STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

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

Prof.dr. F. Loonstra

15 oktober.1958

Het begrip deelbaarheid in de algebra

1958

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

ZW 1958-015

Voordracht in de serie

"Elementaire onderwerpen van hoger standpunt belicht"

door

Prof.Dr F. Loonstra

15 oktober 1958

Het begrip deelbaarheid in de algebra

Stelt R een commutatieve ring met één-element e voor en geldt voor de elementen a,b en c van R

$$a \cdot b = c \ ,$$

dan heet a (en evenzo b) een deler van c en c heet een veelvoud van a (en van b); schrijfwijze $a|c$, $b|c$. Het onderzoek naar de delers van een element c komt dus neer op de bepaling van de mogelijke schrijfwijzen van c als produkt van elementen uit R.

Is a een element van R, waarvoor een a' (in R) bestaat, zodat $a \cdot a'=e$, dan heeft dus a in R een inverse en men noemt a een eenheid van R. De eenheden van R vormen een multiplicatieve groep E (van eenheden). In de ring C (van de gehele getallen) is E van de orde 2; in de ring $C[\sqrt{2}]$ van de getallen $a+b\sqrt{2}$ (a,b geheel) is die groep E oneindig.

Elke deler van een eenheid is een eenheid. Twee elementen a en b van R heten geassocieerd, als er een eenheid ε in E bestaat, zodat $a=b\varepsilon$. In dat geval is a een deler van b, b een deler van a.

Maken we gebruik van het ideaalbegrip, dan geldt: opdat een hoofdideaal (m) in R met R samenvalt, is het nodig en voldoende, dat m een eenheid in R is.

Als in een integriteitsgebied (a)=(b), dan zijn a en b geassocieerd. G.G.D. van 2 elementen a en b in een integriteitsgebied: is d een gemeenschappelijke deler van a en b, zodat elke gem. deler d' van a en b een deler is van d, dan heet d een g.g.d. van a en b; notatie d=(a,b). Twee g.g.d.'s van a en b

zijn dus geassocieerd en omgekeerd is met d ook elke geassocieerde d' een g.g.d. van a en b.
In een integriteitsgebied R heeft het ons in de ring der gehele getallen bekende begrip "onderling ondeelbaar" verschillende generalisaties:

I. a en b hebben <u>geen gemeenschappelijke delers</u>, als ze geen andere gem. delers hebben dan eenheden.

II. b <u>heet priem met</u> a, als uit $a|bx$ volgt: $a|x$.

III. a en b heten <u>onderling ondeelbaar</u> (onderling priem), als in R twee elementen u en v bestaan zodat (de relatie van Bezout) geldt:

$$ua + vb = e.$$

Men kan bewijzen: Uit III volgt II, uit II volgt I.

<u>Stelling 1</u>. Als twee elementen a en b van R een g.g.d. d hebben, dan hebben de elementen $a'=a/d$ en $b'=b/d$ geen gemeenschappelijke delers, d.w.z. a' en b' voldoen aan I.

<u>Stelling 2.</u> Is d een zodanige gem. deler van **a** en b, dat $b'=b/d$ priem is met $a'=a/d$, dan is $d=(a,b)$.

<u>Stelling 3.</u> Als in een integriteitsgebied de eigenschap I gelijkwaardig is met de eigenschap II, dan is nodig en voldoende opdat d een g.g.d. is van a en b, dat $a'=a/d$ en $b'=b/d$ zonder gemeenschappelijke delers zijn.

Een deler van a, die géén eenheid is en evenmin een element, dat geassocieerd is met a, wordt een <u>echte deler</u> van a genoemd.
Met een echte deler d van a correspondeert dus een <u>echte ontbinding</u> $a=d\cdot d'$ van a. Een ontbinding $a=a\cdot\varepsilon$ van a, waarin ε een eenheid is, heet een <u>triviale</u> <u>ontbinding</u> van a. Als $p\neq 0$ is (in een integriteitsgebied R) en p geen echte ontbinding toelaat, dan heet a <u>onontbindbaar</u>. Is p onontbindbaar en bovendien géén eenheid, dan heet p een <u>priemelement</u> of <u>irreducibel</u> element (i).
Een element p van R, dat $\neq 0$ is, geen eenheid is, wordt

<u>priemelement in de stricte zin</u> (ii)

genoemd, als uit $p|ab$ en $p\nmid a$ volgt $p|b$.
Een priemelement in de stricte zin brengt dus een priemideaal voort.

Stelling 4. Elk priemelement in de stricte zin (ii) is priemelement (i).
Stelling 5. In elk integriteitsgebied, waar de eigenschappen I en II equivalent zijn, zijn ook (i) en (ii) equivalent.
Een integriteitsgebied R bezit de eenduidige factorontbinding, als voldaan is aan de beide voorwaarden:
1. Er bestaat voor elk element a($\neq$0 en a geen eenheid) tenminste één schrijfwijze als produkt van priemelementen.

2. De schrijfwijze, zoals bedoeld in 1., is tot op eenheden na eenduidig.

Stelling 6. In een integriteitsgebied met eenduidige factorontbinding is de eigenschap I equivalent met II.

Stelling 7. Is $\mathfrak{J}$ een hoofdideaalring, dan zijn I, II en III equivalent, terwijl in $\mathfrak{J}$ een eventuele ontbinding van de elementen als produkt van priemelementen tot op eenheden na eenduidig is.