STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
AFDELING ZUIVERE WISKUNDE

ZW 1967-001

Voordracht in de serie

"Elementaire onderwerpen vanuit hoger standpunt belicht"

door

Prof.dr. W. Peremans

25 januari 1967

Voortbrengenden en relaties in de groepentheorie.

§1. Inleiding.

Het gebruik van voortbrengenden en relaties is een bekende methode in de groepentheorie. Deze methode zal hier echter worden toegepast in situaties, waarin dit niet gebruikelijk is. Ook zal de methode zelf op een enigszins van de gebruikelijke afwijkende manier worden geïntroduceerd.

In deze inleiding geven we een ruwe schets van hetgeen men gewoonlijk doet.

Uitgangspunt is het begrip "vrije groep". Om deze te vormen gaat men uit van een verzameling S (voortbrengende verzameling).

Men vormt dan "woorden" (eindige rijen), waarvan de "letters" van de gedaante a of a^{-1} zijn met $a \in \mathcal{S}$. Woorden worden met elkaar vermenigvuldigd door ze achter elkaar te schrijven; deze vermenigvuldiging is uiteraard associatief. Woorden als $aa^{-1}bc$ en bc moeten echter hetzelfde groepelement opleveren. Men kan hierin op twee manieren voorzien.

1. Men voert een equivalentierelatie in de verzameling der woorden in. Elementen van de groep zijn dan klassen van woorden; men moet aantonen, dat equivalentie bestand is tegen vermenigvuldiging ("congruentierelatie").
2. Men laat alleen woorden toe, waar nergens aa^{-1} of $a^{-1}a$ in staat (onverkortbare woorden). Elementen van de groep zijn de onverkortbare woorden. Aangezien echter het achter elkaar schrijven van twee onverkortbare woorden geen onverkortbaar woord hoeft op te leveren, moet bij de definitie van product "inkorting" worden toegepast. De associatieve eigenschap van de vermenigvuldiging is nu niet meer triviaal, maar kan bewezen worden.

De overeenstemming in het resultaat van beide methoden bewijst men door aan te tonen, dat iedere klasse in de zin van 1. één en slechts één onverkortbaar woord in de zin van 2. bevat.

Een willekeurige groep H met voortbrengende verzameling $\mathcal{S}$ is homomorf beeld van de vrije groep G met voortbrengende verzameling $\mathcal{S}$. De kern K van deze homomorfe afbeelding levert "relaties", die geldig zijn in H, b.v. $e = a^2 = b^2 = (ab)^2$ enz. (groep van Klein.)

Om, uitgaande van G, de groep H te bepalen, hoeft men echter niet alle relaties op te schrijven. Een voortbrengende verzameling J is voldoende; K is dan de kleinste normale ondergroep van G, die de woorden uit J bevat. De groep, die dan met voortbrengenden en relaties wordt geconstrueerd is de factorgroep G/K; men bedenke, dat elementen van G/K klassen in G zijn.

Het onnatuurlijke van deze methode is, dat men twee maal identificatie door middel van klassenindeling uitvoert. In feite zijn $aa^{-1} = e$ en $a^{-1}a = e$ ook relaties. Dat men deze al a priori invoert is, omdat ook het vrije systeem een groep moet zijn. Laat men deze eis echter varen, dan is de dubbele identificatie onnodig; men gebruikt dan <u>vrije semigroepen</u>.

Equivalentieklassen zijn vaak moeilijk hanteerbaar. Eenvoudiger wordt dit, als men over een overzichtelijk representantensysteem beschikt. Nog beter is het, als men een hanteerbare reductie heeft, die bij een willekeurig woord de ermee equivalente representant (standaardwoord) levert. In dat geval kan men van twee willekeurige woorden ook vaststellen of ze equivalent zijn of niet door te kijken of reductie wel of niet hetzelfde woord oplevert.

§2. Vrije semigroepen; relaties in semigroepen.

Laat $\mathcal{S}$ een verzameling zijn. De vrije semigroep F met voortbrengende verzameling $\mathcal{S}$ heeft als elementen alle niet-lege, eindige rijen van elementen van $\mathcal{S}$ (woorden). De vermenigvuldiging geschiedt door achter elkaar plaatsen.

We kiezen nu relaties $A \equiv B$ in F; dat is een deelverzameling J van de verzameling $F \times F$ der paren (A,B). De kleinste congruentierelatie, die J bevat, is als volgt te krijgen:
$U \sim V$, als er een rij $U_0, U_1, \ldots, U_n$ is met $U_0 = U$, $U_n = V$ en voor $j = 1, \ldots, n$ geldt, dat er X_j, A_j, B_j, Y_j bestaan, zodat $U_{j-1} = X_j A_j Y_j$, $U_j = X_j B_j Y_j$, $(A_j, B_j) \in J$, X_j en Y_j willekeurige woorden, die ook leeg mogen zijn.

De quotiëntsemigroep G van F ten opzichte van deze congruentierelatie heet de semigroep met voortbrengende verzameling $\mathcal{S}$ en verzameling J van relaties.

Op te merken valt, dat het kan gebeuren, dat elementen van $\mathcal{S}$ worden geïdentificeerd. Verder is iedere semigroep (en dus iedere groep) isomorf met een quotiëntsemigroep van een vrije semigroep.

§3. Vrije groepen.

Laat $\mathcal{S}$ een verzameling zijn. Voor iedere $a \in \mathcal{S}$ vormen we a^1 en a^{-1}; verder kiezen we een e. Laat $\mathcal{T}$ de verzameling zijn met elementen e en alle a^1 en a^{-1} voor $a \in \mathcal{S}$. Laat F de vrije semigroep zijn voortgebracht door $\mathcal{T}$. Neem de volgende lijst van relaties:

$$et \equiv t$$
$$te \equiv t$$
$$a^{1}a^{-1} \equiv e$$
$$a^{-1}a^{1} \equiv e$$

voor alle $t \in \mathfrak{T}$ en alle $a \in \mathfrak{F}$. Vorm de quotiëntsemigroep G. Deze is een groep.

Op een woord passen we standaardreductie toe door het van links naar rechts af te tasten tot we één der linkerleden uit bovenstaande lijst van relaties ontmoeten. Als dit geschiedt, vervangen we het linkerlid door het bijbehorende rechterlid; daardoor wordt het woord één letter korter. Dit herhalen we tot het niet meer kan. Zo vinden we bij ieder woord W een ermee equivalent standaardwoord $\mathfrak{S}(W)$. Een standaardwoord is hetzij e hetzij een woord, waarin e niet als letter voorkomt en nergens een opeenvolging van letters van het type $a^{1}a^{-1}$ of $a^{-1}a^{1}$. Het is duidelijk, dat iedere klasse, die een element van G is, minstens één standaardwoord bevat. Men kan bewijzen dat een dergelijke klasse ook hoogstens één standaardwoord bevat. De standaardwoorden vormen dus een representantensysteem. Als men ook het lege woord toelaat, kan men het standaardwoord e door het lege woord vervangen.

§4. Groepuitbreidingen. Traditionele opzet.

Het probleem is om bij gegeven groepen A en Γ alle groepen G te maken, die A als normale ondergroep hebben, zodat G/A isomorf is met Γ.

We geven een ruwe schets van de gebruikelijke constructie. Neem eerst aan, dat G gegeven is; maak een splitsing in (rechter) nevenklassen van A. Een representantensysteem voor deze klassen correspondeert met de elementen van Γ: g_α $(\alpha \in \Gamma)$. Elementen van G zijn eenduidig te schrijven in de vorm ag_α $(a \in A,\ \alpha \in \Gamma)$. Nu ligt $g_\alpha g_\beta$ in de nevenklasse behorend bij $\alpha\beta$. Dus $g_\alpha g_\beta = m(\alpha,\beta)g_{\alpha\beta}$; $m(\alpha,\beta)$ heet een <u>factorensysteem</u> (afbeelding $\Gamma \times \Gamma \to A$). Nu is $ag_\alpha bg_\beta = a(g_\alpha bg_\alpha^{-1})g_\alpha g_\beta$. Omdat A een normale ondergroep is, is $g_\alpha bg_\alpha^{-1} \in A$. Voor vaste α is ${}^\alpha a = g_\alpha a g_\alpha^{-1}$ een <u>automorfie</u> van A; ${}^\alpha a$ is een afbeelding $\Gamma \times A \to A$.

Laat nu omgekeerd een factorensysteem en automorfieën gegeven zijn. We definiëren G als verzameling van paren (a,α) met $a \in A$, $\alpha \in \Gamma$ met als vermenigvuldiging

$$(a,\alpha)(b,\beta) = (a \cdot {}^{\alpha}b \cdot m(\alpha,\beta),\ \alpha\beta).$$

Er moeten nu voorwaarden afgeleid worden, om te bewerkstelligen, dat G een groep is, dat $(a,\alpha) = (a,\varepsilon)(e,\alpha)$, dat A isomorf is met de normale ondergroep der (a,ε) en dat de afbeelding $(a,\alpha) \to \alpha$ een homomorfe afbeelding van G op Γ is. Dit leidt tot de voorwaarden van Schreier.

Wij geven een andere opzet, die als uitgangspunt heeft, dat A en de g_α de groep G voortbrengen.

§5. Groepuitbreidingen. Opzet met voortbrengenden en relaties.

Laat A en Γ groepen zijn; e is het eenheidselement van A, ε het eenheidselement van Γ. We nemen aan, dat A en Γ disjunct zijn. We gaan eerst de eenheidselementen van beide identificeren. Daartoe vormen we $\Gamma_1 = \Gamma \setminus \{\varepsilon\}$ en $\Gamma_2 = \Gamma_1 \cup \{e\}$. We maken Γ_2 op de voor de hand liggende manier tot een met Γ isomorfe groep met e als eenheidselement. Stel verder $\mathfrak{S} = A \cup \Gamma_1$.

Stel verder gegeven:

$m(\alpha,\beta)$, $\Gamma_1 \times \Gamma_1 \to A$, $\alpha \in \Gamma_1$, $\beta \in \Gamma_1$, $m(\alpha,\beta) \in A$,

${}^{\alpha}a$, $\Gamma_1 \times A \to A$, $\alpha \in \Gamma_1$, $a \in A$, ${}^{\alpha}a \in A$.

We vormen de vrije semigroep F met voortbrengende verzameling $\mathfrak{S}$. Met ab zullen we bedoelen het woord met de twee letters a en b, met (ab) het woord met één letter, die het product (in A) is van de elementen a en b van A. Analoog $\alpha\beta$ en $(\alpha\beta)$ in Γ_2.

Neem de volgende lijst van relaties:

$$ab \equiv (ab)$$
$$e\alpha \equiv \alpha$$
$$\alpha a \equiv {}^{\alpha}a \cdot \alpha$$
$$\alpha\beta \equiv m(\alpha,\beta)(\alpha\beta)$$

voor alle $a \in A$, $b \in A$, $\alpha \in \Gamma_1$, $\beta \in \Gamma_1$. Vorm de quotiëntsemigroep G.

We zoeken noodzakelijke en voldoende voorwaarden, op te leggen aan de functies $m(\alpha,\beta)$ en ${}^{\alpha}a$, opdat G een groep is en iedere klasse, die een element van G is, één en slechts één woord bevat van de gedaante $a\rho$ met $a \in A$, $\rho \in \Gamma_2$.

Hiertoe definiëren we een <u>standaardreductie</u>, die bestaat uit het herhaaldelijk toepassen van een van de volgende overgangen:

$$\alpha\ldots \to e\alpha\ldots \qquad \alpha \in \Gamma_1$$

$$ab\ldots \to (ab)\ldots \qquad a \in A,\ b \in A$$

$$a\alpha b\ldots \to (a\cdot{}^{\alpha}b)\alpha\ldots \qquad a \in A,\ b \in A,\ \alpha \in \Gamma_1$$

$$a\alpha\beta\ldots \to (a\cdot m(\alpha,\beta))(\alpha\beta)\ldots \qquad a \in A,\ \alpha \in \Gamma_1,\ \beta \in \Gamma_1.$$

Hierdoor gaat ieder woord W over in een ondubbelzinnig bepaald standaardwoord $\mathcal{S}(W)$, dat equivalent is met W en dat de gedaante a of $a\alpha$ ($a \in A$, $\alpha \in \Gamma_1$) heeft.

Hieruit volgt direct, dat iedere klasse minstens één woord van de gedaante $a\rho$ heeft. We moeten nu eisen, dat dit er hoogstens één is; dit is het geval als:

$$W_1 \sim W_2 \implies \mathcal{S}(W_1) = \mathcal{S}(W_2),$$

en hiervoor is voldoende dat

$\mathcal{S}(XAY) = \mathcal{S}(XBY)$ waarin $A \equiv B$ de gegeven relaties doorloopt.

Voor de standaardreductie geldt echter

$$\mathcal{S}(UV) = \mathcal{S}(\mathcal{S}(U)V)$$

$$\mathcal{S}(cU) = \mathcal{S}(c\,\mathcal{S}(U)),\ c \in A.$$

Hieruit volgt, dat we ermee kunnen volstaan, Y leeg te nemen en X het woord met de ene letter γ ($\gamma \in \Gamma_1$). Hieruit volgt:

Elke klasse van G bevat dan en slechts dan één en slechts één element van de vorm $a\rho$ ($a \in A$, $\rho \in \Gamma_2$) als

$$\left.\begin{aligned} \mathcal{S}(\gamma ab) &= \mathcal{S}(\gamma(ab)) \\ \mathcal{S}(\gamma\alpha a) &= \mathcal{S}(\gamma \cdot {}^{\alpha}a \cdot \alpha) \\ \mathcal{S}(\gamma\alpha\beta) &= \mathcal{S}(\gamma \cdot m(\alpha,\beta) \cdot (\alpha\beta)) \\ \mathcal{S}(\gamma e\alpha) &= \mathcal{S}(\gamma\alpha) \end{aligned}\right\}$$

voor alle $a \in A$, $b \in A$, $\alpha \in \Gamma_1$, $\beta \in \Gamma_1$, $\gamma \in \Gamma_1$.

Het uitwerken van deze betrekkingen wordt bemoeilijkt door het feit, dat bij de reductie letters van de vorm $(\alpha\beta)$ optreden, die in Γ_2 liggen en dus hetzij e, hetzij $\in \Gamma_1$ zijn, hetgeen verschil maakt voor de volgende reductiestappen. Zo worden we genoodzaakt tot gevalonderscheidingen. Deze voorkomen we door een wijziging van de reductie. Hiertoe breiden we eerst de functies uit:

$$m(\rho,\beta),\ \Gamma_2 \times \Gamma_1 \to A,\ \rho \in \Gamma_2,\ \beta \in \Gamma_1,\ m(\rho,\beta) \in A,$$
$${}^{\rho}a\ ,\ \Gamma_2 \times A \to A\ ,\ \rho \in \Gamma_2,\ a \in A\ ,\ {}^{\rho}a \in A,$$

door de definitie: $m(e,\beta) = e$, ${}^{e}a = a$.

We beschouwen nu de volgende gewijzigde lijst van overgangen:

$\alpha\ldots \to e\alpha\ldots$	$\alpha \in \Gamma_1$
$ak\ldots \to (ak)\ldots$	$a \in A,\ k \in A,\ k \neq e$
$a\rho b\ldots \to (a \cdot {}^{\rho}b)\rho\ldots$	$a \in A,\ b \in A,\ \rho \in \Gamma_2$
$a\rho\beta\ldots \to (a \cdot m(\rho,\beta))(\rho\beta)\ldots$	$a \in A,\ \beta \in \Gamma_1,\ \rho \in \Gamma_2$.

Hierdoor wordt W overgevoerd in een woord $\mathcal{S}_1(W)$, dat de gedaante a of $a\rho$ ($a \in A$, $\rho \in \Gamma_2$) heeft, en dat gelijk is aan $\mathcal{S}(W)$, met als uitzondering, dat het gebeuren kan, dat $\mathcal{S}(W)$ de gedaante a en $\mathcal{S}_1(W)$ de gedaante ae (met dezelfde a) heeft. Hieruit volgt, dat voor woorden W, waarvoor $\mathcal{S}_1(W)$ de gedaante $a\rho$ heeft, geldt

$$\mathcal{S}_1(W_1) = \mathcal{S}_1(W_2) \iff \mathcal{S}(W_1) = \mathcal{S}(W_2).$$

Door met de reductie $\mathcal{S}_2$ te werken, wordt nu gemakkelijk het volgende resultaat gevonden:

Elke klasse van G bevat dan en slechts dan één en slechts één element van de vorm $a\rho$ ($a \in A$, $\rho \in \Gamma_2$) als:

$$\left.\begin{aligned} {}^{\gamma_a} \cdot {}^{\gamma_b} &= {}^{\gamma_{(ab)}} \\ m(\gamma,\alpha) \cdot {}^{(\gamma\alpha)}a &= {}^{\gamma}({}^{\alpha}a) \cdot m(\gamma,\alpha) \\ m(\gamma,\alpha) \cdot m((\gamma\alpha),\beta) &= {}^{\gamma}m(\alpha,\beta) \cdot m(\gamma,(\alpha\beta)) \end{aligned}\right\} \quad (*)$$

voor alle $a \in A$, $b \in A$, $\alpha \in \Gamma_1$, $\beta \in \Gamma_1$, $\gamma \in \Gamma_1$; hierin zijn haakjes bij de productvorming in A weer weggelaten.

Het is gemakkelijk te zien, dat als hieraan voldaan is, G ook een groep is, die aan de vereisten van de uitbreidingstheorie voldoet.

Ter wille van de symmetrie wordt het tweede argument in de m-functie ook tot Γ_2 uitgebreid door de definitie:

$$m(\rho,e) = e.$$

Het is dan makkelijk te zien, dat $(*)$ ook blijft gelden als men α, β en γ nu Γ_2 laat doorlopen in plaats van Γ_1.

Als men $m(\rho,\sigma)$ en ${}^{\rho}a$ van te voren geeft als functies $\Gamma_2 \times \Gamma_2 \to A$, resp. $\Gamma_2 \times A \to A$, moeten aan $(*)$ nog de volgende eisen (die hierboven definities waren) worden toegevoegd:

$$m(e,\sigma) = e,\ m(\rho,e) = e,\ {}^{e}a = a,$$

voor alle $\rho \in \Gamma_2$, $\sigma \in \Gamma_2$, $a \in A$.

De voorwaarden $(*)$ zijn juist de voorwaarden van Schreier.