K. P. Hart
Faculteit EWI
TU Delft
Postbus 5031
2600 GA Delft
k.p.hart@tudelft.nl

De stelling van Van der Waerden

Tachtig jaar geleden verscheen in het Nieuw Archief voor Wiskunde een artikel van de hand van B. L. van der Waerden. Achter de onschuldige titel "Beweis einer Baudetschen Vermutung" ging een stelling schuil die nog steeds zijn invloed in de Wiskunde doet gelden.

Wie in MathSciNet naar 'Van der Waerden's theorem' zoekt vindt zo'n 130 recensies. Op een paar na gaan die artikelen over de stelling die Van der Waerden in 1927 in het Nieuw Archief voor Wiskunde publiceerde [17]. Die stelling luidt.

Behauptung (l,k)**.** Es existiert eine Zahl $n = n(l,k)$ mit der folgenden Eigenschaft: Ist die endliche zahlenfolge 1, 2, ..., n in k fremde klassen eingeteilt, so liegt in einer dieser Klassen eine arithmetische Progression von l Zahlen.

De stelling kwam voort uit pogingen een door Baudet uitgesproken vermoeden te bewijzen: *als l een natuurlijk getal is en de verzameling der natuurlijke getallen wordt in twee klassen verdeeld dan bevat één van die verzamelingen een rekenkundig rijtje van lengte l.* In [18] beschreef Van der Waerden hoe hij ("na de lunch") samen met Artin en Schreier aan het probleem ging werken. Het geval $l = 2$ is flauw: men hoeft slechts naar de verzameling $\{1,2,3\}$ te kijken om te zien dat bij een tweedeling één klasse zeker twee elementen heeft. Na wat proberen bleek dat bij elke tweedeling van $\{1,2,3,4,5,6,7,8,9\}$ één van de klassen zeker een rekenkundig rijtje van lengte 3 bevat (de verdeling $\bigl\{\{1,2,4,5\},\{3,4,6,8\}\bigr\}$ laat zien dat 9 minimaal is). Schreier opperde toen dat zoiets wellicht altijd mogelijk was: bij elke l bestaat een getal $W(l)$ zó dat bij elke tweedeling van $\{1,\ldots,W(l)\}$ één van de klassen een rekenkundig rijtje van lengte l bevat. Duidelijk is dat het bestaan van $W(l)$ voor alle l het vermoeden van Baudet impliceert; het omgekeerde is ook waar, dit volgt uit de compactheid van het het topologische product $\{0,1\}^{\mathbb{N}}$. Immers, zij $l \in \mathbb{N}$ en neem aan dat voor elke N een opdeling $\{A_N, B_N\}$ van $\{1,2,\ldots,N\}$ bestaat zó dat in beide klassen geen rekenkundige rij ter lengte l bestaat. Men verkrijgt zo een rij punten $(x_N)_N$ in $\{0,1\}^{\mathbb{N}}$, waarbij $x_N(n) = 0$ als $n \in A_n$ of $n > N$ en $x_N(n) = 1$ als $n \in B_N$. Deze rij heeft een convergente deelrij met limiet x en in de door x bepaalde verdeling van $\mathbb{N}$ bevat geen der klassen een rekenkundige rij ter lengte l, hetgeen strijdt met Baudet's vermoeden. Een argument als dit, waarbij een eindige versie van een bewering uit een oneindige versie wordt afgeleid (of omgekeerd) heet, om voor de hand liggende redenen, een *compactheidsargument*.

Met de waarden $W(2) = 3$ en $W(3) = 9$ in de hand ging men op zoek naar $W(4)$ en, algemeen, naar een methode om $W(l)$ uit $W(l-1)$ te maken, of beter: uit het bestaan van $W(l-1)$ het bestaan van $W(l)$ af te leiden — zoals later zal blijken geven de gangbare bewijzen grove overschattingen van de optimale waarden van de $W(l)$. Artin bedacht toen dat als het bestaan van $W(l)$ voor alle l zou zijn aangetoond men ook het bestaan van $W(l,k)$ kan aantonen, waarbij $W(l,k)$ als $W(l)$ gedefinieerd is, maar dan voor verdelingen in k klassen, dus $W(l) = W(l,2)$. Immers, zij $N = W\bigl(W(l)\bigr)$ en verdeel $\{1,\ldots,N\}$ in vier klassen: A_1, A_2, A_3 en A_4. Er is een rekenkundige rij ter lengte $W(l)$ binnen $A_1 \cup A_2$ of binnen $A_3 \cup A_4$ en binnen die rij is er een van lengte l die in slechts één van de vier klassen ligt. Conclusie: $W(l,4) \leqslant W\bigl(W(l)\bigr)$. Op deze manier vind men bovengrenzen voor $W(l,2^k)$ voor alle k en l en daarmee ook voor $W(l,k)$ voor alle waarden van k en l.

Met deze extra parameter in de stelling richtte de aandacht zich weer op l; de strategie werd om met inductie naar l te bewijzen dat $W(l,k)$ bestaat voor *alle* k. Het voordeel hiervan is dat de inductieaanname veel sterker geworden is dan in het oorspronkelijke probleem. Merk ook op dat $W(2,k)$ eenvoudig te bepalen is: $W(2,k) = k+1$.

Van der Waerden schreef zijn artikel in termen van klassen en equivalente getallen ($a \sim b$ als a en b in dezelfde klasse zitten); ik zal het veelal over kleuren hebben en een rekenkundige rij waarin alle termen dezelfde kleur hebben *monochroom* noemen. Dit sluit meer aan bij het algemene spraakgebruik in de wereld van de Ramsey-achtige stellingen.

Artin kwam op het idee om naar blokken opeenvolgende natuurlijke getallen te kijken. Een kleuring van de natuurlijke getallen met twee kleuren genereert namelijk andere kleuringen: voor elke n wordt $\{n, n+1, \ldots, n+i-1\}$ in twee klassen verdeeld en dat kan op 2^i mogelijke manieren; op deze wijze krijgen we een kleuring van $\mathbb{N}$ met 2^i veel kleuren. Als men de verzameling $\{1, \ldots, W(l-1, 2^i) + i\}$ met twee kleuren kleurt krijgt men een rekenkundige rij A van lengte $l-1$ die slechts één van de 2^i afgeleide kleuren aanneemt; dat wil zeggen dat alle blokken $\{a, a+1, \ldots, a+i-1\}$ op één en dezelfde wijze gekleurd zijn. Daarmee is elke rekenkundige rij $\{a+j : a \in A\}$ monochroom geworden; men kan op deze manier dus grote hoeveelheden monochrome rekenkundige rijen genereren, van lengte $l-1$ weliswaar, maar toch ...

Van der Waerden wist hier goed gebruik van te maken bij het uiteindelijke bewijs. We laten zien hoe men een bovengrens voor $W(3,2)$ kan vinden. Net als in vele bewijzen uit de Ramseytheorie speelt ook hier het idee van een pre-monochrome verzameling een rol. We noemen een rekenkundige rij van lengte l *pre-monochroom* als het beginstuk van lengte $l-1$ monochroom is — het idee zal zijn dat door voldoende veel pre-monochrome rekenkundige rijen een monochroom diagonaaltje te trekken moet zijn.

We hebben de natuurlijke getallen met twee kleuren gekleurd, zeg rood en blauw. In elk drietal (opeenvolgende) getallen zijn er twee die dezelfde kleur hebben; dat impliceert dat in elk blok van vijf, $\{n, n+1, n+2, n+3, n+4\}$, een pre-monochroom rekenkundig rijtje ter lengte 3 zit: onder n, $n+1$, $n+2$ zijn er twee met dezelfde kleur en die zijn met $n+2$ of $n+3$ of $n+4$ tot een (zeker pre-monochroom) drietal uit te breiden. We nemen daarom hierboven $i = 5$ en vinden onder de getallen 1 tot en met $W(2, 2^5) = 33$ twee getallen a en b zó dat $\{a, a+1, a+2, a+3, a+4\}$ en $\{b, b+1, b+2, b+3, b+4\}$ exact dezelfde kleuring vertonen. Binnen die twee blokken kunnen we dan pre-monochrome rekenkundige rijtjes ter lengte 3 vinden en wel op dezelfde relatieve posities, om de gedachten te bepalen op posities 1, 2 en 3. Neem verder $c = b + (b-a)$, dan is $\{a, b, c\}$ een rekenkundige rij. Aangenomen dat $\{a+1, a+2, a+3\}$ niet al monochroom is kunnen we als volgt een monochroom 3-terms rekenkundig rijtje maken: bekijk $\{a+1, b+2, c+3\}$ en $\{a+3, b+3, c+3\}$, dit zijn rekenkundige rijtjes en allebei pre-monochroom: $a+1$ en $b+2$ zijn gelijkgekleurd, zeg rood, en $a+3$ en $b+3$ ook, dus blauw. Dan is òf $\{a+1, b+2, c+3\}$ monochroom rood òf $\{a+3, b+3, c+3\}$ monochroom blauw.

Met een scherp oog is hier het begin van een afschatting van $W(l,2)$ te ontwaren: de blokken moeten allereerst $W(l-1,2)$ lang zijn, om monochrome rijtjes ter lengte $l-1$ te kunnen maken. Het verschil tussen twee opeenvolgende termen in zo'n rij is niet groter dan $(W(l-1,2)-1)/(l-2)$, dus blokken ter lengte $M = W(l-1,2) + (W(l-1,2)-1)/(l-2)$ bevatten zeker pre-monochrome rijen ter lengte l. Daarna moeten we tot $W(l-1, 2^M) + (M-1)$ gaan om een rekenkundige rij ter lengte $l-1$ van blokken met dezelfde kleuring te kunnen vinden; daar moet nog $(W(l-1, 2^M) - 1)/(l-2)$ bij om een extra blok toe te kunnen voegen. Voor $W(3,2)$ komt men zo uit op $33 + 4 + 32 = 69$ als bovengrens; dat is een stuk groter dan de optimale waarde van 9 maar dat is het probleem met een algemeen geldige redenering: die geeft zelden scherpe grenzen.

Het bovenstaande is een vereenvoudiging van de uitleg uit het artikel [18], dat zeer lezenswaardig is en waarin ook een geval met *drie* kleuren wordt uitgelegd. Dat laatste laat zien dat men bij k kleuren kan verwachten $k-1$ diagonaliseerstappen te moeten doen en dit heeft weer grote gevolgen voor de afschattingen van $W(l,k)$, we komen daar later nog op terug. Het oorspronkelijke artikel [17] uit 1927 is ook nog steeds de moeite waard, met pen en papier bij de hand leest het makkelijk weg.

1. Grote verzamelingen

In 1917 had Schur [13] een stelling bewezen die erg op die van Van der Waerden lijkt:

Stelling 1. Bij elke k bestaat een getal $S(k)$ met de eigenschap dat indien $\{1, \ldots, S(k)\}$ in k klassen wordt verdeeld (ten minste) één van die klassen een oplossing van $x + y = z$ bevat.

Er is echter een verschil. Van der Waerden's stelling is, zogezegd, translatie-invariant: als A willekeurig lange rekenkundige rijtjes bevat dan doet $A+1$ dat ook. De stelling van Schur is niet translatie-invariant: de even getallen bevatten wel een oplossing van $x + y = z$, de oneven getallen niet. De invariantie van de stelling van Van der Waerden bracht Erdős en Turán er toe te vragen of er een notie van 'grote verzameling' bestaat zó dat elke 'grote' verzameling willekeurig lange rekenkundige rijtjes bevat en, natuurlijk, dat bij een eindige opdeling van de natuurlijke getallen ten minste één klasse 'groot' is. Een mogelijke kandidaat was 'positieve bovendichtheid' (positive upper density). Voor een deelverzameling A van $\mathbb{N}$ definieert men deze grootheid als volgt:

$$\bar{d}(A) = \limsup_{n \to \infty} \frac{|A \cap \{1, 2, \ldots, n\}|}{n}$$

Het door Erdős en Turán uitgesproken vermoeden was: als $\bar{d}(A) > 0$ dan bevat A willekeurig lange rekenkundige rijen.

In 1952 bewees Roth [11, 12] dat zulke verzamelingen rekenkundige rijen van lengte 3 bevatten. In 1969 verbeterde Szemerédi [15] dit tot lengte 4 en in 1975 bewees hij, tenslotte, het algemene geval [16]. Ik zal me niet aan een samenvatting van de bewijzen wagen; de lengte van het tweede artikel van Szemerédi zou een indicatie moeten zijn van de moeite die het bewijs gekost heeft.

2. Dynamische systemen

In 1981 verscheen het boek [4] waarin Furstenberg een algemene aanpak van combinatorische stellingen door middel van dynamische systemen uiteenzette.

Het basisidee is dat van *herhaling* of *recurrentie*. Een dynamisch systeem bestaat uit een verzameling X en één of meer zelfafbeeldingen van X. Om over recurrentie te kunnen spreken moet X wel van een structuur voorzien zijn; meestal is X voorzien van een metriek of van een maat en zijn de zelfafbeeldingen respectievelijk continu of meetbaar. De stelling van Van der Waerden volgt uit de Meervoudige-Recurrentiestelling van Birkhoff die, ironisch genoeg, vrijwel gelijktijdig bewezen is.

Stelling 2 (Birkhoff's Meervoudige-Recurrentiestelling). Zij X een compacte metrische ruimte en laat T_1, T_2, $\dots$, T_l een (eindig) aantal continue zelfafbeeldingen van X zijn die onderling commuteren. Dan bestaat er een meervoudig-recurrent punt voor deze afbeeldingen, dat wil zeggen een punt x_0 met daarbij een (stijgende) rij $\langle n_k\rangle_k$ natuurlijke getallen zó dat $\lim_k T_i^{n_k}x_0 = x_0$ voor elke i.

Laat nu $\mathbb{N}$ gekleurd zijn met de kleuren 1 tot en met k. In plaats van te bewijzen dat er willekeurig lange rekenkundige rijtjes van één bepaalde kleur bestaan laten we zien dat er willekeurig lange monochrome rekenkundige rijen bestaan; dit is natuurlijk een equivalente bewering.

De ruimte waar we mee werken is $X = \{1, 2, \dots, k\}^{\mathbb{N}}$, voorzien van de standaardmetriek d, gegeven door $d(x, y) = 2^{-n(x,y)}$, waarbij $n(x, y) = \min\{n : x(n) \neq y(n)\}$ als $x \neq y$; en $d(x, x) = 0$ voor alle x. Het is welbekend dat (X, d) compact is. We gebruiken alleen de opschuifafbeelding $T : X \to X$, gedefinieerd door $(Tx)(n) = x(n + 1)$ — elk punt wordt naar links geschoven en de eerste coördinaat wordt vergeten. Elke kleuring van $\mathbb{N}$ met k kleuren bepaalt een punt in X en omgekeerd bepaalt elk punt een kleuring. De stelling van Van der Waerden krijgt daarmee de volgende formulering: voor elk punt x en elke l bestaan a en d in $\mathbb{N}$ zó dat $x(a) = x(a+d) = \cdots = x(a+ld)$. Merk op dat $x(a) = (T^a x)(0)$, $x(a + d) = (T^d T^a x)(0)$, $\dots$, en $x(a + ld) = (T^{ld} T^a x)(0)$ en dat, in het algemeen, $u(0) = v(0)$ gelijkwaardig is met $d(u, v) < 1$; we zoeken dus een a en een d zó dat de punten $T^a x$, $T^{a+d}x$, $\dots$, $T^{a+ld}x$ onderling dichter dan 1 bij elkaar liggen.

We passen de stelling van Birkhoff toe op de afsluiting Y van de baan van x, dus $Y = \mathrm{cl}\{T^n x : n \in \mathbb{N}\}$, met de eerste l machten van T als de familie afbeeldingen. Die machten commuteren onderling en hun beperkingen tot Y zijn zelfafbeeldingen van Y. We krijgen dus een punt $y_0 \in Y$ en een rij $\langle n_k\rangle_k$ natuurlijke getallen zó dat $T^{in_k}y_0 \to y_0$ voor elke i. Kies een k zo groot dat, met $d = n_k$, de punten $T^{id}y_0$ $(i \leqslant l)$ allemaal dichter dan $\frac{1}{4}$ bij y_0 liggen; hun onderlinge afstand is dan kleiner dan $\frac{1}{2}$. Omdat T continu en l eindig is kunnen we een $\delta > 0$ vinden met de eigenschap dat voor elke $y \in X$ met $d(y, y_0) < \delta$ alle afstanden $d(T^{id}y, T^{id}y_0)$ kleiner dan $\frac{1}{4}$ zijn. Kies nu een a zó dat $d(T^a x, y_0) < \delta$, dan geldt $d(T^{a+id}x, y_0) < \frac{1}{2}$ voor alle i; al die punten hebben dus allemaal onderlinge afstand kleiner dan 1, hetgeen we wilden bewerkstelligen.

De stelling van Szemerédi volgt op gelijksoortige wijze uit een maattheoretische versie van de meervoudige-recurrentiestelling.

Stelling 3. Zij $(X, \mathcal{B}, \mu)$ een maatruimte en laat T_1, T_2, $\dots$, T_l een (eindig) aantal maatbewarende zelfafbeeldingen van X zijn die ondeling commuteren. Dan bestaat voor elke $A \in \mathcal{B}$ van positieve maat een $n \in \mathbb{N}$ zó dat $\mu(A \cap T_1^{-n}[A] \cap \cdots T_l^{-n}[A]) > 0$.

Deze stelling wordt toegepast in het product $\{0, 1\}^{\mathbb{Z}}$, voorzien van de producttopologie, met dezelfde schuifafbeelding als boven. We nemen als X de afsluiting van de baan van χ_S, waar S de gegeven verzameling van positieve bovendichtheid is. Op X is een (Borel-)maat μ te definiëren die invariant is onder T en die bovendien de verzameling $A = \{x \in X : x(0) = 1\}$ postieve maat geeft (dit is zeker niet triviaal en gebruikt dat de bovendichtheid van S niet nul is). We gebruiken weer de eerste l machten van T en vinden een d en een punt x in A met de eigenschap dat $T^{id}x \in A$ voor alle i. Dat betekent dat $x(0) = x(d) = x(2d) = \cdots = x(ld) = 1$. Er is dan een punt in de baan van χ_S, zeg $T^a\chi_S$, die op de coördinaten 0, d, $\dots$, ld met x overeenkomt. Maar dat betekent dat $\{a, a + d, \dots, a + ld\} \subseteq S$.

3. Ultrafilters, halfgroepen en idempotenten

Er is geen 'oneindige' versie van de stelling van Van der Waerden in de zin dat er een kleuring van $\mathbb{N}$ is met twee kleuren zonder *oneindig lange* monochrome rekenkundige rijen. Het bewijs is niet zo moeilijk. Er zijn namelijk maar aftelbaar veel van deze rijen, voor elk tweetal natuurlijke getallen één: bij (a, d) hoort $\{a + id : i \in \mathbb{N}\}$ en omgekeerd, als A een rekenkundige rij is hoort nemen we de eerste twee termen a en b, dan hoort A bij $(a, b - a)$.

Neem één of andere aftelling $\{(a_k, d_k) : k \in \mathbb{N}\}$ en kleur $\mathbb{N}$ als volgt, recursief, met twee kleuren rood en blauw. Begin met (a_0, d_0), schrijf $N_0 = a_0 + d_0$ en kleur het interval $[0, N_0]$ zodanig dat a_0 rood wordt en $a_0 + d_0$ blauw. Bij de stap van $k - 1$ naar k bekijken we (a_k, d_k) en kiezen we een i_k zó dat $N_{k-1} < a_k + i_k d_k$. We zetten $N_k = a_k + (i_k + 1)d_k$ en kleuren het interval $(N_{k-1}, N_k]$ zodanig dat $a_k + i_k d_k$ rood wordt en $a_k + (i_k + 1)d_k$ blauw. Op deze manier raakt geen enkele *oneindige* rekenkundige monochroom.

Het is een nuttige oefening eens na te gaan waarom het compactheidsprincipe wel bij het vermoeden van Baudet werkte maar niet bij het maken van oneindig lange monochrome rekenkundige rijen.

In het boek [7] wordt een stelling besproken die, net als de stelling van Van der Waerden, het bestaan van willekeurig grote monochrome verzamelingen van een speciale soort garandeert. Om deze, aan Folkman toegeschreven, stelling te kunnen formuleren hebben we wat notatie nodig. Als S een deelverzameling van $\mathbb{N}$ is dan noteren we met $\sum(S)$ de verzameling van alle sommen van eindige deelverzamelingen van S, dus $\sum\bigl(\{2^n : n \geqslant 0\}\bigr) = \mathbb{N}$ en $\sum\bigl(\{10^n : n \geqslant 0\}\bigr) = \{1, 10, 11, 100, 101, 110, 111, \ldots\}$.

Stelling 4. Als $\mathbb{N}$ met eindig veel kleuren gekleurd wordt dan zijn er willekeurig grote *eindige* verzamelingen S waarvoor $\sum(S)$ monochroom is.

Het bewijs in [7] maakt direct gebruik van de getallen $W(l,k)$ om een grens aan te geven waaronder de gewenste verzameling reeds te vinden is. Dat bewijs is waarschijnlijk niet sterk genoeg om een oneindige verzameling S op te leveren waarvoor $\sum(S)$ monochroom is.

Dat zo'n verzameling toch te vinden is werd in [9] door Hindman bewezen.

Stelling 5. Als $\mathbb{N}$ met eindig veel kleuren gekleurd wordt dan is er een oneindige verzameling S waarvoor $\sum(S)$ monochroom is.

Kort na het verschijnen van Hindman's artikel gaf Glazer een bewijs dat zeer invloedrijk is geweest. Het maakte gebruik van rekenkundige eigenschappen van de Čech-Stonecompactificatie, $\beta\mathbb{N}$, van de (discrete) topologische ruimte $\mathbb{N}$.

De punten van de ruimte $\beta\mathbb{N}$ zijn de *ultrafilters* op $\mathbb{N}$. Een ultrafilter is een maximaal filter en een *filter* op $\mathbb{N}$ is een niet-lege familie deelverzamelingen $\mathcal{F}$ met de volgende eigenschappen: 1) $\emptyset \notin \mathcal{F}$; 2) als $F, G \in \mathcal{F}$ dan $F \cap G \in \mathcal{F}$ en 3) als $F \in \mathcal{F}$ en $G \supseteq F$ dan $G \in \mathcal{F}$. De familie van alle filters is partieel geordend door inclusie en ultrafilters zijn maximaal ten opzichte van die ordening. Een belangrijke karakterizering van ultrafilters is de volgende: $(*)$ als $F \cup G \in \mathcal{F}$ dan $F \in \mathcal{F}$ of $G \in \mathcal{F}$.

Voor elk punt n in $\mathbb{N}$ is $\hat{n} = \{F : n \in F\}$ een ultrafilter en elk ultrafilter met een niet-lege doorsnede is van deze vorm. Wie andere, *vrije*, ultrafilters wil maken moet het Lemma van Zorn toepassen op de familie van alle filters die groter zijn dan het *co-eindige filter* $\mathcal{COF} = \{F : \mathbb{N} \setminus F \text{ is eindig}\}$. Dat iets Keuzeaxioma-achtigs nodig zal zijn wordt geïllustreerd door de volgende observatie van Sierpiński: uit een vrij ultrafilter $\mathcal{U}$ is als volgt een niet-Lebesgue-meetbare verzameling te maken: definieer een afbeelding φ van $\mathcal{P}(\mathbb{N})$ naar $[0,1]$ door $\varphi(A) = \sum_{n \in A} 2^{-n}$. Het beeld $\varphi[\mathcal{U}]$ is dan niet Lebesgue-meetbaar.

In het vervolg van deze paragraaf staan de letters u, v en w voor ultrafilters op $\mathbb{N}$, de punten van $\beta\mathbb{N}$ dus. Het idee van het bewijs van Glazer is om een optelling van ultrafilters definiëren. Dat gaat als volgt. Eerst spreken we af dat $X - n$ een afkorting is voor $\{m : m + n \in X\}$, voor $X \subseteq \mathbb{N}$ en $n \in \mathbb{N}$. Vervolgens definiëren we de *som* $u + v$ van twee ultrafilters u en v door:

$$X \in u + v \Leftrightarrow \{n : X - n \in v\} \in u.$$

Met gaat gemakkelijk na dat dit voor elementen van $\mathbb{N}$ niets nieuws oplevert: $\widehat{m+n} = \hat{m} + \hat{n}$. Ook geldt $\hat{n} + u = u + \hat{n}$ voor alle $u \in \beta\mathbb{N}$ en alle $n \in \mathbb{N}$. In het algemeen geldt $u + v = v + u$ *niet*, maar met enig puzzelen kan men wel aantonen dat de associatieve wet *wel* geldt: $(u+v)+w = u+(u+v)$. Op deze manier is van $\beta\mathbb{N}$ dus een halfgroep gemaakt.

De cruciale opmerking in het bewijs van Glazer is nu de volgende: als u een vrij ultrafilter is dat voldoet aan $u + u = u$ (een *idempotent*) dan bestaat voor elke $U \in u$ een oneindige verzameling S met $\sum(S) \subseteq U$. Zodra men zo'n ultrafilter heeft is het bewijs van de stelling van Hindman rond: het ultrafilter bevat, dankzij eigenschap $(*)$, een monochroom element en daar hoort meteen een S als gevraagd bij.

Voor we het bestaan van een idempotent ultrafilter aantonen laten we eerst zien dat het de beweerde eigenschap heeft. Voor elk verzameling X noteren we $X^u = \{n : X - n \in u\}$; dankzij $u + u = u$ volgt dat $X^u \in u$ als $X \in u$. Neem nu $U_0 \in u$ en kies $s_1 \in U_0 \cap U_0^u$; definieer dan $U_1 = U_0 \cap (U_0 - s_1) \setminus \{s_1\}$, dan zijn U_1 en $U_1 - s_1$ deelverzameling van U_0 en $U_1 \in u$ natuurlijk. We gaan recursief verder: als U_i gevonden is kiezen we $s_{i+1} \in U_i \cap U_i^u$ en stellen we $U_{i+1} = U_i \cap (U_i - s_{i+1}) \setminus \{s_{i+1}\}$. De verzameling $S = \{s_i : i \in \mathbb{N}\}$ is als gewenst: men bewijst eenvoudig dat een eindige som met s_{i+1} als term van laagste index in U_i zit.

Om te bewijzen dat er inderdaad een idempotent ultrafilter is definiëren we een topologie op $\beta\mathbb{N}$: voor elke deelverzameling X van $\mathbb{N}$ schrijven we $\bar{X} = \{u \in \beta\mathbb{N} : X \in u\}$. De familie $\{\bar{X} : X \subseteq \mathbb{N}\}$ is een basis voor een topologie die van $\beta\mathbb{N}$ een compacte Hausdorff ruimte maakt waarin $\{\hat{n} : n \in \mathbb{N}\}$ een (aftelbare) dichte deelverzameling is.

We werken in de verzameling $\mathbb{N}^*$ van alle vrije ultrafilters. Deze verzameling is gesloten, dus compact, en ook gesloten onder de optelling. Het is dus een compacte halfgroep waarin voor elke v de afbeelding $u \mapsto u+v$ continu.is. Dit nu is genoeg om het bestaan van een idempotent aan te tonen. Aanwijzing: pas het Lemma van Zorn toe op de familie van alle niet-lege gesloten verzamelingen F die voldoen aan $F + F \subseteq F$; een *minimaal* element van deze familie bestaat uit één punt.

Wat heeft dit alles met de stelling van Van der Waerden te maken? Welnu, die kan ook met dit soort methoden bewezen worden, ook al is er geen oneindige versie van. In [1] wordt bewezen dat elk element van een *minimale* idempotent willekeurig lange rekenkundige rijen bevat. De minimaliteit is ten opzichte van de partiële ordening $\leqslant$, gedefinieerd door: $u \leqslant v$ dan en slechts dan als $v = u + v = v + u$. Natuurlijk moet vastgesteld worden dat minimale idempotenten bestaan; dat bewijs vergt een diepere studie van de verrassend rijke algebraïsche structuur van de halfgroep $\beta\mathbb{N}$. Het boek [10] biedt hierin een goede inleiding.

Interessant is dat hier de dynamische aanpak en die via ultrafilters bij elkaar komen in de notie van 'centrale verzameling' ('central set'). Een centrale verzameling bevat zowel willekeurig lange rekenkundige rijen als $\sum(S)$ voor een oneindige verzameling S. De definitie van centrale verzameling, volgens Furstenberg [4], is als volgt: $C \subseteq \mathbb{N}$ is centraal als er een dynamisch systeem (X, T) bestaat met daarin een punt x, een uniform recurrent punt y nabij x en een omgeving U van y zó dat $C = \{n : T^n x \in U\}$. Een punt y is *uniform recurrent* als voor elke omgeving U de verzameling $A = \{n : T^n \in U\}$ *syndetisch* is, wat betekent dat $\mathbb{N} = \bigcup_{n \leqslant N}(A - n)$ voor zekere N. Twee punten x en y zijn nabij ('proximal') als $\liminf_n d(T^n x, T^n y) = 0$. Een centrale verzameling kan met behulp van ultrafilters als volgt gekarakteriseerd worden: een verzameling is centraal dan en slechts dan als deze tot een minimale idempotent behoort.

4. Grenzen voor $W(l, k)$

Zodra het bestaan van een getal als $W(l, k)$ is bewezen wil men natuurlijk een idee krijgen van zijn optimale waarde. De bewijzen van de stelling van Van der Waerden die we tot nu toe gezien hebben geven niet echt veel informatie over de getallen $W(l, k)$. Met enig puzzelwerk kan men uit het bewijs van Van der Waerden zelf bovengrenzen voor de $W(l, k)$ distilleren maar door de impliciete dubbele inductie waarin grote machten van k een rol spelen komt men op zeer grove afschattingen, zoals reeds te zien is aan de uit het bewijs verkregen ongelijkheid $W(3, 2) \leqslant 69$.

Hier is nog een verschil tussen Schur en Van der Waerden te zien: Schur gaf expliciet een eenvoudige bovengrens voor zijn $S(k)$, de oorspronkelijke formulering van zijn stelling was namelijk als volgt.

Stelling 6. Verteilt man die Zahlen 1, 2, ..., N irgendwie auf m Zeilen, so müssen, sobald $N > m!e$ wird, in mindestens einer Zeile zwei Zahlen vorkommen, deren Differens in derzelben Zeile enthalten ist.

Met andere woorden: $S(m) \leqslant m!e$. In het bewijs in [13] leidt de aanname dat N een 'slechte' kleuring toelaat onverbiddelijk naar de ongelijkheid $N < m!e$.

In 1988 publiceerde Shelah een artikel, [14], met een veelzeggende titel waarin hij een nieuw combinatorisch bewijs van de stelling van Van der Waerden gaf. Dat bewijs is met inductie naar l, waarbij k vastgehouden wordt. Het levert bovengrenzen voor de getallen $W(l, k)$ die spectaculair kleiner waren dan de tot dan toe bekende.

In het boek [7] wordt $W(l, k)$ tweemaal naar boven afgeschat; eerst door het oorspronkelijke bewijs van Van der Waerden te analyseren en daarna door dat van Shelah na te lopen. Om aan te geven wat de verschillen zijn definieren we een hierarchie van functies van $\mathbb{N}$ naar $\mathbb{N}$. Om te beginnen definiëren we $f_1(x) = 2x$; daarna definieren we, recursief, functies f_m als volgt: $f_{m+1}(1) = 1$ en $f_{m+1}(n+1) = f_m\big(f_m(n)\big)$. In woorden: $f_{m+1}(n)$ ontstaat door f_m herhaaldelijk, n maal, op 1 toe te passen. Dus $f_2(n) = 2^n$ (herhaaldelijk verdubbelen) voor alle n en

$$f_3(n) = 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}\Big\}n$$

(herhaaldelijk machtverheffen). Voor de functie f_4 schiet conventionele notatie te kort. Desalniettemin zijn de functies f_n nog 'klein'; ze behoren tot de klasse van zogeheten *primitief recursieve functies*. De definitie van deze notie, die uit afkomstig is uit de recursietheorie en de theorie van berekenbaarheid, kan men in vrijwel elk boek over logica terugvinden maar, gelukkig, voor onze doeleinden hebben we aan de functies f_n genoeg: een functie f is primitief recursief dan en slechts dan als er een m is zó dat $f = \mathcal{O}(f_m)$. Dit betekent dat de functie f_ω, gedefinieerd door $f_\omega(n) = f_n(n)$, niet primitief recursief is.

Het bewijs van Van der Waerden zelf leidt tot een bovengrens voor $W(l, 2)$ die *niet* primitief recursief is; de grens ligt tussen $f_\omega(l-2)$ en $f_\omega(l)$. Het bewijs van Shelah laat ziet dat $W(\cdot, 2) = \mathcal{O}(f_4)$, voorwaar een stevige verbetering maar nog steeds ontzagwekkend groot.

5. Analytische technieken

We hebben gezien dat de stelling van Van der Waerden op diverse manieren bewezen is: combinatorisch, dynamisch, verzameling-theoretisch en ook analytisch: het bewijs van Roth gaat uit van een zo lang mogelijke rij $u_1 < u_2 < \cdots < u_k$ in een interval $\{1, 2, \ldots, N\}$ *zonder* rekenkundig rijtje ter lengte 3. Een analyse van de functie

$$f(\alpha) = \sum_{i=1}^{k} e^{2\pi i \alpha u_k}$$

leidt tot een bewijs dat $k = o(N)$ en daarmee tot het geval $l = 3$ van de stelling van Szemerédi. De argumenten van Szemerédi, voor $l = 4$ en later voor alle l waren weer combinatorisch van aard. In [5] en [6] gaf Gowers analytische bewijzen van de stelling van Szemerédi. Met gebruikmaking van discrete Fouriertransformaties van functies op de groep $\mathbb{Z}/N\mathbb{Z}$ wist hij de grenzen van Shelah voor $W(l, 2)$ terug te brengen tot

$$2^{2^{2^{2^{2^{l+9}}}}}$$

(dat zijn vijf tweeën). Hier gaapt overigens nog een vrij groot gat: in [7] worden ondergrenzen voor $W(l, 2)$ gegeven die 'slechts' van exponentiële orde zijn.

6. De priemgetallen

Positieve bovendichtheid is niet de enige manier om 'grote' van 'kleine' verzamelingen te onderscheiden. Een andere, veelgebruikte, manier is met behulp van de harmonische reeks. Laten we een verzameling A *harmonisch groot* noemen als $\sum_{n \in A} \frac{1}{n}$ divergeert en *harmonisch klein* als die reeks convergeert. Een nog openstaand probleem is: bevat elke harmonisch grote verzameling willekeurig lange rekenkundige rijen? Een positief antwoord zou onder meer impliceren dat de verzameling P van de priemgetallen willekeurig lange rekenkundige rijen bevat. Dat laatste nu is voorzover ik weet het nieuwste resultaat over de stelling van Van der Waerden: Green en Tao [8] hebben bewezen dat binnen P inderdaad willekeurig lange rekenkundige rijen te vinden zijn.

Merk op dat $\bar{d}(P) = 0$, dit volgt uit de priemgetallenstelling. Als we, zoals gebruikelijk, $|P \cap \{1, 2 \ldots, n\}|$ afkorten met $\pi(n)$ dan geldt

$$\lim_{n\to\infty} \frac{\pi(n)\ln n}{n} = 1$$

en dus geldt $\bar{d}(P) = \lim \frac{1}{\ln n} = 0$. Merkwaardig genoeg berust het bewijs van Green en Tao toch op de stelling van Szemerédi. Uit de samenvatting van [8] halen we de volgende korte beschrijving. De stelling van Szemerédi kan overgebracht worden naar een klasse van verzamelingen die voldoende willekeurig zijn: als een verzameling A voldoende 'willekeurig' is en $B \subseteq A$ heeft positieve bovendichtheid *ten opzichte van* A dan bevat B willekeurig lange rekenkundige rijen. Vervolgens kan men P zien als deelverzameling van zo'n 'willekeurige' verzameling en wel van positieve relatieve bovendichtheid. De techinsche details, en met name de definitie van "willekeurig', vindt men in [8].

Tot slot

In [2] schreef De Bruijn een informatief commentaar op [17] (aanbevolen) waarin met gepaste trots gewag gemaakt werd van het feit dat in het blad van onze vereniging toch maar mooi "one of the most elegant pieces of mathematics ever produced" verschenen is. De daarop volgende zin is, zoals dit artikel heeft laten zien, zeer profetisch geweest: "The influence of this little paper, now 50 years old, has not yet come to an end." Ik denk dat we die '50' nu gerust door '80' kunnen vervangen.

Referenties

[1] Vitaly Bergelson en Neil Hindman, *Nonmetrizable topological dynamics and Ramsey theory*, Transactions of the American Mathematical Society **320** (1990), 293–320

[2] N. G. de Bruijn, *B. L. van der Waerden on arithmetic progressions in sets of integers. Commentary*, in E. M. J. Bertin, H. J. M. Bos en A. W. Grootendorst (eds) *Two decades of mathematics in the Netherlands*, Mathematisch Centrum, Amsterdam, (1978), 110–124.

[3] P. Erdős en P. Turán, *On some sequences of integers*, Journal of the London Mathematical Society **11** (1936), 261–264

[4] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory.* M. B. Porter Lectures, Princeton University Press, Princeton, N.J., (1981)

[5] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geometric and Functional Analysis **8** (19980, 529–551

[6] W. T. Gowers, *A new proof of Szemerédi's theorem*, Geometric and Functional Analysis **11** (2001), 465–588

[7] Ronald L. Graham, Bruce L. Rothschild and Joel H. Spencer, *Ramsey Theory* (second edition), John Wiley & Sons Inc., New York (1990)

[8] Ben Green en Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, `arXiv:math.NT/0404188`

[9] N. Hindman, *Finite sums from sequences within cells of a partition of* $\mathbb{N}$, Journal of Combinatorial Theory. Series A **17** (1974), 1–11

[10] Neil Hindman en Dona Strauss, *Algebra in the Stone-Čech compactification*, de Gruyter Expositions in Mathematics 27, Walter de Gruyter & Co., Berlin, 1998

[11] Klaus Roth, *Sur quelques ensembles d'entiers*, C. R. Acad. Sci. Paris **234** (1952), 388–390

[12] Klaus Roth, *On certain sets of integers*, Journal of the London Mathematical Society **28** (1953), 104–109

[13] I. Schur, *Über die Kongruenz* $x^m + y^m = z^m \pmod p$, Jahresbericht der Deutschen Mathematiker-Verein **25** (1917), 114-117

[14] Saharon Shelah, *Primitive reursive bounds for Van der Waerden numbers*, Journal of the American Mathematical Society **1** (1988), 683–697

[15] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Mathematicae Academiae Scientiarum Hungaricae **20** (1969), 89–114

[16] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica **27** (1975), 199–245

[17] Bartel L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde **15** (1927), 212–216.

[18] Bartel L. van der Waerden, *How the proof of Baudet's conjecture was found.* 1n *Studies in Pure Mathematics*, ed. L. Mirsky. Academic Press, New York, (1971), 251–260.