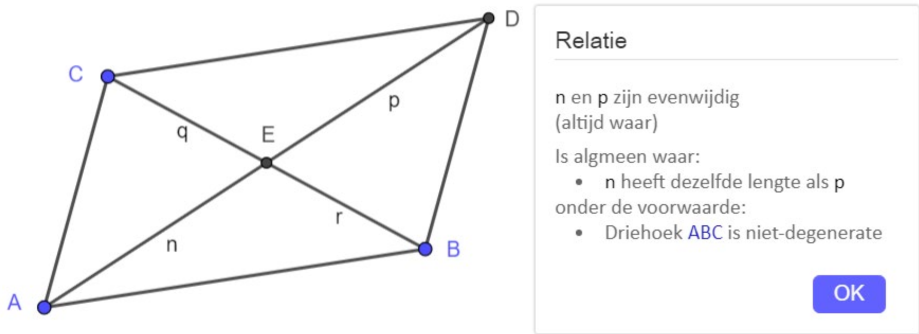
Een andere dimensie van GeoGebra

André Heck
Korteweg-de Vries Instituut
Universiteit van Amsterdam
a.j.p.heck@uva.nl

Samenvatting

Met GeoGebra kun je relaties tussen meetkundige objecten numeriek verifiëren. Maar de software kan ook op eigen kracht relaties bewijzen en hierbij condities opstellen. Onderstaande schermafdruk illustreert bijvoorbeeld dat GeoGebra zonder hulp van buiten kan bewijzen dat in een parallellogram het snijpunt van de diagonalen elk van deze diagonalen in stukken van gelijke lengte verdeelt.



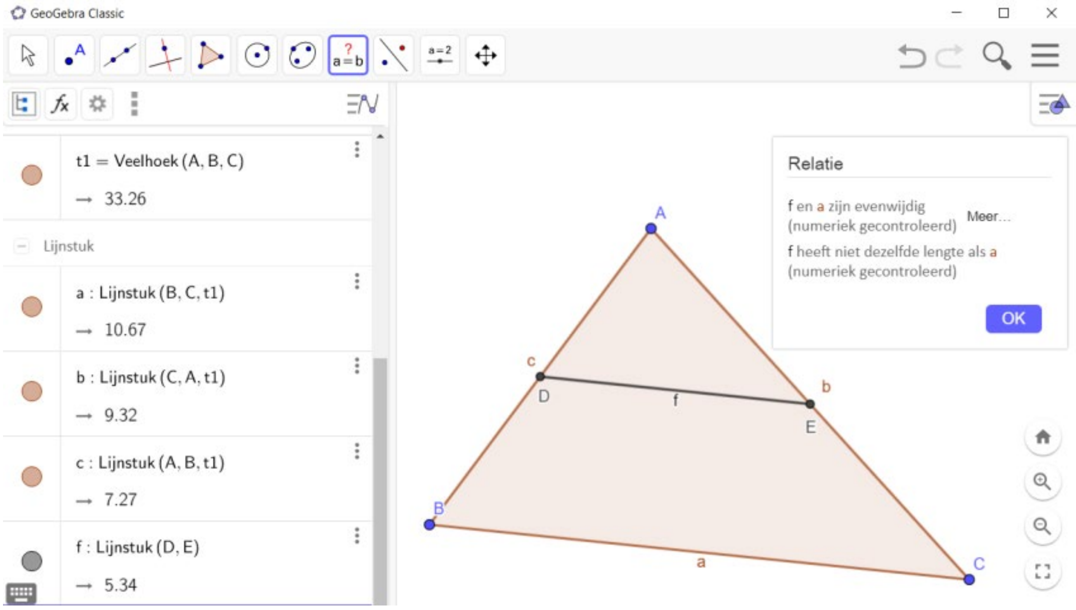
We gaan diverse voorbeelden van geautomatiseerde bewijsvoering van meetkundige stellingen bespreken en onder de motorkap van GeoGebra kijken hoe dat dan gedaan wordt. We lichten alvast een tipje van de sluier op: een meetkundige stelling in het platte valk wordt via coördinaten getranscribeerd naar een algebraïsch probleem in een hoog-dimensionale ruimte. Met wiskundig geschut kan zo'n probleem soms opgelost worden en tevens noodzakelijke voorwaarden opgesteld worden. Omgekeerd kun je via deze computerondersteund analytische aanpak meetkundige stellingen ontdekken. Ook dit illustreren we met voorbeelden. Het onthullen en bewijzen van meetkundige stellingen is zo van een heel andere dimensie dan gebruikelijk is in vlakke meetkunde.

Inleidende voorbeelden

Stelling 1

Stel ABC is een driehoek, D is het midden van de zijde AB, en E is het midden van de zijde AC. Dan is het segment DE evenwijdig aan de zijde BC en is de lengte van DE gelijk aan de helft van de lengte van BC.

GeoGebra heeft het gereedschap RELATIE om numeriek eigenschappen te verifiëren. Onderstaande schermafdruk laat zien dat de evenwijdigheid gecontroleerd kan worden, maar dat het pakket alleen de ongelijkheid van de lengte van het lijnstuk *DE* en de lengte van de zijde *BC* kan achterhalen. Dit komt omdat de verificatie numeriek gedaan wordt en er dan afrondingsfouten kunnen optreden (zie: *BC*=10.67, *DE*=5.34).



Klik je vervolgens op de MEER knop in de Relatie-uitvoer, dan wordt het BEWIJS-gereedschap in GeoGebra aangeroepen en kan het pakket zelfstandig de evenwijdigheid van lijnstuk en zijde aantonen: de boodschap (NUMERIEK GECONTROLEERD) verandert dan in (ALTIJD WAAR). Er is dan sprake van **geautomatiseerde bewijsvoering van meetkundige stellingen**.

De vraag die we ons stellen is hoe GeoGebra zo'n stellige uitspraak over evenwijdigheid kan doen en waarom het niet de relatie tussen de lengtes kan bewijzen.

Om te achterhalen wat Geogebra op de achtergrond doet, starten we het programma in een Windows POWERSHELL met argument --LOGLEVEL=INFO. We doen de constructie dan over en krijgen meer details te zien (zie onderstaande schermafdruk).

De precieze tekst in het logboek is niet belangrijk, maar we zien wel dat GeoGebra een algebraïsche bewijsmethode kiest en uitvoert. De meetkundige context wordt vertaald in vergelijkingen opgebouwd met generieke coördinaten van punten in de meetkundige figuur. We hebben bijvoorbeeld $A = (v_7, v_8), B = (v_9, v_{10}), C = (v_{11}, v_{12}), D = (v_{13}, v_{14}), E = (v_{15}, v_{16})$ en daarbij worden hypothesen opgesteld zoals $2v_{13} = v_7 + v_9$ en $2v_{14} = v_8 + v_{10}$ voor het punt *D*, zijnde het midden van *AB*. Uit de hypothesen moet de evenwijdigheid van *DE* en *AB* afgeleid kunnen worden en dit wordt ook vertaald in algebraïsche zin: $\frac{v_{16}-v_{14}}{v_{15}-v_{13}} = \frac{v_{12}-v_{10}}{v_{11}-v_9}$ (gelijke hellingen). Als veeltermvergelijking kun je dit herschrijven als

$$(v_{15} - v_{13})(v_{12} - v_{10}) - (v_{16} - v_{14})(v_{11} - v_9) = 0.$$

In de schermafdruk zijn de haakjes in de veelterm aan de linkerkant weggewerkt. Om de evenwijdigheid te bewijzen moet je dus de veeltermvergelijking uit de hypothesen kunnen afleiden. In het BEWIJS-gereedschap binnen GeoGebra is de aanpak anders, namelijk REDUCTIO AB ADSURDUM: nu wordt aangetoond dat

$$(v_{15} - v_{13})(v_{12} - v_{10}) - (v_{16} - v_{14})(v_{11} - v_9) \neq 0$$

leidt tot een tegenspraak. Deze ongelijkheid wordt vertaald via de zogeheten **truc van Rabinowitsch** in een veeltermvergelijking door een extra variabele v_{22} in te voeren:

$$\big((v_{15} - v_{13})(v_{12} - v_{10}) - (v_{16} - v_{14})(v_{11} - v_9)\big) \cdot v_{22} - 1 = 0.$$

In de schermafdruk kun je ook nog zien dat GeoGebra gebruik maakt van het gegeven dat een meetkundige stelling niet verandert wanneer je de meetkundige figuur transleert. Om deze reden kun je voor *A* het punt (0,0) nemen. Dit scheelt twee variabelen in het algebraïsch rekenen. Maar nog steeds heb je dan 9 variabelen en 5 vergelijkingen. De oorspronkelijke vraagstelling in de tweedimensionale ruimte $\mathbb{R}^2$ is hiermee getranscribeerd naar een probleem in de 9-dimensionale ruimte $\mathbb{R}^9$, waarin bewezen moet worden dat een stelsel van veeltermvergelijkingen een lege oplossingsverzameling heeft. We zullen later zien dat het bewijs geleverd kan worden door de gereduceerde Gröbner basis van een stelsel veeltermvergelijkingen uit te rekenen en op te merken dat deze gelijk is aan {1}.

```
Windows PowerShell
GeoGebra: 8:43:6 DEBUG: ?: A = (0.59, 2.71) /* free point */
GeoGebra: 8:43:6 DEBUG: ?: // Free point A(v7,v8)
GeoGebra: 8:43:6 DEBUG: ?: v7 is free
GeoGebra: 8:43:6 DEBUG: ?: v8 is free
GeoGebra: 8:43:6 DEBUG: ?: B = (-3.21, -1.89) /* free point */
GeoGebra: 8:43:6 DEBUG: ?: // Free point B(v9,v10)
GeoGebra: 8:43:6 DEBUG: ?: v9 is free
GeoGebra: 8:43:6 DEBUG: ?: v10 is free
GeoGebra: 8:43:6 DEBUG: ?: C = (6.25, -3.45) /* free point */
GeoGebra: 8:43:6 DEBUG: ?: // Free point C(v11,v12)
GeoGebra: 8:43:6 DEBUG: ?: v11 is free
GeoGebra: 8:43:6 DEBUG: ?: v12 is free
GeoGebra: 8:43:6 DEBUG: ?: f1 = Polygon[A, B, C] /* Polygon A, B, C */
GeoGebra: 8:43:6 DEBUG: ?: a = Segment[B, C, f1] /* Segment B, C */
GeoGebra: 8:43:6 DEBUG: ?: D = Midpoint[A, B] /* Midpoint of A, B */
GeoGebra: 8:43:6 DEBUG: ?: // Constrained point D(v13,v14)
GeoGebra: 8:43:6 DEBUG: ?: Hypotheses:
GeoGebra: 8:43:6 DEBUG: ?: Adding poly #1: 2v_{13}-v_{9}-v_{7}
GeoGebra: 8:43:6 DEBUG: ?: Adding poly #2: 2v_{14}-v_{10}-v_{8}
GeoGebra: 8:43:6 DEBUG: ?: E = Midpoint[A, C] /* Midpoint of A, C */
GeoGebra: 8:43:6 DEBUG: ?: // Constrained point E(v15,v16)
GeoGebra: 8:43:6 DEBUG: ?: Hypotheses:
GeoGebra: 8:43:6 DEBUG: ?: Adding poly #3: 2v_{15}-v_{11}-v_{7}
GeoGebra: 8:43:6 DEBUG: ?: Adding poly #4: 2v_{16}-v_{12}-v_{8}
GeoGebra: 8:43:6 DEBUG: ?: f = Segment[D, E] /* Segment D, E */
GeoGebra: 8:43:6 DEBUG: ?: Processing numerical object
GeoGebra: 8:43:6 DEBUG: ?: Hypotheses have been processed.
GeoGebra: 8:43:6 DEBUG: ?: Thesis equations (non-denied ones):
GeoGebra: 8:43:6 DEBUG: ?: Thesis reductio ad absurdum (denied statement), product of factors:
GeoGebra: 8:43:6 DEBUG: ?: (v15*v12-v13*v12-v16*v11+v14*v11-v15*v10+v13*v10+v16*v9-v14*v9)*v17-1
GeoGebra: 8:43:6 DEBUG: ?: Adding poly #5: -1+v_{17}v_{15}v_{12}-v_{17}v_{13}v_{12}-v_{17}v_{16}v_{11}+v_{17}v_{14}v_{11
}-v_{17}v_{15}v_{10}+v_{17}v_{13}v_{10}+v_{17}v_{16}v_{9}-v_{17}v_{14}v_{9}
GeoGebra: 8:43:6 DEBUG: ?: substitutions: {v7=0, v8=0}
GeoGebra: 8:43:6 DEBUG: ?: Eliminating system in 9 variables (5 dependent)
GeoGebra: ============== restarted ===============
GeoGebra: 8:43:6 DEBUG: ?: input = [[ff:=""],[aa:=eliminate([2*v13-v9,2*v14-v10,2*v15-v11,2*v16-v12,-1+v17*v15*v12-v17*v
13*v12-v17*v16*v11+v17*v14*v11-v17*v15*v10+v17*v13*v10+v17*v16*v9-v17*v14*v9],revlist([v13,v14,v15,v16,v17]))],[bb:=size
(aa)],[for ii from 0 to bb-1 do ff+=("["+(ii+1)+"]: [1]:  unicode95uunicode91u1]=1");cc:=factors(aa[ii]);dd:=size(cc);fo
r jj from 0 to dd-1 by 2 do ff+=("  unicode95uunicode91u"+(jj/2+2)+"]="+cc[jj]); od; ff+=(" [2]: "+cc[1]);for kk from 1
to dd-1 by 2 do ff+=(","+cc[kk]);od;od],[if(ff=="") begin ff:=[0] end],ff][5]
GeoGebra: 8:43:6 DEBUG: ?: result = [1]: [1]:  unicode95uunicode91u1]=1  unicode95uunicode91u2]=1 [2]: 1,1
GeoGebra: 8:43:6 DEBUG: ?: Considering NDG 1...
GeoGebra: 8:43:6 DEBUG: ?: Found a better NDG score (0) than Infinity
GeoGebra: 8:43:6 DEBUG: ?: Statement is GENERALLY TRUE
GeoGebra: 8:43:6 DEBUG: ?: Benchmarking: 120 ms
GeoGebra: 8:43:6 DEBUG: ?: STATEMENT IS TRUE (yes/no: TRUE)
GeoGebra: 8:43:6 DEBUG: ?: OUTPUT for ProveDetails: undefined = {true}
```

We gaan eerst eens zelf aan de slag om een algebraïsch bewijs van de stelling te leveren. We doen dit op een manier die qua notatie voorbereidt op een algemene aanpak.

We beginnen met een driehoek *ABC* waarvan de hoekpunten vrije coördinaten hebben: $A(u_1, u_2), B(u_3, u_4)$ en $C(u_5, u_6)$. Hoe vrij deze keuze werkelijk is zullen we later bekijken. De middens *D* en *E* van de twee zijden *AB* en *AC* van de driehoek *ABC* hebben coördinaten die afhangen van de eerdere coördinaten. Zeg $D(x_1, x_2)$ en $E(x_3, x_4)$, dan hebben we vier vergelijkingen die de constructie van de meetkundige figuur beschrijven:

$$2x_1 = u_1 + u_3,\ \ 2x_2 = u_2 + u_4,\ \ 2x_3 = u_1 + u_5\ ,\ \ 2x_4 = u_2 + u_6$$

Evenwijdigheid levert (kijk naar verhoudingen van coördinaten van richtingsvectoren $\overrightarrow{DE}$ en $\overrightarrow{BC}$):

$$(x_4 - x_2)(u_5 - u_3) - (x_3 - x_1)(u_6 - u_4) = 0$$

Het bewijs komt er op neer dat je controleert dat de laatste vergelijking klopt voor variabelen die voldoen aan de eerste 4 vergelijkingen. Als je x_1, x_2, x_3, x_4 vervangt in de laatste vergelijking door de bijpassende uitdrukkingen uit de eerste 4 vergelijkingen en haakjes wegwerkt, dan krijg je 0=0.

Merk op dat het gegeven dat *ABC* een driehoek is, en dat de hoekpunten dus verschillend en niet op één lijn liggend verondersteld worden, niet in de algebraïsche vertaling verwerkt is. Dit betekent dat de coördinaten van de punten minder vrij zijn dan aanvankelijk gesuggereerd is. Ook de terug-vertaling van de vergelijking $(x_4 - x_2)(u_5 - u_3) - (x_3 - x_1)(u_6 - u_4) = 0$ is eigenlijk niet even-wijdigheid, maar de bewering *B=C* of *D=E* of *DE* is evenwijdig met *BE*.

We hebben op algebraïsche wijze dus eigenlijk het volgende aangetoond:

Stel D is het midden van een lijnstuk AB en E is het midden van een lijnstuk AC, dan is DE evenwijdig met BC, of B=C of D=E.

Omdat $D \neq E$ volgt uit $B \neq C$, kunnen we ook schrijven:

Stel B en C zijn verschillende punten, stel A is niet een punt op de lijn door B en C, en stel D is het midden van een lijnstuk AB en E is het midden van een lijnstuk AC, dan is DE evenwijdig BC.

Opgave 1: Bewijs algebraïsch dat de lengte van *DE* gelijk is aan de helft van de lengte van *BC, oftewel dat* $d(B.C)$.

Opgave 2: De meeste meetkundige eigenschappen zijn invariant onder verschuiving en draaiing van de meetkundige figuur. Ga na dat het algebraïsche bewijs bijna een trivialiteit wordt als je veronder-stelt dat *B* de oorsprong is en *C* een punt op de x-as is; we nemen dus $B(0,0)$ en $C(u_5, 0)$ als uit-gangspunt.

We kijken nog wat verder naar het voorbeeld en schrijven de vier vergelijkingen die de constructie van de meetkundige figuur beschrijven op als

$$2x_1 - u_1 - u_3 = 0,\ \ 2x_2 - u_2 - u_4 = 0,\ \ 2x_3 - u_1 - u_5 = 0,\ \ 2x_4 - u_2 - u_6 = 0.$$

We nemen nu de vier linkerzijden en beschouwen deze als veeltermen $H_1,\ H_2,\ H_3,\ H_4$:

$$H_1 = 2x_1 - u_1 - u_3,\ \ H_2 = 2x_2 - u_2 - u_4,\ \ H_3 = 2x_3 - u_1 - u_5,\ \ H_4 = 2x_4 - u_2 - u_6$$

De linkerzijde van de regel voor evenwijdigheid is de veelterm S gegeven door

$$S = (x_4 - x_2)(u_5 - u_3) - (x_3 - x_1)(u_6 - u_4)$$

en die laat zich herschrijven (ga dit zelf na!) als

$$S = \tfrac{1}{2}(u_5 - u_3)(H_4 - H_2) - \tfrac{1}{2}(u_6 - u_4)(H_3 - H_1)$$

In wiskundige terminologie kunnen we zeggen: De veelterm S is element van het ideaal voortge-bracht door de veeltermen H_1, H_2, H_3, H_4. Een punt $(u_1, u_2, u_3, u_4, u_5, u_6, x_1, x_2, x_3, x_4)$ dat nulpunt is van elk van de 4 veeltermen H_1, H_2, H_3, H_4 is dan vanzelf ook een nulpunt van de veelterm S.

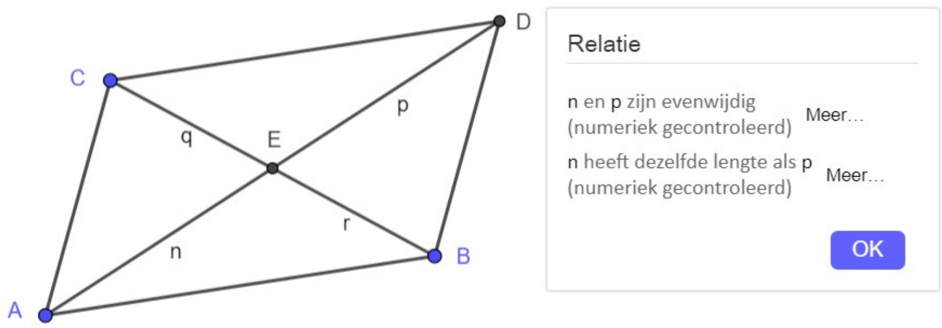
Stelling 2

In een parallellogram verdeelt het snijpunt van de diagonalen elk van deze diagonalen in twee stukken van gelijke lengte.

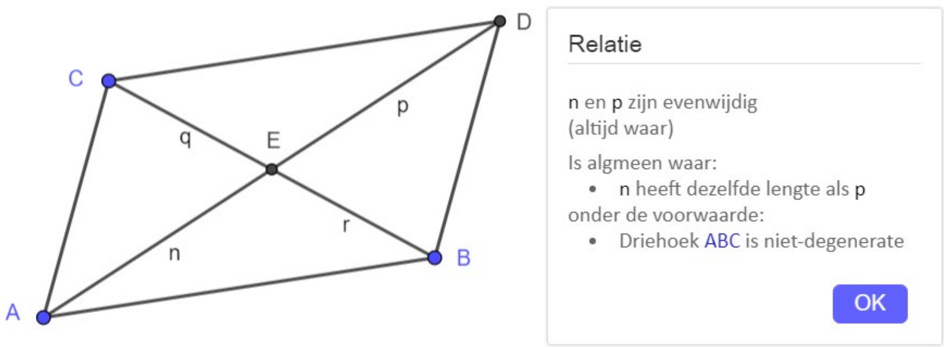
We hebben onderstaande meetkundige tekening op de volgende manier geconstrueerd

1. Teken een lijnstuk *AB*
2. Teken een lijnstuk *AC* met een andere richting dan *AB*
3. Construeer een rechte lijn door *C* parallel aan het lijnstuk *AB*
4. Construeer een rechte lijn door *B* parallel aan het lijnstuk *AC*
5. Construeer het snijpunt *D* van de twee rechte lijnen
6. Maak de lijnen onzichtbaar
7. Teken de lijnstukken *CD* en *BD*
8. Teken de diagonalen *AD* en *BC*
9. Construeer het snijpunt E van de twee diagonalen
10. Maak de diagonalen onzichtbaar
11. Teken de lijnstukken *AE*, *ED*, *CE* en *EB*

We vragen met het Relatie-gereedschap bekende eigenschappen van de lijnstukken *AE* en *ED* op: numeriek kan GeoGebra achterhalen dat de lijnstukken evenwijdig zijn en gelijke lengte hebben



Drukken we op de Meer knoppen in de Relatie-uitvoer, dan wordt het Bewijs-gereedschap in GeoGebra aangeroepen en kan het pakket zelfstandig de evenwijdigheid van de lijnstukken en de gelijkheid van lengtes bepalen: de boodschap (numeriek gecontroleerd) verandert dan voor evenwijdigheid in (altijd waar). Voor de gelijkheid van lengtes is de uitspraak ingewikkelder: het is in het algemeen waar, namelijk onder de voorwaarde dat de driehoek *ABC* niet-ontaard is. [1]



[1] In de Nederlandse vertaling van GeoGebra staan taalfouten en is de naamgeving niet altijd even voorspelbaar. Als het in praktijk kan, is gebruik van de Engelse versie aan te raden.

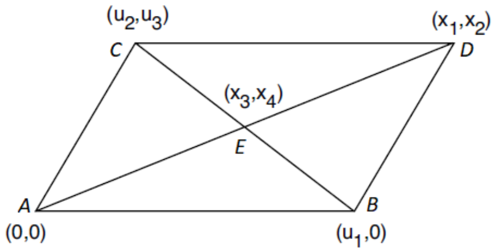
Windows PowerShell

```
GeoGebra: 9:32:45 DEBUG: ?: // Free point A(v1,v2)
GeoGebra: 9:32:45 DEBUG: ?: v1 is free
GeoGebra: 9:32:45 DEBUG: ?: v2 is free
GeoGebra: 9:32:45 DEBUG: ?: B = (0.91, -0.65) /* free point */
GeoGebra: 9:32:45 DEBUG: ?: // Free point B(v3,v4)
GeoGebra: 9:32:45 DEBUG: ?: v3 is free
GeoGebra: 9:32:45 DEBUG: ?: v4 is free
GeoGebra: 9:32:45 DEBUG: ?: f = Segment[A, B] /* Lijnstuk [A, B] */
GeoGebra: 9:32:45 DEBUG: ?: C = (-5.29, 2.87) /* free point */
GeoGebra: 9:32:45 DEBUG: ?: // Free point C(v5,v6)
GeoGebra: 9:32:45 DEBUG: ?: v5 is free
GeoGebra: 9:32:45 DEBUG: ?: v6 is free
GeoGebra: 9:32:45 DEBUG: ?: g = Segment[A, C] /* Lijnstuk [A, C] */
GeoGebra: 9:32:45 DEBUG: ?: h = Line[C, f] /* Rechte door C evenwijdig met f */
GeoGebra: 9:32:45 DEBUG: ?: Hypotheses:
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #1: v_{7}-v_{5}-v_{3}+v_{1}
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #2: v_{8}-v_{6}-v_{4}+v_{2}
GeoGebra: 9:32:45 DEBUG: ?: i = Line[B, g] /* Rechte door B evenwijdig met g */
GeoGebra: 9:32:45 DEBUG: ?: Hypotheses:
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #3: v_{9}-v_{5}-v_{3}+v_{1}
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #4: v_{10}-v_{6}-v_{4}+v_{2}
GeoGebra: 9:32:45 DEBUG: ?: D = Intersect[h, i] /* Doorsnede van h en i */
GeoGebra: 9:32:45 DEBUG: ?: // Constrained point D(v11,v12)
GeoGebra: 9:32:45 DEBUG: ?: Hypotheses:
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #5: v_{11}v_{8}-v_{12}v_{7}-v_{11}v_{6}+v_{7}v_{6}+v_{12}v_{5}-v_{8}v_{5}
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #6: v_{11}v_{10}-v_{12}v_{9}-v_{11}v_{4}+v_{9}v_{4}+v_{12}v_{3}-v_{10}v_{3}
GeoGebra: 9:32:45 DEBUG: ?: l = Segment[C, B] /* Lijnstuk [C, B] */
GeoGebra: 9:32:45 DEBUG: ?: m = Segment[A, D] /* Lijnstuk [A, D] */
GeoGebra: 9:32:45 DEBUG: ?: E = Intersect[l, m] /* Doorsnede van l en m */
GeoGebra: 9:32:45 DEBUG: ?: // Constrained point E(v13,v14)
GeoGebra: 9:32:45 DEBUG: ?: Hypotheses:
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #7: v_{13}v_{6}-v_{14}v_{5}-v_{13}v_{4}+v_{5}v_{4}+v_{14}v_{3}-v_{6}v_{3}
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #8: -v_{13}v_{12}+v_{14}v_{11}+v_{13}v_{2}-v_{11}v_{2}-v_{14}v_{1}+v_{12}v_{1}
GeoGebra: 9:32:45 DEBUG: ?: n = Segment[A, E] /* Lijnstuk [A, E] */
GeoGebra: 9:32:45 DEBUG: ?: p = Segment[E, D] /* Lijnstuk [E, D] */
GeoGebra: 9:32:45 DEBUG: ?: Processing numerical object
GeoGebra: 9:32:45 DEBUG: ?: Hypotheses have been processed.
GeoGebra: 9:32:45 DEBUG: ?: Thesis equations (non-denied ones):
GeoGebra: 9:32:45 DEBUG: ?: Thesis reductio ad absurdum (denied statement), product of factors:
GeoGebra: 9:32:45 DEBUG: ?: (2*v14*v12-v12^2+2*v13*v11-v11^2-2*v14*v2+v2^2-2*v13*v1+v1^2)*v20-1
GeoGebra: 9:32:45 DEBUG: ?: Adding poly #9: -1+2v_{20}v_{14}v_{12}-v_{20}v_{12}^{2}+2v_{20}v_{13}v_{11}-v_{20}v_{11}^{2}
-2v_{20}v_{14}v_{2}+v_{20}v_{2}^{2}-2v_{20}v_{13}v_{1}+v_{20}v_{1}^{2}
GeoGebra: 9:32:45 DEBUG: ?: substitutions: {v1=0, v2=0}
GeoGebra: 9:32:45 DEBUG: ?: Eliminating system in 13 variables (9 dependent)
GeoGebra: ============== restarted ===============
GeoGebra: Running a probabilistic check for the reconstructed Groebner basis. If successfull, error probability is less
than 1e-07 and is estimated to be less than 10^-16. Use proba_epsilon:=0 to certify (this takes more time).
GeoGebra: // Groebner basis computation time 1.55064e+06 Memory -1e-06M
GeoGebra: 9:32:45 DEBUG: ?: input = [[ff:=""],[aa:=eliminate([v7-v5-v3,v8-v6-v4,v9-v5-v3,v10-v6-v4,v11*v8-v12*v7-v11*v6+
v7*v6+v12*v5-v8*v5,v11*v10-v12*v9-v11*v4+v9*v4+v12*v3-v10*v3,-v13*v12+v14*v11,v13*v6-v14*v5-v13*v4+v5*v4+v14*v3-v6*v3,-1
+2*v20*v14*v12-v20*v12^2+2*v20*v13*v11-v20*v11^2],revlist([v7,v8,v9,v10,v11,v12,v13,v14,v20]))],[bb:=size(aa)],[for ii f
rom 0 to bb-1 do ff+=("["+(ii+1)+"]: [1]:  unicode95uunicode91u1]=1");cc:=factors(aa[ii]);dd:=size(cc);for jj from 0 to
dd-1 by 2 do ff+=("  unicode95uunicode91u"+(jj/2+2)+"]="+cc[jj]); od; ff+=(" [2]: "+cc[1]);for kk from 1 to dd-1 by 2 do
 ff+=(","+cc[kk]);od;od],[if(ff=="") begin ff:=[0] end],ff][5]
GeoGebra: 9:32:45 DEBUG: ?: result = [1]: [1]:  unicode95uunicode91u1]=1  unicode95uunicode91u2]=v4*v5-v6*v3 [2]: 1,1
GeoGebra: 9:32:45 DEBUG: ?: Considering NDG 1...
GeoGebra: 9:32:45 DEBUG: ?: Trying to detect polynomial v5*v4-v6*v3
GeoGebra: 9:32:45 DEBUG: ?: v5*v4-v6*v3 means collinearity for [A = (-6.73, -2.27), B = (0.91, -0.65), C = (-5.29, 2.87)
]
GeoGebra: 9:32:45 DEBUG: ?: Found a better NDG score (1) than Infinity
GeoGebra: 9:32:45 DEBUG: ?: Statement is GENERALLY TRUE
GeoGebra: 9:32:45 DEBUG: ?: Benchmarking: 52 ms
GeoGebra: 9:32:45 DEBUG: ?: STATEMENT IS TRUE (yes/no: TRUE)
GeoGebra: 9:32:45 DEBUG: ?: OUTPUT for ProveDetails: undefined = {true, {"Driehoek <b><font color="#1B1BCD">A</font></b>
<b><font color="#1B1BCD">B</font></b><b><font color="#1B1BCD">C</font></b> is niet-degenerate"}}
```

Er is dus echt sprake van geautomatiseerde bewijsvoering van meetkundige stellingen, met tegelijkertijd precies uitzoeken onder welke voorwaarden de bewering waar is. Natuurlijk hadden we een niet-ontaarde driehoek ABC in gedachten, maar het computerprogramma kan onze gedachten niet raden en moet extra zijn best doen om correctheid aan te tonen en zo nodig voorwaarden af te leiden. In het volgende logboek van GeoGebra, dat gestart is in een Windows POWERSHELL met het argument --LOGLEVEL=INFO, kunnen we veel van bovenstaande terugvinden.

De precieze tekst in het logboek is niet belangrijk, maar we zien in onderstaande schermafdruk wel dat GeoGebra een algebraïsche bewijsmethode kiest en uitvoert, namelijk een methode gebaseerd op het gebruik van een zogenaamde **gereduceerde Gröbner basis**. Ook is in het scherm te zien dat een randvoorwaarde in de gedaante van een veelterm-ongelijkheid bepaald wordt: met de coördinaten $A(0,0), B(v_5,v_6), C(v_7,v_8)$ moet kennelijk gelden dat $v_7v_6 - v_8v_5 \neq 0$, oftewel dat *A*, *B* en *C* niet op één lijn liggen. Dit is hetzelfde als beweren dat de driehoek niet ontaard is.

We gaan weer eerst eens zelf aan de slag om een algebraïsch bewijs van de stelling te leveren. De vertaling naar algebra kunnen we als volgt doen. Voor het punt *A* mogen we de oorsprong kiezen en het punt *B* kunnen we op de *x*-as kiezen, zeg $B(u_1,0)$. Dan houden we nog het vrije punt $C(u_2,u_3)$ over. Voor de resterende punten die hiervan afhangen schrijven we $D(x_1,x_2)$ en $E(x_3,x_4)$. Zie onderstaande figuur



De hypothese dat we met een parallellogram *ABCD* te maken hebben levert twee vergelijkingen op volgens de optelregel voor vectoren $\left(\overrightarrow{AB} + \overrightarrow{AC}\right)$:

$$\begin{aligned} x_1 - u_1 - u_2 &= 0 \\ x_2 - u_3 &= 0 \end{aligned}$$

De twee linkerzijden noemen we H_1 en H_2. Voor het snijpunt van de twee diagonalen krijgen we de volgende twee vergelijkingen door vertaling dat *E* op het lijnstuk *AD* resp. *E* op het lijnstuk *BC* ligt:

$$A, E, D \text{ op één lijn: } \frac{x_4}{x_3} = \frac{x_2}{x_1}, \qquad B, E, C \text{ op één lijn: } \frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}$$

In termen van veeltermen krijgen we dan:

$$\begin{aligned} x_1x_4 - x_2x_3 &= 0 \\ (u_2 - u_1)x_4 - u_3(x_3 - u_1) &= 0 \end{aligned}$$

De twee linkerzijden noemen we H_3 en H_4.

Denk niet dat dit de enige algebraïsche vertalingen zijn: bijvoorbeeld zouden we voor het gegeven dat *ABCD* een parallellogram ook de hypothese kunnen opstellen dat AC evenwijdig is met BD en daarom gelijke hellingen moeten hebben. In dat geval krijg je de vergelijking

$$u_2x_2 - u_3(x_1 - u_1) = 0$$

Maar dit is een meer ingewikkelde vergelijking dan de lineaire vergelijking $x_1 - u_1 - u_2 = 0$ die we eerder geïntroduceerd hebben.

Opgave 3: Laat zien dat $u_2x_2 - u_3(x_1 - u_1) = 0$ afgeleid kan worden uit het tweetal vergelijkingen $x_1 - u_1 - u_2 = 0$ en $x_2 - u_3 = 0$. Toon ook aan dat $x_1 - u_1 - u_2 = 0$ volgt uit het tweetal vergelijkingen $u_2x_2 - u_3(x_1 - u_1) = 0$ en $x_2 - u_3 = 0$, mits we aannemen dat $u_3 \neq 0$.

Kortom, we hebben vier hypothesen $H_1 = 0,\ H_2 = 0,\ H_3 = 0,\ H_4 = 0$ en we moeten de volgende twee conclusies over lengtes hieruit afleiden:

$$|AE|^2 = |ED|^2 \text{ geeft: } \quad x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$$
$$|BE|^2 = |EC|^2 \text{ geeft: } \quad (x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2$$

Uitwerken van deze veeltermvergelijkingen leidt dan tot:

$$x_1^2 - 2x_1x_3 - 2x_2x_4 + x_2^2 = 0$$
$$2u_1x_3 - 2u_2x_3 - 2u_3x_4 - u_1^2 + u_2^2 + u_3^2 = 0$$

Laten we de veeltermen aan de linkerzijden van deze twee gelijkheden S_1 respectievelijk S_2 noemen. We moeten dus aantonen dat $S_1 = 0$ en $S_2 = 0$ uit de hypothesen volgt. Maar dit is helemaal niet zo gemakkelijk om met pen en papier uit te voeren. Uit $H_1 = 0,\ H_2 = 0$ volgt dat we de substituties $x_1 = u_1 + u_2,\ x_2 = u_3$ kunnen toepassen in de vergelijkingen $H_3 = 0,\ H_4 = 0$. Uitwerken geeft het volgende stelsel van vergelijkingen:

$$u_3x_3 = (u_1 + u_2)x_4$$
$$u_1u_3 - x_3x_3 = (u_1 - u_2)x_4$$

Optellen van beide vergelijkingen geeft:

$$u_1u_3 = 2u_1x_4$$

Als $u_1 \neq 0$, en dat willen we natuurlijk ook om niet in een ontaarde situatie verzeild te raken, dan volgt hieruit:

$$x_4 = \tfrac{1}{2}u_3$$

Substitutie in de vergelijking $u_3x_3 = (u_1 + u_2)x_4$ geeft dan:

$$u_3x_3 = \frac{(u_1 + u_2)}{2}u_3$$

Als nu maar $u_3 \neq 0$, en dat is natuurlijk weer nodig om niet een ontaarde figuur te vermijden, dan krijgen we:

$$x_3 = \tfrac{1}{2}(u_1 + u_2)$$

Substitutie van de vier gevonden uitdrukkingen voor x_1, x_2, x_3, x_4 in de veeltermen S_1 en S_2 levert dan in beide gevallen 0 op, hetgeen bewezen moest worden.

Het bijzondere in bovenstaand bewijs is dat twee condities die met het niet-ontaard zijn van de figuur te maken hebben vanzelf naar boven komen drijven.

Transcriptie in veeltermvergelijkingen van coördinaten

De aanpak van geautomatiseerde bewijsvoering van een meetkundige stelling is gebaseerd op het idee om

1. een meetkundig probleem te transcriberen tot een algebraïsch probleem (meestal in een hoog-dimensionale ruimte);
2. het gestelde algebraïsche probleem op te lossen;
3. de oplossing in meetkundige termen te interpreteren.

Het algebraïsche probleem is meestal een probleem dat in termen van veeltermen geformuleerd kan worden in een hoog-dimensionale ruimte. Veel voorkomende transcripties gaan als volgt. We nemen de punten $A(x_1, x_2)$, $B(x_3, x_4)$, $C(x_5, x_6)$, $D(x_7, x_8)$. Dan hebben we de volgende vertalingen van meetkundige beweringen in veeltermvergelijkingen.

A = B : $x_3 - x_1 = 0$ en $x_4 - x_2 = 0$ Deze twee vergelijkingen werken in praktijk beter dan één vergelijking gebaseerd op een afstand zoals $(x_3 - x_1)^2 + (x_4 - x_2)^2 = 0$

***A, B, C* op één lijn**: richtingen van lijnstukken *AB* en *BC* moeten gelijk zijn en dus $\frac{x_4 - x_2}{x_3 - x_1} = \frac{x_6 - x_4}{x_5 - x_3}$ en als veeltermvergelijking wordt dit: $(x_4 - x_2)(x_5 - x_3) - (x_6 - x_4)(x_3 - x_1) = 0$

Parallelle lijnstukken *AB* en *CD* : de hellingen van deze lijstukken moeten gelijk zijn. Dus

$$\frac{x_4 - x_2}{x_3 - x_1} = \frac{x_8 - x_6}{x_7 - x_5}$$

oftewel als veeltermvergelijking:

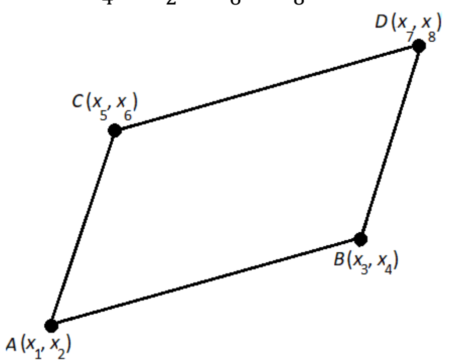
$$(x_4 - x_2)(x_7 - x_5) - (x_3 - x_1)(x_8 - x_6) = 0$$

Parallellogram *ABCD* (als in onderstaande figuur): vectoroptelling $\overrightarrow{AB} + \overrightarrow{AC} = \overrightarrow{AD}$ geeft:

$$x_3 - x_1 + x_5 - x_1 = x_7 - x_1$$
$$x_4 - x_2 + x_6 - x_2 = x_8 - x_2$$

oftewel

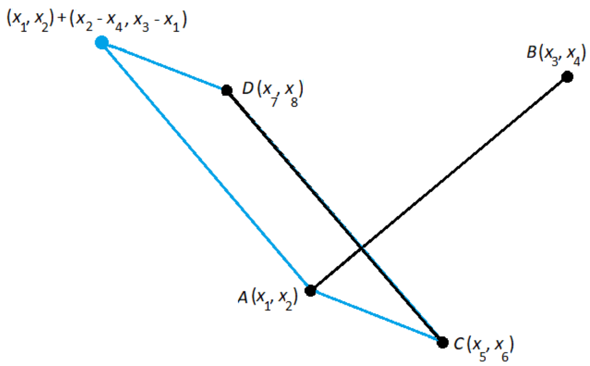
$$x_3 - x_1 + x_5 - x_7 = 0$$
$$x_4 - x_2 + x_6 - x_8 = 0$$



Loodrechte lijnstukken *AB* en *CD* : inproduct van de vectoren $\overrightarrow{AB}$ en $\overrightarrow{CD}$ gelijkstellen aan nul geeft :

$$(x_3 - x_1)(x_7 - x_5) + (x_4 - x_2)(x_8 - x_6) = 0$$

Loodrechte lijnstukken *AB* en *CD van gelijke lengte*: door rotatie over 90 graden van één lijnstuk kun je twee parallelle lijnstukken maken waarvan de hoekpunten een parallellogram vormen.



Er geldt dan

$$x_2 - x_4 + x_5 - x_1 = x_7 - x_1$$
$$x_3 - x_1 + x_6 - x_2 = x_8 - x_2$$

oftewel

$$x_2 - x_4 + x_5 - x_7 = 0$$
$$x_3 - x_1 + x_6 - x_8 = 0$$

C* is het midden van lijnstuk *AB : dit geeft

$$2x_5 - x_1 - x_3 = 0$$
$$2x_6 - x_2 - x_4 = 0$$

Lijnstukken *AB* en *CD* hebben gelijke lengte : dit vertaalt in

$$(x_3 - x_1)^2 + (x_4 - x_2)^2 - (x_7 - x_5)^2 + (x_8 - x_6)^2 = 0$$

C* ligt op cirkel door punt *B* met centrum *A : de straal van de cirkel is bekend, namelijk gelijk aan de lengte van het lijnstuk *AB*. Dus moet voor een punt *C* op de cirkel gelden:

$$(x_5 - x_1)^2 + (x_6 - x_2)^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 = 0$$

De Gröbner basis methode in vogelvlucht

Motivering

In de algebraïsche formulering van een meetkundig probleem hebben we onderscheid gemaakt tussen onafhankelijke (vrije) variabelen $u_1, u_2, \dots, u_m$, afkomstig als coördinaten van vrij te kiezen punten in een meetkundige figuur, en afhankelijke variabelen $x_1, x_2, \dots, x_n$, horende bij punten die geconstrueerd zijn in de meetkundige figuur. De constructie van de meetkundige figuur levert de hypothesen van een meetkundige stelling op in de vorm van veeltermvergelijkingen

$$H_1(u_1, u_2, \dots, u_m, x_1, x_2, \dots, x_n) = 0$$
$$H_2(u_1, u_2, \dots, u_m, x_1, x_2, \dots, x_n) = 0$$
$$\vdots$$
$$H_s(u_1, u_2, \dots, u_m, x_1, x_2, \dots, x_n) = 0$$

De meetkundige stelling wordt ook vertaald in een veeltermvergelijking, zeg

$$S(u_1, u_2, \dots, u_m, x_1, x_2, \dots, x_n) = 0.$$

Het algebraïsche probleem dat opgelost moet worden is de vraag of de stelling volgt uit de hypothesen, oftewel of de vergelijking $S = 0$ afgeleid kan worden uit de vergelijkingen $H_1 = 0, \dots, H_s = 0$.

Deze vraagstelling staat centraal in algebraïsche meetkunde en in dit vakgebied zijn verschillende methoden ontwikkeld om de vraag te beantwoorden. Een van de methoden is gebaseerd op het begrip **Gröbner basis**. Het voert te ver om dit begrip met volledige wiskundige strengheid te behandelen, maar we kunnen wel toelichten waar het om draait. We doen dit aan de hand van een eenvoudig stelsel van veeltermvergelijkingen dat we oplossen op een manier die lijkt op de methode van Gauss eliminatie bij een stelsel van lineaire vergelijkingen.

Voorbeeld

We bekijken de volgende drie veeltermen

$$f_1 = x - y - z$$
$$f_2 = x + y - z^2$$
$$f_3 = x^2 + y^2 - 1$$

en we proberen de verzameling $\boldsymbol{V(f_1, f_2, f_3)}$ van gemeenschappelijke nulpunten te bepalen. In algebraïsche meetkunde heet deze verzameling de **affiene variëteit gedefinieerd door $\boldsymbol{f_1, f_2, f_3}$**. We kunnen ook **het ideaal $\boldsymbol{\langle f_1, f_2, f_3 \rangle}$ voortgebracht door $\boldsymbol{f_1, f_2, f_3}$** definiëren als

$$\langle f_1, f_2, f_3 \rangle = \left\{ \sum_{i=1}^{3} p_i f_i \ : \ p_1, p_2, p_3 \text{ veeltermen in } x, y, z \right\}$$

We noemen het een ideaal omdat het een verzameling *I* van veeltermen in x, y, z is met de volgende drie eigenschappen

1. $0 \in I$
2. Als $f, g \in I$ dan $f + g \in I$
3. Als $f \in I$ en p een veelterm in x, y, z is, dan $p \cdot f \in I$

Als $f_1(x,y,z) = 0, f_2(x,y,z) = 0, f_3(x,y,z) = 0$ dan geldt voor elke veelterm $f \in \langle f_1, f_2, f_3 \rangle$ dat $f(x,y,z) = 0$. Je kan het ideaal $\langle f_1, f_2, f_3 \rangle$ dus beschouwen als de verzameling van alle veeltermen die 'polynomiaal af te leiden' zijn uit de vergelijkingen $f_1 = 0, f_2 = 0, f_3 = 0$. De *Basisstelling van Hilbert* zegt dat elk ideaal in de verzameling van alle mogelijke veeltermen over een getallenverzameling zoals complexe getallen (niet binnen de reële getallen) door een eindige verzameling van veeltermen wordt voortgebracht. Een Gröbner basis is een speciale verzameling van voortbrengers die je instaat stelt om gemakkelijker de gemeenschappelijke nulpunten te bepalen. In ons voorbeeld van drie vergelijkingen in drie onbekenden kan een Gröbner basis op een heuristische wijze tot stand komen.

We roepen de veeltermen in herinnering:

$$f_1 = x - y - z$$
$$f_2 = x + y - z^2$$
$$f_3 = x^2 + y^2 - 1$$

Net als in de Gauss-eliminatie methode kiezen we een term in de eerste veelterm f_1 om hiermee gelijksoortige termen in de andere veeltermen weg te vegen. We kiezen in ons voorbeeld de variabele x en kunnen deze in de tweede veelterm f_2 eenvoudig verwijderen:

$$g_2 = f_2 - f_1 = 2y - z^2 + z$$

We zeggen dat **$\boldsymbol{f_2}$ reduceert tot $\boldsymbol{g_2}$ modulo $\boldsymbol{f_1}$** en noteren dit met $\boldsymbol{f_2 \rightarrow_{f_1} g_2}$.

Voor verwijdering van termen met een x in de derde veelterm f_3 moeten we meer werk verzetten:

$$f_3 \rightarrow_{f_1} xy + xz + y^2 - 1 \qquad (= f_3 - x \cdot f_1)$$

en we kunnen met de nieuwe termen waar x in voor komt doorgaan; in eerste instantie doen we dit met de term xy:

$$xy + xz + y^2 - 1 \rightarrow_{f_1} xz + 2y^2 + yz - 1 \rightarrow_{f_1} 2y^2 + 2yz + z^2 - 1$$

Wat we nu gerealiseerd hebben is een overgang van het oorspronkelijke stelsel van vergelijkingen tot een nieuw stelsel:

$$g_1 = x - y - z$$
$$g_2 = 2y - z^2 + z$$
$$g_3 = 2y^2 + 2yz + z^2 - 1$$

dat dezelfde oplossingen heeft door de wijze waarop het geconstrueerd is, namelijk $g_2 = f_2 - f_1$ en $g_3 = (x + y + z) \cdot f_1$. Met andere woorden $V(f_1, f_2, f_3) = V(g_1, g_2, g_3)$. We gaan met het nieuwe stelsel verder rekenen.

Net als in de Gauss-eliminatie methode kiezen we een term in de tweede veelterm g_2 om hiermee gelijksoortige termen in de andere veeltermen weg te vegen. We kiezen in ons voorbeeld de variabele y en kunnen deze in de eerste veelterm g_1 eenvoudig verwijderen:

$$h_2 = 2g_1 - g_2 = 2x - z^2 - z$$

Voor verwijdering van termen met een y in de derde veelterm g_3 moeten we meer werk verzetten:

$$\begin{aligned} 2g_3 = 4y^2 + 4yz + 2z^2 - 2 &\to_{g_2} 2yz^2 + 2yz + 2z^2 - 2 \\ &\to_{g_2} 2yz + z^4 - z^3 + 2z^2 - 2 \\ &\to_{g_2} z^4 + z^2 - 2 \end{aligned}$$

Definieer $h_2 = 2g_3 - (2y + z^2 + z) \cdot g_2 = z^4 + z^2 - 2$ dan hebben we nu een nieuw stelsel dat in ‘driehoeksvorm’ is:

$$h_1 = 2x - z^2 - z$$
$$h_2 = 2y - z^2 + z$$
$$h_3 = z^4 + z^2 - 2$$

Door de constructie van het nieuwe stelsel weten we dat

$$V(f_1, f_2, f_3) = V(g_1, g_2, g_3) = V(h_1, h_2, h_3)$$

oftewel dat het laatst gevonden stelsel dezelfde gemeenschappelijke nulpunten heeft als het oorspronkelijke stelsel. Maar dit nieuwe stelsel is gemakkelijk op te lossen vanwege de speciale vorm. We kunnen de veelterm h_3 ontbinden

$$h_3 = z^4 + z^2 - 2 = (z^2 - 1)(z^2 + 2)$$

Hieruit is snel in te zien dat er vier nulpunten zijn binnen de complexe getallen, namelijk

$$z = 1, z = 2, z = i\sqrt{2}, z = -i\sqrt{2}$$

en dat er dus maar twee reële oplossingen zijn. Invullen van deze nulpunten in de andere twee vergelijkingen $h_1 = 0, h_2 = 0$ levert de bijpassende waarden van x en y op.

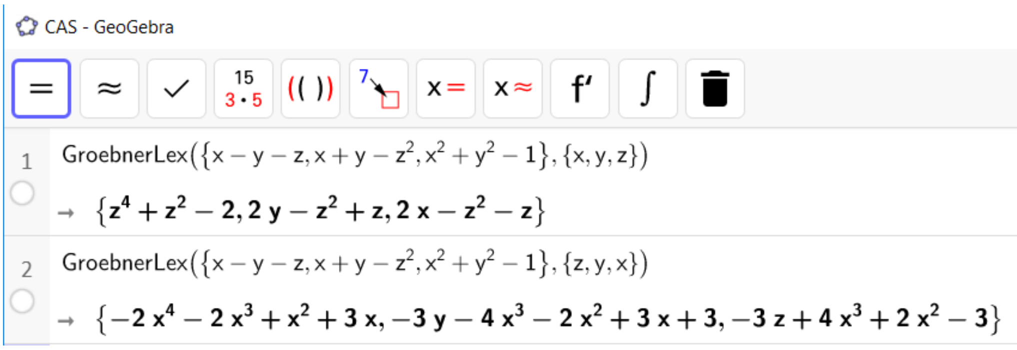
Uit de gevolgde constructie (en omkeerbaarheid van de operaties) volgt ook de gelijkheid van de idealen:

$$\langle f_1, f_2, f_3 \rangle = \langle g_1, g_2, g_3 \rangle = \langle h_1, h_2, h_3 \rangle$$

Wat we gevonden hebben zijn handigere voortbrengers van het oorspronkelijke ideaal. Dit blijkt een Gröbner basis te zijn (wat dat ook moge betekenen op dit moment).

Berekening van een Gröbner basis in GeoGebra

GeoGebra kan de Gröbner basis ook uitrekenen in het ingebouwde computeralgebrasysteem: je hoeft er alleen maar om te vragen, waarbij je wel de volgorde van belangrijkheid van de variabelen x, y en z moet aangeven (in overeenstemming met de keuzes die we in de reductieprocessen gemaakt hebben omtrent belangrijkheid van termen in een veelterm). Onderstaande schermafdruk illustreert dit.



De ordening van ééntermen in een veelterm speelt dus een rol in de Gröbner basis methode. De **lexicografische ordening met $x \succ y \succ z$** betekent dat $x^i y^j z^k \succ x^p y^q z^r$ dan en slechts dan als de eerste niet-nul component van $(i-p, j-q, k-r)$ positief is. We hebben dan

$$\begin{aligned} 1 &\prec z \prec z^2 \prec \cdots \prec y \prec yz \prec yz^2 \prec \cdots \\ &\prec y^2 \prec y^2z \prec y^2z^2 \prec \cdots \prec x \prec xz \prec xz^2 \prec \cdots \\ &\prec xy \prec xy^2 \prec \cdots \prec x^2 \prec \cdots \end{aligned}$$

De **gegradeerde lexicografische ordening met $x \succ y \succ z$** betekent dat ééntermen eerst volgens hun totale graad in alle variabelen samen gerangschikt worden en pas bij gelijke totale graad door de gewone lexicografische ordening gerangschikt worden. In dit geval hebben we dus:

$$\begin{aligned} 1 &\prec z \prec y \prec x \prec z^2 \prec yz \prec y^2 \prec xz \prec xy \prec x^2 \\ &\prec z^3 \prec y^2z \prec yz^2 \prec y^3 \prec xz^2 \prec xyz \prec xy^2 \prec x^2z \prec x^2y \prec x^3 \prec \cdots \end{aligned}$$

De **gegradeerde omgekeerde lexicografische orde met $x \succ y \succ z$** rangschikt ééntermen eerst volgens stijgende totale graad in alle variabelen samen; pas bij gelijke totale graad wordt de volgorde bepaald door de omgekeerde lexicografische orde waarin $x^i y^j z^k \succ x^p y^q z^r$ dan en slechts dan als de laatste niet-nul component van $(i-p, j-q, k-r)$ positief is. In de gegradeerde omgekeerde lexicografische orde geldt:

$$\begin{aligned} 1 &\prec z \prec y \prec x \prec z^2 \prec yz \prec xz \prec y^2 \prec xy \prec x^2 \\ &\prec z^3 \prec yz^2 \prec xz^2 \prec y^2z \prec xyz \prec x^2z \prec y^3 \prec xy^2 \prec x^2y \prec x^3 \prec \cdots \end{aligned}$$

Al deze ordeningen zijn in GeoGebra beschikbaar en hebben prettige eigenschappen zoals behoud van ordening bij vermenigvuldiging met een éénterm. Een gegeven ordening stelt je in staat om bij een veelterm f te kunnen spreken van de **leidende term**, genoteerd als $\mathrm{lt}(f)$, en de **leidende coëfficiënt**, gedefinieerd als de coëfficiënt van de leidende term van f en genoteerd als $\mathrm{lc}(f)$. De eerdere reductiestappen bestonden steeds uit een volgende operatie: **f reduceert tot $\overline{f}$ modulo g** (genoteerd als $f \to_g \overline{f}$) als er een term t in f is die deelbaar is door de leidende term van de veelterm g en $\overline{f} = f - \frac{t}{\mathrm{lt}(f)} \cdot g$. Als er geen verdere reducties meer mogelijk zijn dan is een **normaalvorm van f m.b.t. g** gevonden.

Wat is eigenlijk een Gröbner basis?

We kunnen reductie en normaalvorm niet alleen met één veelterm doen, maar ook invoeren voor een eindige verzameling $G = \{g_1, \dots, g_m\}$: een veelterm f reduceert tot $\overline{f}$ modulo G als er een g_j in G is zodanig dat $f \to_{g_j} \overline{f}$. Een normaalvorm van f m.b.t. G is dan een veelterm die na een eindig aantal reductiestappen verkregen wordt en waarvan geen enkele term meer deelbaar is door de leidende termen van de veeltermen in G. In het algemeen is een normaalvorm niet uniek. Een verzameling G heet een **Gröbner basis** (bij een gekozen termordening) dan en slechts als normaalvormen modulo G uniek zijn. Het **Buchberger algoritme** is een basismethode om een Gröbner basis te berekenen. Het resultaat hiervan, zeg GB, is niet uniek. Maar wanneer je er voor zorgt dat de leidende coëfficiënten van alle veeltermen in GB gelijk aan 1 zijn en voor elke veelterm $g \in GB$ geldt dat deze gelijk is aan zijn normaalvorm modulo $GB \setminus \{g\}$, dan is de Gröbner basis wel uniek en noemen we het de **gereduceerde Gröbner basis**. Net als veel computeralgebrasystemen is GeoGebra minder streng in de leer en staat het om redenen van leesbaarheid toe dat leidende coëfficiënten ongelijk aan 1 zijn in berekende Gröbner bases. Voor onze toepassing van Gröbner bases in geautomatiseerde bewijsvoering van meetkundige stellingen speelt dit geen enkele rol.

Hoe gebruik je Gröbner bases bij bewijzen van meetkundige stellingen?

Keren we terug naar de algebraïsche formulering van een meetkundig probleem uit het begin van deze sectie, waarin we hypothesen in de vorm van een affiene variëteit bij veeltermen $H_1, \dots, H_s$ hebben en een veelterm S bij een meetkundige stelling hoort. Wat we moeten aantonen is dat $S(u_1, u_2, \dots, u_{m,} x_1, x_2, \dots, x_n) = 0$ voor elke $(u_1, u_2, \dots, u_{m,} x_1, x_2, \dots, x_n) \in V(H_1, \dots, H_s)$. Anders geformuleerd, moeten we aantonen dat de variëteit $V(f_1, f_2, f_3)$ deelverzameling is van de affiene variëteit $V(S)$. Hiervoor staan verschillende methoden ter beschikking.

Methode 1: Als S in het ideaal $\langle H_1, \dots, H_s \rangle$ voortgebracht door de hypothesen zit, dan is de meetkundige stelling waar. We moeten dus lidmaatschap van een ideaal nagaan en dat kan met een Gröbner basis GB van het ideaal $\langle H_1, \dots, H_s \rangle$. Je hoeft dan enkel te controleren dat de normaalvorm van S m.b.t. GB gelijk is aan 0. Omdat GeoGebra geen commando aanbiedt om een normaalvorm te berekenen, moeten we het op een andere manier doen, namelijk checken of de Gröbner basis GB van het ideaal $\langle H_1, \dots, H_s \rangle$ gelijk is aan de Gröbner basis $v$an het ideaal $\langle H_1, \dots, H_s, S \rangle$.

Passen we deze methode toe op het eerste voorbeeld (Stelling 1), dan zijn de Gröbner bases van $\langle H_1, \dots, H_4 \rangle$ en $\langle H_1, \dots, H_4, S \rangle$ gelijk aan elkaar. Bijvoorbeeld zijn deze Gröbner bases in de lexicografische ordening met $u_1 \prec u_2 \prec \cdots \prec u_6 \prec x_1 \prec x_2 \prec x_3 \prec x_4$ gelijk aan $\langle H_1, \dots, H_4 \rangle$.

Denk niet dat deze methode zaligmakend is en gemakkelijk de bewijsvoering afrondt want bijvoorbeeld in Stelling 2, waarin tweedeling van diagonalen bewezen moet worden, biedt Methode 1 niet direct soelaas, simpelweg omdat de niet-ontaardheid van meetkundige figuur niet in de berekeningen meegenomen wordt en tot problemen leidt. Maar wanneer je de Gröbner basis van $\langle H_1, \dots, H_4 \rangle$ berekent in de lexicografische ordening met $u_1 \prec u_2 \prec u_3 \prec x_1 \prec x_2 \prec x_3 \prec x_4$ dan krijg je $\langle u_1(2x_4 - u_3), 2u_2x_3 - 2u_2x_4 - u_1u_3, x_2 - u_3, x_1 - u_1 - u_2 \rangle$. Het is dan duidelijk dat je twee gevallen moet onderscheiden: $u_1 = 0$, hetgeen een ontaarde situatie is, en $2x_4 - u_3 = 0$. Als je nu de Gröbner basis van $\langle 2x_4 - u_3, 2u_2x_3 - 2u_2x_4 - u_1u_3, x_2 - u_3, x_1 - u_1 - u_2 \rangle$ berekent, dan krijg je $\langle 2x_4 - u_3, u_3(2x_3 - u_1 - u_2), x_2 - u_3, x_1 - u_1 - u_2 \rangle$. Het is dan duidelijk dat je twee gevallen moet onderscheiden: $u_3 = 0$, hetgeen weer een ontaarde situatie is, en $2x_3 - u_1 - u_2 = 0$. De slot-conclusie is dat afgezien van twee ontaarde situaties we te maken hebben met de gemeenschappelijke nulpunten van de Gröbner basis $\langle 2x_4 - u_3, 2x_3 - u_1 - u_2, x_2 - u_3, x_1 - u_1 - u_2 \rangle$. Als je aan dit ideaal de twee conclusies S_1, S_2 toevoegt, dan krijg je dezelfde de Gröbner basis. Dus afgezien van de ontaarde situaties is de stelling van tweedeling van diagonalen bewezen.

Als je niks te maken wilt hebben met de ontaarde situatie kun je gewoon werken in de verzameling van veeltermen in de variabelen x_1, x_2, x_3, x_4 met rationale functies in de variabelen u_1, u_2, u_3 als coëfficiënten. Je kunt dan volstaan met aantonen dat de Gröbner bases van de idealen $\langle H_1, \dots, H_4 \rangle$ en $\langle H_1, \dots, H_4, S_1, S_2 \rangle$ in de lexicografische ordening $x_1 \prec x_2 \prec x_3 \prec x_4$ aan elkaar gelijk zijn.

In feite kun je de eis dat S in het ideaal $I = \langle H_1, \dots, H_s \rangle$ voortgebracht door de hypothesen zit afzwakken door te verlangen dat een macht van S in I zit. Anders geformuleerd, kunnen we volstaan met eisen dat S in het radicaal van I, gedefinieerd als $\{f : f^n \in I \text{ voor zekere } n \in \mathbb{N}\}$, zit. Het radicaal van een ideaal I noteren we met $\sqrt{I}$. De volgende stelling helpt om lidmaatschap van een radicaal te bewijzen.

Stelling. *De volgende beweringen zijn equivalent:*

(a) $S \in \sqrt{\langle H_1, \dots, H_s \rangle}$
(b) $1 \in \langle H_1, \dots, H_s, S \cdot y - 1 \rangle$ *in de verzameling veeltermen in* $u_1, u_2, \dots, u_m, x_1, x_2, \dots, x_n, y$, *oftewel de gereduceerde Gröbner basis van* $\langle H_1, \dots, H_s, S \cdot y - 1 \rangle$ *is gelijk aan* $\{1\}$.

Dit verandert niets aan de toepassing van de Gröbner basis methode in de twee concrete voorbeelden van meetkundige stellingen. Het brengt ons bij methode 2.

Methode 2: Als de gereduceerde Gröbner basis van $\langle H_1, \dots, H_s, S \cdot y - 1 \rangle$ gelijk is aan $\{1\}$, dan is de meetkundige stelling die met de veelterm S correspondeert waar.

Methode 2 kan dus een meetkundige stelling bewijzen, maar doet verder geen definitieve uitspraak over de correctheid van een meetkundige stelling. Het kan namelijk best zijn dat de hypothesen nog ontaarde situaties toestaan. In de algebraïsche vertaling betekent dit dat bepaalde algebraïsche uitdrukkingen ongelijk aan nul moeten zijn. We kunnen dit inbouwen in de volgende methode via de truc van Rabinowitsch:

Methode 3: In het geval van hypothesen in de vorm van veeltermen $H_1, \dots, H_s$ en extra condities in de vorm van veeltermongelijkheden $D_1 \neq 0, \dots, D_t \neq 0$ is een meetkundige stelling die met de veelterm S correspondeert in het algemeen waar wanneer de gereduceerde Gröbnerbasis van het ideaal $\langle H_1, \dots, H_s, D_1 \cdot y_1 - 1, \dots, D_t \cdot y_2 - 1, S \cdot y - 1 \rangle$ gelijk is aan $\{1\}$. Vaak wordt hierbij een lexicografische ordening $u_1 \prec \cdots \prec u_m \prec x_1 \prec \cdots \prec x_n \prec y_1 \prec \cdots \prec y_t \prec y$ gebruikt.

Soms weet je niet goed op voorhand welke conditie of condities nog nodig zijn. Maar ook hier kan Gröbner basis theorie bij helpen. Zo kun je bijvoorbeeld gaan zoeken in de Gröbner basis van het ideaal $\langle H_1, \dots, H_s, S \cdot y - 1 \rangle$ naar veeltermen die enkel de variabelen $u_1, u_2, \dots, u_m$ bevatten. Deze moeten dan ongelijk aan 0 gesteld worden. Bijvoorbeeld krijg je in het voorbeeld bij de berekening van de Gröbner basis van $\langle H_1, \dots, H_4, S \cdot y - 1 \rangle$ een resultaat waarin de veelterm $u_1 \cdot u_3$ staat. Dit levert dus de conditie $u_1 u_3 \neq 0$ die we eerder gebruikt hebben voor de bewijsvoering.

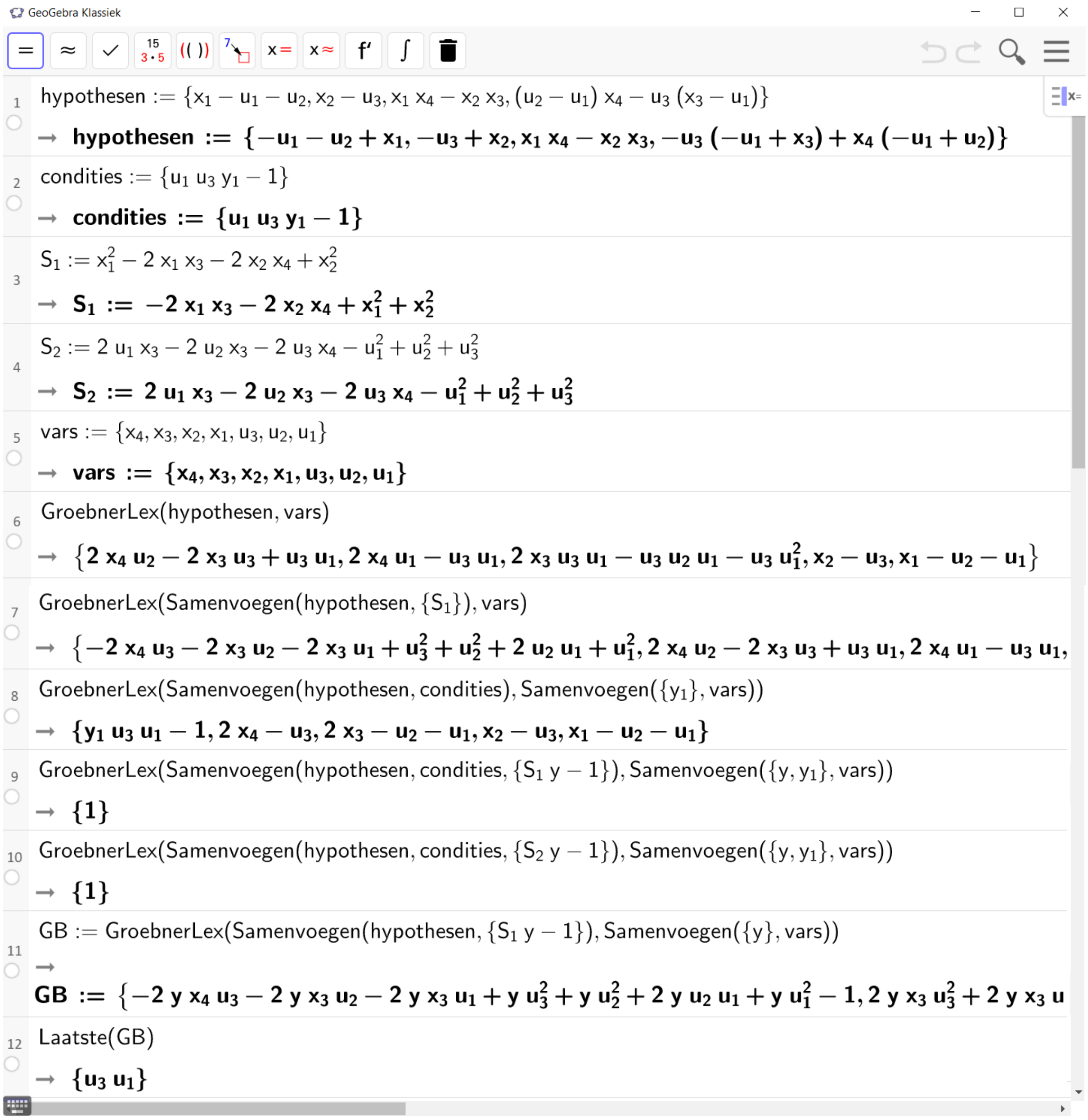
Voorbeelden van bewijsvoering m.b.v. Gröbner bases in GeoGebra

We gaan de eerder beschreven methodes van bewijsvoering eens toepassen op enkele meetkundige stellingen.

Stelling 2

In een parallellogram verdeelt het snijpunt van de diagonalen elk van deze diagonalen in twee stukken van gelijke lengte.

We geven een schermafdruk van een CAS-venster in GeoGebra horende bij dit eerder besproken voorbeeld. We verwijzen naar de eerdere toelichting die door deze schermafdruk ondersteunt wordt. Deze laat zien dat Methode 3 goed werkt wanneer geschikte condities toegevoegd zijn om een ontaarde figuur te vermijden en dat deze condities ook op te sporen zijn via een Gröbner basis methode

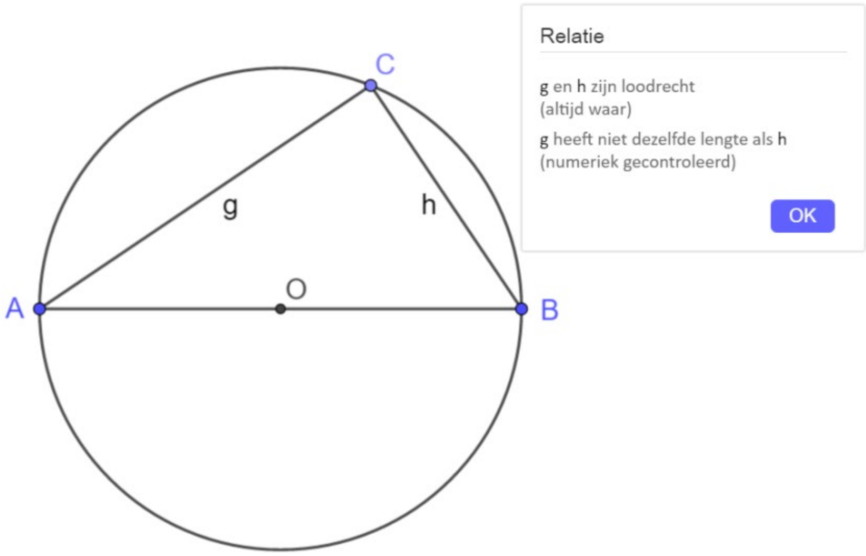


Stelling 3 (Cirkelstelling van Thales)

Een driehoek ingeschreven in een cirkel, en waarvan één zijde een middellijn van de cirkel vormt, is een rechthoekige driehoek.

Onderstaande schermafdruk illustreert dat het BEWIJS-gereedschap in GeoGebra dit automatisch aankan. De constructie bestaat uit een beperkt aantal stappen:

1. Teken een lijnstuk *AB*
2. Construeer het midden van het lijnstuk AB en noem dit punt *O.*
3. Teken een cirkel met middelpunt *O* en die door *A* en *B* gaat.
4. Neem een willekeurig punt *C* op de cirkel.
5. Teken de lijnstukken *AC* en *BC*; noem deze lijnstukken $g$respectievelijk h.
6. Ga met het RELATIE-gereedschap na dat $g \perp h$



We bewijzen dit in coördinaten op de manier die GeoGebra in principe ook hanteert. Als oorsprong van het assenstelsel kiezen we het middelpunt van de cirkel. Voor de coördinaten van de punten *A* en *B* kunnen we dan nemen $A(-u_1, 0)$ en $B(u_1, 0)$. We kiezen een willekeurig punt $C(u_2, u_3)$ op de cirkel en dat geeft de veeltermvergelijking $u_2^2 + u_3^2 = u_1^2$ oftewel $u_2^2 + u_3^2 - u_1^2 = 0$. We moeten bewijzen dat de lijnstukken *AC* en *BC* loodrecht op elkaar staan. In coördinaten betekent dit (inproduct van $\overrightarrow{AC}$ en $\overrightarrow{BC}$ gelijk aan nul) dat aan de veeltermvergelijking $u_2^2 + u_3^2 - u_1^2 = 0$ moet gelden. Maar dat is precies één van de hypothesen. In dit geval is de conclusie evident en hoeven we niet eens ontaarde gevallen $u_1 = 0$ $(A = B)$ en $u_3 = 0$ $(C = A$ of $C = B)$ te onderscheiden.

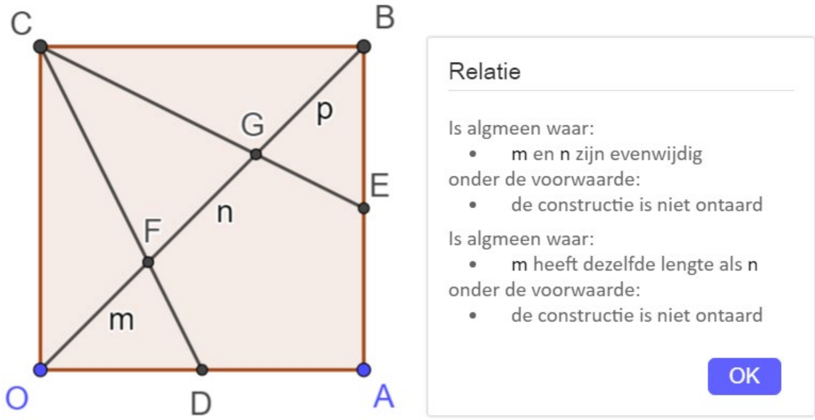
Stelling 4

Deze stelling komt uit een ICMI studie *School Mathematics in the 1990s* voorbereid door Howson en Wilson en gepubliceerd onder deze titel door Cambridge University Press in 1986 (red. G. Howson & J.-P. Kahane).

Neem een vierkant OABC. Dan delen de twee lijnen die C verbinden met de middens van OA en AB de hoofddiagonaal OB in drie stukken van gelijke lengte.

Onderstaande schermafdruk illustreert dat het BEWIJS-gereedschap in GeoGebra dit automatisch aankan. De constructie bestaat uit een beperkt aantal stappen:

1. Teken een vierkant *OABC*
2. Construeer de middens van de lijnstukken *OA* en *AB*, en noem deze punten *D* en *E.*
3. Teken de twee lijnstukken van *C* naar *D* en *E*.
4. Teken de hoofddiagonaal van *O* naar *B*.
5. Construeer de snijpunten van de lijstukken *CD* en *CE* met de hoofddiagonaal; noem deze punten *F* en *G*.
6. Maak de hoofddiagonaal onzichtbaar en teken de lijnstukken *OF*, *OG*, *GB* en noem deze lijnstukken *m*, *n*, respectievelijk *p*
7. Ga met het RELATIE-gereedschap na *m* en *n* evenwijdig en van gelijke lengte zijn (als je tenminste van een niet-ontaarde figuur uitgegaan bent).



We bewijzen dit in coördinaten op de manier die GeoGebra in principe ook hanteert. Als oorsprong van het assenstelsel kiezen we het punt *O* linksonder in het vierkant (vandaar deze naamkeuze). Het punt *A* veronderstellen we op de horizontale as te liggen op afstand u.Hiermee zijn de coördinaten van de hoekpunten van het vierkant vastgelegd: $A(u,0), B(u,u), C(0,u)$. De coördinaten van de middens *D* en *E* op de lijnstukken *OA* en *AB* liggen dan per definitie ook vast: $D\left(\frac{1}{2}u,0\right), E\left(u,\frac{1}{2}u\right)$. Een voor de hand liggende conditie is natuurlijk de eis $u \neq 0$, maar die laten we eerst nog even buiten beschouwing. De geconstrueerde punten *F* en *G* geven we coördinaten $F(x_1,x_2), G(x_3,x_4)$. Voor deze punten kunnen we veeltermvergelijkingen opstellen die onze hypothesen vormen: het gegeven dat *F* en G op *OB* liggen geeft de vergelijkingen $x_1 - x_2 = 0, x_3 - x_4 = 0$. Het punt *F* is het snijpunt van *CD* en *OB*, en het gegeven dat *F* dus op *CD* ligt, vertaalt in de vergelijking $u - 2x_1 - x_2 = 0$. Op eenzelfde manier kunnen we voor het punt *G*, zijnde het snijpunt van *CE* en *OB* en dus liggend op *CE*, de vergelijking $u + x_3 - 2x_4 = 0$ opstellen. Samenvattend, hebben we de volgende veeltermen gevonden die de hypothesen beschrijven in het bij de stelling horende algebraïsche probleem:

$$x_1 - x_2, \qquad x_3 - x_4, \qquad u - 2x_1 - x_2, \qquad u + x_3 - 2x_4$$

Dat de lijnstukken *m*, *n*, en *p* evenwijdig zijn en zelfs in elkaars verlengde liggen is per definitie juist. De stelling draait uiteindelijk om de bewering dat dit lijnstukken van gelijke lengte zijn. Met andere woorden: de lengte van elk lijnstuk zal gelijk moeten zijn aan één derde van de lengte van de hoofddiagonaal *OB*. Het is gemakkelijker om met kwadraten van lengtes algebraïsch te rekenen. Bijvoorbeeld wordt de bewering dat het kwadraat van de lengte van *OF* één negende van het kwadraat van de lengte *OB* is ($|OF|^2 = \frac{1}{9}|OB|^2$) vertaald in de veeltermvergelijking $x_1^2 + x_2^2 - \frac{2}{9}u^2 = 0$. Evenzo kan je door de bewering dat de lengte van *OG* gelijk is aan twee derde van de lengte van de hoofddiagonaal afleiden dat $x_3^2 + x_4^2 - \frac{8}{9}u^2 = 0$. Tot slot geeft de relatie tussen de lengte van *GB* en de lengte van de hoofdiagonaal de veeltermvergelijking: $(u - x_3)^2 + (u - x_4)^2 - \frac{2}{9}u^2 = 0$. Samenvattend zijn de veeltermen die bij de stelling horen gelijk te stellen aan:

$$S_1 \stackrel{\text{def}}{=} x_1^2 + x_2^2 - \frac{2}{9}u^2, \qquad S_2 \stackrel{\text{def}}{=} x_3^2 + x_4^2 - \frac{8}{9}u^2, \qquad S_3 \stackrel{\text{def}}{=} (u - x_3)^2 + (u - x_4)^2 - \frac{2}{9}u^2$$

De veeltermen die in Methode 3 gebruikt worden zijn met nieuwe variabelen y, z, w te schrijven als:

$$S_1 \cdot y - 1, \qquad S_2 \cdot z - 1, \qquad S_3 \cdot w - 1$$

Wanneer we de gereduceerde Gröbner basis van de het ideaal voortgebracht door de hypothesen en de stellingen bepalen in de lexicografische ordening met $u \prec x_1 \prec x_2 \prec x_3 \prec x_4$ dan is deze niet gelijk aan de Gröbner basis van enkel de hypothesen wat de term u^2 daar in voor. Dit motiveert de introductie van de conditie $u \neq 0$ die via de truc van Rabinowitsch leidt tot de veelterm $u \cdot y_1 - 1$. Volgens de Methode 3 hoeven we nu alleen de Gröbner basis van het ideaal voortgebracht door de veeltermen passend bij de hypothesen, condities en stellingen (met extra geïntroduceerde variabelen) uit te rekenen en vast te stellen dat deze gelijk is aan {1}. Dit blijkt ook het resultaat te zijn volgens onderstaande schermafdruk van een CAS-venster in GeoGebra.

1 hypothesen := $\{x_1 - x_2, x_3 - x_4, u - 2\,x_1 - x_2, u + x_3 - 2\,x_4\}$

→ **hypothesen :=** $\{x_1 - x_2, x_3 - x_4, u - 2\,x_1 - x_2, u + x_3 - 2\,x_4\}$

2 condities := $\{u\,y_1 - 1\}$

→ **condities :=** $\{u\,y_1 - 1\}$

3 $S_1 := x_1^2 + x_2^2 - \frac{2}{9}\,u^2$

→ $S_1 := -\frac{2}{9}\,u^2 + x_1^2 + x_2^2$

4 $S_2 := x_3^2 + x_4^2 - \frac{8}{9}\,u^2$

→ $S_2 := -\frac{8}{9}\,u^2 + x_3^2 + x_4^2$

5 $S_3 := (u - x_3)^2 + (u - x_4)^2 - \frac{2}{9}\,u^2$

→ $S_3 := -\frac{2}{9}\,u^2 + (u - x_3)^2 + (u - x_4)^2$

6 vars := $\{x_4, x_3, x_2, x_1, u\}$

→ **vars :=** $\{x_4, x_3, x_2, x_1, u\}$

7 GroebnerLex(hypothesen, vars)

→ $\{x_4 - u, -x_3 + u, 3\,x_2 - u, -3\,x_1 + u\}$

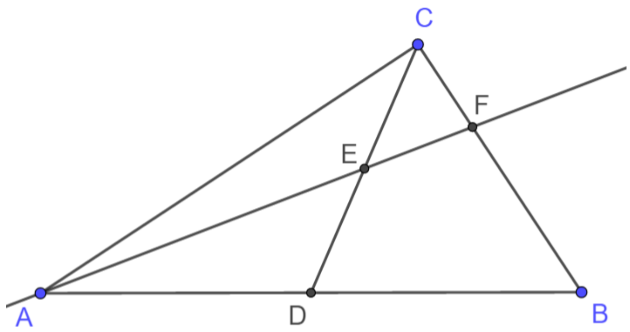
8 GroebnerLex(Samenvoegen(hypothesen, $\{S_1, S_2, S_3\}$), vars)

→ $\{u^2, 3\,x_1 - u, 3\,x_2 - u, x_3 - u, x_4 - u\}$

9 GroebnerLex(Samenvoegen(hypothesen, condities, $\{S_1\,y - 1, S_2\,z - 1, S_3\,w - 1\}$), Samenvoegen($\{z, w, y, y_1\}$, vars))

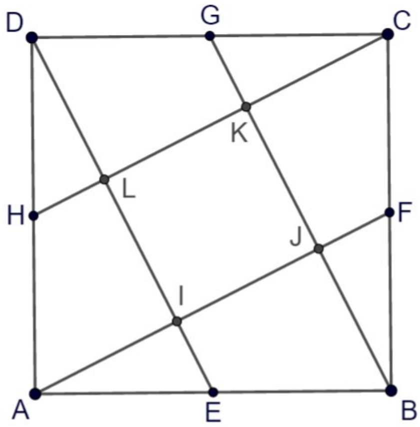
→ $\{1\}$

Opgave 4: Laat *D* het midden zijn van de zijde *AB* in een driehoek *ABC*. Laat *E* het midden zijn van het lijnstuk *CD*. Laat *F* het snijpunt zijn van het lijnstuk *BC* en de lijn door de punten *A* en *E*. Bewijs dat de lengte van het lijnstuk *BF* tweemaal de lengte van het lijnstuk *FC* is.



Stelling 5 ("1/5 vierkant")

Construeer in een vierkant *ABCD* de middens *E*, *F*, *G*, *H* van de zijden zoals in onderstaande figuur. Construeer de lijnstukken *DE*, *GB*, *AF* en *HC.* De onderlinge snijpunten van deze lijnstukken, zijnde de punten *I*, *J*, *K*, en *L*, vormen een vierkant *IJKL* waarvan de oppervlakte gelijk is aan éénvijfde van de oppervlakte van het vierkant *ABCD*.



Het RELATIE-gereedschap merkt enkel op dat de oppervlakten van de vierkanten verschillen. Maar met de Gröbner basis techniek kunnen we de stelling ook bewijzen! We nemen daarvoor een assenstelsel met oorsprong *A* en met *B* op de horizontale as met coördinaten $(u, 0)$ voor zekere $u \neq 0$. Dit levert de veelterm $u \cdot y_1 - 1$ in Methode 3 op. Voor de andere punten op het vierkant *ABCD* kunnen we dan de coördinaten vastleggen: $C(u, u)$, $D(0, u)$, $E\left(\frac{1}{2}u, 0\right)$, $F\left(u, \frac{1}{2}u\right)$, $G\left(\frac{1}{2}u, u\right)$, $H\left(0, \frac{1}{2}u\right)$. Voor de andere punten in de figuur nemen we $I(x_1, x_2)$, $J(x_3, x_4)$, $K(x_5, x_6)$, $L(x_7, x_8)$. We stellen de veeltermen op die de hypothesen vormen volgens de eerder geïntroduceerde transcriptiemethode. Bijvoorbeeld geldt voor punt *I* dat dit op het lijnstuk *AF* en *DE* moet liggen en dat deze eigenschappen vertaald worden naar veeltermvergelijkingen $x_1 - 2x_2 = 0$ en $u - 2x_1 - x_2 = 0$. Iets soortgelijks kunnen we doen voor de punten *J*, *K* en *L*. Zo krijgen we de volgende veeltermen die de hypothesen van de stelling vormen:

$x_1 - 2x_2$, $\quad u - 2x_1 - x_2$, $\quad x_3 - 2x_4$, $\quad 2u - 2x_3 - x_4$, $\quad 2u - 2x_5 - x_6$,

$u + x_5 - 2x_6$, $\quad u + x_7 - 2x_8$, $\quad u - 2x_7 - x_8$.

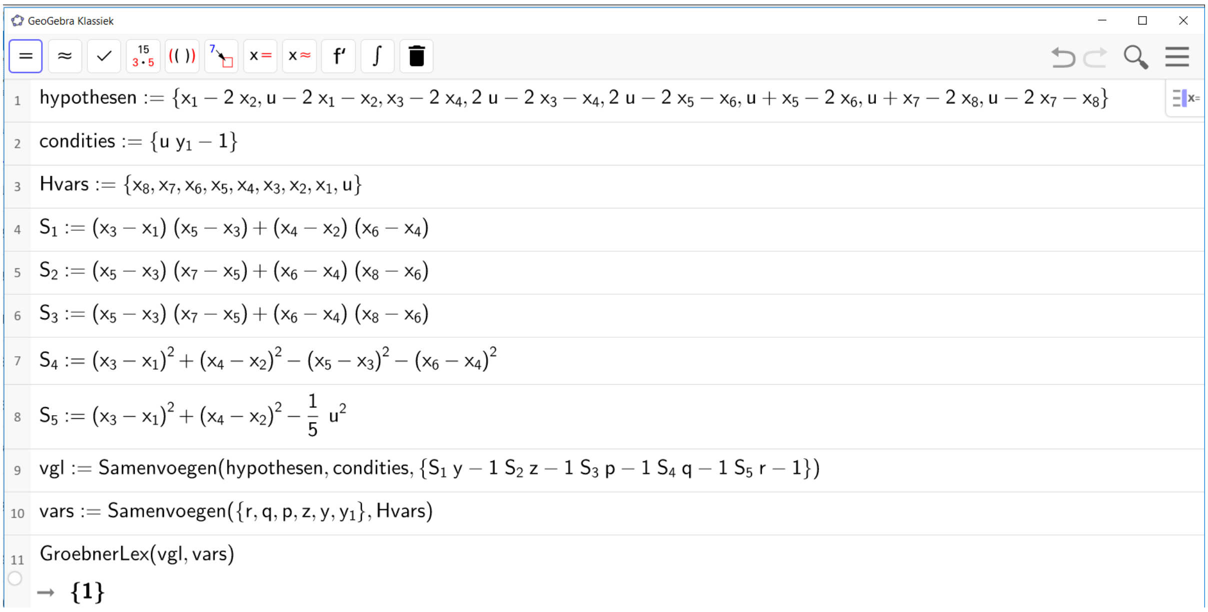
Rest ons nog veeltermen op te stellen die bij de stelling passen. We bepalen de relaties op basis van de eigenschappen dat *IJ* en *JK* loodrecht op elkaar moeten staan, dat *JK* en *KL* loodrecht op elkaar staan, en dat *KL* loodrecht staat op *LI* (dan staan vanzelf *LI* en *IK* loodrecht op elkaar en hebben we een rechthoek. Verder bepalen we de veelterm die vastlegt dan *IJ* en *KL* dezelfde lengte hebben. Dan is er dus sprake van een vierkant. Tot slot moeten we nog de veelterm bepalen die de te bewijzen relatie tussen de twee oppervlakten beschrijft. De veeltermen die bij de stelling horen zijn dan gelijk te stellen aan (ga zelf na!):

$$S_1 \stackrel{\text{def}}{=} (x_3 - x_1)(x_5 - x_3) + (x_4 - x_2)(x_6 - x_4),$$
$$S_2 \stackrel{\text{def}}{=} (x_5 - x_3)(x_7 - x_5) + (x_6 - x_4)(x_8 - x_6),$$
$$S_3 \stackrel{\text{def}}{=} (x_5 - x_3)(x_7 - x_5) + (x_6 - x_4)(x_8 - x_6),$$
$$S_4 \stackrel{\text{def}}{=} (x_3 - x_1)^2 + (x_4 - x_2)^2 - (x_5 - x_3)^2 - (x_6 - x_4)^2,$$
$$S_5 \stackrel{\text{def}}{=} (x_3 - x_1)^2 + (x_4 - x_2)^2 - \tfrac{1}{5}u^2.$$

De veeltermen die bij de stellingen in Methode 3 gebruikt worden zijn met nieuwe variabelen y, z, p, q, r te schrijven als:

$$S_1 \cdot y - 1, \qquad S_2 \cdot z - 1, \qquad S_3 \cdot p - 1, \qquad S_3 \cdot q - 1, \qquad S_3 \cdot r - 1$$

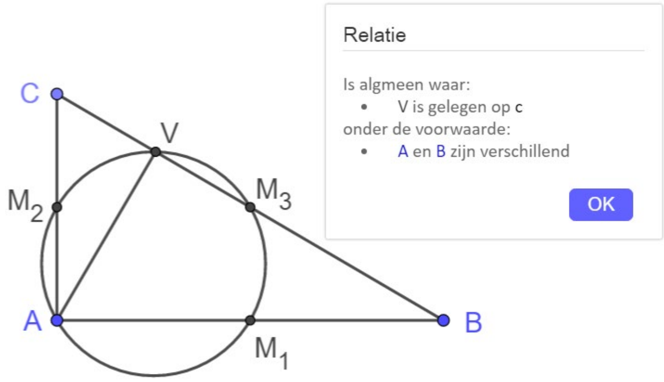
We hoeven dan alleen de Gröbner basis van het ideaal voortgebracht door de veeltermen passend bij de hypothesen, condities en stellingen (met extra geïntroduceerde variabelen) uit te rekenen en vast te stellen dat deze gelijk is aan {1}. Dit blijkt ook het resultaat te zijn volgens onderstaande schermafdruk van een CAS-venster in GeoGebra.



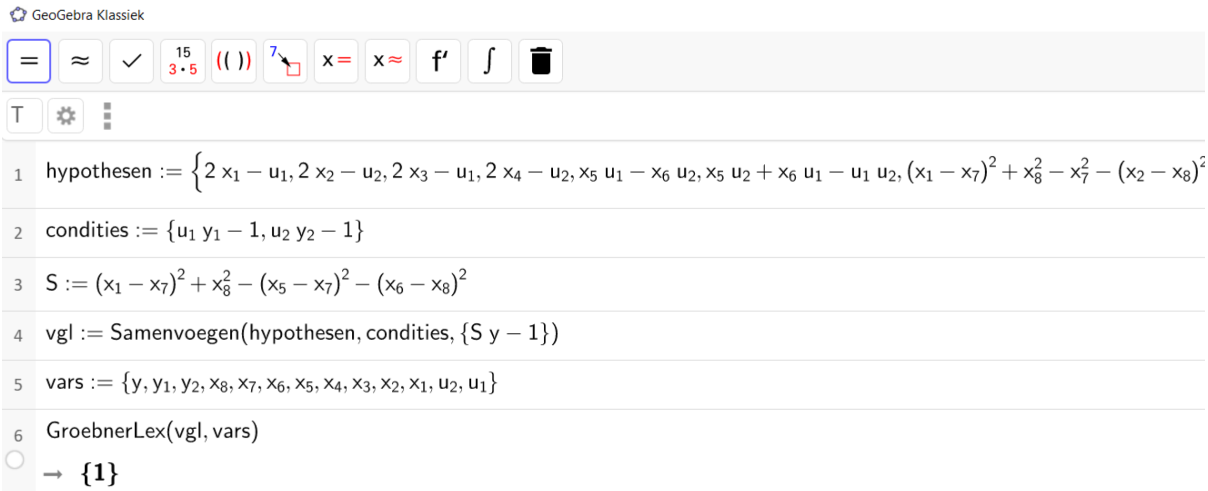
Stelling 6 (Cirkelstelling van Apollonius)

In een rechthoekige driehoek ABC met rechte hoek in hoekpunt A liggen de middens van de zijden van de driehoek en het voetpunt van de hoogtelijn van A naar BC op een cirkel.

In onderstaande schermafdruk is de situatie uit de stelling geschetst en kun je ook zien dat het Bewijs-gereedschap van GeoGebra kan aantonen dat het voetpunt ligt op de cirkel door de middens, als tenminste A en B verschillen. Opmerkelijk genoeg wordt niet vermeld dat A en C moeten verschillen. Misschien komt dit doordat de cirkel dan ook niet te construeren is.



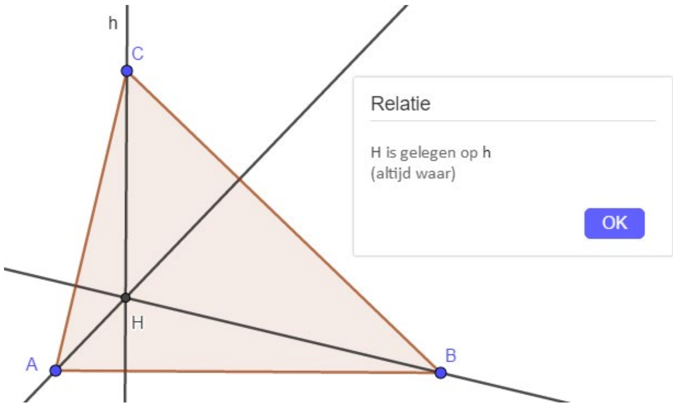
We gaan de stelling weer vertalen naar een algebraïsch probleem. We nemen een assenstelsel met oorsprong A, B op de horizontale as op afstand u_1 van A gelegen, en C op de verticale as op afstand u_2 van A gelegen. De coördinaten van de hoekpunten zijn dus $A(0{,}0)$, $B(u_1, 0)$, $C(0, u_2)$. Voor de middens van de zijden nemen we de volgende coördinaten: $M_1(x_1, 0)$, $M_2(0, x_2)$, $M_3(x_3, x_4)$. Dan hebben we al de volgende hypothesen: $2x_1 - u_1 = 0$, $2x_2 - u_2 = 0$, $2x_3 - u_1 = 0$, $2x_4 - u_2 = 0$. Het voetpunt V geven we de coördinaten (x_5, x_6). Het gegeven dat $AV \perp BC$ en dat B, H, C op één lijn liggen leidt tot de volgende vergelijkingen: $x_5 \cdot u_1 - x_6 \cdot u_2 = 0$, $x_5 \cdot u_2 + x_6 \cdot u_1 - u_1 \cdot u_2 = 0$. Drie punten die niet op één lijn liggen, zoals de middens van de driehoek, liggen op een cirkel. We veronderstellen dat het middelpunt M van deze cirkel coördinaten heeft. Dit levert nog twee hypothesen op: $d(M, M_1) = d(M, M_2)$ geeft $(x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_2 - x_8)^2 = 0$ en $d(M, M_1) = d(M, M_3)$ geeft $(x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$. De bewering dat V op de cirkel door de middens ligt betekent dat $d(M, M_1) = d(M, V)$ moet gelden. Dit levert de volgende vergelijking op: $(x_1 - x_7)^2 + x_8^2 - (x_5 - x_7)^2 - (x_6 - x_8)^2 = 0$. Om een niet-ontaarde figuur te specificeren moeten we eisen dat $u_1 \neq 0$ en $u_2 \neq 0$. Daarna is alles in gereedheid om Methode 3 toe te passen. Onderstaande schermafdruk toont het succes van deze Gröbner basis methode.



Stelling 7

De hoogtelijnen van een driehoek ABC gaan door één punt

Het bewijsgereedschap van GeoGebra kan dit aantonen (zie schermafdruk) en wij zullen dit met de Gröbner basis methode ook bewijzen. Daarvoor nemen we een assenstelsel met oorsprong *A* zodanig dat B op de horizontale as ligt. Als coördinaten van de hoekpunten van de driehoek nemen we $A(0,0)$, $B(u_1, 0)$, $C(u_2, u_3)$. We herformuleren de stelling als volgt: laat $H(x_1, x_2)$ het snijpunt zijn van de hoogtelijnen vanuit de hoekpunten *A* en *B*. We tonen aan dat *H* dan ook ligt op de hoogtelijn vanuit hoekpunt *C* .



We stellen nu de vergelijkingen op die de hypothesen vormen: de conditie dat de lijn *AH* loodrecht op de lijn *BC* staat betekent dat $x_1 \cdot (u_2 - u_1) + x_2 \cdot u_3 = 0$; de conditie dat de lijn *BH* loodrecht op de lijn *AC* staat betekent dat $u_2 \cdot (x_1 - u_1) + x_2 \cdot u_3 = 0$. De stelling is bewezen als we kunnen aantonen dat $x_1 = u_2$. Maar dat is in deze formulering haast een trivialiteit: uit de twee hypothesen volgt $x_1 \cdot (u_2 - u_1) = u_2 \cdot (x_1 - u_1)$ oftewel $x_1 \cdot u_2 - x_1 \cdot u_1 = u_2 \cdot x_1 - u_2 \cdot u_1$. Dit is te herschrijven als $u_1 \cdot (x_1 - u_2) = 0$. Als we een niet-ontaarde figuur bekijken, en dus $u_1 \neq 0$ veronderstellen, moet wel gelden dat $x_1 - u_2 = 0$ en dus $x_1 = u_2$. Dit verklaart ook een beetje dat de Gröbner basis methoden soepel verlopen als je de conditie $u_1 \neq 0$ inbouwt via de truc van Rabinowitsch. Onderstaande schermafdruk illustreert dat zowel Methode 1 (met de conditie ingebouwd) als Methode 3 de gewenste bewijsvoering levert.

1	hypothesen := $\{x_1\,(u_2 - u_1) + x_2\,u_3, u_2\,(x_1 - u_1) + x_2\,u_3\}$
2	condities := $\{u_1\,y_1 - 1\}$
3	S := $x_1 - u_2$
4	vars := $\{y_1, x_2, x_1, u_3, u_2, u_1\}$
5	GroebnerLex(Samenvoegen(hypothesen, condities), vars) → $\{\mathbf{y_1\,u_1 - 1, x_2\,u_3 + u_2^2 - u_2\,u_1, x_1 - u_2}\}$
6	GroebnerLex(Samenvoegen(hypothesen, condities, {S}), vars) → $\{\mathbf{y_1\,u_1 - 1, x_2\,u_3 + u_2^2 - u_2\,u_1, x_1 - u_2}\}$
7	GroebnerLex(Samenvoegen(hypothesen, condities, {S · y − 1}), samenvoegen({y}, vars)) → $\{\mathbf{1}\}$

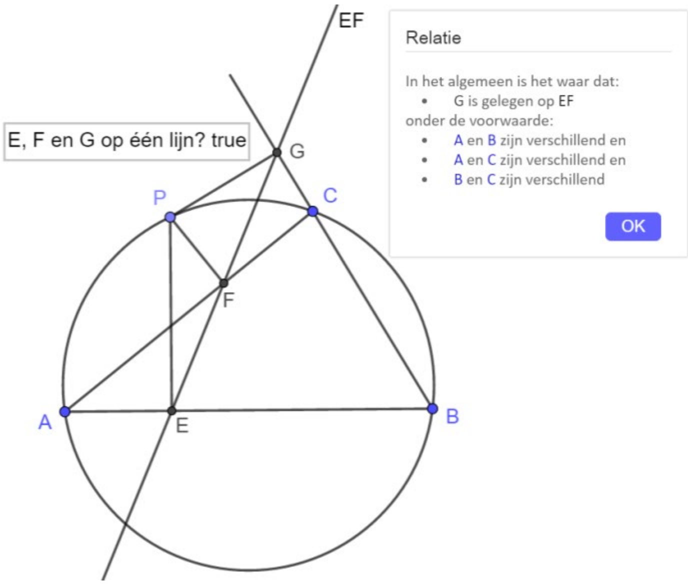
Opgave 5: Ga via de Gröbner basis methode in GeoGebra na dat de middelloodlijnen van een driehoek door één punt gaan.

Opgave 6: Ga via de Gröbner basis methode in GeoGebra na dat de zwaartelijnen van een driehoek door één punt gaan.

Stelling 8 (Stelling van Simson)

Neem op de omgeschreven cirkel van een driehoek ABC een punt P en construeer de loodlijnen vanuit P naar de zijden van de driehoek. De drie voetpunten van deze loodlijnen liggen op één lijn.

Onderstaande schermafdruk illustreert dat het RELATIE-gereedschap in GeoGebra krachtig genoeg is om de bewering te staven voor een niet-ontaarde situatie.



We gaan de stelling weer bewijzen m.b.v. de Gröbner basis methode. We kiezen een assenstelsel zodanig dat de hoekpunten van de driehoek *ABC* de coördinaten $A(0{,}0)$, $B(u_1,0)$, $C(u_2,u_3)$ hebben. Laat $P(x_1,x_2)$ een punt op de omgeschreven cirkel $\mathcal{C}$ zijn. Om deze cirkel $\mathcal{C}$ te beschrijven kiezen we voor het middelpunt $M(x_3,x_4)$. Voor de drie geconstueerde punten *E*, *F* en *G* kiezen we de coördinaten $E(x_1,0)$, $F(x_5,x_6)$, $G(x_7,x_8)$. We kunnen nu onderstaande hypothesen opstellen

M is het middelpunt van omgeschreven cirkel van *ABC* (dus $|AM|^2 = |BM|^2 = |CM|^2$) geeft:

$x_3^2 + x_4^2 = (u_1 - x_3)^2 + x_4^2$ oftewel $u_1^2 - 2 \cdot u_1 \cdot x_3 = 0$

$x_3^2 + x_4^2 = (u_2 - x_3)^2 + (u_3 - x_4)^2$ oftewel $u_2^2 - 2 \cdot u_2 \cdot x_3 + u_3^2 - 2 \cdot u_3 \cdot x_4 = 0.$

We kunnen hieruit wel de coördinaten $M(\frac{1}{2}u_1, (u_2^2 + u_3^2 - u_1 \cdot u_2)/(2u_3)$ afleiden, maar niets hoeft ons er van te weerhouden om de coördinaten $M(x_3,x_4)$ en bijpassende hypothesen te gebruiken.

Het punt *P* ligt op de omgeschreven cirkel $\mathcal{C}$ en $|AM|^2 = |PM|^2$ geeft de vergelijking:

$x_3^2 + x_4^2 = (x_1 - x_3)^2 + (x_2 - x_4)^2$ oftewel $x_1^2 - 2 \cdot x_1 \cdot x_3 + x_2^2 - 2 \cdot x_2 \cdot x_4 = 0.$

De conditie dat *E* een punt van de lijn *AB* is en de conditie dat $PE \perp AB$, samen met de keuze van het assenstelsel, leveren de coördinaten van *E* op.

De conditie dat *F* een punt van de lijn *AC* is en de conditie dat $PF \perp AC$ leveren op:

$u_2 \cdot x_6 - u_3 \cdot x_5 = 0$ en $u_2 \cdot (x_5 - x_1) + u_3 \cdot (x_6 - x_2) = 0$.

De conditie dat *G* een punt van de lijn *BC* is en de conditie dat $PG \perp BC$ leveren op:

$(u_1 - u_2) \cdot x_8 - u_3 \cdot (u_1 - x_7) = 0$ en $(u_2 - u_1) \cdot (x_7 - x_1) + u_3 \cdot (x_8 - x_2) = 0$.

De condities voor niet-ontaardheid van de figuur zijn $u_1 \neq 0, u_3 \neq 0$. (*A* en *B* verschillen, en *C* ligt niet op de lijn *AB*).

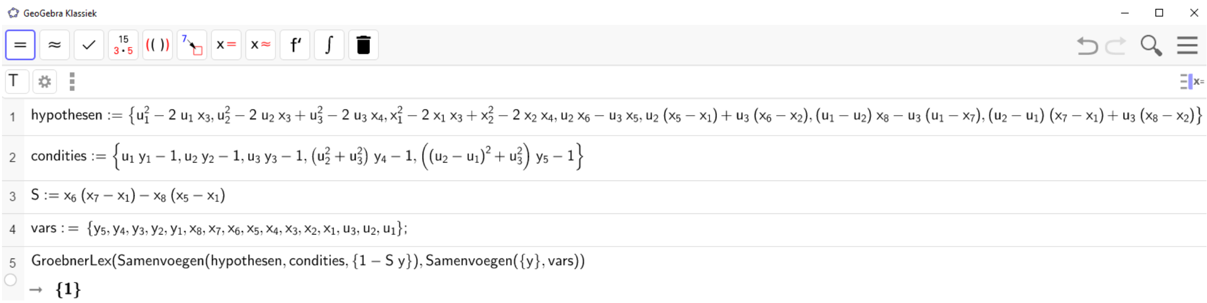
Tenslotte correspondeert de volgende vergelijking met de bewering dat *G* op de lijn *EF* ligt:

$x_6(x_7 - x_1) - x_8(x_5 - x_1) = 0$.

Wanneer je nu Methode 3 met bovenstaande hypothesen en condities toepast, dan vindt je helaas niet dat de Gröbner basis gelijk is aan {1}. Maar dit komt enkel omdat je nog niet voldoende veeltermcondities hebt gespecifieerd om de klus te klaren. Dit heeft ook te maken met het gegeven dat de stelling bewezen moet worden over reële getallen en niet over complexe getallen. Je moet dan extra voorwaarden introduceren. De condities waar GeoGebra zelf mee komt zijn dat de punten *A*, *B*, en C onderling verschillend moeten zijn, maar je kunt bijvoorbeeld ook denken aan voorwaarden dat het punt *P* niet gelijk mag zijn aan *A*, *B* of *C*. In het logboek kun je nalopen dat een Gröbner basis berekend wordt waarvan het resultaat wel gelijk aan {1} is. Best knap zo'n berekening in een hoogdimensionale ruimte. GeoGebra komt zelf met condities zoals

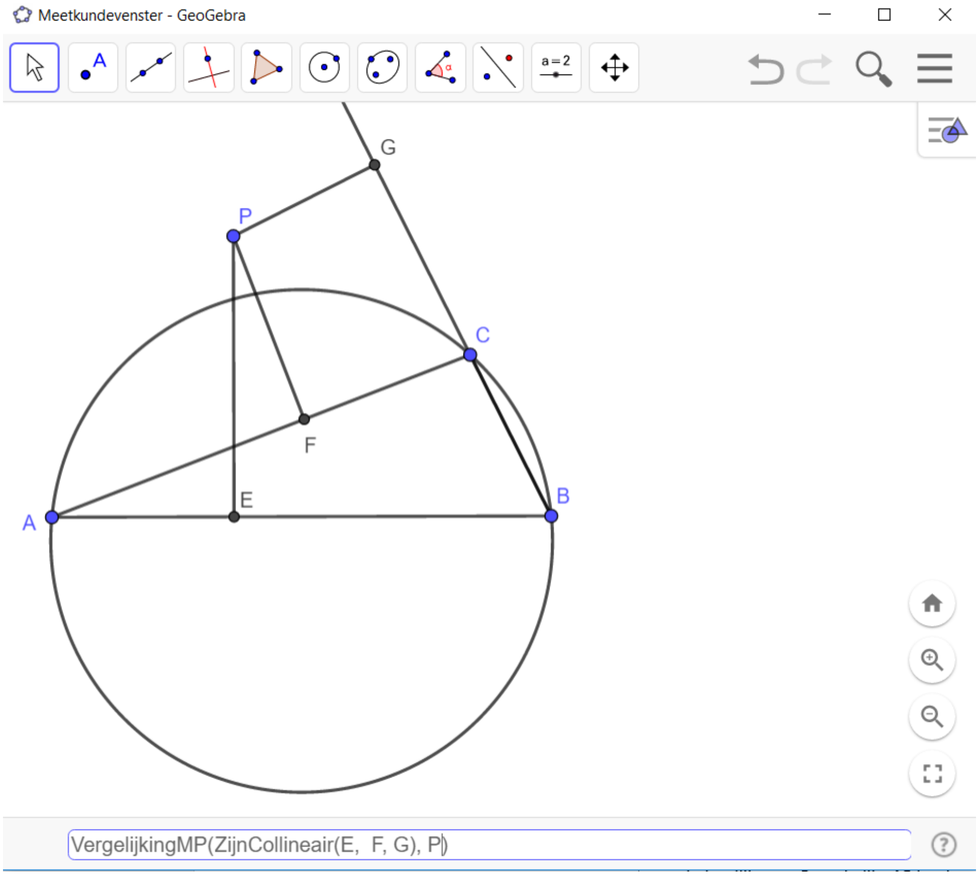
$$u_1 \neq 0,\; u_2 \neq 0,\; u_3 \neq 0,\; u_2^2 + u_3^2 \neq 0,\; u_3^2 + u_2^2 - 2 \cdot u_1 u_2 + u_1^2 \neq 0$$

In onderstaande schermafdruk kun je zien dat Methode 3 onder deze voorwaarden de stelling van Simson aantoont.



Stellingen ontdekken m.b.v. Gröbner bases in GeoGebra

We hebben tot nu toe stellingen bewezen via Gröbner basis methoden. Maar je kunt deze techniek ook gebruiken om stellingen te ontdekken, dat wil zeggen, om condities op te sporen waaronder een meetkundige bewering waar wordt. We doen dit aan de hand van het laatste voorbeeld van de stelling van Simson: een noodzakelijk en voldoende voorwaarde opdat de voetpunten van loodlijnen vanuit een punt *P* naar deze zijden van een driehoek op één lijn liggen is juist dat *P* op de omgeschreven cirkel van de driehoek ligt. Dit kun je Geogebra laten uitpuzzelen door de meetkundige plaats te bepalen van een punt *P* opdat drie andere geconstrueerde punten op één lijn liggen. Onderstaande schermafdruk laat zien hoe je dit met een commande VERGELIJKINGMP (de Nederlandse vertaling van LOCUSEQUATION). Ook nu start GeoGebra op de achtergrond een Gröbner basis methode om de vergelijking in de coördinaten van *P* op te stellen.



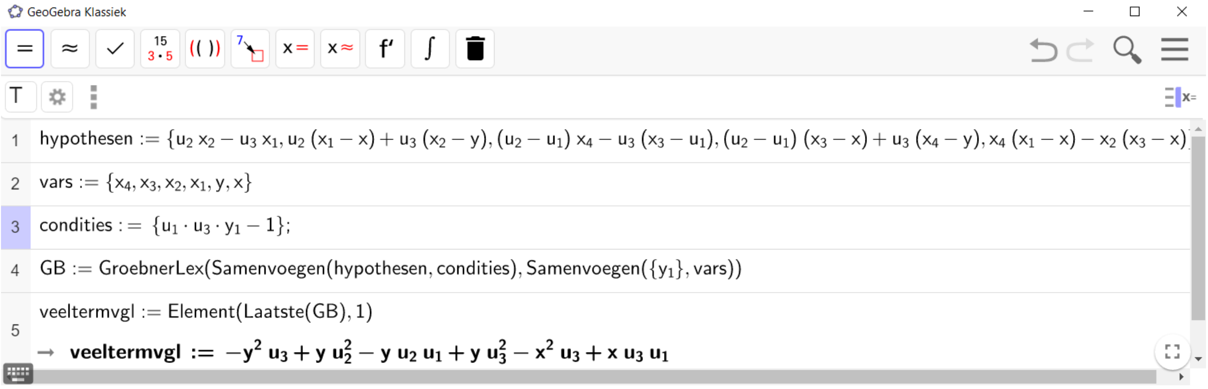
Hoe dit in zijn werk gaat? We bekijken een willekeurige driehoek *ABC* met hoekpunten $A(0,0)$, $B(u_1, 0)$, $C(u_2, u_3)$ zoals in bovenstaande figuur getekend is en we veronderstellen een niet-ontaarde situatie met $u_1 \neq 0$, $u_3 \neq 0$. De niet-ontaardheid vertalen we via de truc van Rabinowitsch tot de veelterm $u_1 \cdot u_3 \cdot y_1 - 1$. We nemen een algemeen punt $P(x, y)$. Het voetpunt *E* van de loodlijn van *P* op de lijn *AB* heeft coördinaten $(x, 0)$. Laat de andere voetpunten zijn $F(x_1, x_2)$ en $G(x_3, x_4)$. We stellen weer veeltermvergelijkingen op die bij de situatie passen:

F ligt op de lijn AC: $u_2 \cdot x_2 - u_3 \cdot x_1 = 0$
$PF \perp AC$ (loodrechte stand): $u_2 \cdot (x_1 - x) + u_3 \cdot (x_2 - y) = 0$

G ligt op de lijn BC: $(u_2 - u_1) \cdot x_4 - u_3 \cdot (x_3 - u_1) = 0$
$PG \perp BC$ (loodrechte stand): $(u_2 - u_1) \cdot (x_3 - x) + u_3 \cdot (x_4 - y) = 0$

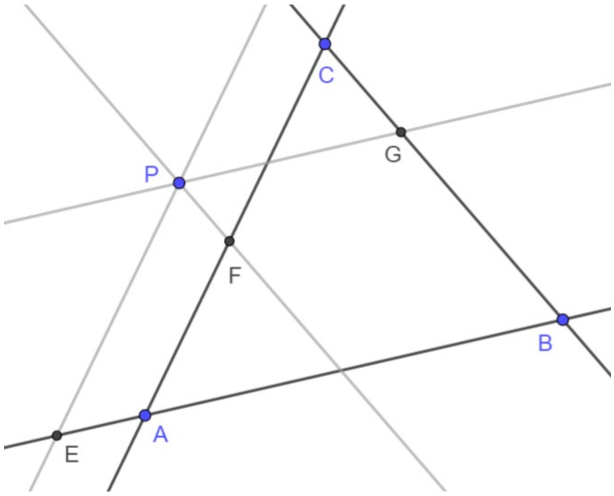
E, *F*, en *G* op één lijn: $x_4 \cdot (x_1 - x) - x_2 \cdot (x_3 - x) = 0$

Het resultaat krijg je nu door de Gröbner basis van de veeltermen aan de linkerkant van de gevonden veergelijkingen en de bij niet-ontaardheid passende veelterm te bepalen t.o.v. de lexicografische ordering met $x \prec y \prec x_1 \prec x_2 \prec x_3 \prec x_4 \prec y_1$. In deze basis kijk je naar het laatste element want dit is een vergelijking waarin de veeltermrelatie in de variabelen x, y. In onderstaande schermafdruk zie je het resultaat van de berekening in GeoGebra.



Het punt $P(x, y)$ ligt dus op de kromme met $x^2 - u_1 \cdot x + y^2 - y \cdot (u_2^2 + u_1 \cdot u_2 - u_3^2)/u_3 = 0$ als karakteriserende vergelijking. Dit is de vergelijking van een cirkel; in dit geval is het een bijzondere cirkel, namelijk de omgeschreven cirkel van de driehoek.

Opgave 7: Neem een willekeurige driehoek *ABC* en een willekeurig *P* in het vlak. Laat *E* de parallelle projectie van *P* op de lijn *AB* zijn, *F* de parallelle projectie van *P* op de lijn *AC*, en *G* de parallelle projectie van *P* op de lijn *BC* zoals in onderstaande constructie.



Zoek uit wanneer *E*, *F*, *G* op één lijn liggen.