STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1959 - 014

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

Prof.Dr. W. Peremans

14 oktober 1959

V E E L T E R M E N

1959

STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM-O.

ZW 1959-014

Voordracht in de serie

"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof.Dr W. Peremans

14 oktober 1959

VEELTERMEN

§1. Inleiding. De in een veelterm $3x^2+5x+7$ optredende letter x kan opgevat worden als een veranderlijke in de zin van het functiebegrip: de veelterm is een functie die gedefinieerd is op een bepaalde verzameling (b.v. de rationale getallen) en voegt aan ieder element van die verzameling een functiewaarde toe, die gevonden wordt door dat element voor x te substitueren. Deze opvatting is strijdig met de geest van de algebra, waar het opereren (optellen, vermenigvuldigen enz.) primair is. Bovendien zou men, als men op deze wijze het optreden van "letters" in de algebra zou willen verklaren, de veelterm ax^2+bx+c als een functie van vier veranderlijken moeten opvatten. Ten slotte is het onaangenaam, dat men a priori zou moeten vastleggen, in welke verzameling de x mag variëren.

Een andere interpretatie is, dat men de x opvat als een onbepaalde, dat is een symbool, waaraan a priori geen enkele betekenis wordt toegekend. Daarnaast zijn er ook symbolen voor de bekende algebraïsche operaties, zoals het plusteken voor de optelling (het symbool voor de vermenigvuldiging is meestal onzichtbaar), en haakjes. Uit deze symbolen kunnen op bepaalde wijze door achter elkaar zetten "welgevormde" symboolrijen worden gemaakt, die veeltermen worden genoemd. Sommige van deze veeltermen noemt men gelijk, of identiek. De regels volgens welke dit spel gespeeld wordt, worden hier niet gepreciseerd. Het is het spel, dat op de middelbare school als het "rekenen met letters" wordt beoefend. De zin van het spel is gelegen in het z.g. substitutieprincipe. Dit bestaat hierin, dat een getal α gekozen wordt, dat voor x "gesubstitueerd"moet worden.

Hierbij moeten de operatiesymbolen door de corresponderende operaties voor getallen worden vervangen. Door de opbouw van de veelterm te volgen, komt men ertoe, aan elke veelterm op deze wijze een getal toe te voegen, dat men aanduidt als de waarde van de veelterm bij de substitutie van α voor x. Bij identieke veeltermen blijkt men dan dezelfde waarde te verkrijgen. De geldigheid van dit laatste is bij deze opbouw geen vanzelfsprekendheid, maar een stelling, die bewezen moet worden. Het spreekt vanzelf, dat hetgeen hier voor veeltermen in één veranderlijke is geschetst, evenzo uitvoerbaar is voor veeltermen in meer veranderlijken.

De abstracte (axiomatische) algebra stelt dit nog in een zuiverder licht. Hetgeen we zo juist hebben geconstrueerd, wordt daar de polynoomring $Z[x]$ in één veranderlijke x over de ring der gehele getallen genoemd. Voor substitutie komen niet alleen in aanmerking "getallen", maar ook elementen van een willekeurige commutatieve ring. Men werkt daar trouwens nog met algemenere polynoomringen $R[x]$, waarbij een vaste commutatieve ring R gegeven is, welker elementen voor de "coëfficiënten" der polynomen mogen worden gebruikt. Het substitutieprincipe wordt nu een homomorfieprincipe: bij ieder element α van R bestaat een homomorfe afbeelding van $R[x]$ in R, waarbij de elementen van R op zichzelf worden afgebeeld en x op α .

De invoering van de polynoomring geschiedt echter gewoonlijk niet op een wijze, die in overeenstemming is met de hierboven geschetste principes, waarbij de onbepaalde en de operatietekens als symbolen zonder betekenis worden ingevoerd. Dit kan echter wel, en wel met het formalisme, dat men in de algebra het invoeren van vrije algebraïsche systemen noemt. Dit beschrijven we nu eerst voor groepen in plaats van voor ringen.

§ 2. Vrije groepen. Gegeven zij een verzameling X van symbolen, die voortbrengenden worden genoemd. Gevraagd wordt een groep V (de vrije groep voortgebracht door X), die de volgende eigenschappen heeft:

1°. X is een deelverzameling van V en V wordt als groep door X voortgebracht (d.w.z. iedere ondergroep van V, die X bevat, valt met V samen);

2^{o}. bij iedere groep G en bij iedere afbeelding van X in G, bestaat een homomorfe afbeelding van V in G, die voor de elementen van X met de gegeven afbeelding samenvalt.

We zullen nu een dergelijke groep V bepalen. We vatten de elementen van X op als "letters" en vormen nu "woorden" door deze letters achter elkaar te schrijven. Dit is het symbolisch weergeven van de vermenigvuldiging in de groep. We willen ook de inversevorming weergeven. In een groep geldt echter $(ab)^{-1}=b^{-1}a^{-1}$. Op grond hiervan is het blijkbaar voldoende de exponent -1 alleen bij de letters te schrijven. We staan dus ook toe, dat in een woord sommige der letters van de exponent -1 zijn voorzien. Als in een woord W ergens aa^{-1} of $a^{-1}a$ optreedt, zullen we het woordt dat uit W ontstaat door deze aa^{-1} of $a^{-1}a$ te schrappen,klaarblijkelijk met W moeten identificeren. We bespreken nu twee methoden om de constructie voort te zetten.

Eerste methode. We nemen als element voor V alleen die woorden, waarop het bovenstaande schrapproces niet meer kan worden toegepast (normaalwoorden). We moeten nu een vermenigvuldiging van twee normaalwoorden W_1 en W_2 definiëren; uiteraard geschiedt dit in eerste instantie door ze achter elkaar te schrijven: W_1W_2. Het resultaat hoeft dan echter geen normaalwoord te zijn; we moeten dus nog eventueel op de grens van W_1 en W_2 een aantal malen schrappen. Na eindig veel schrappingen ontstaat dan een normaalwoord, dat het product van W_1 en W_2 genoemd wordt. Daar het mogelijk is, dat er bij dit schrapproces ten slotte niets meer overblijft, moet ook het "lege woord" als woord worden toegelaten. Dit lege woord is kennelijk het eenheidselement van de groep. Ook het inverse W^{-1} van het woord W is makkelijk te vormen: schrijf de letters van W in omgekeerde volgorde en zet de exponenten -1 precies bij die letters, waarbij ze op de corresponderende plaats in W niet staan. Alleen de associatieve eigenschap $(W_1W_2)W_3 = W_1(W_2W_3)$ moet nog bewezen worden. Als A en B normaalwoorden zijn noemen we het woordenpaar A,B passend, als het woord AB een normaalwoord is. Dat wil zeggen, dat A of B leeg is of dat, als A en B geen van beide leeg zijn, de laatste letter van A en de eerste letter van B niet "invers zijn".

Nu is $\left.\begin{matrix} W_1 = AB \\ W_2 = B^{-1}C \end{matrix}\right\}$ met A,C passend, dus $W_1W_2=AC$. We onderscheiden twee gevallen.

1°. W_3 begint niet met C^{-1}. Dan geldt $C=DE$, $W_3=E^{-1}F$, met D niet leeg en D,F passend. Dan is $(W_1W_2)W_3=ADF$. Verder is $W_2W_3=B^{-1}DF$ en $W_1=AB$, dus $W_1(W_2W_3)=ADF$, omdat A,C en dus A,D passend zijn en D niet leeg is.

2°. $W_3=C^{-1}D$. We onderscheiden weer twee gevallen.

A. A,D zijn passend. Dan is $(W_1W_2)W_3=AD$. Stel nu $B^{-1}=EF$, $D=F^{-1}G$ met E,G passend. Dan is $W_2W_3=EG$ en $W_1=AF^{-1}E^{-1}$. Nu is A,D passend, dus $A,F^{-1}G$ passend, dus AF^{-1}, G passend, dus $W_1(W_2W_3)=AF^{-1}G=AD$.

B. A,D zijn niet passend. Stel $A=EF$, $D=F^{-1}G$ met F niet leeg en E,G passend. Dan is $(W_1W_2)W_3=EG$. Nu is A,B passend, dus EF,B passend, dus F,B passend, dus B^{-1},F^{-1} passend; verder is F^{-1} niet leeg, dus $W_2W_3=B^{-1}F^{-1}G$ en $W_1(W_2W_3)=EG$.

Hiermee is een groep V verkregen, die kennelijk door X wordt voortgebracht. Dat deze groep ook aan de tweede homomorfie-eis voldoet is vrijwel triviaal.

Tweede methode. We werken nu niet met normaalwoorden, maar met alle woorden, waarvan er echter sommige moeten worden geïdentificeerd. Behalve de hierboven besproken schrapping, laten we ook de inverse operatie van toevoeging toe, waarbij in een woord ergens aa^{-1} of $a^{-1}a$ wordt ingelast. Twee woorden A en B heten equivalent als er een eindige rij woorden $W_o,W_1,\ldots,W_n$ bestaat met $W_o=A$ en $W_n=B$ en zodat W_k uit W_{k-1} ontstaat door een toevoeging of schrapping ($k=1,\ldots,n$). Het is duidelijk, dat deze relatie reflexief, symmetrisch en transitief is; de equivalentieklassen behorende bij deze relatie zijn de elementen van V. Vermenigvuldiging geschiedt door uit elke klasse een representant te kiezen en deze representanten achter elkaar te schrijven. Het is makkelijk te bewijzen, dat de verkregen klasse onafhankelijk is van de keuze der representanten. Dat een groep verkregen wordt, is duidelijk (de associatieve eigenschap is nu triviaal!) Ook de homomorfie-eigenschap is eenvoudig te bewijzen, als men eerst aan woorden op voor de hand liggende wijze elementen van G toevoegt en vervolgens aantoont, dat aan equivalente woorden hetzelfde element wordt toegevoegd. Het enige, dat minder triviaal is dan bij de eerste methode, is dat V door X wordt voortgebracht. We moeten daartoe aantonen, dat twee verschillende letters x en y (of eigenlijk de woorden die uit

de ene letter x resp. y bestaan) niet equivalent zijn. Dit volgt echter eenvoudig uit de homomorfie-eigenschap en uit het feit, dat er groepen bestaan die meer dan één element bevatten. Neem een groep G van orde ≥ 2. Voeg aan x en y twee verschillende elementen van G toe en aan andere letters willekeurige elementen van G. Uit de homomorfie-eigenschap volgt dan direct, dat x en y niet equivalent zijn.

De tweede methode leidt sneller tot het doel dan de eerste, maar heeft het nadeel minder expliciet de elementen van V aan te geven. Het voornaamste voordeel van de tweede methode is voor ons het feit, dat ze zich makkelijker tot generalisatie leent.

§3. Vrije algebraïsche systemen. Voor een algebraïsch systeem A zijn gegeven een collectie Ω van operaties, die op de verzameling A werken. Elk van de operaties O is een functie van een eindig aantal veranderlijken $O(x_1,\ldots,x_n)$ gedefinieerd voor iedere groep $x_1,\ldots,x_n$ van elementen van A en met functiewaarden in A. We vergelijken alleen gelijksoortige systemen met elkaar, dat zijn systemen, waarbij er een eenduidig verband bestaat tussen de collecties der operaties, en waarbij de corresponderende operaties van evenveel veranderlijken afhangen. We geven de corresponderende operaties dan ook dezelfde naam. Dit is in overeenstemming met het gebruik in de algebra, dat ons toestaat om, als we bijv. twee ringen beschouwen, in beide een operatie "optelling" aan te treffen, en deze zelfs in beide met het hetzelfde symbool aan te duiden.

Naast de operaties stellen we nu operatiesymbolen, dit zijn functiesymbolen met een even groot aantal lege plaatsen als er veranderlijken in de operatie zijn. Dus in het algemeen iets van de gedaante O(, ,). Hiernaast nemen we een verzameling X van "letters". Deze letters, of termen van de nulde orde, kunnen op de lege plaatsen in de operatiesymbolen worden ingevuld, hetgeen een term van de eerste orde oplevert. Vult men termen van de nulde of de eerste orde in een operatiesymbool in, dan ontstaat een term van de tweede orde enz. Zo krijgt men bij de gebruikelijke schrijfwijze van de optellings- en vermenigvuldigingssymbolen bijv.

$$((x+y)z) + yu,$$

hetgeen een term van de derde orde is.

Schrijft men tussen twee termen een gelijkteken, dan krijgt men een gelijkheid.

Bij iedere afbeelding van X in een algebraïsch systeem A kan een afbeelding der termen in A met inductie naar de orde worden geconstrueerd, waarbij de operatiesymbolen in de termen met de corresponderende operaties in A overeenstemmen. Dit noemt men substitutie.

Een algebraïsche gelijkheidsstructuur verkrijgt men door een aantal gelijkheden als axioma's uit te roepen en die algebraïsche systemen A tot de structuur te rekenen, waarvoor geldt, dat iedere substitutie in A alle axioma's van de structuur in werkelijke gelijkheden tussen elementen van A overvoert.

Het begrip groep is een gelijkheidsstructuur, als men vermenigvuldiging en inversevorming als operaties kiest en als axioma's:

$$x(yz) = (xy)z,$$
$$xx^{-1} = yy^{-1},$$
$$x(xx^{-1}) = x\ .$$

Ook ringen vormen een gelijkheidsstructuur, als men optelling, aftrekking en vermenigvuldiging als operaties kiest.

Bij een gelijkheidsstructuur kan men nu makkelijk een vrij algebraïsch systeem voortgebracht door X maken, door in de verzameling der termen, die termen te identificeren, die bij iedere substitutie in ieder algebraïsch systeem, dat tot de structuur behoort, gelijke elementen oplevert. Men krijgt dan een systeem met operaties, die op de voor de hand liggende wijze worden gedefinieerd. Dit systeem voldoet aan de axioma's en voldoet ook aan de homomorfie-eis (die op analoge wijze als voor groepen te formuleren is). Om aan te tonen, dat geen twee elementen van X worden geïdentificeerd, moeten we de veronderstelling maken, dat de structuur een systeem met minstens twee elementen bevat. Als dat zo is kan hetzelfde bewijs, dat hierboven bij groepen is gebruikt, weer dienst doen.

Dit vrije algebraïsche systeem wordt bij groepen de vrije groep en bij commutatieve ringen, de polynoomring over de gehele getallen. Ook polynoomringen over willekeurige commutatieve ringen kunnen met een kunstgreep hieruit verkregen worden.