STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
AFDELING ZUIVERE WISKUNDE

Voordracht in de serie
"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof. dr. H.J.A. Duparc

26 oktober 1966

ZW 1966-010

Ontbinding in factoren

Nauwelijks is men begonnen met het leren rekenen of een eerste kennismaking met het ontbinden in factoren treedt op. Reeds bij het vak rekenen op de lagere school is dit een geregeld beoefende bezigheid. Behalve dat men deze activiteit leerzaam vindt heeft men haar nodig om op een redelijke manier het rekenen met breuken te bedrijven. Immers bij vereenvoudigen en bij optellen van breuken treden de begrippen GGD en KGV op, welke in dit stadium het beste kunnen worden behandeld via ontbinding in factoren en wel met name ontbinding in priemfactoren. Geleidelijk aan komt men dan tot de twee volgende hoofdeigenschappen:

I. Elk natuurlijk getal is in ondeelbare natuurlijke getallen te ontbinden;

II. De sub I bedoelde ontbinding is ondubbelzinnig.

Hoewel het bewijs van eigenschap I eenvoudiger is dan dat van eigenschap II, is de feitelijke uitvoering van de ontbinding van een natuurlijk getal een voor velen moeizame zaak, voor enkelingen een (soms tijd-

rovend) tijdverdrijf.
Omdat er meer gebieden in de wiskunde zijn, waar het probleem der ontbinding in factoren aan de orde komt en omdat daarin de beweringen I en II niet steeds gelden, is het goed de bewijzen ervan hier te releveren en ze daarbij zo te formuleren dat ze ook op andere zaken dan de natuurlijke getallen kunnen worden toegepast.
Het aanloopje daarbij is dat bij natuurlijke getallen eerst de welbekende delingsalgorithme wordt ingevoerd, d.w.z. de mogelijkheid om bij twee natuurlijke getallen a en b een tweetal niet-negatieve gehele getallen q en r te vinden met

$$a = q\,b + r \quad \text{en} \quad 0 \leq r < b.$$

Dit proces, reeds gegeven door Euclides, voert tot de welbekende algorithme van Euclides ter bepaling van de GGD van twee natuurlijke getallen; uit die alorithme volgt ook nog dat die GGD te schrijven is in de gedaante ua + vb met gehele u en v. Is dit werk eenmaal verricht, dan dient een volgend te passeren punt in deze gedachtenketen zich aan als

Het Lemma: Indien een priemgetal p deelbaar is op een product ab van twee natuurlijke getallen, dan is het deelbaar op tenminste een van beide factoren, anders gezegd:

$$\text{uit } p \mid ab,\ p \nmid a \text{ volgt } p \mid b.$$

Immers, beschouw de GGD d van a en p. Deze is wegens het ondeelbaar zijn van p hetzij gelijk aan p, hetzij gelijk aan 1. Was hij gelijk aan p, dan zou gelden $p \mid a$, hetgeen strijdt met de onderstelling $p \nmid a$.
Derhalve is die GGD gelijk aan 1. Volgens het voorafgaande bestaan er dan gehele u en v met $1 = ua + vp$ dus

$$(1) \qquad b = uab + vpb.$$

Uit $p \mid ab$, $p \mid vpb$ volgt dan $p \mid b$.
Is eenmaal Het Lemma bewezen dan is het nog maar een peuleschilletje om bij twee hypothetische ontbindingen $m = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ van eenzelfde natuurlijke getallen m de identiteit van de verzameling der priemgetallen q en die der priemgetallen p aan te tonen.

Zoals gezegd is deze gedachtengang gegeneraliseerd. Wij noemen de hoofdzaken van dit proces.
Eerst definieert men het begrip hoofdideaalring. Een hoofdideaalring is een integriteitsgebied, waarin elk ideaal een hoofdideaal is.
Vervolgens voert men in het begrip Euclidische ring.
Hieronder wordt een integriteitsgebied verstaan, waarin aan elk element a dat van nul verschilt een niet-negatief geheel getal $g(a)$ is toegevoegd waarvoor de volgende twee eigenschappen gelden:
1e: Als $ab \neq 0$, dan geldt $g(ab) \geq g(a)$;
2e: Voor elke a en b met $a \neq 0$ bestaan elementen q en r met $b = qa + r$, waarbij hetzij $r = 0$, hetzij $g(r) < g(a)$.

Een meer enigszins geschoold mathematicus voelt hoe door invoering van deze twee begrippen het hierboven voor natuurlijke getallen gegeven bewijs tot abstracter verzamelingen is uit te breiden. Daarbij komt men dan tot de volgende stellingen:

Elke Euclidische ring is een hoofdideaalring.

In elke hoofdideaalring bezit elk element een ondubbelzinnige ontbinding in priemelementen.

Wij gaan aan de bewijzen van deze stellingen voorbij en releveren alleen dat men onderweg nog op een eigenaardigheid stuit, die men niet ontmoet bij de natuurlijke getallen. Als voor van nul verschillende elementen p en q geldt $p|q$ en $q|p$, dan behoeven p en q niet gelijk te zijn. (Voorbeeld: $p = 3$, $q = -3$ bij de verzameling der gehele getallen). Men noemt twee dusdanige getallen p en q geassocieerd. Stelt men $q = up$, $p = vq$, dan ziet men $q = uvq$, dus $uv = 1$. Noemt men alle delers van het element 1 eenheden, dan ziet men dat het quotiënt van twee geassocieerde elementen een eenheid is. Wil men nu grondeigenschap II redden, dan moet men ontbinden waarbij geassocieerde elementen optreden identificeren. (Voorbeeld: bij de gehele getallen: $15 = 3 \times 5 = (-3) \times (-5)$; opmerking: bij de gehele getallen neme men $g(a) = |a|$).

Voorbeelden van Euclidische ringen zijn er diverse. Wij noemden reeds de verzameling der gehele getallen.
Verder geldt: De ring $K[x]$ der veeltermen met coëfficiënten, die tot een lichaam K behoren, is Euclidisch. Hierbij neme men voor een veelterm $f = f(x)$ als $g(f)$ eenvoudig de graad van $f(x)$. Wie zich de moeite neemt het bewijs na te lopen, bespeurt reeds direct dat de delingsalgorithme de noodzaak van deling der coëfficiënten met zich meebrengt; vandaar dat wij eisten dat die tot een lichaam K behoren. Hierbij zij nog opgemerkt dat alle elementen k van K eenheden zijn en dat f en kf dus geassocieerd zijn.
Belangrijke toepassingen zijn hier de volgende gevallen:
1e: K is de verzameling der rationale getallen;
2e: K is de verzameling der reële getallen;
3e: K is de verzameling der rationale complexe getallen;
4e: K is de verzameling van alle complexe getallen;
5e: K is de verzameling der restklassen modulo p van de gehele getallen, waarbij p priem is.
Dat in het vijfde geval het getal p niet samengesteld mag zijn toont het voorbeeld

$$(x + 1)(x - 1) \equiv (x + 3)(x - 3) \pmod 8$$

Trouwens, de restklassen modulo een samengestel getal vormen geen lichaam.
Weinig is nog gezegd over de in het begin genoemde eigenschap I, de uitvoerbaarheid der ontbinding. In de gevallen 1e t/m 4e staat de hoofdstelling der algebra hiervoor borg en in geval 5e een beschouwing die zegt dat bij elke te ontbinden veelterm het aantal te onderzoeken ongelijke delers principieel eindig is.
Waar de hoofdstelling der algebra slechts de theoretische garantie biedt van ontbindbaarheid, blijven practische hulpeigenschappen gewenst. Enerzijds vindt men die in gevallen als 2e en 4e in de numerieke hoek. (approximatie - methoden, met name van lineaire en quadratische factoren), anderzijds biedt in gevallen als 1e

een stelling van Gauss hulp door het probleem in wezen terug te voeren tot dat van veeltermen met gehele coëfficiënten. Een stelling die in de schoolwiskunde nuttig was (en elders nuttig blijft) is de (welbekende) factorstelling: Als a een nulpunt is van een veelterm f(x), dan is f(x) te schrijven in de gedaante (x - a) g(x).

Bij de gevallen 1e en 3e kan men voor lineaire factoren x - a van een veelterm f(x) zich beperken tot eindig veel mogelijkheden voor het getal a, omdat a n.l. een deler moet zijn van de bekende term van f(x) of een daarmee in verband staand gemakkelijk aan te geven getal.

Wij gaan aan al deze practische zaken, die ieder wel eens op zijn mathematische levensweg heeft ontmoet, hier voorbij en stippen nog even met een enkel woord aan het gebruik dat men maakt van de uitvoerbaarheid en ondubbelzinnigheid van een ontbinding in priemfactoren.

De structuur van een onbepaalde integraal met als integrand een rationale functie is verzekerd zodra de noemer van die rationale functie is ontbonden (bij bepaalde integralen is men tegenwoordig wel zo wijs om "moeilijk" ontbindbare noemers te laten voor wat ze zijn en ze direct numeriek aan te pakken). Bij het oplossen van een lineaire differentiaal- of differentievergelijking (met constante coëfficiënten) moeten eerst algebraïsche vergelijkingen, worden opgelost (de karakteristieke vergelijking; de indiciaalvergelijking). Prefereert men een oplossingsmethode met behulp van transformaties van Laplace, dan ontmoet men onderweg weer - net als in de integraalrekening - het probleem der breuksplitsing, dus der ontbinding van een veelterm, die ergens in een noemer verschijnt. Ook blijft de hoofdstelling der algebra onontbeerlijk bij het bepalen der eigenwaarden, van een matrix, waarbij voor de berekening ervan diverse numerieke procédé's zijn uitgedacht.

De hierboven met 5e aangeduide rubriek vindt veelvuldig toepassing in de theorie der schuifregisters en coderingsproblemen in moderne informatietechnieken.

Inmiddels is ook de theorie voortgeschreden. Geruime tijd geleden werd opgemerkt dat de getallen van Gauss (dat zijn getallen a + bi met gehele a en b) een Euclidische ring vormen. Stelt men n.l. $g(a + bi) = a^2 + b^2$,

dan geldt voor twee dergelijke getallen α en β allereerst $g(\alpha\beta) = g(\alpha)\,g(\beta) \geq g(\alpha)$, want voor elke $\beta \neq 0$ heeft men $g(\beta) \geq 1$. Verder geldt voor α en β met $\alpha \neq 0$ het bestaan van een quotient $\gamma = \frac{\beta}{\alpha} = c + di$ met reële rationale c en d. Kiest men c_1 resp. d_1 als het meest naburige gehele getal van c resp. d dan geldt $|c_1 - c| \leq \frac{1}{2}$, $|d_1 - d| \leq \frac{1}{2}$, dus voor $\gamma_1 = c_1 + d_1 i$ heeft men $g(\gamma - \gamma_1) \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$.
Derhalve geldt $\beta = \gamma_1\alpha + \rho_1$ met γ_1 geheel en dus ook $\rho_1 = (\gamma - \gamma_1)\alpha$ geheel, waarbij $g(C_1) \leq g(\gamma - \gamma_1)\,g(\alpha) \leq \frac{1}{2}g(\alpha)$, waaruit de Euclidiciteit en dus de ondubbelzinnigheid der ontbinding volgt.
Een toepassing, waarop wij hier niet nader ingaan is de mogelijkheid om elk ondeelbaar viervoud +1 te schrijven in de gedaante $r^2 + s^2$ met gehele r en s. Die schrijfwijze is onder de onderstelling $0 \leq r \leq s$ zelfs ondubbelzinnig.
Ook voor de getallen $a + b\sqrt{2}$ en $a + b\sqrt{-2}$ (a en b geheel) gelden de beweringen I en II over ontbinding. De ondubbelzinnigheid berust andermaal op de Euclidiciteit en deze op haar beurt op een analoge beschouwing als zoeven. Bij $\alpha(\neq 0)$ en β bestaat er een quotiënt $\gamma = \frac{\beta}{\alpha} = c + di$ en daarbij is op dezelfde wijze als zoeven een $\gamma_1 = c_1 + d_1 i$ te bepalen. Voert men nu in $g(a) = |a^2 - 2b^2|$ getallen $a + b\sqrt{2}$ en $g(a) = a^2 + 2b^2$ bij de getallen $a + b\sqrt{-2}$, dan blijft in beide gevallen

$$g(\gamma - \gamma_1) \leq (c - c_1)^2 + 2(d - d_1)^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$$

en de Euclidische algorithme is gered.
Dat dit type bewijs voor grotere $|n|$ bij getallen $a + b\sqrt{n}$ (a en b geheel) spaak loopt, is te voorzien. De gevolgen zijn er dan ook naar. Men heeft $10 = 2 \times 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$ en nadat is vastgesteld dat de vier factoren in deze twee ontbindingen priem zijn en niet paarsgewijze geassocieerd, is de dubbelzinnigheid manifest.
Hiermee is meteen het probleem geboren: Voor welke n is de ontbinding der bedoelde getallen ondubbelzinnig en voor welke niet? Hierbij zij nog opgemerkt dat voor $n \equiv 1 \pmod 4$ om bepaalde redenen niet moet worden gewerkt met getallen $a + b\sqrt{n}$ maar met $a + b(\frac{1}{2} + \frac{1}{2}\sqrt{n})$ (a en b geheel).

Het dient nog te worden opgemerkt dat weliswaar uit Euclidiciteit de ondubbelzinnigheid der ontbinding volgt, maar niet andersom. Er zijn inderdaad waarden van n, waarvoor de betrokken ring niet Euclidisch is, maar waarbij de ontbinding toch ondubbelzinnig is.
Voor negatieve n heeft men kunnen bewijzen dat de enige Euclidische gevallen zijn $n = -1, -2, -3, -7, -11$; daarenboven is de ontbinding ook nog ondubbelzinnig in de gevallen $n = -19, -43, -67, -163$ en eventueel nog voor één verder geval (waarvan is aangetoond dat het voldoet aan $-n > 5.10^9$, zodat men zou kunnen aanvoeren dat het onwaarschijnlijk is dat dit nog optreedt).
Voor positieve n blijkt de Euclidiciteit alleen te gelden bij $n = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 47, 51, 57, 73$; de verdere positieve n, waarbij de ontbinding nog wel ondubbelzinnig is, zonder dat de Euclidische algorithme geldt, zijn lang niet volledig bekend; hiertoe behoort onder meer $n = 23$.
Zonder bewijs vermelden wij nog dat er ingewikkelder voorbeelden van Euclidische ringen zijn, zoals de ring der getallen

$$a + b\sqrt{2} + ci + \tfrac{1}{2}di(1 + \sqrt{2}),\ (a, b, c, d \text{ geheel})$$

Dit is ook het geval met de getallen $a + b\sqrt{2} + c\sqrt{3} + \tfrac{1}{2}d(1 + \sqrt{3})\sqrt{2}$ en met $a + bV + cV^2 + dV^3$ (waarbij $V^5 = 1$, $V \neq 1$) voor gehele a, b, c en d.
En hiermede zijn de algebraïsche Euclidische ringen stellig nog niet uitgeput. Wij willen ze verder laten voor wat ze zijn en nu overgaan tot een ander type ringen van meer analytische origine.

Wij gaan uit van de welbekende formule uit de analyse

$$(au)' = au' + a'u,$$

welke na invoering van de differentiaaloperator D te schrijven is in de gedaante

$$D(au) = a\,Du + a'u.$$

In operatorentaal is dit te formuleren door de gelijkheid

$$d\,a = a\,D + a';$$

immers beide operatoren leveren bij toepassing op een willekeurige

functie u hetzelfde effect. Men kan nu op verschillende manieren D^2a uitrekenen, hetzij via de welbekende regel van Leibniz , hetzij als volgt:

$$D^2a = D(aD + a') = (Da)\,D + Da' = (aD + a')D + a'D + a'' =$$

$$= aD^2 + 2a'D + a'',$$

welke twee methoden overigens in wezen hetzelfde zijn. Voor willekeurige natuurlijke n geldt iets analoogs, n.l.

$$(2) \qquad D^n a = \sum_{k=0}^{n} \binom{n}{k} a^{(k)} D^{n-k}.$$

Het onderscheid van de hier ontmoete polynomen in D is dat de "onbepaalde" D en de elementen a van het grondlichaam in het algemeen niet verwisselbaar zijn: $Da \neq aD$.
Toch is het in zekere zin veilig rekenen met dergelijke polynomen. Gelijkheid definieert men het beste door ze in de standaardgedaante $\sum_{\nu=0}^{n} b_\nu D^\nu$ te brengen en dan gelijkheid der coëfficiënten van iedere macht van D te eisen. Optelling en aftrekking zijn vrijwel triviaal als men ze "gewoon" definieert en de vermenigvuldiging

$$\sum_{\nu=0}^{n} b_\nu D^\nu \,.\, \sum_{\mu=0}^{m} c_\mu D^\mu$$

van twee veeltermen in D resp. van de graad n en m (dus met $b_n \neq 0$, $c_m \neq 0$) voert met behulp van de bovengegeven omwerking van $D^\nu c_\mu$ na termsgewijze uitwerking (dat is au fond toepassing van de distributieve wet) tot een veelterm $\sum_{\kappa=0}^{m+n} p_\kappa D^\kappa$.

Hierin is $p_{m+n} = b_n c_m \neq 0$ aangezien de coëfficiënten tot een integriteitsgebied behoren (immers ze behoren tot het lichaam der willekeurig vaak differentieerbare functies).
Het kost weinig moeite om in te zien dat dergelijke polynomen een ring vormen. Dat die ring in het algemeen niet commutatief is, leert het voorbeeld

$$(D - a)(D - b) = D^2 - (a + b)D + ab - b';$$

want $(D - a)(D - b) = (D - b)(D - a)$ dan en slechts dan als $a' = b'$, een in het algemeen niet geldige bewering.

De vraag rijst of deze polynoomring Euclidisch is. Definieert men de graad van een polynoom op de normale wijze, dan blijkt de graad van een product ook hier gelijk te zijn aan de som der graden der factoren. Dat is al één stap op de goede weg.

Men vraagt nu naar een rechter delingsalgoritme. Zij $\alpha = a(D) = \sum_{\nu=0}^{n} a_\nu D^\nu$; $\beta = b(D) = \sum_{\mu=0}^{m} b_\mu D^\mu$; $n \geq m$.

Er blijken nu inderdaad polynomen $\kappa = q(D)$ en $\rho = r(D)$ te zijn met $\alpha = \kappa\beta + \rho$ en hetzij $\rho = 0$ hetzij $g(\rho) < g(\beta)$. Dat dit zo is blijkt als men op de normale manier aan het delen gaat. Het quotient κ moet natuurlijk beginnen met $q_{n-m}D^{n-m}$ en daarbij neme men q_{n-m} zo dat het verschil

$$a(D) - (q_{n-m}D^{n-m})\, b(D)$$

een lagere graad heeft dan n. Dit komt er op neer dat $a_n - q_{n-m}\, b_m = 0$, dus $q_{n-m} = \frac{a_n}{b_m}$. Wel realisere men zich dat de uitwerking van dit verschil vele malen toepassing van formule (2) vergt. Hoe dan ook, het is van ten hoogste de graad $n - 1$ en als men mits $n - 1 \geq m$ daarna het proces voortzet kan men een tweede term van $q(D)$ op analoge wijze bepalen, enz.

Het proces is zover voort te zetten totdat uiteindelijk een verschil (rest) optreedt van lagere graad dan het getal m of $g(b)$, ofwel totdat een rest nul optreedt. Evenzo bestaat er een linker-deling.

Onze ring is - hoewel niet commutatief - dus wel (rechts en links) Euclidisch. Het wordt nu spannend of hij een ondubbelzinnige ontbinding toelaat. Wij oriënteren ons even aan de analyse en wel via een analogon van de factorstelling. Als u een oplossing is van de lineaire differentiaalvergelijking $f(D)\, u = 0$, dan is de lineaire differentiaaloperator te ontbinden in de vorm $f(D) = g(D)(D - \frac{u'}{u})$.

Inderdaad op grond van onze delingsalgorithme heeft men

$$f(D) = g(D)(D - \frac{u'}{u}) + r,$$

waarbij r of nul is of een veelterm van lagere graad dan de eerste, dus r is een element van het grondlichaam K, d.w.z. een functie (die al of niet de nul-functie kan zijn). Derhalve

$$0 = f(D)u = g(D)(D - \frac{u'}{u})u + ru = g(D)(u' - u') + ru = ru.$$

Uit $u \neq 0$ volgt $r = 0$ en het bewijs is geleverd.

Omgekeerd, als men weet $f(D) = g(D)(D - a)$ en men bepaalt een functie u met $\frac{u'}{u} = a$ dan voldoet u aan de differentiaalvergelijking $f(D)u = 0$, een feit dat zich in één regel laat verifiëren.

Nu is iedereen bekend, dat een differentiaalvergelijking als b.v. $u'' - 5u' + 6u = 0$, in operatorenschrijfwijze $(D^2 - 5D + 6)u = 0$, oneindig veel oplossingen $u = c_1e^{2x} + c_2e^{3x}$ (c_1, c_2 willekeurige constanten) bezit. Dus de drieterm $D^2 - 5D + 6$ is op oneindig veel manieren te ontbinden en wel

$$D^2 - 5D + 6 = (D - b)(D - \frac{2c_1e^{2x} + 3c_2e^{3x}}{c_1e^{2x} + c_2e^{3x}}) .$$

Na enig gecijfer vindt men $b = \frac{3c_1e^{2x} + 2c_2e^{3x}}{c_1e^{2x} + c_2e^{3x}}$ en door variatie der waarden c_1 en c_2 vindt men al die genoemde ontbindingen. Het zeer speciale geval $c_1 = 0$ geeft de ontbinding $(D - 2)(D - 3)$; het even speciale geval $c_2 = 0$ geeft $(D - 3)(D - 2)$, welbekende zaken uit de analyse.

Wij moeten tot formule (1) terugkeren om te doorgronden dat het niet-commutatief zijn van de ring der polynomen f(D) ondanks de Euclidiciteit niet tot een eenduidigheid der ontbindingen voert. Toen immers werd die eenduidigheid uit Het Lemma gehaald en in het bewijs van dat lemma trok men conclusies uit $b = uab + vpb$, waarbij b.v. $ab = wp$. Zolang wij echter de factoren p en b hier dus beide polynomen in D in de tweede term in het rechterlid niet mogen verwisselen, sterker nog, zolang wij niet weten of pb misschien tevens in een gedaante b^*p (met geschikt te kiezen b^*) is te brengen bezit b geen (rechtse) deler p en komt ons lemma op losse schroeven te staan.

Nu omtmoetten wij eerder al het verschijnsel van gelijkwaardige ontbindingen als $15 = 3 \times 5 = (-3) \times (-5)$ en de vraag ligt voor de hand of er

in ons geval iets te redden is. Inderdaad is dit, in het voetspoor van O. Ore (1932) mogelijk, waarbij op een zeer speciale wijze, alle hierboven gevonden oneindig vele ontbindingen van een veelterm als $D^2 - 5D + 6$ als equivalent worden verklaard.

Wij geven enkele hoofdzaken van de theorie van Ore. Daarbij gaan wij nogmaals uit van de delings-algorithme van twee polynomen $\alpha = a(D)$ en $\beta = b(D)$ van het beschouwde type:

$$\begin{aligned}
\alpha &= \kappa_1\beta + \beta_1 \\
\beta &= \kappa_2\beta_1 + \beta_2 \\
\beta_1 &= \kappa_3\beta_2 + \beta_3 \\
&\cdots\cdots \\
\beta_{n-2} &= \kappa_n\beta_{n-1} + \beta_n \\
\beta_{n-1} &= \kappa_{n+1}\beta_n
\end{aligned}$$

Men vormt nu de uitdrukking

$$\phi = \beta_{n-1}\beta_n^{-1} \circ\circ\circ \beta_1\beta_2^{-1} \circ \beta\beta_1^{-1} \circ \alpha\beta^{-1} ,$$

waarvan allereerst (door volledige inductie) is vast te stellen dat ze een veelterm in de grootheden $\kappa_1, \circ\circ\circ, \kappa_{n+1}$ en dus zelf een veelterm is. Het getal $\kappa = \phi\beta = \beta_{n-1}\beta_n^{-1}\circ\circ\circ\beta\beta_1^{-1}\alpha$ is dan zowel een veelvoud van α als van β. Bij voorkeur richt men het zo in dat de eerste coëfficiënt van κ gelijk is aan 1. Het laat zich aantonen dat het het gemeenschappelijke veelvoud van α en β is van de laagste graad, een KGV dus van α en β; men schrijft $\kappa = [\alpha, \beta]$. Nu voeren wij nog de grootheid β^* in, die gedefinieerd wordt door $\beta^* = \kappa\alpha^{-1} = \phi\beta\alpha^{-1} = [\alpha, \beta]\alpha^{-1}$. Deze willen wij opvatten als een nieuw soort geassocieerde van β. Dat β^* niet alleen door β, maar ook door α bepaald wordt, leert ons dat dit nieuwe begrip geassocieerde ingewikkelder is dan het klassieke. Toch voelt de lezer al dat dit wel zal leiden tot de stelling dat twee ontbindingen van onze polynomen dezelfde zijn, afgezien van vervanging van factoren door hun geassocieerden-nieuwe-stijl. Het zou te ver voeren om de theorie en met name het nieuwe begrip geassocieerde hier volledig te behandelen. Wij beperken ons tot een eenvoudig voorbeeld.

Stel dat een quadratisch polynoom π in D twee verschillende ontbindingen in lineaire factoren bezit $\pi = \alpha\beta = \gamma\delta$ (dus $(\alpha, \gamma) = 1$).
Vorm dan de KGV κ van β en δ als boven en daarna de grootheid

$$\delta^* = \kappa\beta^{-1} = [\beta, \delta]\beta^{-1}.$$

Het is gemakkelijk in te zien dat juist doordat de bedoelde ontbindingen verschillend zijn - het bedoelde KGV gelijk is aan π, dus $\delta^* = \pi\beta^{-1} = \alpha$
Bij gevolg zijn de factoren α en δ geassocieerd; enz. De redenering moge triviaal lijken, zij is het echter niet, zoals bij verdere uitwerking blijkt.
Zij $\beta = D - p$; $\delta = D - q$; $p \neq q$ (want $\beta \neq \delta$).
De Euclidische algorithme leert nu

$$D - p = 1.\ (D - q) + q - p, \text{ dus } \kappa_1 = 1;\ \delta_1\beta_1 = q - p;$$

$$D - q = (uD + v)(q - p) \text{ met } \kappa_2 = uD + v;\ \delta_2 = 0.$$

De functies u en v moeten nog worden bepaald uit

$$D - q = u(q - p)D + u(q' - p') + v(q - p),$$

hetgeen na enig cijferwerk voert tot

$$u = \frac{1}{q-p}\ ;\ v = -\frac{q}{q-p} - \frac{q'-p'}{(q-p)^2}\ .$$

Daarna vindt men

$$\delta\delta_1^{-1}\beta = (uD + v)(D - p) = uD^2 + (v - up)D - vp - up$$

en $[\beta, \delta]$ ontstaat hieruit door voorvermenigvuldiging met u^{-1}.
Na invullen van de gevonden waarden voor u en v bewijst men

$$(3) \qquad [D - p, D - q] = D^2 - \left\{q+p + \frac{q'-p'}{(q-p)}\right\}D + qp + \frac{q'p-qp'}{(q-p)}\ .$$

Stel nu eens dat men heeft

$$(D - 2)(D - 3) = (D - r)(D - q).$$

Dan moet dus gelden (op grond van (3) met $p = 3$, $p' = 0$)

$$5 = q+3 + \frac{q'}{q-3};\quad 6 = 3q + \frac{3q'}{q-3}$$

Beide relaties voeren tot

$$q = (2 - q)(q - 3),$$

welke differentiaalvergelijking door scheiding van veranderlijken kan worden opgelost. Er komt successievelijk

$$\int \frac{dq}{(2-q)(q-3)} = \int dx; \quad \ln\left|\frac{q-2}{q-3}\right| = x + C;$$

$$\frac{q-2}{q-3} = C_0\, e^x; \quad q = \frac{2-3C_0\, e^x}{1-C_0\, e^x} = \frac{2e^{2x}-3C_0\, e^{3x}}{e^{2x}-C_0\, e^{3x}},$$

een uitkomst die door de substitutie $C_0 = -\frac{C_2}{C_1}$ in de vroeger gevondene $\frac{2C_1\, e^{2x}+3C_2\, e^{3x}}{C_1\, e^{2x}+C_2\, e^{3x}}$ overgaat.

Wij laten het bij dit voorbeeld en vermelden dat de theorie in vrijwel ongewijzigde vorm is uit te breiden tot gevallen, waar als grondrelatie niet meer geldt $Da = aD + a'$, maar algemener $Da = a_1D + a_0$, waarbij de functies a_1 en a_0 door a worden bepaald. Kiest men $a_1 = a$ en $a_0 = a'$ dan krijgt men het oude geval terug; Kiest men $a_1 = Ea$; $a_0 = \Delta a$ dan krijgt men het geval waarbij D de differentieoperator is.

Zelfs blijken generalisaties mogelijk met een grondrelatie

$Da = a_2D^2 + a_1D$ of algemener $Da = \sum_{\nu=1}^{p} a_\nu D^\nu$, waarbij n vast is en $a_1, \ldots, a_n$ functies zijn die door a bepaald zijn en met a tot een gegeven (grond)lichaam behoren. Doordat hier het begrip graad zijn houvast verliest, verloopt de behandeling moeizamer. Zelfs blijkt dat men in dergelijke gevallen eenheden van een zeer ongewoon type vindt, n.l. eenheden die zelf weer polynoom zijn die dus buiten het grondlichaam vallen. Door een juiste ingreep is zelfs ook nu nog de ontbindingstelling te redden, zoals recente onderzoekingen van Ir. Th.H.M. Smits in Delft hebben geleerd.