Bachelorscriptie

Som- en verschilverzamelingen

Merlijn Staps

28 januari 2014

Inhoudsopgave

Inleiding **3**

1 Somverzamelingen en verschilverzamelingen **5**

1.1 Definities en triviale observaties 5

1.2 Twee lemma's van Ruzsa 7

2 Verzamelingen met een kleine somverzameling **8**

2.1 Verzamelingen met $\sigma(A) < 2$ 8

2.2 Verzamelingen met kleine somverzameling in $\mathbb{Z}$ en $\mathbb{Z}/p\mathbb{Z}$ 11

2.3 De stelling van Freiman 13

3 De ongelijkheid van Plünnecke **16**

4 Kleine somverzamelingen en kleine verschilverzamelingen zijn equivalent **20**

4.1 Approximate groups 20

4.2 De ongelijkheid $\delta(A) \leq \sigma(A)^2$ 22

4.3 De ongelijkheid $\sigma(A) \leq \delta(A)^2$ 25

5 Conclusie **28**

Referenties **31**

Inleiding

Deze scriptie gaat over som- en verschilverzamelingen. Gegeven een verzameling A is de *somverzameling* van A de verzameling van getallen die te schrijven zijn als de som van twee elementen van A. Als bijvoorbeeld $A = \{-8, 1, 4, 13, 40\}$, dan is de somverzameling van A de verzameling $\{-16, -7, -4, 2, 5, 8, 14, 17, 26, 32, 41, 44, 53, 80\}$. Het element -7 zit bijvoorbeeld in deze somverzameling omdat $-7 = -8 + 1$ terwijl 26 in deze somverzameling zit omdat $26 = 13 + 13$. Deze verzameling noteren we met $A + A$. Hoeveel elementen $A + A$ heeft ten opzichte van A drukken we uit met de grootheid $\sigma(A)$. Deze is gedefinieerd als het quotiënt $|A + A|/|A|$ van het aantal elementen in de somverzameling van A en het aantal elementen in A. In ons voorbeeld hebben $A + A$ en A respectievelijk 14 en 5 elementen, dus dan is $\sigma(A) = \frac{14}{5} = 2.8$. Het blijkt dat $A + A$ altijd minstens zoveel elementen heeft als A, dus er geldt $\sigma(A) \geq 1$.

De somverzameling van de meeste verzamelingen bevat veel meer elementen dan de oorspronkelijke verzameling. Voor die verzamelingen geldt dus dat $\sigma(A)$ veel groter is dan 1. Er zijn echter ook verzamelingen waarvan de somverzameling niet veel groter is dan de oosrpronkelijke verzameling. Bekijk bijvoorbeeld de verzameling $B = \{2, 3, 4\}$. Deze heeft als somverzameling $B + B = \{4, 5, 6, 7, 8\}$, dus er geldt $\sigma(B) = \frac{5}{3} < 2$. De somverzameling van B heeft dus minder dan twee keer zo veel elementen als B zelf. Er zijn ook verzamelingen A waarvoor $|A + A| = |A|$. Bekijk bijvoorbeeld de verzameling A hierboven maar dan als verzameling van getallen modulo 15, dus als deelverzameling van $\mathbb{Z}/15\mathbb{Z}$. Dan is $A = \{1, 4, 7, 10, 13\}$ (want modulo 15 is $-8 \equiv 7$ en $40 \equiv 10$), met als somverzameling $A + A = \{2, 5, 8, 11, 14\}$. In dit geval heeft $A + A$ dus precies zoveel elementen als A. In beide voorbeelden van verzamelingen met een kleine σ heeft deze verzameling een speciale structuur: zowel de verzameling $\{2, 3, 4\}$ als de verzameling $\{1, 4, 7, 10, 13\}$ bestaat uit een rekenkundige rij. In deze scriptie stellen we de vraag wat er in algemene zin gezegd kan worden over de structuur van verzamelingen waarvan de somverzameling klein is.

Naast somverzamelingen hebben we ook verschilverzamelingen: gegeven een verzameling A is de *verschilverzameling* van A de verzameling $A - A$ van getallen die te schrijven zijn als het verschil van twee elementen uit A. Net zoals bij somverzamelingen kunnen we vragen welke verzamelingen een kleine verschilverzameling hebben. Van de twee verzamelingen hierboven die een kleine somverzameling hebben, kan worden nagegaan dat ze ook geen al te grote verschilverzameling hebben. Dit blijkt in het algemeen waar te zijn: verzamelingen met een kleine somverzameling hebben ook een kleine verschilverzameling en vice versa. Een tweede probleem waar we naar kijken is hoe precies we dit verband aan kunnen geven: als we een

verzameling hebben met een kleine somverzameling, hoe groot kan de verschilverzameling dan zijn? En andersom, als we een verzameling hebben met een kleine verschilverzameling, hoe groot kan de somverzameling dan zijn?

In hoofdstuk 1 presenteren we de belangrijkste definities. Verder behandelen we daar een aantal begrippen en lemma's die later van pas komen.

Hoofdstuk 2 gaat over verzamelingen met een kleine somverzameling. We kijken eerst naar verzamelingen A zodat $\sigma(A) < 2$. We behandelen verder de stelling van Freiman, die grofweg zegt dat elke verzameling met een kleine somverzameling op een rekenkundige rij lijkt.

De laatste twee hoofdstukken gaan over het verband tussen som- en verschilverzamelingen. In hoofdstuk 3 bewijzen we een ongelijkheid die zegt dat een verzameling met een kleine somverzameling ook kleine "hogere orde"-somverzamelingen heeft: als er weinig getallen te schrijven zijn als som van twee elementen uit A, kunnen er ook niet al te veel getallen zijn die te schrijven zijn als een som van, zeg, vijf elementen van A. We kijken verder naar een aantal toepassingen van deze ongelijkheid.

Voor het schrijven van de drie eerste hoofdstukken heb ik vooral gebruik gemaakt van een recent artikel van Sanders [10] en het boek *Additive combinatorics* van Tao en Vu [11], het standaardwerk op dit vakgebied.

Hoofdstuk 4 begint met het geven van expliciete ongelijkheden die laten zien dat verzamelingen met een kleine somverzameling ook een kleine verschilverzameling hebben en vice versa: er blijkt te gelden dat $\delta(A) \leq \sigma(A)^2$ en dat $\sigma(A) \leq \delta(A)^2$, waarbij δ het analoog van σ voor verschilverzamelingen is. We behandelen ook het begrip "approximate group" (in het Nederlands te vertalen als "bijna-groep"): dit is een andere manier om een verzameling met kleine som- en verschilverzameling te beschrijven. De laatste twee paragrafen van dit hoofdstuk gaan verder in op de ongelijkheid $\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2$. We onderzoeken of de exponenten $\frac{1}{2}$ en 2 in deze ongelijkheid optimaal zijn. We presenteren ook een paar nieuwe resultaten: het gelijkheidsgeval van deze ongelijkheid en gelijkheidsgevallen van een aantal resultaten uit hoofdstuk 3.

De scriptie is geschreven onder begeleiding van Gunther Cornelissen.

1 Somverzamelingen en verschilverzamelingen

1.1 Definities en triviale observaties

Gegeven een verzameling A is de bijbehorende *somverzameling* de verzameling

$$\{a+b : a,b \in A\}$$

van getallen die te schrijven zijn als de som van twee getallen uit A (die niet verschillend hoeven te zijn). Deze verzameling noteren we met $A+A$. Analoog heeft A een *verschilverzameling*

$$A-A = \{a-b : a,b \in A\}.$$

Uiteraard kunnen we dit alleen doen als A een verzameling is waarop een optelling is gedefinieerd. Om ervoor te zorgen dat zowel de som als het verschil van elk tweetal elementen van A gedefinieerd is, veronderstellen we dat A een deelverzameling is van een gegeven abelse groep Z (waarvan we de groepsoperatie als optelling noteren). Wanneer Z eindig voortgebracht is kan Z geschreven worden als een eindig product van cyclische groepen $\mathbb{Z}/n\mathbb{Z}$ en $\mathbb{Z}$. We eisen dat de verzameling A eindig is en niet-leeg; hier gaan we in het vervolg altijd vanuit. Anders dan de groep Z die mogelijk oneindig is, komen we dus geen oneindige verzamelingen tegen.

We beginnen met een aantal observaties over de aantallen elementen $|A+A|$ en $|A-A|$ in de somverzameling en verschilverzameling van A. Merk op dat voor $a \in A$ de verzameling $a+A = \{a+b : b \in A\}$ bevat is in $A+A$. Hieruit volgt dat $|A+A| \geq |a+A| = |A|$. Verder geeft ieder paar elementen uit A aanleiding tot hoogstens één element van $A+A$. Dit leidt tot de ongelijkheid $|A+A| \leq |A|^2$. In het bijzonder is $A+A$ ook weer een eindige verzameling. Analoog geldt er $|A| \leq |A-A| \leq |A|^2$. De bovengrenzen zijn hier eenvoudig scherper te maken, zie lemma 1.2.

Voor twee deelverzamelingen A en B van Z definiëren we $A+B = \{a+b : a \in A, b \in B\}$ en $A-B = \{a-b : a \in A, b \in B\}$. Als generalisatie van de hierboven genoemde ongelijkheden hebben we het volgende lemma.

Lemma 1.1. *Er geldt dat* $\max(|A|,|B|) \leq |A \pm B| \leq |A||B|$.

Bewijs. Merk op op dat de afbeelding $\varphi : A \to A \pm B$ met $\varphi : a \mapsto a \pm b$ voor $b \in B$ injectief is. Daaruit volgt dat $|A| \leq |A \pm B|$. Analoog geldt $|B| \leq |A \pm B|$, dus $\max(|A|,|B|) \leq |A \pm B|$. Verder heeft $A \times B$ precies $|A||B|$ elementen, dus $|A \pm B| \leq |A||B|$ want dat is het aantal paren (a,b) met $a \in A$ en $b \in B$. □

Deze grenzen zijn in het algemeen scherp: zie lemma 2.1 voor het gelijkheidsgeval voor de ondergrens en merk op dat als we A en B zien als de deelverzamelingen $\{(a,0) : a \in A\}$ en $\{(0,b) : b \in B\}$ van $Z \times Z$ dat dan in de bovengrens gelijkheid geldt. In het geval van $A = B$ is het mogelijk om een kleinere bovengrens te geven:

Lemma 1.2. *Er geldt* $|A| \leq |A+A| \leq \frac{|A|(|A|+1)}{2}$ *en* $|A| \leq |A-A| \leq |A|^2 - |A| + 1$.

Bewijs. De ondergrenzen volgen uit lemma 1.1. Voor de eerste bovengrens merken we op dat dat $|A+A| \leq |A|^2$ omdat er $|A|^2$ paren elementen van A zijn. Voor elk paar (a,b) met $a \neq b$ tellen we zowel $a+b$ als $b+a$. Omdat er $\frac{|A|(|A|-1)}{2}$ zullke paren zijn, geldt er $|A+A| \leq |A|^2 - \frac{|A|(|A|-1)}{2} = \frac{|A|(|A|+1)}{2}$.
Voor de tweede bovengrens merken we weer op dat $|A-A| \leq |A|^2$ omdat er $|A|^2$ paren elementen van A zijn. Omdat het paar (a,a) voor iedere $a \in A$ als verschil $a-a=0$ geeft tellen we het element $0 \in A-A$ precies $|A|$ keer en dus $|A|-1$ keer te veel. Er geldt dus $|A-A| \leq |A|^2 - |A| + 1$. □

De grenzen in lemma 1.2 zijn scherp: voor een deelgroep van Z worden de ondergrenzen bereikt (zie ook gevolg 2.2) terwijl voor een verzameling $A = \{1, 2, \ldots, 2^n\} \subset Z = \mathbb{Z}$ de bovengrenzen worden bereikt.

Het is gebruikelijk om $|A+A|$ en $|A-A|$ te bekijken relatief ten opzichte het aantal elementen van A. We definiëren de *verdubbelingsconstante* van een verzameling A als $\sigma(A) = \frac{|A+A|}{|A|}$ en de *verschilconstante* als $\delta(A) = \frac{|A-A|}{2}$. Uit lemma 1.2 volgt dan dat $1 \leq \sigma(A) \leq \frac{|A|+1}{2}$ en $1 \leq \delta(A) \leq |A| - 1 + \frac{1}{|A|}$.

Een ander nuttig begrip is dat van de *symmetrieverzameling* van een verzameling A. Deze is voor $A \subset Z$ gedefinieerd als $\mathrm{Sym}(A) = \{h \in Z : A + h = A\}$. Zij $h \in \mathrm{Sym}(A)$ en kies een $a \in A$. Dan is $a+h$ bevat in A, dus $h \in A - a \subset A - A$.[1] Er geldt dus dat $\mathrm{Sym}(A) \subset A - A$. De volgende propositie geeft twee andere eigenschappen van $\mathrm{Sym}(A)$.

Propositie 1.3. *De symmetrieverzameling* $\mathrm{Sym}(A)$ *van* A *is een eindige deelgroep van* A *en* A *is te schrijven als een vereniging van nevenklassen van* $\mathrm{Sym}(A)$.

Bewijs. We gaan eenvoudig na dat $\mathrm{Sym}(A)$ een groep is door te controleren dat aan alle eisen is voldaan. Merk op dat als $a \in A$, dat dan $a + \mathrm{Sym}(A) \subset A$ (immers, $A + s = A$ voor $s \in \mathrm{Sym}(A)$, dus $a + s \in A$). We concluderen dat

$$A = \bigcup_{a \in A} (a + \mathrm{Sym}(A)).$$

[1] We schrijven $X \subset Y$ wanneer ieder element van X ook in Y zit (waarbij $X = Y$ dus ook mogelijk is). We schrijven $X \subsetneq Y$ wanneer $X \subset Y$ maar $X \neq Y$.

Dus A is bevat in een vereniging nevenklassen van $\mathrm{Sym}(A)$. Het is bovendien mogelijk om $a_1, \ldots, a_r \in A$ te kiezen zodat

$$A = \bigsqcup_{1 \leq i \leq r} (a_i + \mathrm{Sym}(A)),$$

waarbij we het symbool $\sqcup$ gebruiken om een disjuncte vereniging aan te geven. Hieruit volgt ook dat $\mathrm{Sym}(A)$ eindig is, want we zien dat $|\mathrm{Sym}(A)| \leq |A|$. □

1.2 Twee lemma's van Ruzsa

We presenteren nog twee handige gereedschappen: het bedekkingslemma van Ruzsa en de Ruzsa-driehoeksongelijkheid.

De Ruzsa-driehoeksongelijkheid [8] is het volgende algemene lemma:

Lemma 1.4 (Ruzsa-driehoeksongelijkheid)**.** *Voor $A, B, C \subset Z$ geldt*

$$|B||A - C| \leq |A - B||B - C|.$$

Bewijs. We bewijzen dit door een injectieve afbeelding $\varphi : B \times (A-C) \to (A-B) \times (B-C)$ te construeren. Kies eerst een afbeelding $\psi : (A - C) \to A \times C$ die een $y \in A - C$ naar een paar $(a, c) \in A \times C$ stuurt met $y = a - c$. Voor $(b, y) \in b \times (A - C)$ definiëren we nu $\varphi(b, y)$ als $(a - b, b - c)$, waarbij $(a, c) = \psi(y)$. Veronderstel dat $(a - b, b - c) = \varphi(b, y) = \varphi(b', y') = (a' - b', b' - c')$. Dan geldt $y = a - c = (a - b) + (b - c) = (a' - b') + (b' - c') = a' - c' = y'$. Dus $(a, c) = \psi(y) = \psi(y') = (a', c')$, dus $a = a'$. Omdat $a - b = a' - b'$ volgt er nu dat $b = b'$, dus $(b, y) = (b', y')$. We concluderen dat φ injectief is. □

De terminologie komt voort uit het feit dat de *Ruzsa-afstand* $d(A, B)$ gedefinieerd door

$$d(A, B) = \log \left(\frac{|A - B|}{\sqrt{|A||B|}} \right)$$

nu voldoet aan de driehoeksongelijkheid $d(A, C) \leq d(A, B) + d(B, C)$ voor $A, B, C \subset Z$. Dit volgt door de ongelijkheid in lemma 1.4 aan beide kanten te delen door $|B|\sqrt{|A||C|}$ en vervolgens aan beide kanten de logaritme te nemen.

We zeggen dat een verzameling A kan worden *bedekt* met k translaties van een verzameling B indien er een verzameling C bestaat met $|C| = k$ zodat $A \subset B + C$. Er geldt dus bijvoorbeeld dat A bedekt kan worden met $|A|$ translaties van $\mathrm{Sym}(A)$ (zie lemma 1.3). Merk op dat we

hier niet eisen dat ieder element van $B + C$ ook een element van A is, wat in dit voorbeeld wel het geval is. Het bedekkingslemma van Ruzsa [9] laat zien dat verzamelingen efficiënt kunnen worden bedekt met verschilverzamelingen.

Lemma 1.5 (Bedekkingslemma van Ruzsa)**.** *Zij $A, B \subset Z$. Dan kan A worden bedekt met hoogstens $\frac{|A+B|}{|B|}$ translaties van $B - B$.*

Bewijs. Schrijf $B_a = B + a$ voor $a \in A$. Er geldt dan $|B_a| = |B|$ en $B_a \subset A + B$. Neem een zo groot mogelijke verzameling $Y \subset A$ zodat de B_y disjunct zijn voor $y \in Y$. Dan geldt $|Y| \leq \frac{|A+B|}{|B|}$. We gaan bewijzen dat we A met $|Y|$ translaties van $B - B$ kunnen bedekken, door te bewijzen dat $A \subset B - B + Y$. Omdat Y maximaal is, is er voor iedere $a \in A$ een $y \in Y$ met $B_a \cap B_y \neq \emptyset$ (mogelijk $a = y$). Er zijn dan dus $b, b' \in B$ met $b + a = b' + y$, dus $a = b' - b + y \in B - B + Y$. Omdat a willekeurig is, geldt er dus $A \subset B - B + Y$, precies wat we wilden bewijzen. □

2 Verzamelingen met een kleine somverzameling

In dit hoofdstuk onderzoeken we verzamelingen met een kleine somverzameling, dus verzamelingen A waarvoor $\sigma(A)$ klein is. Dit zijn verzamelingen met veel "additieve structuur" [11]; er zijn in zo'n verzameling veel additieve relaties zoals $a+b = c+d$ tussen de elementen. In het bijzonder kijken we naar verzamelingen waarvoor $\sigma(A) < 2$.

2.1 Verzamelingen met $\sigma(A) < 2$

We zagen eerder al dat $\sigma(A) \geq 1$, dus een eerste stap is het klassificeren van die verzamelingen A waarvoor $\sigma(A) = 1$. Daartoe bewijzen we eerst het volgende algemenere lemma.

Lemma 2.1. *Er geldt $|A + B| = |A|$ dan en slechts dan als er een eindige deelgroep G van Z bestaat zodat B bevat is in een nevenklasse van G en A een vereniging van nevenklassen van G is.*

Bewijs. Stel dat $|A + B| = |A|$. We mogen aannemen aan dat $0 \in B$ omdat we B kunnen transleren. Dan is $A \subset A + B$, waaruit volgt dat $A = A + B$, dus $A + b = A$ voor $b \in B$. Dus is $B \subset \mathrm{Sym}(A)$. Vanwege propositie 1.3 is A een vereniging van nevenklassen van $G = \mathrm{Sym}(A)$, een eindige deelgroep van Z.
Als andersom $B = G + x$ voor zekere $x \in Z$ en A een vereniging van nevenklassen van G is,

schrijven we $A = \bigsqcup_{i=1}^{r}(G + y_i)$ met $y_i \in Z$ zodat de nevenklassen $G + y_i$ disjunct zijn voor $1 \leq i \leq r$. Er geldt dan

$$A + B = \{g + x + g' + y_i : g, g' \in G, 1 \leq i \leq r\} = \{h + x + y_i : h \in G, 1 \leq i \leq r\} = A + x$$

dus $|A + B| = |A|$. We hebben gebruikt dat $\{g + g' : g, g' \in G\} = G$. □

Op dezelfde manier kunnen de verzamelingen A en B zodat $|A - B| = |A|$ geklassificeerd worden; in het bijzonder zien we dus dat $|A+B| = |A|$ dan en slechts dan als $|A-B| = |A|$. Dit is ook direct uit lemma 2.1 af te leiden. Uit dit lemma volgt de beloofde klassificatie van verzamelingen A met $\sigma(A) = 1$:

Gevolg 2.2. *Er geldt $\sigma(A) = 1$ dan en slechts dan als A een nevenklasse is van een eindige deelgroep van Z.*

Bewijs. Pas lemma 2.1 toe met $B = A$. We zien dat dat $|A + A| = |A|$ dan en slechts dan als A bevat is in een nevenklasse van een deelgroep G van Z en A een vereniging is van nevenklassen van dezelfde groep; oftewel precies wanneer A een nevenklasse is van een eindige deelgroep van Z. □

We zien dus dat verzamelingen A met minimale $\sigma(A)$ nevenklassen van eindige deelgroepen van Z zijn. Ook wanneer $\sigma(A)$ groter is dan 1 maar toch niet al te groot is, kan er iets over de structuur van de verzameling A gezegd worden: het blijkt dan dat A zich "ongeveer" als een groep gedraagt. Dit zullen we hieronder expliciet maken. In hoofdstuk 4 zullen we laten zien dat dit soort verzamelingen zich ook laten beschrijven in termen van zogeheten approximate groups. Om te bekijken wat er gebeurt als $\sigma(A)$ iets groter is dan 1 gebruiken we de onderstaande stelling van Kneser [5].

Stelling 2.3 (Stelling van Kneser)**.** *Voor $A, B \subset Z$ geldt $|A+B| \geq |A|+|B|-|\operatorname{Sym}(A+B)|$.*

Voor het bewijs verwijzen we naar [11], stelling 5.5. Het bewijs is technisch maar staat op zichzelf: er wordt geen gebruik gemaakt van andere resultaten. Met behulp van deze stelling zijn de verzamelingen A waarvoor $\sigma(A) < \frac{3}{2}$ te klassificeren. Dit is gevolg 5.6 in [11].

Stelling 2.4. *Er geldt $\sigma(A) < \frac{3}{2}$ dan en slechts dan als A bevat is in een nevenklasse van een deelgroep G van Z met $|G| < \frac{3|A|}{2}$.*

Bewijs. Als $A \subset (G + x)$ met $|G| < \frac{3|A|}{2}$, dan geldt $A + A \subset (G + x) + (G + x) = G + 2x$, dus $|A + A| \leq |G + 2x| = |G| < \frac{3|A|}{2}$, dus $\sigma(A) < \frac{3}{2}$.

Stel nu dat $\sigma(A) < \frac{3}{2}$. We mogen aannemen dat $0 \in A$, zodat $A \subset A + A$. Definieer G als de symmetriegroep $\operatorname{Sym}(A + A)$ van $A + A$. Uit de stelling van Kneser volgt dat

$|A+A| \geq 2|A| - |G|$. We zien nu dat

$$2|A| - |G| \leq |A+A| < \frac{3|A|}{2},$$

dus $|G| > \frac{|A|}{2}$. Daaruit volgt dan dat $|A+A| < \frac{3|A|}{2} \leq 3|G|$. We zagen al eerder dat $A+A$ een vereniging van nevenklassen van $G = \mathrm{Sym}(A+A)$ is. Omdat $|A+A| < 3|G|$ is $A+A$ één nevenklasse van G of de vereniging van twee verschillende nevenklassen. Stel dat het laatste het geval is, dus dat $A+A = (G+x) \sqcup (G+y)$ met $x-y \notin G$. Er geldt $A \subset A+A$ en $2|G| = |A+A| < \frac{3|A|}{2}$ dus $|A| > \frac{4|G|}{3}$, dus A bevat zowel elementen uit de nevenklasse $x+G$ als uit de nevenklasse $y+G$. Zij $g+x$, $g'+y \in A$ met $g, g' \in G$. Dan geldt $g+x+g'+y = (g+g')+x+y \in A+A$, dus $x = x+y-x \in G$ of $y = x+y-y \in G$. We concluderen dat één van de twee nevenklassen precies G is, dus $A+A = G \cup (G+y)$ met $y \notin G$. Omdat $2(g'+y) = 2g'+2y \in A+A$ geldt er dat $2y \in G$ of $2y \in G+y$. Als $2y \in G+y$ geldt $y \in G$, tegenspraak, dus $2y \in G$. We concluderen dat $A+A+y = A+A$, want onder optelling met y worden de nevenklassen G en $G+y$ omgewisseld. Dus $y \in \mathrm{Sym}(A+A) = G$, tegenspraak.
We concluderen dat $A+A = x+G$ voor een zekere $x \in Z$. Dan geldt $A \subset A+A = x+G$, dus A is bevat in een nevenklasse van een groep G waarvan we weten dat $|G| = |A+A| < \frac{3|A|}{2}$. Dat voltooit het bewijs. □

Wanneer $\sigma(A) < \frac{3}{2}$ blijkt zelfs dat de groep G die we vinden voldoet aan $|G| \leq |A|\sigma(A)$, aangezien $|G| = |A+A|$. Er geldt dus dat als $\sigma(A) < \frac{3}{2}$, dat er dan een deelgroep G van Z bestaat met $|G| \leq |A|\sigma(A)$ zodat A bevat is in een nevenklasse van G.

We bekijken nu een voorbeeld met $\sigma(A) = \frac{3}{2}$ waar A niet bevat is in een nevenklasse van groep van orde $\frac{3}{2}|A| = \sigma(A)|A|$. Kies namelijk $Z = \mathbb{Z}/4n\mathbb{Z}$ en $A = \{a \in Z : a \equiv 0, 1 \mod 4\}$. Dan geldt $A+A = \{a \in Z : a \equiv 0, 1, 2 \mod 4\}$, dus $|A+A| = \frac{3|A|}{2}$. Een nevenklasse van een deelgroep van Z die A bevat kan echter alleen heel Z zijn en heeft dus grootte $2|A|$ (dit volgt omdat $|A| = |Z|/2$ maar A is zelf geen deelgroep van Z).

In dit voorbeeld is $A+A$ een verzameling die niet efficiënt in één nevenklasse te bevatten is, maar kan $A+A$ wel efficiënt worden bevat in een vereniging van nevenklassen. Met andere woorden kan $A+A$ efficiënt worden bedekt door translaties van een deelgroep van Z.

Dit blijkt in het algemeen het geval te zijn wanneer $\sigma(A) < 2$. Onderstaande is propositie 1.2 in Sanders, maar die wordt aldaar niet bewezen.

Stelling 2.5. *Stel dat $\sigma(A) = 2-\epsilon$, waarbij $0 < \epsilon \leq 1$. Dan is er een deelgroep G van Z zodat $|G| \leq \sigma(A)|A|$ en een constante $C_\epsilon > 0$ zodat A bedekt kan worden met C_ϵ translaties van G. In het bijzonder kunnen we $C_\epsilon = \frac{2-\epsilon}{\epsilon}$ kiezen.*

Bewijs. We gebruiken weer de stelling van Kneser. Kies als groep $G = \mathrm{Sym}(A + A)$, dan geldt volgens de stelling van Kneser dat

$$|A + A| \geq |A| + |A| - |G|$$

en dus

$$|G| \geq 2|A| - |A + A| = 2|A| - (2 - \epsilon)|A| = \epsilon|A|.$$

We weten verder dat $A + A$ de vereniging is van een aantal, zeg ℓ, nevenklassen van G, en dus geldt er dat $|A + A| = \ell|G|$ met $\ell \in \mathbb{Z}_{>0}$. Volgens lemma 1.5 kan A bedekt worden met $\frac{|A+G|}{|G|}$ translaties van $G - G = G$. Aangezien $A \subset A + A$ geldt er

$$|A + G| \leq |A + A + G| = |A + A| = \ell|G|,$$

dus $\frac{|A+G|}{|G|} \leq \ell$. Bovendien geldt

$$(2 - \epsilon)|A| = |A + A| = \ell|G| \geq \ell\epsilon|A|,$$

dus $\ell \geq \frac{2-\epsilon}{\epsilon}$. We concluderen dat A bedekt kan worden met

$$\frac{|A + G|}{|G|} \leq \ell \leq \frac{2 - \epsilon}{\epsilon}$$

translaties van G, en G is ook daadwerkelijk een deelgroep van Z met

$$|G| \leq \ell|G| = |A + A| = \sigma(A)|A|.$$

We hebben dus bewezen dat deze stelling waar is met $C_\epsilon = \frac{2-\epsilon}{\epsilon}$. □

Voor $\sigma(A) < 2$ kan A dus bevat worden in translaties van groepen die niet al te groot zijn. In tegenstelling tot de voorafgaande stellingen is dit echter geen klassificatie, want niet iedere verzameling A die aan de voorwaarden van de stelling voldoet zal ook voldoen aan $\sigma(A) < 2$.

2.2 Verzamelingen met kleine somverzameling in $\mathbb{Z}$ en $\mathbb{Z}/p\mathbb{Z}$

In deze paragraaf passen we de stellingen uit de vorige paragraaf toe wanneer Z de groep $\mathbb{Z}$ van gehele getallen is en wanneer Z de groep $\mathbb{Z}/p\mathbb{Z}$ van gehele getallen modulo een priemgetal p is.

We bekijken eerst het geval waarin de onderliggende groep Z de groep $\mathbb{Z}$ van gehele getallen is. Dan heeft Z slechts één eindige deelgroep, namelijk $\{0\}$. We bekijken wat de stellingen

uit het vorige deel in dit geval zeggen. Volgens gevolg 2.2 geldt er als $A \subset \mathbb{Z}$ dat $\sigma(A) = 1$ dan en slechts dan als A een nevenklasse is van een eindige deelgroep van $\mathbb{Z}$; er geldt dus $|A + A| = |A|$ dan en slechts dan als A uit één element bestaat. Volgens stelling 2.4 is $\sigma(A) < \frac{3}{2}$ dan en slechts dan als A bevat is in een nevenklasse van een deelgroep $G \subset \mathbb{Z}$ met $|G| < \frac{3|A|}{2}$. Dit is dus ook alleen het geval als $|A| = 1$. We bekijken ten slotte stelling 2.5. Veronderstel dat $\sigma(A) = 2 - \epsilon$ met $0 < \epsilon \leq 1$. Dan is er een deelgroep G van $\mathbb{Z}$ met $|G| \leq \sigma(A)|A|$ en een constante C_ϵ zodat A bevat is in de vereniging van C_ϵ translaties van G. Er geldt hier weer $G = \{0\}$ dus $|G| = 1$, dus er moet gelden dat $C_\epsilon \geq |A|$, oftewel $|A| \leq \frac{2-\epsilon}{\epsilon} = \frac{\sigma(A)}{2-\sigma(A)}$. In dit geval is $|A|$ dus begrensd.

Behalve het feit dat Z alleen de triviale groep als eindige deelgroep heeft, beschikt $\mathbb{Z}$ over een ordening. Dit kunnen we gebruiken om de volgende stelling te bewijzen.

Stelling 2.6. *Zij $A \subset \mathbb{Z}$. Dan geldt $\sigma(A) \geq 2 - \frac{1}{|A|}$. Er geldt gelijkheid als en alleen als A een rekenkundige rij is.*

Bewijs. We moeten bewijzen dat $|A + A| \geq 2|A| - 1$. We gebruiken dat $\mathbb{Z}$ een ordening heeft en schrijven $A = \{a_1, a_2, \ldots, a_n\}$ met $n = |A|$ en $a_1 < a_2 < \cdots < a_n$. Dan geldt

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n$$

en dat zijn $2n - 1$ verschillende getallen. Er volgt $|A + A| \geq 2n - 1 = 2|A| - 1$. Voor het gelijkheidsgeval merken we op dat als $b_1 < b_2 < \cdots < b_{2n-1}$ en $c_1 < c_2 < \cdots < c_{2n-1}$ elementen van $A + A$ zijn, dat er dan moet gelden dat $b_i = c_i$ voor alle i. Kies $b_1 < b_2 < \cdots < b_{2n-1}$ als het rijtje $a_1 + a_1 < a_1 + a_2 < \cdots < a_1 + a_n < a_2 + a_n < \cdots < a_n + a_n$ hierboven, en bekijk de ordening c_i'tjes

$$a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < \cdots < a_2 + a_n < \cdots < a_n + a_n.$$

Voor $3 \leq i \leq n$ is $b_i = a_1 + a_i$ en $c_i = a_2 + a_{i-1}$. Er volgt dat $a_i = a_{i-1} + a_2 - a_1$, dus $a_i = a_1 + (i-1)(a_2 - a_1)$ voor $1 \leq i \leq n$. Dus A is een rekenkundige rij. □

Hiermee kunnen we de verzamelingen in $\mathbb{Z}$ klassificeren met verdubbeling kleiner dan 2. Hoewel we daar voor algemene Z niet toe in staat waren, kunnen we dus voor $Z = \mathbb{Z}$ wel precies aangeven welke verzamelingen A voldoen aan $\sigma(A) < 2$.

Gevolg 2.7. *Zij $A \subset \mathbb{Z}$. Dan is $\sigma(A) < 2$ dan en slechts dan als A een rekenkundige rij is.*

Bewijs. Als $\sigma(A) < 2$ geldt $|A + A| \leq 2|A| - 1$. Uit bovenstaande stelling volgt $2|A| - 1 \leq |A + A|$. We concluderen dat $\sigma(A) < 2$ dan en slechts dan als $|A + A| = 2|A| - 1$, oftewel dan en slechts dan als A een rekenkundige rij is. □

Als $Z = \mathbb{Z}/p\mathbb{Z}$ met p priem heeft Z ook weinig deelgroepen: alleen $\{0\}$ en $\mathbb{Z}/p\mathbb{Z}$ zelf. Als voorbeeld kijken we wat stelling 2.4 hier zegt. Er geldt $\sigma(A) < \frac{3}{2}$ dan en slechts dan als A bevat is in een nevenklasse van een deelgroep G van $\mathbb{Z}/p\mathbb{Z}$ met $|G| < \frac{3|A|}{2}$. Er geldt dus $\sigma(A) < \frac{3}{2}$ dan en slechts dan als $|A| = 1$ of $|A| > \frac{2p}{3}$.

Ook in $\mathbb{Z}/p\mathbb{Z}$ blijkt stelling 2.6 te gelden, althans zolang $2|A| - 1 \leq p$. Uit de stelling van Kneser volgt zelfs de volgende algemenere variant:

Stelling 2.8 (Cauchy-Davenport)**.** *Als $A, B \subset \mathbb{Z}/p\mathbb{Z}$ geldt $|A + B| \geq \min(|A| + |B| - 1, p)$.*

Bewijs. Pas de stelling van Kneser toe op A en B. Als $\mathrm{Sym}(A+B) = \{0\}$ is $|\mathrm{Sym}(A+B)| = 1$ en zijn we klaar. Als $\mathrm{Sym}(A + B) = \mathbb{Z}/p\mathbb{Z}$ is $x + A + B = A + B$ voor alle $x \in \mathbb{Z}/p\mathbb{Z}$. Hieruit volg dat $A + B = \mathbb{Z}/p\mathbb{Z}$, dus $|A + B| = p$. Al met al geldt er $|A + B| \geq |A| + |B| - 1$ of $|A + B| = p$, waaruit de conclusie volgt. □

2.3 De stelling van Freiman

We hebben gezien dat er iets over de structuur van een verzameling A zodat $\sigma(A) < 2$ gezegd kan worden: zo'n verzameling kan efficiënt worden bedekt met translaties van een niet al te grote deelgroep van Z (stelling 2.5). Voor $\sigma(A) = 1$ is A een nevenklasse van een eindige deelgroep van Z, terwijl A zich dus voor $\sigma(A) < 2$ "ongeveer" als (nevenklasse van) een deelgroep van Z gedraagt.

In algemene zin is het mogelijk iets te zeggen over de structuur van een verzameling A zodat $\sigma(A) < K$, waarbij $K > 1$ een vast gekozen constante is. Er blijken twee soorten structuur mogelijk, die allebei aanleiding geven tot verzamelingen met beperkte σ. De ene soort is de groepsstructuur. Een groep (of een nevenklasse daarvan) heeft een σ van 1 terwijl ook verzamelingen die zich "ongeveer" als groep gedragen een kleine somverzameling hebben (zie stelling 2.4 en stelling 2.5). De andere soort structuur is die van een rekenkundige rij. We zagen al dat een rekenkundige rij in $\mathbb{Z}$ een σ kleiner dan 2 heeft (stelling 2.6).

In het algemeen geldt dat een verzameling met $\sigma(A) < K$ zich ongeveer gedraagt als een combinatie van een nevenklasse van een eindige deelgroep van Z en een (naar meer dimensies gegeneraliseerde) rekenkundige rij. We zullen dit eerst preciezer definiëren.

Met een *convex lichaam* bedoelen we een deelverzameling $S \subset \mathbb{R}^d$ die niet-leeg, open, begrensd en convex is. Convex wil zeggen dat voor α, $\beta \in S$ ook $t\alpha + (1 - t)\beta \in S$ met $0 \leq t \leq 1$. We noemen S *symmetrisch* als $S = -S$.

We definiëren een *gecentreerde convexe progressie* als een verzameling $P \subset Z$ waarvoor er een symmetrisch convex lichaam $Q \subset \mathbb{R}^d$ bestaat, zodat er een groepshomomorfisme $\varphi : \mathbb{Z}^d \to Z$ is met $\varphi(\mathbb{Z}^d \cap Q) = P$. Hierbij noemen we P *d-dimensionaal*. Een gegeneraliseerde rekenkundige rij (zie [11])

$$\{a + n_1 v_1 + \cdots + n_d v_d : 0 \leq |n_i| < N_i\} \subset \mathbb{Z}$$

voor a, v_1, ..., $v_d \in \mathbb{Z}$ en zekere N_1, ..., $N_d > 0$ is een voorbeeld van een d-dimensionale gecentreerde convexe progressie, dus deze definitie geeft inderdaad een generalisatie van het begrip rekenkundige rij. Een *gecentreerde convexe nevenklasseprogressie* is nu een deelverzameling van Z die te schrijven is als som van een deelgroep van Z en een gecentreerde convexe progressie. Dit is dus een verzameling die de structuur van een groep combineert met de structuur van een gegeneraliseerde rekenkundige rij.

De volgende propositie laat zien dat de σ van een dergelijke verzameling inderdaad beperkt is. Het bewijs komt uit [10] (lemma 4.2).

Propositie 2.9. *Voor iedere d en voor iedere d-dimensionale gecentreerde convexe nevenklasseprogressie M geldt dat $\sigma(M) \leq 9^d$. Er geldt dus $\sigma(M) = \exp(O(d))$.*

Bewijs. Schrijf $M = P + H$, met P een d-dimensionale gecentreerde convexe progressie, $P = \varphi(Q \cap \mathbb{Z}^d)$, Q een convex lichaam in $\mathbb{R}^d$ en H een deelgroep van Z. Voor $x \in 2 \cdot Q$ definiëren we de verzameling $U_x = x + \frac{1}{4} \cdot Q$ (we gebruiken hier de notatie $2 \cdot Q$ voor de verzameling $\{2q : q \in Q\}$, niet te verwarren met $2Q = Q + Q = \{q + q' : q, q' \in Q\}$). Bekijk een deelverzameling $X \subset 2 \cdot Q$ zodat alle U_x voor $x \in X$ disjunct zijn. We bewijzen dat $|X| \leq 9^d$. Stel dat $|X| > 9^d$ en zij $Y \subset X$ eindig met $|Y| > 9^d$. We geven de inhoud van een verzameling $S \subset \mathbb{R}^d$ aan met $\mu(S)$. Dan geldt $\mu(U_y) = \mu(Q)4^{-d}$ voor $y \in Y$ en alle U_y zijn disjunct, zodat

$$\mu(U) = \sum_{y \in Y} \mu(U_y) = |Y|\mu(Q)4^{-d} > 9^d \mu(Q) 4^{-d} = \mu\left(\frac{9}{4} \cdot Q\right).$$

met $U = \bigcup_{y \in Y} U_y \subset \frac{9}{4} \cdot Q$, wat een tegenspraak is. Dus $|X| \leq 9^d$ en in het bijzonder is X een eindige verzameling. Hieruit volgt ook dat er een verzameling $X \subset 2 \cdot Q$ met deze eigenschap is die maximaal is. Voor $t \in 2 \cdot Q$ is er dan een $x \in X$ met $t + \frac{1}{4} \cdot Q \cap x + \frac{1}{4} Q \neq \emptyset$ voor een zekere $x \in X$. Er geldt dan dus

$$2 \cdot Q \subset X + \frac{1}{4} \cdot Q - \frac{1}{4} \cdot Q = X + \frac{1}{2} \cdot Q.$$

Er volgt dan ook dat

$$\begin{aligned} P+P &= \varphi(Q\cap\mathbb{Z}^d)+\varphi(Q\cap\mathbb{Z}^d)\\ &= \varphi(Q\cap\mathbb{Z}^d+Q\cap\mathbb{Z}^d)\\ &= \varphi((Q+Q)\cap\mathbb{Z}^d)\\ &\subset \varphi(2\cdot Q\cap\mathbb{Z}^d)\\ &\subset \varphi\left(\left(X+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)\\ &= \bigcup_{x\in X}\varphi\left(\left(x+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)=\bigcup_{x\in X}P_x, \end{aligned}$$

met $P_x=\varphi\left((x+\frac{1}{2}\cdot Q)\cap\mathbb{Z}^d\right)$. Voor iedere $x\in X$ zodat P_x niet leeg is kiezen we nu een element $t_x\in P_x$ en we definiëren $T=\{t_x : x\in X, P_x\neq\emptyset\}$. Er geldt $|T|\leq|X|$. We merken nu op dat als $u\in P+P$, er een x is zodat $u\in P_x$. Dan geldt

$$\begin{aligned} u-t_x &\in P_x-P_x\\ &= \varphi\left(\left(x+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)-\varphi\left(\left(x+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)\\ &= \varphi\left(\left(x+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d-\left(x+\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)\\ &= \varphi\left(\left(x+\frac{1}{2}\cdot Q-x-\frac{1}{2}\cdot Q\right)\cap\mathbb{Z}^d\right)\\ &= \varphi\left(Q\cap\mathbb{Z}^d\right)=P. \end{aligned}$$

We concluderen dat $u\in P+t_x$, dus er geldt $P+P\subset P+T$. We concluderen nu dat

$$M+M=(P+H)+(P+H)=P+P+H+H\subset P+T+H+H=P+T+H=M+T,$$

dus

$$\sigma(M)=\frac{|M+M|}{|M|}\leq\frac{|M||T|}{|M|}=|T|\leq|X|\leq 9^d.$$

We concluderen dat $\sigma(M)\leq 9^d$ voor alle d-dimensionale gecentreerde convexe nevenklassenprogressies M, dus $\sigma(M)=\exp(O(d))$. □

Ook wanneer een verzameling A bedekt kan worden met translaties van een gecentreerde convexe nevenklasseprogressie is $\sigma(A)$ beperkt.

Propositie 2.10. *Zij $A\subset Z$ en veronderstel dat er een d-dimensionale gecentreerde convexe nevenklasseprogressie M is zodat $|M|\leq e^d|A|$ en zodat A door e^d translaties van M bedekt wordt. Dan is $\sigma(A)=\exp(O(d))$, dus er is een constante C zodat voor iedere A en voor iedere d geldt dat als aan bovenstaande voorwaarden voldaan is, dan $\sigma(A)\leq e^{C\cdot d}$.*

Bewijs. Zij X zodat $|X| \leq e^d$ en $A \subset X + M$. Dan geldt er

$$\begin{aligned} |A + A| &\leq |X + M + X + M| \\ &\leq |X|^2 |M + M| \\ &\leq e^{2d} \exp(O(d)) |M| \\ &\leq e^{2d} \exp(O(d)) e^d |A| \\ &= \exp(O(d)) |A|. \end{aligned}$$

Dus $\sigma(A) = \exp(O(d))$. □

De stelling van Freiman keert het resultaat van propositie 2.10 om: iedere verzameling A met $\sigma(A) \leq K$ kan bedekt worden met translaties van een gecentreerde convexe nevenklasseprogressie M waarbij de dimensie van M, de grootte $|M|/|A|$ van M ten opzichte van A en het aantal verzamelingen in de bedekking alleen van K afhangen. Verzamelingen met een kleine σ kunnen dus geheel beschreven worden in termen van nevenklassen van groepen en gecentreerde convexe progressies.

Stelling 2.11 (Stelling van Freiman)**.** *Zij $A \subset Z$ zodat $\sigma(A) \leq K$. Dan bestaat er een getal $d(K)$ dat alleen van K afhangt, zodat er een d-dimensionale gecentreerde convexe nevenklasseprogressie M is zodat A bedekt kan worden met* $\exp(d(K))$ *translaties van M en* $|M| \leq \exp(d(K))|A|$.

Het bewijs van deze stelling laten we achterwege, zie daarvoor [3]. Later zullen we wel een bewijs geven voor het geval waarin Z een torsiegroep is (stelling 3.5).

3 De ongelijkheid van Plünnecke

We zagen eerder al dat verzamelingen A voldoen aan de eigenschap dat $\delta(A) = 1$ dan en slechts dan als $\sigma(A) = 1$ (in beide gevallen als A een nevenklasse is van een deelgroep van Z; zie gevolg 2.2). In algemene zin blijkt te gelden dat een verzameling met een kleine δ ook een kleine σ heeft en vice versa, dus verzamelingen met een kleine somverzameling hebben een kleine verschilverzameling en andersom. Verder geldt voor een dergelijke verzameling A waarvoor $\sigma(A)$ en $\delta(A)$ klein zijn ook dat de verzamelingen

$$nA - mA = \{a_1 + \cdots + a_n - b_1 - \cdots - b_m : a_i \in A, b_i \in A\}$$

niet al te groot kunnen zijn. In het bijzonder zullen we laten zien dat $|nA - mA| \leq \sigma(A)^{m+n}|A|$ (de ongelijkheid van Plünnecke-Ruzsa, stelling 3.4).

In hoofdstuk 4 gaan we verder in op het verband tussen δ en σ. In dit hoofdstuk behandelen we bovengenoemde ongelijkheid en een aantal vergelijkbare resultaten, die we in hoofdstuk 4 nodig hebben. Verder zullen we een speciaal geval van de stelling van Freiman, stelling 2.11, bewijzen.

Om de ongelijkheden als die van Plünnecke-Ruzsa te bewijzen gebruiken we onderstaand lemma dat pas recent is ondekt [1]. Het bewijs is gebaseerd op het bewijs wat in [1] wordt gepresenteerd. Ook in [10] wordt een bewijs gegeven. Dat bewijs is echter niet correct omdat het voorlaatste ongelijkheidsteken verkeerd om staat.

Lemma 3.1 (Lemma van Petridis)**.** *Zij $A, X \subset Z$ en $K \geq 1$ zodat $|A+X| = K|X|$ terwijl $|A+X'| \geq K|X'|$ voor alle $X' \subset X$. Dan geldt voor $C \subset Z$ dat $|A+X+C| \leq K|X+C|$.*

Bewijs. We bewijzen dit met inductie naar $|C|$. Als $|C| = 0$ of $|C| = 1$ geldt er gelijkheid. Stel nu dat $|A+X+C| \leq K|A+C|$ en zij $C' = C \sqcup \{c\}$, dus we voegen een element c aan de verzameling C toe. We bewijzen dat $|X+A+C'| \leq K|X+C'|$. Er geldt

$$X + A + C' = (X + A + C) \cup ((X + A + c) \backslash (X' + A + c))$$

waarbij $X' = \{x \in X : x + A + c \subset X + A + C\}$. Er geldt $X' + A + c \subset X + A + c$ dus $|(X + A + c)\backslash(X' + A + c)| = |X + A + c| - |X' + A + c|$. Er geldt dus

$$|X+A+C'| \leq |X+A+C|+|X+A+c|-|X'+A+c| = |X+A+C|+|X+A|-|X'+A|,$$

waarbij we gebruiken dat de vereniging van twee verzamelingen hoogstens zoveel elementen bevat als de twee verzamelingen samen. Uit onze aannames volgt dat $|X+A+C| \leq K|X+C|$ (de inductiehypothese), dat $|X + A| = K|X|$, en dat $|X' + A| \geq K|X'|$ (want $X' \subset X$). Dus er geldt

$$|X + A + C'| \leq K(|X + C| + |X| - |X'|).$$

Er geldt verder dat

$$X + C' = (X + C) \sqcup ((X + c)\backslash(Y + c)),$$

waarbij $Y = \{x \in X : x+c \in X+C\}$. Dit is een disjuncte vereniging, dus er geldt aangezien $Y + c \subset X + x$ dat

$$|X + C'| = |X + C| + |X + c| - |Y + c| = |X + C| + |X| - |Y|.$$

Wanneer $x \in Y$ geldt $x + c \in X + C$, dan geldt dus ook $x + A + c \subset X + A + C$. Dus er geldt $Y \subset X'$, waaruit we concluderen dat $|Y| \leq |X'|$. Dit betekent dat

$$|X + C'| = |X + C| + |X| - |Y| \geq |X + C| + |X| - |X'|.$$

We concluderen dat

$$|X + A + C'| \leq K(|X + C| + |X| - |X'|) \leq K(|X + C'|),$$

waarmee de inductie voltooid is. □

De ongelijkheden van Plünnecke zijn hier eenvoudig uit af te leiden. Eerst hebben we onderstaand tussenresultaat.

Gevolg 3.2. *Zij $A, B \subset Z$ en $K \geq 1$ zodat $|A + B| \leq K|B|$. Dan is er een niet-lege deelverzameling X van B zodat $|nA + X| \leq K^n|X|$ voor $n \in \mathbb{Z}_{\geq 0}$.*

Bewijs. Kies $X \subset B$ niet-leeg zodat $\frac{|A+X|}{|X|}$ minimaal is. Dan is $\frac{|A+X|}{|X|} \leq \frac{|A+X'|}{|X'|}$ voor $X' \subset X$ en bovendien is $\frac{|A+X|}{|X|} \leq K$. Uit lemma 3.1 volgt nu dat $|A + X + C| \leq K|X + C|$ voor $C \subset Z$. Kies $C = (n-1)A$. Dan vinden we $|na + X| \leq K|X + (n-1)A|$, waaruit met inductie volgt dat $|nA + X| \leq K^n|X|$ voor $n \geq 0$. □

Uit dit gevolg kunnen we de ongelijkheid van Plünnecke [6] afleiden.

Stelling 3.3 (Ongelijkheid van Plünnecke)**.** *Zij $A \subset Z$. Er geldt $|nA| \leq \sigma(A)^n|A|$ voor $n \in \mathbb{N}$.*

Bewijs. Pas gevolg 3.2 toe met $A = B$. Dan vinden we dat er een deelverzameling X van A bestaat zodat $|nA + X| \leq \sigma(A)^n|X|$ voor $n \geq 0$. Dan geldt er dus

$$|nA| \leq |nA + X| \leq \sigma(A)^n|X| \leq \sigma(A)^n|A|$$

want $X \subset A$ en $X \neq \emptyset$. □

Merk op dat deze ongelijkheid in het algemeen niet scherp is: voor $n = 1$ en $n = 2$ staat er bijvoorbeeld $|A| \leq \sigma(A)|A|$ en $|A + A| \leq \sigma(A)^2|A|$, waarbij we een factor $\sigma(A)$ "te veel" hebben. In hoofdstuk 4 bewijzen we dat als $\sigma(A) > 1$ er inderdaad geen gelijkheid geldt (stelling 4.9).

Een algemenere variant van deze ongelijkheid die ook geldt voor verschilverzamelingen is de volgende. Dit is stelling 6.29 in [11] en gevolg 3.5 in [10].

Stelling 3.4 (Ongelijkheid van Plünnecke-Ruzsa)**.** *Zij $A \subset Z$. Dan is $|nA - mA| \leq \sigma(A)^{n+m}|A|$ voor $n, m \in \mathbb{Z}_{\geq 0}$.*

Bewijs. Uit gevolg 3.2 volgt dat er een $X \subset A$ is zodat $|rA + X| \leq \sigma(A)^r|X|$ voor $r \geq 0$. Dan is dus $|nA + X| \leq \sigma(A)^n|X|$ en $|-mA - X| = |mA + X| \leq \sigma(A)^m|X|$. De

driehoeksongelijkheid van Ruzsa (lemma 1.4) zegt dat $|K||J-L| \leq |J-K||K-L|$ voor J, K, $L \subset Z$. Als we deze toepassen met $J = nA$, $K = -X$ en $L = mA$, vinden we dat

$$\begin{aligned} |nA - mA| &\leq \frac{|nA + X||-mA - X|}{|X|} \\ &\leq \frac{\sigma(A)^n|X|\sigma(A)^m|X|}{|X|} \\ &= \sigma(A)^{m+n}|X| \\ &\leq \sigma(A)^{m+n}|A|, \end{aligned}$$

precies wat we moesten bewijzen. □

Met behulp van deze stelling kunnen we de stelling van Freiman bewijzen in het geval dat Z een torsiegroep is, dus als er een $r \in \mathbb{Z}_{>0}$ bestaat zodat $rz = 0$ voor alle $z \in Z$. Dit is propositie 4.3 in [10], waar ook onderstaand bewijs van afkomstig is.

Stelling 3.5 (Stelling van Freiman-Ruzsa)**.** *Veronderstel dat Z voldoet aan $rZ = \{0\}$. Stel dat $A \subset Z$ en $\sigma(A) = K$. Dan voldoet de groep $G = \langle A \rangle$ voortgebracht door A aan $|G| \leq K^2 r^{K^4}|A|$.*

Bewijs. We zullen het bedekkingslemma van Ruzsa (lemma 1.5) gebruiken om $2A - A$ te bedekken met translaties van $A - A$. Volgens dit lemma volstaan $\frac{|3A-A|}{|A|}$ translaties. Volgens de Plünnecke-ongelijkheden geldt

$$|3A - A| \leq \sigma(A)^4|A| = K^4|A|,$$

dus er is een verzameling T met $|T| \leq K^4$ zodat $2A - A \subset T + A - A$. Merk op dat $nA + (A - A) = (n-1)A + 2A - A \subset (n-1)A + T + (A - A)$. Met inductie volgt er dat $nA + (A-A) \subset nT + (A-A)$ voor $n \geq 1$. Zij H de groep voortgebracht door T. Er volgt dat $|H| \leq r^{|T|}$ en $nT + A - A \subset H + A - A$. Er geldt dus $nA \subset nA + (A-A) \subset H + A - A$ voor alle n. Hetzelfde geldt voor $-nA$ omdat $H + A - A$ symmetrisch is. We concluderen dat de groep $\langle A \rangle$ voortgebracht door A bevat is in $H + A - A$, dus $|\langle A \rangle| \leq |H + A - A| \leq |H||A - A| \leq r^{K^4}K^2|A|$ aangezien $|A - A| \leq K^2|A|$ (stelling 3.4 met $m = n = 1$). □

Aangezien G een groep is, is G een d-dimensionale gecentreerde convexe nevenklasseprogressie voor iedere d. Wanneer we $d(K) = 2\log(K) + K^4 \log(r)$ kiezen geldt $\exp(d(K)) = K^2 r^{K^4}$ en zien we dat we hier daadwerkelijk met een speciaal geval van stelling 2.11 te maken hebben. Merk op dat het niet verwonderlijk is dat we hier alleen het "nevenklase-deel" van de gecentreerde convexe nevenklassenprogressie nodig hebben; in een torsiegroep Z is iedere rekenkundige rij bevat in een nevenklasse van een deelgroep van Z.

4 Kleine somverzamelingen en kleine verschilverzamelingen zijn equivalent

In dit hoofdstuk laten we zien dat verzamelingen met kleine σ ook een kleine δ hebben en andersom. Hiervoor gebruiken we de resultaten uit het vorige hoofdstuk. We hebben eerder verzamelingen met een kleine σ beschreven in termen van gegeneraliseerde rekenkundige rijen en nevenklassen van deelgroepen (zie stelling 2.11). Hier zullen we een nieuw begrip invoeren dat deze structuren omvat: dat van een approximate group.

4.1 Approximate groups

Voordat we het hebben over approximate groups laten we eerst zien dat $\delta \leq \sigma^2$ (dus verzamelingen met een kleine somverzameling hebben ook een kleine verschilverzameling) en $\sigma \leq \delta^2$ (dus verzamelingen met een kleine verschilverzameling hebben ook een kleine somverzameling).

Stelling 4.1. *Zij $A \subset Z$. Dan is $\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2$.*

Bewijs. Pas de driehoeksongelijkheid van Ruzsa $|B||A-C| \leq |A-B||B-C|$ (lemma 1.4) toe met $C = A$ en $B = -A$. Dan vinden we $\delta(A) \leq \sigma(A)^2$. Pas gevolg 3.2 toe met $B = -A$. Dan vinden we dat er een niet-lege $X \subset -A$ is zodat $|2A + X| \leq \delta(A)^2|X|$. Dan geldt ook

$$|A + A| \leq |2A + X| \leq \delta(A)^2|X| \leq \delta(A)^2|A|,$$

dus $\sigma(A) \leq \delta(A)^2$. Al met al vinden we $\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2$. □

We zullen later verder ingaan op deze ongelijkheid en kijken of de exponenten $\frac{1}{2}$ en 2 verbeterd kunnen worden.

We definiëren nu het begrip *approximate group*, waarmee we verzamelingen met een kleine som- en verschilverzameling kunnen beschrijven [2]. Met een K-approximate group bedoelen we een deelverzameling H van Z zodat H symmetrisch is, $0 \in H$ en $H+H$ bedekt kan worden met hoogstens K translaties van H. Hierbij moet $K \geq 1$ aangezien $|H + H| \geq |H|$. Een 1-approximate group is niets anders dan een deelgroep van Z:

Propositie 4.2. *Een verzameling $H \subset Z$ is een deelgroep van Z dan en slechts dan als H een 1-approximate group is.*

Bewijs. Als H een deelgroep van Z is geldt $-H = H$, $0 \in H$ en $H + H = H$. Als H een 1-approximate group is kan $H + H$ bedekt worden met 1 translatie van H. Dit betekent dat $|H + H| \leq |H|$, dus $\sigma(H) \leq 1$. Dit betekent dat $\sigma(H) = 1$, en daaruit volgt met gevolg 2.2 dat H een nevenklasse van een deelgroep van Z is. Omdat $0 \in H$ moet H zelf een deelgroep van Z zijn. □

Verder geldt dat hoe groter K is, hoe meer K-approximate groups er zijn: de eisen worden dan minder sterk. In het bijzonder is een K-approximate group ook een L-approximate group voor $L \geq K$.

De volgende stelling laat zien dat $\delta(A)$ en $\sigma(A)$ klein zijn dan en slechts dan als A een translatie van een niet al te grote approximate group is. Zie ook propositie 2.26 in [11].

Stelling 4.3. *Zij $A \subset Z$ en $K \geq 1$. Dan zijn de volgende beweringen equivalent in de zin dat als de i-de bewering geldt voor een zekere C_i, dat dan de j-de bewering ook geldt voor een C_j die af mag hangen van C_i:*

(i) $\sigma(A) \leq K^{C_1}$;

(ii) $\delta(A) \leq K^{C_2}$ *(oftewel* $|A - A| \leq K^{C_2}|A|$*);*

(iii) $|nA - mA| \leq K^{C_3(m+n)}|A|$ *voor* $m, n \geq 0$;

(iv) A is een translatie van een K^{C_4}-approximate group H met $|H| \leq K^{C_4}|A|$.

Bewijs. Uit stelling 4.1 volgt dat (i) en (ii) equivalent zijn. We bewijzen dat (i), (iii) en (iv) equivalent zijn.
Uit de Ruzsa-Plünnecke-ongelijkheid (stelling 3.4) volgt dat als $\sigma(A) \leq K^{C_1}$, dat dan $|nA - mA| \leq K^{C_1(m+n)}|A|$ voor $n, m \geq 0$, dus (i) $\Longrightarrow$ (iii). We bewijzen dat (iii) $\Longrightarrow$ (iv). Zij $H = A - A$. Dan is H symmetrisch en is $0 \in H$. Verder geldt volgens het bedekkingslemma van Ruzsa (lemma 1.5) dat $H + H = 2A - 2A$ bedekt kan worden met $\frac{|2A-2A+A|}{|A|} \leq K^{5C_3}$ translaties van A, dus H is een K^{5C_3}-approximate group. Verder geldt $|H| = |A - A| \leq K^{2C_3}|A| \leq K^{5C_3}|A|$ en is A bevat in $A - A + a$ voor een $a \in A$, dus aan (iv) is voldaan. We bewijzen ten slotte dat (iv) $\Longrightarrow$ (i). Er geldt als aan (iv) voldaan is dat

$$|A + A| \leq |(a + H) + (a + H)| = |H + H| \leq K^{C_4}|H| \leq K^{2C_4}|A|,$$

dus $\sigma(A) \leq K^{2C_4}$. □

Gezien ook (gegeneraliseerde) rekenkundige rijen een kleine σ hebben (zie ook propositie 2.9) zal het geen verrassing zijn dat dit ook K-approximate groups zijn voor een lage K. Dit illustreren we met de volgende propositie, voorbeeld 3 uit [2].

Propositie 4.4. *Zij $v_1, \ldots, v_d \in \mathbb{Z}$. Zij verder $N_1, \ldots, N_d \in \mathbb{Z}_{>0}$.*

$$L = \{n_1 v_1 + \cdots + n_d v_d : 0 \leq |n_i| \leq N_i, n_i \in \mathbb{Z}\} \subset \mathbb{Z}$$

een gegeneraliseerde rekenkundige rij. Dan is L een 2^d-approximate group.

Bewijs. Het is duidelijk dat $0 \in L$ en dat L symmetrisch is. We hoeven dus alleen te laten zien dat $L + L$ bedekt kan worden met 2^d translaties van L. Er geldt

$$\begin{aligned} L + L &= \{n_1 v_1 + \cdots + n_d v_d + m_1 v_1 + \cdots + m_d v_d : 0 \leq |n_i|, |m_i| \leq N_i, n_i, m_i \in \mathbb{Z}\} \\ &= \{n_1 v_1 + \cdots + n_d v_d : 0 \leq |n_i| \leq 2N_i, n_i \in \mathbb{Z}\} = 2 \cdot L. \end{aligned}$$

Zij

$$M = \{\pm N_1 \pm N_2 \pm \cdots \pm N_d\} \subset \mathbb{Z}$$

waarbij de $\pm$-tekens onafhankelijk van elkaar kunnen worden gekozen. Dan is $|M| \leq 2^d$ en bovendien is

$$L + L = 2 \cdot L \subset \bigcup_{m \in M} (m + L)$$

omdat een element van $2 \cdot L$ op de i-de coördinaat een element van $[-2N_i, 2N_i]$ heeft staan, dat hoogstens N_i van $+N_i$ of $-N_i$ afwijkt. We kunnen $L + L$ dus bedekken met (hoogstens) 2^d translaties van L, dus inderdaad is L een 2^d-approximate group. □

4.2 De ongelijkheid $\delta(A) \leq \sigma(A)^2$

Deze en de volgende paragraaf worden besteed aan een nadere analyse van stelling 4.1. We bekijken eerst de afschatting $\delta(A) \leq \sigma(A)^2$ die aangeeft dat verzamelingen met een kleine somverzameling ook een kleine verschilverzameling hebben. We bekijken of we de constante 2 door een lagere constante kunnen vervangen. Dit kan alleen als het gelijkheidsgeval alleen bestaat uit verzamelingen A waarvoor $\delta(A) = \sigma(A) = 1$. Een eerste stap is daarom de analyse van het gelijkheidsgeval van deze ongelijkheid.

Stelling 4.5. *Er geldt $\delta(A) = \sigma(A)^2$ dan en slechts dan als A een deelgroep is van Z, oftewel dan en slechts dan als $\sigma(A) = \delta(A) = 1$.*

Bewijs. Om de verzamelingen met $\delta(A) = \sigma(A)^2$ te klassificeren, bekijken we het bewijs van de ongelijkheid $\delta(A) \leq \sigma(A)^2$. In het bewijs is gebruik gemaakt van de Ruzsa-driehoeksongelijkheid $|B||A - C| \leq |A - B||B - C|$, toegepast met $C = A$ en $B = -A$. Er is dus een afbeelding $\psi : A - A \to A^2$ gekozen zodat als $\psi(u) = (a, b)$ er geldt dat $a - b = u$.

Vervolgens is een injectieve afbeelding $\varphi : A \times (A-A) \to (A+A)^2$ geconstrueerd die (b, y) naar $(a_1 + b, b + a_2)$ stuurt waarbij $\psi(y) = (a_1, a_2)$. Er geldt gelijkheid alleen als φ ook surjectief is. Voor iedere $(k, \ell) \in (A+A)^2$ zijn er dan a_1, b, a_2 in A zodat $b + a_1 = k$, $b + a_2 = \ell$ en $\psi(a_1 - a_2) = (a_1, a_2)$. Kies $k = \ell$. Dan zijn er a_1, b, a_2 in A met $b + a_1 = k = \ell = b + a_2$ en $\psi(0) = \psi(a_1 - a_2) = (a_1, a_2)$. We concluderen dat a_1 vast ligt, dus voor iedere $k \in A + A$ is er een $b \in A$ met $k = b + a_1$. Hieruit volgt dat $A + A \subset a_1 + A$, oftewel $|A + A| = |A|$. Dus $\sigma(A) = 1$, en A is een nevenklasse van een deelgroep van Z (gevolg 2.2). Dus ook $\delta(A) = 1$ Het is duidelijk dat als $\sigma(A) = \delta(A) = 1$ er ook daadwerkelijk gelijkheid geldt. □

Omdat het gelijkheidsgeval van de ongelijkheid $\delta(A) \leq \sigma(A)^2$ alleen bestaat uit verzamelingen A met $\sigma(A) = \delta(A) = 1$, is er mogelijk ruimte om de exponent in deze ongelijkheid te verlagen. Toch blijkt dat deze exponent in het algemeen optimaal is. Het voorbeeld is afkomstig van [7]: het blijkt dat slim gekozen verzamelingen in $\mathbb{Z}^d$ weinig sommen hebben maar veel verschillen.

Stelling 4.6. *Zij C een constante zodat $\delta(A) \leq \sigma(A)^C$ geldt voor iedere eindige deelverzameling A van iedere commutatieve groep Z. Dan is $C \geq 2$.*

Bewijs. We kiezen een $d \in \mathbb{N}$ en bekijken het simplex S in $\mathbb{R}^d$ gegeven door

$$S = \{(x_1, \ldots, x_d) : x_i \geq 0, x_1 + \cdots + x_d \leq N\}$$

voor een zeker geheel getal N. De inhoud V van S wordt gegeven door

$$V = \int_0^N \int_0^{N-x_1} \cdots \int_0^{N-x_1-\cdots-x_{d-1}} 1 \, dx_d \cdots dx_1 = \frac{N^d}{d!}.$$

De inhoud van $S + S = \{x + y : x, y \in S\} = \{2x : x \in S\}$ is gelijk aan $2^d V$. We bepalen de inhoud van $S - S$. Er geldt

$$S - S = \{(y_1, \ldots, y_d) : \sum_{i \in B} y_i \leq N, \sum_{i \in C} y_i \geq -N\}$$

met $B = \{1 \leq i \leq d : y_i > 0\}$ en $C = \{1 \leq i \leq d : y_i \leq 0\}$ zodat $\{1, 2, \ldots, d\} = B \sqcup C$. De inhoud van $S - S$ is dan gelijk aan

$$\sum_{B \subset \{1,2,\ldots,d\}} \int_0^N \int_0^{N-b_1} \cdots \int_0^{N-b_1-\cdots-b_{r-1}} \int_0^N \int_0^{N-c_1} \cdots \int_0^{N-c_1-\cdots-c_{s-1}} 1 \, dc_s \cdots dc_1 db_r \cdots db_1$$

waarbij $B = \{b_1, \ldots, b_r\}$ en $C = \{c_1, \ldots, c_s\}$. De uitdrukking rechts is gelijk aan $\frac{N^d}{r!s!} =$

$\frac{N^d}{|B|!(d-|B|)!}$, dus de inhoud van $S - S$ is gelijk aan

$$\sum_{B\subset\{1,2,\ldots,d\}} \frac{N^d}{|B|!(d-|B|)!} = \sum_{b=0}^{d} \binom{d}{b} \frac{N^d}{b!(d-b)!}$$
$$= \frac{N^d}{d!} \sum_{b=0}^{d} \binom{d}{b}^2 = \binom{2d}{d} \frac{N^d}{d!} = \binom{2d}{d} V.$$

Er geldt $\sum_{b=0}^{d} \binom{d}{b}^2 = \binom{2d}{d}$ omdat aan beide kanten het aantal manieren om een deelverzameling van d elementen uit $\{1, 2, \ldots, 2d\}$ te kiezen staat; aan de linkerkant tellen we dit apart voor $0 \leq b \leq d$ waar b het aantal elementen is wat we uit $\{1, 2, \ldots, d\}$ kiezen. Zij A de verzameling roosterpunten in S, dus $A = S \cap \mathbb{Z}^d$. Dan is $A \sim V$, $A + A \sim 2^d V$ en $A - A \sim \binom{2d}{d} V$ (met de notatie $X \sim Y$ bedoelen we hier dat $\lim_{N\to\infty} X/Y = 1$). Er geldt dus $\sigma(A) \sim 2^d$ en $\delta(A) \sim \binom{2d}{d}$. Omdat we N willekeurig groot kunnen kiezen, moet er gelden dat

$$\binom{2d}{d} \leq 2^{dC}$$

oftewel

$$C \geq \frac{\log(\binom{2d}{d})}{\log(2^d)}$$

voor alle $d \geq 1$. We zullen laten zien dat

$$\lim_{d\to\infty} \frac{\log(\binom{2d}{d})}{\log(2^d)} = 2.$$

Hieruit volgt dan dat $C \geq 2$. Merk op dat

$$\frac{4^d}{2d+1} \leq \binom{2d}{d} \leq 4^d$$

aangezien de binomiaalcoëfficiënten $\binom{2d}{0}, \binom{2d}{1}, \ldots, \binom{2d}{2d}$ optellen tot $2^{2d} = 4^d$ en $\binom{2d}{d}$ van deze $2d + 1$ binomiaalcoëfficiënten de grootste is (en in het bijzonder dus minstens zo groot als het gemiddelde). Hieruit volgt dat

$$2 - \frac{\log(2d+1)}{d \log 2} = \frac{\log(\frac{4^d}{2d+1})}{\log(2^d)} \leq \frac{\log(\binom{2d}{d})}{\log(2^d)} \leq \frac{\log(4^d)}{\log(2^d)} = 2.$$

Aangezien zowel de linkerkant als de rechterkant naar 2 gaat voor $d \to \infty$, geldt hetzelfde voor $\frac{\log(\binom{2d}{d})}{\log(2^d)}$. Dus inderdaad $C \geq 2$. □

De gegeven voorbeelden leven in $Z = \mathbb{Z}^d$ voor zekere d. Er is niets bijzonders aan deze keuze van Z; deze voorbeelden kunnen ook worden "vertaald" naar een voorbeeld in bijvoorbeeld $Z = \mathbb{Z}$ met behulp van een afbeelding

$$\mathbb{Z}^d \to \mathbb{Z} : (x_1, \ldots, x_d) \mapsto (x_1, Mx_2, M^2x_3, \ldots, M^{d-1}x_d)$$

voor voldoende grote M (gekozen aan de hand van de coördinaten van de elementen in het gebruikte voorbeeld).

4.3 De ongelijkheid $\sigma(A) \leq \delta(A)^2$

In de vorige paragraaf zagen we dat de exponent 2 in $\delta(A) \leq \sigma(A)^2$ niet verbeterd kan worden. Hier analyseren we de ongelijkheid $\sigma(A) \leq \delta(A)^2$. Mogelijk bestaat hier wel een $C < 2$ zodat $\sigma(A) \leq \delta(A)^C$ in het algemeen waar is. Een voorwaarde hiervoor is dat het gelijkheidsgeval wederom alleen uit de verzamelingen A waarvoor $\sigma(A) = \delta(A) = 1$ bestaat. Dit blijkt inderdaad het geval te zijn. Om dat te kunnen bewijzen, hebben we eerst de gelijkheidsgevallen van lemma 3.1 en gevolg 3.2 nodig.

Lemma 4.7 (Lemma 3.1 met gelijkheidsgeval)**.** *Zij $A, X \subset Z$ en $K \geq 1$ zodat $\frac{|A+X|}{|X|} = K$ terwijl $\frac{|A+X'|}{|X'|} > K$ voor alle $\emptyset \subsetneq X' \subsetneq X$. Dan geldt voor $D \subset Z$ dat $|A+X+D| \leq K|X+D|$. Voor een $D \subset Z$ geldt gelijkheid dan en slechts dan als voor iedere keuze van $C \subset D$ en $c \in D \backslash C$ aan één van de volgende voorwaarden voldaan is:*

(i) er geldt $X + c \subset X + C$;

(ii) er geldt $(X + A + C) \cap (X + A + c) = \emptyset$.

Merk op dat we ten opzichte van lemma 3.1 een extra voorwaarde hebben toegevoegd: dat de ongelijkheid $\frac{|A+X'|}{|X'|} \geq K$ strikt is voor $X' \subsetneq X$. Dit heeft geen grote gevolgen, aangezien voor toepassingen van dit lemma het bestaan van een verzameling X met de genoemde eigenschappen meestal voldoende is.

Bewijs. De ongelijkheid $|A + X + D| \leq K|X + D|$ volgt uit lemma 3.1.
We bekijken voor het gelijkheidsgeval de afschattingen die gebruikt zijn in het bewijs van lemma 3.1. Verder gebruiken we dezelfde notatie als in dit bewijs. In het bewijs is gebruik gemaakt van inductie naar $|C|$. In de inductiestap van C naar $C' = C \sqcup \{c\}$ worden naast de inductiehypothese de volgende afschattingen gebruikt:

- we hebben $X + A + C' = (X + A + C) \cup ((X + A + c)\backslash(X' + A + c))$ en gebruiken de afschatting $|X + A + C'| \leq |X + A + C| + |(X + A + c)\backslash(X' + A + c)|$. Er geldt gelijkheid precies als we te maken hebben met een disjuncte vereniging, dus als en alleen als $(X + A + C) \cap ((X + A + c)\backslash(X' + A + c)) = \emptyset$;
- we gebruiken dat $|A + X'| \geq K|X'|$. Hier geldt vanwege onze extra aanname gelijkheid als en alleen als $X' = \emptyset$ of $X' = X$;
- we gebruiken dat $|Y| \leq |X'|$, waar $Y \subset X'$. Hier geldt gelijkheid als en alleen als $Y = X'$.

Dit geeft aanleiding tot drie voorwaarden voor het optreden van gelijkheid gegeven $C \subset D$ en $c \in D\backslash C$:

(A) er geldt $(X + A + C) \cap ((X + A + c)\backslash(X' + A + c)) = \emptyset$;

(B) er geldt $X' = \emptyset$ of $X' = X$;

(C) er geldt $Y = X'$.

We laten zien dat dit drietal voorwaarden equivalent is aan de voorwaarden die in het lemma genoemd worden. Hiermee is het lemma bewezen, aangezien er gelijkheid geldt als en alleen als er overal in het bewijs gelijkheid geldt ongeacht de "inductieroute" die we nemen van $\emptyset$ naar D.

We laten eerst zien dat als voor zekere $C \subset D$ en $c \in D\backslash C$ voldaan is aan (i) of (ii) dat dan voorwaarden (A)-(C) gelden. Stel eerst dat (i) het geval is. Dan is $Y = X$, dus ook $X' = X$ want $Y \subset X' \subset X$. Aan (B) en (C) is nu duidelijk voldaan. Aangezien $(X + A + c)\backslash(X' + A + c) = \emptyset$ is er ook voldaan aan (A). Stel nu dat (ii) geldt. Dan is duidelijk aan (A) voldaan. Verder volgt er dat $X' = \emptyset$, dus ook $Y = \emptyset$ en ook aan (B) en (C).

We laten nu zien dat als (A), (B) en (C) waar zijn, dat dan ook (i) of (ii) waar is. Stel eerst dat $X' = \emptyset$. Dan is $\emptyset = (X+A+C)\cap((X+A+c)\backslash(X'+A+c)) = (X+A+C)\cap(X+A+c)$, dus dan is (ii) waar. Stel nu dat $X' = X$. Dan volgt $Y = X$, dus voor alle $X = \{x \in X : x + c \subset X + C\}$. Dit impliceert dat $X + c \subset X + C$. □

De volgende stelling geeft het gelijkheidsgeval van gevolg 3.2.

Stelling 4.8 (Gevolg 3.2 met gelijkheidsgeval)**.** *Zij $A, B \subset Z$ niet-leeg en $K \geq 1$ zodat $|A + B| \leq K|B|$. Dan is er een niet-lege deelverzameling X van B zodat $|nA + X| \leq K^n|X|$*

voor $n \in \mathbb{Z}_{\geq 0}$.
Als er gelijkheid geldt voor zekere $n \geq 2$*, is* $A - A$ *bevat in* $\mathrm{Sym}(X)$.

Bewijs. Kies $X \subset B$ niet-leeg zodat $\frac{|A+X|}{|X|}$ minimaal is en vervolgens zodat $|X|$ minimaal is. Dan geldt er dat $\frac{|A+X'|}{|X'|} > K$ voor $\emptyset \subsetneq X' \subsetneq X$. Uit lemma 4.7 volgt dat $|A + X + D| \leq K|X + D|$ voor $D \subset Z$. Kies $D = (n-1)A$. Dan vinden we $|nA + X| \leq K|X + (n-1)A|$, waaruit met inductie volgt dat $|nA + X| \leq K^n|X|$ voor $n \geq 0$ (dit is geheel analoog aan het bewijs van gevolg 3.2).

We bewijzen nu de tweede bewering, over het gelijkheidsgeval. Als $|A| \leq 1$ is het duidelijk, dus stel dat $|A| \geq 2$.
Als er gelijkheid geldt voor een $n \geq 2$, geldt er ook voor alle lagere n gelijkheid. In het bijzonder geldt er gelijkheid voor $n = 2$, waaruit volgt dat er voor $D = A$ gelijkheid geldt in lemma 4.7. Kies $C = \{a\} \subset D$ en $c \subset D$ met $c \neq a$. Dan volgt er dat $X + c \subset X + a$ (i) of $(X + A + a) \cap (X + A + c) = \emptyset$ (ii). Merk op dat (ii) niet waar kan zijn, want voor $x \in X$ is $x + a + c$ bevat in beide verzamelingen aan de linkerkant. Dus voor iedere $a, c \in A$ met $a \neq c$ geldt $X + c \subset X + a$. Omdat dit even grote verzamelingen zijn, geldt er dus dat $X + c = X + a$ voor $a, c \in A$ (de voorwaarde $a \neq c$ is niet meer nodig dus die laten we vallen). Er geldt dus $X + c - a = X$ voor $a, c \in A$, dus $X + A - A = X$. Hieruit volgt dat $A - A \subset \mathrm{Sym}(X)$. □

Hiermee kunnen we bijvoorbeeld laten zien dat er in stelling 3.3 alleen gelijkheid geldt wanneer $\sigma(A) = 1$, oftewel dat er wanneer $\sigma(A) > 1$ geen gelijkheid geldt:

Stelling 4.9. *Zij* $A \subset Z$ *zodat* $\sigma(A) > 1$*. Dan is* $|nA| < \sigma(A)^n|A|$ *voor* $n \geq 1$.

Bewijs. De niet-strikte ongelijkheid volgt uit stelling 3.3. Verder geldt er voor $n = 1$ per aanname geen gelijkheid. Voor $n \geq 2$ is in het bewijs gebruik gemaakt van gevolg 3.2, dat is toegepast met $A = B$. Uit stelling 4.8 volgt nu dat als er gelijkheid geldt, dat dan $A - A \subset \mathrm{Sym}(X)$. Dat betekent hier dat $|A - A| \leq |\mathrm{Sym}(X)| \leq |X| \leq |A|$, want $X \subset B = A$. Oftewel $\delta(A) = 1$, en dan is ook $\sigma(A) = 1$. Als $\sigma(A) > 1$ geldt er dus geen gelijkheid. □

We gaan nu verder met de ongelijkheid $\sigma(A) \leq \delta(A)^2$. Om te bepalen wanneer $\sigma(A) = \delta(A)^2$ gaan we na wat we in het bewijs van deze ongelijkheid precies gebruikt hebben. De ondergrens hebben we als volgt afgeleid met behulp van de resultaten in hoofdstuk 3: uit gevolg 3.2 volgt het bestaan van een $X \subset -A$ zodat $|nA + X| \leq \delta(A)^n|X|$ voor $n \geq 0$, wat voor $n = 2$ leidt tot de conclusie

$$|A + A| \leq |2A + X| \leq \delta(A)^2|X| \leq \delta(A)^2|A|,$$

dus $\sigma(A) \leq \delta(A)^2$. We bewijzen dat uit $\sigma(A) = \delta(A)^2$ volgt dat $\sigma(A) = \delta(A) = 1$, oftewel dat A een nevenklasse is van een eindige deelgroep van Z.

Stelling 4.10. *Voor $A \subset Z$ geldt $\sigma(A) = \delta(A)^2$ als en alleen als $\sigma(A) = \delta(A) = 1$.*

Bewijs. Als $\sigma(A) = \delta(A) = 1$ geldt er $\sigma(A) = \delta(A)^2$. Stel nu dat $\sigma(A) = \delta(A)^2$, dus dat er gelijkheid geldt in de ongelijkheid $\sigma(A) \leq \delta(A)^2$. Als er gelijkheid geldt, geldt er overal in het bewijs gelijkheid. In het bijzonder geldt er gelijkheid in gevolg 3.2. Daaruit volgt met stelling 4.8 dat $A - A$ bevat is in $\mathrm{Sym}(X)$ voor zekere $X \subset -A$. Omdat X een vereniging nevenklassen van $\mathrm{Sym}(X)$ is, volgt hieruit dat $|A - A| \leq |\mathrm{Sym}(X)| \leq |X| \leq |A|$, dus $\delta(A) \leq 1$. Dus $\delta(A) = 1$, waaruit direct ook volgt dat $\sigma(A) = 1$. □

Gezien dit resultaat heeft het zin om de volgende vraag te stellen.

Vraag 4.11. *Bestaat er een constante $C < 2$ zodat $\sigma(A) \leq \delta(A)^C$ voor alle $A \subset Z$?*

Voor een verzameling A is het te verwachten dat $\sigma(A) \leq \delta(A)$ omdat elk tweetal verschillende elementen $a, b \in A$ twee verschillen $a - b$ en $b - a$ oplevert terwijl dit tweetal maar één som $a + b = b + a$ oplevert. Dit zou tot het vermoeden kunnen leiden dat de ongelijkheid $\sigma(A) \leq \delta(A)$ algemeen waar is, dus dat het antwoord op vraag 4.11 ja is voor $C = 1$. Het volgende voorbeeld laat echter zien dat er ook verzamelingen bestaan waarvoor $\sigma(A) > \delta(A)$ oftewel $|A + A| > |A - A|$: bekijk $A = \{0, 2, 3, 4, 7, 11, 12, 14\} \subset \mathbb{Z} = Z$. Voor deze verzameling geldt $|A+A| = 26$ en $|A-A| = 25$. Voor deze verzameling geldt dus $\sigma(A) = 26/8$ en $25/8$, dus hieruit volgt dat als het antwoord op vraag 4.11 bevestigend is voor een zekere C, dat dan $C \geq \frac{\log(26/8)}{\log(25/8)} = 1.03442$. Een verzameling A waarvoor $|A+A| > |A-A|$ heet ook wel een *MSTD-verzameling*, waarbij de afkorting staat voor "more sums than differences".

Een voorbeeld dat een hogere ondergrens voor C oplevert kan gevonden worden in [4]: voor de verzameling

$$B = \{0, 1, 2, 4, 5, 9, 12, 13, 17, 20, 21, 22, 24, 25, 29, 32, 33, 37, 40, 41, 42, 44, 45\} \subset \mathbb{Z}$$

met 23 elementen geldt $|B + B| = 91$ en $|B - B| = 83$ waaruit volgt dat

$$C \geq \frac{\log(91/23)}{\log(83/23)} = 1.0717.$$

Betere voorbeelden zijn mij niet bekend. Al met al lijkt er genoeg ruimte om de exponent 2 uit stelling 4.1 te verkleinen.

5 Conclusie

De eerste vraag waarin we geïnteresseerd waren, was wat er te zeggen is over de structuur van verzamelingen met een kleine somverzameling. We hebben gezien dat als de somverzameling

van een verzameling erg klein is, dat het dan mogelijk is om al zulke verzamelingen te klassificeren in termen van nevenklassen van eindige deelgroepen van Z (stelling 2.4): er geldt $\sigma(A) < \frac{3}{2}$ als en alleen als A bevat is in een nevenklasse van een deelgroep G van Z met $|G| < \frac{3|A|}{2}$. Verder hebben we de algemene stelling van Freiman (stelling 2.11) behandeld, die laat zien dat alle verzamelingen met $\sigma(A) \leq K$ voor een zekere constante K te beschrijven zijn in termen van gecentreerde convexe nevenklassenprogressies, een begrip dat twee mogelijke structuren omvat: de structuur van een groep en de structuur van een (gegeneraliseerde) rekenkundige rij. Voor torsiegroepen hebben we deze stelling ook bewezen, daarbij volstond alleen de groepsstructuur (zie stelling 3.5).

In hoofdstuk 4 hebben we laten zien dat verzamelingen met een kleine somverzameling ook een kleine verschilverzameling hebben en vice versa. Verzamelingen met een kleine somverzameling bleken ook te beschrijven zijn in termen van "approximate groups", een generalisatie van het begrip groep dat ook (gegeneraliseerde) rekenkundige rijen omvat (stelling 4.3). Om dit resultaat af te leiden hebben we eerst een aantal ongelijkheden bewezen die somverzamelingen relateren aan "hogere orde"-somverzamelingen en aan verschilverzamelingen; de meest algemene van deze ongelijkheden was die van Plünnecke-Ruzsa (stelling 3.4) die zegt dat $|nA - mA| \leq \sigma(A)^{m+n}|A|$.

Het tweede probleem dat we hebben bekeken, is hoe groot de somverzameling van een verzameling kan zijn gegeven de grootte van verschilverzameling en analoog hoe groot de verschilverzameling van een verzameling kan zijn gegeven de grootte van de somverzameling. Met behulp van de ongelijkheid van Plünnecke-Ruzsa hebben we de ongelijkheid

$$\sigma(A)^{1/2} \leq \delta(A) \leq \sigma(A)^2 \tag{5.1}$$

bewezen die een grens geeft op de grootte van de somverzameling gegeven de verschilverzameling en andersom. Ik heb zelf verder onderzoek gedaan naar deze ongelijkheden, met als doel om te bekijken of de exponenten $\frac{1}{2}$ en 2 optimaal zijn. Een voorwaarde daarvoor is dat het ongelijkheidsgeval in beide ongelijkheden alleen bestaat uit verzamelingen A waarvoor $\sigma(A) = \delta(A) = 1$, oftewel nevenklassen van eindige deelgroepen van Z. Dit blijkt inderdaad het geval te zijn: ik was in staat om het volgende resultaat te bewijzen.

Stelling 5.1. *Als voor een verzameling $A \subset Z$ ergens in de ongelijkheid* (5.1) *gelijkheid geldt, dan is A een nevenklasse van een eindige deelgroep van Z.*

Voor de ongelijkheid $\delta(A) \leq \sigma(A)^2$ was dit redelijk eenvoudig te bewijzen (stelling 4.5), maar dat was voor de ongelijkheid $\sigma(A) \leq \delta(A)^2$ (stelling 4.10) niet het geval. Om van die ongelijkheid het gelijkheidsgeval te bepalen had ik ook gelijkheidsgevallen nodig van onder andere het lemma van Petridis (zie lemma 4.7).

De eerste ongelijkheid $\delta(A) \leq \sigma(A)^2$ is scherp, zie stelling 4.6. Van de tweede ongelijkheid $\sigma(A) \leq \delta(A)^2$ is niet bekend of deze ook geldt voor een exponent $C < 2$; het is enkel bekend dat deze niet waar is voor een exponent $C < 1.07$. De theorie die is ontwikkeld in de laatste paragraaf, waaronder de gelijkheidsgevallen van de ongelijkheden in hoofdstuk 3, lijkt niet te kunnen worden toegepast om de ongelijkheid $\sigma(A) \leq \delta(A)^C$ te bewijzen voor een $C < 2$.

Referenties

[1] Gowers, T. A new way of proving sumset estimates (2011). Zie `http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/`.

[2] Green, B.J. What is... an approximate group? *Not. Am. Math. Soc.* **59** (2012), 655-656.

[3] Green, B.J., en Ruzsa, I.Z. Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc. (2)* **75** (2007), 163-175.

[4] Hegarty, P.V. Some explicit constructions of sets with more sums than differences. *Acta Arith.* **130** (2007), 61-77.

[5] Kneser, M. Abschätzungen der asymptotischen Dichte von Summenmengen. *Math. Z* **58** (1953), 459-484.

[6] Plünnecke, H. *Eigenschaften und Abschätzungen von Wirkingsfunktionen*, BMwF-GMD-22 Gesellschaft für Mathematik und Datenverarbeitung, Bonn 1969.

[7] Ruzsa, I.Z. Sumsets and structure (2008). Zie `http://www.math.cmu.edu/~af1p/Teaching/AdditiveCombinatorics/Additive-Combinatorics.pdf`.

[8] Ruzsa, I.Z. Sums of finite sets. In: *Number Theory: New York Seminar*, D.V. Chudnovsky, G.V. Chudnovsky en M.B. Nathanson, Springer-Verlag (1996), 281-293.

[9] Ruzsa, I.Z. An analog of Freiman's theorem in groups. In *Structure Theory of Set Addition*, *Astérisque* **258** (1999), 323-326.

[10] Sanders, T. The structure theory of set addition revisited. *Bull. Amer. Math. Soc.* **50** (2013), 93-127.

[11] Tao, T. en Vu, V. *Additive combinatorics*. Cambridge University Press (2006).