STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

Zw 1957 - 019

Over een getallen-theoretisch probleem voortgekomen uit de groepentheorie

W. Peremans

21 oktober 1957

1957

Over een getallen-theoretisch probleem voortgekomen uit de groepentheorie.

ZW 1957-019

21 oktober 1957

Zeer geachte Professor Loonstra,

In het volgende geef ik een elementair bewijs van de door U gevonden getallentheoretische stelling, waar U donderdag j.l. met mij over sprak.

Stelling. Zij n een natuurlijk getal en laten $\alpha,\beta,\ldots$ elementen voorstellen van de additieve groep van de restklassen modulo n. Laat $m(\alpha,\beta)$ aangeven een willekeurige functie, die gedefinieerd is voor alle α en β, als waarden gehele getallen heeft en daarbij voldoet aan het volgende drietal betrekkingen:

(1) $\quad m(0,\alpha) = m(\alpha,0) = 0$

(2) $\quad m(\alpha,\beta) = m(\beta,\alpha)$

(3) $\quad m(\alpha+\beta,\gamma) + m(\alpha,\beta) = m(\alpha,\beta+\gamma) + m(\beta,\gamma).$

Laten twee functies $m(\alpha,\beta)$ en $m'(\alpha,\beta)$ die aan bovenstaande eisen voldoen, aequivalent heten als er gehele getallen $c(\alpha)$ bestaan, zodanig dat

(4) $\quad m(\alpha,\beta) - m'(\alpha,\beta) = c(\alpha+\beta) - c(\alpha) - c(\beta).$

Dan geldt: er zijn precies n niet-aequivalente stelsels oplossingen $m(\alpha,\beta)$.

Om deze stelling te bewijzen voeren we eerst een reductie van de gegevens uit. We zullen steeds (3) gebruiken in de volgende vorm:

(3') $\quad m(\alpha,\beta+\gamma) = m(\alpha+\beta,\gamma) + m(\alpha,\beta) - m(\beta,\gamma).$

We tonen nu de volgende bewering aan:

Bewering: Zij $m(\alpha,\beta)$ een functie met gehele waarden, gedefinieerd voor alle α en β. Onderstel dat $m(0,0)=0$ en dat (3) geldt voor $\beta=1$. Dan is (3) algemeen geldig en gelden ook (1) en (2).

Bewijs. Er is gegeven dat (3) geldt voor $\beta=1$. Onderstel dat (3) geldt voor een bepaalde waarde van β. Dan vinden we, door (3) toe te passen met $1+\gamma$ in plaats van γ,

$$m(\alpha,\beta+(1+\gamma)) = m(\alpha+\beta,1+\gamma) + m(\alpha,\beta) - m(\beta,1+\gamma).$$

Passen we op de eerste en de derde term in het rechterlid, (3) toe met $\beta=1$, dan vinden we:

$$\begin{aligned} m(\alpha,\beta+1+\gamma) &= m(\alpha+\beta+1,\gamma) + m(\alpha+\beta,1) - m(1,\gamma) \\ &\quad + m(\alpha,\beta) - m(\beta+1,\gamma) - m(\beta,1) + m(1,\gamma) \\ &= m(\alpha+\beta+1,\gamma) + m(\alpha+\beta,1) + m(\alpha,\beta) - m(\beta,1) - m(\beta+1,\gamma), \end{aligned}$$

wat bij toepassing van (3) met $(\alpha,\beta,1)$ in plaats van (α,β,γ) levert:

$$m(\alpha,\beta+1+\gamma) = m(\alpha+\beta+1,\gamma) + m(\alpha,\beta+1) - m(\beta+1,\gamma).$$

Dit is (3) voor het stel $(\alpha,\beta+1,\gamma)$. Door volledige inductie volgt dat (3) algemeen geldt.

We laten nu zien dat (2) is af te leiden uit (3). Toepassing van (3') op het stel $(1,\beta,1)$ geeft:

$$m(1,\beta+1) = m(\beta+1,1) + m(1,\beta) - m(\beta,1).$$

Door volledige inductie naar β volgt hieruit dat algemeen $m(1,\beta) = m(\beta,1)$, daar dit voor $\beta=1$ juist is. Toepassing van (3') op het stel $(2,\beta,2)$ geeft:

$$m(2,\beta+2) = m(\beta+2,2) + m(2,\beta) - m(\beta,2).$$

Hieruit volgt door volledige inductie dat $m(2,\beta)=m(\beta,2)$; want deze relatie is triviaal voor $\beta=2$ en reeds bewezen voor $\beta=1$. Door toepassing van (3') op $(3,\beta,3)$, enz. vinden we zo dat algemeen geldt $m(\alpha,\beta)=m(\beta,\alpha)$.

Tenslotte leert toepassing van (3) met $\beta=\gamma=0$ dat $2m(\alpha,0)=m(\alpha,0)+m(0,0)$. Wegens $m(0,0)=0$ is dus algemeen $m(\alpha,0)=m(0,\alpha)=0$. Daarmee is de bewering aangetoond.

We recapituleren dat we voor m slechts hoeven te eisen dat

(1') $$m(0,0) = 0$$

(3") $$m(\alpha,\gamma+1) = m(\alpha+1,\gamma) + m(\alpha,1) - m(1,\gamma)$$

en dat hieruit o.a. volgt dat steeds $m(\alpha,0)=0$. Dan kunnen we, als de waarden $m(\alpha,1)$ voorgeschreven zijn, met behulp van (3") de waarden $m(\alpha,\gamma)$ $(\gamma\neq 0,1)$ successievelijk berekenen; voor elke $m(\alpha,\gamma)$ hebben we precies één vergelijking die $m(\alpha,\gamma)$ uitdrukt in functiewaarden voor lagere γ. Dus leidt elk stelsel waarden $m(\alpha,1)$ tot precies één oplossing van de vergelijkingen (1), (2), (3). We zullen nagaan onder welke omstandigheden deze ene oplossing aequivalent is met de nuloplossing.

Voor zulk een oplossing $m(\alpha,\beta)$ geldt wegens (4):

(5) $$m(\alpha,\beta) = c(\alpha+\beta) - c(\alpha) - c(\beta),$$

met zekere gehele getallen $c(\alpha)$. Aan deze betrekking is voldaan als geldt

(5') $$m(\alpha,1) = c(\alpha+1) - c(\alpha) - c(1),$$

d.w.z. als (5) geldt voor $\beta=1$. Immers, is (5) vervuld voor een zekere waarde van β, dan hebben we ook, krachtens (3"), (2) en (5'),

$$\begin{aligned} m(\alpha,\beta+1) &= m(\alpha+1,\beta) + m(\alpha,1) - m(1,\beta) \\ &= m(\alpha+1,\beta) + m(\alpha,1) - m(\beta,1) \\ &= c(\alpha+\beta+1) - c(\alpha+1) - c(\beta) \\ &\quad + c(\alpha+1) - c(\alpha) - c(1) \\ &\quad - c(\beta+1) + c(\beta) + c(1) \\ &= c(\alpha+\beta+1) - c(\alpha) - c(\beta+1). \end{aligned}$$

We moeten dus nagaan, wanneer aan (5') te voldoen is, d.w.z. aan

(6) $$x = A_n y ,$$

waarin x de $(n-1)$-vector is met componenten $m(1,1), m(2,1),\ldots,$ $\ldots m(n-1,1)$, y de vector met componenten $c(1), c(2),\ldots,c(n-1)$ en A de $(n-1) \times (n-1)$ - matrix

$$A_n = \begin{pmatrix} -2 & 1 & & & & \\ -1 & -1 & 1 & & & \\ -1 & & -1 & 1 & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \\ -1 & & & & -1 & 1 \\ -1 & & & & & -1 \end{pmatrix}.$$

Tellen we bij de eerste rij de overige op, dan vinden we

$$\det A_n = -n \begin{vmatrix} -1 & 1 & & & \\ & -1 & 1 & & \\ & & \ddots & \ddots & \\ & & & -1 & 1 \\ & & & & -1 \end{vmatrix} = (-1)^{n-1} n.$$

We zien dus dat de stellen $m(\alpha,1)$ die tot een oplossing voeren, welke aequivalent is met de nuloplossing, gegeven worden door de punten x in de Cartesische ruimte R_{n-1}, welke uit de punten y met gehele coördinaten ontstaan door toepassing van een vaste, geheeltallige transformatie A met determinant $\pm n$. Vatten we R_{n-1} als additieve groep t.a.v. de optelling op, dan betekent $x \sim 0$ dit dat de x een deelmodulus met index n vormen van de modulus, bestaande uit alle roosterpunten in R_{n-1}. Verder zijn twee x-en aequivalent, als hun verschil tot die deelmodulus behoort. Daaruit volgt dat er precies n niet-aequivalente oplossingen $m(\alpha,\beta)$ zijn.

Met hartelijke groeten,

C.G. Lekkerkerker

Zeer geachte Professor Loonstra,

Hieronder geef ik nog een tweede bewijs voor Uw stelling. Dit bewijs wijkt weliswaar niet essentieel af van het hiervóór gegeven bewijs van Lekkerkerker, maar verloopt in de details toch wel enigszins anders.

Laat Z de additieve groep van de gehele getallen zijn en Z_n de additieve groep van de gehele getallen modulo n, waarin n een natuurlijk getal is. Laat K_n de klasse zijn van de functies $m(\alpha,\beta)$ met $\alpha,\beta \in Z_n$, $m(\alpha,\beta) \in Z$, die voldoen aan

$$(1) \qquad m(\alpha+\beta,\gamma) + m(\alpha,\beta) = m(\alpha,\beta+\gamma) + m(\beta,\gamma),$$

$$(2) \qquad m(\alpha,\beta) = m(\beta,\alpha),$$

$$(3) \qquad m(\alpha,0) = 0$$

voor alle $\alpha,\beta,\gamma \in Z_n$. Noem twee elementen $m(\alpha,\beta)$ en $m'(\alpha,\beta)$ van K_n equivalent als er een functie $c(\alpha)$ met $\alpha \in Z_n$, $c(\alpha) \in Z$ bestaat, zo dat

$$(4) \qquad m'(\alpha,\beta) = m(\alpha,\beta) + c(\alpha+\beta) - c(\alpha) - c(\beta)$$

voor alle $\alpha,\beta \in Z_n$. Laat L_n de verzameling van de equivalentieklassen van K_n onder deze equivalentie zijn.

Bewering. L_n heeft n elementen.

Bewijs. Het is triviaal, dat, als $m(\alpha,\beta) \in K_n$ en als $c(\alpha)$ een functie met $\alpha \in Z_n$, $c(\alpha) \in Z$ en $c(0)=0$ is en als $m'(\alpha,\beta)$ door (4) gedefinieerd wordt, dan $m'(\alpha,\beta) \in K_n$.

Stel $m(\alpha,\beta) \in K_n$. Definieer $c(\alpha)$ door

$$(5) \qquad c(0) = c(1)=0,\ c(k) = -\sum_{j=1}^{k-1} m(j,1) \text{ voor } k=2,\ldots,n-1,$$

en $m'(\alpha,\beta)$ door (4). Dan geldt:

$$(6) \qquad m'(k,1) = 0 \text{ voor } k=1,\ldots,n-2,$$

want uit (4) volgt

$$m'(k,1) = m(k,1) - \sum_{j=1}^{k} m(j,1) + \sum_{j=1}^{k-1} m(j,1) = 0 \text{ voor } k=2,\ldots,n-2,$$

en

$$m'(1,1) = m(1,1) - m(1,1) = 0.$$

Ieder element van L_n bevat dus een $m(\alpha,\beta)$ die voldoet aan

$$(7) \qquad \begin{cases} m(k,1) = 0 \text{ voor } k=0,\ldots,n-2, \\ m(n-1,1) = N \text{ (N geheel)}. \end{cases}$$

We bewijzen nu dat iedere $m(\alpha,\beta) \in K_n$, die aan (7) voldoet, ook voldoet aan

$$(8) \qquad \begin{cases} m(k,l) = 0 & \text{als } 0 \le k \le n-1,\ 0 \le l \le n-1,\ k+l \le n-1, \\ m(k,l) = N & \text{"} \quad 0 \le k \le n-1,\ 0 \le l \le n-1,\ k+l \ge n, \end{cases}$$

zodat $m(\alpha,\beta) \in K_n$ door (7) ondubbelzinnig bepaald is.

We bewijzen dit door volledige inductie naar l. Voor l=0 volgt (8) uit (3). Stel nu dat (8) voor een zekere l met $0 \le l \le n-2$ geldt. Uit (1) volgt

$$m(k,l+1) = m(k+1,1) + m(k,l) - m(1,1).$$

Uit (7) en $0 \leq l \leq n-2$ volgt dat $m(l,1)=0$. We onderscheiden nu drie gevallen:

1° $k+l \leq n-2$, dan is $m(k+l,1)=0$ volgens (7) en $m(k,l)=0$ volgens inductieveronderstelling, dus $m(k,l+1)=0$.

2° $k+l=n-1$, dan is $m(k+l,1)=N$ volgens (7) en $m(k,l)=0$ volgens inductieveronderstelling, dus $m(k,l+1)=N$.

3° $k+l \geq n$. Uit $k \leq n-1$ en $l \leq n-2$ volgt $k+l \leq 2n-3$. Uit $n \leq k+l \leq 2n-3$ volgt $k+l \not\equiv n-1 \pmod n$, dus $m(k+l,1)=0$ volgens (7). Verder is $m(k,l)=N$ volgens inductieveronderstelling, dus $m(k,l+1)=N$.

We bewijzen nu dat iedere functie $m(\alpha,\beta)$ met $\alpha,\beta \in Z_n$ en $m(\alpha,\beta) \in Z$, die aan (8) voldoet, een element van K_n is. Dat (2) en (3) vervuld zijn, is triviaal. We moeten bewijzen dat

$$m(j+k,l) + m(j,k) = m(j,k+l) + m(k,l)$$

voor $0 \leq j \leq n-1$, $0 \leq k \leq n-1$, $0 \leq l \leq n-1$ geldt. We onderscheiden vier gevallen:

1° $j+k \leq n-1$, $k+l \leq n-1$, dan is $m(j+k,l) = m(j,k+l)$ en $m(j,k) = m(k,l)=0$.

2° $j+k \leq n-1$, $k+l \geq n$, dan is $m(j,k)=0$, $m(k,l)=m(j+k,l)=N$ en $m(j,k+l)=m(j,k+l-n)=0$ wegens $j+k+l-n \leq n-2$.

3° $j+k \geq n$, $k+l \leq n-1$; analoog 2°.

4° $j+k \geq n$, $k+l \geq n$, dan is $m(j,k) = m(k,l) = N$ en $m(j+k,l) = m(j+k-n,l) = m(j,k+l-n) = m(j,k+l)$.

We hebben dus bewezen dat er bij ieder element uit K_n een daarmee equivalent element uit K_n bestaat, dat aan (7) voldoet en omgekeerd, dat er bij ieder geheel getal N één en slechts één element uit K_n bestaat dat aan (7) voldoet (dit element is bepaald door (8)).

We moeten dus nu nog nagaan welke functies uit K_n, die aan (7) voldoen, onderling equivalent zijn. Laat $m(\alpha,\beta)$ en $m'(\alpha,\beta)$ twee van zulke functies zijn met bijbehorende N, resp. N'. Veronderstel, dat ze equivalent zijn. Dan bestaat er een functie $c(\alpha)$ met $\alpha \in Z_n$, $c(\alpha) \in Z$ en $c(0)=0$, zo dat (4) vervuld is. Dit geeft op grond van (4) en (7):

$$(9)\quad \begin{cases} 0 = c(k+1) - c(k) - c(1) \text{ voor } k=0,\ldots,n-2, \\ N'-N = -c(n-1) - c(1), \end{cases}$$

want $c(n) = c(0) = 0$. Door optelling vinden we hieruit:

$$(10)\quad N'-N = -nc(1),$$

dus

$$(11)\quad N' \equiv N \pmod n.$$

Laat nu omgekeerd (11) vervuld zijn. Men kan dan $c(1)$ uit (10) bepalen, $c(0)=0$ kiezen, en vervolgens $c(2),\ldots,c(n-1)$ successievelijk zo bepalen, dat (9) vervuld is. Definieert men nu de functie $m''(\alpha,\beta)$ door

$$m''(\alpha,\beta) = m(\alpha,\beta) + c(\alpha+\beta) - c(\alpha) - c(\beta),$$

dan volgt uit (9), dat $m''(\alpha,\beta)$ aan (7) met N' inplaats van N voldoet en dus dezelfde functie is als $m'(\alpha,\beta)$. Hieruit volgt dat $m'(\alpha,\beta)$ equivalent is met $m(\alpha,\beta)$.

We hebben dus bewezen, dat $m(\alpha,\beta)$ en $m'(\alpha,\beta)$ dan en slechts dan equivalent zijn als (11) vervuld is.

Dus L_n heeft n elementen. Met vriendelijke groeten,

W. Peremans