Een massaformule voor abelse groepen

Gonzalez Arroyo, D.W.

D.W. Gonzalez Arroyo

Een massaformule voor abelse groepen

Bachelorscriptie, 14 juli 2011

Scriptiebegeleider: dr. Bart de Smit

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

Laat $X = \{1, \ldots, p^n\}$ zijn, waarbij $n, p \in \mathbb{Z}_{>0}$ en p een priemgetal is. Nu luidt de vraag:

Vraag 1.1 *Hoeveel abelse groepsstructuren zijn er op X?*

Een andere manier om deze vraag te stellen: Hoeveel $\mathbb{Z}$-moduulstructuren met p nilpotent zijn er op X? Een eenvoudiger soortgelijk probleem is om te bepalen hoeveel $\mathbb{F}_p[t]$-moduulstructuren er zijn op X, waarbij t nilpotent is.

Stelling 1.2 *Laat $X = \{1, \ldots, p^n\}$ zijn, waarbij $n, p \in \mathbb{Z}_{>0}$ en p een priemgetal. Het aantal* $\mathbb{F}_p[t]$-moduulstructuren *op X, met t nilpotent, is*

$$\frac{p^n! \cdot p^{n^2-n}}{\prod_{i=0}^{n-1}(p^n - p^i)}.$$

Het bewijs is gebaseerd op twee stellingen.

Stelling 1.3 *Zij gegeven V een n-dimensionale vectorruimte over een lichaam k. Dan bestaat er een bijectie tussen V^{n-1} en de verzameling van nilpotente endomorfismen van V*

Stelling 1.4 *Laat $X = \{1, \ldots, p^n\}$ zijn, waarbij $n, p \in \mathbb{Z}_{>0}$ en p een priemgetal. Het aantal* $\mathbb{F}_p$-moduulstructuren *op X wordt gegeven door*

$$\frac{p^n!}{\prod_{i=0}^{n-1}(p^n - p^i)}$$

In deze scriptie zullen we de stellingen **1.3** en **1.4** bewijzen. Nu volgt stelling **1.2** als volgt.

Een $\mathbb{F}_p[t]$-moduulstructuur is een $\mathbb{F}_p$-moduulstructuur M met $t \in \mathrm{End}_{\mathbb{F}_p}(M)$. Iedere $\mathbb{F}_p$-moduulstructuur op X is isomorf met $\mathbb{F}_p^n$. Dan is t te beschouwen als een nilpotente $n \times n$-matrix over $\mathbb{F}_p$. Het aantal $\mathbb{F}_p[t]$-moduulstructuren op X met t nilpotent bepalen we nu door het aantal $\mathbb{F}_p$-moduulstructuren op X te vermenigvuldigen met het aantal nilpotente $n \times n$-matrices over $\mathbb{F}_p$. De stelling **1.3** geeft nu dat het aantal nilpotente $n \times n$-matrix over $\mathbb{F}_p$ gelijk is aan

$$p^{n^2-n}$$

In feite is het aantal abelse groepsstructuren op X hetzelfde, maar dat wordt niet bewezen in deze scriptie.

2 Tellen van $\mathbb{F}_p$-moduulstructuren

In deze sectie bewijzen we Stelling **1.4**.

Notatie 2.1 *Laat S de verzameling bijecties $f : X \to \mathbb{F}_p^n$ zijn*

Definitie 2.2 *Zij gegeven een bijectie $f \in S$, dan definieren we de optelling en scalaire vermenigvuldiging door*

$$a + b = f^{-1}(f(a) + f(b)), \quad a, b \in X;$$

$$\lambda a = f^{-1}(\lambda f(a)), \quad a \in X, \lambda \in \mathbb{F}_p,$$

Dit geeft een $\mathbb{F}_p$-moduulstructuur op X met f een isomorfisme.

Notatie 2.3 *Laat $\mathrm{GL}_n(\mathbb{F}_p)$ de groep zijn van inverteerbare $n \times n$-matrices over $\mathbb{F}_p$.*

Lemma 2.4 *De orde van $\mathrm{GL}_n(\mathbb{F}_p)$ is gelijk aan $\prod_{i=0}^{n-1}(p^n - p^i)$.*

Bewijs: Laat $A \in \mathrm{GL}_n(\mathbb{F}_p)$ zijn. Dan geldt er dat de eerste kolom van de matrix ongelijk aan nul is. Dit geeft $(p^n - 1)$ mogelijkheden. De tweede kolomvector mag niet bevat zijn in de lineaire deelruimte opgespannen door de eerste kolomvector. Deze ruimte heeft grootte p. Voor de tweede kolomvector zijn er $(p^n - p)$ mogelijkheden. De i-de kolomvector mag niet bevat zijn in de lineaire deelruimte opgespannen door de eerste $i - 1$ kolomvector. De grootte van deze ruimte is p^{i-1}. Er zijn $(p^n - p^{i-1})$ mogelijkheden voor de $i - de$ kolomvector. Op deze manier vinden we dat er $\prod_{i=0}^{n-1}(p^n - p^i)$ mogelijkheden zijn voor A.
$\square$

Definitie 2.5 *Laat $\phi : \mathrm{GL}_n(\mathbb{F}_p) \times S \to S$ gedefinieerd zijn door*

$$(f, g) = f \circ g$$

Dit is een werking van de groep $\mathrm{GL}_n(\mathbb{F}_p)$ op S. We weten dat S nu verdeeld wordt in disjuncte banen. Alle banen hebben gelijke lengte $|\mathrm{GL}_n(\mathbb{F}_p)|$. Uit lemma **2.4** volgt nu dat alle banen gelijke lengte $\prod_{i=0}^{n-1}(p^n - p^i)$ hebben. Het aantal banen wordt dan gegeven door

$$\frac{p^n!}{\prod_{i=0}^{n-1}(p^n - p^i)}.$$

Nu geldt er dat twee bijecties $f, g \in S$ aanleiding geven tot dezelfde $\mathbb{F}_p$-moduulstructuur op X d.e.s.d.a. f, g in dezelfde baan zitten. Zojuist hebben we laten zien dat het aantal banen gelijk is aan $\frac{p^n!}{\prod_{i=0}^{n-1}(p^n - p^i)}$. Hiermee hebben we dus de stelling bewezen.

3 Parametrisatie van nilpotente endomorfismen

In dit hoofdstuk willen we stelling **1.3** bewijzen.

Definitie 3.1 *Een endomorfisme ϕ van een vectorruimte V over k is nilpotent als er een $m \in \mathbb{Z}_{\geq 0}$ bestaat zo dat $\phi^m = 0$.*

Notatie 3.2 *Laat V een vectorruimte zijn, dan is* $\mathrm{Nilp}(V)$ *de verzameling van alle nilpotente endomorfismen van V.*

Laat V een n-dimensionale vectorruimte over k zijn. Nu willen we een bijectie $P : V^{n-1} \to \mathrm{Nilp}(V)$ definiëren.

Definitie 3.3 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $v_0, \ldots, v_{n-1} \in V$ met $v_0 = 0$, dan worden $b_0, \ldots, b_{n-1}$ gedefinieerd door*

$$b_i = \begin{cases} \inf\ S \setminus \langle b_0, \ldots, b_{i-1} \rangle & \text{als } v_i \in \langle b_0, \ldots, b_{i-1} \rangle; \\ v_i & \text{als } v_i \notin \langle b_0, \ldots, b_{i-1} \rangle. \end{cases}$$

De vectoren $b_0, \ldots, b_{n-1}$ zijn lineair onafhankelijk, want voor ieder $i \leq n-1$ geldt $b_i \notin \langle b_0, \ldots, b_{i-1} \rangle$

Definitie 3.4 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $v_0, \ldots, v_{n-1} \in V$ met $v_0 = 0$, dan wordt de verzameling $I_{v_1,\ldots,v_{n-1}}$ gedefinieerd als*

$$\{j \leq n-1 : b_i \neq v_i\} \cup \{n\}.$$

Definitie 3.5 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij $v_0, \ldots, v_{n-1} \in V$ met $v_0 = 0$ gegeven, dan wordt de lineaire afbeelding $\phi_{v_1,\ldots,v_{n-1}}$ gedefinieerd door*

$$\phi_{v_1,\ldots,v_{n-1}}(b_i) = \begin{cases} b_{i+1} & \text{als} i+1 \notin I_{v_1,\ldots,v_{n-1}}; \\ \\ v_{\sup\{j \leq i : j \in I_{v_1,\ldots,v_{n-1}}\}} & \text{als} i+1 \in I_{v_1,\ldots,v_{n-1}}. \end{cases}$$

We zullen laten zien dat de afbeelding $\phi_{v_1,\ldots,v_{n-1}}$ nilpotent is. Dit geeft nu aanleiding tot de volgende definitie.

Definitie 3.6 (Parametrisatie nilpotente endomorfisme) *Zij V een n-dim vectorruimte met geordende basis S. De afbeelding $P : V^{n-1} \longrightarrow$* $\mathrm{Nilp}(V)$ *wordt gedefinieerd door*

$$P(v_1, \ldots, v_{n-1}) = \phi_{v_1,\ldots,v_{n-1}}.$$

Lemma 3.7 *Laat V een n-dim vectorruimte zijn met geordende basis S. Zij gegeven $v_1, \ldots, v_{n-1} \in V$, dan is de lineaire afbeelding $P(v_1, \ldots, v_{n-1})$ nilpotent.*

Bewijs: Laat $f = P(v_1, \ldots, v_{n-1})$ zijn. Nu bewijzen we met inductie dat voor iedere $s \in I_{v_1,\ldots,v_{n-1}}$ geldt

$$f(\langle b_0, \ldots, b_{s-1} \rangle) \subset \langle b_0, \ldots, b_{s-1} \rangle \text{ en } f^s(\langle b_0, \ldots, b_{s-1} \rangle) = 0 \qquad (*).$$

- Stap 1
  Voor $s = 0$ is het duidelijk.
- Stap 2
  Veronderstel dat $s \in I_{v_1,\dots,v_{n-1}}$ zo dat $(*)$ geldt. Nu bewijzen we dat $m = \inf\{k \in I_{v_1,\dots,v_{n-1}} : k > s\}$ ook voldoet aan $(*)$. De vectoren $b_s, \dots, b_{m-1}$ worden gegeven door $b_s = \inf\ S \setminus \langle b_0, \dots, b_{s-1}\rangle, f(b_s), \dots, f^{m-s-1}(b_s)$ waarbij $f^{m-s} \in \langle b_0, \dots, b_{s-1}\rangle$. Nu geeft de hypothese dat $f^m(\langle b_0, \dots, b_{m-1}\rangle) = 0$ en $f(\langle b_0, \dots, b_{m-1}\rangle) \subset \langle b_0, \dots, b_{m-1}\rangle$.
- Stap 3
  Door Stap 2 te herhalen vinden we dat $(*)$ geldt voor $s = n$, ofwel f is nilpotent. $\square$

De volgende opmerking is bedoeld ter verduidelijking van definitie **3.3** tot en met **3.6**. De opmerking kan overgeslagen worden.

Opmerking 3.8 In definitie 3.3 tot en met 3.5 wordt een lineaire afbeelding f gedefinieerd waarvoor $s_1 \dots, s_k \in S$ en $p_1, \dots, p_k \in \mathbb{Z}_{>0}$ met $s_1 < s_2 < \dots < s_k$ bestaan zo dat

$$\begin{array}{lllll}
f^0(s_1) = s_1, & f(s_1) = v_1 & , f^2(s_1) = v_2 & , \dots & , f^{p_1-1}(s_1) = v_{p_1-1}, \\
f^0(s_2) = s_2, & f(s_2) = v_{p_1+1} & , f^2(s_2) = v_{p_1+2} & , \dots & , f^{p_2-1}(s_2) = v_{p_1+p_2-1}, \\
\dots & \dots & \dots & \dots & \dots \\
f^0(s_k) = s_k, & f(s_k) = v_{n-p_k+1}, & f^2(s_k) = v_{n-p_k+2}, & \dots & , f^{p_k-1}(s_k) = v_{n-1}
\end{array}$$

een basis is van V, waarbij

$$s_1 = \inf S, \quad s_i = \inf\{s \in S : s \notin \langle f^0(s_1), f(s_1), \dots, f^{p_i-1}(s_i)\rangle\},$$

$$f^{p_1}(s_1) = 0, \quad f^{p_2}(s_2) = v_{p_1}, \quad f^{p_3}(s_3) = v_{p_1+p_2}, \ \dots \ , \quad f^{p_k}(s_k) = v_{p_1+\dots+p_{k-1}},$$
$$v_{p_1+\dots+p_i} \in \langle f^0(s_1), f(s_1), \dots, f^{p_{i-1}-1}(s_i)\rangle.$$

Representeren we de afbeelding f nu met respect tot bovenstaande basis als een matrix A , dan

$$A = \begin{pmatrix}
0 & & & * & & & & * & \\
1 & \ddots & & * & & & & * & \\
& \ddots & 0 & * & & & & * & \\
& & 1 & * & & & & * & \\
& & & 0 & 0 & & & * & \\
& & & & 1 & \ddots & & * & \\
& & & & & \ddots & 0 & * & \\
& & & & & & 1 & * & \\
& & & & & & & & \ddots
\end{pmatrix}$$

Voorbeeld 3.9

- Zij $V = \mathbb{F}^2$ met geordende basis $S = \{e_1, e_2\}$. Laat $A \in \mathrm{Nilp}(V)$ geschreven als $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Nu kunnen we alle nilpotente endomorfisme bepalen van $\mathbb{F}^2$. Zij gegeven $(x_1, x_2) \in \mathbb{F}^2$, dan onderscheiden we volgens Definitie 1 nu twee situaties. In de eerste situatie nemen we $\mathbf{x} = (x_1, x_2) \in \langle e_1 \rangle$, ofwel $x_2 = 0$. Dit betekent dat we het rijtje $b_0 = e_1$ en $b_1 = e_2$ krijgen. Nu geeft Definitie 4 dat
$$\phi_{\mathbf{x}} = \begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix}.$$
In de tweede situatie nemen we $(x_1, x_2) \notin \langle e_1 \rangle$ en nu krijgen we $b_0 = e_1$ en $b_1 = (x_1, x_2)$. Nu geeft Definitie 4 dat $\phi_{0,\mathbf{x}}(e_1) = (x_1, x_2)$ en $\phi_{\mathbf{x}}((x_1, x_2)) = 0$. Hieruit vinden we nu dat
$$\phi_{\mathbf{x}} = \begin{pmatrix} x_1 & \frac{-x_1^2}{x_2} \\ x_2 & -x_1 \end{pmatrix}.$$

- Zij $V = \mathbb{F}^3$ met geordende basis $S = \{e_1, e_2.e_3\}$. Neem nu $v_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ en $v_2 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ waarbij $x_1, x_2, x_3 \neq 0$. Nu wordt $b_0 = e_1$, $b_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ en $b_2 = e_2$. Vervolgens geldt er nu dat $\phi_{v_1,v_2}(b_0) = v_1$, $\phi_{v_1,v_2}(b_1) = 0$ en $\phi_{v_1,v_2}(b_2) = v_1$. We weten vervolgens dat $e_3 = \frac{1}{x_3}(v_1 - x_1 e_1 - x_2 e_2)$. Nu geldt er dat $\phi_{v_1,v_2}(e_3) = \frac{1}{x_3}(-x_1 v_1 - x_2 v_2)$. Representeren we ϕ_{v_1,v_2} met respect tot de standaardbasis S als een matrix A, dan
$$A = \begin{pmatrix} x_1 & x_1 & \frac{-(x_1^2 + x_1 x_2)}{x_3} \\ x_2 & x_2 & \frac{-(x_2^2 + x_1 x_2)}{x_3} \\ x_3 & x_3 & -x_1 - x_2 \end{pmatrix}.$$

Opmerking 3.10 Om te bewijzen dat P een bijectie is, gaan we een afbeelding $P' : \mathrm{Nilp}(V) \to V^{n-1}$ definieren met de eigenschap dat $P \circ P' = \mathrm{Id}$ en $P' \circ P = \mathrm{Id}$. Indien we een dergelijke functie gevonden hebben is duidelijk dat P een bijectie is.

Definitie 3.11 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $f \in \mathrm{End}(V)$, dan worden de vectoren $a_0, \ldots, a_{n-1}$ gedefinieerd door*
$$a_0 = \inf S;$$
$$a_i = \begin{cases} \inf S \setminus \langle a_0, \ldots, a_{i-1} \rangle & \textit{als } f(a_{i-1}) \in \langle (a_0, \ldots, a_{i-1}) \rangle; \\ f(a_{i-1}) & \textit{anders.} \end{cases}$$

De vectoren $a_0, \ldots, a_{n-1}$ zijn lineair onafhankelijk. Dit volgt uit het feit dat voor iedere $i \leq n-1$ geldt $a_i \notin \langle a_0, \ldots, b_{i-1} \rangle$

Definitie 3.12 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $f \in \mathrm{End}(V)$, dan wordt I_f gedefinieerd als de verzameling*

$$I_f = \{j \in \{1, \dots, n-1\} : f(a_{j-1}) \neq a_j\} \cup \{0, n\}$$

Opmerking 3.13 Nu geldt:

$$I_f = \{s : f(\langle a_0, \dots, a_{s-1}\rangle) \subset \langle a_0, \dots, a_{s-1}\rangle\}$$

Definitie 3.14 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $f \in \mathrm{End}(V)$, dan worden de vectoren $v'_0, \dots, v'_{n-1}$ gedefinieerd door*

$$v'_i = \begin{cases} a_i & \text{als } i \notin I_f \\ f^{\inf\{k \geq 1 \ : \ i+k \ \in \ I_f\}}(a_i) & \text{als } i \in I_f. \end{cases}$$

Definitie 3.15 *Laat V een n-dimensionale vectorruimte zijn met geordende basis S. Zij gegeven $f \in \mathrm{Nilp}(V)$, dan wordt $P' : \mathrm{Nilp}(V) \to V^{n-1}$ gedefinieerd door*

$$P'(f) = (v'_1, \dots, v'_{n-1})$$

De volgende opmerking is bedoeld ter verduidelijking van definitie **3.11** tot en met **3.14**. De opmerking kan overgeslagen worden.

Opmerking 3.16 Wat wordt gedaan bij definitie 3.9 tot en met 3.12 is het volgende:

- Kies nu $s_1 = \inf S$ en schrijf de vectoren

  $$s_1, f(s_1), \dots, f^{p_1-1}(s_1)$$

  totdat $f^{p_1}(s_1) \in \langle s_1, f(s_1), \dots, f^{p_1-1}(s_1)\rangle$.

- Kies vervolgens $s_2 = \inf\{s \in S : s \notin \langle s_1, f(s_1), \dots, f^{p_1-1}(s_1)\rangle\}$ en schrijf de vectoren

  $$s_2, f(s_2), \dots, f^{p_2-1}(s_2)$$

  totdat $f^{p_2}(s_2) \in \langle s_1, f(s_1), \dots, f^{p_1-1}(s_1), s_2 \dots, f^{p_2-1}(s_2)\rangle$.

- ga zo door...

Op deze manier vinden we $s_1, \dots, s_k \in S$ met $\inf\ S = s_1 < \dots < s_k$ en $p_1, \dots, p_k \in \mathbb{Z}_{>0}$ zo dat

$$\begin{array}{lllll} s_1, & f(s_1), & f^2(s_1), & \dots & , f^{p_1-1}(s_1) \\ s_2, & f(s_2), & f^2(s_2), & \dots & , f^{p_2-1}(s_2) \\ \dots & \dots & \dots & \dots & \dots \\ s_k, & f(s_k), & f^2(s_k), & \dots & , f^{p_k-1}(s_k) \end{array}$$

een basis is van V. Dit rijtje is dan het rijtje $a_0, \dots, a_{n-1}$. Nu geldt er dat $f^{p_i}(s_i) \in \langle s_1, \dots, f^{p_i-1}(s_i)\rangle$. Vervolgens wordt het rijtje $v'_0, \dots, v'_{n-1}$ nu gemaakt door $s_1, \dots, s_k$ te vervangen door $f^{p_1}(s_1), \dots, f^{p_k}(s_k)$.

Lemma 3.17 *Laat V een n-dimensionale vectorruimte zijn met S een geordende basis. Zij gegeven $f \in \text{Nilp}(V)$ en $i \in I_f$ met $i \neq n$, dan geldt $v'_i \in \langle a_0, \ldots, a_{i-1} \rangle$.*

Bewijs: Laat $l = \inf\{k \geq 1 \ : \ i+k \ \in \ I_f\}$. Wegens definitie **3.11** geldt er $v'_i = f^l(a_i)$. Laat $l = \inf\{k \ : \ i+k \ \in \ I_f\}$. Nu geldt er dus dat $v'_i = f^l(a_i)$ met $f^l(a_i) \in \langle a_0, \ldots, a_{i+l-1} \rangle$. Laat $U = \langle a_0, \ldots, a_{i-1} \rangle$ zijn en definiëer $W = \langle a_0, \ldots, a_{i+l-1} \rangle / U$. Dan is W een l-dimensionale vectorruimte. Laat $\bar{f} : W \to W$ gegeven door

$$\bar{f}(a + U) = f(a) + U.$$

Nu moeten we wel laten zien dat $\bar{f}$ welgedefinieerd is. Veronderstel $a + U = a' + U$, dan geldt $a' = a+u$ met $u \in U$. Nu geldt dat $f(a')+U = f(a+u)+U = f(a)+f(u)+U$, vanwege $f(\langle a_0, \ldots, a_{i-1} \rangle) \subset \langle a_0, \ldots, a_{i-1} \rangle$ geldt er dat $f(a') + U = f(a) + U$. Nu weten we dat f nilpotent is. Dit betekent dat $\bar{f}$ nilpotent is. De dimensie van W is l , dus concluderen we dat $\bar{f}^l = 0$, ofwel $\bar{f}^l(a_i) = f^l(a_i) + U = U$. □

Stelling 3.18 *Zij V een n-dimensionale vectorruimte met geordende basis S. Laat P, P' de afbeeldingen zijn in definitie **3.6** en **3.12**, dan geldt $P \circ P' = Id$ en $P' \circ P = Id$.*

Bewijs: We beginnen met het bewijzen van $P \circ P' = Id$.
Laat $f \in \text{Nilp}(V)$ zijn en $a_0, \ldots, a_{n-1}, I_f, v'_1, \ldots, v'_{n-1}$ als in definitie **3.11** tot en met **3.13**. Laat $b_0, \ldots, b_{n-1}, I_{v'_1,\ldots,v'_{n-1}}, \phi_{v'_1,\ldots,v'_{n-1}}$ als in definitie **3.3** tot en met **3.5**

- Stap 1
  $a_0 = \inf \ S$ en $b_0 = \inf \ S$ met $0 \in I_f \cap I_{v'_1,\ldots,v'_{n-1}}$, dus $a_0 = b_0$

- Stap 2
  Veronderstel dat $a_i = b_i$ voor $i \in \{0, \ldots, s\}$ en $I_f \cap \{0, \ldots, s\} = I_{v'_1,\ldots,v'_{n-1}} \cap \{0, \ldots, s\}$ met $s < n - 1$.
  We gaan bewijzen dat $a_{s+1} = b_{s+1}$ en $I_f \cap \{0, \ldots, s+1\} = I_{v'_1,\ldots,v'_{n-1}} \cap \{0, \ldots, s+1\}$.
  Er zijn nu twee gevallen
  (1) $s + 1 \in I_f$
  Nu geldt dat $f(a_s) \neq a_{s+1}$. Dit betekent wegens definitie **3.9** dat $f(a_s) \in \langle a_0, \ldots, a_s \rangle$, ofwel $a_{s+1} = \inf \ S \setminus \langle a_0, \ldots, a_s \rangle$. Lemma 3.16 geeft nu dat $v'_{s+1} \in \langle a_0, \ldots, a_s \rangle$. De hypothese geeft vervolgens dat $v'_{s+1} \in \langle b_0, \ldots, b_s \rangle$. Nu is $s+1 \in I_{v'_1,\ldots,v'_{n-1}}$ Wegens definitie **3.3** geldt nu dat $b_s+1 = \inf \ S \setminus \langle b_0, \ldots, b_s \rangle$, hetgeen betekent dat $b_{s+1} = a_{s+1}$
  (2) $s + 1 \notin I_f$
  Nu geldt er dat $v'_{s+1} = a_{s+1}$ wegens definitie **3.9**. Nu geldt $v'_{s+1} \notin \langle b_0, \ldots, b_s \rangle$ wegens de hypothese. Nu geldt er volgens definitie **3.3** dat $b_{s+1} = v_{s+1}$ en volgens definite **3.4** dat $s + 1 \notin I_{v'_1,\ldots,v'_{n-1}}$. We vinden $b_{s+1} = a_{s+1}$

- Stap 3
  Door Stap 2 te herhalen vinden we dat $b_i = a_i$ voor $i \in \{0, \ldots, n-1\}$ en $I_f = I_{v'_1,\ldots,v'_{n-1}}$

De volgende stap is om te laten zien dat $f = \phi_{v'_1,\ldots,v'_{n-1}}$.

Zij gegeven $i \in \{0, \ldots, n-1\}$. Dan onderscheiden we twee gevallen

- $i+1 \in I_f$
  Laat $X = \sup \{j \in I_f : j \leq i\}$ zijn en $Y = \inf\{k : k + X \in I_f\}$. Nu geldt er dat $Y = i - X + 1$. Nu geldt er wegens definitie **3.5** dat $\phi_{v'_1,\ldots,v'_{n-1}}(a_i) = v'_X$. Wegens definitie **3.13** geldt er nu dat $v'_X = f^Y(a_X)$. Per definitie **3.11** geldt dat $a_X, \ldots, a_i$ worden gegeven door

$$a_X, f(a_X), \ldots, f^{i-X}(a_X)$$

  Nu vinden we dus dat $f^Y(a_X) = f^{i-X+1}(a_X) = f(a_i)$, hetgeen betekent dat $f(a_i) = \phi_{v'_1,\ldots,v'_{n-1}}(a_i)$.

- $i+1 \notin I_f$
  Nu geldt er wegens definitie **3.5** dat $\phi_{v'_1,\ldots,v'_{n-1}}(a_i) = a_{i+1}$ en wegens definitie van I_f dat $a_{i+1} = f(a_i)$.

We hebben dus laten zien dat $f, \phi_{v'_1,\ldots,v'_{n-1}}$ gelijke beelden hebben op de basis $a_0, \ldots, a_{n-1}$. Dus geldt er $f = \phi_{v'_1,\ldots,v'_{n-1}}$, waarbij $\phi_{v'_1,\ldots,v'_{n-1}} = P \circ P'(f)$.

Nu laten we zien dat $P' \circ P$.Laat $v_1, \ldots, v_{n-1} \in V$ zijn. Laat $b_0, \ldots, b_{n-1}, I_{v_1,\ldots,v_{n-1}}$, $\phi_{v_1,\ldots,v_{n-1}}$ zijn als in definitie **3.3** tot en met **3.5**. Laat behorende bij $\phi_{v_1,\ldots,v_{n-1}}$: $a_0, \ldots, a_{n-1}, I_{\phi_{v_1,\ldots,v_{n-1}}}, v'_1 \ldots, v'_{n-1}$ zijn als in definitie **3.11** tot en met **3.13**. We zullen nu even een wat eenvoudigere notatie N voor $\phi_{v_1,\ldots,v_{n-1}}$ gebruiken.

- Stap 1
  $b_0 = \inf \ S$ en $a_0 = \inf \ S$ en $0 \in I_{v_1,\ldots,v_{n-1}} \cap I_N$

- Stap 2
  Veronderstel dat $b_i = a_i$ voor $i \in \{0, \ldots, s\}$ en $I_{v_1,\ldots,v_{n-1}} \cap \{0, \ldots, s\} = I_N \cap \{0, \ldots, s\}$ met $s < n-1$.
  We gaan bewijzen dat $b_i = a_i$ voor $i \in \{0, \ldots, s+1\}$ en $I_{v_1,\ldots,v_{n-1}} \cap \{0, \ldots, s+1\} = I_N \cap \{0, \ldots, s+1\}$
  Er zijn nu twee gevallen

  (1) $s+1 \in I_{v_1,\ldots,v_{n-1}}$
  Nu geldt er dat $b_{s+1} = \inf \ S \setminus \langle b_0, \ldots, b_s\rangle$ Laat $X = \sup\{j \in I_{v_1,\ldots,v_{n-1}} : j \leq s\}$ zijn. Nu geldt wegens definitie **3.5** dat $N(b_s) = v_X$. Nu geldt er wegens de definitie **3.3** van $I_{v_1,\ldots,v_{n-1}}$ dat $N(b_s) \in \langle b_0, \ldots, b_{X-1}\rangle$ waarbij $X \leq s$. Hieruit en uit de aanname volgt nu dat $N(a_s) \in \langle a_0, \ldots, a_s\rangle$. Hieruit vinden we dat $a_{s+1} = \inf \ S \setminus \langle a_0, \ldots, a_s\rangle$ en wegens de hypothese geldt dat $a_{s+1} = b_{s+1}$. Vanwege $a_{s+1} \neq N(a_s)$ volgt dat $s+1 \in I_N$.
  (2) $s+1 \notin I_{v_1,\ldots,v_{n-1}}$
  Nu geldt wegens definitie **3.4** dat $b_{s+1} = v_{s+1}$ en wegens definitie **3.5** $N(b_s) = b_{s+1}$, ofwel $N(a_s) \notin \langle a_0, \ldots, a_s\rangle$. Nu geldt dat $a_{s+1} = N(a_s) = N(b_s) = b_{s+1}$ en bovendien geldt nu $s+1 \notin I_N$

- Stap 3
  Door nu Stap 2 te herhalen vinden we dat $b_i = a_i$ voor $i \in \{0, \ldots, n-1\}$ en

$I_{v_1,\ldots,v_{n-1}} = I_N$

De volgende stap is om te laten zien dat $v_1, \ldots, v_{n-1}$ gelijk zijn aan $v'_1, \ldots, v'_{n-1}$
Zij gegeven $i \in \{1, \ldots, n-1\}$. Nu onderscheiden we twee gevallen

- $i \in I_{v_1,\ldots,v_{n-1}}$
  Laat $X = \inf\{k \geq 1 : i + k \in I_{v_1,\ldots,v_{n-1}}\}$ en $Y = \sup\{j \in I_{v_1,\ldots,v_{n-1}} : j \leq i + k\}$ zijn. Nu geldt $Y = i$. Wegens definitie **3.13** geldt dat $v'_i = N^X(b_i)$. Dit laatste is gelijk aan $N(a_{i+X-1})$. Dit laatste is wegens definitie **3.5** gelijk aan v_Y, ofwel $v'_i = v_i$

- $i \notin I_{v_1,\ldots,v_{n-1}}$
  Nu geldt wegens definitie **3.13** dat $v'_i = b_i$ en wegens de definitie van $I_{v_1,\ldots,v_{n-1}}$ dat $v_i = b_i$, ofwel $v_i = v'_i$

We hebben nu dus laten zien dat $v_1, \ldots, v_{n-1}$ gelijk zijn aan $v'_1, \ldots, v'_{n-1}$, waarbij $P' \circ P(v_1, \ldots, v_{n-1}) = (v'_1, \ldots, v'_{n-1})$. Hieruit vinden we dat $P' \circ P = Id$. $\square$

Nu Stelling **3.17** bewezen is kunnen we concluderen dat P een bijectie is. Dit betekent dat we Stelling **1.3** hebben bewezen.