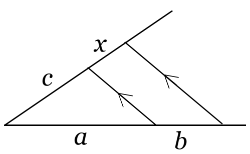
Wat te bewijzen is (56)

Rubriek

Op twaalfjarige leeftijd kreeg ik van mijn tante een langwerpige zwarte doos cadeau. Vol verwachting opende ik het deksel en zie, daar lagen op een bedje van zwart fluweel een passer en nog een paar andere tekenattributen. Ik was er heel verguld mee en nu, na meer dan zestig jaar, ligt die passerdoos nog steeds in de la van mijn bureau, zij het in een wat deplorabele staat en tamelijk werkeloos, want een passer gebruik ik nog zelden. Maar in de meetkundelessen van de eerste klas van de HBS was dat anders. Constructieopgaven, ook wel werkstukken genoemd, verschenen in de les aan de lopende band en ik vond die heel spannend. Het zal de combinatie van denken en handelen geweest zijn die mij aansprak. Mijn leraar was streng en eiste dat we bij de oplossing van zessen klaar waren: *1.gegeven; 2.te construeren; 3.analyse; 4.constructie; 5.bewijs; 6.discussie.* Ja, dat waren nog eens tijden. Over de spelregel dat de enige toegestane instrumenten passer en liniaal (zonder schaalverdeling) waren, bestond geen misverstand. De Griekse oorsprong van die regel bleef achter onze horizon en ik herinner me niet dat er over de klassieke problemen als de verdubbeling van de kubus en de trisectie van de hoek werd verteld.

Construeerbare getallen

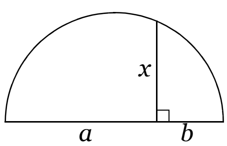
In de schoolboeken kwamen na de basisconstructies (oprichten en neerlaten van een loodlijn, constructie van een bissectrice, enzovoort), constructies van driehoeken vanuit drie gegevens aan bod. Later in de leergang was er aandacht voor constructies gebaseerd op meetkundige plaatsen en weer later, in klas 2 of 3, voor constructies van ‘de vierde evenredige’ en de ‘middelevenredige’. Bij deze laatste twee, die al in boek VI van de *Elementen* van Euclides te vinden zijn (de proposities 12 en 13), sta ik even stil.



$a : b = c : x$

ofwel

$x = \dfrac{bc}{a}$

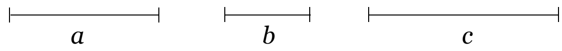


$a : x = x : b$

ofwel

$x = \sqrt{ab}$

De figuren illustreren de analyse bij die constructies. In de uitvoering kunnen de gegeven lijnsegmenten a, b en c op een rechte worden geplaatst met behulp van de passer, kunnen evenwijdige lijnen worden geconstrueerd door overbrenging van overeenkomstige hoeken en zijn de constructie van de halve cirkel op het lijnstuk $a+b$ en de loodlijn op dat lijnstuk gebaseerd op de eigenschap van de middelloodlijn. Deze beide basisconstructies maakten dat er algebra kon binnensluipen in de meetkundeles. In de meeste meetkundeboekjes kon je dan een paragraaf met als kopje ‘constructies van lijnstukken’ vinden. Een voorbeeld van een dergelijke opgave is:



Te construeren:

$$x = \frac{a^2 b}{c^2} \qquad y = \sqrt{a^2 + bc} \qquad z = \sqrt[4]{abc^2}$$

Het ‘tweetrapskarakter’ maakte dat er algebraïsch inzicht nodig is om deze opdracht tot een goed einde te brengen. De hints voor de oplossing kan ik in pure formulevorm geven:

$$x = \frac{a \cdot \frac{ab}{c}}{c} \qquad y = \sqrt{a^2 + (\sqrt{bc})^2} \qquad z = \sqrt{\sqrt{ac} \cdot \sqrt{bc}}$$

met de opmerking dat bij de constructie van y ook de stelling van Pythagoras om de hoek komt kijken. De boekenschrijvers zorgden ervoor dat de algebravormen homogeen en van de eerste graad waren. Maar deze paragraaf was wel een vreemde eend in de bijt van de vlakke meetkunde en ik vermoed dat er leraren waren die dit, in geval van tijdnood, oversloegen. Ik raad ook dat de achtergrond van dit type opgaven terug te voeren is tot de problemen uit de Oudheid die te maken hebben met het al of niet construeerbaar zijn van zekere reële getallen.

Bij het bewijs dat sommige constructies niet lukken met passer en liniaal wordt sinds een paar honderd jaar gebruik gemaakt van het idee dat de *construeerbare reële getallen* (ook wel *Euclidische getallen* genoemd) een *lichaam* vormen. Noem ik de verzameling van zulke getallen nu verder **E**, dan betekent dit dat bij elk paar getallen x, y uit **E** ook $x+y$, $x-y$, $x \cdot y$ en x/y tot **E** behoren. De bewering met betrekking tot product en quotiënt berust op de constructie van een vierde evenredige bij de lijnstukken 1, x en y. De constructie van de middelevenredige maakt dat het lichaam **E** nog een bijzondere eigenschap heeft, namelijk dat bij elk getal uit **E** de vierkantswortel uit dat getal (en daarmee ook de vierde, achtste, zestiende, ... machtswortel) element is van **E**. De derdemachtswortel uit een element van **E** zit in het algemeen niet in **E**, en daarop berust het feit dat zowel de verdubbeling van de kubus als de driedeling van bijvoorbeeld een hoek van 60° niet kan slagen met passer en liniaal.

Constructies en coördinaten

Een constructie met passer en liniaal bestaat uit een eindige keten van constructiestappen, waarbij elke stap een van de volgende vijf handelingen is:

1. *het verbinden van twee punten door een rechte;*
2. *het snijden van twee rechten;*
3. *het tekenen van een cirkel met gegeven middelpunt en gegeven lijnsegment als straal;*
4. *het snijden van een cirkel met een rechte lijn;*
5. *het snijden van twee cirkels.*

Ieder met een beetje ervaring op het gebied van analytische meetkunde snapt dat elk van deze handelingen kan worden uitgevoerd in een cartesisch coördinatensysteem met gegeven lengte-eenheid en dan vertaald kan worden in termen van vergelijkingen. Zo komt handeling 4 algebraïsch neer op het oplossen van een stelsel van de vorm:

$$\begin{cases} x^2 + y^2 + Ax + By + C = 0 \\ Px + Qy + R = 0 \end{cases}$$

waarbij A, B, C, P, Q, R construeerbare getallen zijn. De oplossing ervan leidt tot een vierkantsvergelijking.

Elk punt met rationale coördinaten is – denk aan de constructie van de vierde evenredige – construeerbaar. Bevind ik me nu in het veld van de rationale punten dan kan handeling 4 (en 5) *grensoverschrijdend* zijn, dat wil zeggen, zij kan twee reële punten opleveren buiten het 'rationale veld'. Dat gebeurt als de discriminant (D) van de bijpassende vierkantsvergelijking positief, maar niet het kwadraat van een rationaal getal is.

Op de x-as kan elk getal van de vorm $a + b\sqrt{D}$, met a, b en D rationaal, worden geconstrueerd. De verzameling van deze getallen is gesloten voor optellen, aftrekken, vermenigvuldigen en delen. Voor de operatie delen licht ik dit toe met behulp van een techniek die vroeger uitvoerig werd beoefend op school, namelijk het 'wortelvrij' maken van de noemer:

$$\frac{a + b\sqrt{D}}{p + q\sqrt{D}} = \frac{(a + b\sqrt{D})(p - q\sqrt{D})}{(p + q\sqrt{D})(p - q\sqrt{D})}$$

$$= \frac{(ap - bqD) + (bp - aq)\sqrt{D}}{p^2 - q^2 D}$$

Dat de uitkomst weer van de gewenste vorm is, volgt uit het feit dat de rationale getallen een lichaam (**Q**) vormen. Ik merk nog op dat $p^2 - q^2 D \neq 0$.

De getallen van de vorm $a + b\sqrt{D}$ met a, b, D in **Q** vormen dus zelf ook een lichaam (zeg $\mathbf{L_1}$). Dit nieuwe lichaam omvat **Q** en is een 'deellichaam' van **E**.

In het veld van punten met coördinaten in $\mathbf{L_1}$ kan ik nu ook weer een van de vijf constructiehandelingen uitvoeren. Het is duidelijk dat alleen de handelingen van het type 4 of 5 grensoverschrijdend kunnen zijn. Als dat het geval is, ontstaat er een nieuw lichaam $\mathbf{L_2}$ dat $\mathbf{L_1}$ echt omvat (en deel is van **E**).

Ter illustratie nu eerst even een getallenvoorbeeld. De middelevenredige van de lijnstukken met lengte 1 en 2 levert het getal $\sqrt{2}$, waarvan al zo'n twee-en-een-half millennium bekend is dat het niet in **Q** zit.
$\mathbf{L_1}$ bevat nu de getallen $a + b\sqrt{2}$ met a, b in **Q**.
Nu kan ik bijvoorbeeld de middelevenredige van 1 en $\sqrt{2}$ construeren. Dat $\sqrt{2}$ niet het kwadraat is van een getal uit $\mathbf{L_1}$ is eenvoudig te verifiëren. Immers, uit

$$(a + b\sqrt{2})^2 = \sqrt{2}$$

volgt

$$a^2 + 2b^2 = 0 \text{ en } 2ab = 1$$

en dit stelsel heeft geen oplossingen.
Zo krijg ik een nieuw lichaam $\mathbf{L_2}$ met als elementen de getallen $a_1 + b_1\sqrt[4]{2}$ waarbij a_1, b_1 in $\mathbf{L_1}$.
Vervolgens kan ik bijvoorbeeld de middelevenredige van 1 en $3\sqrt{2} + 5\sqrt[4]{2}$ construeren en komt er een nieuw lichaam $\mathbf{L_3}$ met als elementen de getallen

$$a_2 + b_2\sqrt{3\sqrt{2} + 5\sqrt[4]{2}}$$

waarbij a_2, b_2 in $\mathbf{L_2}$.
Zo kan ik eindeloos doorgaan met het toevoegen van grensoverschrijdende construeerbare getallen. Maar hoe je het ook in het vat giet, een getal als $\sqrt[3]{2}$ krijg je daarmee niet te pakken. Dat zal ik nu aantonen.

Verdubbeling van de kubus

Een bewijs van onmogelijkheid is bijna per definitie een bewijs uit het ongerijmde. Dus stel ik dat $\sqrt[3]{2}$ in een eindig aantal stappen te construeren is, startend vanuit een lijnstuk met lengte 1 en moet ik aantonen dat dit onherroepelijk tot tegenspraak voert.

Bij elke grensoverschrijdende constructiestap is er sprake van de constructie van een vierkantswortel uit een element van een deellichaam van **E**.

Wil $\sqrt[3]{2}$ een element van **E** zijn, dan moet er een opklimmende rij **Q**, $\mathbf{L_1}$, $\mathbf{L_2}$, ... , $\mathbf{L_{n+1}}$ van deellichamen van **E** bestaan, zodat $\sqrt[3]{2}$ in $\mathbf{L_{n+1}}$ ligt, maar niet in het daaraan voorafgaande lichaam $\mathbf{L_n}$. Dat betekent dat

$$\sqrt[3]{2} = a_n + b_n\sqrt{D_n}$$

met a_n, b_n, D_n in $\mathbf{L_n}$ en $b_n \neq 0$ en $D_n > 0$ en ook dat $\sqrt{D_n}$ in $\mathbf{L_{n+1}}$, maar niet in $\mathbf{L_n}$ ligt.

Uit $(a_n + b_n\sqrt{D_n})^3 = 2$ volgt na uitwerken

$$\begin{cases} a_n^3 + 3a_n b_n^2 D_n = 2 \\ 3a_n^2 b_n + b_n^3 D_n = 0 \end{cases}$$

Omdat $b_n \neq 0$ is de tweede relatie equivalent met

$$3a_n^2 + b_n^2 D_n = 0$$

hetgeen wegens $D_n > 0$ een conflict geeft.
Zo is met elementaire algebra bewezen dat $\sqrt[3]{2}$ niet in een eindig aantal stappen met passer en liniaal kan worden geconstrueerd.

De derdegraadsvergelijking

De onmogelijkheid van de constructie van $\sqrt[3]{2}$ is een bijzonder geval ($p = 0$, $q = 2$) van deze stelling
Als x_1 *een irrationale wortel is van de vergelijking* $x^3 = px + q$ *met* p, q *rationaal, dan behoort* x_1 *niet tot* **E**.
Bij het bewijs van deze stelling kan deels dezelfde weg worden gevolgd.

Het gaat nu dus om de vergelijking

$$x^3 = px + q$$

waarbij p en q rationaal zijn en waarbij bovendien geen van de oplossingen een rationaal getal is.

Veronderstel nu dat x_1, x_2, x_3 de wortels zijn van de vergelijking. Ten minste één daarvan is reëel, de twee andere kunnen óf reëel óf toegevoegd complex zijn.
Zeker is dat geldt $x_1 + x_2 + x_3 = 0$, als gevolg van de identiteit:

$$x^3 - px - q = (x - x_1)(x - x_2)(x - x_3)$$

Stel dat $n(n \geq 1)$ het *kleinste* getal is waarvoor een reële wortel van de vergelijking kan worden geconstrueerd via een rijtje van de lichamen **Q**, $\mathbf{L_1}$, $\mathbf{L_2}$, ..., $\mathbf{L_{n+1}}$ (*)
Voor de betreffende wortel (zeg x_1) geldt dan:

$$x_1 = a_n + b_n\sqrt{D_n}$$

waarbij a_n, b_n en D_n aan dezelfde condities voldoen als in het geval van de verdubbeling van de kubus.
Substitutie van x_1 in de vergelijking levert op:

$$\begin{cases} a_n^3 + 3a_n b_n^2 D_n = pa_n + q \\ 3a_n^2 b_n + b_n^3 D_n = pb_b \end{cases}$$

In de tweede betrekking kan b_n worden uitgedeeld en dan bevatten beide vergelijkingen slechts een even macht van b_n. Het gevolg daarvan is dat er nog twee irrationale wortels moeten zijn. Eén daarvan is

$$x_2 = a_n - b_n\sqrt{D_n}$$

Immers, substitutie hiervan in $x^3 = px + q$ geeft dezelfde twee betrekkingen als na substitutie van x_1.
Omdat $x_1 + x_2 + x_3 = 0$ volgt nu dat $x_3 = -2a_n$.

Maar dat betekent dat x_3 in $\mathbf{L_n}$ zit en dat is nu juist in tegenspraak met de veronderstelling (*).

De trisectie van de hoek

In december 1997 ontmoette ik tijdens een congres in Cochabamba een enthousiaste Boliviaanse wiskundeleraar die mij zijn oplossing van de driedeling van de hoek wilde demonstreren. Van een groot stuk papier vouwde hij heel handig een liniaal, prikte daar in de uiteinden gaatjes in zodat hij hem ook als passer kon gebruiken en maakte op het schoolbord razendsnel een indrukwekkende constructie. Het kostte mij flink wat moeite om de vinger op de zere plek te leggen, maar hoe moest ik hem overtuigen dat bijvoorbeeld een hoek van 60° niet met passer en liniaal eerlijk in drieën kan worden verdeeld? De formule:

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

begreep hij heel goed. Dat een hoek van 20° alleen dan kan worden geconstrueerd als het getal cos20° op de getallenlijn kan worden geconstrueerd, snapte hij ook. En het was een ministapje dat dit neerkomt op de construeerbaarheid van een wortel van de vergelijking

$$4x^3 - 3x = \tfrac{1}{2}$$

Toen werd het moeilijk voor mij en kon ik hem alleen, denkend aan een artikel van A.W. Grootendorst in *Euclides* jaargang 58, nog een vaag verhaal vertellen over Wantzel die in 1837 via irreducibele polynomen en lichaamsuitbreidingen de onmogelijkheid bewees. Verwijzing naar de zogenaamde Galois-theorie had natuurlijk geen zin. Zijn gelaatsuitdrukking verried dat hij mij wel op gezag wilde geloven, maar dat is toch wat je in wiskunde juist niet wil...

Met mijn kennis van nu (welke politicus zei dat ook al weer?) had ik een beter figuur kunnen slaan. De hier eerder behandelde stelling leidt direct tot uitsluitsel. Voor het gemak herschrijf ik de vergelijking (via de substitutie $2x = y$) als $y^3 = 3y + 1$.

Het enige wat nog moet gebeuren, is nagaan of deze vergelijking een rationale wortel kan hebben. Stel s/t is een onvereenvoudigbare breuk (dat wil zeggen met gehele teller en noemer die relatief priem zijn) die een wortel is van bovenstaande *y*-vergelijking.

Substitutie geeft: $s^3 = 3st^2 + t^3$ (**).

Hieruit volgt dat t een deler is van s, dus vanwege de onderlinge ondeelbaarheid van s en t geldt $t = 1$.
Net zo volgt $s = 1$, maar substitutie van $s = t = 1$ in (**) geeft 1 = 4. Klaar.

Martin Kindt, M.Kindt@uu.nl