komt naar voren in de volgende propositie.

**Propositie 4.17.** Voor $n \geq 0$ is $T_n(X)$ het unieke polynoom wat voldoet aan $T_n(\cos(\theta)) = \cos(n\theta)$.

*Bewijs.* Het bewijs van het eerste deel gaat met inductie. Voor $n \in \{0, 1\}$ is de claim waar, dus neem aan dat $n \geq 1$ en stel dat de claim geldt voor alle $m \leq n$. Dan geldt met behulp van de somformules

$$\begin{aligned} T_{n+1}(\cos(\theta)) &= 2\cos(\theta)\cos(n\theta) - \cos((n-1)\theta) \\ &= 2\cos(\theta)\cos(n\theta) - \cos(n\theta)\cos(\theta) - \sin(n\theta)\sin(\theta) \\ &= \cos(\theta)\cos(n\theta) - \sin(\theta)\sin(n\theta) = \cos((n+1)\theta) \end{aligned}$$

Dit toont aan dat de Chebyshev polynomen aan de gelijkheid voldoen. Als moet gelden dat $T_0(\cos(\theta)) = 1$ voor alle $\theta$, moet $T_0$ wel constant 1 zijn, zo ook $T_1(X) = X$. Dit toont aan dat $T_0$ en $T_1$ vast liggen. Begin nu met $T_{n+1}(\cos(\theta)) = \cos((n+1)\theta)$ en we vinden de recurrentie uit de definitie terug door de gelijkheden uit onze inductiestap van eerder om te draaien. Aangezien polynomen van graad $n$ vast liggen bij door $n+1$ waardes, volgt hieruit dat de polynomen uniek zijn.

□

**Gevolg 4.18.** Voor $(a_0, \ldots, a_n) \in \mathbb{R}^{n+1}$, laat $(b_0, \ldots, b_n) \in \mathbb{R}^{n+1}$ de coëfficiënten die verkregen worden door het omschrijven van $\sum_{i=0}^{n} a_i X^i$ naar $\sum_{i=0}^{n} b_i \cos(i\theta)$. De afbeelding

$$\mathbb{R}^{n+1} \to \mathbb{R}^{n+1}, (a_0, \ldots, a_n) \mapsto (b_0, \ldots, b_n)$$

is een lineair isomorfisme.

*Bewijs.* Dat de afbeelding lineair is volgt direct uit de power reduction formulas, aangezien elke $b_i$ een lineaire combinatie van $a_j$'s is. Met behulp van propositie 4.17 vinden we bij een combinatie $\sum_{i=0}^{n} b_i \cos(i\theta)$ een uniek polynoom $\sum_{i=0}^{n} b_i T_i(X)$ terug. De afbeelding is hiermee inverteerbaar en hiermee een lineair isomorfisme.

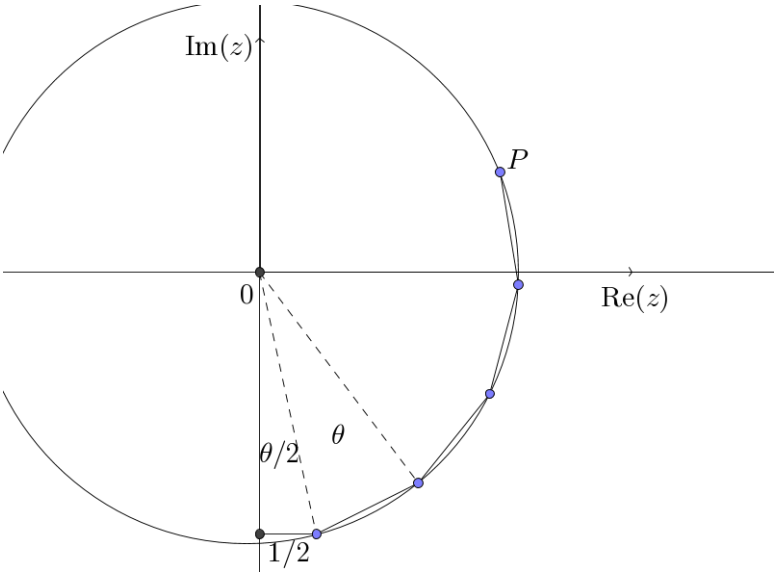
□

Hiermee kunnen we dus een polynoom $f$ vinden zo dat

$$f(\cos(\theta)) = \frac{1}{2} + \sum_{i=1}^{n} \cos(i\theta)$$

Merk op dat $f$ niet monisch is. De kopterm is wel positief, zo volgt uit de definitie van Chebyshev polynomen. Deze term is namelijk gelijk aan $2^n$. Door vermenigvuldiging van $f$ met $2^{-n}$ vinden we een polynoom $\widetilde{f}$ dat monisch is en dezelfde nulpunten heeft als $f$. Met het lineaire isomorfisme uit gevolg 4.18 weten we ook dat de $b_i$ die bij $\widetilde{f}$ horen nog steeds positief zijn. Als we aantonen

dat de nulpunten van $f$ aan de restricties voldoen, hebben we dus aangetoond dat er een construeerbare voortbrenger van $\mathbb{Q}(\alpha)$ is voor elke totaal reële $\alpha$. Voor het bewijs hiervan gaan we $f(\cos(\theta))$ omschrijven naar een wat eenvoudigere uitdrukking.




De bovenstaande illustratie geeft een schets van de situatie. De buitenhoeken moeten de hoek $\theta$ zijn, en de lengtes zijn achtereenvolgend $\frac{1}{2}, 1, 1, \ldots, 1$. Nu is $f(\cos(\theta))$ gelijk aan het reële deel van het laatste punt.

**Lemma 4.19.** Neem aan dat $\theta \in (0, \pi)$. Er geldt

$$f(\cos(\theta)) = \frac{\sin\left(\left(n + \frac{1}{2}\right)\theta\right)}{2\sin\left(\frac{\theta}{2}\right)}$$

*Bewijs.* Merk op dat de punten op een cirkel liggen, waarvan de de straal $r$ kunnen uitrekenen met behulp van $\theta$. We hebben

$$r = \frac{1}{2\sin(\frac{\theta}{2})}$$

Verder kunnen we hiermee het reële deel van het laatste punt van de constructie uitrekenen, en dit is precies $f(\cos(\theta))$. Als we het plaatje tegen de klok in roteren, dan kunnen we dit figuur zien als een cirkel met straal $r$ om de oorsprong, en dan wordt $f(\cos(\theta))$ de hoogte van het geroteerde punt. Dit is gelijk aan

$$f(\cos(\theta)) = r\sin\left(\left(n + \frac{1}{2}\right)\theta\right) = \frac{\sin\left(\left(n + \frac{1}{2}\right)\theta\right)}{2\sin\left(\frac{\theta}{2}\right)}$$

□

Met deze uitdrukking kunnen we de restricties nagaan. We kunnen allereerst $f(\cos(\theta)) = 0$ oplossen, dit is precies als $\sin\left(\left(n+\frac{1}{2}\right)\theta\right) = 0$, dus als

$$\theta = \frac{k\pi}{n+\frac{1}{2}}$$

voor een of andere $k \in \mathbb{Z}$. Merk op dat $\theta_1 = \frac{\pi}{n+\frac{1}{2}}$ een oplossing is en dat $\alpha = \cos(\theta_1)$ een nulpunt van $f$ is dat voldoet aan de gestelde eisen. Er geldt namelijk $\theta_1 < \frac{\pi}{n}$, waardoor zelfdoorsnijding uitgesloten is en we gaan nu aantonen dat de afgeleide van $f(\cos(\theta))$ niet 0 is in $\theta_1$.

**Lemma 4.20.** Laat $f_\theta(\theta) := \frac{d}{d\theta} f(\cos(\theta))$ voor $\theta \in (0, \pi)$. Als $f(\cos(\theta_0)) = 0$, dan geldt $f_\theta(\theta_0) \neq 0$.

*Bewijs.* Er geldt

$$f_\theta(\theta) = \frac{2\left(n+\frac{1}{2}\right)\sin\left(\frac{\theta}{2}\right)\cos\left(\left(n+\frac{1}{2}\right)\theta\right) - \cos\left(\frac{\theta}{2}\right)\sin\left(\left(n+\frac{1}{2}\right)\theta\right)}{4\sin^2\left(\frac{\theta}{2}\right)}$$

In $\theta_0$ geëvalueerd levert dit de volgende uitdrukking op:

$$f_\theta(\theta_0) = \frac{2\left(n+\frac{1}{2}\right)\cos\left(\left(n+\frac{1}{2}\right)\theta_1\right)}{4\sin\left(\frac{\theta_0}{2}\right)}$$

Aangezien de sinus verdwijnt op $\left(n+\frac{1}{2}\right)\theta_0$, is de cosinus hier niet 0 en is deze uitdrukking dus ongelijk aan 0.

□

We moeten alleen nog aantonen dat $f$ ook separabel is. We maken gebruik van de volgende propositie.

**Propositie 4.21.** Alle nulpunten van $f$ en de afgeleide $f'$ liggen in $[-1, 1]$.

*Bewijs.* We hebben nulpunten van $f(\cos(\theta))$ voor

$$\theta \in \left\{ \frac{\pi}{n+\frac{1}{2}}, \frac{2\pi}{n+\frac{1}{2}}, \ldots, \frac{n\pi}{n+\frac{1}{2}} \right\}$$

Omdat dit hoeken tussen 0 en $\pi$ in zijn en de cosinus daar injectief is, volgt dat dit $n$ verschillende nulpunten van $f$ oplevert. Omdat tussen elk tweetal nulpunten van $f$ een minimum of maximum moet liggen, volgt dat ook alle nulpunten van $f'$ in dit interval liggen.

□

Voor het bewijs van de volgende propositie hebben we nog niet nodig dat $f'$ al zijn nulpunten tussen $-1$ en 1 liggen, maar dit zal later van pas komen.

**Propositie 4.22.** Het polynoom $f$ is separabel.

*Bewijs.* Laat $f'$ de afgeleide van het polynoom $f$. Dan geldt

$$f_\theta(\theta) = -\sin(\theta) f'(\cos(\theta))$$

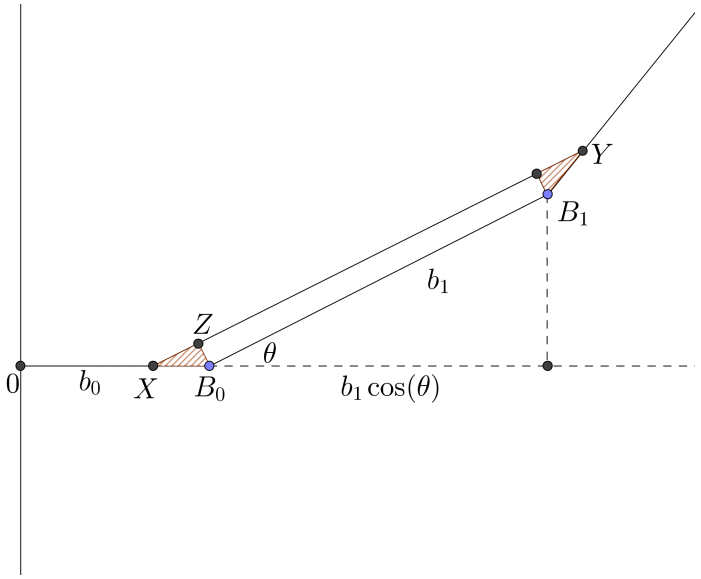
dus $f'(\cos(\theta)) = -\frac{f_\theta(\theta)}{\sin(\theta)}$ als $\sin(\theta) \neq 0$. In het bewijs van lemma 4.20 hebben we laten zien dat $f_\theta$ geen nulpunten deelt met $f(\cos(\theta))$. Hieruit volgt dat er geen $\theta$ is zo dat $f(\cos(\theta)) = f'(\cos(\theta)) = 0$ zo lang $\sin(\theta) \neq 0$. Als $\sin(\theta) = 0$, dan is $\theta = k\pi$ voor een $k \in \mathbb{Z}$, waardoor $\sin\left(\left(n + \frac{1}{2}\right)\theta\right) = \sin\left(nk\pi + \frac{k\pi}{2}\right) \neq 0$. Er volgt $f(\cos(\theta)) \neq 0$, dus $f$ deelt geen nulpunten met $f'$ op het interval $[-1, 1]$. Uit de propositie 4.21 volgt dat $f$ separabel is.

□

We kunnen nu bijna elk totaal reëel getal construeren. We hebben alleen nog nodig dat we gegeven de hoek $\theta$ ook de lengte $\cos(\theta)$ kunnen construeren.

**Propositie 4.23.** Laat $\alpha = \cos(\theta)$ voldoen aan de voorwaarden voor de Derickx-constructie. Dan is $\alpha$ construeerbaar.

*Bewijs.* De Derickx-constructie geeft ons dat we de hoek $\theta$ kunnen construeren. Allereerst een schets van de situatie.




Laat $B_0, B_1, B_2$ de eerste drie buigpunten van de constructie zijn. De punten $0 \neq X \neq B_0$ en $B_1 \neq Y \neq B_2$ kiezen we op de lijnstukken $0B_0$ en $B_1B_2$ zo dat de afstanden tussen $B_0$ en $X$ en $B_1$ en $Y$ gelijk zijn. Het enige wat we van die punten nodig hebben is dat ze op de aangegeven lijnstukken liggen, dus deze afstand kiezen we $2^{-m}$ voor de kleinste $m \geq 1$ waarvoor $X$ en $Y$ op die lijnstukken liggen. De gearceerde driehoeken zijn nu waar we in geïnteresseerd zijn. Laat $Z$ het derde hoekpunt van de driehoek met hoekpunten $X$ en $B_0$. Uit wat simpele meetkunde volgt dat de hoek $\angle ZXB_0$ gelijk is aan $\theta$, waardoor $\cos(\theta) = \frac{d(Z,X)}{2^{-m}}$, dus $\cos(\theta) = 2^m d(Z, X)$. Er volgt dat $\alpha = \cos(\theta)$ construeerbaar is, aangezien $d(Z, X)$ dat is.

□

Met al het voorwerk wat we nu gedaan hebben, kunnen we de volgende stelling bewijzen.

**Stelling 4.24.** Laat $\alpha \in \overline{\mathbb{Q}}$ totaal reëel. Dan is $\alpha$ construeerbaar.

*Bewijs.* Wegens stelling 4.4 ligt $\mathbb{Q}(\alpha)$ dicht in $\mathbb{R}^n$. De $U$ uit 4.6 bevat een element wat komt van een monisch polynoom $\widetilde{f}$ wegens gevolg 4.18 en lemma 4.20. Dit polynoom komt weer van een element buiten de discriminantlocus in $\mathbb{R}^n$ wegens Propositie 4.22. De $V$ van 4.11 is dus niet leeg en bevat omdat $\mathbb{Q}(\alpha)$ dicht ligt in $\mathbb{R}^n$ een element van $\mathbb{Q}(\alpha)$. Wegens gevolg 4.14 bevat $V$ een voortbrenger van $\mathbb{Q}(\alpha)$. Wegens propositie 4.23 is elk element uit $\mathbb{Q}(\alpha)$ in $V$ construeerbaar, dus volgt dat we een voortbrenger van $\mathbb{Q}(\alpha)$ kunnen construeren, dus is $\alpha$ construeerbaar.

□

### 4.4.2 Reële algebraïsche getallen

Het grootste deel van het werk is gedaan met het construeren van totaal reële getallen. We laten allereerst $\alpha \in \overline{\mathbb{Q}}$ met $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ en signatuur $(r, s)$ voor $r > 0$.

We bekijken de uitdrukking

$$f_c(\cos(\theta)) = c + \frac{1}{2} + \sum_{i=1}^{n} \cos(i\theta)$$

Dankzij gevolg 4.18 weten we dat $f_c$ een polynoom van graad $n$ is. De uitdrukking van lemma 4.19 blijft ook redelijk ongewijzigd:

$$f_c(\cos(\theta)) = c + \frac{\sin\left(\left(n + \frac{1}{2}\right)\theta\right)}{2\sin\left(\frac{\theta}{2}\right)}$$

Het optellen van een geschikte constante $c$ zorgt ervoor dat reële nulpunten verdwijnen. Hierdoor komen er complexe nulpunten bij. Het idee is dat we $c$ zo kunnen kiezen dat er $r$ reële nulpunten overblijven en dat er geen dubbele nulpunten komen.

**Lemma 4.25.** Laat $\theta_1 < \theta_2$ zo dat $f_0$ in $\theta_1$ en $\theta_2$ een lokaal minimum aanneemt. Dan is $f_0(\cos(\theta_1)) < f_0(\cos(\theta_2))$.

*Bewijs.* Omdat we alleen maar hoeken tussen 0 en $\pi$ bekijken, weten we dat $\theta_1, \theta_2 \in (0, \pi)$. Er geldt op dat interval dat $2\sin\left(\frac{\theta}{2}\right)$ strikt stijgend is, dus $f_0$ is als functie in $\theta$ een product van een periodieke en een strikt dalende functie. Dit wil zeggen dat $f_0$ een soort periodieke functie is met een dalende amplitude, waaruit volgt dat de mimima steeds groter worden.

□

**Notatie 4.26.** We laten $k$ het aantal lokale minima van $f_0(\cos(\theta))$ zijn en we nummeren deze met $M_1 < M_2 < \cdots < M_k$.

Deze notatie gebruiken we voor de volgende propositie.

Elk minimum van $f_0$ is kleiner dan 0. Zou er namelijk een minimum niet-negatief zijn, zou dit een dubbel of complex nulpunt van $f_0$ opleveren, wat in tegenspraak is met wat we eerder bewezen hebben.

**Propositie 4.27.** Er is een $c > 0$ zo dat $f_c$ signatuur $(r, s)$ heeft en separabel is.

*Bewijs.* Kies $c \in (-M_{s+1}, -M_s)$. Nu heeft $f_c(\cos(\theta))$ precies $s$ minima die groter zijn dan 0, hiermee zijn $2s$ reële nulpunten verdwenen. De signatuur van $f_c$ is daarom gelijk aan $(r, s)$. Omdat $c$ strikt tussen $-M_s$ en $-M_{s+1}$ ligt, zijn de resterende reële nulpunten enkelvoudig. De niet-reële nulpunten zijn enkelvoudig omdat de nulpunten van de afgeleide van $f_c$ wegens propositie 4.21 reëel zijn.

□

De $c$ uit propositie 4.27 zorgt er nu bijna voor dat $f_c$ aan de eisen voldoet. We hebben alleen nog een geschikt nulpunt van $f_c$ nodig, en daar helpt het volgende lemma bij.

**Lemma 4.28.** Laat $\theta_1$ als in 4.20. Dan is $f_0(\cos(\theta))$ dalend op een interval dat $(0, \theta_1]$ bevat.

*Bewijs.* We gebruiken de afgeleide die we in het bewijs van lemma 4.20 berekend hebben. Als we een $\theta < \theta_1$ kiezen geldt $\sin\left(\frac{\theta}{2}\right) > 0$, $\cos\left(\frac{\theta}{2}\right) > 0$ omdat $\theta_1 < \frac{\pi}{n}$. Voor $\theta \in \left(\frac{\theta_1}{2}, \theta_1\right)$ geldt dat $\cos\left(\left(n + \frac{1}{2}\right)\theta\right) < 0$, terwijl $\sin\left(\left(n + \frac{1}{2}\right)\theta\right) > 0$. We zien dat de afgeleide uit 4.20 dus negatief is op dit stuk. Een tekenwissel van de afgeleide op de rest van het interval zou een eerder nulpunt of een minimum wat groter is dan 0 betekenen, en is dus niet mogelijk. Omdat de afgeleide in $\theta_1$ niet 0 is, is het lemma bewezen.

□

**Opmerking 4.29.** We kunnen nu bijna bewijzen dat $f_c$ geschikt is voor de Derickx-constructie. Het enige wat we nog nodig hebben is dat er geen zelfdoorsnijding plaats vindt. Merk hiervoor op dat alle buigpunten van deze configuratie op een cirkel liggen. Zelfdoorsnijding is dus alleen mogelijk als we een hoek $\theta \geq \frac{2\pi}{n+1}$ nodig hebben om een nulpunt te krijgen. De conditie $\theta < \frac{2\pi}{n+1}$ is dus voldoende om zelfdoorsnijding uit te sluiten.

**Stelling 4.30.** Er is een $c \neq 0$ zo dat $f_c$ signatuur $(r, s)$ heeft en een nulpunt $\alpha = \cos(\theta)$ heeft voor een $\theta \in (0, \pi)$ die geschikt is voor de Derickx-constructie.

*Bewijs.* Laat $\theta_1$ als hiervoor. Kies een $c$ als in 4.27. Omdat $f_c(\cos(\theta))$ dalend is voor $\theta_1$, weten we dat het eerste nulpunt van $f_c$ voor het eerste minimum komt. Schrijf $g(\theta) = \frac{1}{2\sin\left(\frac{\theta}{2}\right)}$ en $h(\theta) = \sin\left(\left(n + \frac{1}{2}\right)\theta\right)$, dan is $f_0(\cos(\theta)) = g(\theta)h(\theta)$. De afgeleide van $f_c(\cos(\theta))$ is nu gelijk aan $h'(\theta)g(\theta) + h(\theta)g'(\theta)$. Als $h$ in $\theta_0$ zijn eerste minimum aanneemt, is de afgeleide van $f_0(\cos(\theta))$ hier gelijk aan $h(\theta_0)g'(\theta_0) > 0$. Het eerste minimum van $f_0(\cos(\theta))$ ligt dus voor het eerste

minimum van $h(\theta)$, wegens de tussenwaardestelling. Nu ligt er dus een nulpunt van $f_c(\cos(\theta))$ in het interval $(\theta_1, \theta_0)$. Voor elke $\theta$ in dit interval geldt

$$\theta < \theta_0 = \frac{3}{2} \cdot \frac{\pi}{n + \frac{1}{2}} < \frac{2\pi}{n+1}$$

Met onze eerdere opmerking volgt dat $f_c$ en zijn eerste nulpunt geschikt zijn voor de Derickx-constructie.

□

Net als in het totaal reële geval, hebben we nu dus een element gevonden in de $V$ uit 4.11. Hieruit kunnen we de volgende stelling afleiden.

**Stelling 4.31.** Laat $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$. Dan is $\alpha$ construeerbaar.

*Bewijs.* Aangezien $\alpha$ reëel is heeft het een minimumpolynoom met een reële wortel. Hieruit volgt dat de signatuur van $\alpha$ gelijk is aan $(r, s)$ voor $r > 0$. De rest van het bewijs is nu analoog aan dat van stelling 4.24.

□

Met alle reële algebraische getallen hebben we samen met de lichaamsoperaties uit de vlakke origami genoeg om heel $\overline{\mathbb{Q}}$ te construeren.

**Stelling 4.32.** Elke $\alpha \in \overline{\mathbb{Q}}$ is construeerbaar.

Daarmee zijn we aan het eind gekomen van alle constructieproblemen: met origami is alles mogelijk.

# Referenties


[AZ] Martin Aigner & Günter M. Ziegler. Proofs from THE BOOK, Fourth Edition, pagina's 81-84. Springer, ISBN: 978-3-642-00855-9, 2010.

[Al] Roger C. Alperin. A Mathematical Theory of Origami Constructions and Numbers, pagina 129. Jaar van publicatie: 2000. URL:

`http://nyjm.albany.edu/j/2000/6-8.pdf`

[AL] Roger C. Alperin & Robert J. Lang, "One-, Two-, and Multi-Fold Origami Axioms", pagina 2. Jaar van publicatie: 2009. URL:

`http://www.langorigami.com/science/math/quintisection/041_Alperin_article.pdf`

[HH] Humiaki Huzita, "Axiomatic Development of Origami Geometry", pagina's 143-158. *Proceedings of the First International Meeting of Origami Science and Technology*, Humiaki Huzita, 1989.

[Ki] James King. Origami-Constructible Numbers, pagina's 5-9. Jaar van publicatie: 2004. URL:

`http://www.cs.mcgill.ca/~jking/papers/origami.pdf`

[PT] José Ignacio Royo Prieto & Eulàlia Tramuns. Abelian and non-abelian numbers via 3D Origami, pagina's 3-9. Jaar van publicatie: 2014. arXiv:1408.0880. URL:

`http://arxiv.org/pdf/1408.0880v1.pdf`

[W1] Wikipedia contributors, Chebyshev polynomials. Gepubliceerd door *Wikipedia, The Free Encyclopedia*. Datum: 26-06-2015. URL:

`https://en.wikipedia.org/w/index.php?title=Chebyshev_polynomials&oldid=667969082`

[W2] Wikipedia contributors, List of trigonometric identities. Gepubliceerd door *Wikipedia, The Free Encyclopedia*. Datum: 26-06-2015. URL:

`https://en.wikipedia.org/w/index.php?title=List_of_trigonometric_identities&oldid=668235681`