CONSTRUCTIES MET PASSER EN LINIAAL, MOGELIJKHEDEN EN ONMOGELIJKHEDEN

GESCHREVEN DOOR
BEREND KROUWELS

Technische Universiteit Delft

DELFT, AUGUSTUS 2022

STUDENT NUMMER:	4921909
LOOPTIJD PROJECT:	18 FEBRUARI 2022 – 31 AUGUSTUS 2022
BEOORDELINGSCOMMISSIE:	DR. J. A. M. DE GROOT, TU DELFT, BEGELEIDER
	DR. IR. J. H. WEBER, TU DELFT

EEN DIGITALE VERSIE VAN DIT WERK IS TE VINDEN OP
HTTP://REPOSITORY.TUDELFT.NL/.

Samenvatting

Dit onderzoek gaat over de mogelijkheden en onmogelijkheden met betrekking tot constructies met passer en ongemarkeerde liniaal. Hier werken we met de euclidische meetkunde en zullen we dus ook beginnen met de vijf postulaten van Euclides en een aantal toepassingen ervan. Er zal besproken worden wat het betekent voor een punt of constructie om construeerbaar te zijn, hiervoor zal gedefinieerd moeten worden wat het betekent voor een getal om construeerbaar te zijn. Vervolgens komen de volgende meetkundige problemen aan bod: de driedeling van een hoek, de verdubbeling van een kubus, de kwadratuur van een cirkel en de construeerbaarheid van regelmatige veelhoeken. Om te laten zien wat wel en niet mogelijk is wordt er gebruik gemaakt van moderne algebra, zo kan een constructie probleem omgeschreven worden naar een concreet algebraïsch probleem. Hiervoor maken we gebruik van de theorie rondom lichaamsuitbreidingen en de Galois theorie.

Inhoudsopgave

Lijst van figuren

1 Introductie

Wiskunde wordt al millennia lang beoefend, in de tijd van de grieken ging dit nog op simpele wijze, want de moderne technieken die wij nu hebben in bijvoorbeeld de algebra waren toen nog niet uitgevonden. Dit literatuuronderzoek gaat over de mogelijke constructies met passer en ongemarkeerde liniaal. Hierbij beginnen we rond 300 vC, rond deze tijd heeft Euclides van Alexandrië namelijk Στοιχεία geschreven, De Elementen, dit is de grondlegging van de meetkunde zoals wij die kennen. [8] Hoewel er meerdere soorten meetkunde zijn, waaronder elliptische en hyperbolische meetkunde waar niet het vijfde postulaat van Euclides, maar een ander postulaat aangenomen wordt, richten wij ons in dit onderzoek slechts op de euclidische meetkunde.

De wiskunde die in de afgelopen eeuwen is ontdekt helpt ons om vele problemen aan te pakken die men daarvoor niet op kon lossen. Zo zullen we in dit verslag ook gebruik maken van relatief nieuwe algebraïsche concepten. Met behulp van theorie over lichaamsuitbreidingen kunnen wij onder andere de drie (destijds onopgeloste) klassieke meetkundige problemen oplossen: De driedeling van een hoek, de verdubbeling van een kubus en de kwadratuur van een cirkel. Ook zullen we bespreken voor welke n de regelmatige n-hoek geconstrueerd kan worden met passer en ongemarkeerde liniaal, hierbij zullen we gebruik maken van de Galois theorie. Dit is door meerdere wiskundigen ontwikkeld naar aanleiding van bevindingen van Évariste Galois in de 19e eeuw die zijn werk niet af kon maken voor hij stierf in een duel. [9]

We zullen dit verslag beginnen met de vijf postulaten van Euclides waarmee de wiskunde is begonnen. Vervolgens komen hier een aantal toepassingen en wat veel voorkomende constructies aan bod. Hierna zal de moderne algebraïsche achtergrond geïntroduceerd worden waarmee de vroeger onoplosbare problemen opgelost kunnen worden. We zullen beginnen met een aantal definities en theorieën over polynomen waarna lichaamsuitbreidingen aan bod komen. Daarna komt er een stuk over de Galois theorie waar we uiteindelijk de fundamentele stelling van de Galois theorie zullen geven en we het kort over cyclotomische lichaamsuitbreidingen gaan hebben.
Vervolgens leggen we uit welke punten en constructies te construeren zijn, hiervoor zullen we eerst definiëren wat het betekent voor een getal om construeerbaar te zijn. Daarna hebben we alle benodigde hulpmiddelen om verscheidene meetkundige problemen te bekijken en op te lossen. Dit zijn de drie hiervoor genoemde klassieke meetkundige problemen die we vooral zullen oplossen met de theorie over lichaamsuitbreidingen en de graad van deze lichaamsuitbreidingen. Als laatste zullen we regelmatige veelhoeken gaan bekijken waar we naar de stelling van Gauss-Wantzel toe gaan werken die ons vertelt voor welke n een regelmatige n-hoek construeerbaar is. Hiervoor zullen we gebruik maken van onder andere de fundamentele stelling van de Galois theorie.

2 De axioma's van Euclides

In dit hoofdstuk worden de axioma's van Euclides beschreven, dit zijn de vijf postulaten uit het werk Στοιχεῖα (De Elementen) van Euclides [2] die de fundering vormen voor de Euclidische meetkunde. Voordat Euclides in zijn werk deze postulaten benoemt geeft hij 23 definities. Een aantal hiervan worden hier ook genoemd, zoals vertaald in De Elementen van Euclides door dr. E. J. Dijksterhuis, de overige definities kunnen ook in dit boek gevonden worden. [2]

I. Een punt is, wat geen deel heeft.

II. Een lijn is een breedtelooze lengte.

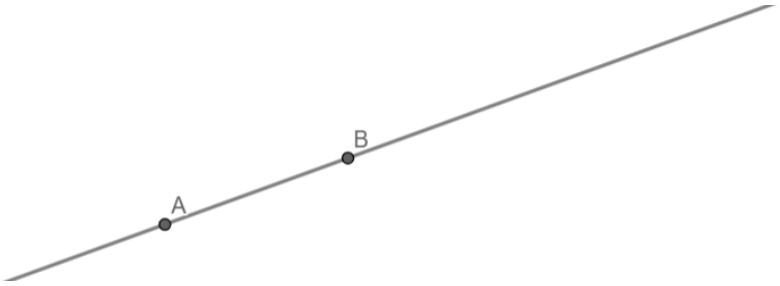
VIII. Een vlakke hoek is de helling tot elkaar van twee lijnen in een plat vlak, die elkaar ontmoeten en die niet op een rechte liggen.

X. Wanneer een rechte, op een rechte staande, de aan elkaar grenzende hoeken aan elkaar gelijk maakt, is elk der gelijke hoeken recht en de opstaande lijn heet de loodlijn op die, waarop ze staat.

XVIII. Een middellijn van den cirkel is een rechte lijn, getrokken door het middelpunt en naar beide zijden beëindigd door den omtrek van den cirkel, welke lijn ook den cirkel middendoor deelt.

2.1 De vijf postulaten

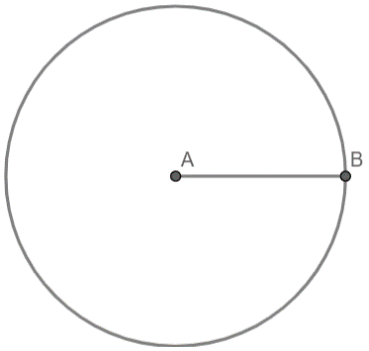
1. Laat geëischt worden, van elk punt naar elk [punt] een rechte lijn te trekken.
Dit postulaat zegt dat door twee punten altijd een rechte lijn gemaakt kan worden. Gegeven twee punten A en B, dan kunnen wij een lijn construeren die door allebei deze punten gaat. Hierbij ontstaat de lijn door punten A en B. Ook ontstaat het lijnstuk AB, het deel van de lijn van punt A tot punt B. De lengte van lijnstuk AB, die later wordt gedefinieerd, wordt aangeduid met $|AB|$.



Figuur 1: Het eerste postulaat van Euclides gevisualiseerd, een lijn door punten A en B.

2. En een beëindigde rechte samenhangend in rechte lijn te verlengen.
Elke rechte lijn kan eindeloos als rechte lijn uitgebreid worden. Een lijnstuk is dan ook altijd onderdeel van een oneindige lijn. Met het verlengde van een lijnstuk wordt een deel van de oneindige lijn, waar het lijnstuk onderdeel van is, bedoeld.

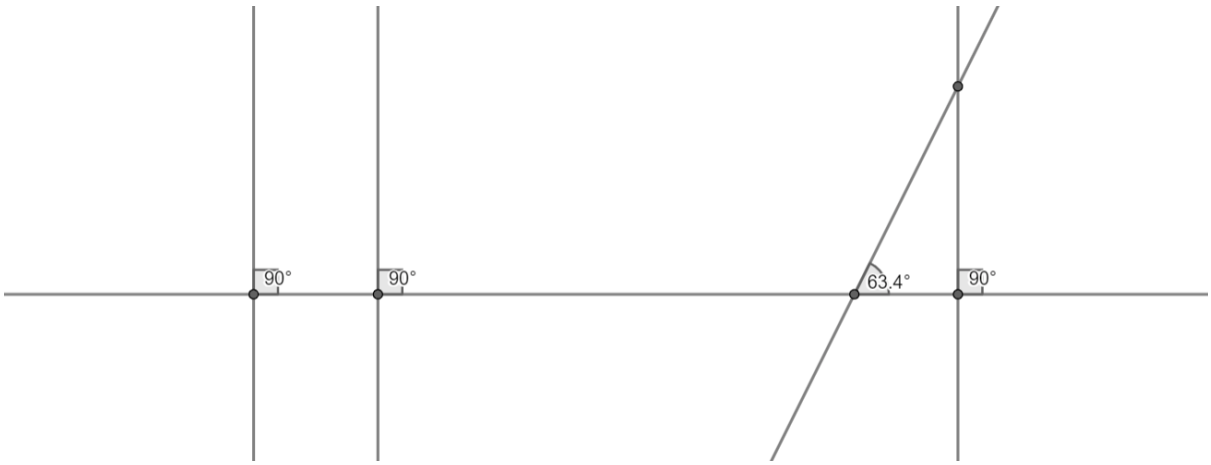
3. En dat met elk middelpunt en elken afstand een cirkel beschreven wordt.
Elk lijnstuk en elk punt kunnen de straal en middelpunt zijn van een cirkel. Dit houdt in dat, gegeven een lijnstuk AB en een punt C, wij een cirkel kunnen construeren met straal $|AB|$ en middelpunt C (hierbij kan C ook gelijk zijn aan punt A of B).



Figuur 2: Het derde postulaat van Euclides, een cirkel met middelpunt A en straal $|AB|$.

4. En dat alle rechte hoeken aan elkaar gelijk zijn.
Een rechte hoek, zie Definitie X, is een hoek van 90° of $\frac{\pi}{2}$ rad. Dit postulaat vertelt ons dat alle rechte hoeken gelijk zijn. In de meetkunde van Euclides zijn er twee dingen die we kunnen meten, afstand en de hoek. De afstand wordt gemeten aan de hand van een referentie lijnstuk dat de lengte 1 wordt gegeven. Als eenheid om hoeken te meten koos Euclides voor de rechte hoek (een hoek van 45° word dan een halve rechte hoek bijvoorbeeld), de rechte hoek wordt namelijk veel gebruikt in de Elementen. Bijvoorbeeld bij postulaat 5.

5. En dat, wanneer een rechte, die twee rechten treft, de binnenhoeken aan denzelfden kant kleiner dan twee rechte [hoeken] maakt, de twee rechten, tot in het oneindige verlengd, elkaar ontmoeten aan den kant, waar de hoeken zijn, die kleiner zijn dan twee rechte.
Dit postulaat wordt ook wel het parallellen postulaat genoemd, hij vertelt ons dat als twee lijnen een derde lijn zo snijden dat de som van de binnenhoeken aan een kant kleiner is dan twee rechte hoeken, dan moeten deze twee lijnen elkaar onvermijdelijk snijden als ze genoeg verlengd worden. Met de binnenhoeken worden de hoeken tussen de twee (in Figuur 3 verticale) lijnen in, aan dezelfde kant van de derde (in Figuur 3 horizontale) lijn bedoeld. Als de som van deze hoeken kleiner is dan de som van twee rechte hoeken (dus kleiner dan 180°), dan lopen de twee lijnen niet parallel aan elkaar en snijden ze elkaar dus als ze ver genoeg worden doorgetrokken.



Figuur 3: Het vijfde postulaat van Euclides gevisualiseerd, links twee parallelle lijnen, rechts twee lijnen die niet parallel lopen.

De eerste twee postulaten laten de werking van een ongemarkeerde liniaal zien. Om omslachtigheid tegen te gaan zal in dit verslag *met een liniaal altijd een ongemarkeerde liniaal bedoeld worden*. Het derde postulaat gaat over de werking van de passer. Het vierde postulaat vertelt ons dat alle rechte hoeken hetzelfde zijn en het laatste postulaat vertelt ons dat parallelle lijnen elkaar nooit snijden.
Buiten het gebruik van een rechte hoek als eenheid is het onduidelijk waarom Euclides het vierde postulaat precies heeft toegevoegd aan de Elementen. Een theorie is dat Euclides dit postulaat later toegevoegd zou hebben omdat hij het nodig zou vinden voor postulaat 5 [11], dit is echter onwaarschijnlijk. Postulaat 5 kan namelijk herschreven worden zodat de rechte hoek niet genoemd wordt: *"Als twee lijnen een derde lijn zo snijden dat de som van de binnenhoeken aan een kant kleiner is dan de som van de binnenhoeken aan de andere kant, dan moeten deze twee lijnen elkaar onvermijdelijk snijden als ze genoeg verlengd worden."*.

2.2 Het assenstelsel

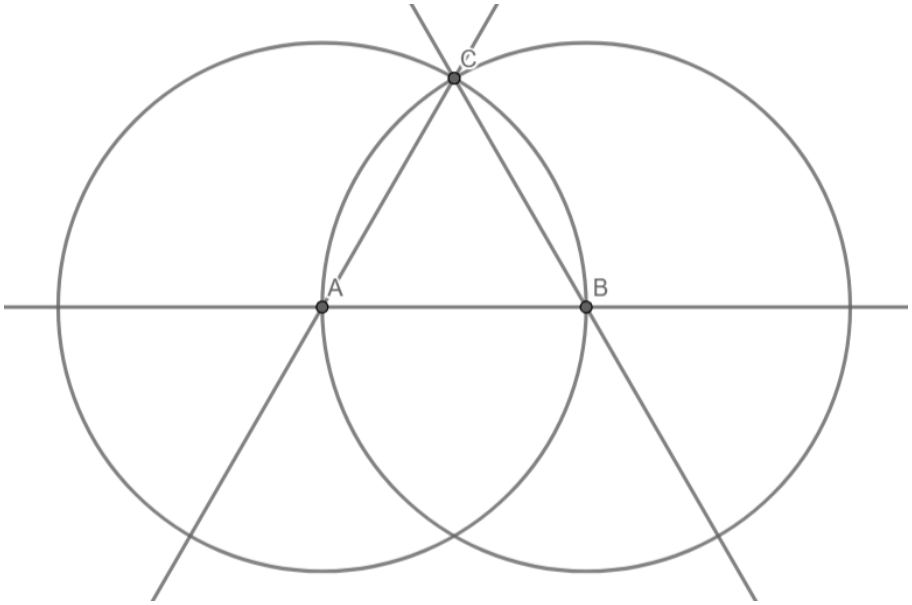
De vijf postulaten zijn de basis van de Euclidische wiskunde die we gaan gebruiken. Wij kunnen met behulp van deze postulaten namelijk een vlak $\mathbb{R}^2$ opzetten. Dit doen wij door een eerste punt O te plaatsen, dit noemen wij de oorsprong. Nu plaatsen wij een tweede punt A, niet op dezelfde plek als het eerste punt. We construeren de lijn door O en A en noemen dit de x-as, waarbij we de richting van O naar A de positieve richting noemen. De lengte van het ontstane lijnstuk OA noemen wij lengte 1, dus $|OA| = 1$.
Nu maken we een loodrechte lijn op de x-as door punt O (zie Hoofdstuk 3), dit noemen we de y-as. De positieve richting van de y-as nemen we zo dat als we de y-as een kwartslag (90° of $\frac{\pi}{2}$ rad) met de klok mee draaien deze dezelfde richting heeft als de x-as.
Nu hebben we een assenstelsel en een eenheid (de lengte van lijnstuk OA). Later zullen we zien dat we vanuit deze eenheid onder andere alle getallen uit $\mathbb{Q}$ en wortels van deze getallen kunnen construeren. De getallen die wij kunnen construeren noemen we de construeerbare getallen. Wij kunnen dan ook alle punten vinden waarvan zowel het x als het y coördinaat construeerbare getallen zijn.

3 Toepassingen van de postulaten

In dit hoofdstuk zullen de toepassingen van de postulaten van Euclides besproken worden. Ten eerste zal de werking van de passer en de liniaal bekeken worden. De werking van de liniaal is beschreven in postulaten 1 en 2, we kunnen een lijn construeren door twee bestaande punten en wij kunnen elke geconstrueerde lijn eindeloos verlengen. De werking van de passer is beschreven in postulaat 3; Gegeven een geconstrueerd punt en een lijnstuk, dan kan er een cirkel gemaakt worden met dit punt als middelpunt en de lengte van het lijnstuk als straal.
Net als bij het opzetten van het assenstelsel in Paragraaf 2.2 begin je altijd met een leeg vlak. Op dit lege vlak zet je je eerste twee punten op willekeurige verschillende plekken. Je kan nu een lijn tussen deze punten trekken waardoor er een lijnstuk ontstaat wat je de lengte 1 geeft. Hier vanuit is het mogelijk om nieuwe punten te creëren door nieuwe cirkels en lijnen te construeren. Een aantal nuttige constructies zullen hieronder besproken worden.

3.1 Constructies

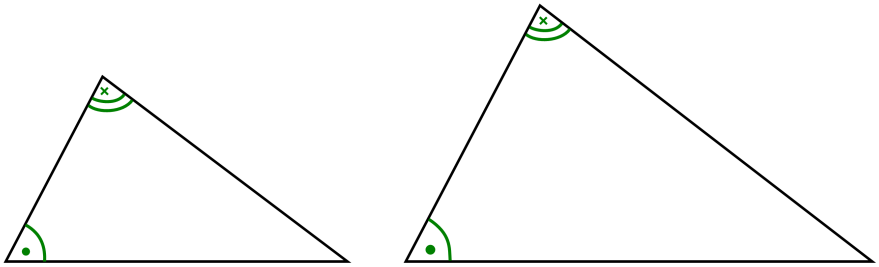
Gelijkzijdige driehoek: (Figuur 4) Een gelijkzijdige driehoek is een driehoek waarvan alle drie de zijden dezelfde lengte hebben, elke hoek van deze driehoek is 60°. Om een gelijkzijdige driehoek te maken begin je met een lijnstuk AB. Vervolgens construeer je de cirkel met middelpunt A en straal $|AB|$ en de cirkel met middelpunt B en straal $|AB|$. Een van de snijpunten van deze cirkels noem je punt C. Trek nu de lijnen door de punten A en C en door de punten B en C. Er geldt nu dat $|AB| = |BC| = |AC|$, dus is de driehoek ABC een gelijkzijdige driehoek met zijdes van lengte $|AB|$.



Figuur 4: De constructie van een gelijkzijdige driehoek.

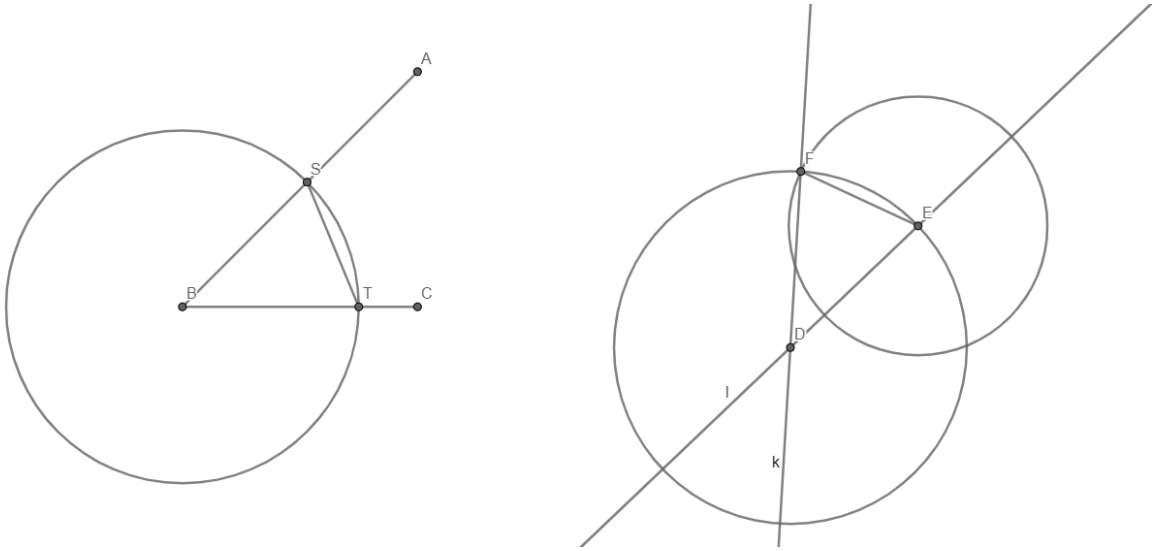
Gelijkvormige driehoeken: (Figuur 5) De gelijkvormigheid van driehoeken houdt in dat alle drie de hoeken hetzelfde zijn, dit komt goed van pas omdat de verhoudingen tussen de zijdes van een driehoek gelijk zijn voor elk van de gelijkvormige driehoeken. Om te laten zien dat een driehoek gelijkvormig is, is het voldoende om te laten zien dat twee hoeken van de driehoeken hetzelfde zijn. Volgens Propositie XXXII in de Elementen van Euclides is de som van de

binnenhoeken van een driehoek altijd 180°[2]. Als je dus twee hoeken weet kan de derde berekend worden door de som van de 2 bekende hoeken af te trekken van 180°.
Gelijkvormige driehoeken zijn gelijk als de zijdes even lang zijn. Er zijn meerdere manieren om te laten zien dat driehoeken gelijk zijn. Twee hiervan zijn Propositie IV en Propositie VIII van Euclides.
Propositie IV: Als twee driehoeken twee stel even lange zijden hebben en de hoek tussen deze zijden even groot zijn, dan zijn de zijden overstaande aan de gegeven hoek ook even lang.
Propositie VIII: Als twee driehoeken twee zijden van de ene even lang hebben als twee zijden van de ander en ook hun basissen even lang zijn, dan zijn de hoeken tussen beide lange zijden even groot.
Deze propositie zegt dat als een driehoek 3 gelijke zijden heeft, waarbij er twee de zijden worden genoemd en een de basis, dan is de hoek tussen de twee zijden even groot. Dit kan worden toegepast met elke zijde als basis en dus zijn dan alle drie de hoeken even groot. Als alle drie de hoeken even groot zijn en alle zijdes komen overeen, dan zijn twee driehoeken gelijk.



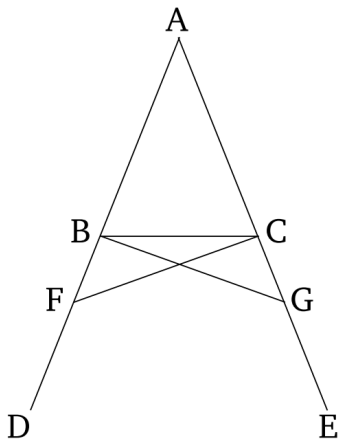
Figuur 5: Twee gelijkvormige driehoeken.
Bron: Uptuition.id [15]

Hoeken kopiëren: (Figuur 6) Een hoek kan gekopieerd worden met behulp van gelijkvormige driehoeken. Stel we hebben hoek ABC welke gekopieerd moet worden, dus we willen lijn k maken door punt D, die op lijn l ligt, zo dat de hoek tussen lijn l en k gelijk is aan de hoek ABC. Construeer dan een cirkel met middelpunt B en een willekeurige straal zodat de cirkel zowel lijnstuk AB als lijnstuk BC snijdt. Het snijpunt van de cirkel en lijnstuk AB noemen we S en het snijpunt van de cirkel en lijnstuk BC noemen we T, maak nu lijnstuk ST. Er ontstaat een driehoek BTS, merk op dat $|BS| = |BT|$. Construeer nu de cirkel met middelpunt D en straal BT. Noem, afhankelijk van de kant waar je de hoek wilt kopiëren, een van de snijpunten van deze cirkel met lijn l het punt E. Maak nu cirkel met middelpunt E en straal ST, deze snijdt de vorige cirkel in twee punten, afhankelijk van de kant waar je de hoek wilt kopiëren noem je een van deze snijpunten punt F. Maak nu lijn k door punten D en F. Merk op dat, omdat $|DE| = |DF| = |BS| = |BT|$ en $|EF| = |ST|$, volgens Propositie VIII de hoek FDE nu gelijk aan hoek SBT, maar deze hoek is hetzelfde als hoek ABC en dus maakt lijn k een hoek met lijn l die even groot is als hoek ABC.



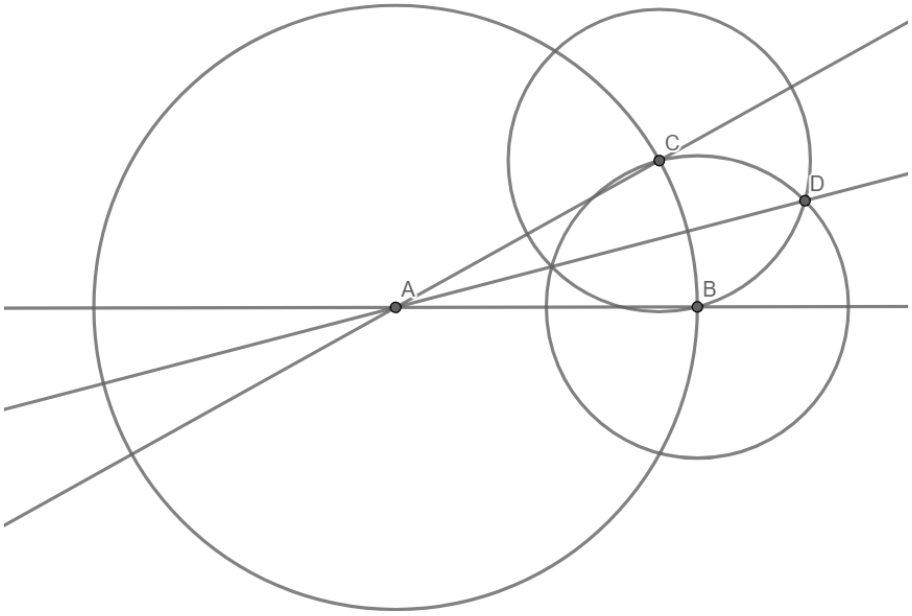
Figuur 6: Het kopiëren van hoek *ABC* naar punt *D*.

Gelijkbenige driehoek: (Figuur 7) Een gelijkbenige driehoek is een driehoek waarvan twee zijdes even lang zijn en de basis arbitraire lengte heeft. Een voorbeeld van een gelijkbenige driehoek is de gelijkzijdige driehoek. Volgens Propositie V van Euclides zijn de hoeken aanliggend aan de basis even groot.
Propositie V: In een gelijkbenige driehoek zijn de hoeken aanliggend aan de basis even groot.
Laat *ABC* een gelijkbenige driehoek zijn met zijdes *AB* en *AC* even lang en laat punten *D* en *E* in het verlengde van lijnstukken *AB* en *AC* liggen respectievelijk (aan de kant van punten *B* en *C*). Neem een willekeurig punt *F* op *BD* en construeer punt *G* op *CE* zo dat $|AF| = |AG|$ (doe dit door de cirkel met middelpunt *A* en straal $|AF|$ te construeren). Maak nu de lijnstukken *CF* en *BG*, nu ontstaan twee driehoeken FCA en BGA. Omdat $|AF| = |AG|$ en $|AB| = |AC|$ en omdat de hoek *FAC* hetzelfde is als hoek *BAG* geldt dat $|FC| = |BG|$ volgens Propositie IV. De andere hoeken van de driehoeken zijn ook gelijk door Propositie IV nog twee keer toe te passen, dus hoek ACF is even groot als hoek *ABG* en hoek AFC is even groot als hoek *AGB*. Omdat $|AB| = |AC|$ en $|AF| = |AG|$ geldt ook dat $|BF| = |CG|$. We wisten ook al dat $|FC| = |BG|$, dus zijn driehoeken FCB en GCB gelijk aan elkaar volgens Propositie VIII (ze bevatten beide ook zijde *BC*). Dus de hoeken FCB en BGC zijn even groot.
Omdat de hoeken *ABG* en ACF even groot zijn en in deze hoeken FCB en GBC even groot zijn, zijn de hoeken *ABC* en *ACB*, die het resterende deel van de hoeken *ABG* en ACF zijn, ook even groot.



Figuur 7: De gelijkbenige driehoek.
Bron: Euclid's Elements of Geometry [4]

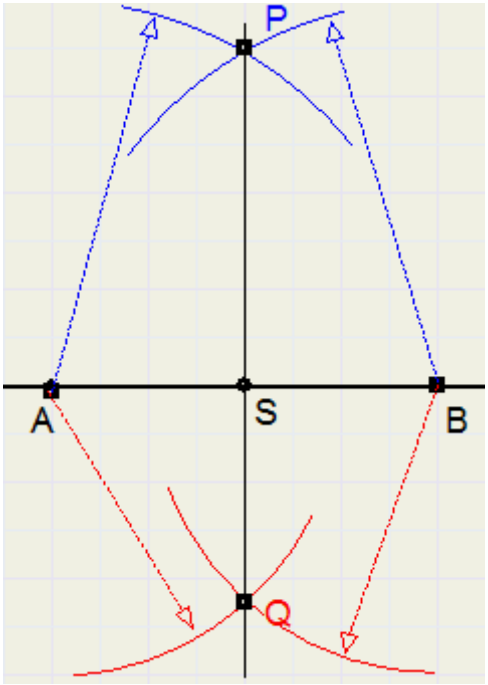
Bissectrice: (Figuur 8) De bissectrice van een hoek is de lijn die een hoek in twee gelijke hoeken deelt. Begin met twee lijnen die elkaar snijden in punt A. Maak nu een cirkel met middelpunt A en willekeurige straal, de snijpunten van de cirkel en de twee lijnen noemen we B en C, let op dat de gekozen snijpunten bepalen van welke hoek je de bissectrice gaat nemen, wij gaan de bissectrice van hoek BAC construeren. Maak hiervoor een cirkel met middelpunt B en straal $|BC|$ en een cirkel met middelpunt C en straal $|BC|$. Een van de snijpunten van deze cirkels noem je punt D. Maak nu de lijnstukken CD en BD. Er ontstaan nu twee driehoeken ABD en ADC. Omdat zijden AB en AD even lang zijn als zijden AC en AD en omdat de zijden (of basissen) BD en CD even lang zijn zegt Propositie VIII dat hoeken BAD en CAD gelijk zijn. Dus is de lijn door punten A en D de bissectrice van hoek BAC.



Figuur 8: De constructie van een bissectrice.

Middelloodlijn: (Figuur 9) Het maken van de middelloodlijn is relatief eenvoudig, maar een veel gebruikte constructie in de meetkunde. De middelloodlijn van lijnstuk AB is de lijn die

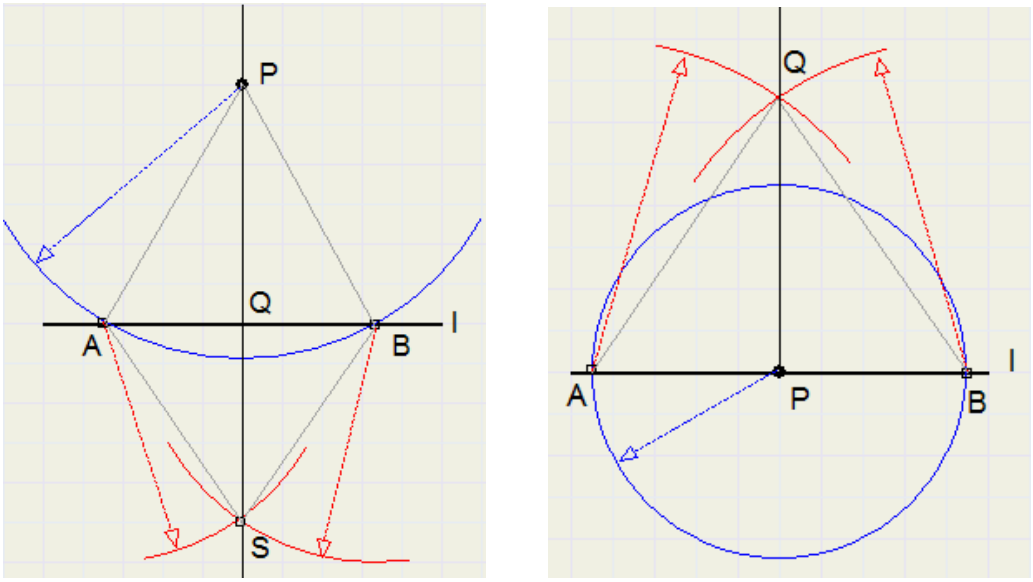
loodrecht op dit lijnstuk staat en precies door het midden van dit lijnstuk gaat. We beginnen met lijnstuk AB, vervolgens construeren we de cirkel met middelpunt A en straal $|AB|$ en de cirkel met middelpunt B en straal $|AB|$. De snijpunten van deze cirkels noemen we P en Q. Maak nu de lijn door punten P en Q. Het snijpunt van deze lijn met lijnstuk AB noemen we S. We kunnen nu de lijnstukken AP, BP, AQ en BQ maken. Dit geeft twee driehoek AQP en QBP. Merk op dat $|AP| = |BP|$, $|AQ| = |BQ|$ en dat PQ in beide driehoeken zit. Volgens Propositie VIII zijn dit gelijke driehoeken en zijn de hoeken APQ en BPQ gelijk aan elkaar. Als we nu kijken naar de driehoeken ASP en SBP weten we dat $|AP| = |BP|$ en zit SP in beide driehoeken. Ook zijn de hoeken APQ en BPQ gelijk aan elkaar, dus volgens Propositie IV geldt $|AS| = |SB|$ en dus zijn de driehoeken ASP en SBP gelijk aan elkaar volgens Propositie VIII. Omdat dit gelijke driehoeken zijn, zijn de hoeken ASP en PSB gelijk aan elkaar. Maar als een rechte lijn die op een rechte lijn staat de aan elkaar grenzende hoeken gelijk maakt, dan zijn beide hoeken rechte hoeken en staan de lijnen loodrecht op elkaar (Definitie X). Dus is de lijn door PQ de middelloodlijn van lijnstuk AB.



Figuur 9: De constructie van een middelloodlijn.
Bron: DavData.nl [3]

Loodlijn: (Figuur 10) Een loodlijn is een lijn die loodrecht op een andere lijn staat, de hoeken die ontstaan tussen de twee lijnen zijn dus rechte hoeken. Een loodlijn kan op twee manieren gemaakt worden: een loodlijn neerlaten vanaf een punt dat niet op de lijn ligt of een loodlijn oprichten door een punt op de lijn. Beide manieren worden hier beschreven.
Gegeven zijn lijn l en punt P. We gaan eerst uit van het geval waar punt P niet op lijn l ligt. Construeer een cirkel met middelpunt P en willekeurige straal groot genoeg zodat er twee snijpunten met lijn l ontstaan, noem deze snijpunten A en B. Maak nu de cirkel met middelpunt A en straal $|AP|$ en de cirkel met middelpunt B en straal $|BP|$. Deze cirkels snijden elkaar in punt P en in een nieuw punt dat we S noemen. Trek nu de lijn door punten P en S, deze lijn gaat door P en is de middelloodlijn van lijnstuk AB (zie bovenstaand, de middelloodlijn). Er ontstaan nu 2 driehoeken, AQP en QBP, omdat $|AP| = |BP|$ (A en B liggen op dezelfde cirkel), omdat $|PQ|$ in beide driehoeken zit en omdat $|AQ| = |BQ|$ (middelloodlijn), zijn de

driehoeken gelijk en zijn de hoeken AQP en PQB gelijk aan elkaar (volgens Propositie VIII, zie gelijkvormige driehoeken). Maar als een rechte lijn die op een rechte lijn staat de aan elkaar grenzende hoeken gelijk maakt, dan zijn beide hoeken rechte hoeken en staan de lijnen loodrecht op elkaar (Definitie X). (Figuur 10a)
Als punt P op lijn l ligt, dan maak je een cirkel met middelpunt P en willekeurige straal. Noem de snijpunten van de cirkel met de lijn punten A en B. Construeer dan de middelloodlijn van lijnstuk AB. (Figuur 10b)



(a) Loodlijn neerlaten van punt P op lijn l.

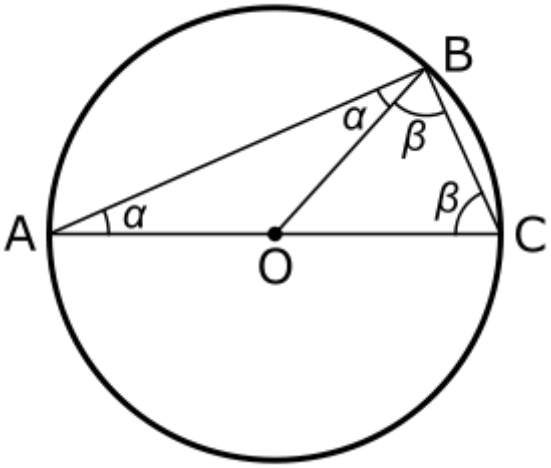
(b) Loodlijn oprichten vanuit punt P op lijn l.

Figuur 10: Twee manieren om loodlijnen te construeren.
Bron: DavData.nl [3]

Parallelle lijnen: Gegeven een lijn l en een punt P niet op lijn l, we willen een lijn construeren door punt P die parallel loopt aan lijn l. Laat de loodlijn neer van punt P op lijn l en noem deze lijn k. Richt nu de loodlijn op vanuit punt P op lijn k en noem deze lijn m. Postulaat 5 kan nu rechtstreeks worden toegepast waar de parallelle lijnen de lijnen l en m zijn en waar k de derde lijn is die gesneden wordt. De lijnen l en k en de lijnen k en m snijden elkaar loodrecht, dus alle aanliggende hoeken zijn gelijk en zijn rechte hoeken. Dus is de som van de binnenhoeken gelijk aan twee rechte hoeken en ontmoeten de lijnen l en m elkaar niet als ze in het oneindige verlengt worden. Dus is lijn m parallel aan lijn l.

Stelling van Thales: (Figuur 11) De stelling van Thales gaat over de hoeken van een koorden driehoek, dit is een driehoek waarbij een van de zijdes de middellijn van een cirkel is en de derde hoekpunt ook op de cirkel ligt. Deze driehoek is gemakkelijk te construeren, begin met een lijn en een punt O op deze lijn. Maak een cirkel met willekeurige straal en middelpunt O, deze snijdt de lijn op punten A en C. Neem een willekeurig punt B op de cirkel dat niet samenvalt met punten A of C en teken de lijnen AB en BC. Nu is driehoek ABC een koorden driehoek. De stelling van Thales vertelt ons nu dat hoek ABC een rechte hoek is. Dit kunnen we zien door de lijn door de punten O en B te construeren. Omdat O het middelpunt is van de cirkel geldt $|OA| = |OB| = |OC|$, OBA is daarom een gelijkbenige driehoek en hoeken OBA en OAB zijn dus gelijk aan elkaar en noemen we α (zie Propositie V, gelijkbenige driehoeken). Ook is OCB een gelijkbenige driehoek en zijn hoeken OCB en CBO dus gelijk aan elkaar en noemen

we β. Voor de driehoek *ACB* geldt dat alle hoeken bij elkaar opgeteld 180° zijn (Propositie XXXII uit de Elementen van Euclides) [2]. Hieruit volgt dat $\alpha + (\alpha + \beta) + \beta = 180^\circ$, dit kan versimpeld worden tot $\alpha + \beta = 90^\circ$ en dus is hoek *ABC* een rechte hoek. Er zijn meerdere bewijzen voor de stelling van Thales, zo is er een ander bewijs te vinden in de Elementen van Euclides. [2]



Figuur 11: De stelling van Thales.
Bron: Wikipedia.nl [5]

4 Algebraïsche achtergrond

In dit hoofdstuk worden een aantal definities en lemma's uitgelegd die nodig zullen zijn bij latere bewijzen. Om te beginnen zijn er een aantal begrippen die uitgelegd moeten worden.

4.1 Algebraïsche getallen en polynomen

Gegeven zijn lichamen K en L zo dat $K \subseteq L$.
Algebraïsche getallen: Met een algebraïsch getal bedoelen we een getal $\alpha \in L$ dat een nulpunt is van een polynoom $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ met $a_i \in K, (a_n \neq 0)$.
Irreducibele polynomen: Een irreducibel polynoom over een lichaam K is een polynoom (met coëfficiënten in lichaam K) dat niet gefactoriseerd kan worden in twee of meer polynomen over lichaam K van lagere graad. Merk op dat bij een irreducibel polynoom $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ geldt dat a_0 niet 0 kan zijn, anders kan het polynoom namelijk gefactoriseerd worden in x en $a_1 + a_2x + \ldots + a_nx^{n-1}$.
Monische polynomen: Een monisch polynoom over K is een polynoom waarbij de coëfficiënt van de term met de hoogste macht 1 is. Een monisch polynoom neemt dus de vorm $a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + x^n$ aan met $a_i \in K$.
Minimaalpolynomen: De minimaalpolynoom in K van een algebraïsch getal $\alpha \in L$ is een irreducibel monisch polynoom in lichaam K dat α als nulpunt heeft. De graad (degree) van α, genoteerd als $\deg(\alpha)$, is de graad van de minimaal polynoom van α. Deze polynoom bestaat voor elk algebraïsch getal.

Nu volgt er een stelling die we vaker nodig gaan hebben, de rationale wortelstelling. Deze stelling zegt iets over het bestaan van rationale wortels van polynomen.

Stelling 4.1 (*Rationale wortelstelling*)**.** [6] *Als de vergelijking*

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, (a_n \neq 0)$$

met gehele coëfficiënten een rationale oplossing heeft, dan kan deze geschreven worden als $\frac{p}{q}$*, waar p en q gehele getallen en relatief priem zijn zó dat p een factor is van* a_0 *en q een factor is van* a_n*.*

Bewijs. Laat $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ met $a_0, \ldots, a_n \in \mathbb{Z}$. Stel $P(\frac{p}{q}) = 0$ voor $p,q \in \mathbb{Z}$ relatief priem, dan:

$$P(\frac{p}{q}) = a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_1(\frac{p}{q}) + a_0 = 0.$$

Beide kanten vermenigvuldigen met q^n geeft:

$$a_np^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0. \tag{4.1}$$

De term met a_0 naar de andere kant verplaatsen en de p uit de resterende termen halen geeft:

$$p(a_np^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1q^{n-1}) = -a_0q^n.$$

Dus p deelt a_0q^n en omdat p en q relatief priem zijn deelt p de term a_0. Andersom kunnen we bij Vergelijking 4.1 ook de a_n term naar de andere kant verplaatsen en de q uit de resterende termen halen:

$$q(a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \cdots + a_0q^{n-1}) = -a_np^n.$$

Dus q deelt a_np^n en omdat q en p relatief priem zijn deelt q de term a_n □

4.2 Lichaamsuitbreidingen

In dit deel gaan we kijken naar lichamen en lichaamsuitbreidingen. Ook zullen we van de lichaamsuitbreidingen een aantal belangrijke eigenschappen bespreken.

Definitie 4.2. *Als L een lichaam is en $K \subseteq L$, dan is K een deellichaam van L als K een lichaam is waarbij de operaties van L zijn geërfd. L wordt dan ook wel een uitbreidingslichaam van K genoemd.*

Definitie 4.3. *Een lichaam $K \subseteq L$ kan met een set $S \subseteq L$ uitgebreid worden tot een lichaam, het uitbreidingslichaam wordt genoteerd als $K(S)$ en noemen we een lichaamsuitbreiding van K met S. Dit is de intersectie van alle deellichamen in L die zowel K als S bevatten, $K(S)$ is dus het kleinste deellichaam van L dat K en S bevat. De lichaamsuitbreiding wordt genoteerd als $K(S) : K$.*
Een lichaamsuitbreiding wordt algebraïsch genoemd als alle elementen S algebraïsch zijn over K.

Lemma 4.4. [12](6.1) *Een lichaamsuitbreiding L van een lichaam K is een vectorruimte over K. Hier zijn de vectoren de elementen uit L en de scalairen zijn de elementen uit K. De operaties*

$$(\lambda, u) \to \lambda u \quad (\lambda \in K, u \in L)$$
$$(u, v) \to u + v \quad (u, v \in L)$$

definiëren hierbij de structuur van de vectorruimte over L.

Bewijs. De set L is een vectorruimte op K als de twee beschreven operaties aan de volgende zeven axioma's voldoen:
1. $u+v = v+u$ voor alle u,$v \in L$.
2. $(u+v)+w = v+(u+w)$ voor alle u,v,$w \in L$.
3. Er bestaat een $0 \in L$ zo dat $0+u = u$ voor alle $u \in L$.
4. Voor elke $u \in L$ bestaat er een $-u \in L$ zo dat $u+(-u) = 0$.
5. Als $\lambda \in K$, u,$v \in L$, dan geldt $\lambda(u+v) = \lambda u + \lambda v$.
6. Als 1 de multiplicatieve identiteit van K is, dan geldt $1u = u$ voor alle $u \in L$.
7. Als $\lambda, \mu \in K$, dan geldt $\lambda(\mu u) = (\lambda\mu)u$ voor alle $u \in L$.
Elk van deze axioma's geldt voor deze twee operaties , omdat K een deellichaam is van L. □

Een belangrijke eigenschap van een lichaamsuitbreiding $L : K$ is de graad van de lichaamsuitbreiding.

Definitie 4.5. *De graad van een lichaamsuitbreiding L van een lichaam K, genoteerd als $[L : K]$, is de dimensie van L als vectorruimte over K.*

Het volgende lemma laat ons de graad van een lichaamsuitbreiding berekenen als we de graad weten van een aantal kleinere lichaamsuitbreidingen.

Lemma 4.6. [12](6.4) *Laat $K \subseteq L \subseteq M$ lichamen zijn en laat $M : L$ en $L : K$ eindig dimensionale lichaamsuitbreidingen zijn. Dan is $M : K$ een eindige lichaamsuitbreiding en geldt $[M : K] = [M : L][L : K]$.*

Bewijs. Laat $(x_i)_{i\in I}$ een basis zijn voor L als vectorruimte over K en laat $(y_j)_{j\in J}$ een basis voor M over L zijn. Voor alle $i \in I$ en $j \in J$ hebben we dat $x_i \in L$ en $y_j \in M$. We zullen nu laten zien dat $(x_i y_j)_{i\in I, j\in J}$ een basis is voor M over K (hier is $x_i y_j$ het product in het lichaam M). Aangezien de dimensies gelijk zijn aan het aantal elementen in de basis volgt de theorie.

Eerst laten we de lineaire onafhankelijk zien. Stel een eindige lineaire combinatie van de basis elementen is 0:

$$\sum_{i,j} k_{ij} x_i y_j = 0 \qquad (k_i j \in K)$$

Dit kunnen we opschrijven als:

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0$$

Omdat de coëfficiënten $\sum_i k_{ij} x_i = 0$ in L liggen en de y_j lineair onafhankelijk zijn over L, krijgen we

$$\sum_i k_{ij} x_i = 0$$

Nogmaals, omdat de coëfficiënten k_{ij} in K liggen en de x_i onafhankelijk zijn over K krijgen we dat $k_{ij} = 0$ voor alle $i \in I, j \in J$. Dus de elementen $x_i y_j$ zijn lineair onafhankelijk over K.

Nu laten we zien dat de $x_i y_j$ heel M over K uitzetten. Elk element $m \in M$ kan geschreven worden als

$$m = \sum_j \lambda_j y_j$$

Voor een zekere $\lambda_j \in L$, omdat de y_j M uitzetten over L. Ook kan voor elke $j \in J$ λ_j geschreven worden als

$$\lambda_j = \sum_i \lambda_{ij} x_i$$

Bij elkaar krijgen we dan

$$m = \sum_{i,j} \lambda_{ij} x_i y_j$$

En dus is het aantal elementen in de basis van $M : K$ gelijk aan het aantal elementen in de basis van $M : L$ maal het aantal elementen in de basis van $L : K$. □

In dit verslag hebben we voornamelijk te maken met het lichaam $\mathbb{Q}$ en lichaamsuitbreidingen van $\mathbb{Q}$ in $\mathbb{R}$. Hierbij zullen we meestal gebruik maken van lichaamsuitbreidingen met een enkel getal. Definitie 4.3 geldt nog steeds, maar voor een enkel getal maken we vaak gebruik van een andere notatie. Bijvoorbeeld, de uitbreiding van $\mathbb{Q}$ met getal α noteren we als $\mathbb{Q}(\alpha)$, dit is het kleinste deellichaam van $\mathbb{R}$ dat zowel $\mathbb{Q}$ als α bevat. De graad wordt genoteerd als $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Lemma 4.7. [12](5.14) *Laat K een deellichaam van lichaam L zijn en laat $\alpha \in L$ algebraïsch over K zijn met graad n (het minimaalpolynoom van α in K is van graad n). Dan is $K(\alpha) : K$ een lichaamsuitbreiding waarvoor geldt dat $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ een basis is voor de vectorruimte $K(\alpha)$ over K. Merk op dat voor de graad van de lichaamsuitbreiding geldt $[K(\alpha) : K] = n$.*

Bewijs. Het bewijs van dit lemma is te vinden in het boek Galois Theory van Ian Stewart [12]. □

Als we bovenstaand lemma toepassen op $\mathbb{Q} \subset \mathbb{R}$ en $\alpha \in \mathbb{R}$ algebraïsch over $\mathbb{Q}$, dan nemen de elementen in de lichaamsuitbreiding $\mathbb{Q}(\alpha)$ de vorm $\sum_{i=0}^{n-1} c_i \alpha^i$ met $c_i \in \mathbb{Q}$ aan.

Voorbeeld: We willen het lichaam $\mathbb{Q}$ uitbreiden met $\sqrt[3]{2}$. Dan is het minimaalpolynoom van $\sqrt[3]{2}$ over $\mathbb{Q}$ de polynoom $x^3 - 2$, deze polynoom heeft graad 3, dus $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. De lichaamsuitbreiding noteren wij als $\mathbb{Q}(\sqrt[3]{2})$ en de elementen zijn van de vorm $\sum_{i=0}^{2} c_i (\sqrt[3]{2})^i = c_0 + c_1 2^{\frac{1}{3}} + c_2 2^{\frac{2}{3}}$ waarbij $c_0, c_1, c_2 \in \mathbb{Q}$.

Een lichaam kan ook met meerdere getallen uitgebreid worden. Het volgende lemma laat zien dan de volgorde waarin je een lichaam uitbreid met meerdere getallen niet uit maakt.

Lemma 4.8. *Voor lichaam $\mathbb{Q}$ en $\alpha, \beta \in \mathbb{R}$ geldt dat $\mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\beta)(\alpha)$. Dit noteren we als $\mathbb{Q}(\alpha, \beta)$.*

Bewijs. Eerst gaan we laten zien dat $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha)(\beta)$ en $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\beta)(\alpha)$. Vervolgens laten we zien dat $\mathbb{Q}(\alpha)(\beta) \subseteq \mathbb{Q}(\alpha, \beta)$ en $\mathbb{Q}(\beta)(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$ om dan tot de conclusie te komen dat al deze lichamen gelijk zijn aan elkaar.

$\mathbb{Q}(\alpha)(\beta)$ is een lichaam dat zowel $\mathbb{Q}$, α als β bevat, dus $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha)(\beta)$. Op dezelfde manier is $\mathbb{Q}(\beta)(\alpha)$ een lichaam dat zowel $\mathbb{Q}$, β als α bevat, dus ook $\mathbb{Q}(\beta, \alpha) \subseteq \mathbb{Q}(\alpha)(\beta)$.

Het lichaam $\mathbb{Q}(\alpha, \beta)$ bevat $\mathbb{Q}$ en α, dus $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$. $\mathbb{Q}(\alpha, \beta)$ bevat dus zowel $\mathbb{Q}(\alpha)$ als β, dus $\mathbb{Q}(\alpha)(\beta) \subseteq \mathbb{Q}(\alpha, \beta)$. Op dezelfde manier kunnen we beredeneren dat $\mathbb{Q}(\alpha, \beta)$ zowel $\mathbb{Q}$ als β bevat, dus $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha, \beta)$. Beide $\mathbb{Q}(\beta)$ en α zitten in het lichaam $\mathbb{Q}(\alpha, \beta)$, dus $\mathbb{Q}(\beta)(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$ en daarmee hebben we laten zien dat $\mathbb{Q}(\alpha)(\beta) = \mathbb{Q}(\beta)(\alpha) = \mathbb{Q}(\alpha,\beta)$. □

4.3 Galois theorie

Ook zijn er nog een paar definities en stellingen met betrekking tot de Galois theorie die besproken moeten worden. De Galois theorie is nodig in het bewijs van de Stelling van Gauss-Wantzel in Hoofdstuk 7.

Om te beginnen zijn er een paar definities over splijtlichamen en de bijbehorende lichaamsuitbreidingen

Definitie 4.9. *Als K een deellichaam van $\mathbb{C}$ is en f een polynoom is over K, $f \neq 0$, dan splijt f over K als het uitgedrukt kan worden als een product van lineaire factoren*

$$f(x) = k(x - \alpha_1) \cdots (x - \alpha_n)$$

waar $k, \alpha_1, \ldots, \alpha_n \in K$.

Definitie 4.10. *Een deellichaam L van $\mathbb{C}$ is een splijtlichaam voor de polynoom $f \neq 0$ over het deellichaam K van $\mathbb{C}$ als $K \subseteq L$ en*
(1) f splijt over L.
(2) $L = K(\sigma_1, \ldots, \sigma_n)$, waar $\sigma_1, \ldots, \sigma_n$ de nulpunten van f in K zijn.

Definitie 4.11. *Een algebraïsche lichaamsuitbreiding $L : K$ is normaal als elk irreducibele polynoom f over K met minimaal een nulpunt in L het lichaam L splijt.*

Lemma 4.12. [12](9.9) *Een lichaamsuitbreiding $L:K$ is normaal en eindig als en slechts als L een splijtlichaam is voor een polynoom over K.*

Bewijs. Zie Galois theorie [12]. □

Definitie 4.13. *Laat $L:K$ een lichaamsuitbreiding zijn zo dat K een deellichaam is van het deellichaam L van $\mathbb{C}$. Een K-automorfisme van L is een automorfisme α van L zo dat*

$$\alpha(k) = k \text{ voor alle } k \in K$$

We zeggen dat $k \in K$ gefixeerd wordt door α als bovenstaande definitie geldt.

Definitie 4.14. *De Galois Groep $Gal(L:K)$ van een lichaamsuitbreiding $L:K$ is de groep van alle K-automorfismes van L onder de operatie van de compositie van functies.*

Nu volgt een deel over quotiëntgroepen, deze komen terug in de volgende stelling en in het bewijs van de Stelling van Gauss-Wantzel.

Definitie 4.15. *Voor een groep G en normale subgroep H van G is de quotiëntgroep van H in G, geschreven als (G/H), lees "G modulo H", de verzameling van nevenklasses van H in G. Dat is de verzameling*

$$\{g * H : g \in G\}$$

Waar $*$ de groepsoperatie van groep G is. Omdat H normaal is volgt dat $(g_1 * H)(g_2 * H) = (g_1 g_2) * H$ en dat definieert een groepsoperatie op deze verzameling.

Lemma 4.16. *Als G abels is, dan is de quotiëntgroep (G/H) ook abels.*

Bewijs. Laat H een ondergroep van G zijn, dan $gH = \{gh|h \in H\} = \{hg|h \in H\} = Hg$ voor alle $g \in G$ omdat G abels is, dus is H normaal. $G/H = \{g * H : g \in G\}$. Laat g_1H,$g_2H \in G/H$, dan $(g_1H)(g_2H) = g_1g_2H = g_2g_1H = (g_2H)(g_1H)$, omdat G abels is. Dus is G/H ook abels. □

Definitie 4.17. *Laat F een lichaam zijn en laat G een ondergroep zijn van de F-automorfisme groep. Dan is het gefixeerde lichaam van G de verzameling*

$$Fix(G) = \{f \in F : \forall \sigma \in G : \sigma(f) = f\}$$

Nu gaan we de fundamentele stelling van de Galois theorie nog benoemen. We zullen deze stelling niet bewijzen, het bewijs is te vinden in het boek Galois Theory van Ian Stewart. [12]

Laat $\mathscr{F}$ de verzameling met tussenlichamen zijn (dat is, tussenlichamen M zo dat $K \subseteq M \subseteq L$) en laat $\mathscr{G}$ de verzameling van alle ondergroepen H van G zijn, dus $H \subseteq G$ en H is een groep met groepsbewerking van G. We definiëren twee afbeeldingen als volgt

$$* : \mathscr{F} \to \mathscr{G}$$

$$^\dagger : \mathscr{G} \to \mathscr{F}$$

waar als $M \in \mathscr{F}$, dan is $M*$ de groep met alle M-automorfismes van L. Als $H \in \mathscr{G}$, dan is $H^\dagger$ het gefixeerde lichaam van H.

Stelling 4.18 (Fundamentele stelling van de Galois theorie)**.** [12](12.2) *Als $L:K$ een eindige normale lichaamsuitbreiding is in $\mathbb{C}$ met Galois groep G en als $\mathscr{F},\mathscr{G},*,^{\dagger}$ gedefinieerd zijn als hierboven, dan:*
1. De Galois groep G heeft orde $[L:K]$, dus $|G|=[L:K]$.
2. De afbeeldingen $*$ en † zijn elkaars inverse en zetten een een-op-een correspondentie op tussen $\mathscr{F}$ en $\mathscr{G}$.
3. Als M een tussenlichaam is, dan

$$[L:M]=|M*|, \qquad [M:K]=|G|/|M*|$$

4. Een tussenlichaam M is een normale lichaamsuitbreiding van K als en slechts als $M*$ een normale subgroep van G is.
5. Als een tussenlichaam M een normale uitbreiding van K is, dan is de Galois groep van $M:K$ isomorf met de quotiëntgroep $(G/M)*$.

Als laatste moeten we cyclotomische lichaamsuitbreidingen en hun verbanden met Galois groepen benoemen. Hiervoor hebben we eerst nog twee definities nodig.

Definitie 4.19 (Phi functie van Euler)**.** [14] *De phi functie $\phi(n)$ van een positief geheel getal n geeft het aantal positieve gehele getallen $m<n$ waarvoor geldt dat m en n relatief priem zijn, dus* $\gcd(m,n)=1$.

Bijvoorbeeld $\phi(8)=4$, namelijk de getallen 1, 3, 5 en 7.

Definitie 4.20. *Een n-de eenheidswortel is een complex getal $\zeta_n^k=e^{\frac{2k\pi i}{n}}$ dat een van de oplossingen is voor de vergelijking $x^n-1=0$. Een eenheidswortel wordt primitief genoemd als n en k relatief priem zijn, een primitieve eenheidswortel wordt soms genoteerd als ζ_n.*

Definitie 4.21. *Een n-cyclotomische lichaamsuitbreiding is een lichaamsuitbreiding $K(\zeta_n):K$ waar ζ_n een n-de eenheidswortel is.*

Stelling 4.22. [12](21.9)
Laat ζ_n een n-de eenheidswortel zijn, dan
(1) De Galois groep $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$ bestaat uit de $\mathbb{Q}$-automorfismes Ψ_j die zijn gedefinieerd als

$$\Psi_j(\zeta_n)=\zeta_n^j$$

waar $0\leq j\leq n-1$ en j is relatief priem met n.
(2) $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$ is isomorf met $(\mathbb{Z}/n\mathbb{Z})^*$ en is een abelse groep.
(3) De graad van de Galois groep $Gal(\mathbb{Q}(\zeta_n):\mathbb{Q})$ is gelijk aan $\phi(n)$.

Bewijs. (1) Laat $\gamma\in\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})$, dan is $\gamma(\zeta)$ een nulpunt van x^n-1, dus $\gamma=\Psi_j$ voor een zekere j.
Als j en n een gemeenschappelijke factor hebben, zeg $d>1$, dan is Ψ_j niet surjectief waardoor het geen $\mathbb{Q}$-automorfisme is.
Als j en n wel relatief priem zijn, dan bestaan er gehele getallen a en b zo dat $aj+bn=1$, dan $(\zeta_n^n=1)$

$$\zeta_n=\zeta_n^{aj+bn}=\zeta_n^{aj}\zeta_n^{bn}=(\zeta_n^j)^a$$

dus ligt ζ_n in de afbeelding van Ψ_j, dus is Φ_j een $\mathbb{Q}$-automorfisme.
(2) $\Psi_j\Psi_k=\Psi_{jk}$, dus is de functie $\Psi_j\to j$ is een isomorfisme van $\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})$ naar $\mathbb{Z}_n^*$. Ook weten we dat $\mathbb{Z}_n^*$ abels is, dus is $\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})$ ook abels door het isomorfisme.
(3) $|\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})|=|\mathbb{Z}_n^*|=\phi(n)$ □

Lemma 4.23. [12](20.3) *Laat G een Galois groep zijn. Als G abels is en* $|G| = 2^k$ *voor gehele positieve m, dan is er een reeks normale groepen*

$$G = G_k \geq \ldots \geq G_1 \geq G_0 = \{1\}$$

Waarbij $|G_i| = 2^i$ *voor* $0 \leq i \leq k$.

Bewijs. Zie Galois Theory [12]. □

5 Construeerbaarheid

In dit hoofdstuk gaan we bespreken wat construeerbaarheid precies inhoudt en zien we een stelling die later goed van pas zal komen. We beginnen met een lijnstuk waarvan we de lengte gelijk stellen aan 1. Om nu te laten zien welke getallen construeerbaar zijn is het nuttig om te bekijken welke operaties we kunnen uitvoeren met passer en liniaal. Het blijkt later dat we kunnen optellen, aftrekken, vermenigvuldigen, delen en worteltrekken, elk van deze operaties staat in dit hoofdstuk beschreven. Ook laten we zien dat dit ook de enige getallen zijn die we kunnen maken met passer en liniaal. De volgende definitie zullen we dit hoofdstuk toelichten.

Definitie 5.1. *Een reëel getal x is construeerbaar als en slechts als het het mogelijk is om in een eindig aantal stappen, met passer en ongemarkeerde liniaal, een lijnstuk te maken met lengte* $|x|$.

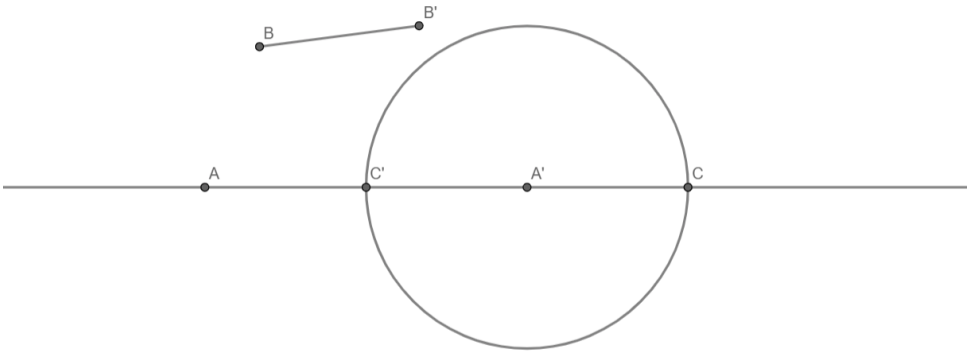
We gaan de gelijkheid van twee verzamelingen aantonen. De eerste verzameling is de verzameling van alle getallen die we kunnen construeren met passer en liniaal, deze noemen we de C. De tweede verzameling noemen we V en bevat alle getallen die gemaakt kunnen worden vanuit het getal 1 en de operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken. We gaan gelijkheid van deze twee sets bewijzen door te laten zien dat het deelverzamelingen van elkaar zijn. Om dit te doen laten we zien dat elk element van V in C zit, dus dat elk getal in V te construeren is.

5.1 Operaties met passer en ongemarkeerde liniaal

In deze subsectie staan alle wiskundige operaties beschreven die te construeren zijn met passer en liniaal. We beginnen met optellen en aftrekken, hiermee bedoelen we de operaties $(+)$ en $(-)$ respectievelijk zoals we deze ook kennen over de reële getallen. Vervolgens laten we vermenigvuldigen en delen zien, hiermee bedoelen we de operaties $(\cdot)$ en $(\div)$ zoals bekend over $\mathbb{R}$. Als laatste zullen we zien dat ook worteltrekken, de operatie $(\sqrt{})$ zoals bekend over $\mathbb{R}$, mogelijk is met passer en liniaal.

Optellen en aftrekken: Als a en b construeerbaar zijn, dan zijn $a+b$ en $a-b$ ook construeerbaar.

Bewijs. Stel we willen de construeerbare getallen a en b bij elkaar optellen. Neem de punten A en A' en de punten B en B' zo dat $|AA'| = a$ en $|BB'| = b$. Teken de lijn door punten A en A' en construeer de cirkel met midden A' en straal b. Deze cirkel snijdt de lijn door A en A' op twee plaatsen C en C'. Laat C aan de andere kant van A' zitten dan A, dan $|AC| = a+b$ en $|AC'| = a-b$. □



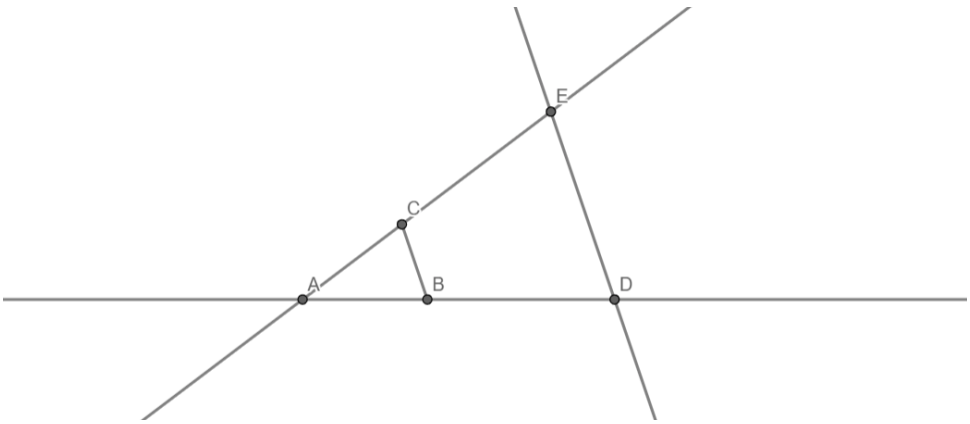
Figuur 12: Het optellen en aftrekken met passer en liniaal.

Vermenigvuldigen: Als a en b construeerbaar zijn, dan is $a \cdot b$ ook construeerbaar.

Bewijs. Neem de lijn door punten A en B waarbij $|AB| = 1$ en B rechts op de lijn ligt van A. Neem ook de lijn door punten A en C met $|AC| = a$, waarbij punt C niet op de lijn door AB ligt. Maak nu lijnstuk BC om de driehoek ABC te verkrijgen. Kies nu op de lijn door AB een punt D rechts van A zo dat $|AD| = b$. Construeer door punt D nu de lijn parallel aan lijnstuk BC. Het snijpunt van deze nieuwe lijn en de lijn door AC noemen we punt E. Omdat $\angle ABC$ dezelfde hoek heeft als $\angle ADE$ en $\angle BAC$ gelijk is aan $\angle DAE$ hebben we nu twee gelijkvormige driehoeken. Nu kan $|AE|$ worden berekend met behulp van de gelijkvormigheid van de driehoeken.

$$\begin{aligned} \frac{|AE|}{|AD|} &= \frac{|AC|}{|AB|} \\ \frac{|AE|}{b} &= \frac{a}{1} \\ |AE| &= a \cdot b \end{aligned}$$

Dus lijnstuk $|AE|$ heeft nu lengte $a \cdot b$ wat betekent dat wij het product van a en b hebben geconstrueerd. □



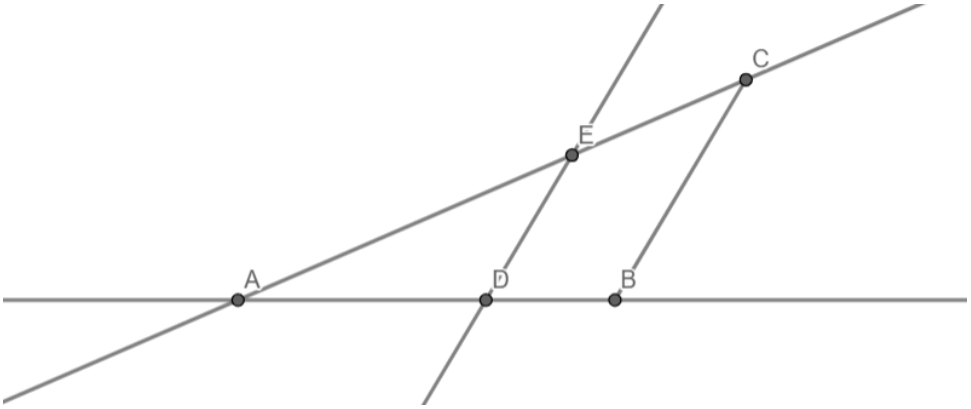
Figuur 13: Het vermenigvuldigen met passer en liniaal, hier is $b > 1$ genomen.

Delen: Als a en b construeerbaar zijn en $b \neq 0$, dan is a/b ook construeerbaar.

Bewijs. Neem de lijn door AB met $|AB| = b$ en B rechts van A. Neem de lijn door AC met $|AC| = a$, waarbij punt C niet op de lijn door AB ligt. Maak nu lijnstuk BC om de driehoek ABC te verkrijgen. Kies nu op de lijn door AB een punt D zo dat $|AD| = 1$, waarbij punt D rechts van A ligt. Construeer door punt D nu de lijn parallel aan lijnstuk BC. Het snijpunt van dit nieuwe lijnstuk en de lijn door AC noemen we punt E. Omdat $\angle ABC$ dezelfde hoek heeft als $\angle ADE$ en omdat $\angle EAD$ en $\angle CAB$ gelijk zijn hebben we nu twee gelijkvormige driehoeken. Zo kan $|AE|$ worden berekend.

$$\frac{|AE|}{|AD|} = \frac{|AC|}{|AB|}$$
$$\frac{|AE|}{1} = \frac{a}{b}$$

□



Figuur 14: Het delen met passer en liniaal, hier is $b > 1$ genomen.

Nu het mogelijk is om te delen kunnen alle rationele getallen geconstrueerd worden met behulp van de gehele getallen en deze operatie.

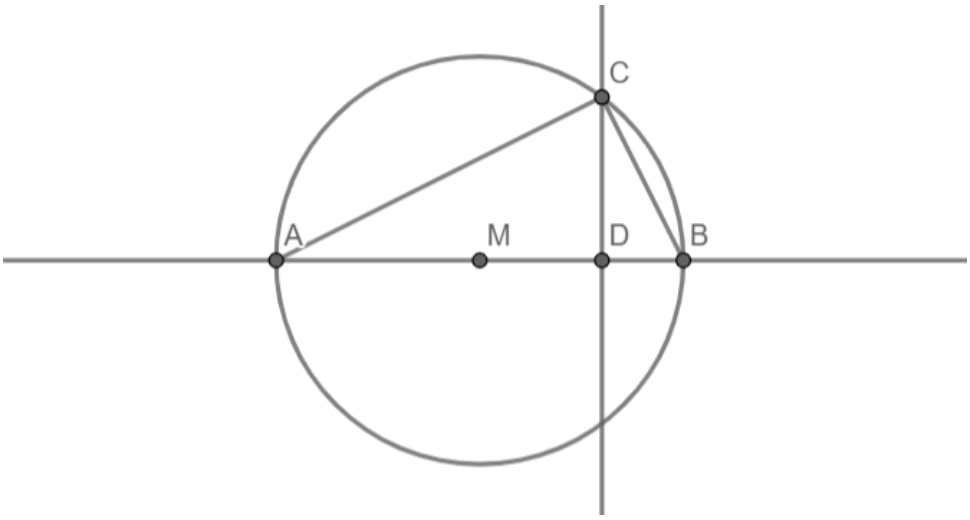
Worteltrekken: Als a construeerbaar is, dan is $\sqrt{a}$ ook construeerbaar.

Bewijs. Maak de lijn door A en B met $|AB| = a+1$ en B rechts van A. Laat M het middelpunt zijn van het lijnstuk AB. Construeer nu de cirkel met middelpunt M met diameter $a+1$ zodat deze door de punten A en B gaat. Kies nu punt D op lijnstuk AB zo dat $|AD| = a$ en $|DB| = 1$ en maak de loodrechte lijn op lijnstuk AB door D welke de cirkel snijdt op punt C. Construeer vanuit punt C de lijnstukken AC en BC. Nu hebben we dat $\angle ADC$ en $\angle BDC$ rechte hoeken zijn. Omdat de hoeken van een driehoek bij elkaar opgeteld 180 graden moeten zijn (Propositie XXXII uit de Elementen van Euclides) [2], hebben we dat $\angle CAD$ en $\angle ACD$ samen 90 graden moeten zijn. Ook hebben we dat $\angle ACB$ 90 graden is (Stelling van Thales, zie Hoofdstuk 3) en dus dat $\angle ACD$ en $\angle BCD$ samen 90 graden zijn. Dus zijn hoeken $\angle CAD$ en $\angle BCD$ gelijk, namelijk 90 graden min de hoek van $\angle ACD$. Dus omdat er 2 gelijke hoeken zijn in de driehoeken hebben we te maken met twee gelijkvormige driehoeken ADC en CBD. Zo kan de

lengte van lijnstuk CD worden berekend.

$$\begin{aligned}\frac{|CD|}{|AD|} &= \frac{|BD|}{|CD|}\\ \frac{|CD|}{a} &= \frac{1}{|CD|}\\ |CD|^2 &= a\\ |CD| &= \sqrt{a}\end{aligned}$$

□



Figuur 15: Het worteltrekken met passer en liniaal, hier is $a > 1$ genomen.

Optellen, aftrekken, vermenigvuldigen, delen en worteltrekken is allemaal mogelijk met passer en liniaal. Hiermee hebben we laten zien dat alle elementen in verzameling V ook in verzameling C zitten, ofwel $V \subseteq C$.
We kunnen nu dus heel $\mathbb{Q}$ maken en wortels nemen van deze getallen. Zo zijn bijvoorbeeld de volgende getallen construeerbaar, gegeven dat a, b en c construeerbaar zijn:

$$abc$$
$$\sqrt{\frac{a+b}{c^2}}$$
$$a+\sqrt[8]{\frac{b}{c}}$$

Het is mogelijk om 4e, 8e, 16e,... wortels te nemen, omdat als a construeerbaar is, dan is $\sqrt{a}$ construeerbaar, evenals $\sqrt{\sqrt{a}}$ enzovoort.

5.2 Gelijkheid van verzameling V en C

We hebben nu al laten zien dat $V \subseteq C$, nu rust het ons slechts nog om te laten zien dat C een deelverzameling is van V, alle getallen die gemaakt kunnen worden met het getal 1, optellen, aftrekken, vermenigvuldigen, delen en worteltrekken.
Om dit te laten zien gaan we na hoe er een nieuw punt gevonden kan worden met passer en liniaal, dit kan op drie verschillende manieren:

1. De intersectie van twee lijnen
2. De intersectie van een lijn en een cirkel
3. De intersectie van twee cirkels

In Hoofdstuk 2 hebben we gezien dat er met passer en liniaal een coördinaten systeem gemaakt kan worden. We kunnen nu dus de lijnen en cirkels die wij construeren beschrijven met behulp van formules. Stel we hebben twee geconstrueerde punten A en B, dan kunnen we deze in het coördinaten systeem beschrijven als $A = (x_A,y_A)$ en $B = (x_B,y_B)$. Merk op dat x_A, x_B, y_A en y_B construeerbaar zijn, we kunnen namelijk de loodlijn vanaf punten A en B naar de x-as en y-as construeren (zie Hoofdstuk 3) en dan de afstand van dat snijpunt tot de oorsprong nemen. We noemen een punt P met coördinaten (x_P,y_P) dan ook construeerbaar als de getallen x_P en y_P construeerbaar zijn. Nu kunnen we de formule van deze lijn als volgt berekenen:

Als $x_A = x_B$ en $y_A \neq y_B$, dan is de formule voor de lijn $x = x_A$, merk op dat alle constanten in de formule (alleen x_A in dit geval) construeerbaar zijn.
Als $y_A = y_B$ en $x_A \neq x_B$, dan is de formule voor de lijn $y = y_A$, merk weer op dat alle constanten in de formule construeerbaar zijn.
Als $x_A \neq x_B$ en $y_A \neq y_B$, dan kunnen we zonder verlies van generaliteit aannemen dat $x_B > x_A$. Dan krijgen we de formule $y = \frac{y_B - y_A}{x_B - x_A}x + c$. De constante c kan gevonden worden door de coördinaten van punt A in te vullen. Omdat x_A, y_A, x_B en y_B construeerbaar zijn en omdat we kunnen optellen, aftrekken, vermenigvuldigen en delen met passer en liniaal krijgen we dat de constante c ook construeerbaar is.
De formule van een lijn kan dus gegeven worden door $x = c$ met c construeerbaar of door $y = ax + b$ met a en b construeerbaar.

Op dezelfde manier kunnen we laten zien dat de formule van een cirkel slechts construeerbare parameters bevat. We beginnen met twee construeerbare punten A en B, nu maken we een cirkel met middelpunt A en straal AB. De formule van een cirkel met middelpunt $M = (x_M,y_M)$ en straal r is gegeven door $(x - x_M)^2 + (y - y_M)^2 = r^2$, dus de formule voor deze geconstrueerde cirkel is

$$(x - x_A)^2 + (y - y_A)^2 = |AB|^2.$$

Merk op dat het rechterdeel de lengte bevat van lijnstuk AB, omdat dit een geconstrueerd lijnstuk is is deze lengte dus construeerbaar (de lengte is gelijk aan $\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}$). Omdat x_A, y_A, x_B en y_B construeerbaar zijn en omdat we kunnen optellen, aftrekken, vermenigvuldigen, delen en worteltrekken met passer en liniaal hebben we dat alle parameters in de formule van een geconstrueerde cirkel construeerbaar zijn.

Nu we weten dat geconstrueerde lijnen en cirkels beschreven kunnen worden door formules met slechts construeerbare parameters, kunnen we kijken de manieren waarop we nieuwe punten kunnen construeren.

5.2.1 De intersectie van twee lijnen

Als eerste onderzoeken we de intersectie van twee geconstrueerde lijnen. Een geconstrueerde lijn is een lijn die gemaakt is met passer en liniaal en kunnen we opschrijven in de vorm $y = ax + b$ of in de vorm $x = c$ waarbij a, b en c construeerbare getallen zijn. Als deze lijnen

niet parallel lopen, dan snijden deze lijnen (Postulaat 5) en is het snijpunt van deze lijnen te berekenen door het stelsel van de vergelijkingen van de lijnen op te lossen. Laat a, b, c en d construeerbare getallen zijn en laat $a \neq c$, dan:

$$\begin{aligned} y &= ax+b \\ y &= cx+d \end{aligned}$$

$$\begin{aligned} ax+b &= cx+d \\ (a-c)x &= d-b \\ x &= \frac{d-b}{a-c} \end{aligned}$$

$$y = a\frac{(d-b)}{a-c} + b$$

Zo kunnen de coördinaten x en y van het snijpunt gevonden worden. Als een van de lijnen in de vorm $x = c$ en de andere lijn in de vorm $y = ax+b$ is, dan kan het nieuwe punt makkelijker berekend worden, namelijk $x = c$ en $y = ac+b$. Om deze construeerbare coördinaten te vinden wordt er slechts gebruik gemaakt van de vier rekenkundige operaties optellen, aftrekken, delen en vermenigvuldigen. Dit zijn operaties die V karakteriseren, dus zitten de coördinaten van de punten die op deze wijze gevonden worden ook in de verzameling V.

5.2.2 De intersectie van een lijn en een cirkel

Nu gaan we geval 2 bekijken waar een nieuw punt gevonden wordt door de intersectie van een geconstrueerde lijn en een geconstrueerde cirkel te nemen. Een geconstrueerde cirkel is een cirkel die we kunnen opschrijven in de vorm $(x-a)^2 + (y-b)^2 = c^2$ waar a, b en c construeerbare getallen zijn. Neem nu de intersectie van deze cirkel en de lijn $y = px+q$ met p en q construeerbare getallen, dan kunnen wij het snijpunt berekenen door het volgende stelsel vergelijkingen op te lossen:

$$\begin{aligned} y &= px+q \\ (x-a)^2 + (y-b)^2 &= c^2 \end{aligned}$$

Substitueren geeft:

$$\begin{aligned} (x-a)^2 + (px+q-b)^2 &= c^2 \\ x^2 + a^2 - 2ax + p^2x^2 + q^2 + b^2 + 2pqx - 2bpx - 2bq &= c^2 \\ (1+p^2)x^2 + (-2a+2pq-2bp)x + (a^2+q^2+b^2-2bq-c^2) &= 0 \end{aligned}$$

Hoewel deze vergelijking er wat omslachtig uit ziet kunnen wij met behulp van de wel bekende ABC formule de oplossing voor x vinden. Deze ABC formule geeft nul, een of twee oplossingen voor x, voor de vergelijking $\alpha x^2 + \beta x + \gamma = 0$ geeft dit de oplossingen $x = \frac{-\gamma \pm \sqrt{D}}{2\alpha}$ met $D = \beta^2 - 4\alpha\gamma$. Om vervolgens de y te vinden vullen we de gevonden x in bij de formule voor de lijn $y = px+q$. Merk op dat niet alle lijnen en cirkels snijpunten hebben, er zijn slechts snijpunten als de gevonden D niet negatief is.
Deze ABC formule en onze hierboven gemaakte stappen maken slechts gebruik van de operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken. Dit houdt in dat de coördinaten van de nieuwe gevonden punten in de verzameling V zitten.

5.2.3 De intersectie van twee cirkels

Als laatste onderzoeken we de intersectie van twee geconstrueerde cirkels. Wij nemen de cirkels $(x-a)^2+(y-b)^2=c^2$ en $(x-p)^2+(y-q)^2=r^2$ waarbij a, b, c, p, q en r construeerbare getallen zijn. Dan berekenen wij de snijpunten door het volgende systeem op te lossen:

$$\begin{aligned}(x-a)^2+(y-b)^2&=c^2\\(x-p)^2+(y-q)^2&=r^2\end{aligned}$$

$$\begin{aligned}x^2+a^2-2ax+y^2+b^2-2by&=c^2\\x^2+p^2-2px+y^2+q^2-2qy&=r^2\end{aligned}$$

We trekken vervolgens de vergelijkingen van elkaar af. Zo elimineren we de x^2 en y^2 om de vergelijking van een lijn te krijgen.

$$(2p-2a)x+(2q-2b)y+a^2+b^2-p^2-q^2=c^2-r^2$$

$$y=\frac{(a-p)}{q-b}x+\frac{c^2+p^2+q^2-a^2-b^2-r^2}{2q-2b}$$

Merk op dat dit alleen werkt als $q\neq b$. Als $q=b$ en $p\neq a$, dan kunnen wij dezelfde methode gebruiken om x uit te drukken in y. Als $q=b$ en $p=a$, dan hebben de cirkels hetzelfde middelpunt en hebben ze geen snijpunten of is het dezelfde cirkel.

De verkregen vergelijking is de construeerbare lijn die door de snijpunten loopt van de twee cirkels. Deze punten kunnen we berekenen zoals beschreven bij de intersectie van een lijn en een cirkel. Dit geeft een of twee punten waarvan de coördinaten in de verzameling V zitten.

Nu hebben we laten zien dat voor alle drie de mogelijke manieren waarop een nieuw punt gevonden kan worden met passer en liniaal de coördinaten van dat punt in de verzameling V zitten. Omdat de enige nieuwe getallen die wij met passer en liniaal kunnen construeren in de verzameling V zitten, weten we nu dat C een deelverzameling van V is, dus $C\subseteq V$.
We weten nu dat V en C deelverzamelingen van elkaar zijn, dus is de verzameling V gelijk aan de verzameling C. Dus alle getallen die met passer en liniaal geconstrueerd kunnen worden zijn getallen die gemaakt kunnen worden met het getal 1, optellen, aftrekken, vermenigvuldigen, delen en worteltrekken.

5.3 Lichaamsuitbreidingen over $\mathbb{Q}$ met een construeerbaar getal

In deze paragraaf gaan we een algebraïsch gevolg behandelen betreffende de graad van lichaamsuitbreidingen. Deze blijkt handig bij latere bewijzen over de construeerbaarheid van bepaalde constructies.

Neem een construeerbaar getal α, dan weten we dat dit getal verkregen is door slechts de operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken te gebruiken. Merk op dat optellen, aftrekken, vermenigvuldigen en delen lichaamsoperaties zijn, dus door door deze

vier operaties te gebruiken blijf je in hetzelfde algebraïsche lichaam. Met deze vier operaties kunnen wij met het getal 1 het lichaam $\mathbb{Q}$ opzetten, dit betekent dat alleen het worteltrekken het lichaam $\mathbb{Q}$ uitbreid.
Zo kunnen wij bijvoorbeeld het lichaam $\mathbb{Q}$ uitbreiden met $\sqrt{2}$, dan geldt

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}).$$

Het minimaalpolynoom van $\sqrt{2}$ in $\mathbb{Q}$ is x^2-2. Dit is een tweedegraads polynoom, dus de graad van $\sqrt{2}$ is 2. Dit is daarom een tweedegraads lichaamsuitbreiding waarbij de elementen van de vorm $a+b\sqrt{2}$ met $a,b \in \mathbb{Q}$ zijn.

Stel wij willen dit lichaam nogmaals uitbreiden met bijvoorbeeld $\sqrt{3}$, dan geldt

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

waarbij de elementen in $\mathbb{Q}(\sqrt{2},\sqrt{3})$ van de vorm $c+d\sqrt{3}$ zijn met $c,d \in \mathbb{Q}(\sqrt{2})$. De minimaalpolynoom van $\sqrt{3}$ in $\mathbb{Q}(\sqrt{2})$ is x^2-3. Dit is een tweedegraads vergelijking en dus $\Big[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\Big] = 2$. Merk op dat

$$\Big[\mathbb{Q}(\sqrt{2},\sqrt{3})\Big] = \Big[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\Big] \cdot \Big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\Big] = 2 \cdot 2 = 2^2$$

Op deze manier kunnen wij het lichaam steeds maar uitbreiden met nieuwe wortels $\sqrt{\beta}$ waarbij $\sqrt{\beta}$ nog niet in het lichaam zit, maar β wel. Hierbij kan β ook een combinatie zijn van andere wortels die eerder zijn toegevoegd, in het voorbeeld zou β dus $\sqrt{2}+\sqrt{3}$ kunnen zijn wat resulteert in het veld $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}})$.

Dit kunnen we wat algemener maken. We geven $\mathbb{Q}$ de naam F_0, dan geven we de eerste lichaamsuitbreiding $\mathbb{Q}(\sqrt{x})$ de naam F_1. Let op dat hierbij geldt dat $x \in F_0$ én $\sqrt{x} \notin F_0$. We kunnen op dezelfde manier de tweede lichaamsuitbreiding $F_1(\sqrt{y}) = \mathbb{Q}(\sqrt{x},\sqrt{y})$ de naam F_2 geven. Hierbij geldt dat $y \in F_1$ én $\sqrt{y} \notin F_1$. Op deze manier kunnen wij de lichamen F_3, F_4, enzovoort maken. Merk nu op dat elke lichaamsuitbreiding van graad 2 is, dus $[F_1 : F_0] = [F_2 : F_1] = 2$. Hieruit volgt voor een n-de lichaamsuitbreiding F_n dat

$$[F_n : F_0] = [F_n : F_{n-1}] \cdot [F_{n-1} : F_{n-2}] \cdot \ldots \cdot [F_1 : F_0] = 2^n.$$

Dit resultaat kunnen we gebruiken om wat te zeggen voor het construeerbare getal α. We weten, omdat α opgebouwd uit de vijf construeerbare operaties, dat $\alpha \in F_n$ voor een zekere n. Neem bijvoorbeeld $\alpha = \frac{1}{4}+\sqrt{3}-2\sqrt{\sqrt{2}+\sqrt{3}}$, dan weten we dat $\alpha \in \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}})$. We kunnen nu het uitbreidingslichaam van α over $\mathbb{Q}$ nemen, dan geldt

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}\left(\sqrt{2},\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}}\right).$$

We weten dat de graad van $\mathbb{Q}(\alpha)$ een gehele deler is van $\Big[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}}) : \mathbb{Q}\Big] = 2^3$, de graad moet dus 1, 2, 4 of 8 zijn, merk op dat dit allemaal machten van 2 zijn.
In het algemene geval betekent dit dat voor een zekere construeerbare $\alpha \in F_n$ geldt dat $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq F_n$. Maar dan is de graad van $\mathbb{Q}(\alpha)$ een deler van $[F_n : \mathbb{Q}] = 2^n$. Dus is de graad van $\mathbb{Q}(\alpha)$ een macht van 2. Formeel geeft dit de volgende stelling.

Stelling 5.2. *Als $\alpha \in \mathbb{R}$ construeerbaar is, dan is de graad van de lichaamsuitbreiding $\mathbb{Q}(\alpha)$ een macht van 2, ofwel $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ waarbij n een geheel getal is.*

Bewijs. Laat α een willekeurig construeerbaar getal zijn. Dan is α in een eindig aantal stappen met passer en liniaal geconstrueerd, oftewel door een eindig aantal keer de operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken toe te passen te beginnen met een getal uit $\mathbb{Q}$.
Stel α is geconstrueerd in k stappen, dan kunnen we alle tussenstappen om tot α te komen opschrijven als $\alpha_0, \alpha_1, \ldots, \alpha_k$ waarbij $\alpha_0 \in \mathbb{Q}$ en $\alpha_k = \alpha$. ($\sqrt{2}+1$ geeft bijvoorbeeld $\alpha_0 = 2, \alpha_1 = \sqrt{2}, \alpha_2 = \sqrt{2}+1$)

Omdat $\alpha \in \mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_k)$, volgt uit Lemma 4.6 dat de graad van lichaamsuitbreiding $\mathbb{Q}(\alpha)$ een deler van de graad van lichaamsuitbreiding $\mathbb{Q}(\alpha_0, \ldots, \alpha_k)$. Namelijk, ($\alpha = \alpha_k$): $[\mathbb{Q}(\alpha_0, \ldots, \alpha_k) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0, \ldots, \alpha_k) : \mathbb{Q}(\alpha_k)] \cdot [\mathbb{Q}(\alpha_k) : \mathbb{Q}]$.
We willen nu laten zien dat de graad van de lichaamsuitbreiding $\mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_k)$ een macht van 2 is. Dit doen we door het lichaam $\mathbb{Q}$ een voor een uit te breiden met de α_i. Merk op dat $\alpha_0 \in \mathbb{Q}$, dus $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 1$. We gaan nu α_i toevoegen, gegeven dat $\alpha_0, \ldots, \alpha_{i-1}$ al zijn toegevoegd. Als in stap i een van de operaties optellen, aftrekken, vermenigvuldigen of delen wordt gebruikt blijf je in hetzelfde lichaam zitten, dus als we een van deze vier operaties gebruiken, dan $[\mathbb{Q}(\alpha_0, \ldots, \alpha_i) : \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})] = 1$.
Als in stap i de operatie worteltrekken is gebruikt, dan geldt $\alpha_i = \sqrt{\alpha_{i-1}}$ waarbij $\alpha_{i-1} \in \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})$. Als $\sqrt{\alpha_{i-1}} \notin \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})$, dan is de minimaalpolynoom van α_i in dit lichaam gegeven door $x^2 - \alpha_{i-1}$, dit is een tweedegraads vergelijking, dus is α_i van graad 2 en is volgens Lemma 4.7 de graad van de lichaamsuitbreiding gelijk aan 2. Als $\sqrt{\alpha_{i-1}} \in \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})$ dan is de minimaalpolynoom van α_i in dit lichaam gegeven door $x - \sqrt{\alpha_{i-1}}$, dit is een eerstegraads vergelijking dus de lichaamsuitbreiding heeft in dit geval graad 1.
Ongeacht van de gebruikte operatie in stap i is de graad van de lichaamsuitbreiding $\mathbb{Q}(\alpha_0, \ldots, \alpha_i) : \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})$ dus gelijk 1 of 2.

Volgens Lemma 4.6 geldt

$$\begin{aligned}[\mathbb{Q}(\alpha_0, \ldots, \alpha_k) : \mathbb{Q}] = &[\mathbb{Q}(\alpha_0, \ldots, \alpha_k) : \mathbb{Q}(\alpha_0, \ldots, \alpha_{k-1})] \cdot [(\mathbb{Q}(\alpha_0, \ldots, \alpha_{k-2}))(\alpha_{k-1})] \cdot \ldots \\ &\cdot [\mathbb{Q}(\alpha_0, \alpha_1) : \mathbb{Q}(\alpha_0)] \cdot [\mathbb{Q}(\alpha_0) : \mathbb{Q}]\end{aligned}$$

Ook is in bovenstaand paragraaf laten zien dat elke $[\mathbb{Q}(\alpha_0, \ldots, \alpha_i) : \mathbb{Q}(\alpha_0, \ldots, \alpha_{i-1})]$ gelijk is aan 1 of 2. Dit betekent dat het product van al deze uitbreidingen, de rechterkant van de vergelijking, een macht is van 2. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ een deler is van $[\mathbb{Q}(\alpha_0, \ldots, \alpha_k) : \mathbb{Q}]$, dit betekent dat $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ met n geheel. □

We hebben nog een aantal andere stellingen over de construeerbaarheid van een getal die later van pas komen.

Stelling 5.3. [12](7.11) *$\alpha \in \mathbb{R}$ is construeerbaar als en slechts als het lichaam $\mathbb{Q}(\alpha)$ verkregen kan worden door een reeks aan tweedegraads lichaamsuitbreidingen, dus*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_k = \mathbb{Q}(\alpha)$$

waarbij $F_i = F_{i-1}(\sqrt{\alpha_i})$ voor een zekere $\alpha_i \in F_{i-1}$ met $\sqrt{\alpha_i} \notin F_{i-1}$.

Bewijs. Als α construeerbaar is dan volgt uit het bewijs van Stelling 5.2, waarbij de lichaamsuitbreidingen van graad 1 worden weggelaten, dat er een reeks lichamen is zo dat

$$\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_k \supseteq \mathbb{Q}(\alpha)$$

waarbij $[F_{i+1} : F_i] = 2$ voor $0 \leq i < k-1$. Laat nu

$$M_j = L_j \cap \mathbb{Q}(\alpha)$$

En beschouw de L_j en M_j nu als vectorruimtes over $\mathbb{Q}$, deze zijn eindig dimensionaal. Merk op dat M_j lichamen zijn en dat $M_j \subseteq L_j$, daarom is $\dim(M_j) \leq \dim(L_j)$. We weten dat $\dim(L_{j+1}) = 2\dim(L_j)$ voor $0 \leq j < k-1$. Dus of $M_{j+1} = M_j$ of $\dim(M_{j+1}) = 2\dim(M_j)$. Laat de lichamen M_{j+1} weg als $M_{j+1} = M_j$. Hernoem de resulterende rij naar F_0,F_1,...,F_k met $K_0 = \mathbb{Q}$. Ook weten we nu dat $F_k = \mathbb{Q}$, dus als als α construeerbaar is bestaat de gewenste reeks aan tweedegraads lichaamsuitbreidingen.

Nu andersom: stel $\mathbb{Q}(\alpha)$ kan verkregen worden door een reeks aan lichaamsuitbreidingen

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_k = \mathbb{Q}(\alpha)$$

Waarbij $F_i = F_{i-1}(\sqrt{\alpha_i})$ voor een zekere $\alpha_i \in F_{i-1}$. Het is mogelijk om met passer en liniaal wortels te construeren, dus gegeven dat wij F_{i-1} kunnen construeren kunnen wij hieruit ook F_i construeren. Dit doen we namelijk door $\sqrt{\alpha_i}$ toe te voegen aan F_i waarbij $\alpha_i \in F_{i-1}$ en $\sqrt{\alpha_i} \notin F_i$. Dit samen met het feit dat wij $\mathbb{Q}$ kunnen construeren geeft met behulp van inductie op i dat wij alle F_j kunnen construeren en daarmee dus ook $F_k = \mathbb{Q}(\alpha)$ en dus is α construeerbaar. □

We hebben in Hoofdstuk 3 al gezien dat we met passer en liniaal een coördinaten systeem op kunnen zetten. In plaats van gebruik te maken van een x-as en y-as kunnen we ook gebruik maken van een reële en imaginaire as, in dit geval gaan we kijken naar complexe getallen. Net als bij de construeerbaarheid van een punt $P = (x_P, y_P)$, wat construeerbaar is als x_P en y_P construeerbaar zijn, is een complex getal $z = a + bi$ construeerbaar als en slechts als $a,b \in \mathbb{R}$ construeerbaar zijn.

Definitie 5.4. *Een getal $z \in \mathbb{C}$ is construeerbaar als het punt z in een eindig aantal stappen met passer en liniaal geconstrueerd kan worden in het complexe vlak.*

Stelling 5.5. *Het getal $z \in \mathbb{C}$, met $z = a + bi$, is construeerbaar als en slechts als $a,b \in \mathbb{R}$ construeerbaar zijn.*

Bewijs. Laat $z \in \mathbb{C}$ construeerbaar zijn met $z = a + bi$. Dan kunnen we in het complexe assenstelsel, met oorsprong O, de loodlijnen van punt z naar zowel de reële als de imaginaire as maken (zie Hoofdstuk 3). Nu snijdt de loodlijn door z op de reële as de reële as in punt A en snijdt de loodlijn door z op de imaginaire as de imaginaire as in punt B. We hebben nu twee lijnstukken, OA met $|OA| = a$ en OB met $|OB| = b$, dus hebben we twee lijnstukken met lengtes a en b geconstrueerd, dus zijn a en b construeerbaar.

Laat $a,b \in \mathbb{R}$ construeerbaar zijn, dan hebben wij dus twee geconstrueerde lijnstukken in het complexe vlak met lengtes a en b. Laat deze lengtes op de reële as liggen met $|A_1A_2| = a$ en $|B_1B_2| = b$. We construeren een cirkel met middelpunt O, de oorsprong, en straal a en

het snijpunt van deze cirkel en de reële as noemen we punt A. Als $a \geq 0$ dan nemen we de positieve reële as, als $a < 0$ nemen we de negatieve reële as. Op dezelfde manier kunnen we punt B maken op de imaginaire as zodat $|OB| = b$. Nu maken we de loodlijn door punt A op de reële as en loodlijn door het punt B op de imaginaire as (zie Hoofdstuk 3). Het snijpunt van deze loodlijnen levert geconstrueerd punt $z = a + bi$ op in het complexe vlak en dus is $z \in \mathbb{C}$ construeerbaar. □

Voordat we verder gaan moeten we definiëren wat optellen, aftrekken, vermenigvuldigen, delen (volgt uit het delen) en worteltrekken is met complexe getallen.

Optellen en aftrekken: Optellen en aftrekken met complexe getallen $z = a + bi$ en $w = c + di$, met $a, b, c, d \in \mathbb{R}$, doen wij door het reële en imaginaire gedeelte los bij elkaar op te tellen. Dit geeft $z + w = (a + c) + (b + d)i$ en $z - w = (a - c) + (b - d)i$.

Vermenigvuldigen en delen: Als we twee complexe getallen $z = a + bi$ en $w = c + di$, met $a, b, c, d \in \mathbb{R}$, willen vermenigvuldigen, dan doen wij dit als volgt. Schrijf je getallen eerst om in poolcoördinaten $z = r(\cos(\phi) + i\sin(\phi))$ en $w = q(\cos(\psi) + i\sin(\psi))$, $r,q,\phi,\psi \in \mathbb{R}$, nu krijgen we $zw = rq(\cos(\phi + \psi) + i\sin(\phi + \psi))$. De stralen van z en w, r en q, worden dus vermenigvuldigd en de hoeken, ϕ en ψ, worden bij elkaar opgeteld. We kunnen dus ook z/w uitrekenen als $w \neq 0$, dat is immers hetzelfde als $z\frac{1}{w}$ waar $\frac{1}{w} = \frac{c-di}{(c+di)(c-di)} = \frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}i$.

Worteltrekken: Als wij de wortel van een complex getal $z = a + bi$, met $a, b \in \mathbb{R}$ willen berekenen doen wij dit door eerst het complexe getal uit te drukken in poolcoördinaten, dit geeft $z = r(\cos(\phi) + i\sin(\phi))$, $r,\phi \in \mathbb{R}$. Worteltrekken doen we nu door de wortel te nemen van de straal r en de hoek ψ door 2 te delen, dit geeft $\sqrt{z} = \sqrt{r}(\cos(\frac{\phi}{2}) + i\sin(\frac{\phi}{2}))$.

Nu willen we, op dezelfde wijze als met de reële getallen, laten zien dat dit alle construeerbare getallen zijn. We maken twee verzamelingen, V' en C'. Hier bevat V' alle getallen die verkregen kunnen worden met optellen, aftrekken, vermenigvuldigen, delen en worteltrekken uit 1 en i. C' bevat alle punten in $\mathbb{C}$ die je met passer en liniaal kunt construeren gegeven een lijnstuk van lengte 1 en i. We willen laten zien dat deze twee verzamelingen gelijk zijn aan elkaar.

$V' \subseteq C'$: We kunnen met passer en liniaal twee complexe getallen optellen en aftrekken, namelijk we nemen complexe getallen $z = a + bi$ en $w = c + di$, met $a, b, c, d \in \mathbb{R}$. Dan $z + w = (a + c) + (b + d)i$, maar $a + c$ en $b + d$ kunnen wij construeren, dit zijn namelijk gewoon reële getallen. Dus kunnen wij $z + w$ ook construeren. Op dezelfde manier komen we erachter dat $z - w$ ook construeerbaar is.
We kunnen ook complexe getallen vermenigvuldigen en delen met passer en liniaal. Laat z en w complexe getallen zijn met $z = r(\cos(\phi) + i\sin(\phi))$ en $w = q(\cos(\psi) + i\sin(\psi))$, met $r, q, \phi, \psi \in \mathbb{R}$. Dan is $zw = rq(\cos(\phi + \psi) + i\sin(\phi + \psi))$. Hiervoor zijn de stralen rq vermenigvuldigd, dit zijn reële getallen dus dit kunnen wij construeren en aftekenen op de reële as. Ook kunnen wij de hoeken ϕ en ψ bij elkaar optellen door de hoek ψ tegen hoek ϕ aan te leggen (zie Hoofdstuk 3). Trek nu de lijn vanuit de oorsprong die hoek $\phi + \psi$ maakt met de reële as en maak de cirkel met middelpunt de oorsprong en straal rq. Het snijpunt van de cirkel en de lijn is het punt zw en dit punt is dus construeerbaar. Op deze manier kunnen wij ook delen, namelijk $\frac{z}{w} = z\frac{1}{w}$.
Worteltrekken van complexe getallen is uiteindelijk ook nog mogelijk met passer en liniaal.

We hebben al gezien dat de wortel van het complexe getal $z = r(\cos(\phi) + i\sin(\phi))$, met $r, \phi \in \mathbb{R}$ gelijk is aan $\sqrt{z} = \sqrt{r}(\cos(\frac{\psi}{2}) + i\sin(\frac{\psi}{2}))$. Wij kunnen $\sqrt{r}$ construeren omdat r een reëel getal is en wij kunnen de hoek $\frac{\psi}{2}$ construeren met de bissectrice (zie Hoofdstuk 3). Dus wij kunnen de wortel van complexe getallen construeren en daarmee hebben we laten zien dat $V' \subseteq C'$.

Nu moeten we nog laten zien dat $C' \subseteq V'$. De operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken zijn construeerbaar bij de complexe getallen. Om deze reden kunnen we voor deze inclusie dezelfde redenatie als in Hoofdstuk 5.2 volgen, maar dan in $\mathbb{C}$ om tot het resultaat te komen dat $C' \subseteq V'$ en dus $V' = C'$.

Nu kunnen we de volgende stelling bewijzen.

Stelling 5.6. *Het getal $z \in \mathbb{C}$ is construeerbaar als en slechte als het lichaam $\mathbb{Q}(z)$ verkregen kan worden door een reeks aan tweedegraads lichaamsuitbreidingen, dus*

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_k = \mathbb{Q}(z)$$

waarbij $F_i = F_{i-1}(\sqrt{z_i})$ voor een zekere $z_i \in F_{i-1}$ met $\sqrt{z_i} \notin F_{i-1}$.

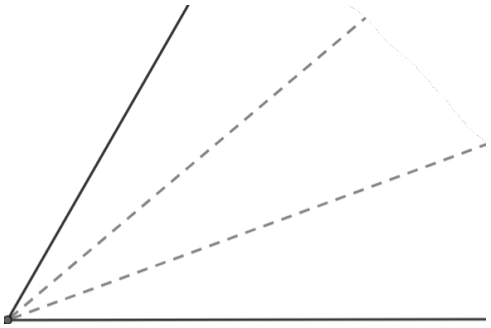
Bewijs. Het bewijs van deze stelling is hetzelfde als het bewijs voor Stelling 5.3, alleen is $\alpha \in \mathbb{C}$ en zijn de operaties optellen, aftrekken, vermenigvuldigen, delen en worteltrekken zoals gedefinieerd voor complexe getallen. □

6 Drie klassieke meetkundige problemen

In dit hoofdstuk gaan we drie klassieke meetkundige problemen bespreken, namelijk de driedeling van een hoek, de verdubbeling van de inhoud van een kubus en de kwadratuur van de cirkel. Elk van deze problemen is niet mogelijk met passer en liniaal en dit zullen we per probleem laten zien.

6.1 Driedeling van een hoek

Als eerste zal de driedeling van een hoek besproken worden. De vraag die we gaan beantwoorden luidt:
Kunnen we in een eindig aantal stappen met passer en liniaal elke willekeurige hoek in drie gelijke hoeken delen?



Figuur 16: De driedeling van een hoek.

Hoewel de bissectrice van een hoek relatief eenvoudig is om te maken (zie Hoofdstuk 2), blijkt dat de driedeling niet voor alle hoeken te construeren is. Dus we hebben geen algoritme om een willekeurige hoek in drieën te delen. Om te laten zien dat het niet mogelijk is om elke hoek in drieën te delen gaan we een voorbeeld gebruiken. Hiervoor maken wij gebruik van de hoek van 60°. Deze hoek kunnen wij maken door een gelijkzijdige driehoek te construeren (zie Hoofdstuk 3).

Voordat we het bewijs gaan geven is er een lemma die wij gaan gebruiken, de derdehoekregel voor de cosinus:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Nu hebben we alle benodigde hulpmiddelen om te laten zien dat een hoek van 60° niet in drie gelijke hoeken gedeeld kan worden.

Bewijs. Laat de lijn L_1 gelijk lopen met de x-as en maak de lijn L_2 die L_1 snijdt door de oorsprong in een hoek van 60°Ḋit kan door een gelijkzijdige driehoek te construeren (zie Hoofdstuk 3)waarvan een hoek op de oorsprong ligt en een zijde gelijk loopt met L_1. De andere zijde door de oorsprong noemen we dan L_2.
Door de hoek van 60° te driedelen maken we een lijn L_3 die een hoek van 20° maakt met de x-as. Als wij L_3 kunnen maken, dan kunnen wij met behulp van de eenheidscirkel ook de coördinaten $(\cos(20°), \sin(20°))$ vinden, dit is namelijk het snijpunt tussen L_3 en de eenheidscirkel. Dus als wij L_3 kunnen construeren kunnen wij zowel de cosinus als de sinus

van 20° construeren.

We gaan nu gebruik maken van de derdehoekregel voor de cosinus.

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Neem hier voor θ een waarde van 20°.

$$\cos(60^\circ) = 4\cos^3(20^\circ) - 3\cos(20^\circ)$$

$$8\cos^3(20^\circ) - 6\cos(20^\circ) - 1 = 0$$

Als we hier $2\cos(20^\circ)$ substitueren door x ontstaat de volgende derdegraads vergelijking:

$$x^3 - 3x - 1 = 0 \tag{6.1}$$

We willen laten zien dat $\cos(20^\circ)$ niet construeerbaar is. Aangezien we x als volgt hebben gekozen, $x = 2\cos(20^\circ)$, voldoet het om te laten zien dat de oplossing voor Vergelijking 6.1 geen construeerbare oplossing heeft.

Stelling 4.1 stelt dat als Vergelijking 6.1 een rationale oplossing heeft, dat deze in de vorm $\frac{p}{q}$ geschreven kan worden, waar p een gehele deler is van -1 en q een gehele deler is van 1. Dus als hij bestaat, moet een rationale oplossing 1 of -1 zijn. Na korte inspectie blijkt dat zowel 1 als -1 geen oplossingen zijn voor Vergelijking 6.1. Dus er is geen rationale oplossing voor de vergelijking.

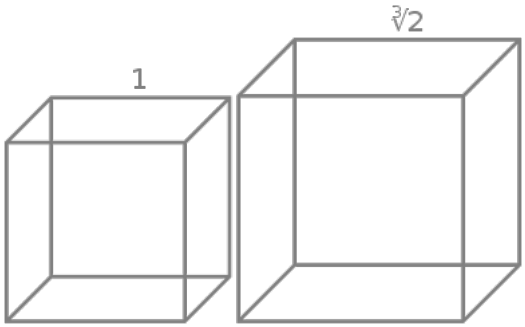
Vergelijking 6.1 is van graad 3, dit betekent dat als wij deze vergelijking kunnen ontbinden over $\mathbb{Q}$ in factoren dat minstens een van deze factoren van graad 1 is. We hebben al gezien dat er geen rationale oplossingen zijn voor $x^3 - 3x - 1 = 0$. Dit betekent dat wij de vergelijking niet kunnen omschrijven in lineaire factoren over $\mathbb{Q}$, dus is de vergelijking irreducibel over $\mathbb{Q}$.

Hieruit volgt dat de lichaamsuitbreiding $\mathbb{Q}(\cos(20^\circ))$ van graad 3 is, maar volgens Stelling 5.2 is $\cos(20^\circ)$ dan niet construeerbaar. Dit houdt in dat de hoek van 20° niet construeerbaar is en dat de hoek van 60° niet in drieën gedeeld kan worden. Dus kan niet elke willekeurige hoek in drie gelijke hoeken gedeeld worden met passer en liniaal. □

6.2 Verdubbeling van een kubus

Met de verdubbeling van een kubus wordt bedoeld:

Gegeven een willekeurige kubus, kunnen we een kubus construeren met een inhoud die 2 keer zo groot is als de inhoud van de gegeven kubus?



Figuur 17: De verdubbeling van een kubus met zijde 1.
Bron:. Wikipedia.nl [13]

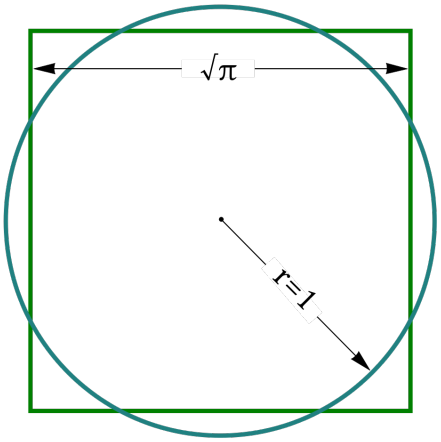
Bewijs. Het bewijs hiervan volgt dezelfde redenering als het bewijs voor de driedeling van een hoek. We beginnen met een kubus met zijdes van lengte 1, deze kubus heeft inhoud 1. Om een kubus te maken met een verdubbelde inhoud moeten we een kubus maken met inhoud 2. Omdat alle zijdes gelijk zijn betekent dit dat elke zijde lengte $\sqrt[3]{2}$ moet hebben. We weten dat $\sqrt[3]{2}$ een oplossing is voor de vergelijking $x^3-2=0$. Zoals ook beschreven is in Paragraaf 6.1, als $x^3-2=0$ ontbonden kan worden in factoren over $\mathbb{Q}$, dan betekent dat dat minstens een van deze factoren van graad 1 is. Volgens de Rationale Wortelstelling (Stelling 4.1) zijn de enige mogelijke rationale oplossingen $x=\pm 1$ en $x=\pm 2$, echter werken deze oplossingen allemaal niet voor de vergelijking $x^3-2=0$. Dit betekent dat $x^3-2=0$ geen oplossingen in $\mathbb{Q}$ heeft, dus is de polynoom x^3-2 irreducibel over $\mathbb{Q}$.

Aangezien de polynoom x^3-2 irreducibel is over $\mathbb{Q}$ en van graad 3 is, vertelt dit ons dat de lichaamsuitbreiding $\mathbb{Q}(\sqrt[3]{2})$ van graad 3 is. Uit Stelling 5.2 volgt dat $\sqrt[3]{2}$ niet construeerbaar is. Er is dus een kubus, de kubus met zijdes van lengte 1, waarvoor wij geen kubus kunnen maken met een inhoud die twee keer zo groot is. Dus kunnen wij niet voor elke willekeurige kubus een kubus construeren met een inhoud twee maal zo groot als de inhoud van de eerste kubus. □

6.3 De kwadratuur van een cirkel

Het laatste probleem wat we gaan bekijken is de kwadratuur van een cirkel. Hiermee wordt bedoeld:

Gegeven een cirkel met willekeurige straal, kunnen we een vierkant maken met dezelfde oppervlakte als de gegeven cirkel?



Figuur 18: De kwadratuur van een cirkel met straal 1.
Bron:. Wikipedia.nl [10]

Bewijs. Om te laten zien dat dit niet voor elke willekeurige cirkel mogelijk is laten we het zien voor een cirkel met straal $r = 1$. De oppervlakte van een cirkel is gelijk aan πr^2, dus onze cirkel heeft oppervlakte π. Een vierkant met oppervlakte π heeft zijdes van lengte $\sqrt{\pi}$. De vraag is dus of wij het getal $\sqrt{\pi}$ kunnen construeren.

Als wij $\sqrt{\pi}$ kunnen construeren, dan kunnen wij ook π construeren (vermenigvuldig de wortel met zichzelf). Om Stelling 5.2 te kunnen gebruiken moeten we een primitief polynoom over $\mathbb{Q}$ vinden waarvan π en nulpunt is. In 1882 heeft Ferdinand von Lindemann een handige eigenschap gevonden van π [7].

Stelling 6.1 (*1882, Lindemann*)**.** *π is transcendent. Ofwel π is geen nulpunt van een (niet nul) polynoom van eindige graad met rationale coëfficiënten.*

Volgens bovenstaande stelling is er dus geen polynoom van eindige graad zo dat π een nulpunt is van dit polynoom. Maar dan kan de graad van de lichaamsuitbreiding $\mathbb{Q}(\pi)$ geen eindig getal zijn. Volgens Stelling 5.2 is π geen construeerbaar getal en is de kwadratuur van een willekeurige cirkel dus niet te construeren. □

Merk op dat, omdat een transcendent getal geen nulpunt is van een polynoom met eindige graad, we op bovenstaande manier kunnen beredeneren dat geen enkel transcendent getal construeerbaar is.

7 Regelmatige veelhoeken

In dit hoofdstuk worden regelmatige veelhoeken besproken en de construeerbaarheid ervan. Een regelmatige veelhoek is een veelhoek waarvan alle zijdes even lang zijn en alle hoeken gelijk zijn. Een veelvoorkomend voorbeeld van een regelmatige veelhoek is de gelijkzijdige driehoek of het vierkant.

Een manier om regelmatige veelhoeken te beschrijven is door te kijken naar de complexe getallen. We kunnen namelijk de punten die wij construeren ook beschrijven als een complex getal, hierbij is de x-as het reële gedeelte en is de y-as het imaginaire gedeelte. De hoekpunten van een regelmatige veelhoek liggen allemaal op een cirkel. Een mogelijke manier om de hoekpunten te vinden van een n-voudige veelhoek is om de oplossingen te vinden voor de vergelijking $x^n - 1$, in dit geval liggen alle hoekpunten op de eenheidscirkel. De oplossingen voor deze formule zijn eenheidswortels van de vorm $\zeta_n^k = e^{\frac{2k\pi i}{n}}$, hier is de n dezelfde als in de vergelijking $x^n - 1$ en is $k \in \{1,\ldots,n-1\}$. Een eenheidswortel wordt primitief genoemd als n en k relatief priem zijn, de meest gebruikte primitieve eenheidswortel is waar $k = 1$, deze noteren we als ζ_n. De oplossingen voor $x^n - 1$ zijn $\{1,\zeta_n,\zeta_n^2,\ldots,\zeta_n^{n-1}\}$. Deze getallen zijn construeerbaar als en slechts als ζ_n construeerbaar is, dus een regelmatige n-hoek is construeerbaar als en slechts als $\zeta_n = e^{\frac{2\pi i}{n}}$ construeerbaar is. Voordat we gaan onderzoeken voor welke ζ_n dit zo is, zijn er een definitie en een aantal lemma's die onze zoektocht naar welke n-hoeken construeerbaar zijn makkelijker zullen maken.
Voor gemak zullen we in dit hoofdstuk de volgende definitie gebruiken.

Definitie 7.1. *Een positief geheel getal n is constructief als de regelmatige n-hoek construeerbaar is met passer en liniaal.*

De stelling die wij dit hoofdstuk willen geven is de Stelling van Gauss-Wantzel, deze stelt precies welke vorm een getal moet zijn om constructief te zijn. Voordat wij de Stelling van Gauss-Wantzel kunnen bewijzen hebben we nog een paar definities en lemma's nodig.

Definitie 7.2. *Een Fermatgetal is een natuurlijk getal van de vorm* $F_n = 2^{2^n} + 1$.

Fermat vermoedde dat elk Fermatgetal een priemgetal is, maar dit bleek onjuist te zijn, dus de volgende definitie moet hieraan toegevoegd worden.

Definitie 7.3. *Een Fermat priemgetal is een Fermatgetal dat priem is.*

De Fermatgetallen $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ en $F_4 = 65537$ zijn wel Fermat priemgetallen, $F_5 = 4294967297$ niet, dit is o.a. deelbaar door 641.

Lemma 7.4. *Als* $2^k + 1$ *een oneven priemgetal is, dan is k een macht van 2.*

Bewijs. Laat k een positief geheel getal zijn, maar geen macht van 2. Dan moet het een oneven priemgetal als factor hebben $s > 0$ en krijgen we $k = rs$, waar $1 \leq r < k$.
Voor positief geheel getal m geldt $(a-b)|(a^m - b^m)$. Als we $a = 2^r$, $b = -1$ en $m = s$ nemen, krijgen we (s is oneven)

$$(2^r + 1)|(2^{rs} + 1)$$

en dus

$$(2^r + 1)|(2^k + 1)$$

Merk op dat $1 < 2^r + 1 < 2^k + 1$, dus is $2^k + 1$ geen priemgetal voor k positief geheel. □

Voor het bewijs van de Stelling van Gauss-Wantzel hebben we ook nog twee lemma's nodig over de ϕ functie van Euler (Definitie 4.19). Het eerste lemma is een zeer bekend lemma wat met bewijs te vinden is in vele algebra boeken.

Lemma 7.5. *Laat p een priemgetal zijn, dan* $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ *met k een positief geheel getal en als m,n relatief priem zijn, dan geldt* $\phi(mn) = \phi(m)\phi(n)$.

Lemma 7.6. $\phi(n) = 2^m$ *met m een positief geheel getal als en slechts als*

$$n = 2^r p_1 \dots p_s$$

waar r en s gehele getallen zijn en $p_1, \dots, p_s$ *oneven Fermat priemgetallen zijn van de vorm*

$$p_j = 2^{2^{r_j}} + 1$$

met r_j *positieve gehele getallen.*

Bewijs. Laat $n = 2^r p_1^{\alpha_1} \dots p_s^{\alpha_s}$, waar $p_1, \dots, p_s$ verschillende oneven priemgetallen zijn met $\alpha_i \geq 1$. Dan $\phi(n) = 2^{r-1} p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)$. Neem nu aan dat $\phi(n) = 2^m$. Een macht van 2 is niet deelbaar door een oneven priemgetal, dus geldt $\alpha_i \leq 1$ voor alle i (anders krijgen we $p_i | 2^m$), dus $\alpha_i = 1$ voor alle i. Ook moet elke deler van een macht van 2 ook een macht van 2 zijn, dus $p_j - 1$ is een macht van 2 voor alle i. Hieruit volgt dat de priemgetallen p_j van de vorm $p_j = 2^k + 1$ moeten zijn. Maar als een getal van de vorm $2^k + 1$ een priemgetal is, dan $k = 2^d$ met d geheel (Lemma 7.4), dus is $p_j = 2^{2^{r_j}} + 1$ voor alle j en dus is n van de gewenste vorm.
Neem nu aan dat $n = 2^r p_1 \dots p_s$ waar $p_1, \dots, p_s$ verschillende Fermat priemgetallen zijn, dus $p_i = 2^{2^{r_i}} + 1$. Dan geldt

$$\phi(n) = 2^{r-1} p_1^{1-1}(p_1 - 1) \dots p_s^{1-1}(p_s - 1) = 2^{r-1}(p_1 - 1) \dots (p_s - 1) = 2^{r-1} 2^{2^{r_1}} \cdots 2^{2^{r_s}}$$

of $\phi(n) = 2^{2^{r_1}} \cdots 2^{2^{r_s}}$ als $r = 0$. In beide gevallen is $\phi(n)$ een macht van 2.
Dus is $\phi(n)$ een macht van 2 als en slechts als

$$n = 2^r p_1 \dots p_s$$

waar r en s gehele getallen zijn en $p_1, \dots, p_s$ oneven priemgetallen van de vorm

$$p_j = 2^{2^{r_j}} + 1$$

met r_j positieve gehele getallen. □

Stelling 7.7 (Gauss-Wantzel)**.** [12](20.13) *De regelmatige n-hoek is construeerbaar met passer en liniaal als en slechts als*

$$n = 2^r p_1 \dots p_s$$

waar r en s gehele getallen zijn en $p_1, \dots, p_s$ *oneven Fermat priemgetallen zijn van de vorm*

$$p_j = 2^{2^{r_j}} + 1$$

met r_j *niet-negatieve gehele getallen.*

Bewijs. Merk op dat het construeren van een regelmatige n-hoek hetzelfde is als het construeren van alle n-de eenheidswortels ζ_n^k in het complexe vlak, beginnend met de punten 0 en 1, alle ζ_n^k vormen dan bij elkaar de hoekpunten van de n-hoek.

Neem een primitieve n-de eenheidswortel $\zeta_n = \exp(\frac{2\pi i}{n})$. Nu zijn alle n-de eenheidswortels gegeven door $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$. Omdat de verzameling van construeerbare getallen een lichaam is, zijn al deze eenheidswortels construeerbaar als en slechts als ζ_n construeerbaar is. Dus een regelmatige n-hoek is construeerbaar als en slechts als ζ_n construeerbaar is.

Volgens Stelling 5.6 is ζ_n construeerbaar als en slechts als $\mathbb{Q}(\zeta_n)$ verkregen kan worden door een reeks aan tweedegraads lichaamsuitbreidingen, dus

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_k = \mathbb{Q}(\zeta_n)$$

waarbij $[F_i : F_{i-1}] = 2$.
De lichaamsuitbreiding $\mathbb{Q}(\zeta_n)$ is een n-cyclotomische uitbreiding, volgens Stelling 4.22 geldt hiervoor dat $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ een Galois groep is met graad (kardinaliteit) $\phi(n)$.

Als ζ_n construeerbaar is, dan geldt (Stelling 5.6 en Lemma 4.6)

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_1 : F_0]$$

waarbij $[F_i : F_{i-1}] = 2$, en dus $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k$ met k geheel (Stelling 4.18 (1)), dus dan is $n = 2^r p_1 \ldots p_s$ met $p_1, \ldots, p_s$ verschillende oneven Fermat priemgetallen (Lemma 7.6).

We moeten nu nog laten zien dat als $\phi(n) = 2^k$ met k geheel, want dan is ζ_n construeerbaar. Dit doen we door te laten zien dat lichamen $F_0, \ldots, F_k$ bestaan zo dat

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_1 : F_0]$$

en $[F_i : F_{i-1}] = 2$

Om dit te kunnen laten zien moet de Galois groep van de lichaamsuitbreiding $\mathbb{Q}(\zeta_n) : \mathbb{Q}$, genoteerd als $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$, abels zijn en moet $|G|$ een macht van 2 zijn. Als dit het geval is dan is er volgens Lemma 4.23 een reeks groepen $G_0, \ldots, G_k$ zo dat

$$G = G_0 \geq \ldots \geq G_1 \geq G_0 = \{1\}$$

Waarbij $[G_i : G_{i-1}] = 2$.

Lemma 4.12 stelt dat de lichaamsuitbreiding $\mathbb{Q}(\zeta_n) : \mathbb{Q}$ een eindige normale lichaamsuitbreiding is als en slechts als $\mathbb{Q}(\zeta_n)$ een splijtlichaam is voor een polynoom over $\mathbb{Q}$. Het minimaalpolynoom van ζ_n is $x^n - 1$. Dit polynoom splijt over lichaam $\mathbb{Q}(\zeta_n)$, want
(1) het kan uitgedrukt worden als een product van lineaire factoren

$$(x - \zeta_n^0)(x - \zeta_n)(x - \zeta_n^2) \cdots (x - \zeta_n^{n-1})$$

waar $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \in \mathbb{Q}(\zeta_n)$, dit zijn de nulpunten van de polynoom $x^n - 1$.
(2) Het is duidelijk dat $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1})$. Ook geldt $\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1})$ aangezien $1, \zeta_n, \ldots, \zeta_n^{n-1} \in \mathbb{Q}(\zeta_n)$, dus

$\mathbb{Q}(\zeta_n) = \mathbb{Q}(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1})$. (1) en (2) samen geeft dat de de polynoom $x^n - 1$ het lichaam $\mathbb{Q}(\zeta_n)$ splijt (Definitie 4.10). Dus volgens Lemma 4.12 is $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ een eindige normale lichaamsuitbreiding.

We mogen dus Stelling 4.18 (5) gebruiken, dit vertelt ons dat $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Ook vertelt Stelling 4.22 ons dat $(\mathbb{Z}/n\mathbb{Z})^*$ abels is. Volgens Stelling 4.18 (1) geldt dan $|G| = |\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$ wat wij aannemen dat een macht van 2 is. Dus is er een reeks normale groepen $G_0, \ldots, G_k$ zo dat

$$G = G_k \geq \ldots \geq G_1 \geq G_0 = \{1\}$$

Waarbij $|G_i| = 2^i$ (Lemma 4.23).
Maak nu $F_i = G_i^\dagger$ met † zoals gedefinieerd in Hoofdstuk 4 (voor Stelling 4.18). Dan is er volgens Stelling 4.18 (2) een een-op-een correspondentie tussen de groepen G_i en de lichamen F_i, dus is

$$\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_k = \mathbb{Q}(\zeta_n)$$

waarbij $[F_i : F_{i-1}] = |G_i|/|G_{i-1}| = 2$. Maar als dit waar is dan is ζ_n construeerbaar en is n dus constructief.

Dus $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k$ als en slechts als n constructief is.
Volgens Lemma 7.6 is dit waar als en slechts als

$$n = 2^r p_1 \ldots p_s$$

waar r en s gehele getallen zijn en $p_1, \ldots, p_s$ oneven priemgetallen van de vorm

$$p_j = 2^{2^{r_j}} + 1$$

met r_j niet-negatieve gehele getallen. Dus is n constructief als en slechts als n van bovenstaande vorm is. □

8 Nawoord

In dit onderzoek is uitgelegd hoe moderne algebra gebruikt kan worden om meetkundige problemen op te lossen die men vroeger niet kon oplossen. Wiskunde is een vakgebied dat zich constant blijft ontwikkelen en het is mooi om te zien dat problemen die destijds onoplosbaar leken via een compleet andere tak van de wiskunde toch opgelost kunnen worden. Je begint je af te vragen wanneer er oplossingen komen voor problemen die wij nu als onmogelijk beschouwen, zoals P versus NP of , en hoe deze oplossingen er dan uit zullen zien. Een van de mooiere stellingen die gebruikt is in dit verslag vind ik Stelling 5.3 en zijn complexe variant, namelijk dat een getal α construeerbaar is als en slechts als het lichaam $\mathbb{Q}(\alpha)$ uit een reeks tweedegraads lichaamsuitbreidingen verkregen kan worden. Het bewijs hiervan is simpel te volgen, maar toch elegant en deze stelling wordt in het bewijs van Gauss-Wantzel gebruikt om een verbinding te maken tussen de lichaamsuitbreiding $\mathbb{Q}(\zeta_n) : \mathbb{Q}$ en zijn Galois groep.

Als iemand verder gaat met dit literaire onderzoek kan ik zeker nog aanraden om een aantal verschillende regelmatige veelhoeken te construeren. De n-hoeken met hogere n hebben steeds meer stappen nodig, waardoor ik denk dat dit een mooi onderzoek kan zijn. Het is ook nog interessant om onderzoek te doen naar andere soorten meetkunde waarbij het parallellen postulaat van Euclides niet wordt aangenomen, maar een ander postulaat. Een voorbeeld hiervan is de elliptische meetkunde waarbij niet op een vlak, maar op een (elliptische) bol gewerkt wordt, hier is het bijvoorbeeld mogelijk om een driehoek te construeren met drie rechte hoeken.

Tot slot wil ik graag nog mijn begeleider Joost de Groot bedanken voor zijn flexibiliteit en de hulp die hij heeft geboden gedurende dit project. Zijn begeleiding heeft ervoor gezorgd dat ik mijn project op enthousiaste wijze af heb kunnen ronden.

Berend Krouwels
Delft, augustus 2022

Referenties

[1] D. Bailey. *Simple proofs: The impossibility of trisection*. Sep 2018. URL: https://mathscholar.org/2018/09/simple-proofs-the-impossibility-of-trisection/ (bezocht op 14-05-2022).

[2] E. Dijksterhuis. *De Elementen van Euclides*. P. Noordhoff, 1929.

[3] D. Dirkse. *constructies met Passer en Liniaal*. 2022. URL: http://www.davdata.nl/passer_liniaal.html.

[4] R. Fitzpatrick. *Euclid's Elements of Geometry*. 2de ed. 2008.

[5] Inductiveload. *Thales' Theorem*. 2007. URL: https://commons.wikimedia.org/wiki/File:Thales%27_Theorem.svg.

[6] M. Li en C. Boo. *Rational Root Theorem*. URL: https://brilliant.org/wiki/rational-root-theorem/ (bezocht op 29-07-2022).

[7] F. von Lindemann. „Ueber die Zahl π". In: *Mathematische Annalen* 20 (1882), p. 213–225.

[8] J. O'Connor en E. Robertson. *Euclid of Alexandria*. Jan 1999. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Euclid/ (bezocht op 23-08-2022).

[9] J. O'Connor en E. Robertson. *Évariste Galois*. Dec 1996. URL: https://mathshistory.st-andrews.ac.uk/Biographies/Galois/ (bezocht op 23-08-2022).

[10] Plynn9. *Squaring the circle*. 2006. URL: https://commons.wikimedia.org/wiki/File:Squaring_the_circle.svg.

[11] A. Seidenberg. „Did Euclid's Elements, Book I, Develop Geometry Axiomatically?" In: *Archive for History of Exact Sciences* 14.4 (1975), p. 269–271. ISSN: 00039519, 14320657. URL: http://www.jstor.org/stable/41133436 (bezocht op 14-07-2022).

[12] I. Stewart. *Galois Theory*. 4de ed. Chapman & Hall / CRC Press, 2015.

[13] P. Taxel. *Cube and doubled cube*. 2016. URL: https://commons.wikimedia.org/wiki/File:Cube_and_doubled_cube.svg.

[14] E. Weisstein. *Totient Function*. URL: https://mathworld.wolfram.com/TotientFunction.html (bezocht op 19-08-2022).

[15] Will. *Congruent and Similar Triangles*. 2021. URL: https://uptuition.id/congruent-and-similar-triangles/.