De stelling van Abel-Ruffini

Liam Verhakkelaer

Inhoud

Inleiding

Het bewijs dat hier gegeven wordt van de stelling van Abel-Ruffini is grotendeels gebaseerd op het bewijs uit David Antins vertaling van"*100 Great Problems of Elementary Mathematics Their History and Solution*" van Heinrich Dörrie (Heinrich Dörrie, 1965). Het bewijs uit dit boek is weer gebaseerd op een theorema van Kronecker, dat gepubliceerd werd in 1856 in *Monatsberichte der Berliner Akademie*. Dit bewijs is evenwel zeer gecondenseerd en verwijst bijvoorbeeld slechts naar de, voor het bewijs van de stelling belangrijke, Theorema van Waring aangaande symmetrische polynomen, zonder hiervan een bewijs te geven. Bovendien is de terminologie verwarrend. In David Antins vertaling wordt bijvoorbeeld steeds het woord groep gebruikt voor zowel ringen als lichamen, zodat de lezer gemakkelijk in de knoop kan raken en daardoor vastloopt. Dat laatste is jammer en onnodig. Het bewijs van de stelling van Abel-Ruffini is inderdaad niet gemakkelijk, maar is goed te volgen met enig doorzettingsvermogen door iemand die het niveau heeft van zeg vwo wiskunde D.

Kennis van complexe getallen is een voorwaarde, alhoewel de eigenschappen van complexe getallen nog eens worden opgesomd, is het beter jezelf eerst hierin (nog eens) te trainen voor je hier aan begint, als je hier niet regelmatig mee werkt. Elementaire kennis aangaande priemgetallen, alhoewel de lezer intuïtief wellicht voldoende hiermee uit de voeten kan, maakt het begrijpen van bepaalde stappen makkelijker. Kennis van integraalrekening is niet nodig, maar differentiëren (differentiëren van veeltermen met product- en kettingregel) zo nu en dan wel. Bewijsvoering middels volledige inductie en uit het ongerijmde komt ook geregeld voor. Het is beter dit van te voren (ook nog eens) te bestuderen, als je hier niet geregeld mee werkt. In de tijd van internet mag het zich nog moeten toe-eigenen van de hier genoemde voorkennis, indien onvoldoende aanwezig, evenwel geen grote problemen opleveren. Het leren rekenen met complexe getallen, gebruik maken van eigenschappen van priemgetallen, het begrijpen van deze vormen van bewijsvoering etc. is niet overdreven moeilijk. Indien de lezer vindt dat ringen en lichamen hier onvoldoende uitgebreid worden behandeld, dan zijn hierover ook legio video's of inleidende documenten te vinden op het web. Eigenlijk weet iedere vwo en havo wiskunde B scholier intuïtief al wat lichamen zijn en een ring is zo mogelijk nog eenvoudiger. Lezers met kennis van groepen, ringen en lichamen, zullen zich er wellicht over verbazen dat groepen niet worden behandeld. De reden is eenvoudig: we hebben geen groepen nodig, alleen ringen van veeltermen en lichamen van waarden.

Afwijkend van wat doorgaans gebruikelijk is bij verhandelingen over de stelling van Abel-Ruffini, is het weglaten van een bespreking en afleiding van de formules van Cardano en Ferrari. Hier is bewust voor gekozen, omdat dit in geen enkel opzicht bijdraagt aan het begrijpen van het bewijs van de stelling van Abel-Ruffini en op het internet hier legio bewijzen van zijn te vinden. Bij de lezer wordt zo bovendien niet de valse verwachting gewekt, dat hij bij het bestuderen van de formules van Cardano en Ferrari zich al kennis heeft eigen gemaakt, die helpt bij het begrijpen van het bewijs van de stelling van Abel-Ruffini. Voor een uitgebreide goed te volgen bespreking van de formules van Cardano en Ferarri is het werk van Peter Pesics "*Abel's Proof*" (Pesic, 2003) zeer geschikt.

Voordat we beginnen aan een uitgebreide versie van het op David Antins vertaling gebaseerde bewijs, zullen we eerst een aantal belangrijke fundamentele zaken, zoals de grootste gemeenschappelijke deler van getallen en veeltermen, het Euclidisch Algoritme, stellingen mb.t. reducibele en irreducibele veeltermen etc. vrij uitgebreid behandelen. De lezer is zo volledig op de hoogte van een aantal belangrijke begrippen en algoritmes die in het bewijs uit de vertaling slechts worden genoemd of zeer summier worden toegelicht. Eveneens meen ik er in geslaagd te zijn om duidelijker te verwijzen naar voorgaande bewezen stellingen, maar vooral ook om beter toe te lichten waarom een bepaalde stap op basis van een zekere stelling legitiem is. Getrainde wiskundigen mogen het zelfs onnodig uitgebreid vinden, maar zij zijn hier niet de doelgroep.

In ieder geval is wat mij betreft de idee die binnen de academische wereld bij veel wiskundigen leeft, namelijk dat de stelling van Abel-Ruffini alleen begrepen kan worden door een derdejaars wiskunde student (sommigen maken het helemaal bont en hebben het over een graduate course van een jaar) die een heel semester de moderne abstracte versie van Galois theorie heeft moeten doorploegen, behoorlijk ontkracht met de verschijning van dit document. Nogmaals, in dit pakweg 46 pagina's

tellend bewijs moet iemand die wiskunde D op het vwo goed heeft doorlopen zijn weg weten te vinden! Eigenlijk is het te bizar voor woorden om te denken dat het wiskundig kunststukje van de destijds jonge man Abel, niet binnen het bereik zou liggen van het begripsvermogen van een wiskundig voldoende onderlegde middelbare scholier met doorzettingsvermogen, zoals ze op iedere school voor het voortgezet onderwijs altijd zijn te vinden.

Abels theorema (De Stelling van Abel-Ruffini)
Voor de oplossing van een vijfdegraads vergelijking met rationale coëfficiënten bestaat geen formule uitgedrukt in wortelvormen, rationale getallen en de coëfficiënten van de termen in de vergelijking.
Een wortelvorm is uiteraard hetzelfde als een gebroken macht.

Slordig geformuleerd:
om de oplossingen te vinden van de vergelijking $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$, waarbij a, b, c, d, e en f geschreven kunnen worden als breuken, bestaat niet iets soortgelijks als een abc-formule.

Voor de oplossing (het vinden van de nulwaarden van) een tweedegraadsvergelijking

$ax^2 + bx + c = 0$

hebben we de bekende abc formule

$x_1, x_2 = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$
Waarbij we zonder uitzondering hiermee bedoelen dat $x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$ en $x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$.

Analoog bedoelen we met $x_1, x_2 = \frac{-b \mp \sqrt{b^2-4ac}}{2a}$ dat $x_1 = \frac{-b-\sqrt{b^2-4ac}}{2a}$ en $x_2 = \frac{-b+\sqrt{b^2-4ac}}{2a}$.

De regel $-\pm \equiv \mp$ is de reden dat $\pm$ kan "omklappen".
Het theorema van Abel is niet even snel te bewijzen. Een aantal concepten moeten we daarvoor eerst duidelijker neerzetten.

1 Lichaam en lichaamsuitbreidingen
De rationale getallen weergegeven met $\mathbb{Q}$, vormen een zogenaamd lichaam. Dit houdt in dat

1) De uitkomst van de bekende berekeningen alleen maar bestaande uit getallen uit $\mathbb{Q}$ haakjes (evenveel linker, "(", als rechter, ")", haakjes), de bewerkingen + (optelling) en $\cdot$ (vermenigvuldiging), altijd weer een getal uit $\mathbb{Q}$ oplevert. We zeggen daarom dat $\mathbb{Q}$ gesloten is ten aanzien van de bekende berekeningen.
2) Er een rationaal getal 1 is dat vermenigvuldigd met ieder getal uit $\mathbb{Q}$ weer dit getal oplevert.
3) Er een rationaal getal 0 is dat opgeteld bij ieder getal uit $\mathbb{Q}$ weer dit getal oplevert.
4) Ieder rationaal getal, behalve 0, een rationale inverse heeft voor de vermenigvuldiging, zodat vermenigvuldiging van een rationaal getal met zijn inverse 1 oplevert.
5) Ieder rationaal getal een rationale inverse heeft voor de optelling, zodat optelling van een rationaal getal met zijn inverse 0 oplevert.

Voorbeelden
De inverse van $-\frac{3}{4}$ voor de vermenigvuldiging is $-\frac{4}{3}$, immers $-\frac{3}{4} \cdot -\frac{4}{3} = 1$
De inverse van $-\frac{3}{4}$ voor de optelling is $\frac{3}{4}$, immers $-\frac{3}{4} + \frac{3}{4} = 0$

Het gesloten zijn van een lichaam is een belangrijke eigenschap.
Van $\mathbb{Q}$ bestaan zogenaamde lichaamsuitbreidingen. Een lichaamsuitbreiding vormt ook weer een lichaam. Als we bijvoorbeeld behalve rationale getallen ook $\sqrt{2}$ gaan gebruiken in onze berekeningen, dan rekenen we binnen het lichaam dat we noteren als $\mathbb{Q}(\sqrt{2})$. Als we daarnaast ook nog eens bijvoorbeeld $\sqrt{5}$ willen gebruiken dan noteren we deze lichaamsuitbreiding als $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ enz.

Voorbeelden
Neem $\mathbb{Q}(\sqrt{3},\ \sqrt{5})$
De berekening $4\sqrt{3} + \frac{\sqrt{3}}{\sqrt{5}} \cdot 6\sqrt{5}$ heeft als uitkomst $10\sqrt{3}$, wat in overeenstemming is met de geslotenheid van $\mathbb{Q}(\sqrt{3},\ \sqrt{5})$.

De inverse van $\sqrt{5}$ is $\frac{1}{5}\sqrt{5}$, wat in overeenstemming is met de geslotenheid van $\mathbb{Q}(\sqrt{3},\ \sqrt{5})$.

De inverse van een veelterm in $\sqrt{5}$, zeg de berekening $3 + 4\sqrt{5} - 7\left(\sqrt{5}\right)^7$, is

$$\frac{1}{3 + 4\sqrt{5} - 7\left(\sqrt{5}\right)^7}$$

Nu is het niet altijd mogelijk om van berekeningen die kunnen worden weergegeven als veeltermen van de toegevoegde waarde de inverse uit te drukken in veeltermen van de toegevoegde waarde, zoals wel mogelijk bleek voor $\frac{1}{\sqrt{5}}$. De noodzaak om de inverse voor de vermenigvuldiging te handhaven gebied evenwel dat we ons tevreden moeten stellen met het gegeven dat waarden weergegeven als berekeningen van toegevoegde waarden niet altijd als veeltermen van de toegevoegde waarde kunnen worden weergegeven, maar b.v. als quotiënt van twee veeltermen.

Dat de willekeurige lichaamsuitbreiding $\mathbb{Q}(\alpha, \beta, \gamma, \dots)$ gesloten is, is makkelijk in te zien. Immers iedere algebraïsche uitdrukking bestaande uit de symbolen $\alpha, \beta, \gamma, \dots$ en rationale getallen, zal na een correcte herleiding geen andere dan deze symbolen en rationale getallen kunnen bevatten. Door als regel te gebieden dat de inversen van berekeningen met $\alpha, \beta, \gamma, \dots$ voor de vermenigvuldiging en de optelling dan eveneens worden toegevoegd, zijn de lichaamseigenschappen gegarandeerd. Merk op dat deze regel niet nodig is binnen de rationale getallen $\mathbb{Q}$, maar dat dit wel nodig is als we bijvoorbeeld het zuiver imaginaire getal i of irrationale waarden zoals π of $\sqrt{2}$ toevoegen. Aangezien we complexe nulwaarden gaan beschouwen is de toevoeging van i wel van belang. Toevoegingen zoals π hebben we hier niet nodig.
In het algemeen gebruiken we het symbool $\mathcal{L}$ om een lichaam aan te geven. $\mathcal{L}(\alpha)$ is dan eveneens een lichaam, maar ook een lichaamsuitbreiding van $\mathcal{L}$.

2 Veeltermen en ringen
Onder $\mathcal{L}[x]$ verstaan we de ring (wordt hierna toegelicht) van veeltermen in x, met coëfficiënten uit het lichaam $\mathcal{L}$. We noemen x de variabele van de veelterm. Een veelterm (ook wel polynoom genoemd) $f(x)$ van $\mathcal{L}[x]$ wordt een veelterm over $\mathcal{L}$ genoemd. Let goed op verschil tussen zeg $\mathcal{L}[\alpha]$ en $\mathcal{L}(\alpha)$; de eerste notatie met vierkante haken slaat op veeltermen met variabele α en met coëfficiënten uit $\mathcal{L}$, terwijl de tweede notatie met ronde haken slaat op een lichaamsuitbreiding door een waarde α toe te voegen. Neem

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Met variabele x en coëfficiënten a_i dan is de graad van een veelterm de exponent van de variabele met de hoogste macht. De graad van f is dus n. We noteren $\deg(f) = n$. Waarbij deg afkomstig is van het Engelse woord voor graad, degree. Voor het gemak noteren we soms f in plaats van $f(x)$. We noemen a_n de leidende coëfficiënt. Als de leidende coëfficiënt 1 is, dus $a_n = 1$, dan noemen we f monisch. De veelterm $p(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is dus monisch. We zeggen ook wel dat p een monische veelterm of een monische polynoom is.

*Belangrijk is het inzicht dat een **veelterm** slaat op de **vorm***! In de vergelijking

$$x^2 - 1 = (x + 1) \cdot (x - 1)$$

is het linker lid een veelterm. Dit in tegenstelling tot het rechter lid dat geen veelterm is, maar het product van twee veeltermen! Dit subtiel onderscheid maken tussen de vorm en rekenkundig gelijk zijn aan elkaar als we getallen gaan invullen voor x, is één van de oorzaken die het bewijzen van de stelling van Abel tot een lastige onderneming maakt.

De constante veelterm $f(x) = a_0$ heeft alle coëfficiënten behalve a_0 niet noodzakelijkerwijs, gelijk aan nul. Als eveneens $a_0 = 0$ dan is f de nulpolynoom.
Nu vormen veeltermen over een lichaam $\mathcal{L}$ een zogenaamde ring $\mathcal{L}[x]$. Een ring bleek uiteindelijk na veel uitproberen door wiskundigen om zaken efficiënt te kunnen omschrijven en gebruiken een handig concept. Bijvoorbeeld om het geheel van veeltermen als gesloten geheel waarmee enigszins kan worden gerekend, weer te geven. Voor de ring $\mathcal{L}[x]$ gelden, net zoals voor iedere ring, de volgende regels.

1) De uitkomst van de bekende berekeningen alleen maar bestaande uit veeltermen uit $\mathcal{L}[x]$ haakjes (evenveel linker, "(", als rechter, ")", haakjes), de bewerkingen + (optelling) en · (vermenigvuldiging), altijd weer een veelterm uit $\mathcal{L}[x]$ oplevert. We zeggen daarom dat $\mathcal{L}[x]$ gesloten is ten aanzien van de bekende berekeningen, met uitsluiting van ÷.
2) Er is een nulpolynoom (de veelterm waarvan alle coëfficiënten gelijk nul zijn) die opgeteld bij iedere veelterm uit $\mathcal{L}[x]$ weer deze veelterm oplevert.
3) Voor iedere polynoom is er een inverse voor de optelling. De optelling van een veelterm met zijn inverse geeft de nulpolynoom.

De veeltermen over $\mathcal{L}$ vormen geen lichaam, aangezien er geen inverse veelterm over $\mathcal{L}$ is voor een veelterm uit $\mathcal{L}[x]$ ten aanzien van de vermenigvuldiging. Het is waar dat bijvoorbeeld $3x^4 \cdot \frac{1}{3}x^{-4} = 1$, maar $\frac{1}{3}x^{-4}$ is geen veelterm, aangezien de variabele het grondtal is van een macht met een negatieve exponent.

Voorbeeld
De inverse veelterm van $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is
$$-f(x) = -a_n x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$$

De gehele getallen, $\mathbb{Z}$, vormen net als veeltermen over een zeker lichaam ook een ring, de natuurlijke getallen, $\mathbb{N}$, evenwel niet (waarom wel en waarom niet?).

3 Het deler-algoritme voor veeltermen (polynomen)
Laat $f(x)$ en $g(x)$ veeltermen zijn, maar niet de nulpolynoom, over $\mathcal{L}$. Dan zijn er unieke veeltermen $q(x)$ en $r(x)$ uit $\mathcal{L}[x]$ zo dat
$$f(x) = q(x) \cdot g(x) + r(x)$$

Met $\deg(r) < \deg(g)$ of $r(x) = 0$. Als $f(x)$ en $g(x)$ over $\mathbb{Z}$ (de gehele getallen) zijn en $g(x)$ is *monisch*, dan zijn $q(x)$ en $r(x)$ ook uit $\mathbb{Z}[x]$ (inderdaad $\mathbb{Z}$ is geen lichaam, maar een groep, want $\mathbb{Z}$ is gesloten ten aanzien van berekeningen die alleen bestaan uit gehele getallen, haakjes en " +", dus zonder " · ").

Door middels een staartdeling g op f te delen (betekent hetzelfde als f delen door g) is dit gemakkelijk in te zien. Zie het voorbeeld hieronder

$g(x) = x^2 - 4x + 3 \,/\, f(x) = x^4 - x^3 - 2x - 77 \setminus q(x) = x^2 + 3x + 9$

$$\begin{array}{rl} & \underline{x^4 - 4x^3 + 3x^2} \\ & 3x^3 - 3x^2 - 2x - 77 \\ & \underline{3x^3 - 12x^2 + 9x} \\ & 9x^2 - 11x - 77 \\ & \underline{9x^2 - 36x + 27} \\ r(x) = & 25x - 50 \end{array}$$

Dus

$$\frac{f(x)}{g(x)} = \frac{x^4 - x^3 - 2x - 77}{x^2 - 4x + 3} = x^2 + 3x + 9 + \frac{25x - 50}{x^2 - 4x + 3} = q(x) + \frac{r(x)}{g(x)}$$

Dus

$$f(x) = q(x) \cdot g(x) + r(x)$$

Als $g(x)$ niet monisch zou zijn dan is het niet gegarandeerd dat $q(x)$ en $r(x)$ ook over $\mathbb{Z}$ zijn.
Ook dit is met een geschikt voorbeeld gemakkelijk in te zien. We nemen nu als leidende coëfficiënt van $g(x)$ het getal 2 ($g(x)$ is nu nog steeds over $\mathbb{Z}$, maar niet meer monisch).

$g(x) = 2x^2 - 4x + 3 \,/\, f(x) = x^4 - x^3 - 2x - 77 \setminus q(x) = \frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{4}$

$$\begin{array}{rl} & x^4 - 2x^3 + 1\frac{1}{2}x^2 \\ & \text{----------} \\ & x^3 - 1\frac{1}{2}x^2 - 2x - 77 \\ & x^3 - 2x^2 + 1\frac{1}{2}x \\ & \text{----------} \\ & \frac{1}{2}x^2 - 3\frac{1}{2}x - 77 \\ & \frac{1}{2}x^2 - x + \frac{3}{4} \\ & \text{----------} \\ r(x) = & -2\frac{1}{2}x - 77\frac{3}{4} \end{array}$$

Het is zo duidelijk dat als we het proces van delen van $g(x)$ op $f(x)$ nalopen en de leidende coëfficiënt van $g(x)$ niet 1 is, de veeltermen $q(x)$ en rest $r(x)$ niet gegarandeerd over $\mathbb{Z}$ zijn.

Als $r(x) = 0$ dan noemen we $g(x)$ een **deler** van $f(x)$.

Het Euclidisch Algoritme voor polynomen en haar gevolgen
In deze paragraaf gaan we ons verdiepen in het Euclidisch algoritme voor het vinden van de grootste gemeenschappelijke deler van twee polynomen, om vervolgens deze grootste gemeenschappelijke deler als lineaire combinatie van deze twee polynomen te kunnen weergeven.

Laten we beginnen met het vinden van de grootste gemeenschappelijke deler van twee (altijd gehele) getallen. Bijvoorbeeld 180 en 210. Dit kan bijvoorbeeld door beide getallen te ontbinden (in priemfactoren).
De eerste 8 priemgetallen zijn 2, 3, 5, 7, 11, 13, 17 en 23, zodat

$180 = 6 \cdot 30 = 3 \cdot 2 \cdot 6 \cdot 5 = 3 \cdot 2 \cdot 3 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$ en
$210 = 30 \cdot 7 = 2 \cdot 3 \cdot 5 \cdot 7$

De gemeenschappelijke priemfactoren zijn 2 (één keer), 3 (één keer) en 5. De grootste

gemeenschappelijke delen van 180 en 210 is $2 \cdot 3 \cdot 5 = 30$. We noteren $ggd(180,210) = 30$.

Merk verder op dat

$$\begin{aligned} 210 &= 7 \cdot 30 \\ 180 &= 6 \cdot 30 \qquad \text{dus} \\ 210 - 180 &= 1 \cdot 30 \end{aligned}$$

Waardoor $30 = 210 + -1 \cdot 180$, dus $ggd(180,210) = 210 + -1 \cdot 180$

We hebben zo de ggd van 210 en 180 geschreven als een zogenaamde lineaire combinatie van 210 en 180 (met gebruikmaking van alleen maar gehele getallen).

Doorgaans is ontbinden een onhandige methode om de ggd van twee getallen (en zeker om later van twee polynomen) te vinden en de ggd te schrijven als een lineaire combinatie van deze twee getallen. Het is beter om het Euclidisch algoritme te gebruiken. We laten eerst een toepassing zien en tonen daarna aan dat we zo inderdaad de ggd hebben gevonden.

Vind de ggd van 140 en 297.

140 / 297 \ 2 $\qquad 297 = 2 \cdot 140 + 17 \quad dus \quad 17 = 297 - 2 \cdot 140$
280
rest1 17

17/ 140 \ 8 $\qquad 140 = 8 \cdot 17 + 4 \quad dus \quad 4 = 140 - 8 \cdot 17$
136
rest2 4

4 / 17 \ 4 $\qquad 17 = 4 \cdot 4 + 1 \quad dus \quad 1 = 17 - 4 \cdot 4$
16
rest3 1

1 / 4 \ 4 $\qquad 4 = 4 \cdot 1 \quad waardoor \quad ggd(140, 297) = 1$
4
0 geen rest

Je begint dus met het delen van de grootste door de kleinste getal van de twee gegeven getallen. Als dit een *rest1* oplevert, deel je het kleinste getal door de *rest1*. Als dit weer een *rest2* oplevert deel je rest1 door *rest2* enz., totdat je geen rest meer krijgt. Het laatste rest, *rest3* in ons voorbeeld, is de ggd. Overigens, omdat $ggd(140, 297) = 1$ en niet een ander getal zeggen we dat 140 en 297 relatief priem zijn.

Door terug te rekenen met de laatste sommen achter "dus" kunnen we $ggd(140, 297)$ schrijven als een lineaire combinatie van 140 en 297. Immers

$$ggd(140, 297) = 1 = [17] - 4 \cdot (4) = [17] - (140 - 8 \cdot [17])$$
$$= [297 - 2 \cdot 140] - (140 - 8 \cdot [297 - 2 \cdot 140]) = 33 \cdot 297 - 70 \cdot 140$$

Maar hoe weten we zo zeker dat 1 inderdaad de grootste gemeenschappelijke deler van 140 en 297 is?

Bewijs dat met het Euclidisch algoritme de ggd wordt gevonden
Pas nu het Euclidisch algoritme toe op twee willekeurige getallen a en b, waarbij we zonder de algemeenheid te schaden veronderstellen dat $a < b$. We krijgen zo

$$b = n0 \cdot a + r1$$
$$a = n1 \cdot r1 + r2$$
$$r1 = n2 \cdot r2 + r3$$
$$r2 = n3 \cdot r3 + r4$$
$$r3 = n4 \cdot r4$$

We nemen in deze algemene situatie aan dat er geen rest $r5$ meer is. Uiteraard had dit wel gekund maar ergens moet dit proces stoppen bij een kleinste rest aangezien we alleen maar met gehele getallen werken en $0 < r4 < r3 < r2 < r1$ (Ga na!).

Merk op dat $r4$ een deler is van $r3$ (laatste regel). Maar dan is $r4$ ook een deler van $r2$, aangezien $r4$ een deler is van $n3 \cdot r3$ en $r4$ en dus ook van de som van $n3 \cdot r3$ en $r4$ (tweede regel). Zo is $r4$ dan ook een deler van $r1$ (derde regel) , van a (tweede regel) en tenslotte ook van b (eerste regel). De laatste rest is dus een deler van a en b.
Neem voorts aan dat d ook een willekeurige deler is van a en b. En herschrijf de eerste vier regels verkregen met het Euclidisch algoritme. We noteren

$$r1 = b - n0 \cdot a$$
$$r2 = a - n1 \cdot r1$$
$$r3 = r1 - n2 \cdot r2$$
$$r4 = r2 - n3 \cdot r3$$

Omdat d een deler is van b en a is d ook een deler van $r1 = b - n0 \cdot a$.
Omdat d een deler is van a en $r1$ is d ook een deler van $r2 = a - n1 \cdot r1$
Omdat d een deler is van $r2$ en $r1$ is d ook een deler van $r3 = r1 - n2 \cdot r2$
Omdat d een deler is van $r3$ en $r2$ is d ook een deler van $r4 = r2 - n3 \cdot r3$

Maar dan is $d \leq r4$. Dus iedere deler van a en b is kleiner of gelijk aan $r4$, zodat $ggd(a, b) = r4$.

De laatste rest is dus de grootste gemeenschappelijke deler.

Einde bewijs

Gevolg Euclidisch algoritme: de ggd van twee getallen kan als lineaire combinatie van deze twee getallen worden geschreven.

Bewijs
Om in het algemene voorbeeld a en b als lineaire combinatie van $ggd(a, b)$ te schrijven passen we een aantal opeenvolgende substituties toe.

$$ggd(a,b) = r4 = r2 - n3 \cdot r3 = r2 - n3 \cdot (r1 - n2 \cdot r2) = (1 + n2 \cdot n3)r2 - n3 \cdot r1$$
$$= (1 + n2 \cdot n3)(a - n1 \cdot r1) - n3 \cdot r1$$
$$= (1 + n2 \cdot n3)a - (n1 + n1 \cdot n2 \cdot n3 + n3)r1$$
$$= (1 + n2 \cdot n3)a - (n1 + n1 \cdot n2 \cdot n3 + n3)(b - n0 \cdot a)$$
$$= (1 + n2 \cdot n3 + n0 \cdot n1 + n0 \cdot n1 \cdot n2 \cdot n3 + n0 \cdot n3) \cdot a - (n1 + n1 \cdot n2 \cdot n3 + n3) \cdot b$$

Het proces levert als gevolg van de opeenvolgende substituties vanzelfsprekend het gestelde gevolg op.

Einde bewijs

Dan gaan we nu hetzelfde doen voor veeltermen. We beginnen met een voorbeeld.

Beschouw de polynomen

$$f(x) = x^4 - x^3 - 2x - 77$$

en

$$g(x) = x^2 - 4x + 3$$

We delen nu g op f (vanwege de volgorde bij een staartdeling spreken we van delen op en niet delen door) en delen volgens het Euclidisch algoritme verder iedere rest op zijn voorgaande deler tot we geen rest meer hebben.

$$x^2 - 4x + 3 \,/\, x^4 - x^3 - 2x - 77 \setminus x^2 + 3x + 9$$
$$\underline{x^4 - 4x^3 + 3x^2}$$
$$3x^3 - 3x^2 - 2x - 77$$
$$\underline{3x^3 - 12x^2 + 9x}$$
$$9x^2 - 11x - 77$$
$$\underline{9x^2 - 36x + 27}$$
$$rest1 = \quad 25x - 50$$

$$25x - 50 \;\; / \, x^2 - 4x + 3 \setminus \tfrac{1}{25}x + -\tfrac{2}{25}$$
$$\underline{x^2 - 2x}$$
$$-2x + 3$$
$$\underline{-2x + 4}$$
$$laatste\ rest = \quad -1$$

$$-1 \,/\, 25x - 50 \setminus -25x + 50$$
$$\underline{25x}$$
$$-50$$
$$\underline{-50}$$
$$0 \qquad \text{geen rest}$$

We kunnen nu achtereenvolgens noteren

$$f(x) = x^4 - x^3 - 2x - 77 = (x^2 + 3x + 9)(x^2 - 4x + 3) + 25x - 50$$
$$= (x^2 + 3x + 9) \cdot g(x) + rest1$$

en

$$g(x) = x^2 - 4x + 3 = \left(\frac{1}{25}x + -\frac{2}{25}\right)(25x - 50) - 1 = \left(\frac{1}{25}x + -\frac{2}{25}\right) \cdot rest1 + laatste\ rest$$

Overhevelen geeft

$$rest1 = f(x) - (x^2 + 3x + 9) \cdot g(x)$$

en

$$laatste\ rest = g(x) - \left(\frac{1}{25}x + -\frac{2}{25}\right) rest1$$

De laatste uitdrukking geeft na substitutie

$$laatste\ rest = g(x) - \left(\frac{1}{25}x + -\frac{2}{25}\right)(f(x) - (x^2 + 3x + 9) \cdot g(x)) =$$

$$= \left(-\frac{1}{25}x + \frac{2}{25}\right) \cdot f(x) + \left(1 + \left(\frac{1}{25}x + -\frac{2}{25}\right)(x^2 + 3x + 9)\right) \cdot g(x)$$

Hieruit valt af te leiden dat

$$1 = -1 \cdot -1 = -1 \cdot laatste\ rest = \left(\frac{1}{25}x - \frac{2}{25}\right) \cdot f(x) + -\left(1 + \left(\frac{1}{25}x + -\frac{2}{25}\right)(x^2 + 3x + 9)\right) \cdot g(x)$$

Het linker lid is nu een constante veelterm waarvan de leidende coëfficiënt 1 is, dus deze veelterm is monisch. Deze veelterm is tevens een grootste gemeenschappelijke deler van f en g, immers uit

$$rest1 = f(x) - (x^2 + 3x + 9) \cdot g(x)$$
$$laatste\ rest = g(x) - \left(\frac{1}{25}x + -\frac{2}{25}\right) rest1$$

volgt dat als veelterm $p(x)$ een deler is van $f(x)$ en $g(x)$, dat $p(x)$ dan ook een deler van $rest1$ en daarom ook een deler van de $laatste\ rest = -1$ is en dus ook van de monische veelterm 1 is.

Als we nu de ggd van $f(x)$ en $g(x)$ definiëren als de **monische veelterm** die beide veeltermen deelt, en dat iedere gemeenschappelijke deler van f en g ook deze monische veelterm deelt kunnen we uit het voorgaande concluderen dat $ggd(f, g) = 1$.

Omdat $ggd(f, g) = 1$ zijn f en g ook nog eens relatief priem.

Uiteindelijk zien we zo middels

$1 = -1 \cdot -1 = laatste\ rest \cdot -1 = \left(\frac{1}{25}x - \frac{2}{25}\right) \cdot f(x) + -\left(1 + \left(\frac{1}{25}x + -\frac{2}{25}\right)(x^2 + 3x + 9)\right) \cdot g(x)$

dat er polynomen $s(x) = \frac{1}{25}x - \frac{2}{25}$ en $t(x) = -\left(1 + \left(\frac{1}{25}x + -\frac{2}{25}\right)(x^2 + 3x + 9)\right)$ zijn zodat

$$ggd(f, g) = s(x) \cdot f(x) + t(x) \cdot g(x)$$

Oefening

Gegeven is de polynoom $h(x) = x^4 - x^3 - 2x + 2$ en wederom $g(x) = x^2 - 4x + 3$.
Laat zien dat

$$ggd(h, g) = x - 1 = \left(\frac{1}{25}\right) h(x) + \frac{1}{25}(-x^2 - 3x - 9)g(x)$$

Samenvatting 3

1. Rekenregel voor de graad van twee veeltermen:
   $\deg(f + g) = \max\{\deg(f), \deg(g)\}$ en $\deg(f \cdot g) = \deg(f) + \deg(g)$. Vrij triviale regels.

2. Deler-algoritme. Laat $f(x)$ en $g(x)$ veeltermen zijn en $g(x)$ niet de nulpolynoom, over $\mathcal{L}$. Dan zijn er unieke veeltermen $q(x)$ en $r(x)$ in $\mathcal{L}[x]$ zo dat

   $$f(x) = q(x) \cdot g(x) + r(x)$$

   Met $\deg(r) < \deg(g)$ of $r(x) = 0$. Als $f(x)$ en $g(x)$ over $\mathbb{Z}$ zijn en $g(x)$ is *monisch*, dan zijn $q(x)$ en $r(x)$ ook uit $\mathbb{Z}[x]$.

   Merk op dat wegens de rekenregel voor graden volgt dat $\deg(f) \geq \deg(g)$.

A. Neem twee willekeurige polynomen f en g, dan hebben deze een unieke grootste gemeenschappelijke deler, genoteerd als $ggd(f, g)$; $ggd(f, g)$ is per definitie een monische polynoom (anders kan er geen unieke ggd worden gedefinieerd).

B. Uit het voorgaande valt de volgende vanzelfsprekende stelling af te leiden. Er zijn polynomen $s(x)$ en $t(x)$ zo dat $ggd(f, g) = s(x) \cdot f(x) + t(x) \cdot g(x)$.

C. Als $ggd(f, g) = 1$ noemen we f en g relatief priem. Er bestaan in dit belangrijke geval derhalve twee polynomen $s(x)$ en $t(x)$ zodanig dat $s(x)f(x) + t(x)g(x) = 1$.

4 Reducibele en irreducibele veeltermen (polynomen)

Lichaamsuitbreidingen (nog een keer) en deellichamen
Nu was $\mathbb{Q}$ een lichaam van rationale getallen (te schrijven als een breuk). Het lichaam $\mathbb{Q}(\sqrt{2}\,)$ is een zogenaamde lichaamsuitbreiding van $\mathbb{Q}$. We noemen $\mathbb{Q}$ daarom een deellichaam van $\mathbb{Q}(\sqrt{2}\,)$. Nu is $\mathbb{Q}(\sqrt{2},\sqrt{5}\,)$ een lichaamsuitbreiding van zowel $\mathbb{Q}$ als van $\mathbb{Q}(\sqrt{2}\,)$, die beide weer deellichamen zijn van $\mathbb{Q}(\sqrt{2}\,,\sqrt{5}\,)$. We zeggen voordehand liggend dat $\mathbb{Q}(\sqrt{2}\,)$ tussen $\mathbb{Q}$ en $\mathbb{Q}(\sqrt{2}\,,\sqrt{5}\,)$ in ligt.

Nulwaarde van een veelterm
Laat $f(x)$ een niet-constante polynoom (variabele veelterm) uit $\mathcal{L}[x]$ zijn, dan is α een nulwaarde van $f(x)$ als $f(\alpha)=0$. Merk op dat α niet noodzakelijkerwijs uit $\mathcal{L}$ is.

Stelling 4.1
Laat $f(x)$ een variabele veelterm uit $\mathcal{L}[x]$ zijn, en laat α een nulwaarde van $f(x)$ zijn. Dan is $x-\alpha$ een deler van $f(x)$.

Bewijs
Neem de lichaamsuitbreiding $\mathcal{U}$ die α bevat. Volgens het deler-algoritme zijn er veeltermen $q(x)$ en $r(x)$ uit $\mathcal{U}[x]$ zodanig dat

$$f(x)=q(x)(x-\alpha)+r(x)$$

met $\deg(r)<\deg(x-\alpha)=1$ of $r(x)=0$, waarmee $r(x)$ een constante veelterm is, zeg $r(x)=a_0$. Door α in te vullen krijgen we $f(\alpha)=q(\alpha)(\alpha-\alpha)+a_0$, oftewel de rest $r(x)=a_0=0$. Dus $x-\alpha$ is een deler is van$f(x)$ en we kunnen $f(x)$ schrijven in de vorm $f(x)=q(x)\cdot(x-\alpha)$.

Einde bewijs

Een variabele veelterm $f(x)$ over een bepaald lichaam $\mathcal{L}$ is ***irreducibel*** over $\mathcal{L}$ als $f(x)$ niet geschreven kan worden als het product van twee veeltermen uit $\mathcal{L}$, beide met een graad lager dan $\deg(f)$; in alle andere gevallen noemen we $f(x)$ ***reducibel*** over $\mathcal{L}$. Dat de graad van beide polynomen lager moet zijn is cruciaal, anders kunnen we $f(x)$ triviaal voor ieder $c\neq 0$ schrijven als $c\cdot\frac{1}{c}f(x)$. Dat we ons beperken tot variabele veeltermen levert ons de "uniciteit van ontbinden in factoren" op (verderop wordt dit bewezen). Zonder de eis zou iedere constante veelterm uit $\mathcal{L}[x]$ reducibel zijn. Bijvoorbeeld x en $1\cdot x$ worden in dat geval twee verschillende ontbindingen van x in polynomen die "irreducibel" zijn over $\mathcal{L}$. Anders dan de situatie bij het **deler-algoritme** en het **Euclidisch algoritme**, is irreducibel zijn ten nauwste verbonden met het omvattende lichaam. Bijvoorbeeld, x^2-2 is irreducibel over $\mathbb{Q}$, maar reducibel over $\mathbb{Q}(\sqrt{2}\,)$:

$$x^2-2=(x-\sqrt{2}\,)(x+\sqrt{2}\,)$$

Stelling 4.2
Laat $f(x)$ een variabele veelterm uit $\mathcal{L}[x]$ zijn met leidende coëfficiënt c en laat tevens $g_i(x)$, met $1\leq i\leq n$, veeltermen zijn uit $\mathcal{L}[x]$. Dan volgt

(A) $f(x)$ is irreducibel over $\mathcal{L}$

$\Leftrightarrow$

(B) $f(x)$ deelt $g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_n(x)$ $\quad \Longrightarrow \quad$ $f(x)$ is een deler van minstens één van de $g_i(x)$

Bewijs

$(A) \Longrightarrow (B)$ Middels inductie.

Neem $n = 2$, dan hebben we: $f(x)$ is irreducibel en $f(x)$ een deler is van $g_1(x) \cdot g_2(x)$. We moeten nu aantonen dat $f(x)$ minstens één van twee veeltermen in het rechterlid deelt. Als $f(x)$ één van beide, zeg zonder de algemeenheid te schaden $g_1(x)$, deelt, dan zijn we klaar. Neem nu het andere geval namelijk dat $f(x)$ geen deler is van $g_1(x)$. Maar dan moet aangezien $ggd(f, g_1)$ zowel $f(x)$ als $g_1(x)$ deelt, gelden dat $ggd(f, g_1) = \frac{1}{c} \cdot f(x)$ of $ggd(f, g_1) = 1$. De eerste mogelijkheid vervalt, aangezien $f(x)$ geen deler is van $g_1(x)$. Volgens het Euclidisch algoritme zijn er nu veeltermen $s(x)$ en $t(x)$ uit $\mathcal{L}[x]$ zodanig dat $s(x) \cdot f(x) + t(x) \cdot g_1(x) = 1$, dus

$$s(x) \cdot f(x) \cdot g_2(x) + t(x) \cdot \underbrace{g_1(x) \cdot g_2(x)}_{f \text{ deelt } g_1 \cdot g_2} = g_2(x)$$

Aangezien $f(x)$ beide termen in het linker lid deelt, deelt $f(x)$ ook het rechter lid $g_2(x)$. Maar dan deelt $f(x)$ is een deler van minstens één van de $g_i(x)$, met $1 \leq i \leq 2 = n$. Voor $n = 2$ klopt daarmee zo het gestelde.

Onze inductiehypothese voor $n > 2$ is nu: *Als $f(x)$ het product van $n - 1$ veeltermen deelt, dan deelt $f(x)$ minstens één van deze veeltermen*.

Voor $n > 2$ hebben we wederom dat $f(x)$ veelterm $g_1(x)$ wel of niet deelt. In het eerste geval zijn we klaar. In het tweede geval volgt net als hiervoor dat op grond van het Euclidisch algoritme er nu veeltermen $s(x)$ en $t(x)$ uit $\mathcal{L}[x]$ zijn zodat $s(x) \cdot f(x) + t(x) \cdot g_1(x) = 1$, dus

$$s(x) \cdot f(x) \cdot g_n(x) + t(x) \cdot \underbrace{g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_n(x)}_{f \text{ deelt } g_1 \cdot g_2 \cdot \ldots \cdot g_n} = g_2(x) \cdot \ldots \cdot g_n(x)$$

Bijgevolg deelt $f(x)$ het product van de $n - 1$ veeltermen $g_2(x), \ldots, g_n(x)$ in het rechterlid. Volgens de inductiehypothese is $f(x)$ dan een deler is van minstens één van deze $n - 1$ veeltermen $g_i(x)$ met $2 \leq i \leq n$. Waarmee $(A) \Longrightarrow (B)$ is aangetoond.

$(A) \Longleftarrow (B)$

Uit het ongerijmde. Neem aan dat $f(x)$ reducibel is. Dan zijn er $g(x)$en $h(x)$ uit $\mathcal{L}[x]$, allebei niet constant, zodat $f(x) = g(x) \cdot h(x)$. In dat geval is triviaal gezien $f(x)$ een deler van $g(x) \cdot h(x)$. Onder de aanname van (B) is $f(x)$ een deler van $g(x)$ of $h(x)$, dus $g(x)$ of $h(x)$ moet minstens de graad van $f(x)$ hebben, maar omdat $f(x) = g(x) \cdot h(x)$ kan $g(x)$ noch $h(x)$ noch het product $g(x) \cdot h(x)$ een graad hoger hebben dan $f(x)$. De enige overgebleven optie is dat $g(x)$ dezelfde graad heeft als $f(x)$ en $h(x)$ een constante is of dat $g(x)$ constant is en $h(x)$ dezelfde graad heeft als $f(x)$. Dat is in tegenspraak met de voorwaarde dat $g(x)$ en $h(x)$ beide niet constant is. In dat geval verwerpen we de aanname dat $f(x)$ reducibel is. Dus $f(x)$ is reducibel.

Einde bewijs

Stelling 4.3
Laat $f(x)$ een variabele veelterm uit $\mathcal{L}[x]$ zijn, en laat α een nulwaarde van $f(x)$ zijn. Dan zijn equivalent:

A. $f(x)$ is irreducibel over $\mathcal{L}$ (dus α is dan niet uit $\mathcal{L}$!).
B. Geen enkele veelterm uit $\mathcal{L}[x]$ met α als nulwaarde, heeft een lagere graad dan de graad van $f(x)$.
C. $f(x)$ is een deler van iedere veelterm uit $\mathcal{L}[x]$ met α als nulwaarde.

Bewijs

A. $\Longrightarrow$ B.
Omdat $f(x)$ een variabele veelterm uit $\mathcal{L}[x]$ is met nulwaarde α, zijn er dergelijke veeltermen met een laagste graad. Laat $g(x)$ zo'n veelterm zijn. Uit het deler-algoritme volgt dat er veeltermen $q(x)$ en $r(x)$ uit $\mathcal{L}[x]$ zijn, zodanig dat

$$f(x) = q(x) \cdot g(x) + r(x)$$

met $\deg(r) < \deg(g)$ of met $\deg(r) = 0$. Als we α invullen voor x krijgen we $r(\alpha) = 0$. Omdat veronderstelt is dat $g(x)$ een veelterm is met de laagst mogelijke graad met α als nulwaarde en $\deg(r) < \deg(g)$ zijn we verplicht $r(x) = 0$ te nemen, dus dat $r(x)$ de nulpolynoom is (die geen nulwaarden heeft gezien de onbepaaldheid, omdat iedere waarde anders een nulwaarde van de nulpolynoom zou zijn). Dus $f(x) = q(x) \cdot g(x)$. Omdat $f(x)$ wegens A. over $\mathcal{L}$ irreducibel is en $g(x)$ een variabele veelterm is (een constante veelterm heeft geen nulwaarden), mag $g(x)$ geen lagere graad hebben dan die van $f(x)$ (bijgevolg moet $q(x)$ een constante veelterm zijn). Hier is alleen aan voldaan als $\deg(f) = \deg(g)$, waaruit B. volgt.

B. $\Longrightarrow$ C.
Laat $g(x)$ een veelterm uit $\mathcal{L}[x]$ zijn met α als nulwaarde. Volgens het deler-algoritme zijn er veeltermen $q(x)$ en $r(x)$ uit $\mathcal{L}[x]$, zodanig dat

$$g(x) = q(x) \cdot f(x) + r(x)$$

met $\deg(r) < \deg(f)$ of $r(x) = 0$. Invullen van α voor x levert $r(\alpha) = 0$. Omdat wegens B. $f(x)$ de laagste graad heeft van veeltermen met α als nulwaarde moet $r(x) = 0$ worden genomen, waardoor $g(x) = q(x) \cdot f(x)$ (let wel iedere veelterm is een deler van zichzelf; verwar dit niet met reducibel zijn). Dus $f(x)$ deelt $g(x)$, waaruit C. volgt.

C. $\Longrightarrow$ A.
Veronderstel dat $f(x) = g(x) \cdot h(x)$, waarbij $g(x)$ en $h(x)$ veeltermen uit $\mathcal{L}[x]$ zijn (die daarmee deler zijn van $f(x)$). Omdat $f(\alpha) = 0$, is ofwel $g(\alpha) = 0$ of $h(\alpha) = 0$. Zonder de algemeenheid te schaden kunnen we veronderstellen dat $g(\alpha) = 0$. In dat geval moet volgens de veronderstelling in C. $f(x)$ een deler zijn van $g(x)$, want α is een nulwaarde van $g(x)$. Kennelijk delen $f(x)$ en $g(x)$ elkaar en moet wel gelden dat ze dezelfde graad hebben (en in dit geval is $\deg(h) = 0$). Aangezien $g(x)$ geen graad lager dan die van $f(x)$ heeft, is $f(x)$ irreducibel over $\mathcal{L}$, waaruit A. volgt.

Einde Bewijs

Het eenvoudige voorbeeld $f(x) = x^2 - 5$ is instructief. $f(x)$ is in dat geval een polynoom uit $\mathbb{Q}[x]$ en heeft als nulwaarde, $\sqrt{5}$. De nulwaarde is niet uit $\mathbb{Q}$ en $f(x)$ is irreducibel in $\mathbb{Q}$. Laat nu $g(x)$ ook uit $\mathbb{Q}$ zijn met als nulwaarde $\sqrt{5}$, dan moet gelden voor een zekere veelterm $h(x)$ (wegens stelling 4.1) dat $g(x) = h(x) \cdot \left(x - \sqrt{5}\right)$. Stel dat $g(x)$ een lagere graad heeft dan $f(x)$, dan moet $h(x)$ een constante veelterm zijn. In dat geval krijgen we $g(x) = c \cdot \left(x - \sqrt{5}\ \right) = c \cdot x - c \cdot \sqrt{5}$, maar wegens zijn constante term is $g(x)$ dan niet uit $\mathbb{Q}[x]$. Dus $g(x)$ heeft zeker geen lagere graad dan $f(x)$.

Stelling 4.4
Laat $f(x)$ en $g(x)$ monische variabele veeltermen zijn uit $\mathcal{L}[x]$ die ook irreducibel zijn over $\mathcal{L}$. Als $f(x)$en $g(x)$ een gemeenschappelijke nulwaarde hebben, dan zijn ze gelijk.

Bewijs
Uit Stelling 4.3 moet worden geconcludeerd dat $f(x)$ en $g(x)$ elkaar delen. Dus zeker is dat $g(x)$ een deler is van $f(x)$. Omdat $f(x)$ irreducibel is zal voor zekere constante c moeten opgaan: $f(x) = c \cdot g(x)$. Hieruit volgt dat $c = 1$, anders is $f(x)$ niet monisch als $g(x)$ monisch is. Maar dan hebben we $f(x) = g(x)$.

Uit Stellingen 4.3 en 4.4 volgt: als er een (variabele) veelterm uit $\mathcal{L}[x]$ is met nulwaarde α, dan is er een unieke (variabele) veelterm die monisch is en de laagste graad heeft van dergelijke veeltermen uit $\mathcal{L}[x]$. Deze veelterm noemen we de ***minimale polynoom*** van α over $\mathcal{L}$; deze noteren we als $\min(\alpha, \mathcal{L})$. Cruciaal is dat $\min(\alpha, \mathcal{L})$ irreducibel is. Eveneens is cruciaal dat $\min(\alpha, \mathcal{L})$ precies die veeltermen uit $\mathcal{L}[x]$ deelt die α als nulwaarde hebben. Dit laatste volgt uit de unieke wijze waarop iedere variabele veelterm uit $\mathcal{L}[x]$ kan worden ontbonden (zoals altijd in factoren). Hieronder in stelling 4.5 gaan we dat laatste bewijzen.

Stelling 4.5
Als $f(x)$ een variabele veelterm is uit $\mathcal{L}[x]$, dan kan $f(x)$ ontbonden worden (in factoren) in de vorm

$$f(x) = a \cdot g_1(x)^{d_1} \cdot g_2(x)^{d_2} \cdot \ldots \cdot g_m(x)^{d_m}$$

Waarbij a de leidende coëfficiënt is van $f(x)$, de exponenten d_j natuurlijke getallen zijn en de grondtallen $g_j(x)$ van elkaar verschillende monische polynomen zijn uit $\mathcal{L}[x]$, die niet reducibel zijn over $\mathcal{L}$. De factoren a en $g_j(x)^{d_j}$ zijn uniek. De factorisatie is daarmee uniek, afgezien van de volgorde van de factoren.

Bewijs
Als $f(x)$ irreducibel is over $\mathcal{L}$, dan is $a \cdot (\frac{1}{a} \cdot f(x))$, met a de leidende coëfficiënt van $f(x)$, de bedoelde factorisatie (ontbonden in factoren). Als $f(x)$ evenwel reducibel is over $\mathcal{L}$, kan $f(x)$ ontbonden worden in twee variabele veeltermen uit $\mathcal{L}[x]$, ieder met een graad lager dan $\deg(f)$. We herhalen dit proces voor ieder van deze twee veeltermen, enz. Aangezien de zo verkregen factoren een steeds lagere graad krijgen, eindigt de factorisatie in de vorm

$$f(x) = [b_1 \cdot s_1(x)] \cdot [b_2 \cdot s_2(x)] \cdot \ldots \cdot [b_n \cdot s_n(x)]$$

waarbij $b_1, b_2, \ldots, b_n$ uit $\mathcal{L}$ zijn en de $s_1(x), s_2(x), \ldots, s_n(x)$ zijn (variabele) monische polynomen uit $\mathcal{L}[x]$ die irreducibel zijn over $\mathcal{L}$. We krijgen met $a = b_1 \cdot b_2 \cdot \ldots \cdot b_n$ derhalve de factorisatie

$$f(x) = a \cdot s_1(x) \cdot s_2(x) \cdot \ldots \cdot s_n(x)$$

Waarbij a de leidende coëfficiënt van $f(x)$ is (G na!). We *beweren* dat deze factorisatie, afgezien van de volgorde van de factoren, uniek is. Het bewijs is met volledige inductie over n.

Veronderstel nu dat

$$f(x) = c \cdot t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$$

Direct volgt dat $a = c$, omdat de $s_j(x)$ en $t_j(x)$ monisch zijn (Ga na!).

Neem $n = 1$, dan krijgen we

$$s_1(x) = t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$$

Nu is $s_1(x)$ een deler van $f(x)$, waardoor $s_1(x)$ ook een deler is van het product $c \cdot t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$. Aangezien $s_1(x)$ tevens irreducibel is deelt $s_1(x)$ volgens stelling 4.2 minstens één van de veeltermen $t_1(x), t_2(x), \ldots, t_l(x)$, zeg $t_1(x)$. Dus $s_1(x) = k \cdot t_1(x)$, voor zekere constante k. Omdat $s_1(x)$ en $t_1(x)$ beide monisch zijn moeten we $k = 1$ nemen. Waarmee $s_1(x)$ en $t_1(x)$ gelijk zijn. Maar dan kunnen we niet $l > 1$ nemen, immers dan zou $t_2(x) \cdot t_3(x) \cdot \ldots \cdot t_l(x) = 1$ moeten zijn, wat onmogelijk is aangezien $t_2(x), t_3(x), \ldots, t_l(x)$ variabele veeltermen zijn. Derhalve moeten we $l = 1$ nemen, waarmee de *bewering* klopt.

Onze ***inductie onderstelling*** *voor* $n > 1$: *de factorisatie van een veelterm uit* $\mathcal{L}[x]$ *in een constante en* $n - 1$ *irreducibele monische veeltermen uit* $\mathcal{L}[x]$ *is uniek, afgezien van de volgorde van de factoren.*

Neem nu $n > 1$, dan volgt

$$s_1(x) \cdot s_2(x) \cdot \ldots \cdot s_n(x) = t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$$

Waaruit direct volgt dat $s_1(x)$ een deler is van $t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$. Opnieuw volgt uit stelling 4.2 dat $s_1(x)$ deler is van minstens één van de $t_1(x), t_2(x), \ldots, t_l(x)$, zeg, desnoods na herindexeren, $t_1(x)$. We kunnen nu zoals hiervoor concluderen dat $s_1(x)$ en $t_1(x)$ gelijk zijn. We krijgen dan

$$s_2(x) \cdot s_3(x) \cdot \ldots \cdot s_n(x) = t_2(x) \cdot t_3(x) \cdot \ldots \cdot t_l(x)$$

Volgens de *inductie onderstelling* is de factorisatie van bestaande uit $n - 1$ veeltermen en constante 1 in het linker lid uniek, afgezien van de volgorde van de factoren. Derhalve is $s_2(x) \cdot s_3(x) \cdot \ldots \cdot s_n(x)$ afgezien van de volgorde van factoren dezelfde factorisatie als $t_2(x) \cdot t_3(x) \cdot \ldots \cdot t_l(x)$.

Maar dan moet, aangezien tevens a gelijk is aan c en $s_1(x)$ gelijk is aan $t_1(x)$, de factorisatie

$a \cdot s_1(x) \cdot s_2(x) \cdot \ldots \cdot s_n(x)$ dezelfde factorisatie zijn als $c \cdot t_1(x) \cdot t_2(x) \cdot \ldots \cdot t_l(x)$, afgezien van de volgorde van de factoren.

Om het bewijs af te maken schrijven we gelijke factoren als één macht.

Einde bewijs

Samenvatting 4

1. **Stelling 4.1**
   Laat $f(x)$ een variabele veelterm uit $\mathcal{L}[x]$ zijn, en laat α een nulwaarde van $f(x)$ zijn. Dan is $x - \alpha$ een deler van $f(x)$. (niet erg spannende stelling; intuïtief zijn we al geneigd dit voor waar aan te nemen)

2. Laat er een irreducibele veelterm zijn over $\mathcal{L}$, die α als nulwaarde heeft, dan is er tevens een monische polynoom over $\mathcal{L}$, met α als nulwaarde van de laagste graad. Deze veelterm is *uniek*. Dit noemen we de ***minimale polynoom*** van α over $\mathcal{L}$; deze noteren we als $\min(\alpha, \mathcal{L})$. Cruciaal is dat $\min(\alpha, \mathcal{L})$ irreducibel is. Eveneens is cruciaal dat $\min(\alpha, \mathcal{L})$ precies die veeltermen uit $\mathcal{L}[x]$ deelt die α als nulwaarde hebben.

3. **Stelling 4.5**
   Als $f(x)$ een variabele veelterm is uit $\mathcal{L}[x]$, dan is er, afgezien van de volgorde van de factoren, een unieke factorisatie van $f(x)$ van de vorm

$$f(x) = a \cdot g_1(x)^{d_1} \cdot g_2(x)^{d_2} \cdot \ldots \cdot g_m(x)^{d_m}$$

   Waarbij a de leidende coëfficiënt is van $f(x)$, de exponenten d_j natuurlijke getallen zijn en de grondtallen $g_j(x)$ van elkaar verschillende monische polynomen zijn uit $\mathcal{L}[x]$, die niet reducibel zijn over $\mathcal{L}$.

Hierna volgt een herhaling van complexe waarden, weergegeven met $\mathbb{C}$, en veeltermen over $\mathbb{C}$. Naast de Hoofdstelling van de algebra, komt ook het Lemma van Abel en het Theorema van Schoenemann aan bod.

5. Over het "lichaam" van de complexe waarden en veeltermen met een priemgraad

Hier wordt enige voorkennis van complexe waarden verondersteld. We gaan hier meer intuïtionistisch te werk; wat doorgaans als reëel getal wordt geduid noemen we hier reële waarden, om onderscheid te kunnen maken tussen waarden waarmee onbeperkt exact kan worden gerekend, de rationale waarden (rationale waarden zijn goede getallen, dus we kunnen spreken van rationale getallen), en de irrationale waarden die slechts zijn te benaderen en waarmee niet onbeperkt exact kan worden gerekend. Dat met een enkel symbool zoals $\sqrt{2}$ of π sommige irrationale waarden kunnen worden aangeduid, maakt ze niet automatisch tot goede getallen. Sterker nog: er wordt zo veel dubbelzinnigheid en vertroebeling de wiskunde binnengeloodst. Pogingen om irrationale waarden tot getallen te promoveren zijn eveneens dubbelzinnig en leiden vaak tot tegenspraak, of blijken nutteloos, als men deze monsterlijke objecten vanuit verschillende invalshoeken benaderd. Bijvoorbeeld de snede van Dedekind, alsmede de equivalentieklassen van Cauchy, hebben problemen die in de gevestigde wiskunde weliswaar worden genegeerd en gebagatelliseerd, maar dat maakt ze "an sich" niet minder groot. Van het Program van Hilbert (de natuurkundige Johannes Stark schijnt onder de indruk te hebben verkeerd dat Hilbert een jood was; wellicht omdat hij samen met Klein een kring joodse wiskundigen in Göttingen leidde), waarin alles wel berekenbaar, en netjes in systemen te ordenen werd geacht, is uiteindelijk niets terecht gekomen. Bewijzen van Gödel gaven de nekslag en het intuïtionisme van De Brouwer is de enige stroming die nog overeind staat. Het zal mensen met kennis van zaken evenwel niet verbazen dat na de tweede wereldoorlog De Brouwer

een werkverbod werd opgelegd, omdat hij zich onvoldoende expliciet had verzet tegen de bezetter, en vervolgens de hele wiskunde in een formalistisch jasje, dat Hilbert goed zou passen, werd gestoken. Hier wordt de idee gebezigd dat formeel aandoende formuleringen nuttig kunnen zijn om zaken helder en ondubbelzinnig weer te geven, maar dat alles formaliseren leidt tot verwarring en ook tot (andere) dubbelzinnigheden. Eveneens worden bepaalde problemen door formalisering juist aan het zicht onttrokken en verliest een beschouwing zijn subtiele kanten. Dus liever geen abnormale formalistische symbolenbrij, waar alleen de "experts" hun zegje over mogen en "kunnen" doen, om binnen wiskunde nachtmerrieachtige protocollen toestanden te voorkomen.

De complexe waarden, $\mathbb{C}$, vormen onder de bewerkingen "+" en "·" en legitiem gebruik van haakjes een lichaam. We gaan er hier vanuit dat we er mee kunnen rekenen zonder problemen net zoals met (rationale) getallen (de naïeve insteek). Vandaar dat in de titel "lichaam" stond. Enige toelichting is gewenst ten aanzien van het gebruik van het symbool i. Met dit symbool mag gerekend worden zoals we dat gebruikelijk doen, maar we mogen niet met wortels van negatieve getallen rekenen zoals we met wortels van positieve getallen rekenen. Dus
$\sqrt{4} \cdot \sqrt{3} = \sqrt{3 \cdot 4} = \sqrt{12}$ is toegestaan voor positieve waarden, maar $\sqrt{-4} \cdot \sqrt{-3} = \sqrt{-3 \cdot -4} =$
$= \sqrt{12}$ mag niet. Wel mag i^2 worden vervangen door -1 en mag $\sqrt{i^2} = i$ worden genomen. Merk op dat met deze regel $\sqrt{-4} \cdot \sqrt{-3} = \sqrt{i^2 4} \cdot \sqrt{i^2 3} = \sqrt{i^2} \cdot \sqrt{4} \cdot \sqrt{i^2} \cdot \sqrt{3}$
$= i \cdot i\sqrt{4 \cdot 3} = i^2 \cdot \sqrt{12} = -\sqrt{12}$ wordt verkregen. Een ander, wel kloppend resultaat dan het foute resultaat van hiervoor dus. Het beste is het om de wortel van een negatieve waarde meteen te vervangen door i keer de wortel van de bijbehorende positieve waarde om dergelijke tegenstrijdigheden te voorkomen.

Er zijn twee manieren om complexe waarden weer te geven. Namelijk de cartesische vorm en de poolvorm. De cartesische notatie is $z = a + bi$ en de poolnotatie is $z = |z| \cdot e^{\arg(z)} =$
$= |z|(\cos(\arg(z)) + i \cdot \sin(\arg(z))$. Het verband tussen deze twee notaties wordt gegeven door $|z| = \sqrt{a^2 + b^2}$ en $\arg(z) = \arctan\left(\frac{b}{a}\right)$. De waarde $e \approx 2{,}718 \ldots$ is de bekende constante van Napier.

Nu is vooral de poolvorm uitermate geschikt om eenvoudige machtsvergelijkingen over $\mathbb{C}$ op te lossen.

Neem $z^n - C = 0$, waarbij n een natuurlijk getal is. We maken z^n vrij en dit levert $z^n = C$, zodat we $|z|^n e^{n \cdot i \cdot \arg(z)} = |C| e^{i \cdot \arg(C)} = |C|(\cos(\arg(C)) + i \cdot \sin(\arg(C))$ kunnen noteren. Hieruit volgt dat $|z| = \sqrt[n]{|C|}$ en dat $\arg(z) = \frac{\arg(C)}{n} + k \cdot \frac{2\pi}{n}$. Dit betekend dat een n^e-machts machtsvergelijking over $\mathbb{C}$ n verschillende oplossingen heeft, namelijk voor $k = 0$ tot en met $k = n - 1$. De oplossing voor $k = 0$ en $k = n$ zijn gelijk (Ga na!). We kunnen dus ook zeggen voor $k = 1$ tot en met $k = n$, waarmee nog duidelijker kan worden gezien dat er n verschillende oplossingen zijn. Deze oplossingen vormen een regelmatige polygoon met n hoeken in het complexe vlak. Deze oplossing geldt uiteraard voor iedere complexe waarde van C, ongeacht of deze zuiver reëel of zuiver imaginair is.

Stelling 5.1
De veelterm $ax^n - C$ uit $\mathbb{C}[x]$, met n uit $\mathbb{N}$, heeft n nulwaarden.

Bewijs
Ga te werk zoals we zojuist hier aan voorafgaand hebben gedaan.

Einde bewijs.

Laat $z = a + ib = |z|e^{i\cdot\arg(z)}$ een complexe waarde zijn, dan is $\bar{z} = a - ib = |z|e^{-i\cdot\arg(z)}$ zijn complexe geconjugeerde.
We sommen hier de rekenregels voor de complexe geconjugeerde nog eens op. Deze zijn door direct uitschrijven gemakkelijk te bewijzen.

- $\overline{z+w} = \bar{z} + \bar{w}$
- $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $\overline{\frac{z}{w}} = \frac{\bar{z}}{\bar{w}}$
- $\overline{z^n} = \bar{z}^n$

Voor iedere reële waarde geldt bovendien, triviaal, dat $\bar{a} = a$ en voor iedere zuiver imaginaire waarde $\overline{ib} = -ib$

Stelling 5.2 (theorema van de geconjugeerde nulwaarde)
Laat $f(z) = a_n \cdot z^n + \cdots + a_1 \cdot z + a_0$ een veelterm zijn uit $\mathbb{R}[z]$, dus met reële coëfficiënten en laat α een nulwaarde zijn van $f(z)$, dan is $\bar{\alpha}$ ook een nulwaarde van $f(z)$.

Bewijs
$f(\bar{\alpha}) = a_n \cdot \bar{\alpha}^n + \cdots + a_1 \cdot \bar{\alpha} + a_0 = \overline{a_n \cdot \alpha^n + \cdots + a_1 \cdot \alpha + a_0} = \overline{f(\alpha)} = \bar{0} = 0$

Einde bewijs

Dan zijn we nu toe aan een bewijs van de Hoofdstelling van de algebra. Gekozen is voor het (door Cauchy aangepaste) bewijs van Argand (*Annales de Gergonne*, 1815), dat zich onderscheid van andere bewijzen door zijn eenvoud en beknoptheid.

Stelling 5.2 (Hoofdstelling van de algebra)
Iedere vergelijking uit $\mathbb{C}[z]$ van graad n

$$z^n + C_{n-1}z^{n-1} + C_{n-2}z^{n-2} + \cdots + C_0 = 0$$

Heeft n nulwaarden.

Bewijs

EERSTE STAP (de lastigste stap)

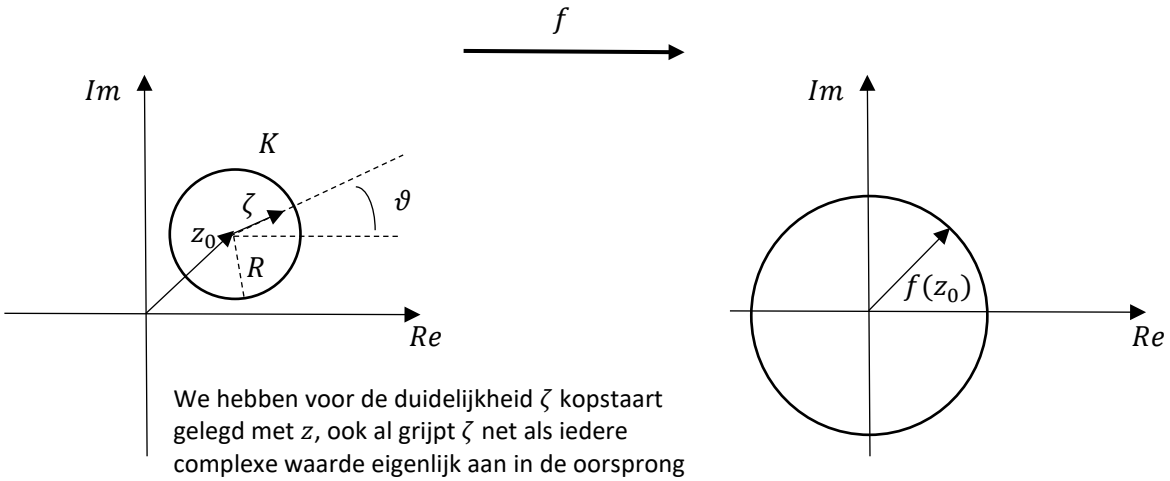
Definieer het rechterlid als de veelterm

$$f(z) = z^n + C_{n-1}z^{n-1} + C_{n-2}z^{n-2} + \cdots + C_0$$

en beschouw vervolgens de waarden die $|f(z)|$ aanneemt in het complexe vlak. Laat $|f(z)|$ de kleinste waarde aannemen voor z_0. Dus voor alle z geldt $|f(z_0)| \leq |f(z)|$, oftewel $\min(|f(z)|) = |f(z_0)|$.

Er dienen zich nu twee mogelijkheden aan:
1. $\min(|f(z)|) = |f(z_0)| > 0$ of
2. $\min(|f(z)|) = |f(z_0)| = 0$

We beginnen met het analyseren van mogelijkheid 1.



We hebben voor de duidelijkheid ζ kopstaart gelegd met z, ook al grijpt ζ net als iedere complexe waarde eigenlijk aan in de oorsprong

In de nabije omgeving van z_0, zeg in het gebiedje binnen en op het cirkeltje K met middelpunt z_0 en straal R, moet nu gelden dat $|f(z)| \geq \min(|f(z)|) = |f(z_0)|$.

Voor ieder z in K is er dan een ζ zodat $z = z_0 + \zeta$, met $\zeta = |\zeta| \cdot e^{i \cdot \vartheta}$.
Waardoor

$$f(z) = f(z_0 + \zeta) = (z_0 + \zeta)^n + C_{n-1}(z_0 + \zeta)^{n-1} + C_{n-2}(z_0 + \zeta)^{n-2} + \cdots + C_0$$

Als we de haakjes wegwerken en rangschikken naar toenemende machten van ζ, krijgen we zo

$$f(z) = z_0^n + C_{n-1} \cdot {z_0}^{n-1} + C_{n-2} \cdot {z_0}^{n-2} + \cdots + C_0 + c_1 \cdot \zeta + c_2 \cdot \zeta^2 + \cdots + c_n \cdot \zeta^n =$$

$$= f(z_0) + c_1 \cdot \zeta + c_2 \cdot \zeta^2 + \cdots + c_n \cdot \zeta^n$$

Omdat meerdere coëfficiënten c_r gelijk nul kunnen zijn, noemen we de eerste coëfficiënt ongelijk nul c, de tweede c', enz. De corresponderende exponenten geven we aan met ν, ν' enz., met $\nu < \nu' < \nu''' < \cdots$ waardoor

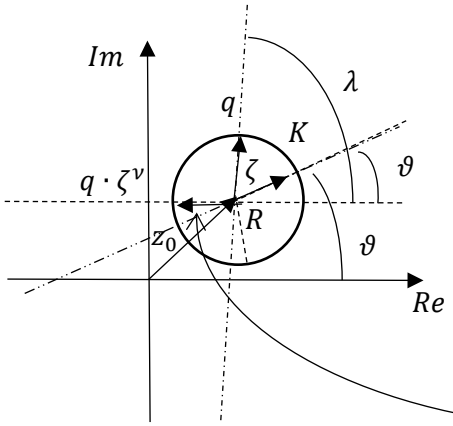
$$f(z) = f(z_0) + c \cdot \zeta^{\nu} + c' \cdot \zeta^{\nu'} + c'' \cdot \zeta^{\nu''} + \cdots$$

Delen door $f(z_0)$ en isoleren van ζ^{ν} resulteert in

$$\frac{f(z)}{f(z_0)} = 1 + \frac{c}{f(z_0)} \cdot \zeta^{\nu} \cdot (1 + \zeta \cdot \xi) = 1 + q \cdot \zeta^{\nu} \cdot (1 + \zeta \cdot \xi)$$

waarbij uiteraard $q = \frac{c}{f(z_0)}$ en ξ een som van verschillende machten van ζ met positieve exponenten en bekende coëfficiënten, zoals $\frac{c''}{c}$, voorstelt.

We beschouwen het product $q \cdot \zeta^{\nu} \cdot (1 + \zeta \cdot \xi)$. We schrijven de eerste factor in de poolvorm, $q = |q| \cdot e^{i\lambda}$. We verkrijgen zo $q \cdot \zeta^{\nu} = |q| \cdot |\zeta|^{\nu} \cdot e^{i(\lambda + \nu \cdot \vartheta)}$. Vanaf nu beperken we ons tot de z waarden in K waarvoor $\lambda + \nu \cdot \vartheta = \pi$.



In de figuur hiernaast liggen de bedoelde z waarden (de eindpunten van de bijbehorende vectoren die aangrijpen in de oorsprong) op het deel van de lijn binnen cirkeltje K met steunvector z_0 en met richtingsvector ζ. Dit deel van de lijn heeft uiteraard lengte $2R$.

Het lijnstuk waarop deze waarden voor z liggen maakt uiteraard een hoek van $\vartheta = \frac{\pi-\lambda}{\nu}$ met de reële as. Voor al deze z waarden wordt $q \cdot \zeta^\nu = |q| \cdot |\zeta|^\nu \cdot e^{i(\lambda+\nu\cdot\vartheta)} = |q| \cdot |\zeta|^\nu \cdot e^{i\pi} = -|q| \cdot |\zeta|^\nu$, waaruit voor ons product volgt $q \cdot \zeta^\nu \cdot (1 + \zeta \cdot \xi) = -|q| \cdot |\zeta|^\nu \cdot (1 + \zeta \cdot \xi)$.

We kunnen nu voor R een steeds kleinere waarde kiezen, zodat wegens $|\zeta| < R$ de tweede factor $1 + \zeta \cdot \xi$ zo min mogelijk van de vector $(1,0)$ verschilt als we maar willen. Maar dan kunnen we de complexe waarde

$$\frac{f(z)}{f(z_0)} = 1 + q \cdot \zeta^\nu \cdot (1 + \zeta \cdot \xi) = 1 - |q| \cdot |\zeta|^\nu \cdot (1 + \zeta \cdot \xi)$$

Zo min mogelijk van de zuiver reële waarde $1 - |q| \cdot |\zeta|^\nu$ laten verschillen als we maar willen. Aangezien $|q| \cdot |\zeta|^\nu > 0$ volgt hier uit dat

$$\left|\frac{f(z)}{f(z_0)}\right| = \frac{|f(z)|}{|f(z_0)|} = |1 - |q| \cdot |\zeta|^\nu \cdot (1 + \zeta \cdot \xi)| < 1$$

$|\zeta|$ is zeer klein, dus $|q| \cdot |\zeta|^\nu$ is zeer klein en $1 + \zeta \cdot \xi \approx (1,0)$. Waarmee de vector $|q| \cdot |\zeta|^\nu \cdot (1 + \zeta \cdot \xi) \approx$ $\approx |q| \cdot |\zeta|^\nu \cdot (1,0) = (\rho, 0)$, met $\rho = |q| \cdot |\zeta|^\nu > 0$, een zeer kleine vector in de richting van $(1,0)$ is. Zodat de vector $1 - |q| \cdot |\zeta|^\nu \cdot (1 + \zeta \cdot \xi) \approx (1,0) - (\rho, 0) = (1 - \rho, 0)$ altijd een kleinere lengte heeft dan die van $(1,0)$

en dus dat $|f(z)| < |f(z_0)| = \min(|f(z)|)$, waarmee we een tegenspraak hebben bereikt. Hiermee houden we alleen de tweede mogelijkheid over, namelijk dat $\min(|f(z)|) = |f(z_0)| = 0$.

Maar dan heeft iedere vergelijking uit $\mathbb{C}[z]$ *tenminste één nulwaarde*.

TWEEDE STAP

Laat α_1 nu een nulwaarde zijn van $f(z)$. Volgens stelling 4.1 is $z - \alpha_1$ nu een deler van $f(z)$, derhalve is er een veelterm $f_1(z)$ over $\mathbb{C}$ (we hebben geen lichaamsuitbreiding van $\mathbb{C}$ nodig, want α_1 is complex) met $\deg(f_1) = \deg(f) - 1 = n - 1$, zodat

$$f(z) = (z - \alpha_1) \cdot f_1(z)$$

Volgens de eerste stap hebben we de garantie dat $f_1(z)$ tenminste één nulwaarde heeft, zeg α_2, zodat er ook een $f_2(z)$ is met $\deg(f_2) = \deg(f_1) - 1 = n - 2$, zodat

$$f_1(z) = (z - \alpha_2) \cdot f_2(z)$$

Analoog krijgen we

$$f_2(z) = (z - \alpha_3) \cdot f_3(z),$$

$$f_3(z) = (z - \alpha_4) \cdot f_4(z),$$

enz. totdat we eindigen met $f_n(z)$, die graad 0 heeft dus een constante, zeg C moet zijn.

$$f_{n-1}(z) = (z - \alpha_n) \cdot f_n(z) = (z - \alpha_n) \cdot C$$

Door in de keten van vergelijkingen te beginnen met de eerste steeds $f_i(z)$ in het linker lid te vervangen door $(z - \alpha_{i+1}) \cdot f_{i+1}(z)$ uit het rechterlid van de opvolgende vergelijking er onder, krijgen we

$$f(z) = (z - \alpha_1) \cdot (z - \alpha_2) \cdot \ldots \cdot (z - \alpha_n) \cdot C$$

Aangezien $f(z) = z^n + C_{n-1}z^{n-1} + C_{n-2}z^{n-2} + \cdots + C_0$ monisch is moeten we wel $C = 1$ nemen. Zo komen we uiteindelijk uit op

$$f(z) = (z - \alpha_1) \cdot (z - \alpha_2) \cdot \ldots \cdot (z - \alpha_n)$$

Voor de vergelijking over $\mathbb{C}$ volgt hieruit

$$z^n + C_{n-1}z^{n-1} + C_{n-2}z^{n-2} + \cdots + C_0 = (z - \alpha_1) \cdot (z - \alpha_2) \cdot \ldots \cdot (z - \alpha_n) = 0$$

De willekeurige gekozen factor $z - \alpha_i$ in het laatste lid wordt identiek nul als $z = \alpha_i$ wordt genomen, waarmee het hele laatste lid identiek nul wordt, dus iedere α_i is een nulwaarde. Als er een andere waarde wordt genomen dan één van de α_i, wordt geen van de factoren en daarmee het hele laatste lid niet identiek nul. Aangezien er tevens n verschillende waarden voor i zijn, zijn er zo precies n nulwaarden, niet meer en niet minder (het is altijd lastig om wat meteen aan de vergelijking wordt gezien onder woorden te brengen; als wat uit deze laatste redenering niet meteen door de lezer werd gezien, moet deze zich afvragen of hij momenteel wel het niveau heeft om de stof te begrijpen).

Einde bewijs

Als we gelijke factoren van $f(z) = (z - \alpha_1) \cdot (z - \alpha_2) \cdot \ldots \cdot (z - \alpha_n)$ uit de hoofdstelling van de algebra als één macht samennemen krijgen we voor zekere $\mu, \nu, \ldots, \tau$
$f(x) = (z - \alpha_\nu)^{d_\nu} \cdot \left(z - \alpha_\mu\right)^{d_\mu} \cdot \ldots \cdot (z - \alpha_\tau)^{d_\tau}$. Omdat de monische veeltermen $(z - \alpha_\nu)$ irreducibel zijn over $\mathbb{C}$ (er zijn geen veeltermen met een lagere graad dan $(z - \alpha_\nu)$ waarvan het product gelijk is aan $(z - \alpha_\nu)$), is, afgezien van de volgorde van factoren, deze factorisatie volgens stelling 4.5 uniek. Dit maakt de nulwaarden α_i tevens uniek. Voor complexe nulwaarden is dat in het algemeen minder gemakkelijk in te zien dan voor reële nulwaarden. De nulwaarde α_μ noemen we een d_μ-voudige nulwaarde.

Een andere opmerkelijke stelling is die van Sturm (1829, *Bulletin de sciences de Férussac*) waarmee we een algoritme verkrijgen om het **aantal** reële oplossingen te vinden van een algebraïsche vergelijking met reële coëfficiënten. Deze gaan we nu nader bestuderen en bewijzen.
We beginnen met een voorbeeld om duidelijk te maken om welk proces het gaat en om de terminologie te verduidelijken.

Voorbeeld 5.1
Bepaal het aantal oplossingen van de vergelijking $x^5 - 3x - 1 = 0$.

Stap 1: herleid de vergelijking op nul: de zo verkregen veelterm duiden we aan met $f^0(x) = x^5 - 3x - 1$. De afgeleide van $f^0(x)$ geven we weer met $f^1(x)$, dus krijgen we:

$f^0(x) = x^5 - 3x - 1,\ \ f^1(x) = 5x^4 - 3$.

Stap 2: Deel nu $f^1(x)$ op $f(x)$. De rest van deze deling laten we van teken laten wisselen, waarmee $f^2(x)$ wordt verkregen. Herhaal dit proces zodanig dat f^{i+2} wordt verkregen door de rest verkregen door f^{i+1} te delen op f^i van teken te laten wisselen . Dit proces stopt als op een gegeven moment een constante uit de deling komt.

De opeenvolging van de veeltermen $f(x),\ f^1(x), f^2(x)$, … noemen we een ***Sturmketting***. We krijgen zo

$f^1(x) = 5x^4 - 3\ /\ f(x) = x^5 - 3x - 1 \setminus \frac{1}{5}x$

$x^5 - \frac{3}{5}x$

$-2\frac{2}{5}x - 1 = -f^2(x)$

$f^2(x) = 2\frac{2}{5}x + 1\ /\ f^1(x) = 5x^4 - 3 \setminus 2\frac{1}{12}x - \frac{125}{144}$

$5x^4 + 2\frac{1}{12}x$

$-2\frac{1}{12}x - 3$
$-2\frac{1}{12}x - \frac{125}{144}$

$-2\frac{19}{144} = -f^3(x)$

Onze Sturmketting is
$f^0(x) = x^5 - 3x - 1\ ,\ f^1(x) = 5x^4 - 3, f^2(x) = 2\frac{2}{5}x + 1$ en $f^3(x) = 2\frac{19}{144}$.

We willen nu over het interval $[-\infty, +\infty]$ het aantal nulwaarden vaststellen. Dit doen we als volgt.

Stap 3: Vul de ondergrens in en stel de tekens vast in de Sturmketting. We krijgen , met
$\text{teken}(f^i(a)) = -$, als $f^i(a) < 0$ en $\text{teken}(f^i(a)) = +$, als $f^i(a) > 0$,

$\text{teken}(f^0(-\infty)) = -\ ,\ \text{teken}(f^1(-\infty)) = +,\ \text{teken}(f^2(-\infty)) = -, \text{teken}(f^3(-\infty)) = +$

wisseling *wisseling* *wisseling*

Het aantal ***tekenwisselingen*** voor de ondergrens is nu 3

Vul daarna de bovengrens in en stel opnieuw de tekens in de Sturmketting vast.

$$\text{teken}(f^0(+\infty)) = +\,,\ \text{teken}(f^1(+\infty)) = +,\ \text{teken}(f^2(+\infty)) = +, \text{teken}(f^3(+\infty)) = +$$

geen wisseling *geen wisseling* *geen wisseling*

Het aantal ***tekenwisselingen*** voor de bovengrens is daarmee 0

Stap 4: Het aantal nulwaarden is het verschil tussen het aantal tekenwisselingen voor de ondergrens en het aantal tekenwisselingen voor de bovengrens. De veelterm $x^5 - 3x - 1$ heeft dus $3 - 0 = 3$ reële nulwaarden, en de vergelijking $x^5 - 3x - 1 = 0$ heeft dus drie reële oplossingen.

Op het interval $[0, +\infty]$ krijgen we voor de ondergrens

$$\text{teken}(f^0(0)) = -\,,\ \text{teken}(f^1(0)) = -,\ \text{teken}(f^2(0)) = +, \text{teken}(f^3(0)) = +$$

Dus aantal tekenwisselingen ondergrens is nu 1. Bijgevolg hebben we nu $1 - 0 = 1$ reële oplossing op het interval $[0, +\infty]$.

Zelf kun je controleren dat volgens dit recept er naar verwachting 2 reële oplossingen zijn over $[-\infty, 0]$.

En dan nu voor de stelling.

Stelling 5.3 (Het theorema van Sturm)
Het *aantal* reële nulwaarden van een veelterm uit $\mathbb{R}[x]$, die enkelvoudig zijn over een interval *waarvan de grenswaarden geen nulwaarden zijn*, is gelijk aan het verschil tussen het aantal tekenwisselingen van de Sturmketting van tekens verkregen voor de grenswaarden van het interval.

Bewijs
We onderscheiden twee gevallen:

I. De reële nulwaarden zijn allemaal enkelvoudig over het gegeven interval.
II. De vergelijking heeft meervoudige nulwaarden over het interval. We zullen laten zien dat het tweede geval ons terugvoert tot het eerste geval.

Laat de vergelijking $F(x) = 0$ (zonder de algemeenheid te schaden kunnen we stellen dat $F(x)$ monisch is, immers van iedere vergelijking met veeltermen die op nul is herleid kan de leidende coëfficiënt tot 1 worden teruggebracht) de van elkaar te onderscheiden nulwaarden $\alpha,\ \beta,\ \gamma, \ldots$ hebben en laat de nulwaarde α a-voudig zijn, β b-voudig, γ c-voudig, … , zo dat

$$F(x) = (x - \alpha)^a \cdot (x - \beta)^b \cdot (x - \gamma)^c \cdot \ldots$$

Voor de afgeleide $F'(x)$ van $F(x)$ verkrijgen we

$$F'(x) = a(x-\alpha)^{a-1}\cdot(x-\beta)^b\cdot(x-\gamma)^c\cdot\ldots + (x-\alpha)^a\cdot b(x-\beta)^{b-1}\cdot(x-\gamma)^c\cdot\ldots + \\ +(x-\alpha)^a\cdot(x-\beta)^b\cdot c(x-\gamma)^{c-1}\cdot\ldots+\cdots$$

Zodat

$$\frac{F'(x)}{F(x)} = \frac{a}{x-\alpha}+\frac{b}{x-\beta}+\frac{c}{x-\gamma}+\cdots = \\ = \frac{a(x-\beta)(x-\gamma)(x-\delta)\ldots + b(x-\alpha)(x-\gamma)(x-\delta)\ldots+\cdots}{(x-\alpha)(x-\beta)(x-\gamma)\ldots}$$

Als we de teller van deze laatste breuk met $t(x)$ aanduiden en de noemer met $n(x)$ en we de hele gebroken functie $\frac{F(x)}{n(x)} = (x-\alpha)^{a-1}\cdot(x-\beta)^{b-1}\cdot(x-\gamma)^{c-1}\cdot\ldots$ gelijk stellen aan $G(x)$, dan volgt met $\frac{F'(x)}{F(x)} = \frac{t(x)}{n(x)}$ en bijgevolg $\frac{F'(x)}{t(x)} = \frac{F(x)}{n(x)} = G(x)$ dat

$$F(x) = G(x)\cdot n(x) \text{ en } F'(x) = G(x)\cdot t(x)\,.$$

Nu hebben de functies $t(x)$ en $n(x)$ geen gemeenschappelijke deler (bijvoorbeeld de factor $(x-\alpha)$ van $n(x)$ komt voor in alle termen van $t(x)$ behalve in de eerste term etc.) en aangezien tevens $\frac{F'(x)}{G(x)} = t(x)$ en $\frac{F(x)}{G(x)} = n(x)$, volgt hieruit dat $G(x)$ de grootste gemeenschappelijke deler is van $F'(x)$ en $F(x)$, zodat $G(x)$ rechtstreeks met het Euclidisch algoritme kan worden bepaald, waaruit meteen $n(x) = \frac{F(x)}{G(x)}$ kan worden bepaald ($G(x)$ is tenslotte een deler van $F(x)$).

Uit de vergelijking $F(x) = 0$ volgen de twee vergelijkingen

$$n(x) = 0 \text{ of } G(x) = 0$$

waarvan de eerste alleen enkelvoudige nulwaarden heeft en de tweede op dezelfde wijze kan worden gereduceerd zoals $F(x) = 0$. Een vergelijking met meervoudige nulwaarden kan daarom altijd omgezet worden in vergelijkingen met bekende coëfficiënten en enkelvoudige nulwaarden.

Het volstaat daarom om het probleem voor geval I. op te lossen. Neem nu

$$f(x) = K\cdot(x-\alpha)\cdot(x-\beta)\cdot(x-\gamma)\cdot\ldots$$

Dus de vergelijking $f(x) = 0$ is een algebraïsche vergelijking waarvan alle nulwaarden enkelvoudig zijn. De afgeleide

$$f'(x) = K\cdot(x-\beta)\cdot(x-\gamma)\cdot\ldots + (x-\alpha)\cdot(x-\gamma)\cdot\ldots + K\cdot(x-\alpha)\cdot(x-\beta)\cdot\ldots$$

verdwijnt dan voor geen enkele nulwaarde van $f(x)$. Nu krijgen we $\frac{f(x)}{f'(x)} = \frac{1}{x-\alpha}+\frac{1}{x-\beta}+\frac{1}{x-\gamma}+\cdots =$ $= \frac{(x-\beta)(x-\gamma)\ldots+(x-\alpha)(x-\gamma)\ldots+(x-\alpha)(x-\beta)\ldots}{(x-\alpha)(x-\beta)(x-\gamma)\ldots} = \frac{t(x)}{n(x)}$ zodat de grootste gemeenschappelijke deler van $f(x)$ en $f'(x)$, $G(x) = \frac{f(x)}{n(x)} = \frac{K\cdot n(x)}{n(x)} = K$, een constante ongelijk nul is. We gebruiken het deler-algoritme om de grootst gemeenschappelijke deler van $f(x)$ en $f'(x)$ te bepalen, waarbij we voor het gemak $f_0(x)$ schrijven voor $f(x)$ en $f_1(x)$ voor $f'(x)$ en voor de quotiënten van de opeenvolgende delingen $q_0(x)$, $q_1(x)$, … en de resten $-f_2(x)$, $-f_3(x)$, … . We verkrijgen zo het volgende schema:

1) $f_0(x) = q_0(x)\cdot f_1(x) - f_2(x)$

2) $f_1(x) = q_1(x)\cdot f_2(x) - f_3(x)$

3) $f_2(x) = q_2(x)\cdot f_3(x) - f_4(x)$ etc.

In dit schema moet er een laatste rest $-f_s(x) = K \neq 0$ zijn, die als constante uiteraard voor geen enkele waarde van x uit het interval van teken kan veranderen. Hier stoppen we het algoritme. De veeltermen $f_0(x), f_1(x), f_2(x), \ldots, f_s(x)$ noemen we een Sturmketting. De naburige veeltermen van $f_1(x)$ zijn $f_0(x)$ en $f_2(x)$ etc.

De Sturm veeltermen bezitten de volgende drie eigenschappen:

i. Voor geen enkele waarde uit het interval verdwijnen twee naburige veeltermen allebei.
ii. Voor een nulwaarde van een veelterm verschillen de twee naburige veeltermen van teken.
iii. Binnen een voldoende kleine omgeving rond een nulpunt van $f_0(x)$ is $f_1(x)$ overal positief of overal negatief.

Bewijs eigenschap i.
Als bijvoorbeeld $f_2(x)$ en $f_3(x)$ verdwijnen voor een zekere waarde uit het interval, dan moet wegens 3) $f_4(x)$ ook verdwijnen voor deze waarde, zodat ook $f_5(x)$ verdwijnt etc., zodat uiteindelijk volgt $f_s(x) = K \neq 0$ ook moet verdwijnen, wat een tegenspraak oplevert. Dus i. moet juist zijn.

Bewijs eigenschap ii.
Als de veelterm $f_3(x)$ verdwijnt voor een waarde uit het interval, zeg σ, dan volgt uit 3) dat

$$f_2(\sigma) = -f_4(\sigma).$$

Bewijs eigenschap iii.
Volgt direct uit de notie dat de nulwaarden van de veelterm enkelvoudig zijn en dat een functie met als voorschrift deze veelterm, daalt of stijgt door een nulpunt en de afgeleide hiervan derhalve voor de bijbehorende nulwaarde respectievelijk positief of negatief is.

We kiezen nu een waarde x uit het interval, noteren het teken van de waarden $f_0(x), f_1(x), \ldots, f_s(x)$ en verkrijgen zo een Sturm tekenketting. Voorwaarde is dat geen enkele van $s + 1$ functies de waarde nul aanneemt. De tekenketting zal als opeenvolgende paren tekens $++$, $--$, $+-$ en $-+$ bevatten.

Er zijn nu twee gevallen te onderscheiden.

Geval 1; $f_0(x)$ heeft <u>geen</u> nulwaarde op een geschikt gekozen interval.
Neem de reële waarden $h < k < l$ en beschouw het ***drietal*** $f_{v-1}(x)$, $f_v(x)$ en $f_{v+1}(x)$, met $v \geq 1$. We stellen dat k *de enige nulwaarde* is tussen h en l van $f_v(x)$ en dat de drie functiewaarden voor de overige waarden tussen en op h en l ongelijk nul zijn (we gaan er vanuit dat we altijd zo'n voldoende kleine omgeving van k kunnen kiezen; dit ligt in de lijn van de enkelvoudigheid van de nulwaarden). Omdat alle nulwaarden enkelvoudig zijn en omdat $f_v(x)$ over het interval een nulwaarde heeft verschillen $f_v(h)$ en $f_v(l)$ van teken. En we hebben *wegens eigenschap i.* dat $f_{v-1}(k) \neq 0$, $f_v(k) = 0$ en $f_{v+1}(k) \neq 0$; voor $l \leq x \leq h$ en voor $x \neq k$ hebben we $f_{v-1}(x) \neq 0$, $f_v(x) \neq 0$ en $f_{v+1}(x) \neq 0$.
Wegens eigenschap ii. Moeten bovendien $f_{v-1}(x)$ en $f_{v+1}(x)$ over dit interval van teken verschillen. We hebben nu

x	h	l
teken $f_{v-1}(x)$	$\pm$	$\pm$
teken $f_v(x)$	$+$	$-$
teken $f_{v+1}(x)$	$\mp$	$\mp$

of

x	h	l
teken $f_{v-1}(x)$	$\pm$	$\pm$
teken $f_v(x)$	$-$	$+$
teken $f_{v+1}(x)$	$\mp$	$\mp$

Uit beide tabellen blijkt dat het **aantal** tekenwisselingen van h naar l **ongewijzigd** één blijft. De bovenste tabel geeft bijvoorbeeld van $++-$ (één tekenwisseling) voor h naar $+--$ (ook één tekenwisseling) voor l.

Aangezien tekenwisselingen alleen plaatsvinden voor een linker en rechtergrens als er een nulwaarde tussen de grenzen zit, kunnen we concluderen **dat het *aantal* tekenwisselingen voor een geschikt gekozen drietal en over een geschikt gekozen interval $\boldsymbol{f_{v-1}(x) \neq 0, f_v(x) = 0}$ en $\boldsymbol{f_{v+1}(x) \neq 0,}$ altijd ongewijzigd** blijft! Als $f_0(x) \neq 0$ op het betreffende interval, is de hele Sturmketting op te delen in drietallen waarvan de middelste functiewaarde nul is (twee drietallen kunnen een veelterm gemeenschappelijk hebben, maar overlappen elkaar niet wat betreft tekenwisselingen!) en eventueel hier tussenliggende delen van Sturmfuncties waarvan geen enkele functiewaarde nul is. In dit geval veranderd het aantal tekenwisselingen dus niet voor de hele Sturmketting!

Geval 2; $\boldsymbol{f_0(x)}$ heeft precies één nulwaarde op een geschikt gekozen interval.
Rest ons nog als enige de situatie voor een nulpunt van $f_0(x)$ te onderzoeken, omdat $f_0(x)$ nooit in het midden van een drietal kan voorkomen. We verkrijgen wegens *eigenschap iii.* De volgende tabel

x	h	l
teken $f_0(x)$	$\pm$	$\mp$
teken $f_1(x)$	$\mp$	$\mp$

We zien dat in dit geval het ***aantal* tekenwisselingen** precies **één *minder*** wordt. Als $f_0(x)$ geen nulwaarde heeft over het interval is het aantal tekenwisselingen evenwel nul. De rest van de Sturmketting is wederom op te delen in drietallen waarvan de middelste functiewaarde nul is en delen waarvan geen enkele Sturmfunctie de waarde nul heeft, maar hiervan weten wij dat daarmee het aantal tekenwisselingen niet verandert.

Samenvattend kunnen we concluderen dat de Sturmketting alleen een tekenwisseling *verliest* als $f(x)$ door een nulpunt gaat. Het totaal aantal verloren tekenwisselingen komt daarmee overeen met het aantal verkregen nulwaarden. Bijgevolg is het verschil in tekenwisselingen tussen de grenzen van een interval gelijk aan het aantal verloren tekenwisselingen en daarmee gelijk aan het aantal nulwaarden van de veelterm over dit interval.

Einde bewijs

Lemma 5.1
Laat p een priemgetal zijn, en laten er twee natuurlijke getallen a en b zijn zodat $a + b = p$, dan is $ggd(a, b) = 1$ oftewel a en b zijn dan relatief priem.

Bewijs
Stel a en b zijn niet relatief priem, dan is er een d die zowel a als b deelt. In dat geval krijgen we $\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d} = \frac{p}{d}$. Aangezien we hebben aangenomen dat d zowel a als b deelt, moet $\frac{a}{d} + \frac{b}{d}$ een natuurlijk getal opleveren, maar dan moet $\frac{p}{d}$ ook een natuurlijk getal opleveren, wat in tegenspraak is met het gegeven dat p een priemgetal is. We moeten dus de aanname dat a en b niet relatief priem zijn verwerpen. Hieruit volgt dat a en b relatief priem zijn als de som $a + b$ priem is.

Stelling 5.4 (Abels Lemma)
Laat p een priemgetal zijn en neem de vergelijking $x^p = C$ uit $\mathcal{L}[x]$. Dan volgt

Als (A) C geen p^{e} macht van een waarde uit $\mathcal{L}$ is

Dan (B) is $x^p = C$ irreducibel over $\mathcal{L}$.

Bewijs
Het bewijs is uit het ongerijmde. *Laat nu de vergelijking $x^p - C = 0$ en daarmee ook de veelterm $x^p - C$ reducibel zijn*. Dan zijn er zekere $\psi(x)$ en $\phi(x)$ uit $\mathcal{L}[x]$ zodat

$$x^p - C = \psi(x) \cdot \phi(x)$$

De nulwaarden van $x^p - C = 0$ (zie Stelling 5.1) zijn van de vorm $r,\ r \cdot \omega,\ r \cdot \omega^2$, …, $r \cdot \omega^{p-1}$, met $r = \sqrt[p]{|C|} \cdot e^{i \cdot \frac{\arg(C)}{p}}$ en $\omega = e^{\frac{i \cdot 2\pi}{p}}$.

Met de hoofdstelling van de algebra kunnen we het linker lid herschrijven en we schrijven ook de monische (Ga na waarom!) veeltermen $\psi(x)$ en $\phi(x)$ uit voor de duidelijkheid. We krijgen $\underbrace{(x-r)(x-r\omega)(x-r\omega^2)\ldots(x-r\omega^{p-1})}_{p\ factoren} = (x^\mu + \cdots + A) \cdot (x^\nu + \cdots + B)$, waarbij A en B nu waarden uit $\mathcal{L}$ moeten zijn, want we nemen nu aan dat $x^p - C$ reducibel is over $\mathcal{L}$.

Het uitschrijven van het product levert voor de constante termen A van $\psi(x)$ en B van $\phi(x)$,

$$A = r^\mu \cdot \omega^M, \qquad B = r^\nu \cdot \omega^N$$

met uiteraard $\mu + \nu = p$ en $M + N = 1 + 2 + \cdots + p - 1 = \frac{(p-1)p}{2}$ (de laatste reeks voor de som van M en N is een rekenkundige reeks, maar niet relevant voor het vervolg van het bewijs).

Aangezien p een priemgetal is hebben μ en ν geen gemeenschappelijke deler, oftewel ze zijn relatief priem. We kunnen met het Euclidisch algoritme twee gehele getallen k en h vinden zodat

$$\mu \cdot h + \nu \cdot k = 1$$

Beschouw nu het product $K = A^h \cdot B^k = (r^\mu \omega^M)^h \cdot (r^\nu \omega^N)^k = r^{\mu h + \nu k} \cdot \omega^{Mh+Nk} = r \cdot \omega^{Mh+Nk}$, zodat $K^p = r^p \cdot (\omega^p)^{Mh+Nk} = r^p \cdot 1^{Mh+Nk} = r^p = C$, immers r is een oplossing van de vergelijking $x^p = C$, waar we mee begonnen.

Merk op dat K een waarde uit $\mathcal{L}$ moet zijn omdat A en B waarden uit $\mathcal{L}$ zijn. Maar dan hebben we, met $C = K^p$, C geschreven als een p^{e} macht van een waarde uit $\mathcal{L}$, wat in tegenspraak is met het gegeven dat C niet geschreven kan worden als een p^{e} macht van een waarde uit $\mathcal{L}$. De aanname dat

$x^p - C$ reducibel is moet daarmee worden verworpen. Dus de vergelijking $x^p = C$ is irreducibel over $\mathcal{L}$ als C geen p^{e} macht van een waarde uit $\mathcal{L}$ is.

Einde bewijs

Een voor het vervolg nuttige stelling is een stelling van Gauss.

Stelling 5.5 (van Gauss)
Als $f(x) = x^N + C_1 x^{N-1} + C_2 x^{N-2} + \cdots + C_N$, een monische veelterm is met coëfficiënten C_i uit $\mathbb{Z}$ en er zijn veeltermen $\psi(x) = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$ en $\phi(x) = x^n + \beta_1 x^{n-1} + \cdots + \beta_n$, zodat $f(x) = \psi(x) \cdot \phi(x)$, met α_i en β_j uit $\mathbb{Q}$, *dan* zijn alle α_i en β_j ook uit $\mathbb{Z}$.

Bewijs
Laat $a_0 = ggd(\alpha_1, \alpha_2, \dots, \alpha_m)$ en $b_0 = ggd(\beta_1, \beta_2, \dots, \beta_n)$. Neem nu a_i en b_j uit $\mathbb{Z}$, zodanig dat $\alpha_i = \frac{a_i}{a_0}$ en $\beta_j = \frac{b_j}{b_0}$, waardoor alle α_i net als alle β_j geen gemeenschappelijke deler meer hebben.
Definieer

$$F(x) = a_0 \cdot b_0 \cdot f(x) = a_0 \cdot b_0 \cdot \psi(x) \cdot \phi(x) = a_0 \psi(x) \cdot b_0 \phi(x) = \Psi(x) \cdot \Phi(x)$$

zodat

$$\Psi(x) = a_0 \cdot (x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$$

en

$$\Phi(x) = b_0 \cdot (x^n + \beta_1 x^{n-1} + \cdots + \beta_n) = b_0 \cdot x^n + b_1 x^{n-1} + \cdots + b_n$$

Laat het priemgetal p een deler zijn van $a_0 \cdot b_0$. Dan is p een deler van alle coëfficiënten van F, maar niet noodzakelijkerwijs van alle coëfficiënten van $\Psi(x)$ en $\Phi(x)$.
We nemen alle termen samen van $\Psi(x)$ die deelbaar zijn door p en noemen deze veelterm $U(x)$. De veelterm met alle termen van $\Psi(x)$ die niet deelbaar zijn door p noemen we $u(x)$. We verkrijgen zo

$$\Psi(x) = U(x) + u(x)$$

Evenzo verkrijgen we

$$\Phi(x) = V(x) + v(x)$$

waarmee

$$F(x) = \big(U(x) + u(x)\big) \cdot (V(x) + v(x))$$

Hieruit isoleren we $u(x) \cdot v(x)$ zodat

$$u(x) \cdot v(x) = F(x) - U(x) \cdot V(x) - U(x) \cdot v(x) - V(x) \cdot u(x)$$

Aangezien $F(x)$, $U(x)$ en $V(x)$ coëfficiënten hebben die deelbaar zijn door p, is het hele rechter lid deelbaar door p. Maar dan is het linker lid $u(x) \cdot v(x)$ ook deelbaar door p! Maar we hebben zojuist verondersteld dat geen van de termen van $u(x)$ en $v(x)$ deelbaar zijn door p, waardoor geen van de termen van $u(x) \cdot v(x)$ deelbaar zijn door p! We hebben zo een tegenspraak verkregen. De tegenstrijdigheid verdwijnt als $a_0 \cdot b_0$ geen enkel priemgetal als deler heeft, met andere woorden als $a_0 = b_0 = 1$, in welk geval dat $\alpha_i = \frac{a_i}{1} = a_i$ en $\beta_j = \frac{b_j}{1} = b_j$ gehele getallen zijn (en dus uit $\mathbb{Z}$).

Einde bewijs

We vervolgen.

Stelling 5.6 (Theorema van Schoenemann)
Als de gehele coëfficiënten C_0, C_1, C_2, …, C_n van de monische veelterm

$$f(x) = C_0 + C_1x + C_2x^2 + \cdots + C_{N-1}x^{N-1} + x^N$$

(uit $\mathbb{Z}[x]$ zoals voor zich spreekt) deelbaar zijn door het priemgetal p, terwijl de constante term C_0 niet deelbaar is door p^2,
dan is $f(x)$ irreducibel over de rationale getallen (dus over $\mathbb{Q}$).

Bewijs
Uit het ongerijmde. Laat $f(x)$ reducibel zijn, zo dat $f(x) = \psi(x) \cdot \phi(x)$, met

$$\psi(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} + x^m$$

en

$$\phi(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} + x^n$$

Volgens de voorgaande stelling van Gauss zijn de coëfficiënten van $\psi(x)$ en $\phi(x)$ geheel. We voeren de vermenigvuldiging van deze twee veeltermen uit en vergelijken de zo verkregen coëfficiënten met die van $f(x)$ in het volgende schema:

$$\begin{aligned} C_0 &= a_0b_0 \\ C_1 &= a_0b_1 + a_1b_0 \\ C_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\text{etc.} \end{aligned}$$

Omdat C_0 niet deelbaar is door p^2, kunnen we zonder de algemeenheid te schaden stellen dat p wel a_0 deelt en b_0 niet deelt. Omdat C_1 en a_0 deelbaar zijn door p en b_0 niet deelbaar is door p, volgt uit de tweede vergelijking uit ons schema dat a_1 deelbaar is door p. Uit de derde vergelijking volgt dan weer dat, omdat C_2, a_0 en a_1 deelbaar zijn door p en b_0 niet deelbaar is door p, dat a_2 deelbaar moet zijn door p, enz. Uiteindelijk moeten we dan concluderen dat $a_m = 1$ deelbaar moet zijn door p, wat absurd is. We moeten daarmee verwerpen dat $f(x)$ reducibel is. Derhalve is hiermee bewezen dat $f(x)$ irreducibel is over $\mathbb{Q}$.

Einde bewijs

Stelling 5.7 (Abels fundamentele theorema aangaande vergelijkingen van irreducibele veeltermen)
Laat de veelterm $f(x)$ irreducibel zijn over $\mathcal{L}$. En neem $F(x)$ uit $\mathcal{L}[x]$.
Als een nulwaarde van de vergelijking $f(x) = 0$ tevens een nulwaarde is van de vergelijking $F(x) = 0$,
dan zijn alle nulwaarden van $f(x)$ ook nulwaarden van $F(x)$ en is $f(x)$ een deler van $F(x)$.

Bewijs
Uit stelling 4.3 volgt dat omdat (A) $f(x)$ irreducibel is over $\mathcal{L}$, dat (C) $f(x)$ een deler is van iedere veelterm uit $\mathcal{L}[x]$ met een zelfde nulwaarde als die van $f(x)$. Dus $f(x)$ is een deler van $F(x)$. In dat geval moet er een $F_1(x)$ te vinden zijn zodanig dat

$$F(x) = F_1(x) \cdot f(x)$$

Als α een willekeurige nulwaarde is van $f(x)$ volgt uit

$$F(\alpha) = F_1(\alpha) \cdot f(\alpha) = F_1(\alpha) \cdot 0 = 0$$

dat een willekeurige nulwaarde van de **vergelijking** $f(x) = 0$ en daarmee iedere nulwaarde van de **vergelijking** $f(x)$, ook een nulwaarde is van de **vergelijking** $F(x) = 0$.

Einde bewijs

Het fundamentele theorema heeft twee directe gevolgen.

Gevolg 5.1
Als een nulwaarde van een **vergelijking** $f(x) = 0$, die irreducibel is in $\mathcal{L}$, ook een nulwaarde is van de **vergelijking** $F(x) = 0$ uit $\mathcal{L}$, die van een lagere graad is, dan zijn alle coëfficiënten van $F(x)$ gelijk nul (triviaal de nulpolynoom gelijk aan nul heeft iedere waarde als nulwaarde).

Gevolg 5.2
Als $f(x) = 0$ irreducibel is over $\mathcal{L}$, dan is er geen andere irreducibele **vergelijking** die een nulwaarde gemeenschappelijk heeft met $f(x) = 0$.

Bewijs
Laat $g(x) = 0$ irreducibel zijn en een nulwaarde gemeenschappelijk hebben met $f(x) = 0$, dan deelt $g(x)$ de veelterm $f(x)$, dus voor zekere $q(x)$ moet gelden $g(x) = q(x) \cdot f(x)$, omdat evenwel $g(x)$ irreducibel is moet $q(x)$ een constante zijn, zeg $q(x) = C$. Dan krijgen we

$$g(x) = C \cdot f(x) = 0$$

Wat in essentie dezelfde vergelijking is als $f(x) = 0$

Einde bewijs

6. Over de coëfficiënten van veeltermen

Dan zijn we nu toe aan het maken van een flinke stap, die een relatie gaat leggen tussen coëfficiënten van veeltermen en de nulwaarden van veeltermen. Van bijvoorbeeld de nulwaarden van een kwadratische vergelijking is bekend dat de oplossing uit te drukken is in een wortelvorm een breuk en de coëfficiënten van de kwadratische vergelijking als deze op nul is herleid en gelijksoortige termen zijn samengenomen. We beperken ons hier tot monische veeltermen, wat de algemeenheid niet schaadt als we het gaan hebben over vergelijkingen die op nul zijn herleid. Bij iedere term kunnen we dan immers de leidende coëfficiënt uitdelen en de oplossing van de vergelijking verandert in dat geval uiteraard niet.

Een waarde ζ uit de lichaamsuitbreiding $\mathcal{L}(\alpha)$ van $\mathcal{L}$ is nu per definitie een zogenaamde gebroken functie met als variabele α, waarvan de teller en noemer veeltermen zijn uit $\mathcal{L}[\alpha]$. Verwar dit niet met veeltermen zoals $f(x)$ die uit $\mathcal{L}[x]$ zijn. Voor zekere $\Psi(\alpha)$ en $\Phi(\alpha)$ uit $\mathcal{L}[\alpha]$ (veeltermen met coëfficiënten uit $\mathcal{L}$ en met variablele α) krijgen we zo $\zeta = \frac{\Psi(\alpha)}{\Phi(\alpha)}$.

Neem nu een veelterm $f(x)$ die *irreducibel* is over een lichaam $\mathcal{L}$. Laat nu α een nulwaarde zijn van $f(x)$, dan is $f(x)$ plotseling wel reducibel in de lichaamsuitbreiding $\mathcal{L}(\alpha)$ van $\mathcal{L}$. Nu volgt uit

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0$$

dat

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$$

waardoor

$$\alpha^n = -a_1\alpha^{n-1} - a_2\alpha^{n-2} - \cdots - a_n$$

Dit heeft als belangrijk gevolg dat iedere veelterm uit $\mathcal{L}[\alpha]$ terug te brengen is tot een veelterm met een graad die niet hoger is dan $n-1$! Bijvoorbeeld

$$\begin{aligned}\Lambda(\alpha) = \alpha^{n+1} = \alpha(\boldsymbol{\alpha^n}) &= \alpha\left(-\boldsymbol{a_1\alpha^{n-1}} - \boldsymbol{a_2\alpha^{n-2}} - \cdots - \boldsymbol{a_n}\right) = -a_1\boldsymbol{\alpha^n} - a_2\alpha^{n-1} - \cdots - a_n \cdot \alpha \\ &= -a_1\left(-\boldsymbol{a_1\alpha^{n-1}} - \boldsymbol{a_2\alpha^{n-2}} - \cdots - \boldsymbol{a_n}\right) - a_2\alpha^{n-1} - \cdots - a_n \cdot \alpha \\ &= (a_1^2 - a_2)\alpha^{n-1} + (a_1a_2 - a_3)\alpha^{n-2} + \cdots + (a_1a_{n-1} - a_n)\alpha + a_1a_n\end{aligned}$$

$\Lambda(\alpha)$ heeft nu een graad van ten hoogste $n-1$. Deze graad kan lager zijn, bijvoorbeeld als $a_1^2 - a_2 = 0$.

Dit voorbeeld maakt voldoende duidelijk hoe iedere veelterm uit $\mathcal{L}[\alpha]$, waar α een nulwaarde is van een veelterm met graad n (aangeduid met $f(x)$ in onze voorgaande beschouwing), terug te brengen is tot een veelterm van, ten hoogste, graad $n-1$.

Voor de waarde $\zeta = \frac{\Psi(\alpha)}{\Phi(\alpha)}$, kunnen we, als $\Psi(\alpha)$ een graad hoger dan $n-1$ heeft, vervangen door $\psi(\alpha)$ die een graad heeft van ten hoogste $n-1$. Evenzo kunnen we $\Phi(x)$ vervangen door een $\phi(x)$ met een graad van ten hoogste $n-1$, zodat

$$\zeta = \frac{\Psi(\alpha)}{\Phi(\alpha)} = \frac{\psi(\alpha)}{\phi(\alpha)}$$

Maar we kunnen een nog eenvoudiger weergave van ζ vinden. Immers aangezien $\phi(x)$ (let op: het argument is nu x, zodat $\phi(x)$ nu uit $\mathcal{L}[x]$ is, net als $f(x)$, en niet uit $\mathcal{L}[\alpha]$!) een lagere graad heeft dan $f(x)$ en $f(x)$ irreducibel is over $\mathcal{L}$, kunnen $f(x)$ en $\phi(x)$ geen gemeenschappelijke deler hebben uit $\mathcal{L}[x]$. Met het Euclidisch algoritme kunnen nu een $u(x)$ en $v(x)$ worden gevonden zodat

$$u(x) \cdot \phi(x) + v(x) \cdot f(x) = 1$$

We nemen nu α voor x en zo volgt

$$u(\alpha) \cdot \phi(\alpha) + v(\alpha) \cdot f(\alpha) = u(\alpha) \cdot \phi(\alpha) + v(\alpha) \cdot 0 = 1$$

Oftewel

$$u(\alpha) = \frac{1}{\phi(\alpha)}$$

zodat

$$\zeta = \psi(\alpha) \cdot \frac{1}{\phi(\alpha)} = \psi(\alpha) \cdot u(\alpha)$$

Maar dan is ζ een veelterm uit $\mathcal{L}[\alpha]$, die net als iedere veelterm uit $\mathcal{L}[\alpha]$ is terug te brengen tot een veelterm van ten hoogste graad $n-1$. Dus er zijn zekere c_i uit $\mathcal{L}$ zodat

$$\zeta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$$

We komen zo tot

Stelling 6.1
Iedere waarde uit een lichaamsuitbreiding $\mathcal{L}(\alpha)$, waar α een nulwaarde is van een *irreducibele* n^e-graads vergelijking uit $\mathcal{L}[x]$, kan worden weergegeven als een veelterm uit $\mathcal{L}[\alpha]$ van graad $n-1$. Dit kan slechts op één manier.

Bewijs
Er rest ons slechts aan te tonen dat er slecht één manier bestaat.
Gegeven is $\zeta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$ uit $\mathcal{L}(\alpha)$. Laat tevens $\zeta = C_0 + C_1\alpha + C_2\alpha^2 + \cdots + C_{n-1}\alpha^{n-1}$, dan volgt

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = C_0 + C_1\alpha + C_2\alpha^2 + \cdots + C_{n-1}\alpha^{n-1}$$

en

$$(c_0 - C_0) + (c_1 - C_1)\alpha + (c_2 - C_2)\alpha^2 + \cdots + (c_{n-1} - C_{n-1})\alpha^{n-1} = 0$$

De veelterm $(c_0 - C_0) + (c_1 - C_1)x + (c_2 - C_2)x^2 + \cdots + (c_{n-1} - C_{n-1})x^{n-1}$ heeft als nulwaarde derhalve α. Krachtens Gevolg 5.1 heeft iedere vergelijking uit $\mathcal{L}[x]$ met een lagere graad dan die van een irreducibele vergelijking met α als nulwaarde alleen maar coëfficiënten gelijk aan nul. We concluderen derhalve dat $c_i - C_i = 0$, zodat $C_i = c_i$, wat de uniciteit van de coëfficiënten van deze weergave en daarmee de uniciteit van deze weergave zelf bewijst.

Einde bewijs

We zien hier veel heen en weer springen tussen veeltermen/vergelijkingen uit $\mathcal{L}[x]$ en $\mathcal{L}[\alpha]$ om een willekeurige waarde uit $\mathcal{L}(\alpha)$ eenduidig en zo eenvoudig mogelijk weer te geven. We gaan hierna nog meer heen en weer slingeren, dus zorg ervoor dat je mentaal niet in de knoop raakt.

We hebben zojuist een eenvoudig voorbeeld gezien van een irreducibele veelterm (over een zeker lichaam) die reducibel werd door een nulwaarde in te voegen (in dit zekere lichaam, dus door een geschikte lichaamsuitbreiding van dit lichaam).

Laten we het meer algemene geval beschouwen waarin *een irreducibele veelterm* $f(x)$ uit $\mathcal{L}[x]$ een graad heeft die priem is, met $\deg\big(f(x)\big) = p$, die reducibel wordt over $\mathcal{L}(\alpha)$, waarbij $\boldsymbol{\alpha}$ een **nulwaarde** is **van** de *irreducibele vergelijking* $\boldsymbol{g(x)} = 0$, met $g(x)$ ook uit $\mathcal{L}[x]$ en $\deg\big(g(x)\big) = q$.

Aangezien $f(x)$ nu reducibel wordt veronderstelt over $\mathcal{L}(\alpha)$ is er een $\psi(x,\alpha)$ en een $\phi(x,\alpha)$ te vinden zodat $f(x) = \psi(x,\alpha)\cdot\phi(x,\alpha)$, met $\deg(\psi) = m$ en $\deg(\phi) = n$, zodat $p = m + n$. Neem nu voor x een waarde r uit $\mathcal{L}$ en vervang α weer door x. Dan is de hieronder gedefinieerde veelterm

$$u(x) = f(r) - \psi(r,x)\cdot\phi(r,x)$$

een veelterm uit $\mathcal{L}[x]$!

Bedenk dat uit $f(x) = \psi(x,\alpha)\cdot\phi(x,\alpha)$ volgt dat $f(r) = \psi(r,\alpha)\cdot\phi(r,\alpha)$, maar dat $f(r) \neq \psi(r,x)\cdot\phi(r,x)$, als voor x een waarde uit $\mathcal{L}$ wordt genomen die vanzelfsprekend altijd ongelijk α is!

Aangezien wel $u(\alpha) = f(r) - \psi(r,\alpha)\cdot\phi(r,\alpha) = 0$, zal $u(x)$ verdwijnen voor alle nulwaarden, zeg $\alpha,\ \alpha',\ \alpha'',\ \ldots$ van de over $\mathcal{L}$ irreducibele vergelijking $g(x) = 0$.

Indien we voor $\mathcal{L}$ nu een willekeurige lichaamsuitbreiding van $\mathbb{Q}$ nemen, volgt dat $f(x) - \psi(x,\alpha') \cdot \phi(x,\alpha') = 0$ en dus $f(x) = \psi(x,\alpha') \cdot \phi(x,\alpha')$, voor ieder waarde van x uit $\mathcal{L}$. In dat geval nemen we ook aan dat ook voor reële en complexe waarden van x deze vergelijking klopt. De rechtvaardiging bestaat uit de notie dat reële en de imaginaire waarden willekeurig dicht benaderd kunnen worden door rationale waarden (let wel dat dit onder bepaalde beschouwingen niet zomaar een triviale aanname is). Voor iedere waarde van x krijgen we zo

$$f(x) = \psi(x,\alpha') \cdot \phi(x,\alpha')$$

En evenzo **het stelsel vergelijkingen** op basis van alle andere q nulwaarden van $g(x)$ ($\deg(g) = q$)

$$f(x) = \psi(x,\alpha) \cdot \phi(x,\alpha)$$

$$f(x) = \psi(x,\alpha') \cdot \phi(x,\alpha')$$

$$f(x) = \psi(x,\alpha'') \cdot \phi(x,\alpha'')$$

etc.

Zodat

$$f(x)^q = \psi(x,\alpha)\phi(x,\alpha) \cdot \psi(x,\alpha')\phi(x,\alpha') \cdot \psi(x,\alpha'')\phi(x,\alpha'') \cdot \ldots =$$

$$= \psi(x,\alpha) \cdot \psi(x,\alpha') \cdot \psi(x,\alpha'') \cdot \ldots \cdot \phi(x,\alpha) \cdot \phi(x,\alpha') \cdot \phi(x,\alpha'') \cdot \ldots = \Psi(x) \cdot \Phi(x)$$

met

$$\Psi(x) = \psi(x,\alpha) \cdot \psi(x,\alpha') \cdot \psi(x,\alpha'') \cdot \ldots$$

en

$$\Phi(x) = \phi(x,\alpha) \cdot \phi(x,\alpha') \cdot \phi(x,\alpha'') \cdot \ldots$$

Omdat beide producten $\Psi(x)$ en $\Phi(x)$ symmetrische veeltermen zijn van de nulwaarden van de veelterm $g(x)$, kan volgens het *theorema van Waring* (zie intermezzo hieronder) ieder van deze producten als een veelterm uit $\mathcal{L}[x]$ worden weergegeven middels de coëfficiënten van $g(x)$. Dus $\Psi(x)$ en $\Phi(x)$ zijn dan beide net als $g(x)$ uit $\mathcal{L}[x]$!

Intermezzo: het theorema van Waring

Wederom starten we met een voorbeeld om duidelijk te maken wat er eigenlijk aan de hand is. Neem bijvoorbeeld de over $\mathcal{L}$ irreducibele monische veelterm $g(t)$ met $\deg(g) = 3$. Volgens de hoofdstelling van de algebra heeft $g(t)$ dan drie nulwaarden, zeg x_1, x_2 en x_3 (alle drie niet uit $\mathcal{L}$ uiteraard), dus we kunnen noteren

$$g(t) = (t - x_1)(t - x_2)(t - x_3) = t^3 - (x_1 + x_2 + x_3)t^2 + (x_1x_2 + x_1x_3 + x_2x_3)t - x_1x_2x_3 = \\ = x^3 + ax^2 + bx + c$$

met $a = -(x_1 + x_2 + x_3)$, $b = x_1x_2 + x_1x_3 + x_2x_3$ en $c = -x_1x_2x_3$, allen uit $\mathcal{L}$.

Neem nu b.v.

$\phi(t,x_1) = t^2 + 2x_1t - 3x_1$, $\phi(t,x_2) = t^2 + 2x_2t - 3x_2$ en $\phi(t,x_3) = t^2 + 2x_3t - 3x_3$,

dan zal onder permutatie van x_1, x_2 en x_3 hetzelfde drietal veeltermen worden verkregen, met andere woorden $\Phi(t) = \phi(t, x_1) \cdot \phi(t, x_2) \cdot \phi(t, x_3)$ is symmetrisch, d.w.z. onveranderlijk als we x_1, x_2 en x_3 onderling verwisselen.

Dan volgt door uitschrijven:

$$\Phi(t) = \phi(t, x_1) \cdot \phi(t, x_2) \cdot \phi(t, x_3) = (t^2 + 2x_1 t - 3x_1)(t^2 + 2x_2 t - 3x_2)(t^2 + 2x_3 t - 3x_3) =$$

$$\begin{aligned} &= t^6 + 2(x_1 + x_2 + x_3)t^5 + [-3(x_1 + x_2 + x_3) + 4(x_1x_2 + x_1x_3 + x_2x_3)]t^4 \\ &\quad - 12(x_1x_2 + x_1x_3 + x_2x_3)t^3 + \\ &-36x_1x_2x_3 \cdot t^2 - 54x_1x_2x_3 \cdot t - 27x_1x_2x_3 \\ &= x^6 - 2a \cdot x^5 + (3a + 4b) \cdot x^4 - 12b \cdot x^3 + 36c \cdot x^2 + 54c \cdot x + 27c \end{aligned}$$

Waarmee we inderdaad alle coëfficiënten van $\Phi(t)$ hebben uitgedrukt in de coëfficiënten van $g(t)$, zodat $\Phi(t)$ net als $g(t)$ uit $\mathcal{L}[t]$ is; $\Phi(t)$ heeft zo net als $g(t)$ coëfficiënten uit $\mathcal{L}$.

Theorema van Waring

Het theorema van Waring staat ook wel bekend als de Newton identiteiten of de Newton-Girard formules

Hier worden de relaties weergegeven tussen twee typen symmetrische veeltermen, namelijk tussen de *machtssommen* en de *elementaire symmetrische veeltermen*.

Ontwikkeld aan de hand van de nulwaarden van een monische veelterm staan ze toe de som van de k^{e} macht van alle nulwaarden van een veelterm uit te drukken in de coëfficiënten van deze veelterm, zonder daadwerkelijk de nulwaarden van deze veelterm te vinden.

Formulering in de vorm van symmetrische polynomen. Neem een veelterm met $\boldsymbol{n}$ **variabelen**. Dergelijke veeltermen zijn symmetrisch indien de veelterm zichzelf oplevert na een willekeurige permutatie (omwisselen) van de n variabelen. Nu definiëren we de **elementaire symmetrische veeltermen met $\boldsymbol{n}$ variabelen**, genoteerd als $\boldsymbol{e_k}$, als volgt

$$e_0 = 1$$

$$e_1 = x_1 + x_2 + x_3 + \cdots + x_n$$

$$\begin{aligned} e_2 = x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_1x_n + \\ + x_2x_3 + x_2x_4 + \cdots + x_2x_n + \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \\ + x_{n-1}x_n \end{aligned}$$

$$\begin{aligned} e_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + \cdots + x_1x_2x_n + \\ + x_1x_3x_4 + x_1x_3x_5 + \cdots + x_1x_3x_n + \\ \ldots\ldots\ldots\ldots\ldots + x_{n-2}x_{n-1}x_n \end{aligned}$$

$$\begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array}$$

$$e_n = x_1x_2x_3 \ldots x_n$$

Neem nu de symmetrische veelterm

$$p_k = \sum_{i=1}^{n} x_i^k = x_1^k + x_2^k + \cdots + x_n^k$$

Dan kunnen we de identiteiten van Newton vast stellen als

$e_1 = p_1$
$2 \cdot e_2 = e_1 \cdot p_1 - p_2$ (de eerste term, $e_1 \cdot p_1$, produceert x_i^2 termen die door $-p_2$ weer verdwijnen)
$3 \cdot e_3 = e_2 \cdot p_1 - e_1 \cdot p_2 + p_3$
$4 \cdot e_4 = e_3 \cdot p_1 - e_2 \cdot p_2 + e_1 \cdot p_3 - p_4$ etc.

Dat de betrekkingen kloppen is door uitschrijven direct te verifiëren. Evenzo valt er dan een patroon te ontdekken in de identiteiten zodat we in het algemeen kunnen stellen dat

$$k \cdot e_k = \sum_{i=1}^{k} (-1)^{i-1} \cdot e_{k-i} \cdot p_i$$

We kunnen nu ook de p_k recursief uitdrukken middels de elementaire symmetrische veeltermen

$p_1 = e_1$
$p_2 = e_1 \cdot p_1 - 2e_2$
$p_3 = e_1 \cdot p_2 - e_2 \cdot p_1 + 3 \cdot e_3$ etc.

We gaan het zojuist verkregen resultaat toepassen op de nulwaarden van een *monische* veelterm, waarbij we de x_i nemen als de nulwaarden en we nemen als variabele t. We definiëren de veelterm

$$g(t) = \prod_{i=0}^{n} (t - x_i) = \sum_{k=0}^{n} (-1)^k a_k t^{n-k}$$

Waarbij we automatisch $a_k = e_k$ verkrijgen.

Middels uitschrijven is dit direct na te gaan. B.v. voor $n = 3$

$$\begin{aligned} g(t) = (t - x_1)(t - x_2)(t - x_3) &= t^3 - (x_1 + x_2 + x_3)t^2 + (x_1x_2 + x_1x_3 + x_2x_3)t - x_1x_2x_3 \\ &= e_0t^3 - e_1t^2 + e_2t - e_3 \end{aligned}$$

Voor de p_k krijgen we dus

$p_1 = a_1$
$p_2 = a_1 \cdot p_1 - 2a_2$
$p_3 = a_1 \cdot p_2 - a_2 \cdot p_1 + 3 \cdot a_3$ etc.

Zowel de e_k als de p_k zijn dus uit te drukken in de a_k, oftewel in de coëfficiënten van $g(x)$, waarbij natuurlijk $\deg(g) = n$ en $0 \leq k \leq n$.

Nu is iedere symmetrische veelterm met variabelen $x_1, \ldots, x_n$ te schrijven als een functie van de e_k en de p_k. Als bijvoorbeeld ${x_1}^l * f(\ldots)$ in deze functie voorkomt dan zal ook ${x_2}^l * f(\ldots)$ hier in voor moeten komen, waarbij $*$ voor zowel $+$ als $\cdot$ kan staan, etc. Waardoor we $p_l * f(\ldots)$ krijgen, ofwel door termen te herrangschikken, ofwel door $f(\ldots)$ buiten haakjes te halen. Dit moet gelden voor iedere factor of term die bestaat uit een enkele ${x_k}^l$ die in een symmetrische functie voorkomt.

Uiteraard moet de uit veeltermen samengestelde $f(\dots)$ ook weer symmetrisch zijn en daarbinnen moet dan eveneens weer voor iedere ${x_k}^l$ net als hiervoor een p_l zijn te formeren als factor of term enz.

Aangezien iedere symmetrische veelterm met de variabelen $x_1, \dots, x_n$ te schrijven is als een functie van de e_k en de p_k, en de e_k en p_k zijn uit te drukken in de a_k, de coëfficiënten van de veelterm $g(t) = \prod_{i=0}^{n}(t - x_i)$, met deze variabelen als nulwaarden, kunnen we concluderen dat ook de coëfficiënten van de veelterm $\Psi(t, x_1, x_2, \dots, x_n) = \psi(t, x_1) \cdot \psi(t, x_1) \cdot \dots \cdot \psi(t, x_n)$ uit te drukken zijn in de coëfficiënten a_k van $g(t)$.

De belangrijke conclusie is dat als de coëfficiënten van $g(t) = \prod_{i=0}^{n}(t - x_i)$ uit een lichaam $\mathcal{L}$ zijn, dat de coëfficiënten van de symmetrische veelterm $\Psi(t, x_1, x_2, \dots, x_n) = \psi(t, x_1) \cdot \psi(t, x_1) \cdot \dots \cdot \psi(t, x_n)$ ook uit $\mathcal{L}$ zijn, terwijl de nulwaarden van $x_1, \dots, x_n$ van $g(t)$ niet noodzakelijkerwijs uit $\mathcal{L}$ hoeven te zijn.

Einde intermezzo

Nu verdwijnt $\Psi(x)$ zeker voor tenminste één nulwaarde van de irreducibele vergelijking $f(x) = 0$, net zoals $\Phi(x)$. Immers $f(x)$ heeft een hogere graad dan b.v. $\phi(\alpha)$ en dus ook meer nulwaarden dan $\phi(\alpha)$. Aangezien $\phi(\alpha)$ minder nulwaarden heeft dan $f(x) = \psi(x, \alpha) \cdot \phi(x, \alpha)$ moet $\psi(x)$ minstens één nulwaarde van $f(x)$ bevatten, waardoor $\Psi(x)$ ook minstens één nulwaarde van $f(x)$ als nulwaarde moet hebben. Wegens Stelling 5.7 (Abels fundamentele theorema over vergelijkingen van de irreducibele veeltermen) deelt $f(x)$ derhalve $\Psi(x)$ en $\Phi(x)$, omdat uit $f(x) = 0$ volgt dat $\Psi(x) = 0$ en $\Phi(x) = 0$. Omdat $f(x)$ irreducibel is en $f(x)^q = \Psi(x) \cdot \Phi(x)$ volgt nu dat er geen andere deler dan $f(x)$ mogelijk is, waardoor

$$\Psi(x) = f(x)^{\mu}, \qquad \Phi(x) = f(x)^{\nu}$$

Met $\mu + \nu = q$. Aangezien $\deg(\Psi) = \deg(\psi(x, \alpha) \cdot \psi(x, \alpha') \cdot \psi(x, \alpha'') \cdot \dots) = q \cdot m$ en evenzo $\deg(\Phi) = q \cdot n$ en $\deg(f) = p$, volgt nu uit de beide vergelijkingen dat

$$m \cdot q = \mu \cdot p\,, \qquad n \cdot q = \nu \cdot p$$

Omdat m en n kleiner dan p zijn, kan p geen deler zijn van m en n. Omdat p tevens priem is, kan p niet voorkomen in de priemfactorontbinding van m en n. Hieruit volgt dat p dan wel een deler van q moet zijn, d.w.z. voor moet komen in de priemfactorontbinding van q.

Samenvattend hebben we zo verkregen, onder de voorwaarde dat $\deg(f)$ priem is: ***als*** (A) $f(x) = 0$ irreducibel is over $\mathcal{L}$, maar ***reducibel*** wordt over $\mathcal{L}(\alpha)$, waarbij α een nulwaarde is van een andere over $\mathcal{L}$ irreducibele vergelijking $g(x) = 0$, ***dat*** (B) $\deg(f)$ een ***deler*** is van $\deg(g)$.
Dus de enige manier waarop een irreducibele vergelijking met een graad die priem is reducibel kan worden door de nulwaarde van een andere irreducibele vergelijking in te voegen, is als de priemgraad de graad van de andere irreducibele vergelijking deelt.

We hebben daarmee de volgende belangrijke stelling bewezen.

Stelling 6.2 (irreducibel, reducibel en priemgraad)
Een irreducibele vergelijking uit $\mathcal{L}[x]$ waarvan de graad priem is, **kan** alleen dan reducibel worden over $\mathcal{L}(\alpha)$, waarbij α een nulwaarde is van een andere irreducibele vergelijking uit $\mathcal{L}[x]$, als de priemgraad van de eerstgenoemde vergelijking een deler is van de graad van de laatstgenoemde vergelijking.

7. De Stelling van Abel-Ruffini

Na de hiervoor verkregen resultaten kunnen we ons richten op de stelling van Abel-Ruffini:

Voor de oplossing van een vergelijking van graad vijf of hoger met rationale coëfficiënten bestaat geen formule uitgedrukt in wortelvormen, rationale getallen en de coëfficiënten van de termen in de vergelijking.

Stelling 6.2 gaat ons vertrekpunt worden. We recapituleren nog eens de basis-ingrediënten die ons scherp zicht geven op de situatie.

Bij een lichaam $\mathcal{L}$ definieerden we een ring van veeltermen, allen met variabele x, genoteerd als $\mathcal{L}[x]$. Alle coëfficiënten van iedere veelterm uit $\mathcal{L}[x]$ zijn per definitie dan uit $\mathcal{L}$.
Een lichaamsuitbreiding van $\mathcal{L}$ door het toevoegen van een waarde α, waarbij α niet uit $\mathcal{L}$ is noteren we met $\mathcal{L}(\alpha)$. Dat wil zeggen dat als we een veelterm $f(x)$ en $g(x)$ uit de ring $\mathcal{L}[x]$ nemen, dat als regel geldt dat de waarde $\frac{f(\alpha)}{g(\alpha)}$ uit $\mathcal{L}(\alpha)$ is. Met deze regel kan direct bewezen worden dat een lichaamsuitbreiding ook daadwerkelijk een lichaam is. We gebruiken dus de ring van veeltermen over een zeker lichaam om een lichaamsuitbreiding van dit lichaam te kunnen construeren. Stelling 6.1 geeft een belangrijk speciaal geval zodat de waarden uit sommige $\mathcal{L}(\alpha)$ als veeltermen uit $\mathcal{L}[\alpha]$ kunnen worden weergegeven.

Neem nu $f(x)$ uit $\mathcal{L}[x]$, dan noemen we de vergelijking $f(x) = 0$ algebraïsch oplosbaar indien er een lichaamsuitbreiding van $\mathcal{L}$ te vinden is, verkregen door breuk- en wortelvormen van waarden uit $\mathcal{L}$. Zo'n lichaamsuitbreiding is in stappen te construeren. Bijvoorbeeld:

1. Bepalen van de a^e wortel $\alpha = \sqrt[a]{L}$, waarbij L een waarde is uit een lichaam $\mathcal{L}$, maar geen a^e macht van een waarde uit $\mathcal{L}$, zodat het lichaam $\mathcal{L}(\alpha)$ kan worden gevormd.
2. Bepalen van de b^e wortel $\beta = \sqrt[b]{A}$, waarbij A een waarde is uit een lichaam $\mathcal{A}$, maar geen b^e macht van een waarde uit $\mathcal{A}$, zodat het lichaam $\mathcal{A}(\beta) = \mathcal{L}(\alpha, \beta)$ is te vormen.
3. Bepalen van de c^e wortel $\gamma = \sqrt[c]{B}$, waarbij B een waarde is uit een lichaam $\mathcal{B}$, maar geen c^e macht van een waarde uit $\mathcal{B}$, zodat het lichaam $\mathcal{B}(\gamma) = \mathcal{L}(\alpha, \beta, \gamma)$ is te vormen, etc. totdat een lichaam $\mathcal{L}(\alpha, \beta, \gamma, \dots)$ is gevormd, waarover de veelterm $f(x)$ reducibel is geworden.

We kunnen verder de belangrijke (!) beperking opleggen dat de wortel-exponenten a, b en c priem moeten zijn, aangezien de noemer van een gebroken exponent kan worden weergegeven als een priemfactorontbinding die weer als geneste wortelvorm zijn weer te geven. Bijvoorbeeld: $\sqrt[15]{u} = u^{\frac{1}{15}} = u^{\frac{1}{3\cdot 5}} = (u^{\frac{1}{5}})^{\frac{1}{3}} = \sqrt[3]{\sqrt[5]{u}}$.

Om onze taak enigszins te verkorten beperken we ons tot vergelijkingen $f(x) = 0$ waarvan de coëfficiënten rationaal zijn, die tevens irreducibel zijn over $\mathbb{Q}$, van oneven priemgraad n (om 2 als enige even priemgetal er buiten te laten).

Laten we van start gaan met het **invoegen van de n^e wortel van 1**

$$\boldsymbol{\eta} = \sqrt[n]{1} = e^{i\cdot\frac{2\pi}{n}}$$

Volgens stelling 6.2 maakt deze toevoeging $f(x)$ nog steeds niet reducibel. Immers η is een oplossing van de vergelijking verkregen uit de meetkundige reeks $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$, die

graad $n-1$ heeft, en dus van een lagere graad is dan de graad van $f(x)=0$ en daarom niet door de graad van de vergelijking $f(x)=0$ kan worden gedeeld.

We voegen tegelijkertijd met iedere toegevoegde wortelvorm de **complexe geconjugeerde** van deze wortelvorm **toe**. Er kunnen zich nu twee gevallen voordoen, namelijk $f(x)$ blijft irreducibel of $f(x)$ wordt reducibel door de toegevoegde wortelvorm en zijn complex geconjugeerde.
Dat we ook de complex geconjugeerde wortelvorm toevoegen is van groot belang. Als we zo door het toevoegen van wortelvormen uiteindelijk uit $\mathbb{Q}$ de lichaamsuitbreiding $\mathcal{K}$ verkrijgen dan zal **van iedere waarde uit $\mathcal{K}$ ook de complex geconjugeerde uit $\mathcal{K}$** zijn. Dit is als volgt in te zien. Iedere waarde uit $\mathcal{K}$ ontstaat uit berekeningen met rationale getallen of toegevoegde wortelvormen uit $\mathcal{K}$, want $\mathcal{K}$ is tenslotte een lichaam. Zo'n berekeningen bestaat uit optellen, vermenigvuldigen en delen van andere $\mathcal{K}$ waarden. Laat nu κ een willekeurige waarde uit $\mathcal{K}$ zijn dan volgt $\kappa = berekening(\alpha,\beta,\gamma,\dots)$ zijn met $\alpha,\ \beta,\ \gamma,\dots$ rationale getallen of de toegevoegde wortelvormen uit $\mathcal{K}$. Maar dan zijn $\bar{\alpha},\ \bar{\beta},\ \bar{\gamma},\dots$ ook automatisch $\mathcal{K}$ waarden en is iedere berekening van deze complex geconjugeerde waarden ook weer een $\mathcal{K}$ waarde. De rekenregels voor complex conjugeren zijn

1. $\overline{z+w} = \bar{z}+\bar{w}$
2. $\overline{z\cdot w} = \bar{z}\cdot\bar{w}$
3. $\overline{\frac{z}{w}} = \frac{\bar{z}}{\bar{w}}$
4. $\overline{z^n} = \bar{z}^n$
5. $\overline{\sqrt[n]{z}} = \sqrt[n]{\bar{z}}$

Zodat $berekening\left(\bar{\alpha},\ \bar{\beta},\ \bar{\gamma},\dots\right) = \overline{berekening(\alpha,\beta,\gamma,\dots)} = \bar{\kappa}$ ook een $\mathcal{K}$ waarde moet zijn.

Laat nu de monische veelterm $\boldsymbol{f(x)}$ **irreducibel** zijn **over** de met wortelvormen verkregen lichaamsuitbreiding $\boldsymbol{\mathcal{K}}$ van $\mathbb{Q}$. Neem nu aan dat er een wortelvorm $\lambda = \sqrt[l]{K}$, oplossing van de vergelijking $g(x) = x^l - K = 0$, is, met K uit $\mathcal{K}$, waardoor $\boldsymbol{f(x)}$ **reducibel** wordt over $\boldsymbol{\mathcal{K}(\lambda)}$. We kunnen dus aannemen dat er (volgens stelling 4.5 unieke) irreducibele monische veeltermen $\psi(x,\lambda)$, $\phi(x,\lambda),\ \chi(x,\lambda),\ \dots$ zijn zodat

$$f(x) = \psi(x,\lambda)\cdot\phi(x,\lambda)\cdot\chi(x,\lambda)\cdot\dots$$

Verder hadden we hierboven schuindikgedrukt aangegeven dat alle wortel-exponenten gebruikt bij lichaamsuitbreidingen priem zijn, dus l is ook priem. Wat inhoud dat $g(x) = x^l - K = 0$ volgens het Lemma van Abel (stelling 5.4) irreducibel is. Immers K is geen l^e macht (dan zou $\sqrt[l]{K}$ immers geen wortelvorm met wortel-exponent l zijn).

Op grond van Stelling 6.1 kunnen we zo concluderen dat, omdat λ de nulwaarde is van de l^e graads irreducibele vergelijking $g(x)=0$, iedere waarde van de lichaamsuitbreiding $\mathcal{K}(\lambda)$ kan worden weergegeven als een veelterm uit $\mathcal{K}[\lambda]$ van graad $l-1$. Aangezien de coëfficiënten van $\psi(x,\lambda)$, $\phi(x,\lambda),\ \chi(x,\lambda),\ \dots$ uit $\mathcal{K}(\lambda)$ zijn kunnen we stellen dat al deze coëfficiënten kunnen worden weergegeven als veeltermen uit $\mathcal{K}[\lambda]$, dus als veeltermen over $\mathcal{K}$.

Volgens stelling 6.2 moet de priemgraad n van $f(x)$ de priemgraad l van $g(x)$ delen. Uit de definitie van een priemgetal volgt zo onmiddellijk dat $l=n$.

De n nulwaarden van de irreducibele vergelijking $g(x) = x^l - K = x^n - K = 0$ zijn zo

$\lambda_0 = \lambda = \sqrt[n]{K}\,, \quad \lambda_1 = \lambda \cdot e^{i\cdot\frac{2\pi}{n}} = \lambda \cdot \eta, \quad \lambda_2 = \lambda \cdot \eta^2, \ldots\ldots, \lambda_\nu = \lambda \cdot \eta^\nu, \ldots\ldots, \lambda_{n-1} = \lambda \cdot \eta^{n-1}$

Merk op dat $\lambda_0 = \lambda_n$. Omdat we $\boldsymbol{\eta}$ **al** hadden **ingevoegd** zijn **alle** $\boldsymbol{\lambda_\nu}$ **uit** $\boldsymbol{\mathcal{K}(\lambda)}$ (ga na!)

Omdat $\boldsymbol{\psi(x,\lambda)}$ **een deler is van** $\boldsymbol{f(x)}$**, is** $\boldsymbol{\psi(x,\lambda_\nu)}$ **ook een deler van** $\boldsymbol{f(x)}$. Dit volgt uit het, in de redenering tussen stelling 6.1 en 6.2, verkregen stelsel

$$f(x) = \psi(x,\alpha) \cdot \phi(x,\alpha)$$

$$f(x) = \psi(x,\alpha') \cdot \phi(x,\alpha')$$

$$f(x) = \psi(x,\alpha'') \cdot \phi(x,\alpha'')$$

etc.

onder de voorwaarde "dat $f(x)$ *een irreducibele veelterm* uit $\mathcal{L}[x]$ is met een graad die priem is, die reducibel wordt over $\mathcal{L}(\alpha)$, waarbij $\boldsymbol{\alpha, \alpha', \alpha'', \ldots}$ **nulwaarden** zijn **van** de *irreducibele vergelijking* $\boldsymbol{g(x) = 0}$, met $g(x)$ ook uit $\mathcal{L}[x]$". Voor α moeten we nu λ nemen ($\lambda_3 = \lambda'''$ enz.) en voor $\mathcal{L}$ moeten we nu $\mathcal{K}$ nemen.

Lemma 7.1
Ieder van de n veeltermen $\psi(x,\lambda_\nu)$ is irreducibel over $\mathcal{K}(\lambda)$.

Bewijs

$$f(x) = \psi(x,\lambda) \cdot \phi(x,\lambda) \cdot \chi(x,\lambda) \cdot \ldots = \psi(x,\lambda) \cdot \Psi(x,\lambda)$$

waarbij $\psi(x,\lambda)$ irreducibel is en $\Psi(x,\lambda) = \phi(x,\lambda) \cdot \chi(x,\lambda)$ uiteraard reducibel over $\mathcal{K}(\lambda)$. Aangezien λ_ν een nulwaarde is van over $\mathcal{K}$ irreducibele vergelijking $g(x) = 0$ moet nu ook volgens de redenering hierboven ook gelden

$$f(x) = \psi(x,\lambda_\nu) \cdot \Psi(x,\lambda_\nu)$$

Stel nu dat $\psi(x,\lambda_\nu)$ reducibel is over $\mathcal{K}(\lambda)$, dan zijn er zekere $u(x,\lambda_\nu)$ en $v(x,\lambda_\nu)$, zodat

$$\psi(x,\lambda_\nu) = u(x,\lambda_\nu) \cdot v(x,\lambda_\nu)$$

zodat

$$f(x) = u(x,\lambda_\nu) \cdot v(x,\lambda_\nu) \cdot \Psi(x,\lambda_\nu)$$

Dit geld voor iedere ν dus ook voor $\nu = 0$, dus voor $\lambda_0 = \lambda$, wat weer betekent dat

$$f(x) = u(x,\lambda) \cdot v(x,\lambda) \cdot \Psi(x,\lambda_0) = u(x,\lambda) \cdot v(x,\lambda) \cdot \Psi(x,\lambda) = \psi(x,\lambda) \cdot \Psi(x,\lambda)$$

zodat $\psi(x,\lambda) = u(x,\lambda) \cdot v(x,\lambda)$, maar dat is niet mogelijk want $\psi(x,\lambda)$ irreducibel over $\mathcal{K}(\lambda)$. De aanname dat $\psi(x,\lambda_\nu)$ reducibel is over $\mathcal{K}(\lambda)$ moet daarmee worden verworpen, dus ieder van de n veeltermen $\psi(x,\lambda_\nu)$ is irreducibel over $\mathcal{K}(\lambda)$.

Einde bewijs

Lemma 7.2
Alle n veeltermen $\psi(x,\lambda_\nu)$ verschillen van elkaar.

Bewijs
Neem eens aan dat $\psi(x,\lambda\eta^\mu)=\psi(x,\lambda\eta^\nu)$, waarin λ zoals hiervoor vervangen kan worden door de nulwaarde $\lambda\eta^{n-\mu}=\lambda\eta^{-\mu}$, waaruit volgt

$$\psi(x,\lambda\eta^\mu)=\psi(x,\lambda\eta^{-\mu}\eta^\mu)=\psi(x,\lambda)$$

en met $H=\eta^{\nu-\mu}$

$$\psi(x,\lambda\eta^\mu)=\psi(x,\lambda\eta^\nu)=\psi(x,\lambda\eta^{-\mu}\eta^\nu)=\psi(x,\lambda\eta^{\nu-\mu})=\psi(x,\lambda\cdot H)$$

zodat

$$\psi(x,\lambda)=\psi(x,\lambda\cdot H)$$

Ook hier kunnen we λ weer vervangen voor $\lambda\cdot H$ waardoor

$$\psi(x,\lambda)=\psi(x,\lambda\cdot H\cdot H)=\psi(x,\lambda\cdot H^2)$$

Evenzo volgt

$$\psi(x,\lambda\cdot H^2)=\psi(x,\lambda\cdot H^3)$$

etc.

Zo verkrijgen we

$$\psi(x,\lambda)=\psi(x,\lambda\cdot H)=\psi(x,\lambda\cdot H^2)=\psi(x,\lambda\cdot H^3)=\cdots=\psi(x,\lambda\cdot H^{n-1})$$

zodat

$$n\cdot\psi(x,\lambda)=\underbrace{\psi(x,\lambda)+\cdots+\psi(x,\lambda)}_{n\ termen}=\psi(x,\lambda\cdot H)+\psi(x,\lambda\cdot H^2)+\cdots+\psi(x,\lambda\cdot H^{n-1})$$

waarmee

$$\psi(x,\lambda)=\frac{\psi(x,\lambda\cdot H)+\psi(x,\lambda\cdot H^2)+\cdots+\psi(x,\lambda\cdot H^{n-1})}{n}$$

Het rechter lid van de laatste vergelijking is echter een symmetrische veelterm van de n nulwaarden $\lambda\cdot H^{n-\nu}$ van de veelterm $g(x)=x^n-K$, wat betekend dat volgens het theorema van Waring de coëfficiënten van $\psi(x,\lambda)$net als de coëfficiënten van $g(x)$ uit $\mathcal{K}$ zijn! Dit resultaat dat we zo voor $\psi(x,\lambda)$ verkregen moet dan ook gelden voor $\phi(x,\lambda)$, $\chi(x,\lambda)$, … zodat we moeten veronderstellen dat $f(x)=\psi(x,\lambda)\cdot\phi(x,\lambda)\cdot\chi(x,\lambda)\cdot\ldots$ reducibel is in $\mathcal{K}$, wat in tegenspraak is met wat we vooorondersteld hebben over $f(x)$. De aanname dat $\psi(x,\lambda\eta^\mu)=\psi(x,\lambda\eta^\nu)$ moet worden verworpen. Aangezien μ en ν willekeurig zijn gekozen, moeten we concluderen dat alle n veeltermen $\psi(x,\lambda_\nu)$ van elkaar verschillen.

Einde bewijs

Uit Lemma 7.1 en 7.2 volgt dat $\psi(x,\lambda_\mu)$ en $\psi(x,\lambda_\nu)$ elkaar niet kunnen delen over $\mathcal{K}(\lambda)$, maar, zoals hierboven door ons verondersteld werd, wel $f(x)$ delen Beschouw nu

$$f(x)=\psi(x,\lambda)\cdot\phi(x,\lambda)\cdot\chi(x,\lambda)\cdot\ldots=\psi(x,\lambda)\cdot U_0(x)$$

Met $U_0(x)=\phi(x,\lambda)\cdot\chi(x,\lambda)\cdot\ldots$

Omdat $\psi(x,\lambda_1)$ de veelterm $f(x)=\psi(x,\lambda)\cdot U_0(x)$ wel deelt, maar $\psi(x,\lambda)=\psi(x,\lambda_0)$ niet deelt, kan het niet anders zijn dan dat $\psi(x,\lambda_1)$ de veelterm $U_0(x)$ deelt. Er is dus een $U_1(x)$ zodat

$$U_0(x) = \psi(x, \lambda_\nu) \cdot U_1(x)$$

zodat

$$f(x) = \psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot U_1(x)$$

Evenzo volgt dat er een $U_2(x)$ moet zijn zodat

$$f(x) = \psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \psi(x, \lambda_2) \cdot U_2(x)$$

aangezien $\psi(x, \lambda_2)$ de veelterm $f(x)$ wel en $\psi(x, \lambda)$ en $\psi(x, \lambda_1)$ niet deelt.
Zo doorgaand concluderen we dat er een $U(x) = U_{n-1}(x)$ moet zijn zodat

$$f(x) = \psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \ldots \cdot \psi(x, \lambda_{n-1}) \cdot U(x) = \Psi(x) \cdot U(x)$$

Met $\Psi(x) = \psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \ldots \cdot \psi(x, \lambda_{n-1})$. Aangezien $\Psi(x)$ een symmetrische veelterm is en de λ_ν nulwaarden zijn van $g(x)$ uit $\mathcal{K}[x]$, moeten de coëfficiënten van $\Psi(x)$ ook uit $\mathcal{K}$ zijn volgens het theorema van Waring.

Omdat $f(x)$ ook een veelterm over $\mathcal{K}$ is, kan het niet anders dat $U(x)$ ook een veelterm met coëfficiënten uit $\mathcal{K}$ is (haakjes wegwerken in $\Psi(x) \cdot U(x)$ en daarna gelijksoortige termen samennemen zou als $U(x)$ coëfficiënten uit $\mathcal{K}(\lambda)$ bevat, die alleen met coëfficiënten uit $\mathcal{K}$ van $\Psi(x)$ kunnen worden vermenigvuldigd, coëfficiënten uit $\mathcal{K}(\lambda)$ opleveren voor de zo verkregen veelterm. Deze kan natuurlijk nooit gelijk zijn aan $f(x)$)

Omdat $f(x)$ evenwel irreducibel is over $\mathcal{K}$ en monisch wordt verondersteld en we zonder de algemeenheid te schaden ook $\Psi(x)$ monisch kunnen veronderstellen, zijn we daarom genoodzaakt $U(x) = 1$ te nemen.

Uiteindelijk krijgen we zo

$$f(x) = \psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \ldots \cdot \psi(x, \lambda_{n-1})$$

Aangezien $\deg(f) = n$ moet tevens $\deg\big(\psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \ldots \cdot \psi(x, \lambda_{n-1})\big) = n$. Omdat de $\psi(x, \lambda_\nu)$ allen uit $\psi(x, \lambda)$ ontstaan door λ te vervangen voor λ_ν, moet wel gelden dat $\deg\big(\psi(x, \lambda_\nu)\big) = \deg\big(\psi(x, \lambda)\big)$. Dus

$$\deg\big(\psi(x, \lambda) \cdot \psi(x, \lambda_1) \cdot \ldots \cdot \psi(x, \lambda_{n-1})\big) = n \cdot \deg\big(\psi(x, \lambda)\big) = n$$

zodat

$$\deg\big(\psi(x, \lambda_\nu)\big) = \deg\big(\psi(x, \lambda)\big) = 1$$

Het kan zo niet anders zijn dan dat $f(x)$ in $\mathcal{K}(\lambda)$ op te delen is in n lineaire veeltermen over $\mathcal{K}(\lambda)$. Neem nu $\psi(x, \lambda_\nu) = a_\nu \cdot x + b_\nu$. Omdat $f(x)$ monisch is moet wel gelden $\prod_\nu a_\nu = 1$, maar dan kunnen we met

$$f(x) = \prod_\nu \psi(x, \lambda_\nu) = \prod_\nu a_\nu \cdot x + b_\nu = \prod_\nu a_\nu \cdot \left(x + \frac{b_\nu}{a_\nu}\right) =$$

$$= a_0 \cdot a_1 \cdot \ldots \cdot a_{n-1} \cdot \left(x + \frac{b_0}{a_0}\right) \cdot \left(x + \frac{b_1}{a_1}\right) \ldots \cdot \left(x + \frac{b_{n-1}}{a_{n-1}}\right) = 1 \cdot \left(x + \frac{b_0}{a_0}\right) \cdot \left(x + \frac{b_1}{a_1}\right) \ldots \cdot \left(x + \frac{b_{n-1}}{a_{n-1}}\right)$$

concluderen dat $f(x)$ in $\mathcal{K}(\lambda)$ op te delen is in **monische** lineaire veeltermen over $\mathcal{K}(\lambda)$. Deze monische veeltermen geven we aan met $\phi(x, \lambda_\nu) = \left(x + \frac{b_\nu}{a_\nu}\right)$. Met $-\omega_\nu = \frac{b_\nu}{a_\nu}$ krijgen we

$$\phi(x,\lambda) = x - \omega_0, \qquad \phi(x,\lambda_1) = x - \omega_1, \dots\dots\dots, \quad \phi(x,\lambda_{n-1}) = x - \omega_{n-1}$$

zodat

$$f(x) = \phi(x,\lambda)\cdot\phi(x,\lambda_1)\cdot\ldots\cdot\phi(x,\lambda_{n-1}) = (x-\omega_0)\cdot(x-\omega_1)\cdot\ldots\cdot(x-\omega_{n-1}).$$

Duidelijk is dat de alle ω_ν waarden nulwaarden zijn van $f(x) = 0$. Aangezien $f(x) = 0$ van graad n is en het aantal ω_ν waarden ook n is, **vormen alle $\boldsymbol{\omega_\nu}$ alle nulwaarden van $\boldsymbol{f(x) = 0}$.**
Aangezien λ_ν een nulwaarde is van de over $\mathcal{K}$ irreducibele n^egraads vergelijking $g(x) = 0$ kan volgens stelling 6.1 iedere waarde uit $\mathcal{K}(\lambda)$ als een polynoom uit $\mathcal{K}[\lambda]$ van graad $n-1$ worden weergegeven. De ω_ν zijn uit $\mathcal{K}(\lambda)$, dus kunnen als polynomen van graad $n-1$ uit $\mathcal{K}[\lambda]$ worden weergegeven.

We beschouwen voor de goede orde nog eens de vergelijking $g(x) = x^n - K = 0$, want daar kwam $\lambda = \sqrt[n]{K}$ uit voort. We nemen aan dat in het algemeen $K = |K|\cdot e^{\mathrm{i}\cdot\arg(K)}$. **Als** $\arg(K) = k\cdot 2\pi$, met k een gehele waarde, **dan** is K en dus $\lambda = \sqrt[n]{K}$ reëel. $\arg(K)$ hoeft evenwel niet een veelvoud van 2π te zijn. We lossen $x^n - K = 0$ op. We krijgen $x^n = K = |K|\cdot e^{\mathrm{i}\cdot\arg(K)} = |K|\cdot e^{\mathrm{i}\cdot(\arg(K)+k\cdot 2\pi)}$, met k geheel. Zodat $x = \left(|K|\cdot e^{\mathrm{i}\cdot(\arg(K)+k\cdot 2\pi)}\right)^{\frac{1}{n}} = \sqrt[n]{|K|}\cdot e^{\mathrm{i}\cdot\frac{\arg(K)}{\mathrm{n}}+i\cdot k\cdot\frac{2\pi}{n}} = \sqrt[n]{|K|}\cdot e^{\mathrm{i}\cdot\frac{\arg(K)}{\mathrm{n}}}\cdot \left(e^{i\cdot\frac{n}{2\pi}}\right)^k = \sqrt[n]{K}\cdot\eta^k = \lambda\cdot\eta^k = \lambda_k$. Oftewel $x = \lambda_0 = \lambda \vee x = \lambda_1 \vee \ldots \vee x = \lambda_{n-1}$.
Aangezien η net als λ uit $\mathcal{K}$ is, zijn alle nulwaarden van $g(x) = 0$, de $\lambda_\nu = \lambda\cdot\eta^\nu$, ook uit $\mathcal{K}$

Er zijn dus waarden K_σ uit $\mathcal{K}$ te vinden zodat voor $\lambda = \lambda_0$ uit $\mathcal{K}(\lambda)$ we ω_0 kunnen weergeven als

$$\omega_0 = K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1}$$

Nu worden de $\psi(x,\lambda_\nu)$ uit $\psi(x,\lambda)$ verkregen door λ te vervangen voor λ_ν. Maar dan worden ook de a_ν en b_ν uit a_0 en b_0 worden verkregen door λ te vervangen voor λ_ν. Bijgevolg worden ook alle $\omega_\nu = -\frac{b_\nu}{a_\nu}$ verkregen uit alle $\omega_0 = -\frac{b_0}{a_0}$ door λ te vervangen voor λ_ν. Dit heeft tot gevolg dat

$$\omega_0 = K_0 + K_1\lambda + K_2\lambda^2 + \cdots + K_{n-1}\lambda^{n-1}$$

$$\omega_1 = K_0 + K_1\lambda_1 + K_2{\lambda_1}^2 + \cdots + K_{n-1}{\lambda_1}^{n-1}$$

$$\omega_2 = K_0 + K_1\lambda_2 + K_2{\lambda_2}^2 + \cdots + K_{n-1}{\lambda_2}^{n-1}$$

$$\vdots$$

$$\vdots$$

$$\omega_{n-1} = K_0 + K_1\lambda_{n-1} + K_2{\lambda_{n-1}}^2 + \cdots + K_{n-1}{\lambda_{n-1}}^{n-1}$$

Waar uiteraard alle K_σ, zoals hierboven aangegeven, uit $\mathcal{K}$ zijn en alle λ_ν uit $\mathcal{K}(\lambda)$.

Een aantal belangrijke kenmerken over de ω_ν zijn.

Als $\boldsymbol{\mu \neq \nu}$ dan ook $\boldsymbol{\omega_\mu \neq \omega_\nu}$; alle $\boldsymbol{\omega_\nu}$ verschillen van elkaar.
Uit Lemma 7.1 en 7.2 concludeerden we dat $\psi(x,\lambda_\mu)$ en $\psi(x,\lambda_\nu)$ elkaar niet kunnen delen over $\mathcal{K}(\lambda)$, met vanzelfsprekenderwijs $\mu \neq \nu$. Voor iedere constante, dus ook voor de constante $\frac{a_\mu}{a_\nu}$, moet $\psi(x,\lambda_\mu) \neq \frac{a_\mu}{a_\nu}\cdot\psi(x,\lambda_\nu)$ kloppen. Waaruit volgt $\frac{1}{a_\mu}\cdot\psi(x,\lambda_\mu) \neq \frac{1}{a_\nu}\cdot\psi(x,\lambda_\nu)$ oftewel $\phi(x,\lambda_\mu) \neq \phi(x,\lambda_\nu)$, dus $x - \omega_\mu \neq x - \omega_\nu$, zodat $\omega_\mu \neq \omega_\nu$. Alle nulwaarde van de vergelijking $f(x) = 0$ zijn dus enkelvoudig.

$\omega_{k\cdot n+\nu} = \omega_\nu$, met k geheel.

Dit volgt meteen uit $\lambda_{k\cdot n+\nu} = \lambda \cdot \eta^{k\cdot n+\nu} = \lambda \cdot e^{i\cdot\frac{2\pi(k\cdot n+\nu)}{n}} = \lambda \cdot e^{i\cdot\frac{k\cdot 2\pi n+2\pi\nu}{n}} = \lambda \cdot e^{i\cdot\frac{2\pi\nu}{n}+k\cdot 2\pi} = \lambda \cdot e^{i\cdot\frac{2\pi\nu}{n}} = \lambda_\nu$.

Of nu een willekeurige ω_ν reëel of zuiver complex (niet te verwarren met zuiver imaginair) is, hangt dus af van het al dan niet zuiver complex zijn van de waarden van het grondtal K uit $\lambda = \sqrt[n]{K}$ en het al dan niet zuiver complex zijn van de coëfficiënten K_σ. Aangezien allemaal complexe waarden worden vermenigvuldigd en opgeteld om de ω_ν te bepalen is het onmogelijk om zomaar vast te stellen of een complexe ω_ν reëel of zuiver complex is.

We hebben als uitgangspunt genomen dat de vergelijking $f(x) = 0$ van oneven priemgraad n is met rationale coëfficiënten. Omdat ω_ν een nulwaarde is van de vergelijking $f(x) = 0$ met rationale coëfficiënten is de complex geconjugeerde $\overline{\omega_\nu}$, ook een nulwaarde van $f(x) = 0$. Omdat $f(x) = 0$ een oneven graad heeft en altijd nul of een even aantal complexe nulwaarden heeft, kan het niet anders dan dat $f(x) = 0$ minstens één reële nulwaarde heeft. Laat $\boldsymbol{\omega_R}$ een **reële nulwaarde** van $f(x) = 0$ zijn, dus

$$\omega_R = K_0 + K_1\lambda_R + K_2{\lambda_R}^2 + \cdots + K_\sigma{\lambda_R}^\sigma + \cdots + K_{n-1}{\lambda_R}^{n-1} =$$

$$= K_0 + \cdots + K_\sigma \cdot \eta^{R\sigma} \cdot \lambda^\sigma + \cdots + K_{n-1} \cdot \eta^{R(n-1)} \cdot \lambda^{n-1}$$

is reëel.

We onderscheiden nu twee gevallen

I. Het grondtal K van de wortelvorm $\lambda = \sqrt[n]{K}$ is reëel;
II. Het grondtal K van deze wortelvorm is zuiver complex.

Geval I. $\lambda = \sqrt[n]{K}$ is nu ook reëel. De complexe geconjugeerde van ω_R is nu

$$\overline{\omega_R} = \overline{K_0 + \cdots + K_\sigma{\lambda_R}^\sigma + \cdots + K_{n-1}{\lambda_R}^{n-1}}$$

$$= \overline{K_0} + \cdots + \overline{K_\sigma} \cdot \overline{\lambda_R}^\sigma + \cdots + \overline{K_{n-1}} \cdot \overline{\lambda_R}^{n-1} =$$

$$= \overline{K_0} + \cdots + \overline{K_\sigma} \cdot \overline{\lambda \cdot \eta^R}^\sigma + \cdots + \overline{K_{n-1}} \cdot \overline{\lambda \cdot \eta^R}^{n-1} =$$

$$= \overline{K_0} + \cdots + \overline{K_\sigma \cdot \eta^{R\sigma}} \cdot \lambda^\sigma + \cdots + \overline{K_{n-1} \cdot \eta^{R(n-1)}} \cdot \lambda^{n-1}$$

Waarbij de $\overline{K_\sigma \cdot \eta^{R\sigma}}$ uit $\mathcal{K}$ zijn, want $K_\sigma \cdot \eta^{R\sigma}$ zijn ook uit $\mathcal{K}$.

Aangezien ω_R reëel wordt verondersteld krijgen we met $\overline{\omega_R} = \omega_R$,

$$\overline{\omega_R} - \omega_R = 0$$

Oftewel

$$(\overline{K_0} - K_0) + \cdots + \left(\overline{K_\sigma \cdot \eta^{R\sigma}} - K_\sigma \cdot \eta^{R\sigma}\right) \cdot \lambda^\sigma + \cdots + \left(\overline{K_{n-1} \cdot \eta^{R(n-1)}} - K_{n-1} \cdot \eta^{R(n-1)}\right) \cdot \lambda^{n-1} = 0$$

Nu heeft de irreducibele vergelijking $g(x) = x^n - K = 0$ (Stelling 5.4 Lemma van Abel; n is priem en K is geen n^e macht) de nulwaarde λ als oplossing, net als de vergelijking

$$F(x) = (\overline{K_0} - K_0) + \cdots + \left(\overline{K_\sigma \eta^{R\sigma}} - K_\sigma \eta^{R\sigma}\right) \cdot x^\sigma + \cdots + \left(\overline{K_{n-1}\eta^{R(n-1)}} - K_{n-1}\eta^{R(n-1)}\right) \cdot x^{n-1} = 0$$

die één graad lager is dan de irreducibele vergelijking $g(x) = 0$. De coëfficiënten van beide vergelijkingen zijn uit $\mathcal{K}$. Op basis van Gevolg 5.1 van Stelling 5.7 moeten we nu concluderen dat de coëfficiënten van $F(x)$ identiek nul zijn. Dus $\left(\overline{K_\sigma \eta^{R\sigma}} - K_\sigma \eta^{R\sigma}\right) = 0$, zodat $\overline{K_\sigma \eta^{R\sigma}} = K_\sigma \eta^{R\sigma}$, voor $0 \leq \sigma \leq n-1$ Maar dan moeten **alle $\boldsymbol{K_\sigma \eta^{R\sigma}}$ reëel** zijn, want een complexe waarde is reëel als deze gelijk is aan zijn complexe geconjugeerde.

Verder hebben we

$$\omega_{\nu-R} = K_0 + \cdots + K_\sigma {\lambda_{\nu-R}}^\sigma + \cdots + K_{n-1} {\lambda_{\nu-R}}^{n-1}$$

en

$$\omega_{R-\nu} = \omega_{n+R-\nu} = \omega_{n-(\nu-R)} = K_0 + \cdots + K_\sigma {\lambda_{n-(\nu-R)}}^\sigma + \cdots + K_{n-1} {\lambda_{n-(\nu-R)}}^{n-1} =$$

$$= K_0 + \cdots + K_\sigma {\lambda_{n-(\nu-R)}}^\sigma + \cdots + K_{n-1} {\lambda_{n-(\boldsymbol{\nu-R})}}^{n-1}$$

Omdat $\lambda_{n-\boldsymbol{\rho}} = \lambda \cdot \eta^{n-\rho} = \lambda \cdot e^{i\cdot\frac{2\pi}{n}\cdot(n-\rho)} = \lambda \cdot e^{i\cdot\left(\frac{2\pi}{n}-\rho+2\pi\right)} = \lambda \cdot e^{i\cdot\frac{2\pi}{n}-\rho} = \lambda \cdot \eta^{-\rho} = \lambda_{-\boldsymbol{\rho}}$ volgt

$$\omega_{R-\nu} = \cdots + K_\sigma {\lambda_{-(\nu-R)}}^\sigma + \cdots = \cdots + K_\sigma {\lambda_{-\nu+R}}^\sigma + \cdots =$$

$$= \cdots + K_\sigma (\lambda \cdot \eta^{-\nu+R})^\sigma + \cdots =$$

$$= \cdots + K_\sigma \eta^{R\sigma} \cdot (\lambda\eta^{-\nu})^\sigma + \cdots = \cdots + K_\sigma \eta^{R\sigma} \cdot (\lambda_{-\nu})^\sigma + \cdots$$

Merk op dat wegens $\overline{\lambda_\rho} = \lambda \cdot \overline{\eta^\rho} = \lambda \cdot \overline{e^{i\cdot\frac{2\pi}{n}\cdot\rho}} = \lambda \cdot e^{i\cdot\frac{2\pi}{n}-\rho} = \lambda_{-\rho}$

$$\omega_{R-\nu} = \cdots + K_\sigma \eta^{R\sigma} \cdot \left(\overline{\lambda_\nu}\right)^\sigma + \cdots = \cdots + \overline{K_\sigma \eta^{R\sigma} \cdot \lambda_\nu^\sigma} + \cdots =$$

$$= \cdots + \overline{K_\sigma \eta^{R\sigma} \cdot (\lambda \cdot \eta^\nu)^\sigma} + \cdots = \cdots + \overline{K_\sigma \cdot \lambda^\sigma \cdot \eta^{(R+\nu)\sigma}} + \cdots =$$

$$= \cdots + \overline{K_\sigma \cdot {\lambda_{R+\nu}}^\sigma} + \cdots$$

Dus

$$\omega_{R-\nu} = \overline{K_0 + \cdots + K_\sigma {\lambda_{R+\nu}}^\sigma + \cdots + K_{n-1} {\lambda_{R+\nu}}^{n-1}} = \overline{\omega_{R+\nu}}$$

Voor $\nu \neq 0$ is $\overline{\omega_{R+\nu}} = \omega_{R-\nu} \neq \omega_{R+\nu}$, want alle $\omega_0, \omega_1, \ldots, \omega_{n-1}$ waren verschillend. Voor $\nu = 0$ hadden we al $\overline{\omega_R} = \omega_R$. Dus het even aantal **nulwaarden anders $\boldsymbol{\omega_R}$** zijn allemaal ongelijk aan hun complexe geconjugeerde en **zijn** daarmee **zuiver complex**!

Daarmee hebben we als resultaat voor *Geval I*.

*De vergelijking $f(x) = 0$ met oneven priemgraad n uit $\mathbb{Q}[x]$, die irreducibel is in een lichaamsuitbreiding $\mathcal{K}$ van $\mathbb{Q}$ (middels wortelvormen en de hiervan complexe geconjugeerde wortelvormen), maar reducibel wordt in de lichaamsuitbreiding $\mathcal{K}(\lambda) \equiv \mathcal{K}\left(\sqrt[n]{K}\right)$, met K uit $\mathcal{K}$, bezit één reële nulwaarde en $n-1$ zuiver complexe nulwaarden, **als** in de vergelijking $g(x) = x^n - K$ de waarde K reëel is.*

Geval II. Nu is K zuiver complex. Daarom voegen we zoals voorgeschreven naast de wortelvorm $\lambda = \sqrt[n]{K}$, die $f(x)$ reducibel maakt, ook de complexe geconjugeerd wortelvorm $\bar{\lambda} = \sqrt[n]{\overline{K}}$ toe, zodat de reële waarde $\Lambda = \sqrt[n]{K \cdot \overline{K}}$ ook voorkomt in $\mathcal{K}(\lambda, \bar{\lambda}) = \mathcal{K}(\lambda)$.

Als de toevoeging van de reële waarde $\Lambda = \sqrt[n]{K \cdot \overline{K}}$ alleen voldoende zou zijn om $f(x)$ reducibel te maken (**$K \cdot \overline{K}$ mag dan zeker geen n^e macht zijn van een waarde uit $\mathcal{K}$**, want dan voegen we aan $\mathcal{K}$ een $\mathcal{K}$ waarde toe, waar $f(x)$ nooit reducibel door kan worden!) , krijgen we weer de situatie zoals in *Geval* I. Nu is Λ de oplossing van de **irreducibele vergelijking $h(x) = x^n - K \cdot \overline{K} = 0$**, nemen we Λ in plaats van λ en $h(x)$ in plaats van $g(x)$, zodat we uiteindelijk hetzelfde schuingedrukte resultaat krijgen zoals in *Geval* I.

We nemen derhalve aan dat $f(x)$ nog steeds irreducibel is in $\mathcal{K}(\Lambda)$, maar wel reducibel wordt in $\mathcal{K}(\lambda)$. Merk op dat $\lambda_\nu = \lambda \cdot \eta^\nu$, $\overline{\lambda_\nu} = \bar{\lambda} \cdot \overline{\eta^\nu}$ ook uit $\mathcal{K}(\lambda)$ zijn

Uit

$$\omega_R = K_0 + K_1\lambda_R + K_2{\lambda_R}^2 + \cdots + K_{n-1}{\lambda_R}^{n-1}$$

volgt dat

$$\overline{\omega_R} = \overline{K_0} + \overline{K_1} \cdot \overline{\lambda_R} + \overline{K_2} \cdot \overline{\lambda_R}^2 + \cdots + \overline{K_{n-1}} \cdot \overline{\lambda_R}^{n-1} =$$

$$= \overline{K_0} + \overline{K_1} \cdot \left(\frac{\Lambda}{\lambda_R}\right) + \overline{K_2} \cdot \left(\frac{\Lambda}{\lambda_R}\right)^2 + \cdots + \overline{K_{n-1}} \cdot \left(\frac{\Lambda}{\lambda_R}\right)^{n-1}$$

Omdat ω_R nog steeds reëel is volgt $\overline{\omega_R} = \omega_R$ zodat

$$K_0 + K_1\lambda_R + K_2{\lambda_R}^2 + \cdots + K_{n-1}{\lambda_R}^{n-1} = \overline{K_0} + \overline{K_1} \cdot \left(\frac{\Lambda}{\lambda_R}\right) + \overline{K_2} \cdot \left(\frac{\Lambda}{\lambda_R}\right)^2 + \cdots + \overline{K_{n-1}} \cdot \left(\frac{\Lambda}{\lambda_R}\right)^{n-1}$$

Waaruit volgt

$$K_0{\lambda_R}^{n-1} + K_1{\lambda_R}^{n} + K_2{\lambda_R}^{n+1} + \cdots + K_{n-1}{\lambda_R}^{2n-2} = \overline{K_0} \cdot {\lambda_R}^{n-1} + \overline{K_1} \cdot \Lambda \cdot {\lambda_R}^{n-2} + \overline{K_2} \cdot \Lambda^2 \cdot {\lambda_R}^{n-3} + \cdots + \overline{K_{n-1}} \cdot \Lambda^{n-1}$$

en

$$K_{n-1}{\lambda_R}^{2n-2} + \cdots + K_1{\lambda_R}^{n} + (K_0 - \overline{K_0}){\lambda_R}^{n-1} - \overline{K_1} \cdot \Lambda \cdot {\lambda_R}^{n-2} - \cdots - \overline{K_{n-1}} \cdot \Lambda^{n-1} = 0$$

Met uitzondering van λ_R zijn alle waarden in deze vergelijking uit $\mathcal{K}(\Lambda)$. De vergelijking zelf is uit $\mathcal{K}[\Lambda]$. Aangezien de nulwaarde λ_R van de over $\mathcal{K}(\Lambda)$ irreducibele vergelijking $g(x) = x^n - K = 0$ (n is nog steeds priem en K is geen n^e macht) ook een nulwaarde is van de vergelijking $F(x) = K_{n-1}x^{2n-2} + \cdots + K_1x^n + (K_0 - \overline{K_0})x^{n-1} - \overline{K_1} \cdot \Lambda \cdot\ x^{n-2} - \cdots - \overline{K_{n-1}} \cdot \Lambda^{n-1} = 0$ met coëfficiënten uit $\mathcal{K}(\Lambda)$, kunnen we op basis van Stelling 5.7 (Abels fundamentele theorema over vergelijkingen van de irreducibele veeltermen) concluderen dat alle nulwaarden van $g(x) = 0$ ook nulwaarden zijn van $F(x)$. Dus volgt met $\nu \neq R$ dat

$$K_{n-1}{\lambda_\nu}^{2n-2} + \cdots + K_1{\lambda_\nu}^{n} + (K_0 - \overline{K_0}){\lambda_\nu}^{n-1} - \overline{K_1} \cdot \Lambda \cdot {\lambda_\nu}^{n-2} - \cdots - \overline{K_{n-1}} \cdot \Lambda^{n-1} = 0$$

Terug redenerend komen we zo uiteindelijk tot

$$\overline{\omega_\nu} = \omega_\nu$$

Dus alle ω_ν zijn nu reëel. We komen zo voor *Geval* II tot het resultaat.

De vergelijking $f(x) = 0$ *met oneven priemgraad* n *uit* $\mathbb{Q}[x]$*, die irreducibel is in een lichaamsuitbreiding* $\mathcal{K}$ *van* $\mathbb{Q}$ *(middels wortelvormen en de hiervan complexe geconjugeerde wortelvormen), maar reducibel wordt in de lichaamsuitbreiding* $\mathcal{K}(\lambda) \equiv \mathcal{K}\left(\sqrt[n]{K}\right)$ *en irreducibel is in* $\mathcal{K}(\Lambda) \equiv \mathcal{K}\left(\lambda \cdot \bar{\lambda}\right) \equiv \mathcal{K}\left(\sqrt[n]{K \cdot \bar{K}}\right)$ *met* K *uit* $\mathcal{K}$*, bezit alleen reële nulwaarden,* ***als*** *in de vergelijking* $g(x) = x^n - K$ *de waarde* K *zuiver complex is.*

De combinatie van de resultaten voor *Geval* I *en Geval* II leidt tot …

Stelling 7.1 het theorema van Kronecker
Een algebraïsch oplosbare vergelijking van oneven priemgraad die irreducibel is over de rationale getallen bezit precies één reële nulwaarde of alleen maar reële nulwaarden.

Bewijs
Hierboven zojuist bewezen.

Einde bewijs

Na al dit voorwerk over irreducibele veeltermen, lichaamsuitbreidingen, coëfficiënten die zelf weer veeltermen van nulwaarden van andere irreducibele veeltermen zijn, terwijl deze veeltermen van nulwaarden zelf weer coëfficiënten hebben van een onderlichaam van het lichaam waar deze nulwaarden zelf uit worden gehaald, zijn we dan eindelijk toe aan het bewijzen van …

Stelling 7.2 Abels theorema (De Stelling van Abel-Ruffini)
Voor de oplossing van een vijfdegraads vergelijking met rationale coëfficiënten bestaat in het algemeen geen formule uitgedrukt in wortelvormen, rationale getallen en de coëfficiënten van de termen in de vergelijking.

Bewijs
Beschouw de onderstaande vergelijking van priemgraad vijf, met gehele coëfficiënten.

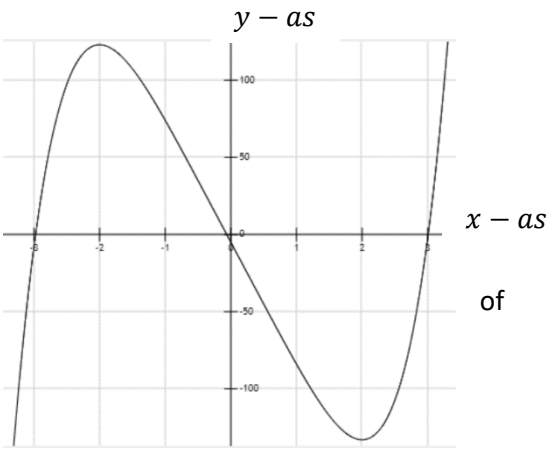
$$f(x) = x^5 - 80x - 5 = 0$$

Omdat alle coëfficiënten geheel zijn en alle coëfficiënten, behalve de leidende coëfficiënt, van de monische veelterm $f(x)$ deelbaar zijn door het priemgetal 5, maar de constante veelterm niet deelbaar is door 5^2, is volgens **Stelling 5.6 (Theorema van Schoenemann),** de vergelijking $f(x) = 0$ irreducibel over de rationale getallen $\mathbb{Q}$.

Volgens de hoofdstelling van de algebra heeft vergelijking $f(x) = 0$ vijf nulwaarden, want het betreft een vijfdegraads vergelijking. Omdat de coëfficiënten van $f(x) = 0$ geheel en dus zeker reëel zijn, is de complexe geconjugeerde van iedere complexe nulwaarde ook altijd een nulwaarde.

We berekenen de coördinaten van de toppen van $f(x)$. $f'(x) = 5x^4 - 80 = 0$ geeft $x = -2 \ \vee \ x = 2$. Met $f(-2) = 123$ en $f(2) = -133$. Dit suggereert de onderstaande grafiek

Uit de grafiek blijkt dat $f(x) = 0$
drie reële nulwaarden heeft.
Maar dan heeft onze vergelijking twee zuiver complexe nulwaarden die elkaars complexe geconjugeerde zijn.



Volgens Stelling 7.1 **het theorema van Kronecker** is een vergelijking zoals de onze alleen maar algebraïsch oplosbaar als deze één reële nulwaarde alleen maar reële nulwaarden heeft.
De logische omkering is dat een niet algebraïsch oplosbare vergelijking meer dan één, maar niet alleen maar reële nulwaarden heeft. Dat laatste is het geval ten aanzien van onze vergelijking; de vijfdegraads vergelijking $f(x) = x^5 - 80x - 5 = 0$ is daarmee algebraïsch niet oplosbaar, d.w.z. er is geen oplossing en dus ook geen formule voor de betreffende nulwaarden uitgedrukt in wortelvormen, rationale getallen en de coëfficiënten van de termen in de vergelijking.

Hieruit volgt: *voor de oplossing van een vijfdegraads vergelijking met rationale coëfficiënten bestaat in het algemeen geen formule uitgedrukt in wortelvormen, rationale getallen en de coëfficiënten van de termen in de vergelijking*.

Einde bewijs

Gemakkelijk valt te bedenken dat voor vergelijkingen van veeltermen van graad vijf en hoger met rationale coëfficiënten in het algemeen niet algebraïsche oplosbaar zijn. Neem bijvoorbeeld $x^n(x^5 - 80x - 5) = 0$ met uiteraard n een natuurlijk getal. Het rechterlid is het product van machten van monische veeltermen, die volgens stelling 4.5 uniek zijn en daarmee ook de nulwaarden, dus…

Uit de grafiek van een derdegraads veelterm uit $\mathbb{Q}[x]$ blijkt dat deze één gemeenschappelijk punt met de x-as heeft (één reële oplossing en twee zuiver complexe oplossingen) of twee (drie reële waarden, één enkelvoudige en een tweevoudige) of drie gemeenschappelijke punten met de x-as (drie reële nulpunten). Dus een derdegraads vergelijking heeft óf een reële oplossing óf alleen maar reële oplossingen. Merk op dat de graad 3 priem is. Er bestaat dan ook een algemene oplossing van rationale waarden en wortelvormen voor een derdegraads vergelijking (formule van Cardano)

Voor een vierdegraads vergelijking bestaat ook zo'n algemene oplossing. De graad is nu niet priem, dus we kunnen niet het theorema van Kronecker gebruiken om het bestaan hiervan vast te stellen (Lodovico Ferrari).

Oefening
Neem een priemgetal p. Laat vervolgens met behulp van **Stelling 5.3 (Het theorema van Sturm)** zien dat de vijfdegraads vergelijking $x^5 - ax - b = 0$, waarbij a en b positieve gehele getallen zijn en $4^4a^5 > 5^5b^4$, algebraïsch niet oplosbaar is.

Doe hetzelfde nog eens voor $x^7 - ax - b$, maar nu met $6^6a^7 > 7^7b^6$.

Nawoord

Nu we hier een bewijs hebben geleverd van de Stelling van Abel-Ruffini, is een terugblik gewenst. De vraag “Wat is gezien het hier geleverde bewijs eigenlijk de werkelijke aard van wiskunde?”, is niet zomaar triviaal te beantwoorden, als deze al volledig is te beantwoorden. Voor het bewijs is taalgebruik, zo nu en dan vrij subtiel, een eerste vereiste. Bovendien gaat de stelling over de *vorm* waarin een oplossing al dan niet kan worden gegoten. Het zich buigen over “de vorm waarin”, staat verder af van de meer mondaine toepassing van wiskunde, die gaat over getallen en waarden van formules en vergelijkingen die benaderd kunnen worden door getallen, dan de gemiddelde persoon gewend is. Bovendien zijn er nog steeds legio wiskundigen (weliswaar een minderheid, maar bepaald niet een met uitsterven bedreigde populatie) die betwijfelen of wortelvormen die niet zijn te reduceren tot rationale getallen daadwerkelijk goede getallen zijn. Goede getallen in deze zin zijn waarden waarvan ondubbelzinnig is vast te stellen dat hier exact mee kan worden gerekend, zonder benaderingen en zonder dat vooraf middels axioma’s en regeltjes de onzichtbare oneindigheden zich goed gaan gedragen.
Als iets duidelijk wordt gemaakt door dit bewijs is het wel dat door het bedrijven van wiskunde, het bewijzen van stellingen, we onverwachts nieuwe gebieden kunnen betreden. Dit komt evenwel met een prijs; de exactheid, die kenmerkend is voor wiskunde, verliezen we zo in toenemende mate uit het oog. Het beeld van wiskunde als een alles doordringende, maar zeker niet alles omvattende, open wetenschap, lijkt zo gerechtvaardigd. Dat wiskunde een geschikt stuk gereedschap is om in alle delen van een organische werkelijkheid onderzoek te kunnen doen, maakt deze organische werkelijkheid automatisch niet meteen tot een volledig wiskundig begrijpelijk geheel, laat staan dat deze werkelijkheid tot illusie kan worden verklaard en het apparaat waarmee onderzoek wordt gedaan bevordert wordt tot de enige echte werkelijkheid. De idee, dat wiskundige kennis, indien correct bedreven, overgaat in kennis die niet kan worden gemathematiseerd, of ook wel, in het minder wenselijke geval, overgaat in een steeds meer nietszeggende abstracte brei die nietszeggendheid camoufleert, is wat mij betreft ten aanzien van kennisvermeerdering, in het licht van o.a. het bewijs van de stelling van Abel-Ruffini, wel het meest in het oog springende vermoeden dat zich zo aandient.

Bibliografie

Heinrich Dörrie, v. d. (1965). *100 Great Problems of Elementary Mathematics Their history and Solution.* New York: Dover Publications, Inc.

Pesic, P. (2003). *Abel's Proof.* Camebridge, Massachusetts: The MIT Press.

Index