

DE UITWISSELINGSSTELLING VAN HUGHES

P.H. RODENBURG,

Instituut voor Informatica, Universiteit van Amsterdam

In the nineteen sixties, N.J.S. Hughes proved a generalization of the Steinitz Exchange Theorem for an abstract notion of dependence. The present note contains a streamlined and detailed rendering of his argument, with some digressions. Among other things it is explained why a theorem of Graczyńska [G] is not Hughes' theorem.

§0. INLEIDING

In de vroege jaren zestig van de vorige eeuw publiceerde N.J.S. Hughes een uitbreiding van de uitwisselingsstelling van Steinitz [S], met een opmerkelijk elegant bewijs. Hij overwoog bovendien een verdere generalisatie, waarin minimale afhankelijke verzamelingen niet per se eindig zijn, en concludeerde dat zijn bewijs tot op zekere hoogte ook binnen de ruimere context stand houdt. De aanleiding voor deze notitie was dat mij niet meteen duidelijk was tot welke hoogte. In het onderstaande herschrijf ik Hughes' betoog *zonder* de a priori aanname dat afhankelijkheid gebaseerd is op eindige verzamelingen. Min of meer vanzelf leidt dat tot een nadere beschouwing van de rol die eindigheid speelt.

§1. VOORBEREIDINGEN

De Hoare-conditionaal

$$F(x) \triangleleft P(x) \triangleright G(x)$$

staat voor: $F(x)$ als $P(x)$ geldt, anders $G(x)$.

Ik noteer $\hat{s}$ voor de eenling $\{s\}$. Als $X \cap Y = \emptyset$,¹ dan noteer ik $X \cup Y$ als $X + Y$. $\mathbb{Z}_+$ is de verzameling der positieve gehele getallen. Natuurlijke getallen gelden ook als verzamelingen: $n = \{0, 1, \dots, n-1\}$. Een rijtje van n elementen van een verzameling V is dan een functie van n naar V . Het *beeld* $\text{Im } \varphi$ van een functie φ is de verzameling van alle waarden van φ . Als X een verzameling elementen is van een groep G , dan is $\text{Sg}^G X$ de door X voortgebrachte ondergroep van G . Om aan te geven dat een deelverzameling een subdomein is (ondergroep, submodule, ...) schrijf ik soms $\leq$ in plaats van $\subseteq$. Zij $\aleph$ een kardinaalgetal: een verzameling X is $\aleph$ -klein als haar machtigheid $|X|$ kleiner is dan $\aleph$, en $\aleph$ -opsombaar als $|X| \leq \aleph$. Eindig is $\aleph_0$ -klein, aftelbaar $\aleph_0$ -opsombaar. De notatie $X \subset Y$ betekent dat $X \subseteq Y$ en $X \neq Y$.

Bij een gegeven (stricte) lineaire orde $\mathbf{X} = \langle X, < \rangle$ noteer ik

$$(\leftarrow x) := \{u \mid u < x\} \text{ en } (\leftarrow x] := \{u \mid u \leq x\} (= \{u \mid u = x \text{ of } u < x\}).$$

Een *bovengrens* van een verzameling $U \subseteq X$ is een $x \in X$ zo dat $\forall u \in U. u \leq x$.

Een *afhankelijkheidsruimte* is een paar $\mathbf{S} = \langle S, \mathcal{D} \rangle$ van een verzameling S en een *afhankelijkheidsbasis* $\mathcal{D}$ in S , dat is, een collectie $\mathcal{D}$ van niet-lege deelverzamelingen van S zo dat

¹ $\emptyset$ voor 'øde samling', al is dat geen gebruikelijk Deens.

$$\begin{aligned}
 (\text{trans}) \quad \hat{d} + X + Y \in \mathcal{D} \ \& \ \forall x \in X(\hat{x} + E_x \in \mathcal{D} \ \& \ d \notin E_x) \Rightarrow \\
 & \exists C \subseteq Y \cup \bigcup_{x \in X} E_x. \hat{d} + C \in \mathcal{D}.
 \end{aligned}$$

Merk op dat als $S \subset T$ en $\mathcal{D}$ een afhankelijkheidsbasis is in S , $\mathcal{D}$ ook een afhankelijkheidsbasis is in T .

VOORBEELD I. Zij S een module over een integriteitsgebied R . Laat $\mathcal{D}$ de collectie zijn der niet-lege eindige $D \subseteq S$ waarvoor $\rho: D \rightarrow R \setminus \hat{0}$ bestaat zo dat

$$(1) \quad \sum_{d \in D} \rho_d d = 0.$$

De collectie $\mathcal{D}$ voldoet aan (trans): laat $d, x_1, \dots, x_m, y_1, \dots, y_n$ onderscheiden elementen zijn van S , en $\lambda, \mu_1, \dots, \mu_m, v_1, \dots, v_n \in R \setminus \hat{0}$, zo dat

$$(2) \quad \lambda d + \mu_1 x_1 + \dots + \mu_m x_m + v_1 y_1 + \dots + v_n y_n = 0;$$

laat verder voor $1 \leq i \leq m$, $z_1^{(i)}, \dots, z_{k_i}^{(i)}$ onderscheiden elementen zijn van $S \setminus \hat{d}$, en $\kappa_0^{(i)}, \dots, \kappa_{k_i}^{(i)} \in R \setminus \hat{0}$, zo dat

$$\kappa_0^{(i)} x_i + \kappa_1^{(i)} z_1^{(i)} + \dots + \kappa_{k_i}^{(i)} z_{k_i}^{(i)} = 0.$$

Definieer:

$$\kappa_0^* = \prod_{i=1}^m \kappa_0^{(i)}; \quad \text{en voor } 1 \leq j \leq k_i, \rho_j^{(i)} = -\prod_{t=1}^{i-1} \kappa_0^{(t)} \cdot \kappa_j^{(i)} \cdot \prod_{t=i+1}^m \kappa_0^{(t)}.$$

Dan geldt, voor $1 \leq i \leq m$,

$$(3.i) \quad \kappa_0^* x_i - \rho_1^{(i)} z_1^{(i)} - \dots - \rho_{k_i}^{(i)} z_{k_i}^{(i)} = 0.$$

Dus

$$\begin{aligned}
 (4) \quad \kappa_0^* \lambda d + \mu_1 \rho_1^{(1)} z_1^{(1)} + \dots + \mu_1 \rho_{k_1}^{(1)} z_{k_1}^{(1)} + \dots + \mu_m \rho_1^{(m)} z_1^{(m)} + \dots + \mu_m \rho_{k_m}^{(m)} z_{k_m}^{(m)} + \\
 + \kappa_0^* v_1 y_1 + \dots + \kappa_0^* v_n y_n = 0.
 \end{aligned}$$

Formule (4) heeft nog niet per se de vorm van formule (1): hetzelfde module-element kan meermaals genoemd worden. We kunnen echter vereenvoudigen door coëfficiënten van gelijke elementen bij elkaar op te tellen. Vervolgens laten we de summanden weg waarvan de coëfficiëntensom op 0 uitkomt. In dit proces blijft d buiten schot. We komen dus uit op een formule

$$(5) \quad \kappa_0^* \lambda d + \beta_1 e_1 + \dots + \beta_u e_u = 0,$$

met $d, e_1, \dots, e_u$ verschillend, $\{e_1, \dots, e_u\} \subseteq \{y_1, \dots, y_n\} \cup \bigcup_{1 \leq i \leq m} \{z_1^{(i)}, \dots, z_{k_i}^{(i)}\}$, en coëfficiënten $\kappa_0^* \lambda, \beta_1, \dots, \beta_u$ allemaal niet-nul.

Een abelse groep is een unitaire module over $\mathbb{Z}$: het bovenstaande definieert dus ook afhankelijkheidsruimten over abelse groepen.

Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte.

Een verzameling $A \subseteq S$ is *afhankelijk* (in $\mathbf{S}$, of in $\mathcal{D}$) als $\mathcal{D} \cap \mathcal{P}A \neq \emptyset$; en anders *onafhankelijk*. Merk op dat uitbreidingen van afhankelijke verzamelingen ook afhankelijk zijn, en deelverzamelingen van onafhankelijke verzamelingen onafhankelijk.

Als $x \in A$ of een verzameling $B \subseteq A$ bestaat zo dat $\hat{x} + B \in \mathcal{D}$, dan heet x *afhankelijk van A* (in $\mathbf{S}$, of in $\mathcal{D}$), notatie $x \sim_{\mathbf{S}} A$, of, als S gefixeerd is, $x \sim_{\mathcal{D}} A$; meestal is het subscript overbodig en schrijven we $x \sim A$.

OPMERKING. In het bijzondere geval van Voorbeeld I dat S een vectorruimte is over een lichaam K betekent $x \sim A$ dat er $n \in \mathbb{N}$, $a: n \rightarrow A$ en $\kappa: n \rightarrow K$ bestaan zo dat $x = \kappa_1 a_1 + \dots + \kappa_n a_n$.

Een verzameling $A \subseteq S$ is *gesloten* als $\forall s \in S. s \sim A \Rightarrow s \in A$. We noteren:

$$\tilde{A} := \{x \in S \mid x \sim A\},$$

de *afsluiting* van A . We hebben hier inderdaad met een afsluitingsoperatie van doen:

PROPOSITIE 1. (i) $A \subseteq \tilde{A}$;

(ii) $A \subseteq B \Rightarrow \tilde{A} \subseteq \tilde{B}$;

(iii) $\tilde{\tilde{A}} = \tilde{A}$.

BEWIJS. (i) Per definitie.

(ii) Als $A \subseteq B$, $x \in \tilde{A}$, en $x \notin B$, dan is er een verzameling $Y \subseteq A$ zo dat $\hat{x} + Y \in \mathcal{D}$. Dan ook $Y \subseteq B$.

(iii) $\tilde{\tilde{A}} \supseteq \tilde{A}$ volgt uit (i). Voor de omgekeerde inclusie, stel $x \sim \tilde{A}$. Als $x \in \tilde{A}$, dan zijn we meteen klaar. Stel $x \notin \tilde{A}$. Dan is er een verzameling $C \subseteq \tilde{A}$ zo dat

$$\hat{x} + C \in \mathcal{D}.$$

Beschouw $c \in C$. Als $c \notin A$, dan is er een verzameling $E_c \subseteq A$ zo dat $\hat{c} + E_c \in \mathcal{D}$. Dan $x \notin E_c$, dus volgens (trans) is er een verzameling

$$Y \subseteq (C \cap A) \cup \bigcup_{c \in C \setminus A} E_c,$$

dus $Y \subseteq A$, zo dat $\hat{x} + Y \in \mathcal{D}$. □

OPMERKING. Propositie 1 impliceert

$$(6) \quad A \subseteq \tilde{B} \Rightarrow \tilde{A} \subseteq \tilde{B},$$

en uit (6) volgt (trans). Stel namelijk dat

$$\hat{d} + X + Y \in \mathcal{D} \ \& \ \forall x \in X (\hat{x} + E_x \in \mathcal{D} \ \& \ d \notin E_x),$$

dan $d \in \widetilde{X+Y}$, en $X + Y \subseteq \widetilde{Y \cup \bigcup_x E_x}$. Dus $d \sim Y \cup \bigcup_x E_x$ volgens (6). Omdat

$$d \notin Y \cup \bigcup_{x \in X} E_x,$$

moet er een verzameling $C \subseteq Y \cup \bigcup_x E_x$ bestaan zo dat $\hat{d} + C \in \mathcal{D}$.

Als $\tilde{A} = S$, dan heet A een *voortbrengende verzameling* van S . Als A bovendien onafhankelijk is, dan heet A een *basis* van S .

OPMERKING. Als S in voorbeeld I een vectorruimte is, dan hebben de uitdrukkingen *voortbrengende verzameling* en *basis* de in de algebra gangbare betekenis. In het algemeen is dat niet zo: $\hat{2}$ is een basis van de $\mathbb{Z}$ -module $\mathbb{Z}$, maar optellen en aftrekken uitgaande van $\hat{2}$ levert alleen even getallen op.

We noteren $x \sim a + B$ voor:

$$\{a, x\} \cap B = \emptyset \text{ en } (x = a \text{ of } \exists C \subseteq B. \{a, x\} + C \in \mathcal{D}).$$

Merk op dat $x \sim a + B \Leftrightarrow a \sim x + B$.

§2. DE UITWISSELINGSSTELLING

Zij $\langle X, < \rangle$ een welorde, en $\mathcal{D}$ een collectie van verzamelingen. We zullen zeggen dat $<$ *$\mathcal{D}$ -maximerend* is als voor alle $U \subseteq X$ en alle $D \in \mathcal{D}$ geldt dat

(1) $U \cap D \neq \emptyset \Rightarrow U \cap D$ heeft een grootste element.

In het bewijs van Stelling 1 (hieronder) kan het lijken dat (1) een te sterke voorwaarde is. De voor de hand liggende verzwakking is echter slechts schijnbaar:

PROPOSITIE 2. Laat $\mathbf{Y} = \langle Y, < \rangle$ een welorde zijn, en $\mathcal{D}$ een collectie van verzamelingen. Als voor alle $D \in \mathcal{D}$ geldt

(a) $Y \cap D \neq \emptyset \Rightarrow Y \cap D$ heeft een grootste element,

en voor alle $y \in Y$

(b) $(\leftarrow y) \cap D \neq \emptyset \Rightarrow (\leftarrow y) \cap D$ heeft een grootste element,

dan is $<$ $\mathcal{D}$ -maximerend.

BEWIJS. Zij $U \subseteq Y$, $D \in \mathcal{D}$, en $U \cap D \neq \emptyset$. Als $U \cap D$ geen bovengrenzen heeft, dan heeft $Y \cap D$ er ook geen, in strijd met (a). Laat y de kleinste bovengrens zijn van $U \cap D$. Als $y \notin U \cap D$, dan $U \cap D \subseteq (\leftarrow y) \cap D$. Laat z het grootste element zijn van $(\leftarrow y) \cap D$. Dan is z een bovengrens van $U \cap D$. Maar $z < y$: tegenspraak. Dus $y \in U \cap D$, en y is daarmee het grootste element van $U \cap D$. $\square$

LEMMA 1. Zij $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte en $<$ een $\mathcal{D}$ -maximerende welordering van een deelverzameling van S . Als voor $x, y \in S$ en $U \subseteq S$ geldt dat $x \sim (\leftarrow y) + U$ en $x \not\sim U$, dan is er een $y' < y$ zodat $x \sim y' + (\leftarrow y') + U$.

BEWIJS. Als $x < y$, dan $x \sim x + (\leftarrow x) + U$. Zij anders $E \subseteq (\leftarrow y) + U$ zo dat

$$\hat{x} + E \in \mathcal{D}.$$

Als $E \subseteq U$, dan $x \sim U$; dus $E \cap (\leftarrow y) \neq \emptyset$. Zij y' het grootste element van $E \cap (\leftarrow y)$. Dan $x \sim y' + (\leftarrow y') + U$. $\square$

STELLING 1 (Hughes). Zij $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte, en daarin A een basis en B een onafhankelijke verzameling. Als $A \setminus B$ en $B \setminus A$ beide een $\mathcal{D}$ -maximerende welordering hebben, dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $B + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is.

BEWIJS. Zij $C = A \cap B$, $X = A \setminus B$, en $Y = B \setminus A$. Laat $<$ de vereniging zijn van een $\mathcal{D}$ -maximerende welordering van X en een $\mathcal{D}$ -maximerende welordering van Y .

Zij $y \in Y$. Dan $y \sim X + C$, want $X + C$ is een basis. Aangezien $y \notin X + C$, is er een $E \subseteq X + C$ zo dat $\hat{y} + E \in \mathcal{D}$. Dan $E \cap X \neq \emptyset$, want $C + Y$ is onafhankelijk. Zij x het grootste element van $E \cap X (= (\hat{y} + E) \cap X)$. Dan

(2) $y \sim x + (\leftarrow y) + (\leftarrow x) + C$.

Laat x_0 de kleinste $x \in X$ zijn zo dat (2) geldt; we definiëren

$$\varphi(y) = x_0.$$

De functie φ is injectief: stel $y < y'$ en $\varphi(y) = \varphi(y') = x$. Dan

(3) $y' \sim x + (\leftarrow y') + (\leftarrow x) + C$,

en

(3*) als $u < x$, dan *niet* $y' \sim u + (\leftarrow y') + (\leftarrow u) + C$.

Uit (2) volgt

(2') $x \sim (\leftarrow y) + (\leftarrow x) + C$.

Omdat $y < y'$, volgt uit (2') wegens Propositie 1(ii)

$$x \sim (\leftarrow y') + (\leftarrow x) + C;$$

met (3) en (§1:6) leidt dat tot de conclusie dat

$$y' \sim (\leftarrow y') + (\leftarrow x) + C.$$

Omdat $C + Y$ onafhankelijk is, $y' \not\sim (\leftarrow y') + C$. Volgens Lemma 1 is er dus een x' zo dat

$$x' < x \text{ en } y' \sim x' + (\leftarrow y') + (\leftarrow x') + C;$$

maar dat is in tegenspraak met (3*).

Nu bewijzen we dat $C + Y + (X \setminus \text{Im } \varphi)$ onafhankelijk is. Als $C + Y + (X \setminus \text{Im } \varphi)$ afhankelijk is, dan is er een $D \in \mathcal{D}$ zo dat $D \subseteq C + Y + (X \setminus \text{Im } \varphi)$. Omdat $C + Y$ en $C + X$ onafhankelijk zijn, zijn $D \cap Y$ en $D \cap (X \setminus \text{Im } \varphi)$ dan niet leeg. Zij x het grootste element van $D \cap (X \setminus \text{Im } \varphi)$, en y het grootste element van $D \cap Y$. Dan geldt (2).

Neem nu y in (2) (bij gegeven $x \in X \setminus \text{Im } \varphi$) minimaal. Zij $x' = \varphi(y)$; dan $x' < x$, volgens de definitie van φ , en $y \sim x' + (\leftarrow y) + (\leftarrow x') + C$, dus

$$(4) \quad y \sim (\leftarrow y) + (\leftarrow x) + C.$$

Uit (2') en (4) volgt wegens (§1:6)

$$x \sim (\leftarrow y) + (\leftarrow x) + C.$$

Omdat $X + C$ onafhankelijk is, $x \not\sim (\leftarrow x) + C$. Volgens Lemma 1 is er daarom een $y' < y$ zodat $x \sim y' + (\leftarrow y') + (\leftarrow x) + C$. Maar dan $y' \sim x + (\leftarrow y') + (\leftarrow x) + C$, in tegenspraak met de minimaliteit van y .

Tenslotte bewijzen we dat $C + Y + (X \setminus \text{Im } \varphi)$ een voortbrengende verzameling is. Formule (2') impliceert dat voor alle $x \in \text{Im } \varphi$, $x \sim Y + (\leftarrow x) + C$, en dus, met inductie over $<$, $x \sim Y + C$. Bijgevolg $\forall x \in X. x \sim C + Y + (X \setminus \text{Im } \varphi)$. Aangezien $C + X$ een voortbrengende verzameling is, is wegens (§1:6) $C + Y + (X \setminus \text{Im } \varphi)$ dus ook een voortbrengende verzameling.

Omdat $B = C + Y$ en $X = A \setminus B$ is daarmee de stelling bewezen. $\square$

§3. DEELRUIMTEN EN DOMINANTIE

We zullen nu, alvorens over te gaan tot de meer aanschouwelijke gevolgen van Stelling 1, de algemene notie van een afhankelijkheidsruimte wat nader onderzoeken. We definiëren deelruimten, en preciseren de intuïtie dat de kleinste elementen van een afhankelijkheidsbasis de belangrijkste zijn.

Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte. Een *deelruimte* van $\mathbf{S}$ is een paar $\mathbf{T} = \langle T, \mathcal{E} \rangle$ waar $T \subseteq S$ en $\mathcal{E} = \mathcal{D} \cap \mathcal{P}T$. Klaarblijkelijk voldoet $\mathcal{E}$ aan (trans), dus $\mathbf{T}$ is een afhankelijkheidsruimte. We noteren $\mathbf{T} \leq \mathbf{S}$.

PROPOSITIE 3. Zij $\mathbf{T} \leq \mathbf{S}$ en $X \subseteq T$. Dan

- (a) X is onafhankelijk in $\mathbf{T} \Leftrightarrow X$ onafhankelijk is in $\mathbf{S}$;
- (b) voor alle $t \in T$, $t \sim_{\mathbf{T}} X \Leftrightarrow t \sim_{\mathbf{S}} X$.

BEWIJS. (a) Voor $U \subseteq X$ geldt: $U \in \mathcal{E} \Leftrightarrow U \in \mathcal{D}$.

(b) Voor $t \in T$ en $U \subseteq X$ geldt: $\hat{t} + U \in \mathcal{E} \Leftrightarrow \hat{t} + U \in \mathcal{D}$. $\square$

Laat $\mathcal{D}$ en $\mathcal{E}$ afhankelijkheidsbases zijn in S ; we zullen zeggen dat $\mathcal{E}$ *globaal gedomineerd* wordt door $\mathcal{D}$, en noteren $\mathcal{E} \leq_g \mathcal{D}$, als

$$\forall E \in \mathcal{E} \exists D \in \mathcal{D}. D \subseteq E;$$

en dat $\mathcal{E}$ *locaal gedomineerd* wordt door $\mathcal{D}$, notatie $\mathcal{E} \leq_l \mathcal{D}$, als

$$\forall s \in S \forall E \in \mathcal{E}. s \in E \in \mathcal{E} \Rightarrow \exists D \in \mathcal{D}. s \in D \subseteq E.$$

Omdat afhankelijkheidsbases bestaan uit niet-lege verzamelingen impliceert locale dominantie globale dominantie.

PROPOSITIE 4. Laat $\mathcal{D}$ en $\mathcal{E}$ afhankelijkheidsbases zijn in een verzameling S . Dan

- (a) $\mathcal{E} \leq_g \mathcal{D} \Leftrightarrow \forall X \subseteq S (X \text{ is afhankelijk onder } \mathcal{E} \Rightarrow X \text{ is afhankelijk onder } \mathcal{D})$.
- (b) $\mathcal{E} \leq_l \mathcal{D} \Leftrightarrow \forall s \in S \forall X \subseteq S (s \sim_{\mathcal{E}} X \Rightarrow s \sim_{\mathcal{D}} X)$.

BEWIJS. (a) ($\Rightarrow$) Stel $\mathcal{E} \leq_g \mathcal{D}$. Als X afhankelijk is onder $\mathcal{E}$, dan $E \subseteq X$ voor zekere $E \in \mathcal{E}$. Neem $D \in \mathcal{D}$ zo dat $D \subseteq E$; dan $D \subseteq X$, dus X is afhankelijk onder $\mathcal{D}$.

($\Leftarrow$) Stel dat alle onder $\mathcal{E}$ afhankelijke verzamelingen ook afhankelijk zijn onder $\mathcal{D}$; dan zijn in het bijzonder de elementen van $\mathcal{E}$ afhankelijk onder $\mathcal{D}$. Dus als $E \in \mathcal{E}$, dan is er een $D \in \mathcal{D}$ zo dat $D \subseteq E$.

(b) ($\Rightarrow$) Stel $\mathcal{E} \leq_l \mathcal{D}$. Als $s \sim_{\mathcal{E}} X$, dan ofwel $s \in X$, en in dat geval ook $s \sim_{\mathcal{D}} X$, of er bestaat een verzameling $U \subseteq X$ zo dat $\hat{s} + U \in \mathcal{E}$. Omdat $\mathcal{D} \geq_l \mathcal{E}$ is er dan een verzameling $V \subseteq U$ zo dat $\hat{s} + V \in \mathcal{D}$; dus $s \sim_{\mathcal{D}} X$.

($\Leftarrow$) Stel $s \in E \in \mathcal{E}$; laat $E' = E \setminus \hat{s}$. Dan $s \sim_{\mathcal{E}} E'$; dus $s \sim_{\mathcal{D}} E'$. Omdat $s \notin E'$ moet er een verzameling $V \subseteq E'$ bestaan zo dat $\hat{s} + V \in \mathcal{D}$; dan $s \in \hat{s} + V \subseteq E$. $\square$

Afhankelijkheidsbases $\mathcal{D}$ en $\mathcal{E}$ zijn *globaal equivalent*, notatie $\mathcal{D} \equiv_g \mathcal{E}$, als ze elkaar wederzijds globaal domineren; en *locaal equivalent*, notatie $\mathcal{D} \equiv_l \mathcal{E}$, als ze elkaar wederzijds lokaal domineren.

GEVOLG 1. Laat $\mathcal{D}$ en $\mathcal{E}$ afhankelijkheidsbases zijn in een verzameling S . Dan

- (a) $\mathcal{E} \equiv_g \mathcal{D} \Leftrightarrow \forall X \subseteq S (X \text{ is afhankelijk onder } \mathcal{E} \Leftrightarrow X \text{ is afhankelijk onder } \mathcal{D})$.
- (b) $\mathcal{E} \equiv_l \mathcal{D} \Leftrightarrow \forall s \in S \forall X \subseteq S (s \sim_{\mathcal{E}} X \Leftrightarrow s \sim_{\mathcal{D}} X)$.
- (c) $\mathcal{D} \leq_g \mathcal{E} \leq_l \mathcal{D} \Rightarrow \forall X \subseteq S (X \text{ is een basis onder } \mathcal{E} \Rightarrow X \text{ is een basis onder } \mathcal{D})$.
- (d) $\mathcal{E} \equiv_l \mathcal{D} \Rightarrow \forall X \subseteq S (X \text{ is een basis onder } \mathcal{E} \Leftrightarrow X \text{ is een basis onder } \mathcal{D})$.

BEWIJS van (c). Stel dat X een basis is onder $\mathcal{E}$. Volgens Propositie 4(b),

$$\forall s \in S s \sim_{\mathcal{E}} X \Rightarrow \forall s \in S s \sim_{\mathcal{D}} X,$$

dus X is een voortbrengende verzameling onder $\mathcal{D}$. En als X afhankelijk is onder $\mathcal{D}$, dan is X afhankelijk onder $\mathcal{E}$, quod non.

(d) volgt uit (c) omdat locale equivalentie globale equivalentie impliceert. $\square$

VOORBEELD II. Laat T en U disjuncte oneindige verzamelingen zijn, en

$$S = T \cup U.$$

Laat $\mathcal{E}$ bestaan uit de coëindige deelverzamelingen van T , en $\mathcal{D}$ uit de coëindige deelverzamelingen van S . Dan is $\mathcal{E}$ een afhankelijkheidsbasis in S : want stel

$$\hat{d} + X + Y \in \mathcal{E} \ \& \ \forall x \in X (\hat{x} + E_x \in \mathcal{E} \ \& \ d \notin E_x);$$

als $x \in X$, dan is $\hat{d} + E_x$ coëindig in T , en als $X = \emptyset$ dan is $\hat{d} + Y$ coëindig in T . En $\mathcal{D} + \mathcal{E}$ is er ook een: stel

$$\hat{d} + X + Y \in \mathcal{D} + \mathcal{E} \ \& \ \forall x \in X (\hat{x} + E_x \in \mathcal{D} + \mathcal{E} \ \& \ d \notin E_x).$$

Als $X = \emptyset$, dan $\hat{d} + Y \in \mathcal{D} + \mathcal{E}$. Als er een $x \in X$ is zo dat $\hat{x} + E_x \in \mathcal{D}$, dan ook

$$\hat{d} + E_x \in \mathcal{D}.$$

Stel dat $X \neq \emptyset$ en dat voor alle $x \in X$, $\hat{x} + E_x \in \mathcal{E}$. Als $d \in T$, dan $\hat{d} + E_x \in \mathcal{E}$, voor willekeurig welke $x \in X$. Als $d \in U$, dan is Y cofinaal in U ; en dan $\hat{d} + E_x + Y \in \mathcal{D}$.

Vanzelfsprekend $\mathcal{E} \leq_l \mathcal{D} + \mathcal{E}$, en $\mathcal{D} + \mathcal{E} \leq_g \mathcal{E}$ omdat $D \cap T \in \mathcal{E}$ als $D \in \mathcal{D}$. Maar $\mathcal{D} + \mathcal{E} \not\leq_l \mathcal{E}$, want als $d \in D \in \mathcal{D}$ dan kan d tot U behoren, en dan $d \notin \bigcup \mathcal{E}$.

Zij $\mathfrak{k}$ een kardinaalgetal en $\mathcal{D}$ een afhankelijkheidsbasis. We noteren $\mathcal{D} \leq_g \mathfrak{k}$ als $\mathcal{D}$ globaal equivalent is met een afhankelijkheidsbasis waarvan de elementen $\mathfrak{k}$ -opsombaar zijn; en $\mathcal{D} <_g \mathfrak{k}$ als $\mathcal{D}$ globaal equivalent is met een afhankelijkheidsbasis die bestaat uit $\mathfrak{k}$ -kleine verzamelingen. Analoog hebben we $\mathcal{D} \leq_l \mathfrak{k}$ en $\mathcal{D} <_l \mathfrak{k}$. We noemen een afhankelijkheidsruimte $\langle S, \mathcal{D} \rangle$ *globaal finitair* als $\mathcal{D} <_g \aleph_0$, en *locaal finitair* als $\mathcal{D} <_l \aleph_0$. Merk op dat lokaal finitaire afhankelijkheidsruimten ook globaal finitair zijn.

LEMMA 2. Zij $\mathfrak{k}$ een kardinaalgetal en $\mathcal{D}$ een afhankelijkheidsbasis.

- (a) Als $\mathcal{D} <_l \mathfrak{k}$, dan $\mathcal{D} <_g \mathfrak{k}$;
- (b) als $\mathcal{D} \leq_l \mathfrak{k}$, dan $\mathcal{D} \leq_g \mathfrak{k}$.

BEWIJS. Simpel. Merk op dat $\mathcal{D} \leq_i \mathfrak{k}$, met $i \in \{l, g\}$, dan en slechts dan als $\mathcal{D} <_i \mathfrak{k}^+$. $\square$

LEMMA 3. Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte en $\mathfrak{k}$ een kardinaalgetal. Dan

- (a) $\mathcal{D} <_g \mathfrak{k} \Leftrightarrow \forall D \in \mathcal{D} \exists D' \in \mathcal{D} (D' \subseteq D \ \& \ |D'| < \mathfrak{k})$;
- (b) $\mathcal{D} <_l \mathfrak{k} \Leftrightarrow \forall D \in \mathcal{D} \forall s \in D \exists D' \in \mathcal{D} (s \in D' \subseteq D \ \& \ |D'| < \mathfrak{k})$;
- (c) $\mathcal{D} \leq_g \mathfrak{k} \Leftrightarrow \forall D \in \mathcal{D} \exists D' \in \mathcal{D} (D' \subseteq D \ \& \ |D'| \leq \mathfrak{k})$;
- (d) $\mathcal{D} \leq_l \mathfrak{k} \Leftrightarrow \forall D \in \mathcal{D} \forall s \in D \exists D' \in \mathcal{D} (s \in D' \subseteq D \ \& \ |D'| \leq \mathfrak{k})$.

In het bijzonder,

- (e) $\mathbf{S}$ is globaal finitair $\Leftrightarrow \forall D \in \mathcal{D} \exists D' \in \mathcal{D} (D' \subseteq D \ \& \ D' \text{ is eindig})$;
- (f) $\mathbf{S}$ is lokaal finitair $\Leftrightarrow \forall D \in \mathcal{D} \forall s \in D \exists D' \in \mathcal{D} (s \in D' \subseteq D \ \& \ D' \text{ is eindig})$.

BEWIJS. (a) $(\Rightarrow)$ Zij $\mathcal{C}$ een afhankelijkheidsbasis die bestaat uit $\mathfrak{k}$ -kleine verzamelingen en globaal equivalent is met $\mathcal{D}$. Zij $D \in \mathcal{D}$. Omdat $\mathcal{D} \leq_g \mathcal{C}$ geldt voor zekere $E \in \mathcal{C}$ dat $E \subseteq D$. Omdat $\mathcal{C} \leq_g \mathcal{D}$ is er een $D' \in \mathcal{D}$ zo dat $D' \subseteq E$. Omdat E $\mathfrak{k}$ -klein is, is D' het ook.

$(\Leftarrow)$ Laat $\mathcal{C} := \{E \in \mathcal{D} \mid E \text{ is } \mathfrak{k}\text{-klein}\}$. Dan $\mathcal{C} \equiv_g \mathcal{D}$.

(b) $(\Rightarrow)$ Zij $\mathcal{C}$ een afhankelijkheidsbasis die bestaat uit $\mathfrak{k}$ -kleine verzamelingen en lokaal equivalent is met $\mathcal{D}$. Zij $s \in D \in \mathcal{D}$. Omdat $\mathcal{D} \leq_l \mathcal{C}$ geldt voor zekere $E \in \mathcal{C}$ dat $s \in E \subseteq D$. Omdat $\mathcal{C} \leq_l \mathcal{D}$ is er een $D' \in \mathcal{D}$ zo dat $s \in D' \subseteq E$. Omdat E $\mathfrak{k}$ -klein is, is D' het ook.

$(\Leftarrow)$ Laat $\mathcal{C} := \{E \in \mathcal{D} \mid E \text{ is } \mathfrak{k}\text{-klein}\}$. Dan $\mathcal{C} \equiv_l \mathcal{D}$.

(c), (d): Zie het bewijs van Lemma 2. $\square$

§4. GEVOLGEN VAN DE UITWISSELINGSSTELLING

Gevolg 1(d) impliceert dat we Hughes' stelling ruimer kunnen formuleren:

GEVOLG 2. Zij $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte, en daarin A een basis en B een onafhankelijke verzameling. Als er een afhankelijkheidsbasis $\mathcal{D}' \equiv_l \mathcal{D}$ is zo dat $A \setminus B$ en $B \setminus A$ beide een $\mathcal{D}'$ -maximerende welordening hebben, dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $B + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is.

GEVOLG 3. Laat A en B onafhankelijke verzamelingen zijn in een afhankelijkheidsruimte $\mathbf{S} = \langle S, \mathcal{D} \rangle$, zo dat $\tilde{B} \subseteq \tilde{A}$. Als er een afhankelijkheidsbasis $\mathcal{D}' \equiv_l \mathcal{D}$ is zo dat $A \setminus B$ en $B \setminus A$ beide een $\mathcal{D}'$ -maximerende welordening hebben, dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $U := B + ((A \setminus B) \setminus \text{Im } \varphi)$ onafhankelijk is en $\tilde{U} = \tilde{A}$.

BEWIJS. A is een basis in $\langle \tilde{A}, \mathcal{D} \cap \mathcal{P}\tilde{A} \rangle$. $\square$

GEVOLG 4. Zij $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte, A een basis, en B een onafhankelijke deelverzameling van S . Als

(a) $\mathcal{D}$ lokaal finitair is, of

(b) $A \setminus B$ eindig is,

dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $B + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is.

BEWIJS. (a) Als een afhankelijkheidsbasis $\mathcal{D}'$ bestaat uit eindige verzamelingen, dan is elke welordering $\mathcal{D}'$ -maximerend. Het is dan voldoende dat $A \setminus B$ en $B \setminus A$ welordeningen toelaten, en in het algemeen volgt dat uit het Keuze-Axioma.

(b) Laat $A \setminus B$ eindig zijn. Zij $B' \subseteq B$ zo dat $A \cap B \subseteq B'$ en $|B' \setminus A| \leq |A \setminus B|$. Er bestaan welordeningen van $A \setminus B (= A \setminus B')$ en $B' \setminus A$, en in een eindige welorde hebben alle niet-lege verzamelingen een grootste element: die welordeningen zijn dus $\mathcal{D}$ -maximerend. Volgens Stelling 1 bestaat er een injectie

$$\varphi: B' \setminus A \rightarrow A \setminus B$$

zo dat $B' + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is.

Als $|B \setminus A| < |A \setminus B|$, dan kunnen we $B' = B$ nemen. Stel dat $|B \setminus A| \geq |A \setminus B|$; neem dan B' zo dat $|B' \setminus A| = |A \setminus B|$. Omdat φ eindig is, is φ surjectief; dus B' is een basis. Omdat B onafhankelijk is, en $B' \subseteq B$, moet gelden dat $B' = B$. $\square$

Gewoon het Steinitz-procédé toepassen geeft een overlappend resultaat:

STELLING 2. Zij S een afhankelijkheidsruimte, A een basis, en B een onafhankelijke deelverzameling van S . Als

(a) $B \setminus A$, of

(b) $A \setminus B$

eindig is, dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $B + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is.

BEWIJS. (a) Met inductie naar $|B \setminus A|$. Als $|B \setminus A| = 0$, dan voldoet de lege injectie. Stel dat een injectie φ als in de stelling omschreven bestaat voor verzamelingen B zo dat $|B \setminus A| = n$. Neem aan dat $|B \setminus A| = n + 1$. Fixeer $b \in B \setminus A$; definieer

$$B' := B \setminus \hat{b}.$$

Volgens aanname bestaat er een injectie $\varphi': B' \setminus A \rightarrow A \setminus B$ zo dat

$$A' := B' + ((A \setminus B) \setminus \text{Im } \varphi')$$

een basis is. Dan $b \sim A'$; $b \notin A'$ en $\hat{b}$ is onafhankelijk, dus er is een $a \in A'$ zo dat $b \sim a + (A' \setminus \hat{a})$. Laat $A'' = A' \setminus \hat{a}$. Dan

$$a \sim b + A'',$$

dus $A'' + \hat{b}$ is een voortbrengende verzameling. Bovendien is $A'' + \hat{b}$ onafhankelijk, want als $b \sim A''$ dan $a \sim A''$, quod non. We kunnen φ dus definiëren op $B \setminus A$ door

$$\varphi(x) = a \triangleleft x = b \triangleright \varphi'(x).$$

(b) Zij $A \setminus B$ eindig. Volgens (a) is er voor elke $B' \subseteq B$ zo dat $B' \setminus A$ eindig is een injectie $\varphi: B' \setminus A \rightarrow A \setminus B'$ zo dat $B' + ((A \setminus B') \setminus \text{Im } \varphi')$ een basis is. In het bijzonder kunnen we B' zo kiezen dat $A \cap B' = A \cap B$. Als $|B' \setminus A| = |A \setminus B|$, dan is φ surjectief; dan is B' een basis, dus $B = B'$ omdat B onafhankelijk is. $\square$

GEVOLG 5. Laat A en B onafhankelijke verzamelingen zijn in een afhankelijkheidsruimte $S = \langle S, \mathcal{D} \rangle$, zo dat $\tilde{B} \subseteq \tilde{A}$. Als

(a) $\mathcal{D} \cap \mathcal{P}\tilde{A}$ lokaal finitair is, of

(b) $A \setminus B$ eindig, of

(c) $B \setminus A$ eindig,

dan bestaat er een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $U := B + ((A \setminus B) \setminus \text{Im } \varphi)$ onafhankelijk is en $\tilde{U} = \tilde{A}$.

BEWIJS. Uit Gevolg 4 en Stelling 2; A is een basis in $\langle \tilde{A}, \mathcal{D} \cap \mathcal{P}\tilde{A} \rangle$. $\square$

§5. FINITAIRE AFHANKELIJKHEIDSRUIMTEN

In een vectorruimte is elke onafhankelijke verzameling bevat in een basis. Het bewijs laat zich als volgt generaliseren.

STELLING 3 (*basisexistentistelling*). Zij A een voortbrengende verzameling in een globaal finitaire afhankelijkheidsruimte $\mathbf{S} = \langle S, \mathcal{D} \rangle$, en B onafhankelijk in $\mathbf{S}$. Dan is er een verzameling $A' \subseteq A$ zo dat $B + A'$ een basis is van $\mathbf{S}$.

BEWIJS. Zij $\mathcal{B}$ de collectie van alle onafhankelijke uitbreidingen van B die bevat zijn in $B \cup A$, geordend door inclusie. Omdat $B \in \mathcal{B}$, $\mathcal{B} \neq \emptyset$. Bovendien is $\mathcal{B}$ gesloten onder verenigingen van ketens; want, zij $\mathcal{C} \subseteq \mathcal{B}$ een keten. Als $\bigcup \mathcal{C}$ niet onafhankelijk is, dan is er een $D \in \mathcal{D}$ zo dat $D \subseteq \bigcup \mathcal{C}$. Laat D' een eindige deelverzameling zijn van D die tot $\mathcal{D}$ behoort. Voor elke $d \in D'$ is er een verzameling $C_d \in \mathcal{C}$ zo dat $d \in C_d$. De keten $\{C_d \mid d \in D'\}$ is eindig, en heeft dus een grootste element C_{d^*} . Dan $D' \subseteq C_{d^*}$, in tegenspraak met de onafhankelijkheid van de elementen van $\mathcal{B}$.

Volgens het Lemma van Zorn bevat $\mathcal{B}$ een maximaal element M . Als $a \in A$, dan $a \sim M$. Anders gezegd, $A \subseteq \tilde{M}$; dus volgens (§1:6), $S = \tilde{A} \subseteq \tilde{M}$, i.e. M is een voortbrengende verzameling. Omdat $M \in \mathcal{B}$ is M ook onafhankelijk. Neem $A' = M \setminus B$. $\square$

GEVOLG 6. In een globaal finitaire afhankelijkheidsruimte is elke onafhankelijke verzameling bevat in een basis.

BEWIJS. Zij $\langle S, \mathcal{D} \rangle$ een globaal finitaire afhankelijkheidsruimte, en $B \subseteq S$ onafhankelijk: pas de stelling toe met $A = S$. $\square$

GEVOLG 7. In een globaal finitaire afhankelijkheidsruimte omvat elke voortbrengende verzameling een basis.

BEWIJS. Zij $\langle S, \mathcal{D} \rangle$ een globaal finitaire afhankelijkheidsruimte, en $A \subseteq S$ een voortbrengende verzameling: pas de stelling toe met $B = \emptyset$. $\square$

Beide gevolgen impliceren

GEVOLG 8. Elke globaal finitaire afhankelijkheidsruimte heeft een basis.

In §7 staan voorbeelden beschreven van afhankelijkheidsruimten zonder bases.

Omdat een basis een voortbrengende verzameling is, hebben we meteen ook:

GEVOLG 9 (Graczyńska). Zij A een basis in een globaal finitaire afhankelijkheidsruimte $\mathbf{S} = \langle S, \mathcal{D} \rangle$, en B onafhankelijk in $\mathbf{S}$. Dan is er een verzameling $A' \subseteq A$ zo dat $B + A'$ een basis is van $\mathbf{S}$.

Graczyńska's bewering, in [G], dat dit de stelling van Hughes is, is niet correct: de clou van die stelling is dat $|B + A'| = |A|$, en dat is hier niet gegarandeerd.

De basisexistentistelling heeft ook een minder triviaal gevolg:

STELLING 4. Globaal finitaire afhankelijkheidsruimten zijn ook lokaal finitair.

BEWIJS. Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een globaal finitaire afhankelijkheidsruimte. Neem $D \in \mathcal{D}$ willekeurig. Laat $\mathcal{E} := \{E \in \mathcal{D} \mid E \subseteq D \text{ en } E \text{ is eindig}\}$, en $T := \bigcup \mathcal{E}$. Uit Lemma 3(f) volgt dat het voldoende is te laten zien dat $T = D$.

De afhankelijkheidsruimte $\mathbf{T} = \langle T, \mathcal{D} \cap \mathcal{P}T \rangle \leq \mathbf{S}$ is globaal (zelfs lokaal) finitair, en heeft dus (gevolg 8) een basis A . Laat $T := X + A$. Stel dat $D \setminus T \neq \emptyset$; zeg

$$D = \hat{d} + X + A + Y.$$

Omdat A een basis is voor $\mathbf{T}$, is er voor elke $x \in X$ een verzameling $E_x \subseteq A$ zo dat $\hat{x} + E_x \in \mathcal{D}$. Omdat ook $d \notin E_x$, is er volgens (trans) een verzameling $C \subseteq A + Y$ zo dat $\hat{d} + C \in \mathcal{D}$. Omdat $\mathbf{S}$ globaal finitair is, is er een eindige verzameling $E \in \mathcal{D}$ zo dat $E \subseteq \hat{d} + C$. Omdat $E \subseteq D$, $E \subseteq T$; dus $E \subseteq A$. Dat is echter in strijd met de onafhankelijkheid van A ; het is dus onmogelijk dat $D \setminus T \neq \emptyset$. $\square$

We concluderen dat in dit geval het onderscheid tussen *globaal* en *lokaal* schijn was: we kunnen eenvoudig spreken van *finitaire* afhankelijkheidsruimten.

We besluiten met een stelling over eindig voortgebrachte afhankelijkheidsruimten.

STELLING 5. Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte. Als $\mathbf{S}$ een eindige voortbrengende verzameling heeft, dan is er een $n \in \mathbb{N}$ zo dat

- (a) $\mathbf{S}$ een basis heeft van machtigheid n ;
- (b) elke deelverzameling van S met meer dan n elementen afhankelijk is;
- (c) $\mathcal{D} \leq_1 n + 1$.

BEWIJS. (a) Zij V een voortbrengende verzameling van eindige machtigheid m . Als V niet onafhankelijk is, zeg $v \in V$ en $v \sim V \setminus \hat{v}$, dan is $V \setminus \hat{v}$ een kleinere voortbrengende verzameling. Zo voortgaande vind je op den duur een basis $B \subseteq V$ van machtigheid $n \leq m$.

(b) Als A onafhankelijk is, dan is er (Stelling 2) een injectie $\varphi: A \setminus B \rightarrow B \setminus A$; dan is $\varphi \cup 1_{A \cap B}$ een injectie van A in B : dus $|A| \leq n$.

(c) Zij $\mathcal{E} := \{D \in \mathcal{D} \mid |D| \leq n + 1\}$. Vanzelfsprekend geldt dan $\mathcal{E} \leq_1 \mathcal{D}$. Voor de omkering, stel $s \in D \in \mathcal{D}$. Als $|D| \leq n + 1$ zijn we meteen klaar. Neem anders $Y \subseteq D \setminus \hat{s}$ van machtigheid n . Zij $D = \hat{s} + X + Y$. Voor elke $x \in X$ is $\hat{x} + Y$ afhankelijk, volgens (b); er is dus een verzameling $Y_x \subseteq Y$ zo dat $\hat{x} + Y_x \in \mathcal{D}$. Volgens (trans) is er dan een verzameling $Y' \subseteq Y$ zo dat $\hat{s} + Y' \in \mathcal{D}$. Omdat $|\hat{s} + Y'| \leq n + 1$, $\hat{s} + Y' \in \mathcal{E}$, en $s \in \hat{s} + Y' \subseteq D$. $\square$

§6. RANG

Waar ze van toepassing is, rechtvaardigt de Uitwisselingsstelling de definitie van de *rang* van een afhankelijkheidsruimte als de kardinaliteit van een basis. Die kardinaliteit is namelijk uniek bepaald:

GEVOLG 10. Zij $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte met bases A en B . Als er een met $\mathcal{D}$ lokaal equivalente afhankelijkheidsbasis $\mathcal{D}'$ bestaat zo dat $A \setminus B$ en $B \setminus A$ beide een $\mathcal{D}'$ -maximerende welordening hebben, dan $|A| = |B|$.

BEWIJS. In de beschreven omstandigheden garandeert Gevolg 2 het bestaan van een injectie $\varphi: B \setminus A \rightarrow A \setminus B$ zo dat $B + ((A \setminus B) \setminus \text{Im } \varphi)$ een basis is. Maar B is al een basis, dus $(A \setminus B) \setminus \text{Im } \varphi = \emptyset$. Dus $A \setminus B = \text{Im } \varphi$, en omdat φ een injectie is,

$$|B \setminus A| = |A \setminus B|.$$

Dus $|A| = |A \cap B| + |A \setminus B| = |A \cap B| + |B \setminus A| = |B|$. $\square$

VOORBEELD I, hervat. Als een module S over een integriteitsgebied de directe som $T \oplus V$ is van een torsiemodule T en een vrije module V , dan is de rang van S de kardinaliteit van een vrij voortbrengende verzameling $X \subseteq V$ (cf. [K, §19] en [Hun, IV§2]).

De rang van de vectorruimte $\mathbb{Q}^\omega$ is $2^{\aleph_0}$. Want, laat X een basis zijn; zeg $|X| = \mathfrak{m}$. Er zijn oneindige onafhankelijke verzamelingen, dus $\mathfrak{m} \geq \aleph_0$. Voor elke $s \in \mathbb{Q}^\omega$ bestaan $n \in \mathbb{N}$ en eindige rijtjes $x: n \rightarrow X$ en $k: n \rightarrow \mathbb{Q}$ zo dat

$$s = k_0 x_0 + \dots + k_{n-1} x_{n-1}.$$

Dus

$$|\mathbb{Q}^\omega| \leq \sum_{n=0}^{\infty} |(\mathbb{Q} \times X)^n| = \sum_{n=0}^{\infty} (\aleph_0 \cdot \mathfrak{m})^n = \sum_{n=0}^{\infty} \mathfrak{m}^n = \aleph_0 \cdot \mathfrak{m} = \mathfrak{m};$$

en omdat $X \subseteq \mathbb{Q}^\omega$, $\mathfrak{m} = |\mathbb{Q}^\omega| = 2^{\aleph_0}$.

Een soortgelijke berekening toont aan dat de rang van de abelse groep $\mathbb{Z}^\omega$ eveneens $2^{\aleph_0}$ is. Laat opnieuw X een basis zijn, van machtigheid $\mathfrak{m} (\geq \aleph_0)$. Voor elke $s \in \mathbb{Z}^\omega$ bestaan $n \in \mathbb{Z}_+$ en eindige rijtjes $x: n \setminus \hat{0} \rightarrow X$ en $k: n \rightarrow \mathbb{Z}$ zo dat

$$k_0 \neq 0 \text{ en } k_0 s = k_1 x_1 + \dots + k_{n-1} x_{n-1}.$$

Gelijke rijtjes bepalen hetzelfde element, want als

$$k_0 s = k_1 x_1 + \dots + k_{n-1} x_{n-1} \text{ en } k_0 s' = k_1 x_1 + \dots + k_{n-1} x_{n-1},$$

waar $k_0 \neq 0$, dan $k_0(s - s') = 0$; omdat $\mathbb{Z}^\omega$ maar één element van eindige orde heeft, volgt daaruit dat $s = s'$. Dus

$$|\mathbb{Z}^\omega| \leq \sum_{n=0}^{\infty} |\mathbb{Z} \times (\mathbb{Z} \times X)^n| = \sum_{n=0}^{\infty} \aleph_0 \cdot (\aleph_0 \cdot \mathfrak{m})^n = \sum_{n=0}^{\infty} \aleph_0 \cdot \mathfrak{m}^n = \aleph_0 \cdot \aleph_0 \cdot \mathfrak{m} = \mathfrak{m};$$

dus $\mathfrak{m} = |\mathbb{Z}^\omega| = 2^{\aleph_0}$.

Noteren we de rang van een module M als $\text{rang}(M)$.

PROPOSITIE 5. Zij M een module over een integriteitsgebied R . Als M' een submodule is van M , dan $\text{rang}(M) = \text{rang}(M/M') + \text{rang}(M')$.

BEWIJS. Laat M een R -module zijn van rang $\mathfrak{k}$, en $M' \leq M$ van rang $\mathfrak{m}$. Laat $X \subseteq M$ en $X' \subseteq M'$ bases zijn; dan $|X| = \mathfrak{k}$ en $|X'| = \mathfrak{m}$. We mogen aannemen dat $X' \subseteq X$. Mocht dat namelijk niet zo zijn, dan bestaat er op grond van Propositie 3(a) en Gevolg 4 een injectie $\varphi: X' \setminus X \rightarrow X \setminus X'$ zo dat $X' + ((X \setminus X') \setminus \text{Im } \varphi)$ een basis is, en kunnen we X vervangen door $X' + ((X \setminus X') \setminus \text{Im } \varphi)$.

Laat $x_1, \dots, x_n$ ($n \geq 1$) onderscheiden elementen zijn van $X \setminus X'$. Als

$$k_1 x_1 + \dots + k_n x_n \in M', \quad \text{met } k_1, \dots, k_n \in R \setminus \hat{0},$$

dan zijn er, op grond van de maximaliteit van X' , $y_1, \dots, y_m \in X'$ ($m \geq 1$) en $r, s_1, \dots, s_m \in R \setminus \hat{0}$ zo dat

$$r(k_1 x_1 + \dots + k_n x_n) + s_1 y_1 + \dots + s_m y_m = 0;$$

maar dat is strijdig met de onafhankelijkheid van X . Dus $\{x + M' \mid x \in X \setminus X'\}$ is onafhankelijk in M/M' .

Als $w \in M \setminus X$, dan zijn er, wegens maximaliteit van X , onderscheiden

$$x_1, \dots, x_n \in X \setminus X' \text{ en } y_1, \dots, y_m \in X' \text{ (} n, m \geq 0 \text{)}$$

en $r, k_1, \dots, k_n, s_1, \dots, s_m \in R \setminus \hat{0}$ zo dat

$$rw + k_1 x_1 + \dots + k_n x_n + s_1 y_1 + \dots + s_m y_m = 0.$$

Dan $rw + k_1x_1 + \dots + k_nx_n \in M'$. Dus $\{x + M' \mid x \in X \setminus X'\}$ is *maximaal* onafhankelijk in M/M' . $\square$

VOORBEELD III. Zij A een abelse groep van rang $\mathfrak{k}$, met torsie-ondergroep T_A ; stel dat A de interne directe som is van T_A en een collectie $\mathcal{B}$ van oneindige cyclische ondergroepen van A . Als B een transversaal is van $\mathcal{B}$ die 0 niet bevat, dan is B een basis van A . Dus $|\mathcal{B}| = \mathfrak{k}$; dat wil zeggen dat de directe som-voorstelling

$$A = \sum \mathcal{B} \oplus T_A$$

uniek is. (De voorstelling van een groep G als een directe som — meestal onder aanvullende voorwaarden — is *uniek* wanneer

$$G = \sum_{i \in I} H_i = \sum_{j \in J} K_j$$

impliceert dat er een bijectie $\varphi: I \xrightarrow{\sim} J$ bestaat zo dat voor alle $i \in I$, $H_i \cong K_{\varphi(i)}$ — cf. [MMT, §5.1].) Men kan zich nu afvragen of een voorstelling van T_A als een directe som van onontbindbare eindige cyclische groepen ook uniek zou zijn.

Onontbindbare eindige cyclische groepen zijn cyclische groepen van priem-macht-orde. Stel dat een torsiegroep T een directe som is van dergelijke groepen. Dan is T ook de directe som van haar maximale primaire ondergroepen; die som-voorstelling is intrinsiek bepaald omdat ieder element tot hoogstens één maximale primaire ondergroep behoort, en dus uniek. Voor een bevestigend antwoord op onze vraag is het dus voldoende om te bewijzen, voor een willekeurig priemgetal p , dat de voorstelling van een abelse p -groep als een directe som van onontbindbare cyclische groepen uniek is.

Zij G een abelse p -groep, en $r \in \mathbb{Z}_+$. Definieer

$$G' := \{g \in G \mid p^r g = 0\};$$

$$H := \text{Sg}^{G'} \{h \in G' \mid p^{r-1}h = 0 \text{ of } \exists g \in G. h = pg\}.$$

Dan $H \leq G' \leq G$, en H bestaat uit de sommen $h + k$ waarin $p^{r-1}h = 0$ en k een p -voud is; G'/H is een $\mathbb{Z}_p$ -module. Definieer een afhankelijkheidsbasis in G'/H als in Voorbeeld I. Zij $\mathcal{A}$ een collectie cyclische ondergroepen van G van orde p^r , en $\mathcal{B}$ een collectie cyclische ondergroepen van G waarvan de orde een andere macht van p is, zo dat

$$(1) \quad G = \sum \mathcal{A} \oplus \sum \mathcal{B}.$$

Laat B een transversaal zijn van $\mathcal{B}$ die van ieder element van $\mathcal{B}$ een voortbrenger bevat.

1° Het is evident dat $\{b + H \mid b \in B\}$ een voortbrengende verzameling is van G'/H .

2° Die verzameling is ook onafhankelijk, en dus een basis van G'/H . Stel namelijk dat voor onderscheiden $b_1, \dots, b_m \in B$ ($m \geq 1$) en $k_1, \dots, k_m \in \mathbb{Z}_p$ geldt dat

$$x := k_1b_1 + \dots + k_mb_m \in H.$$

Dan $x = h + k$, met $p^{r-1}h = 0$ en k een p -voud. Voor zekere $g \in G$ geldt dus

$$p^{r-1}k_1b_1 + \dots + p^{r-1}k_mb_m = p^r g.$$

Ieder element van G is echter de som van een unieke verzameling van representanten van de verschillende summanden in (1); dus $g = 0$, en a fortiori

$$k_1 = \dots = k_m = 0.$$

We concluderen dat $|\mathcal{B}|$ de rang is van G'/H . Die rang is onafhankelijk van de somvoorstelling (1); dat betekent dat het aantal der summanden van orde p^r in

elke directe som-voorstelling van G hetzelfde is, en a fortiori dat de voorstelling (1) modulo isomorfie van de summanden uniek is.

Uitwisseling is niet de enige methode om de toekenbaarheid van een uniek bepaalde rang te bewijzen. Een andere methode is te vinden in [K, §19] en [H, IV§2]. In abstracto komt die op het volgende neer.

STELLING 6. Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte die niet eindig wordt voortgebracht en waarin $\mathcal{D} \leq |A|$ voor iedere voortbrengende verzameling A . Als A en B voortbrengende verzamelingen zijn in $\mathbf{S}$, dan omvat B een voortbrengende verzameling van machtigheid hoogstens $|A|$. In het bijzonder hebben alle bases dezelfde kardinaliteit.

BEWIJS. Laat A en B voortbrengende verzamelingen zijn. Voor elke $a \in A$ bestaat een verzameling $B_a \subseteq B$ zo dat

$$B_a = \hat{a} \text{ of } \hat{a} + B_a \in \mathcal{D},$$

dus $a \sim B_a$. Omdat $\mathcal{D} \leq |A|$ mogen we aannemen dat $|B_a| \leq |A|$. Zij $B' = \bigcup_{a \in A} B_a$. Dan $B' \subseteq B$ en $\forall a \in A. a \sim B'$, dus B' brengt S voort. Bovendien $|B'| \leq |A| \cdot |A| = |A|$. Omdat een basis een minimale voortbrengende verzameling is, volgt de laatste bewering direct. $\square$

GEVOLG 11. Zij $\mathbf{S} = \langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte, met $\mathcal{D} \leq \aleph_0$. Dan bestaat er een kardinaalgetal $\mathfrak{m}$ zo dat iedere voortbrengende verzameling een voortbrengende verzameling omvat van machtigheid $\mathfrak{m}$. In het bijzonder hebben alle bases machtigheid $\mathfrak{m}$.

BEWIJS. Zij A een voortbrengende verzameling van minimale kardinaliteit. Als A eindig is, zeg $|A| = m$, dan is A een basis. Volgens Stelling 5 is $\mathbf{S}$ dan finitair. Gevolg 7 impliceert nu dat elke voortbrengende verzameling van $\mathbf{S}$ een basis omvat; uit Stelling 5 en de minimaliteit van A volgt dat die basis precies m elementen heeft. Als A oneindig is, dan passen we Stelling 6 toe. $\square$

§7. NIET-FINITAIRE AFHANKELIJKHEIDSRUIMTEN

De twee volgende voorbeelden, uit [HugII], illustreren de pathologie van niet-finitaire afhankelijkheidsruimten.

IV. Zij S oneindig en $\mathcal{D} = \{D \subseteq S \mid |D| = \aleph_0\}$. Dan is $\langle S, \mathcal{D} \rangle$ een afhankelijkheidsruimte, want stel dat

$$\hat{d} + X + Y \in \mathcal{D} \text{ \& \& } \forall x \in X (\hat{x} + E_x \in \mathcal{D} \text{ \& } d \notin E_x);$$

dan is ofwel Y oneindig, en dan $\hat{d} + Y \in \mathcal{D}$; of $X \neq \emptyset$, en als $x \in X$, dan is E_x oneindig, dus $\hat{d} + E_x \in \mathcal{D}$. Deze ruimte heeft geen basis, want $A \subseteq S$ brengt S voort dan en slechts dan als A oneindig is, en is onafhankelijk dan en slechts dan als A eindig is. Een aftelbare voortbrengende verzameling impliceert dus niet het bestaan van een basis, zulks in contrast met Stelling 5(a).

V. Twee verzamelingen A en B zijn *bijna gelijk*, notatie $A \approx B$, als $|A| = |B|$ en

$$|A \setminus B| = |B \setminus A| < \aleph_0.$$

Bijna-gelijkheid is evident symmetrisch. De relatie is ook transitief: als $A \approx B$ en $B \approx C$, dan $|A| = |C|$; het kost wat meer moeite om in te zien dat $A \setminus C$ en $C \setminus A$ eindig en gelijkmatig zijn. Laat $m := |A \setminus B|$ en $n := |B \setminus C|$. We stipuleren verder:

$$a = |A \setminus (B \cup C)|, b = |B \setminus (A \cup C)|, d = |(A \cap C) \setminus B|, e = |(B \cap C) \setminus A|, \\ c = |C \setminus (A \cup B)|, f = |(A \cap B) \setminus C|.$$

Dan $m = a + d = b + e$ en $n = b + f = c + d$. Dus $f - d = c - b$; dus

$$f + m - d = c + m - b;$$

dus $a + f = c + e$. Maar $a + f = |A \setminus C|$, en $c + e = |C \setminus A|$.

Laat $\mathcal{P}$ een collectie zijn van paarsgewijs disjuncte oneindige deelverzamelingen van S . We definiëren

$$\mathcal{C} = \{C \subseteq S \mid \exists P \in \mathcal{P}. C \approx P\},$$

en $\mathcal{D} = \{\hat{x} + C \mid C \in \mathcal{C} \text{ en } x \in S \setminus C\}$. Als $y \in D \in \mathcal{D}$, dan is er een $C \in \mathcal{C}$ zo dat $D = \hat{y} + C$, want stel $D = \hat{x} + C'$, met $C' \approx P \in \mathcal{P}$: dan $C = (C' \setminus \hat{y}) + \hat{x}$, dus

$$C \approx C' \approx P.$$

PROPOSITIE 6. $\langle S, \mathcal{D} \rangle$ is een afhankelijkheidsruimte.

BEWIJS. Stel $\hat{d} + X + Y \in \mathcal{D}$ & $\forall x \in X (\hat{x} + E_x \in \mathcal{D} \text{ & } d \notin E_x)$; als $X = \emptyset$, dan $\hat{d} + Y \in \mathcal{D}$; als $x \in X$, dan $\hat{d} + E_x \in \mathcal{D}$. $\square$

PROPOSITIE 7. X is een basis in $\langle S, \mathcal{D} \rangle$ dan en slechts dan als $X \in \mathcal{C}$.

BEWIJS. X is een voortbrengende verzameling dan en slechts dan als

$$\forall s \in S \setminus X \exists C \subseteq X. \hat{s} + C \in \mathcal{D}.$$

Dan $C \in \mathcal{C}$. Als $X \supset C$, dan is X afhankelijk; dus als X een basis is, dan $X = C$. $\square$

In het bijzonder zijn de elementen van $\mathcal{P}$ bases; die hebben niet per se dezelfde kardinaliteit.

Als $\mathcal{P}$ een oneindige collectie van aftelbaar oneindige verzamelingen is, dan bestaat $\mathcal{D}$ uit aftelbaar oneindige verzamelingen. Elke transversaal T van $\mathcal{P}$ is onafhankelijk, want voor iedere $D \in \mathcal{D}$ is er een $P \in \mathcal{P}$ zo dat $D \cap P$ oneindig is. Maar T kan niet worden uitgebreid tot een basis, volgens Propositie 7.

Aan de welordeningsvoorwaarden van Gevolg 2 kan in deze beide gevallen kennelijk net worden voldaan.

Literatuur

- [G] Ewa Graczyńska: Dependence spaces. arXiv:0906.1132v1, juni 2009.
- [HugI] N.J.S Hughes: Steinitz' Exchange Theorem for infinite bases. *Compositio Mathematica* 15 (1962-1964), 113-118.
- [HugII] *Eiusdem*, Steinitz' Exchange Theorem for infinite bases II. *Compositio Mathematica* 17 (1965-1966), 152-155.
- [Hun] Thomas W. Hungerford: *Algebra*. Tweede druk, Springer 1980.
- [K] A.G. Kurosh: *Theory of groups*. Engelse bewerking van Теория Групп door K.A. Hirsch. New York 1955/1960.
- [MMT] Ralph N. McKenzie, George F. McNulty & Walter F. Taylor: *Algebras, lattices, varieties*. Vol. I. Wadsworth, Belmont 1987.
- [S] Ernst Steinitz: Bedingt konvergente Reihen und konvexe Systeme (Teil I). *Journal für die Reine und Angewandte Mathematik* 143 (1913), 128-175.

Appendices

A. Hughes formuleerde voorbeeld IV technisch eleganter, maar, wellicht, minder inzichtelijk. Noem twee verzamelingen A en B *verwant*, notatie $A \equiv B$, als er een bijectie $\varphi: A \rightarrow B$ bestaat zo dat $\{a \in A \mid \varphi(a) \neq a\}$ eindig is. Merk op dat in dat geval ook φ^{-1} een bijectie is, en $\{b \in B \mid \varphi^{-1}(b) \neq b\}$ eindig. Dus verwantschap is symmetrisch. De relatie is ook transitief: als $A \equiv B$ en $B \equiv C$, via respectievelijk φ en ψ , dan is $\psi \circ \varphi$ een bijectie, en $a \neq \psi(\varphi(a))$ impliceert

$$a \neq \varphi(a) \vee (a = \varphi(a) \ \& \ a \neq \psi(a)),$$

dus $\{a \in A \mid \psi(\varphi(a)) \neq a\}$ is eindig.

De begrippen *verwant* en *bijna gelijk* zijn equivalent:

PROPOSITIE. $A \equiv B \Leftrightarrow A \approx B$.

BEWIJS. ($\Rightarrow$) Zij $V := \{a \in A \mid \varphi(a) \neq a\}$ en $W := \{b \in B \mid \varphi^{-1}(b) \neq b\}$. Dan

$$|V| = |\{(b, a) \in \varphi \mid b \neq a\}| = |W|.$$

Merk nu op dat

$$(1) \quad A \setminus B = V \setminus W.$$

Want: ($\subseteq$) Als $a \in A \setminus B$, dan $\varphi(a) \neq a$ omdat $\varphi(a) \in B$, en $a \notin W$ omdat $a \notin B$.

($\supseteq$) Zij $a \in V \setminus W$. Dan $a \in A$ en $\varphi(a) \neq a$; als $a \in B$, dan is ook $\varphi^{-1}(a)$ gedefinieerd, en uit $\varphi(a) \neq a$ volgt $a \neq \varphi^{-1}(a)$, dus $a \in W$, quod non. Dus $a \in A \setminus B$.

Wegens symmetrie geldt ook

$$(2) \quad B \setminus A = W \setminus V.$$

$$\text{Dus } |A \setminus B| = |V \setminus W| = |V| - |V \cap W| = |W| - |V \cap W| = |W \setminus V| = |B \setminus A|.$$

($\Leftarrow$) Laat ψ een bijectie zijn van $A \setminus B$ op $B \setminus A$; dan is $\varphi := \psi \cup 1_{A \cap B}$ een bijectie van A op B ; en $\{a \in A \mid \varphi(a) \neq a\}$ is $A \setminus B$, dus eindig. $\square$

B. Zijn er *natuurlijke* niet-finitaire afhankelijkheidsruimten? Ik heb er geen kunnen vinden. Graczyńska geeft voorbeelden buiten de abelse groepen-sfeer; in zover als ik ze zo kon herformuleren dat ik ze begreep, waren ze triviaal.