Vrije Universiteit Brussel
Falcuteit Wetenschappen en
Bio-Ingenieurswetenschappen
Departement Wiskunde

Groei van groepen

Bachelorproef 1

Charlotte Verwimp

Promotor: Prof. Dr. E. Jespers
Begeleider: G. Janssens

1e semester 2015-2016

Inhoudsopgave

Inleiding **ii**

1 Vrije groepen **1**
1.1 Constructie en uniciteit 1
1.2 Methoden om vrije groepen aan te tonen 3

2 Karakterisaties van klassieke klassen van groepen **7**
2.1 Nilpotente groepen 7
2.2 Oplosbare groepen 8

3 Groei van groepen **10**

4 Uniforme groei van oplosbare groepen **17**
4.1 Constructie van vrije (semi)groepen 17
4.2 Hoofdresultaat 20

A Bewijs van Voorbeeld 3.4. **A-1**

Inleiding

Deze bachelorproef gaat over de groei van groepen. Aangezien hiervoor een zekere voorkennis nodig is, beginnen we met een grondige basis uit de cursus Galoistheorie en definiëren we het begrip 'vrije groep'. Wat de groei van een groep is, wordt uitgelegd in Sectie 3. Kort gezegd telt deze het aantal woorden van lengte n of kleiner. Daarna is het heel eenvoudig aan te tonen dat deze groei polynomiaal, intermediair of exponentieel is. Zo heeft bijvoorbeeld een vrije groep een exponentiële groei.

In dit kader past dan ook het hoofddoel van deze bachelorproef, namelijk Stelling 1.4 uit een artikel van Emmanuel Breuillard [2] bewijzen. Wat zegt deze stelling juist? Wel, deze stelling zegt dat de groei van een oplosbare groep ofwel polynomiaal is (via de Stelling van Gromov), ofwel exponentieel is. De stelling zegt zelfs nog meer. Ze zegt ook hoe snel of sterk deze groep groeit, of anders gezegd hoe weinig voortbrengers je nodig hebt om een vrije semigroep voor te brengen. We willen dus exponentiële groei van groepen aantonen. De typische techniek die men daarvoor gebruikt, is het construeren van deelgroepen waarvan men weet dat ze een exponentiële groei hebben, bijvoorbeeld vrije groepen en vrije semigroepen. Wij zullen vrije semigroepen construeren en dit met behulp van het ping pong lemma.

Daarenboven moest ik ook bepaalde resultaten zelf opnieuw bewijzen, maar op een andere manier als de klassieke methode. Als dit het geval is, wordt het expliciet vermeld bij het bewijs.

Het onderwerp van deze bachelorproef is zeer actueel. Dat maakt natuurlijk dat je er heel veel informatie over vindt en je er heel uitgebreid over kan schrijven. Daarbuiten zijn er ook verbanden te vinden met andere gebieden in de wiskunde, zoals topologie of getaltheorie, wat het onderwerp nog interessanter maakt. Voor deze bachelorproef hebben we ons beperkt tot wat we essentieel vonden om de stelling van Breuillard te kunnen begrijpen.

Conventie: *Doorheen deze bachelorproef veronderstellen we dat* $\mathbb{N} = \{0, 1, 2, \cdots\}$ *en* $\mathbb{N}_0 = \{1, 2, \cdots\}$*, idem voor* $\mathbb{Z}$*,* $\mathbb{Q}$ *en* $\mathbb{R}$*.*

1 Vrije groepen

1.1 Constructie en uniciteit

In deze sectie definiëren we vrije groepen. We doen dit eerst op een constructieve manier en tonen dan dat ze voldoen aan de universele eigenschap. Vervolgens bewijzen we nog een belangrijk lemma, namelijk het ping-pong lemma, dat ons zal helpen om aan te tonen of groepen vrij zijn.

De constructie van een vrije groep gaat als volgt. Zij $X = \{x_i \mid i \in I\}$ een niet-lege verzameling en $X^{-1} = \{x_i^{-1} \mid i \in I\}$ disjunct daarvan. Een woord in het alfabet X is een eindige rij van symbolen uit $X \cup X^{-1}$, met e het lege woord. We kunnen een woord w dus schrijven als $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}$ met $x_i \in X$, $\varepsilon_i = \pm 1$, $r \geq 0$. Een woord is gereduceerd als het geen symbolen van de vorm $x_i^{\varepsilon} x_i^{-\varepsilon}$ bevat. Twee woorden u, v heten equivalent (genoteerd $u \sim v$) als ze gereduceerd (d.w.z. door het verwijderen van woorden van de vorm $x_i^{\varepsilon} x_i^{-\varepsilon}$) hetzelfde woord vormen. Het is eenvoudig na te gaan dat $\sim$ een equivalentierelatie is. De equivalentieklasse van u noteren we $[u]$. Elke equivalentieklasse van een woord in X bevat een uniek gereduceerd woord [14, p.46] en de equivalentieklassen van woorden in het alfabet X vormen een groep met de vermenigvuldiging $[u][v]=[uv]$ als bewerking. Deze groep heet de *vrije groep over* X of de *vrije groep voortgebracht door* X en $|X|$ heet de *rang* van F. Deze groep wordt genoteerd als $F(X)$. Als $|X| = n$ noteren we $F(X)$ ook als F_n.

Vervolgens tonen we aan dat elke groep, die eindig voortgebracht is, een quotiënt is van de vrije groep. Hiervoor maken we gebruik van volgende stelling.

Stelling 1.1. *Zij G een groep voortgebracht door Y en F de vrije groep over X. Als $\alpha : X \to Y$ een surjectie is, dan breidt deze afbeelding uit tot een groepepimorfisme $\sigma : F \to G$. Bijgevolg is elke groep een beeld van een vrije groep.*

Bewijs. Zij $Y = \{y_1, \cdots, y_n\}$ en $X = \{x_1, \cdots, x_m\}$ waarbij $n \leq m$ en zodat voor elke $y_i \in Y$ een $x_j \in X$ bestaat zodat $\alpha(x_j) = y_i$. De afbeelding α breidt dan uit naar een groepshomomorfisme door een element van F via zijn voortbrengers af te beelden naar een element van G. Aangezien α surjectief is en G wordt voortgebracht door Y zal ook de uitbreiding surjectief zijn. Ter verduidelijking, elke $g \in G$ zal te schrijven zijn als

$$g = y_{i_1} \cdots y_{i_k} = \alpha(x_{j_1}) \cdots \alpha(x_{j_k}) = \alpha(x_{j_1} \cdots x_{j_k}) = \alpha(f),$$

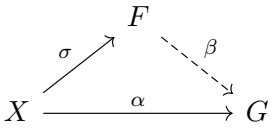
met $f \in F$, $y_{i_1}, \cdots, y_{i_k} \in Y$ en $x_{j_1}, \cdots, x_{j_k} \in X$. We krijgen dus het volgende commutatieve diagram

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ \downarrow & & \downarrow \\ F & \overset{\alpha}{\dashrightarrow} & G \end{array}$$

□

Als we in de vorige stelling $X = Y$ nemen, dan toont de stelling dat een vrije groep voldoet aan de universele eigenschap. Vandaar dat men een vrije groep ook vaak als volgt definiëert.

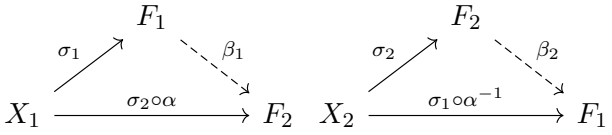
Definitie 1.2. *Zij F een groep, X een niet-lege verzameling, en $\sigma : X \to F$ een functie. Dan heet (F, σ) vrij op X als voor elke groep G en functie $\alpha : X \to G$, een uniek homomorfisme β: $F \to G$ bestaat zodat $\alpha = \sigma \circ \beta$. Een groep die vrij is op een niet-lege verzameling heet een vrije groep.*



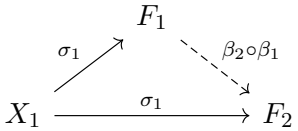
We tonen aan dat twee vrije groepen over eenzelfde niet-lege verzameling X steeds isomorf zijn, zodat we kunnen spreken over de vrije groep op X (d.w.z. $F(X)$ is uniek). We kunnen zelfs meer tonen.

Eigenschap 1.3. *Zij F_1 een vrije groep op een niet-lege verzameling X_1 en F_2 een vrije groep op een niet-lege verzameling X_2, met $|X_1| = |X_2|$. Dan geldt $F_1 \cong F_2$.*

Bewijs. Zij $\sigma_1 : X_1 \to F_1$, $\sigma_2 : X_2 \to F_2$ functies en $\alpha : X_1 \to X_2$ een bijectie. Dan hebben we de volgende commutatieve diagrammen



met β_1 en β_2 homomorfismen. Daaruit volgt dat $\beta_2 \circ \beta_1 \circ \sigma_1 = \beta_2 \circ \sigma_2 \circ \alpha = \sigma_1 \circ \alpha^{-1} \circ \alpha = \sigma_1$ en het diagram



commuteert. Echter ook zal de identiteitsafbeelding 1_{F_1} op F_1 dit diagram laten commuteren. Wegens de uniciteit geldt dan dat $\beta_2 \circ \beta_1 = 1_{F_1}$. Analoog krijgen we dat $\beta_1 \circ \beta_2 = 1_{F_2}$, zodat β_1 een ismomorfisme is en $F_1 \cong F_2$. □

Definitie 1.4. *Een vrije presentatie van een groep G is een epimorfisme π van een vrije groep naar G.*

Wegens Stelling 1.1 weten we dus dat een vrije presentatie $\pi : F \to G$ van een groep G steeds bestaat. Stellen we nu $R = \ker(\pi)$ dan is wegens de eerste isomorfismestelling [9] $R \triangleleft F$ en $F/R \cong G$. Elke groep is dus het quotiënt van een vrije groep. De elementen van R worden de *relaties* van de groep G genoemd. We kunnen G ook schrijven als $\langle X \mid S \rangle$ met X de voortbrengers van F en S de relaties in het alfabet X, zodat $S^F = \ker(\pi)$ (de normale sluiting van S is R). We noteren G ook als $\langle X \mid s = e, s \in S \rangle$, met e het lege woord.

Definitie 1.5. *Het paar $\langle X \mid S \rangle$ noemt men een presentatie van de groep G in functie van de voortbrengers X en de relaties S.*

Voorbeeld 1.6. 1. Diëdergroepen.

(a) $\mathrm{D}_8 = \langle a, b \mid a^4 = b^2 = e, ba = a^{-1}b \rangle \cong F(X)/R$ met $X = \{a, b\}$ en $R = \langle a^4, b^2, bab^{-1}a \rangle$.

(b) $\mathrm{D}_{2n} = \langle a, b \mid a^n = b^2 = e, ba = a^{-1}b \rangle \cong F(X)/R$ met $X = \{a, b\}$, $R = \langle a^n, b^2, bab^{-1}a \rangle$ en $n \in \mathbb{N}_0$.

2. Abelse groepen.

   (a) $G := \langle a, b \mid ab = ba \rangle \cong F(X)/R$ met F de vrije groep op $\{a, b\}$ en $R = \langle aba^{-1}b^{-1} \rangle$.

3. Cyclische groepen.

   (a) $\mathrm{C}_n = \langle x \mid x^n = e \rangle \cong F(X)/R$ met $X = \{x\}$, $R = \langle x^n \rangle$ en $n \in \mathbb{N}$.

   (b) $\mathrm{C}_n \times \mathrm{C}_m = \langle x, y \mid x^n = y^m = e, xy = yx \rangle \cong F(X)/R$ met $X = \{x, y\}$, $R = \langle x^n, y^m, xyx^{-1}y^{-1} \rangle$ en $n, m \in \mathbb{N}$.

1.2 Methoden om vrije groepen aan te tonen

Aantonen dat een gegeven groep vrij is, is in het algemeen niet eenvoudig. Soms werkt dit met de brute force methode, maar vaak gaat dit met een elegantere methode dankzij het ping-pong lemma.

Voorbeeld 1.7. Beschouw de matrices $a, b \in \mathrm{SL}_2(\mathbb{Z})$ gegeven door

$$a = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{en} \quad b = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \quad \text{met } m \in \mathbb{Z}, m \geq 2.$$

De deelgroep van $\mathrm{SL}_2(\mathbb{Z})$ voortgebracht door $\{a, b\}$ is een vrije deelgroep (d.w.z. $\langle a, b \rangle \cong F_2$ de vrije groep op 2 letters).

Eerst zal de brute force methode gebruikt worden en zullen we zien dat deze nogal omslachtig is.

Om na te gaan of een groep G vrij voortgebracht is, moet men aantonen dat geen enkel alternerend product van machten (niet nul) van de voortbrengers gelijk is aan e, het neutrale element van de groep. Elk element heeft dan een unieke uitdrukking als gereduceerd woord en dus geldt de injectiviteit als we het homomorfisme $\sigma : F \to G$ beschouwen met F de vrije groep op de voortbrengers van G. De surjectiviteit volgt uit Stelling 1.1. Dus σ is een isomorfisme en $G \cong F$.

Zij w een willekeurig element in de deelgroep van $\mathrm{SL}_2(\mathbb{Z})$ voortgebracht door $\{a, b\}$. We tonen nu dat $w \neq e$. Door eventueel te conjugeren door een macht van b mogen we veronderstellen dat

$$w = a^{n_1} b^{n_2} \cdots c^{n_r}$$

met $c = a$ of b, en alle $n_i \neq 0$. Zij z_i de eerste rij van de matrix $a^{n_1} b^{n_2} \cdots c^{n_i}$, $i = 1, \cdots, r$. Noteer

$$z_{2k-1} = a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} = (x_{2k-1}, x_{2k}), k = 1, \cdots, .$$

Dan is

$$\begin{aligned} z_{2k} &= z_{2k-1} b^{n_{2k}} = a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}} = (x_{2k+1}, x_{2k}), \\ z_{2k+1} &= z_{2k} a^{n_{2k+1}} = a^{n_1} b^{n_2} \cdots a^{n_{2k-1}} b^{n_{2k}} a^{n_{2k+1}} = (x_{2k+1}, x_{2k+2}), \end{aligned}$$

waarbij $x_{2k+1} = x_{2k-1} + mn_{2k}x_{2k}$ en $x_{2k+2} = x_{2k} + mn_{2k+1}x_{2k+1}$. Deze laatste twee vergelijkingen kunnen herleid worden tot

$$x_{i+2} = x_i + mn_{i+1}x_{i+1},$$

voor $i = 1, 2, \cdots, r-1$. Het resultaat volgt als we aantonen dat $|x_i|$ toeneemt als i stijgt van 1 tot $r+1$. Dit bewijzen we per inductie. Voor $i = 1, 2$ geldt dat x_1 het eerste element van de eerste rij is van

$$a^{n_1} = \begin{pmatrix} 1 & mn_1 \\ 0 & 1 \end{pmatrix},$$

en x_2 is het tweede element van die rij. We krijgen dus dat

$$|x_2| = |mn_1| \geq 1 = |x_1|.$$

De inductiestap is als volgt:

$$|x_{i+2}| \geq m|n_{i+1}||x_{i+1}| - |x_i| \geq 2|x_{i+1}| - |x_i| \geq |x_{i+1}| + 1.$$

Een alternatieve en eenvoudigere manier is via het ping-pong lemma [12]. Voor we dit lemma geven en bewijzen, herhalen we wat een actie is op een verzameling [9].

Definitie 1.8. *Zij X een verzameling en (G,∗) een groep. We zeggen dat G een linkeractie uitvoert op X als er een groepshomomorfisme $\pi : G \to Sym(X) : g \mapsto \pi_g = \pi(g)$ bestaat.*

Merk op dat voorgaande definitie equivalent is met het bestaan van een afbeelding $G \times X \to X : (g, x) \mapsto g \cdot x$, die voldoet aan:

1. $\forall g, h \in G, x \in X : (g * h) \cdot x = g \cdot (h \cdot x)$;
2. $\forall x \in X : e \cdot x = x$.

Lemma 1.9 (Ping-pong lemma). *Zij G een groep voortgebracht door twee elementen a en b. Veronderstel dat er een G-actie bestaat op een verzameling X zodat er niet-lege verzamelingen A,B ⊆ X met $B \nsubseteq A$ bestaan zodat geldt dat*

$$a^n \cdot B \subseteq A \quad en \quad b^n \cdot A \subseteq B$$

voor alle $n \in \mathbb{Z}\backslash\{0\}$. Dan is G vrij voortgebracht door $\{a, b\}$.

Bewijs. Zij F een vrije groep op $\{a, b\}$. Het is voldoende om een isomomorfisme $F \cong G$ te vinden die de identiteitsafbeelding op $\{a, b\}$ uitbreidt. Stelling 1.1 zegt ons dat er steeds een groephomomorfisme $\phi : F \to G$ bestaat die de identiteit op $\{a, b\}$ uitbreidt. Vermits G voortgebracht is door $\{a, b\}$, zal ϕ surjectief zijn. We moeten nu enkel nog de injectiviteit van ϕ aantonen en dan is het lemma bewezen. Veronderstel dat ϕ niet injectief is. Dan bestaat er per definitie een gereduceerd woord $e \neq w \in F$ zodat $\phi(w) = e$. We hebben vier situaties afhankelijk van de eerste en de laatste letter van w:

1. Het woord w begint en eindigt met een macht (niet nul) van a, dus w kan geschreven worden als $a^{n_0} b^{m_1} a^{n_1} \cdots b^{m_k} a^{n_k}$ voor een $k \in \mathbb{N}$ en $n_0, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{Z}\backslash\{0\}$. Dan geldt

$$\begin{aligned} B = e \cdot B = \phi(w) \cdot B &= a^{n_0} \cdot b^{m_1} \cdot a^{n_1} \cdot \ldots \cdot b^{m_k} \cdot a^{n_k} \cdot B \\ &\subseteq a^{n_0} \cdot b^{m_1} \cdot a^{n_1} \cdot \ldots \cdot b^{m_k} \cdot A && \text{ping!} \\ &\subseteq a^{n_0} \cdot b^{m_1} \cdot a^{n_1} \cdot \ldots \cdot a^{n_{k-1}} \cdot B && \text{pong!} \\ &\subseteq \cdots && \vdots \\ &\subseteq a^{n_0} \cdot B \subseteq A \end{aligned}$$

   wat het gegeven $B \nsubseteq A$ tegenspreekt.

2. Het woord w begint en eindigt met een macht (niet nul) van b, dus w kan geschreven worden als $b^{n_0}a^{m_1}b^{n_1}\cdots a^{m_k}b^{n_k}$ voor een $k \in \mathbb{N}$ en $n_0, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{Z}\backslash\{0\}$. Het woord awa^{-1} is dan een gereduceerd woord dat begint en eindigt met een macht (niet nul) van a. Gegeven ϕ is een groepshomomorfisme, dus krijgen we via de eerste situatie dat
$$e = \phi(a) \cdot e \cdot \phi(a)^{-1} = \phi(a) \cdot \phi(w) \cdot \phi(a^{-1}) = \phi(awa^{-1}),$$
wat weer een tegenspraak zal leveren.

3. Het woord w begint met een macht (niet nul) van a en eindigt met een macht (niet nul) van b, dus $w = a^n w' b^m$ met $m, n \in \mathbb{Z}\backslash\{0\}$ en w' een gereduceerd woord dat niet begint met een macht (niet nul) van a en niet eindigt met een macht (niet nul) van b. Zij $r \in \mathbb{Z}\backslash\{0, -n\}$. Dan begint en eindigt $a^r w a^{-r} = a^{r+n} w b^m a^{-r}$ met een macht (niet nul) van a. We krijgen weer
$$e = \phi(a^r) \cdot e \cdot \phi(a)^{-r} = \phi(a^r) \cdot \phi(w) \cdot \phi(a^{-r}) = \phi(a^r w a^{-r}),$$
wat volgens de eerste situatie een tegenspraak levert.

4. Het woord w begint met een macht (niet nul) van b en eindigt met een macht (niet nul) van a, dus $w = b^m w' a^n$ met $m, n \in \mathbb{Z}\backslash\{0\}$ en w' een gereduceerd woord dat niet begint met een macht (niet nul) van b en niet eindigt met een macht (niet nul) van a. De inverse van w bevindt zich in situatie 3 en vermits $\phi(w) = e$ zal ook $\phi(w^{-1}) = e$ wat volgens de derde situatie een tegenspraak levert.

Alle mogelijke situaties leveren een tegenspraak, dus ϕ is injectief en bijgevolg een isomorfisme.

□

Beschouw de matrices $a, b \in SL_2(\mathbb{Z})$ gegeven door
$$a := \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{en} \quad b := \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \quad \text{met } m \in \mathbb{Z}, m \geq 2.$$

Nu tonen we via het ping-pong lemma dat de deelgroep van $\mathrm{SL}_2(\mathbb{Z})$ voortgebracht door $\{a, b\}$ een vrije deelgroep is. Uit [9] weten we dat $\mathrm{SL}_2(\mathbb{Z})$ een linkeractie uitvoert op $\mathbb{R}^2$ via de afbeelding $SL_2(\mathbb{Z}) \times \mathbb{R}^2 \to \mathbb{R}^2 : (X, Y) \mapsto X \cdot Y = XY$ en dit is de gewone matrixvermenigvuldiging. Beschouw de verzamelingen
$$A := \{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| > |y|\} \quad \text{en} \quad B := \{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| < |y|\}$$
van $\mathbb{R}^2$. Dan zijn A en B niet leeg en $B \nsubseteq A$. Voor elke $n \in \mathbb{Z}\backslash\{0\}$ en voor elke $(x, y) \in B$ geldt
$$a^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & mn \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + mny \\ y \end{pmatrix} \in A$$

want wegens de driehoeksongelijkheid en het feit dat $|x| < |y|$ geldt

$$\begin{aligned} |x + mny| &\geq |mny| - |x| \\ &\geq |m||y| - |x| \\ &> |m||y| - |y| \\ &= (|m| - 1)|y| \\ &\geq |y|. \end{aligned}$$

Dus $a^n \cdot B \subseteq A$. Voor elke $(x, y) \in A$ geldt ook

$$b^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ mn & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ mnx + y \end{pmatrix} \in A$$

want wegens de driehoeksongelijkheid en het feit dat $|x| > |y|$ geldt

$$\begin{aligned} |mnx + y| &\geq |mnx| - |y| \\ &\geq |m||x| - |y| \\ &> |m||x| - |x| \\ &= (|m| - 1)|x| \\ &\geq |x|. \end{aligned}$$

Dus ook $b^n \cdot A \subseteq B$. Dit aangetoond, kunnen we het ping-pong lemma, Lemma 1.9, toepassen en besluiten dat $\langle a, b \rangle$ een vrije deelgroep is.

2 Karakterisaties van klassieke klassen van groepen

Naast vrije groepen zijn er ook nog andere klassen van groepen. In deze sectie herhalen we wat nilpotente, oplosbare en polycyclische groepen zijn en geven hun hoofdkarakterisaties.

2.1 Nilpotente groepen

Definitie 2.1. *Een groep G heet nilpotent als er normale deelgroepen $G_0, G_1, \cdots, G_n$ van G bestaan zodat*

1. $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$,
2. $G_{i+1}/G_i \subseteq Z(G/G_i)$ *voor* $0 \leq i \leq n-1$.

Een rij

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n$$

van normale deelgroepen van een groep G noemt men een *centrale rij* als

$$G_{i+1}/G_i \subseteq Z(G/G_i)$$

voor $0 \leq i \leq n$.

Definieer $Z_0(G) = \{e\}$ en voor $i \geq 1$ is $Z_i(G)$ de deelgroep van G gedefinieerd door

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)).$$

Dus is $Z_i(G) = \{g \in G \mid \forall h \in G : [g,h] \in Z_{i-1}(G)\}$ en de rij $\{Z_i(G) \mid i \geq 0\}$ noemt men de *stijgende (of hoogste) centrale rij* van G.

We herhalen wat een commutator en een commutatordeelgroep van een groep zijn [8, p.37].

Definitie 2.2. *De commutator van twee elementen x en y van een groep G wordt gegeven door $[x,y] = x^{-1}y^{-1}xy$. De commutatordeelgroep is de deelgroep van G voortgebracht door alle commutatoren. Notatie: $G' = [G,G] = \langle [g,h] \mid g,h \in G \rangle$.*

De commutatordeelgroep is de kleinste normale deelgroep van G zodat de corresponderende quotiëntgroep abels is.

We noteren $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle$ voor de commutator van H en K, met H en K deelgroepen van G.

Definieer nu $G^1 = G, G' = G^2 = [G,G]$ en $G^{i+1} = [G^i, G]$ voor $i \geq 2$. Dan noemt men

$$G = G^1 \supseteq G^2 \supseteq G^3 \supseteq \cdots$$

de *dalende (of laagste) centrale rij* van G.

Uit de vorige definities halen we nu drie equivalente eigenschappen [8, p.41].

Eigenschap 2.3. *Zij G een groep. Dan zijn equivalent*

1. *G is nilpotent,*
2. *$G^{n+1} = \{e\}$ voor een zekere $n \in \mathbb{N}$,*
3. *$Z_n(G) = G$ voor een zekere $n \in \mathbb{N}$.*

Indien G nilpotent is, dan noemt men het kleinste natuurlijk getal n zodat $Z_n(G) = G$ de *nilpotentieklasse* van G.

Voorbeeld 2.4. 1. Abelse groepen zijn nilpotent, want er geldt dat $[G, G] = \{e\}$.

2. D_8 is nilpotent, want $Z(D_8) = \langle a^2 \rangle$ en $Z_2(D_8) = D_8$ of $G^3 = \{e\}$.

3. $S_3 = \langle a, b \mid a^2 = b^2 = (ab)^3 = e \rangle$ is niet nilpotent, want $(S_3)' = [(S_3)', S_3] = S^3$ zodat $S_3' = S^3 = \cdots \neq \{e\}$.

Voor een eindige nilpotente groep bestaat er een andere karakterisatie met behulp van Sylow p-deelgroepen [9, p. 110].

Definitie 2.5. *Een Sylow p-deelgroep van een groep G is een maximale p-deelgroep van G. Deze deelgroepen hebben orde p^n met n maximaal zodat $|G| = p^n m$ en $p \nmid m$ wegens de Sylow Stellingen.*

Definitie 2.6. *Een eindige groep G is nilpotent als voor elk priemgetal p de groep G een normale Sylow p-deelgroep bevat. Dus $G = \prod_p S_p$ [8, p. 32].*

Equivalent met de vorige definitie, kunnen we ook zeggen dat een eindige groep G nilpotent is als elke twee elementen g_1, g_2 van G, met $ggd(o(g_1), o(g_2)) = 1$, commuteren. Hiermee zien we dat nilpotente groepen korte veralgemeningen zijn van abelse groepen.

2.2 Oplosbare groepen

Definitie 2.7. *Een groep G heet oplosbaar als er normale deelgroepen $G_0, G_1, \cdots, G_n$ van G bestaan zodat*

1. $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$,

2. G_{i+1}/G_i *is abels voor* $0 \leq i \leq n-1$.

Definieer nu $G^{(0)} = G$ en $G^{(n)} = (G^{(n-1)})' = [G^{(n-1)}, G^{(n-1)}]$ voor $n \geq 1$. Dan noemen we

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

de *afgeleide reeks* van G.

Ook hier zijn weer enkele equivalente eigenschappen [8, p.37].

Eigenschap 2.8. *Zij G een groep. Dan zijn equivalent*

1. *G is oplosbaar,*

2. $G^{(n)} = \{1\}$ *voor een zekere* $n \in \mathbb{N}$.

De kleinste n zodat $G^{(n)} = \{1\}$ noemt men de afgeleide lengte van G. Notatie: dl(G).

Definitie 2.9. *Zij G een groep, dan heet G meta-abels als $dl(G) = 2$. Het is dus een groep wiens commutatordeelgroep abels is. Men noemt deze groepen ook wel abels-bij-abels.*

Algemeen definiëren we het volgende.

Definitie 2.10. *Voor eigenschappen X en Y van groepen zegt men dat een groep G X-bij-Y is als er een normale deelgroep N van G bestaat zodat N eigenschap X heeft en G/N eigenschap Y heeft.*

Voorbeeld 2.11.

1. Abelse groepen zijn oplosbaar en hebben als afgeleide lengte 1 aangezien $G^{(1)} = G' = [G, G] = \{e\}$.
2. D_8 is oplosbaar, want D_8 heeft afgeleide lengte 2 aangezien $D_8^{(1)} = \langle a^2 \rangle$ abels is.
3. $S_3 \cong D_6$, dan is $G' = [S_3, S_3] = A_3 \cong C_3$ abels en dus is $G^{(2)} = \{e\}$.
4. Eindige groepen van oneven orde zijn oplosbaar[1].
5. A_4 is oplosbaar met afgeleide lengte 2, namelijk $(A_4)' = [A_4, A_4] = \{e, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$ en dus is $(A_4)^{(2)} = \{e\}$.

Uit de definities merken we op dat nilpotente groepen oplosbaar zijn, want als G_{i+1}/G_i in het centrum van G/G_i zit, dan commuteren al zijn elementen met de elementen van G/G_i en dus ook met die van G_{i+1}/G_i. Bijgevolg is G_{i+1}/G_i abels.

Een deelklasse van deze oplosbare groepen is de klasse van de polycyclische groepen.

Definitie 2.12. *Een groep G heet polycyclisch als er normale deelgroepen $G_0, G_1, \cdots, G_n$ bestaan zodat*

1. $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$,
2. G_{i+1}/G_i *is cyclisch voor* $0 \leq i \leq n-1$.

Polycyclische groepen zijn dus oplosbaar. Ook geldt dat eindig voortgebrachte nilpotente groepen steeds polycyclisch zijn [13, p. 132].

Voorbeeld 2.13.

1. Abelse groepen.
2. D_8 is polycyclisch, want $\langle a \rangle \lhd D_8$ en $D_8/\langle a \rangle = \langle b \rangle$ en $\langle b \rangle$ is cyclisch.
3. A_4 is niet polycyclisch, maar wel oplosbaar.

Voor eindig voortgebrachte groepen hebben we dus de volgende implicaties:

$$\text{abels} \Rightarrow \text{nilpotent} \Rightarrow \text{polycyclisch} \Rightarrow \text{oplosbaar}.$$

[1] Dit is de stelling van Feit en Thompson en is een belangrijk resultaat voor de classificatie van eindige simpele groepen. Het bewijs bevat zo'n 300 pagina's [5].

3 Groei van groepen

Nu we verschillende groepen gedefiniëerd hebben, zullen we de groei van deze groepen bestuderen. *Vanaf nu beschouwen we enkel nog groepen die eindig voortgebracht zijn.*

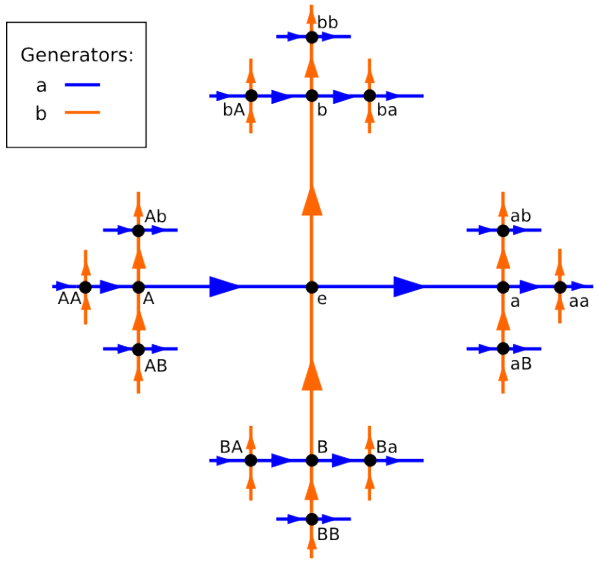
Een eerste belangrijk begrip dat we nodig zullen hebben, is de lengte van een element in een eindig voortgebrachte groep.

Definitie 3.1. *Zij G een eindig voortgebrachte groep en S een voortbrengende verzameling. De lengtefunctie $l_S : G \to \mathbb{N}$ beeldt een element $g \in G$ af op de kleinste $n \in \mathbb{N}$ zodat er een $s_1, s_2, \cdots, s_n \in S \cup S^{-1}$ bestaan met $g = s_1 s_2 \cdots s_n$.*

De lengtefunctie past natuurlijk in de context van Cayley graffen. Zo'n graffen worden meestal met een kleuring gedefinieerd, maar dat zal in ons geval niet echt nodig zijn. We behouden de kleuring wel, maar beschouwen dit gewoon als een label. De kleuring geeft uiteindelijk visueel wel een duidelijker beeld.

Definitie 3.2. *Het Cayley graf Cay(G,S) van een groep G met voortbrengende verzameling S is een gekleurd gerichte graf dat als volgt wordt geconstrueerd.*

- *Elk element g van G is toegewezen aan een knooppunt of top. De verzameling van alle toppen V(Cay(G,S)) van Cay(G,S) is dus precies G.*
- *Elk voortbrengend element s uit S krijgt een label (kleur) c_s om het graf overzichtelijker te maken.*
- *Voor elke $g \in G$ en $s \in S$ zijn de punten die corresponderen tot de elementen g en gs verbonden door een gerichte boog met label c_s. De bogenverzameling E(Cay(G,S)) van Cay(G,S) bestaat uit de paren van de vorm (g, gs) met labeling s.*



Figuur 1: Het Cayley graf van de vrije groep F_2 [18].

Bovenstaande afbeelding geeft het Cayley graf van de vrije groep F_2 met voortbrengers a en b weer, waar $A = a^{-1}$ en $B = b^{-1}$. Op een Cayley graf kunnen we ook een metriek definiëren.

Dat doen we als volgt: voor elke $g, h \in G$ stellen we $d_S(g,h) = \min\{l_S(w) \mid gw = h\}$. Het is dus het minimum aantal bogen of kortste pad tussen g en h in het Cayley graf. Een cyclus in een Cayley graf $Cay(G,S)$ stemt overeen met een relatie in de groep G. Met deze inleidende begrippen, kunnen we vervolgens de groeifunctie definiëren.

Definitie 3.3. *Zij G een eindig voortgebrachte groep met S een voortbrengende verzameling. Beschouw $B_n(G,S) = \{g \in G \mid l_S(g) \leq n\} = (S \cup S^{-1})^n$ de bol met straal n in het Cayley graf Cay(G,S) met als middelpunt de top horende bij het neutrale element e. De groeifunctie van G is gedefinieerd door $\gamma_{G,S}(n) = |B_n(G,S)|$.*

Voorbeeld 3.4.

1. Zij $F_2 = \langle a,b \rangle = \{a^{i_1}b^{i_2}\cdots a^{i_l}b^{i_m} \mid i_1, \cdots, i_m \in \mathbb{Z}\}$ met $S = \{a,b\}$. Dan is de groeifunctie $\gamma_{F_2,\{a,b\}}(n) = 1 + \sum_{i=1}^{n} 4 \cdot 3^{i-1}$. Dit is eenvoudig te verklaren, want achter de laatste letter van het woord kan steeds alles behalve de inverse van dit element geplaatst worden. Voor onze eerste letter hebben we dus vier keuzes $\{a, b, a^{-1}, b^{-1}\}$ en vanaf dan heb je telkens drie keuzes. Algemeen heeft F_m met $S = \{a_1, \cdots a_m\}$ de groeifunctie $\gamma_{F_m,\{a_1,\cdots,a_m\}}(n) = 1 + \sum_{i=1}^{n} 2m(2m-1)^{i-1}$ [11, p. 2].

2. Zij $\mathbb{Z} \times \mathbb{Z} = \langle a,b \mid ab = ba \rangle$ met $S = \{a,b\}$. Dan is de groeifunctie $\gamma_{\mathbb{Z}\times\mathbb{Z},\{a,b\}}(n) = 1 + \sum_{i=1}^{n} 4i = 1 + 4(\frac{n(n+1)}{2})$ [11, p. 4].

3. Zelf heb ik zonder referenties bewezen dat de groeifunctie van $\mathbb{Z}_m$ met voortbrengers $s_1, \cdots, s_m$ gelijk is aan

$$\begin{aligned}\gamma_{\mathbb{Z}_m,\{s_1,\cdots,s_m\}}(n) = &\sum_{p=0}^{n}\sum_{i=1}^{m} 2^i \binom{m}{i} \Bigg[\binom{p+(i-1)}{i-1} \\ &- \left(\sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{p+(i-1)-(2j-1)+1}{i-2} \right) \\ &- \begin{cases} 0 & \text{als i even} \\ \binom{p+(i-1)-(2\lfloor \frac{i}{2} \rfloor + 1)}{i-2} & \text{als i oneven} \end{cases} \Bigg].\end{aligned}$$

   Voor het bewijs verwijzen we naar Bijlage A, aangezien dit niet noodzakelijk is voor het vervolg van deze bachelorproef.

Merk op dat de groeifunctie van een groep afhankelijk is van zijn voortbrengende verzameling. Daarom zullen we een equivalentierelatie invoeren. De groeifunctie is een niet dalende functie $f : \mathbb{N} \to \mathbb{R}^+$. Op een verzameling van monotone niet dalende functies $f, g : \mathbb{N} \to \mathbb{R}^+$ kan men de relatie $\preceq$ definiëren:

$f \preceq g \Leftrightarrow$ Er bestaan $A, C > 0$ en er bestaat $n_0 \in \mathbb{N}$ zodat voor elke $n \geq n_0 : f(n) \leq Ag(Cn)$.

De functies heten equivalent als $f \preceq g$ en $g \preceq f$, genoteerd $f \sim g$. Dit is duidelijk een equivalentierelatie. De equivalentieklasse van γ_G wordt de *groei van G* genoemd. De groeifunctie $\gamma_{G,S}$ is afhankelijk van S, maar de groei γ_G niet.

Eigenschap 3.5. *Zij S_1 en S_2 twee eindig voortbrengende verzamelingen van een eindig voortgebrachte groep G, dan $\gamma_{G,S_1} \sim \gamma_{G,S_2}$.*

Bewijs. Schrijf elk element s_1 van S_1 als woord van elementen in S_2. Stel A_1 de maximale lengte t.o.v. S_2 van deze woorden. Doe dit ook voor de elementen s_2 uit S_2 t.o.v. S_1 en stel A_2 gelijk aan deze maximale lengte. Stel nu $A = \max\{A_1, A_2\}$. Er volgt dan:

$$\begin{array}{lll} \text{Voor elke } x \in G: & \text{als } l_{S_2}(x) = n, \text{ dan } l_{S_1}(x) \leq A_2 n \leq An & \Rightarrow l_{S_1}(x) \leq A_2 l_{S_2}(x) \leq A l_{S_2}(x) \\ & & \Rightarrow \gamma_{G,S_2}(n) \leq \gamma_{G,S_1}(An); \\ & \text{als } l_{S_1}(x) = n, \text{ dan } l_{S_2}(x) \leq A_1 n \leq An & \Rightarrow l_{S_2}(x) \leq A_1 l_{S_1}(x) \leq A l_{S_2}(x) \\ & & \Rightarrow \gamma_{G,S_1}(n) \leq \gamma_{G,S_2}(An). \end{array}$$

□

Dus vanaf nu mogen we bij het bepalen van de groei van een groep zijn voortbrengende verzameling op een gepaste wijze kiezen.

Uit [11, p. 5, p. 19] halen we de volgende eigenschappen over de groei van groepen.

Eigenschap 3.6. *1. Zij G een eindig voortgebrachte groep, H een eindig voortgebrachte deelgroep van G en N een eindig voortgebrachte normale deelgroep van G. Dan gelden de volgende eigenschappen.*

(a) $\gamma_H \preceq \gamma_G$ en $\gamma_{G/N} \preceq \gamma_G$;

(b) Als $[G : H] < \infty$, dan $\gamma_H \sim \gamma_G$;

(c) Als N eindig is, dan is $\gamma_{G/N} \sim \gamma_G$.

2. Zij G_1, G_2 groepen voortgebracht door eindige verzamelingen S_1 en S_2 en met groeifuncties γ_{G_1,S_1} en γ_{G_2,S_2}. Dan is het direct product $G = G_1 \times G_2$ eindig voortgebracht door $S = (S_1 \times \{e\}) \cup (\{e\} \times S_2)$ met groeifunctie $\gamma_{G,S}(n) = \gamma_{G_1,S_1}(n)\gamma_{G_2,S_2}(n)$.

Bewijs.

1. (a) Neem H een deelgroep van G die eindig voortgebracht is, $H = \langle y_1, \cdots, y_n \rangle$ met $y_i \in G$. Schrijf elke y_i in functie van de voortbrengers van G. Stel $k = \max\{l_S(y_i) \mid 1 \leq i \leq n\}$ met S een voortbrengende verzameling van G. Er volgt dan meteen dat $\gamma_H(n) \leq \gamma_G(kn)$ en dus is $\gamma_H(n) \preceq \gamma_G(n)$.
   Neem nu N een normale deelgroep van G. Veronderstel dat G eindig voortgebracht is door $S_G = \{s_1, \cdots, s_m\}$. De quotiëntgroep $G/N = \langle s_1 N, \cdots, s_m N \rangle$ heeft als voortbrengende verzameling $S_{G/N} = \{s_1 N, \cdots, s_m N\}$. Er bestaat dan steeds een afbeelding $B_{S_{G/N}}(G/N, n) \to B_{S_G}(G, n)$ die goed gedefinieerd en injectief is. Fixeer namelijk voor iedere nevenklasse een representant. Voor deze representant $\overline{g}$ fixeer je vervolgens een ontbinding van de vorm $s_{i_1} \cdots s_{i_n} N$. Beeld nu onder de afbeelding iedere representant $\overline{g} = gN$ af op $s_{i_1} \cdots s_{i_n} N$. Deze afbeelding is goed gedefinieerd en injectief. Via deze injectieve afbeelding zien we meteen dat $\gamma_{G/N}(n) \leq \gamma_G(n)$. Aangezien er woorden zijn van lengte n in G die mogelijk niet bereikt worden door woorden van lengte n in G/N, geldt niet noodzakelijk een gelijkheid.

   (b) Stel $[G : H] = s < \infty$ met transversaal $T = \{a_1, \cdots, a_s\}$ ($G = a_1 H \biguplus \cdots \biguplus a_s H$). Zij $S = \{s_1, \cdots, s_m\}$ een voortbrengende verzameling van G. Definieer r als maximale lengte van de elementen $\{a_1, \cdots, a_s\}$ t.o.v. de voortbrengers $s_1, \cdots, s_m$ van G. Neem $h \in H$ zodat $a_i h \in G$ met $l_S(a_i h) \leq n$. Stel $k = l_S(h) \leq n + r$. We kunnen $h \in H$ ook schrijven in functie van de voortbrengende verzameling $S = \{s_1, \cdots, s_m\}$, dus $h = y_1 \cdots y_k$, waarbij elke y_i gelijk is aan een

s_j of s_j^{-1}. We zullen nu h schrijven in functie van elementen van H. Neem a_{i_1} zodat $a_{i_1}H = y_1H$ en schrijf $h = y_1a_{i_1}a_{i_1}^{-1}y_2\cdots y_k$. Neem dan a_{i_2} zodat $a_{i_1}H = y_2a_{i_2}H$ en schrijf $h = y_1a_{i_1}a_{i_1}^{-1}y_2a_{i_2}a_{i_2}^{-1}y_3\cdots y_k$, etc. Uiteindelijk krijgen we $h = y_1a_{i_1}a_{i_1}^{-1}y_2a_{i_2}a_{i_2}^{-1}\cdots a_{i_{k-1}}^{-1}y_ka_{i_k}a_{i_k}^{-1}$. Wegens de keuzes van $a_{i_1},\cdots,a_{i_n}$ geldt dat $y_1a_{i_1}, a_{i_{j-1}}^{-1}y_ja_{i_j} \in H$ voor $j = 2,\cdots,k$. Daaruit volgt dat $a_{i_k} = e$, aangezien $h \in H$. Het element h bestaat dus uit hoogstens k elementen uit H en we hebben getoond dat $l_H(h) \leq k$. Bijgevolg is $\gamma_G(n) \leq [G:H]\gamma_H(n+r) \leq [G:H]\gamma_H((r+1)n)$. Dat $\gamma_H \preceq \gamma_G$ volgt uit (a) en zo hebben we bewezen dat $\gamma_H \sim \gamma_G$.

(c) Neem nu N eindig. Dat $\gamma_{G/N}(n) \leq \gamma_G(n)$ hebben we reeds bewezen. We bewijzen nu dat $\gamma_G(n) \preceq \gamma_{G/N}(n)$. Neem $g = s_{i_1}\cdots s_{i_m} \in G$, dan is $\overline{g} = gN = s_{i_1}N\cdots s_{i_m}N \in G/N$. Er bestaat steeds een $n \in N$ zodat $g = s_{i_1}\cdots s_{i_m}n$ en voor zo'n n zijn er $|N|$ mogelijkheden. Dus exact $|N|$ elementen van G worden een element $\overline{g}$ van G/N. We besluiten dat $\gamma_G(n) \leq |N|\gamma_{G/N}(n)$, waarbij $|N| \in \mathbb{N}_0$.

2. Voor alle (g_1,g_2) uit G met $g_1 \in G_1$ en $g_2 \in G_2$ is $l_S(g_1,g_2) = l_{S_1}(g_1)+l_{S_2}(g_2)$. Definieer $\delta_{G_i,S_i}(n) = |\{g_i \in G_i \mid l_{S_i}(g_i) = n\}|$. Het aantal elementen in G met exacte lengte n zal dan gelijk zijn aan $\sum_{k=0}^{n}\delta_{G_1,S_1}(k)\delta_{G_2,S_2}(n-k)$. Er volgt dat

$$\begin{aligned}
\gamma_{G,S}(n) &= \sum_{i=0}^{n}\sum_{k=0}^{i}\delta_{G_1,S_1}(k)\delta_{G_2,S_2}(i-k)\\
&= \delta_{G_1,S_1}(0)\delta_{G_2,S_2}(0) + \delta_{G_1,S_1}(0)\delta_{G_2,S_2}(1) + \delta_{G_1,S_1}(1)\delta_{G_2,S_2}(0) + \cdots\\
&\quad + \delta_{G_1,S_1}(0)\delta_{G_2,S_2}(n) + \delta_{G_1,S_1}(1)\delta_{G_2,S_2}(n-1) + \cdots + \delta_{G_1,S_1}(n)\delta_{G_2,S_2}(0)\\
&= (\sum_{i=0}^{n}\delta_{G_1,S_1}(i))(\sum_{i=0}^{n}\delta_{G_2,S_2}(i))\\
&= \gamma_{G_1,S_1}(n)\gamma_{G_2,S_2}(n).
\end{aligned}$$

□

Met deze eigenschappen kunnen we de verschillende typen van de groei onderzoeken. Voor een eindig voortgebrachte groep G waarbij het aantal elementen in de kleinste voortbrengende verzameling gelijk is aan m geldt steeds dat $\gamma_G \preceq \gamma_{F_m}$. Inderdaad, want uit Stelling 1.1 volgt dat elke groep het quotiënt is van een vrije groep en Eigenschap 3.6 geeft ons dan het resultaat. De groeifunctie voor de vrije groep F_m is $\gamma_{F_m}(n) = 1 + \sum_{i=1}^{n} 2m(2m-1)^{i-1}$ waaruit volgt dat $\gamma_{F_m} \preceq m^n \sim e^n$ met e de constante van Napier (grondtal van de natuurlijke logaritme). Een groep G kan dus hoogstens een exponentiële groei hebben. Een groeifunctie equivalent met e^{n^d} met $d > 1$ zal bijvoorbeeld niet mogelijk zijn.

Definitie 3.7. *Een groep G heeft een exponentiële groei als $\gamma_G(n) \sim e^n$ en een subexponentiële groei als de limiet $\lim_{n\to\infty}\frac{\ln(\gamma_G(n))}{n}$ convergeert naar nul. Als $\gamma_G(n) \preceq n^d$ voor een $d \geq 1$, zeggen we dat de groep G een polynomiale groei heeft en G heeft een superpolynomiale groei als de limiet $\lim_{n\to\infty}\frac{\ln(\gamma_G(n))}{\ln(n)}$ convergeert naar oneindig. Indien de groep zowel een subexponentiële als een superpolynomiale groei heeft, dan zeggen we dat ze een intermediaire groei heeft.*

Aangezien $\gamma_G(n)$ monotoon stijgend is, is er een trichotomie van groei genres: polynomiale, intermediaire en exponentiële groei. Dat een eindig voortgebrachte groep hoogstens een exponentiële groei heeft, hebben we al getoond. Hierbij zal $\lim_{n\to\infty}\frac{\ln(\gamma_G(n))}{n} \leq \lim_{n\to\infty}\frac{\ln(e^n)}{n} = 1$.

Anderzijds is een groeifunctie ook een niet-dalende functie en dus zal de groei minstens constant zijn. Dit is bijvoorbeeld het geval als G eindig is (zie Eigenschap 3.9). Hierbij zal $\lim_{n\to\infty} \frac{\ln(\gamma_G(n))}{\ln(n)} = \lim_{n\to\infty} \frac{\ln(c)}{\ln(n)} = 0$, met c een constante. Voor een polynomiale groei geldt dat $\lim_{n\to\infty} \frac{\ln(\gamma_G(n))}{\ln(n)} \leq \lim_{n\to\infty} \frac{\ln(n^d)}{\ln(n)} = d$ voor een $d \geq 1$. Als de groei enerzijds groter is dan polynomiaal, dus superpolynomiaal, en anderzijds kleiner is dan exponentieel, dus subexponentieel, dan is ze intermediair. De groei van een eindig voortgebrachte groep is dus ofwel polynomiaal, ofwel intermediar, ofwel exponentieel.

Voorbeeld 3.8. We hernemen de voorbeelden uit Voorbeeld 3.4.

1. $\gamma_{F_m,\{a_1,\cdots,a_m\}}(n) = 1 + \sum_{i=1}^{n} 2m(2m-1)^{i-1} \sim e^n$, dus F_m heeft een exponentiële groei.

2. $\gamma_{\mathbb{Z}\times\mathbb{Z},\{a,b\}}(n) = 1 + \sum_{i=1}^{n} 4i = 1 + 4(\frac{n(n+1)}{2}) \preceq n^2$, dus $\mathbb{Z}\times\mathbb{Z}$ heeft een polynomiale groei.

Eigenschap 3.9. *Eindige groepen hebben een constante groei.*

Bewijs. Zij G is een eindige groep met $|G| = n$, dan is $\gamma_G(k) \leq n$ aangezien G slechts n elementen heeft. We hebben $\gamma_G(k) \leq n \leq nk \preceq k^1$ en G heeft een polynomiale groei. Vanaf een bepaalde lengte k geldt dat $\gamma_G(k) = |G|$ en dus is de groei constant. □

Eigenschap 3.10. *Vrije abelse groepen hebben een polynomiale groei.*

Bewijs. Stel G een vrije abelse groep met m voortbrengers $S = \{s_1, \cdots, s_m\}$. Vermits G abels is kan elk element g van G geschreven worden onder de vorm $g = s_1^{i_1} \cdots s_m^{i_m}$ met $i_j \in \mathbb{Z}$ voor $j = 1, \cdots, m$. De lengte van g is bijgevolg $l(g) = |i_1| + \cdots + |i_m|$. Het aantal woorden van lengte n of minder is dan $\gamma_G(n) = |\{(i_1, \cdots, i_m) \in \mathbb{Z}^m \mid |i_1| + \cdots + |i_m| \leq n\}| \leq n^m$ en we besluiten dat G een polynomiale groei heeft. □

Met behulp van het voorgaande is het mogelijk om een eigen bewijs te geven voor de volgende stelling.

Eigenschap 3.11. *Eindig voortgebrachte nilpotente groepen hebben een polynomiale groei.*

Bewijs. Zij G een nilpotente groep met voortbrengende verzameling $S = \{s_1, \cdots, s_m\}$. We bewijzen per inductie op de nilpotentieklasse k van G dat G een polynomiale groei heeft.

Als $k = 1$, dan is $G^1 = G = \{e\}$ en valt er niets te bewijzen.

Voor $k = 2$ hebben we dat $G^2 = [G, G] = \{e\}$, dus G is abels. Uit Eigenschap 3.10 volgt dan dat G een polynomiale groei heeft.

Stel dat de eigenschap geldt voor nilpotentieklasse $k-1$ (inductiehypothese), dan tonen we dat ze ook geldt voor nilpotentieklasse k. Als G nilpotentieklasse k heeft, dan heeft $G^2 = [G, G]$ nilpotentieklasse $k-1$. We kunnen op G^2 de inductiehypothese toepassen, dus $\gamma_{G^2}(n) \preceq n^d$ voor een $d \geq 1$.

Neem nu $x \in G$ met lengte ten hoogste n, dus $x = x_{i_1} \cdots x_{i_n}$ waar elke $x_i \in S \cup S^{-1}$. We beweren dat $x = s_1^{i_1} \cdots s_m^{i_m} a$, met $a \in [G, G]$ en $0 \leq |i_j| \leq n$. Dit tonen we aan door telkens twee opeenvolgende elementen te verwisselen. Concreter, we zoeken de eerste s_1 of s_1^{-1} die we tegenkomen in x en verplaatsen die helemaal naar links. Om x_{i_j} en $x_{i_{j+1}}$ (twee opeenvolgende elementen) te verwisselen doen we het volgende:

$$x_{i_j} x_{i_{j+1}} = x_{i_{j+1}} x_{i_j} x_{i_j}^{-1} x_{i_{j+1}}^{-1} x_{i_j} x_{i_{j+1}} = x_{i_{j+1}} x_{i_j} [x_{i_j}, x_{i_{j+1}}].$$

Nadat de eerste s_1 of s_1^{-1} helemaal links staat, doen we hetzelfde voor de eerstvolgende s_1 of s_1^{-1} die we tegenkomen. Echter, op een gegeven moment zullen we onze s_1 of s_1^{-1} moeten verwisselen met een commutator. Om x_{i_j} met $[x_{i_k}, x_{i_l}]$ te verwisselen gaan we analoog te werk als voor x_{i_j} en $x_{i_{j+1}}$. We krijgen

$$[x_{i_k}, x_{i_l}]x_{i_j} = x_{i_j}x_{i_j}^{-1}x_{i_k}^{-1}x_{i_l}^{-1}x_{i_k}x_{i_l}x_{i_j} = x_{i_j}[x_{i_k}, x_{i_l}][[x_{i_k}, x_{i_l}], x_{i_j}].$$

We herhalen dit proces tot alle s_1 of s_1^{-1} links staan, hierbij verloopt het verwisselen met commutatoren met drie elementen of meer analoog als ervoor. Als we dit gedaan hebben, doen we hetzelfde voor s_2 of s_2^{-1} die we dan verschuiven naar links tot ze een s_1 of s_1^{-1} links naast zich hebben. We herhalen dit proces tot x van de vorm $s_1^{i_1} \cdots s_m^{i_m} a$ is, met a een product van commutatoren in G^2 (herinner $G = G^1 \supseteq G^2 \supseteq G^3 \supseteq \cdots \supseteq G^{k+1} = \{e\}$). In deze stap van het bewijs heeft G nilpotentieklasse k, dus is $G^{k+1} = [G^k, G] = \{e\}$. We kennen de groei van G^2 al via de inductiehypothese, namelijk $\gamma_{G^2}(n) \preceq n^d$ voor een $d \geq 1$. Nu is de vraag nog wat de lengte van a is, zodat we het aantal mogelijkheden hiervoor kunnen bepalen via de groeifunctie van G^2. Wel, a zal maximaal een lengte van $4n^2 + 6n^3 + \cdots + 2kn^k$ hebben aangezien er maximaal $n^2 + \cdots + n^k$ commutatoren van verschillende lengtes zijn en elke commutator van lengte i is een woord van lengte $2i$. Er zijn hoogstens n^2 commutatoren van lengte 2 ($[a, b]$), omdat we voor a en b elks juist n mogelijkheden hebben, namelijk $x_{i_1}, \cdots, x_{i_n}$. Analoog zijn er dan ook hoogstens n^i commutatoren van lengte i. Uit het vorige bewijs halen we dat er hoogstens n^m mogelijkheden zijn voor $i_1, \cdots, i_m$. Dus $\gamma_G(n) \leq n^m(4n^2+6n^3+\cdots+2kn^k) \preceq n^d$ voor een $d \geq 1$. We besluiten dat G een polynomiale groei heeft. □

Nu we weten dat er drie groei types zijn, definiëren we de groei graad. Deze zal een specifieker beeld geven van hoe snel een bepaalde groep groeit.

Definitie 3.12. *Zij G een groep die een polynomiale groei heeft. De limiet $\limsup_{n\to\infty} \frac{\ln(\gamma_G(n))}{\ln(n)}$ wordt genoteerd door $d(G)$ en wordt de graad van de groei van G genoemd. Zij Σ een voortbrengende verzameling van G. De limiet $\omega(G, \Sigma) = \limsup_{n\to\infty} \gamma_{G,\Sigma}^{1/n}$ wordt de exponentiële groei graad t.o.v. Σ genoemd en $S_G(\Sigma) = \log(\omega(G, \Sigma))$ heet de entropie van (G, Σ). We definiëren ook $S_G = \inf_\Sigma S_G(\Sigma)$ en $\omega(G) = \inf_\Sigma \omega(G, \Sigma)$.*

Opmerking 3.13. De graad van de groei van een groep met een polynomiale groei is onafhankelijk van de voortbrengende verzameling. Dit is eenvoudig in te zien doordat $d \neq d'$ impliceert dat $n^d \not\sim n^{d'}$. Dus als $\gamma_{G,S_1}(n) \sim n^d$ en $\gamma_{G,S_2}(n) \sim n^{d'}$, dan volgt mede uit Eigenschap 3.5 dat $d = d'$.

De exponentiële groei graad daarentegen is duidelijk afhankelijk van de voortbrengende verzameling. Dit komt omdat $a^n \sim b^n$, zelfs al is a niet gelijk aan b.

Uit de definitie volgt dat een groep G een exponentiële groei heeft als en slechts als $\omega(G, S) > 1$, want dan zal $\gamma_{G,S} \sim c^n$ met $c > 1$. Een groep G heeft een subexponentiële groei wanneer $\omega(G, S) = 1$, aangezien

$$0 = \ln(\omega(G, S)) = \ln(\limsup_{n\to\infty} \gamma_{G,\Sigma}^{1/n}(n)) = \limsup_{n\to\infty} \ln(\gamma_{G,\Sigma}^{1/n}(n)) = \lim_{n\to\infty} \frac{\ln(\gamma_{G,\Sigma}(n))}{n}.$$

We zeggen ook dat G een uniforme exponentiële groei heeft als $\omega(G) = \inf_\Sigma \omega(G, \Sigma) > 1$ [4, p. 1].

Voorbeeld 3.14. 1. Als $|G| = k$, dan is $d(G) = 0$ want er bestaat een $n_0 \in \mathbb{N}$ zodat voor alle $n \geq n_0$ geldt dat $\gamma_G(n) = |G| = k$;

2. Als G abels is en voortgebracht wordt door k elementen, dan is $d(G) = k$;

3. Bass en Guivarc'h formule zegt dat voor een nilpotente groep G van nilpotentieklasse k geldt dat $d(G) = \sum_{i=1}^{k} i \cdot \text{rank}(G_i/G_{i+1})$ met $G = G^1 \supseteq G^2 \supseteq G^3 \supseteq \cdots \supseteq G^{k+1} = \{1\}$ en $\text{rank}(G) = \min\{|X| : X \subseteq G, \langle X \rangle = G\}$ [1];

4. $\omega(F_m) = 2m - 1$ [4]. Dus heeft F_m voor $m \geq 2$ een uniforme exponentiële groei.

We zoeken nu een manier om exponentiële groei bij groepen aan te tonen. Dit zullen we doen met behulp van vrije semigroepen. Wij veronderstellen dat deze steeds het eenheidselement bevatten. Dus we werken eigenlijk met vrije monoiden als we over vrije semigroepen spreken.

Definitie 3.15. *Twee elementen x en y in een groep G brengen een vrije semigroep voort als geen elementen in de monoide voortgebracht door x en y gelijk zijn. Er zijn met andere woorden geen relaties met positieve machten tussen de elementen van een vrije semigroep. Notatie: $FM_2 = \langle x, y \rangle$.*

Voorbeeld 3.16. Onderstaand voorbeeld is een voorbeeld van een vrije semigroep die geen vrije groep is:

$$\left\langle \begin{pmatrix} 1/6 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/4 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle = \langle a, b \rangle.$$

Dit is geen vrije groep omdat

$$b^{-1}aba^{-2}bab^{-1}a^{-1}bab^{-2}aba^{-1}b^{-1}aba^{-1} = e.$$

Dat de groep een vrije semigroep is, zal triviaal blijken met behulp van Lemma 4.5.

Definitie 3.17. *Twee elementen $a, b \in G$ vormen een onafhankelijk paar als $\{a, b\}$ een vrije semigroep voortbrengt. We zeggen dat G positieve onafhankelijkheid heeft t.o.v. een voortbrengende verzameling Σ als de diameter van de positieve onafhankelijkheid $d_G^+(\Sigma) = \inf\{n \in \mathbb{N} \mid \Sigma^n$ bezit een onafhankelijk paar$\}$ eindig is. Als $d_G^+ = \sup_\Sigma d_G^+(\Sigma)$ eindig is, dan heeft G uniforme positieve onafhankelijkheid.*

Als $\{a, b\}$ een vrije deelsemigroep voortbrengt, dan zijn er 2^n woorden van lengte exact n in a en b, aangezien we voor elke y_i in $y_1 \cdots y_n$ juist 2 mogelijkheden hebben, namelijk a en b. De groeifunctie van deze vrije deelsemigroup is bijgevolg $\gamma_{FM_2,\{a,b\}}(n) = 2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$. Een vrije deelsemigroep heeft dus een exponentiële groei. De diameter en entropie hebben de volgende relatie:

$$S_G \geq \frac{\log(2)}{d_G^+}.$$

Dit kunnen we snel aantonen met behulp van voorgaande definities.

$$S_G(\Sigma) \geq \log(\limsup_{n\to\infty} \gamma_{G,\Sigma}^{1/n}(n)) = \log(\limsup_{n\to\infty} \gamma_{G,\Sigma}^{1/(nd_G^+(\Sigma))}(nd_G^+(\Sigma))) \geq \log(\limsup_{n\to\infty} \gamma_{FM_2,\{a,b\}}^{1/(nd_G^+(\Sigma))}(n))$$
$$\geq \log(\limsup_{n\to\infty} (2^n)^{1/(nd_G^+(\Sigma))}) \geq \log(2^{1/d_G^+(\Sigma)}) = \frac{\log(2)}{d_G^+(\Sigma)}$$

In zekere zin geldt dus dat hoe sneller een semigroep gevonden wordt, hoe sterker de exponentiële groei zal zijn en als $d_G^+ < \infty$ dan $S_G > 0$. We zullen dus vrije semigroepen (op een uniforme manier) vinden/maken om (uniforme) exponentiële groei aan te tonen.

4 Uniforme groei van oplosbare groepen

4.1 Constructie van vrije (semi)groepen

In Sectie 1 hebben we via het ping pong lemma (Lemma 1.9) een mogelijkheid getoond om vrije groepen te construeren. Dit lemma kan ook gebruikt worden om de stelling van Sanov te bewijzen. Deze stelling gaat als volgt en het bewijs is vrij analoog aan het voorbeeld na Lemma 1.9.

Stelling 4.1. *(Stelling van Sanov [15]) Zij u, v complexe getallen met $|u|, |v| \geq 2$, dan is*

$$\left\langle \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \right\rangle$$

een vrije groep.

Via de stelling van Sanov zien we dat de 'grootte' van de elementen belangrijk is om voortbrengers te vinden van een vrije groep. We definiëren nu velden met een bepaalde notie van 'grootte' analoog aan die van $\mathbb{R}$ en $\mathbb{C}$. Dit zullen de lokaal compacte velden zijn.

Definitie 4.2. *Zij F een veld. Een afbeelding $|\cdot| : F \to \mathbb{R}$ heet een (reële) absolute waarde op F als voor alle $a, b \in F$:*

1. $|a| = 0 \Leftrightarrow a = 0$,
2. $|ab| = |a||b|$,
3. $|a + b| \leq |a| + |b|$.

We noemen een absolute waarde niet-Archimedisch als ze voldoet aan de sterkere eigenschap $|a + b| \leq \max\{a, b\}$. Anders noemen we ze Archimedisch.

Opmerking 4.3. De absolute waarde op een veld die een priem karakteristiek heeft, is steeds niet-Archimedisch. We herinneren dat de karakteristiek van een veld het kleinste natuurlijke getal $c > 0$ is met $\sum_{i=1}^{c} 1 = c1 = 0$. Dus als F een veld is met karakteristiek p en p is priem, dan heeft F een deelveld P dat isomorf is met $\mathbb{F}_p$ het veld met p elementen en we noemen dit deelveld het priemveld van F. Dit priemveld is eindig, dus elk niet nul element x van P is een eenheidswortel, zodat $|x| = 1$.

Merk op dat een absolute waarde een metriek induceert op F, namelijk $d(a, b) = |b - a|$. Een veld heet *lokaal compact* voor een bepaalde absolute waarde als de topologische ruimte geinduceerd door deze absolute waarde lokaal compact is, dus als elk element een compacte omgeving heeft [3, p. 72]. Voorbeelden van lokaal compacte topologische ruimten zijn $\mathbb{R}$ en iedere discrete ruimte. We kunnen bijgevolg op elk veld triviaal een lokaal compacte topologie zetten, namelijk de discrete topologie. In het vervolg zullen we dus steeds spreken over niet-discreet geïnduceerde topologieën. Volgende stelling geeft de classificatie van lokaal compacte velden. Voor een bewijs refereren we naar [17, p. 8-12].

Stelling 4.4. *In karakteristiek 0 zijn alle Archimedisch lokaal compacte velden, als topologische ruimten, isomorf met*

1. $\mathbb{R}$ *of* $\mathbb{C}$ *met de absolute waarde.*

De niet-Archimedische lokaal compacte velden van karakteristiek 0 zijn, als topologische ruimten, homeomorf met

2. *een eindige veld uitbreiding van $\mathbb{Q}_p$, de p-adische getallen met p priem en de p-adische waarde $|\cdot|_p : |\alpha|_p = p^{-k}$, waar $\alpha \in \mathbb{Q}$ en $\alpha = \alpha^* p^k$ zodat p α^* niet deelt.*

Alle lokaal compacte velden van karakteristiek p (p priem) zijn niet-Archimedisch en homeomorf met

3. *eindige veld uitbreidingen van het veld van Laurent polynomialen over een eindig veld $\mathbb{F}_{p^n}$, genoteerd als $\mathbb{F}_{p^n}((X))$. Zij $f(X) \in \mathbb{F}_{p^n}((X))$ een irreducibel polynoom. Voor elke $\frac{g(X)}{h(X)} \in \mathbb{F}_{p^n}((X))$, schrijf $\frac{g(X)}{h(X)} = f(X)^m \frac{a(X)}{b(X)}$ waarbij $f(X)$ zowel $a(X)$ als $b(X)$ niet deelt. Definieer de $f(X)$-adische absolute waarde op $\mathbb{F}_{p^n}((X))$ door $\left|\frac{g(X)}{h(X)}\right|_{f(X)} = ((p^n)^{deg(f)})^{-m}$.*

Een lokaal compact veld met een niet-discrete topologie noemen we een *lokaal veld*.

Neem nu k een veld en beschouw het als affiene ruimte over zichzelf. De automorfismen van de rechte k, $Aut(k)$, zijn eendimensionale affiene transformaties $x \mapsto ax + b$ waarbij we a de dilatatiefactor en b de translatiefactor noemen. Deze affiene transformaties zijn ofwel translaties, waarbij $a = 1$, ofwel zijn het homothetieën, waarbij $a \neq 1$. Deze homothetieën hebben als fixpunt het punt $\frac{b}{1-a}$. Inderdaad, want $\frac{b}{1-a} \mapsto a\frac{b}{1-a} + b = \frac{b}{1-a}$ en andere punten x worden gestuurd op $\frac{b}{1-a} + a\left(x - \frac{b}{1-a}\right)$. We kunnen hier ook matrices bij beschouwen aangezien

$$Aut(k) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in k^\times = k\backslash\{0\}, b \in k \right\} = \mathbb{A}(k).$$

We zien nu bovendien dat $\mathbb{A}(k)$ abels-bij-abels is vermits

$$T = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in k \right\} \trianglelefteq \mathbb{A}(k)$$

abels is (stelt de translaties voor) en

$$Q = \mathbb{A}(k)/T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in k^\times \right\}$$

is ook abels. We associëren met $\mathbb{A}(k)$ de afbeelding

$$\pi : \mathbb{A}(k) \to k^\times : \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$$

die iedere transformatie afbeeldt op zijn dilatatiefactor. We zullen zien dat we vrije semigroepen kunnen maken uit homothetieën, vandaar deze korte herhaling. Dit zal niet zo zijn met translaties, want als $a = 1$ dan zijn de matrices van de vorm $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ commutatief, wat een relatie tussen elementen geeft (dus niet vrij).

Om een vrije groep te construeren maken we meestal gebruik van het ping-pong lemma, wat in meerdere vormen kan voorkomen. Elke vorm heeft zo zijn eigen voordelen. In [2, Lemma 2.1, p. 5] gebruikt Breuillard een vorm die vrije semigroepen construeert aan de hand van homothetieën.

Lemma 4.5. *Zij k een Archimedisch (respectievelijk niet-Archimedisch) lokaal veld. Zij x en y twee homothetieën in $\mathbb{A}(k)$ met respectievelijk, verschillende, fixpunten p en q uit k en dilatatiefactor α en β. Stel dat $|\alpha| \leq \frac{1}{3}$ en $|\beta| \leq \frac{1}{3}$ (respectievelijk < 1). Dan brengen x en y een vrije semigroep voort, dus $\langle x, y\rangle \cong FM_2$.*

Bewijs. Stel $d = |p - q|$. Zij $B(p) = \{z \in k \mid |p - z| < \frac{d}{2}\}$ en $B(q) = \{z \in k \mid |q - z| < \frac{d}{2}\}$ de open bollen met straal $d/2$ (respectievelijk d in het niet-Archimedische geval) en middelpunten p en q. Deze bollen zijn per definitie disjunct. Uit de veronderstelling $|\alpha| \leq \frac{1}{3}$ en $|\beta| \leq \frac{1}{3}$ (respectievelijk < 1) volgt dat x ieder punt in de bol $B(q)$ en $B(p)$ afbeeldt in de bol $B(p)$. Om dit aan te tonen nemen we eerst $z \in B(q)$, dus $|q-z| < d/2$. Dan is $|p-z| \leq |p-q|+|q-z| < d + d/2 = 3d/2$. De homothetie x met fixpunt p en dilatatiefactor $\alpha \leq 1/3$ beeldt z af op $\alpha z+p(1-\alpha)$. Er volgt $|p-x(z)| = |p-\alpha z-p(1-\alpha)| = |p-\alpha z-p+\alpha p| = |\alpha||p-z| < \frac{1}{3}\frac{3d}{2} = \frac{d}{2}$ en x beeldt dus ieder punt in $B(q)$ af in de bol $B(p)$. Neem nu $z \in B(p)$, dus $|p - z| < d/2$. Dan volgt $|p - x(z)| = |\alpha||p - z| < \frac{1}{3}\frac{d}{2} = \frac{d}{6}$ en x beeldt dus ook ieder punt in $B(p)$ af in de bol $B(p)$. Analoog beeldt y ieder punt in de bol $B(p)$ en $B(q)$ af in de bol $B(q)$.

De definitie van een vrije semigroep zegt dat x en y een vrije semigroep voortbrengen als er geen relaties zijn tussen woorden in de monoide voortgebracht door x en y. Veronderstel nu dat $w_1 = x^{n_1}y^{m_1}\cdots x^{n_r}y^{m_r}$ en $w_2 = x^{n'_1}y^{m'_1}\cdots x^{n'_l}y^{m'_l}$ gelijk zijn als niet-triviale elementen uit de monoide voortgebracht door x en y, met $n_i, m_i, n'_j, m'_j, r, l \in \mathbb{N}$. We mogen veronderstellen dat $n_1 = 0$ en $n'_1 > 0$ door beide elementen links te vermenigvuldigen met een negatieve macht van x. Als $n_1 = n'_1$ dan kunnen we beide elementen vermenigvuldigen met een negatieve macht van x zodat $w'_1 = y^{m_1}\cdots x^{n_r}y^{m_r}$ en $w'_2 = y^{m'_1}\cdots x^{n'_l}y^{m'_l}$ en we herhalen het proces. Neem nu $q \in B(q)$, dan is

$$\begin{aligned} w_1(q) &= y^{m_1}\cdots x^{n_r}y^{m_r}(q) = y^{m_1}\cdots x^{n_r}(q_{r_1}) = y^{m_1}\cdots x^{n_{r-1}}y^{m_{r-1}}(q_{r_2}) \\ &= y^{m_1}\cdots x^{n_{r-1}}(q_{(r-1)_1}) = \cdots = y^{m_1}(q_{2_2}) \in B(q) \end{aligned}$$

met $q_{i_1} \in B(q)$ en $q_{i_2} \in B(p)$ voor $i = 2, \cdots, r$. Analoog is $w_2(q) \in B(p)$. Aangezien $w_1 = w_2$ is $w_1(q) = w_2(q) \in B(p) \cap B(q)$. Dit is een tegenspraak, omdat $B(p)$ en $B(q)$ disjuncte bollen zijn. □

Hernemen we Voorbeeld 3.16, dan zien we inderdaad dat dit voorbeeld een vrije semigroep is. We hebben namelijk twee homothetieën a en b met respectievelijk verschillende fixpunten 0 en 8/3 en dilatatiefactoren 1/6 en 1/4.

Lemma 4.5 kan gebruikt worden om [2, Lemma 6.1, p. 13] aan te tonen, maar we leveren een eigen direct bewijs.

Lemma 4.6. *Zij G een groep voortgebracht door twee elementen x en y zodat de normale deelgroep $M = \langle x^n y x^{-n} \mid n \in \mathbb{Z}\rangle$ niet eindig voortgebracht is. Dan brengen de elementen x en yxy^{-1} een vrije semigroep voort.*

Bewijs. Veronderstel dat $\{x, yxy^{-1}\} = \{x, x^y\}$ geen vrije semigroep voortbrengt. Er bestaat dus een relatie

$$x^{r_1}(yxy^{-1})^{s_1}\cdots x^{r_j}(yxy^{-1})^{s_j} = (yxy^{-1})^{m_1}x^{n_1}\cdots(yxy^{-1})^{m_k}x^{n_k} \tag{1}$$

in G, met $r_i, s_i, m_i, n_i \in \mathbb{N}, r_1, m_1 > 0$. We kunnen deze relatie herschrijven:

$$
\begin{aligned}
(1) &\Leftrightarrow x^{r_1}yx^{s_1}y^{-1}x^{r_2}yx^{s_2}y^{-1}\cdots x^{r_j}yx^{s_j}y^{-1} = yx^{m_1}y^{-1}x^{n_1}\cdots yx^{m_k}y^{-1}x^{n_k} \\
&\Leftrightarrow (x^{r_1}yx^{-r_1})(x^{s_1+r_1}y^{-1}x^{-(s_1+r_1)})\cdots(x^{r_j+\sum_{i=1}^{j-1}s_i+r_i}yx^{-(r_j+\sum_{i=1}^{j-1}s_i+r_i)}) \\
&\quad\cdot(x^{\sum_{i=1}^{j}s_i+r_i}y^{-1}x^{-(\sum_{i=1}^{j}s_i+r_i)})x^{\sum_{i=1}^{j}s_i+r_i} \\
&\quad= y(x^{m_1}y^{-1}x^{-m_1})(x^{n_1+m_1}yx^{-(n_1+m_1)})\cdots(x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}y^{-1}x^{-(m_k+\sum_{i=1}^{k-1}n_i+m_i)}) \\
&\quad\cdot x^{\sum_{i=1}^{k}n_i+m_i} \\
&\Leftrightarrow y^{x^{r_1}}(y^{-1})^{x^{s_1+r_1}}\cdots y^{x^{r_j+\sum_{i=1}^{j-1}s_i+r_i}}(y^{-1})^{x^{\sum_{i=1}^{j}s_i+r_i}}x^{\sum_{i=1}^{j}s_i+r_i} \\
&\quad= y^{x^0}(y^{-1})^{x^{m_1}}y^{x^{n_1+m_1}}\cdots(y^{-1})^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}}x^{\sum_{i=1}^{k}n_i+m_i} \\
&\Leftrightarrow x^{\sum_{i=1}^{j}s_i+r_i-(\sum_{l=1}^{k}n_l+m_l)} \\
&\quad= ((y^{-1})^{x^{\sum_{i=1}^{j}s_i+r_i}})^{-1}\cdots((y^{-1})^{x^{s_1+r_1}})^{-1}(y^{x^{r_1}})^{-1}y^{x^0}(y^{-1})^{x^{m_1}}y^{x^{n_1+m_1}} \\
&\qquad\cdots(y^{-1})^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}} \\
&\Leftrightarrow x^{\sum_{i=1}^{j}s_i+r_i-(\sum_{l=1}^{k}n_l+m_l)} \\
&\quad= y^{x^{\sum_{i=1}^{j}s_i+r_i}}\cdots y^{x^{s_1+r_1}}(y^{-1})^{x^{r_1}}y^{x^0}(y^{-1})^{x^{m_1}}y^{x^{n_1+m_1}}\cdots(y^{-1})^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}}
\end{aligned}
$$

Als $\sum_{i=1}^{j}s_i + r_i \neq \sum_{l=1}^{k}n_l + m_l$ en stel $z = max\{\sum_{i=1}^{j}s_i + r_i, \sum_{l=1}^{k}n_l + m_l\}$ dan is $x^{\sum_{i=1}^{j}s_i+r_i-(\sum_{l=1}^{k}n_l+m_l)} \in \langle y, y^x, \cdots, y^{x^z}, y^{-1}, (y^{-1})^x, \cdots, (y^{-1})^{x^z}\rangle$. Neem nu een $n \in \mathbb{N}$, dan is $x^nyx^{-n} \in \langle y, y^x, \cdots, y^{x^z}, y^{-1}, (y^{-1})^x, \cdots, (y^{-1})^{x^z}\rangle$. In dit geval is M dus eindig voortgebracht.

Veronderstel nu dat $\sum_{i=1}^{j}s_i + r_i = \sum_{l=1}^{k}n_l + m_l$. Dan is

$$
\begin{aligned}
e &= y^{x^{\sum_{i=1}^{j}s_i+r_i}}\cdots y^{x^{s_1+r_1}}(y^{-1})^{x^{r_1}}y^{x^0}(y^{-1})^{x^{m_1}}y^{x^{n_1+m_1}}\cdots(y^{-1})^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}} \\
\Leftrightarrow y &= y^{x^{r_1}}(y^{-1})^{x^{s_1+r_1}}\cdots(y^{-1})^{x^{\sum_{i=1}^{j}s_i+r_i}}y^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}}\cdots(y^{-1})^{x^{n_1+m_1}}y^{x^{m_1}}.
\end{aligned}
$$

Dus $y \in \langle y^x, \cdots, y^{x^z}, y^{-1}, (y^{-1})^x, \cdots, (y^{-1})^{x^z}\rangle$. Neem dan $x^nyx^{-n} \in M$, dan geldt

$$
\begin{aligned}
x^nyx^{-n} &= x^ny^{x^{r_1}}(y^{-1})^{x^{s_1+r_1}}\cdots(y^{-1})^{x^{\sum_{i=1}^{j}s_i+r_i}}y^{x^{m_k+\sum_{i=1}^{k-1}n_i+m_i}}\cdots(y^{-1})^{x^{n_1+m_1}}y^{x^{m_1}}x^{-n} \\
&= y^{x^{r_1+n}}(y^{-1})^{x^{s_1+r_1+n}}\cdots(y^{-1})^{x^{n+\sum_{i=1}^{j}s_i+r_i}}y^{x^{m_k+n+\sum_{i=1}^{k-1}n_i+m_i}} \\
&\quad\cdots(y^{-1})^{x^{n_1+m_1+n}}y^{x^{m_1+n}}x^nx^{-n}
\end{aligned}
$$

Hieruit volgt dat

$$\langle y, y^x, \cdots, y^{x^z}, y^{-1}, (y^{-1})^x, \cdots, (y^{-1})^{x^z}\rangle = M.$$

In beide gevallen is M eindig voortgebracht, wat in tegenspraak is met onze veronderstelling. □

4.2 Hoofdresultaat

We werken nu richting het hoofddoel, namelijk de volgende stelling uit een artikel van E. Breuillard [2].

Stelling 4.7. *Zij Γ een eindig voortgebrachte oplosbare groep. Dan is precies een van de volgende eigenschappen geldig.*

1. *Γ is virtueel nilpotent, dus het bevat een nilpotente deelgroep van eindige index, $d_\Gamma^+ = \infty$ en $S_\Gamma = 0$.*

2. *Γ heeft een deelgroep Γ_0 van eindige index zodat $d_{\Gamma_1}^+ \leq 3$ voor elke deelgroep $\Gamma_1 \leq \Gamma_0$ van eindige index.*

Wegens de Stelling van Gromov [6] weten we dat een eindig voortgebrachte groep G een polynomiale groei heeft als en slechts als G een nilpotente deelgroep H bevat van eindige index. Dit toont alvast het eerste deel van Stelling 4.7 aan.

Dankzij het volgende resultaat van J. Groves [7], is het voldoende om het tweede deel van Stelling 4.7 te bewijzen voor meta-abelse groepen en zelfs voor deelgroepen van de affiene transformaties van de affiene rechte k. De stelling wordt gegeven zonder bewijs.

Stelling 4.8. *Zij Γ een eindig voortgebrachte oplosbare groep die niet virtueel nilpotent is en waarvan alle quotiënten virtueel nilpotent zijn. Dan geldt:*

1. *Γ is virtueel meta-abels.*

2. *Als Γ meta-abels is, dan bestaat er een inbedding van Γ in de groep $\mathbb{A}(K)$ van de affiene transformaties van de affiene rechte K, voor een veld K.*

Het tweede deel van deze stelling wordt bewezen via de volgende eigenschap die we ook niet zullen bewijzen [2, p. 10].

Eigenschap 4.9. *Zij H een eindig voortgebrachte meta-abelse groep. Dan bestaat er een veld K en een homomorfisme $\rho : H \to \mathbb{A}(K)$ met de volgende eigenschap. Als H niet virtueel nilpotent (resp. niet polycyclisch) is, dan is $\rho(H)$ eveneens niet virtueel nilpotent (respectievelijk niet polycyclisch).*

Voor het bewijs van Stelling 4.7 zijn we dus op zoek naar twee homothetieën met dilatatiefactor kleiner of gelijk aan $\frac{1}{3}$ en van hoogstens lengte 3 in een willekeurige voortbrengende verzameling S van Γ_1. Deze zullen we nodig hebben om het ping pong lemma Lemma 4.5 te kunnen gebruiken. Om dit lemma toe te passen in de stelling van Breuillards artikel, zullen we eerst een gepaste inbedding moeten vinden van een eindig voortgebracht veld in een lokaal veld, zodat we de norm van de dilatatiefactor kunnen bepalen. Hiervoor gebruiken we een lemma van J. Tits [16]. Een belangrijke voorwaarde in dit lemma is dat K eindig voortgebracht is. Merk op dat we voor het bewijs van Stelling 4.7 in $\mathbb{A}(K)$ zullen werken. Zij $\Gamma \leq \mathbb{A}(K)$ die eindig voortgebracht is. Dan kunnen we ook veronderstellen dat K eindig voortgebracht is, namelijk door de coëfficiënten van de voortbrengers van Γ.

Lemma 4.10. *Zij K een eindig voortgebracht veld en $\alpha \in K$. Als α^{-1} geen algebraisch geheel getal is (het is dus geen wortel van een monische veelterm met coëfficiënten in $\mathbb{Z}$ van karakteristiek 0 en met coëfficiënten in $\mathbb{F}_p$ voor karakterisitiek p), dan bestaat er een inbedding $\sigma : K \hookrightarrow k$ met k een niet-Archimedisch lokaal veld met absolute waarde $|\cdot|_k$ zodat $|\sigma(\alpha)|_k < 1$. Verder bestaat er een constante $\varepsilon = \varepsilon(K) > 0$ (afhankelijk van K) zodat als α en α^{-1} algebraisch gehele getallen zijn (α wordt dan ook een algebraische eenheid genoemd) en $|log|\sigma(\alpha)|_k| < \varepsilon$ voor elke inbedding $\sigma : K \hookrightarrow k$ met k een Archimedisch lokaal veld, dan is α een eenheidswortel ($\alpha^n = 1$ voor een $n \in \mathbb{N}_0$).*

Bewijs. Stel $\beta = \alpha^{-1}$ en zij K_0 het priemveld van K. Voor K van karakteristiek 0 is dit $\mathbb{Q}$ en voor karakteristiek p is dit $\mathbb{F}_p$.

Veronderstel dat β transcendent is over K_0. Er bestaat dus geen polynoom f met coëfficiënten in K_0 zodat $f(\beta) = 0$. Transcendente elementen zijn dicht in elk lokaal compact veld. Neem bijvoorbeeld π die transcendent is in $\mathbb{R}$ over $\mathbb{Q}$. We weten uit [8, p. 55] dat $\{a \in K \mid a \text{ is algebraisch over } K_0\}$ een deellichaam is van K dat K_0 bevat. Veronderstel nu dat $\pi + q$ met $q \in \mathbb{Q}$ algebraisch is in $\mathbb{R}$ over $\mathbb{Q}$, dan zou ook $\pi + q - q$ dat moeten zijn, wat natuurlijk niet kan. Dus voor elke $q \in \mathbb{Q}$ is $\pi + q$ transcendent. Aangezien translaties homeomorfismen zijn en deze topologische eigenschappen zoals dichtheid bewaard, hebben we getoond dat de transcendente elementen van $\mathbb{R}$ over $\mathbb{Q}$ dicht zijn in $\mathbb{R}$. Voor de andere lokale velden zal het bewijs analoog verlopen.

Uit [3] weten we dat een dicht deel van k elk open deel van k snijdt. Dus als we k een niet-Archimedisch lokaal compact veld nemen, dan is $\{\text{transcendente elementen van } k \text{ over } K_0\} \cap k \backslash \overline{B(0,1)} \neq \emptyset$ en neem γ_1 in deze doorsnede. Er geldt dat $|\gamma_1|_k > 1$. Zij nu $\beta_1 = \beta$, dan kunnen we een inbedding $\sigma_1 : K_0(\beta_1) \hookrightarrow k$ vinden die elke $q \in K_0$ afbeeldt op q, $\sigma_1(\beta_1) = \gamma_1$ en de rest volgt via lineaire uitbreiding. We willen nu deze inbedding uitbreiden tot K. Gegeven is dat K eindig voortgebracht is over K_0, dus er bestaan een eindig aantal $\beta_1, \cdots, \beta_l$ zodat $K = K_0(\beta_1, \cdots, \beta_l)$. Nu is $K_0(\beta_1, \beta_2) = K_0(\beta_1)(\beta_2)$, dus definieer σ_2 zodat $\sigma_2(K_0(\beta_1)) = \sigma_1$ en $\sigma_2(\beta_2) = \gamma_2$ met $\gamma_2 \in \{\text{transcendente elementen van } k \text{ over } K_0\} \cap k \backslash \overline{B(0,1)}$ en $\gamma_1 \neq \gamma_2$. Dus uiteindelijk hebben we een inbedding $\sigma : K \hookrightarrow k$.

Als nu $K_0(\beta)$ een algebraische uitbreiding is, dus β is algebraisch (en dus niet transcendent) over K_0, en $|\beta| \leq 1$ voor elke niet-Archimedische absolute waarde $|\cdot|$ op $K_0(\beta)$, dan moet β een algebraisch geheel getal zijn [17] wat in tegenspraak is met het gegeven. Dus er bestaat een niet-Archimedische absolute waarde $|\cdot|_k$ zodat $|\beta|_k > 1$ en daaruit volgt dat $|\sigma(\beta)|_k = |\gamma|_k > 1$ en $|\sigma(\alpha)|_k < 1$.

Voor het tweede deel van het lemma verwijzen we naar [2, p. 5]. □

We bewijzen nu Stelling 4.7 voor eindig voortgebrachte deelgroepen van de affiene rechte $\mathbb{A}(K)$.

Bewijs **(van Stelling 4.7 voor deelgroepen van de affiene rechte)**. Zij $\Gamma \leq \mathbb{A}(K)$ die eindig voortgebracht is. We zijn geïnteresseerd in het maken van vrije semigroepen. Nilpotente groepen kunnen geen vrije semigroepen bevatten wegens Eigenschap 3.6 aangezien ze een polynomiale groei hebben (Eigenschap 3.11) en vrije semigroepen hebben een exponentiële groei. Dus we kunnen ook veronderstellen dat Γ niet nilpotent is of zelfs niet nilpotent-bij-eindig vermits de groeifunctie niet verandert als je naar een deelgroep gaat van eindige index. We bekijken nu verschillende gevallen. We nemen dezelfde notatie als voorheen. Neem $M = \Gamma \cap T$ met T de deelgroep van $\mathbb{A}(K)$ die de translaties voorstelt en $Q = \Gamma/M \cong K^\times$. De afbeelding π is de kanonische projectie van $\mathbb{A}(K)$ naar $K^\times$ zodat we $\mathbb{Q}$ kunnen beschouwen als multiplicatieve deelgroep van $K^\times$.

Het eerste geval is als $\pi(Q) \subseteq \{\text{eenheidswortels van } K\}$. Dan zou ieder element van $\pi(Q)$ (en dus ook van Q aangezien $\pi(Q) \cong Q$) eindige orde hebben en Q is reeds eindig voortgebracht en abels. Dus volgt dat Q eindig is. Aangezien $Q = \Gamma/M$, Q eindig is en M abels is, zou Γ abels-bij-eindig moeten zijn. Uit sectie 2 weten we dat abelse groepen ook nilpotent zijn. Bijgevolg zou Γ nilpotent-bij-eindig moeten zijn, wat in tegenspraak is met onze veronderstelling. Dus $\pi(Q) \not\subseteq \{\text{eenheidswortels van } K\}$.

Voor het tweede geval veronderstellen we dat $\pi(Q) \not\subseteq \{\text{algebraische eenheden van } K\}$. Het doel zal zijn om te tonen dat als $S = \{x_1, \cdots, x_n\}$ een voortbrengende verzameling is van Γ, dat er dan een verzameling $\{a, b\} \in S^3$ bestaat zodat $\langle a, b\rangle \cong FM_2$. Aangezien $\pi(Q) \not\subseteq \{\text{algebraische eenheden van } K\}$ weten we dat er een voortbrenger $x_i \in S$ van Γ bestaat zodat voor de quotiëntafbeelding $\pi : \Gamma \to K^\times$ geldt dat $\pi(x_i) \notin \{\text{algebraische eenheden van } K\}$. Dit wil per definitie zeggen dat $\pi(x_i)$ of $\pi(x_i)^{-1}$ geen algebraisch geheel getal is. Veronderstel eerst dat $\pi(x_i)^{-1}$ geen algebraisch geheel getal is. Uit Lemma 4.10 volgt dat er dan een inbedding $\sigma : K \hookrightarrow \mathbb{Q}_p$ bestaat zodat $|\sigma(\pi(x_i))|_p < 1$. Herinner dat $\pi(x_i) = a$ voor een $a \in K^\times$. Aangezien $|\sigma(a)|_p < 1$ zal $\sigma(x_i)$ een homothetie zijn met dilatatiefactor $\sigma(a)$. We hebben onze homothetieën in $\mathbb{A}(K)$ beschouwd als homothetieën in $\mathbb{A}(\mathbb{Q}_p)$, omdat we in $\mathbb{Q}_p$ de p-adische waarde kunnen bepalen en dus kunnen we nagaan of de homothetie voldoet aan de voorwaarden van het ping-pong lemma, Lemma 4.5. We hebben dus een eerste homothetie x_i gevonden met $|\sigma(a)|_p < 1$ die we kunnen gebruiken voor het ping-pong lemma. Veronderstel dat deze homothetie het punt $q \in K$ fixeert, dus q is het fixpunt van de afbeelding $x \mapsto ax + b$ horende bij x_i. Stel nu dat voor elke $j \in \{1, \cdots, i-1, i+1, \cdots, n\}$ geldt dat q ook een fixpunt is van x_j, dan zou heel de groep Γ het punt q fixeren en dus is $\Gamma = \Gamma_q \subseteq \mathbb{A}(K)_q$, met $\mathbb{A}(K)_q$ de stabilisator van q in $\mathbb{A}(K)$ en Γ_q de stabilisator van q in Γ. De stabilisator $\mathbb{A}(K)_q$ van q is echter abels, maar Γ kan niet abels zijn omdat we verondersteld hebben dat Γ niet nilpotent is. Dus er bestaat $j \neq i : x_j q \neq q$. Er volgt dat $x_j x_i x_j^{-1}$ ook een homothetie is met dilatatiefactor $a_j a a_j^{-1} = a$ (K is een veld en is dus commutatief), waarbij a_j de dilatatiefactor is van x_j. De twee gevonden homothetieën met eenzelfde dilatatiefactor zijn toch verschillend vermits hun fixpunten verschillen. Dus $\{x_i, x_j x_i x_j^{-1}\}$ voldoet aan Lemma 4.5 en vormt een vrije semigroep.

Beschouw voor het laatste geval $\pi(Q) \subseteq \{\text{algebraische eenheden van } K\}$. We nemen nu de contrapositie van het tweede deel van Lemma 4.10. Dus er bestaat een $\varepsilon = \varepsilon(K) = \varepsilon(\Gamma)$ zodat als $\alpha \in K \backslash \{\text{eenheidswortels van } K\}$, dan bestaat er een inbedding $\sigma : K \hookrightarrow k$ met k een Archimedisch veld ($\mathbb{R}$ of $\mathbb{C}$) zodat $|\log|\sigma(\alpha)|_k| > \varepsilon$. Neem nu $n_0 = n_0(\Gamma) \in \mathbb{N}$ zodat $\varepsilon > \log(3)/n_0$. Zij $Q^{n_0} = \{q^{n_0} \mid q \in Q\}$ een deelgroep van Q. Aangezien Q eindig voortgebracht is, kunnen we Q schrijven als $\langle s_1, \cdots, s_l\rangle$. Vermits Q ook abels is, kunnen we Q ook schrijven als $Q = \cup s_1^{i_1} \cdots s_l^{i_l} Q^{n_0}$ met $0 \leq i_1, \cdots, i_l \leq n_0$. Dit is een eindige unie die we kunnen beperken tot een disjuncte unie, waaruit volgt dat Q^{n_0} een deelgroep is van Q van eindige index. Definieer nu $\Gamma_0 = \pi^{-1}(\pi(Q^{n_0}))$. Aangezien $\pi(Q) = \pi(\Gamma)$ en $\mathbb{Q}^{n_0}$ een deelgroep van Q van eindige index is, zal door gewoon de inverse beelden te nemen van de representanten $s_1^{i_1} \cdots s_l^{i_l}$ ook $\Gamma_0 = \pi^{-1}(\pi(Q^{n_0}))$ een deelgroep zijn van $\Gamma = \pi^{-1}(\pi(Q))$ van eindige index. We willen tonen dat $d^+_{\Gamma_1} \leq 3$ voor elke deelgroep Γ_1 van Γ_0 van eindige index. Veronderstel dat Γ_1 eindig voortgebracht is door $\{z_1, \cdots, z_n\}$. Geval 1 zei ons dat $\pi(Q) \not\subseteq \{\text{eenheidswortels van } K\}$, dus bestaat er een $i \in \{1, \cdots, n\}$ zodat $\pi(z_i) \notin \{\text{eenheidswortels van } K\}$. Per definitie van Γ_0 is $z_i = z_0^{n_0} a$ met $z_0 \in Q$ en $a \in M$. Maar dan is $\pi(z_i) = \pi(z_0^{n_0} a) = \pi(z_0^{n_0})\pi(a) = \pi(z_0)^{n_0}$ en dus is $\pi(z_0)$ ook geen eenheidswortel van K. Wegens de contrapositie van het tweede deel van Lemma 4.10 bestaat er een inbedding $\sigma : K \hookrightarrow k$ met $k = \mathbb{R}$ of $k = \mathbb{C}$ zodat $|\log|\sigma(\pi(z_0))|_k| > \varepsilon > \log(3)/n_0$. Door eventueel z_i te vervangen door z_i^{-1} kunnen we besluiten dat $|\sigma(\pi(z_i))|_k = |\sigma(\pi(z_0)^{n_0})|_k < \frac{1}{3}$. We hebben een eerste homothetie gevonden voor Lemma 4.5. De homothetie z_i fixeert een punt $p \in k$. Analoog zoals in geval 2 bestaat er een $j \in \{1, \cdots, i-1, i+1, \cdots, n\}$, zodat $z_j p \neq p$ en $\{z_i, z_j z_i z_j^{-1}\}$ is weer een verzameling van twee homothetieën die voldoet aan Lemma 4.10. □

Opmerking 4.11. Wegens Lemma 3.1 in [2] komen gevallen 2 en 3 van het bewijs overeen

met respectievelijk het niet polycyclisch en wel polycyclisch zijn van Γ.

Voor het algemene geval van Stelling 4.7, dus voor een eindig voortgebrachte oplosbare groep Γ met voortbrengende verzameling S, is het voldoende om hetzelfde te tonen voor een quotiënt van Γ die ook voldoet aan de voorwaarden van Stelling 4.7, aangezien we in Eigenschap 3.6 hebben aangetoond dat de groei van een quotiënt van Γ steeds kleiner is dan de groei van Γ zelf. Dus veronderstel dat Γ niet virtueel nilpotent is, dan wordt in [2, p. 12] bewezen dat er een niet virtueel nilpotent quotiënt Γ/N van Γ bestaat, zodat al zijn eigen quotiënten wel virtueel nilpotent zijn (Γ/N wordt dan een *JNVN groep* genoemd). Via Stelling 4.8 is dit quotiënt dan virtueel meta-abels. Er bestaat dus een deelgroep H van het quotiënt van eindige index dat meta-abels is. Eigenschap 4.9 geeft dan een deelgroep $\rho(H)$ van $\mathbb{A}(k)$. Het bewijs dat we hierboven gaven geeft dan dat $d^+_{\rho(H)} \leq 3$ als $\rho(H)$ niet polycyclisch is wat equivalent is met $\pi(\rho(H)) \nsubseteq \{\text{algebraische eenheden van } K\}$. Als $\rho(H)$ wel polycyclisch is, wat equivalent is met $\pi(\rho(H)) \subseteq \{\text{algebraische eenheden van } K\}$, dan bestaat er dus een deelgroep T van $\rho(H)$ van eindige index en $d^+_T \leq 3$. Nu willen we enkel nog weten wat d_Γ is. Stel dat $\overline{a}, \overline{b} \in \overline{S}^{d^+_{\Gamma/N}}$ met $\overline{S}$ de voortbrengende verzameling van Γ/N zodat $\langle \overline{a}, \overline{b} \rangle \cong FM_2$. Dan volgt dat voor $a, b \in S^{d^+_{\Gamma/N}}$, met $aN = \overline{a}$ en $bN = \overline{b}$, geldt dat $\langle a, b \rangle \cong FM_2$. Stel van niet, dan zal de relatie $r = s$ die $\langle a, b \rangle$ geen vrije groep maakt ook een relatie zijn voor $\langle \overline{a}, \overline{b} \rangle$ in Γ/N, dus $rN = sN$, wat niet kan. Hiermee hebben we getoond dat $d^+_\Gamma \leq d^+_{\Gamma/N}$. De deelgroep H van Γ/N heeft eindige index $l < \infty$, dus $\overline{g} \in \Gamma/N$, dan zal $\overline{g}^l \in H$. Hieruit volgt dat $d^+_{\Gamma/N} \leq d^+_H \cdot [\Gamma/N : H]$. Als nu a, b een vrije semigroep voortbrengen in $\rho(H)$, dan moeten $\rho^{-1}(a)$ en $\rho^{-1}(b)$ ook een vrije semigroep voortbrengen in H met dezelfde redenering als voorheen. Dus is $d^+_H \leq d^+_{\rho(H)}$. We besluiten dat

$$d^+_\Gamma \leq d^+_{\Gamma/N} \leq d^+_H \cdot [\Gamma/N : H] \leq d^+_{\rho(H)} \cdot [\Gamma/N : H].$$

We hebben dus getoond dat we het algemeen geval van Stelling 4.7 steeds kunnen herleiden naar de affiene rechte $\mathbb{A}(k)$. Zo is Stelling 4.7 ook bewezen.

A Bewijs van Voorbeeld 3.4.

We zullen hier bewijzen dat de groeifunctie van $\mathbb{Z}_m$ met voortbrengers $s_1, \cdots, s_m$ gelijk is aan

$$\begin{aligned}\gamma_{\mathbb{Z}_m,\{s_1,\cdots,s_m\}}(n) = &\sum_{p=0}^{n}\sum_{i=1}^{m} 2^i \binom{m}{i} \Bigg[\binom{p+(i-1)}{i-1} \\ &- \left(\sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{p+(i-1)-(2j-1)+1}{i-2} \right) \\ &- \begin{cases} 0 & \text{als i even} \\ \binom{p+(i-1)-(2\lfloor \frac{i}{2} \rfloor+1)}{i-2} & \text{als i oneven} \end{cases} \Bigg].\end{aligned}$$

We veronderstellen $n \geq m$, omdat we anders meer voortbrengers hebben dan letters en dan zullen we ook woorden tellen waarbij we al deze voortbrengers gebruiken, wat niet kan. Als we dan toch het aantal woorden van lengte $n < m$ willen weten, kunnen we bovenstaande formule opsplitsen aangezien we tellen per lengte.

We geven eerst het bewijs voor $m = 3$ en daarna zullen we het veralgemenen.

Bewijs. $\boxed{m = 3}$

We tellen eerst hoeveel woorden er zijn van exact lengte n. Dit doen we door eerst het aantal woorden met één voortbrenger te tellen, dan met twee en uiteindelijk met drie. Hiervoor gebruiken we herhalingscombinatie.

Voor één voortbrenger vinden we één woord van lengte n. We hebben in totaal drie voortbrengers en ook hun inversen. In totaal hebben we dus 6 woorden van lengte n met één voortbrenger.

Voor twee voortbrengers beschouwen we visueel $n+1$ bolletjes, waar we een bolletje moeten veranderen in een streepje die de scheiding maakt tussen de twee verschillende voortbrengers. Dit kunnen we doen omdat we in een abelse groep zitten en we kunnen dus onze voortbrengers bij elkaar zetten. Zetten we bijvoorbeeld het streepje op het tweede bolletje, dan hebben we het woord met een keer de ene voortbrengers en $n-1$ keer de andere. Merk op dat we het streepje niet op de eerste of laatste plaats kunnen zetten, want dat geeft ons een woord met één voortbrenger en die hebben we reeds geteld. We hebben in totaal $\binom{n+1}{1} - 1 - 1$ keuzes voor ons streepje. Dan tellen we nog hoeveel keuzes we hebben voor de voortbrengers. We moeten twee voortbrengers uit de drie gegeven voortbrengers kiezen en vervolgens hebben we voor elke voortbrenger nog eens 2 keuzes, namelijk de voortbrenger zelf of zijn inverse. We hebben in totaal dus

$$2^2 \binom{3}{2} \left[\binom{n-1}{1} - 1 - 1 \right]$$

woorden van lengte n voor twee voortbrengers.

Voor drie voortbrengers beschouwen we visueel $n+2$ bolletjes waar we twee streepjes op moeten zetten. Merk op dat we weer geen streepjes mogen zetten op de eerste en de laatste plaats. Ook mogen we geen twee streepjes vlak naast elkaar zetten, want dan hebben we een voortbrenger minder. Wat we nu gaan doen is alle mogelijke manieren tellen en dan deze

speciale gevallen ervan aftrekken. We hebben in totaal dus $\binom{n+2}{2}$ mogelijkheden. Hiervan trekken we het aantal mogelijkheden af waarbij er een streepje helemaal links of helemaal rechts wordt gezet. We tellen hier dubbel als we het ene streepje helemaal links en het andere streepje helemaal rechts zetten. In totaal hebben we in dit geval dus $\binom{n+1}{1} + \binom{n+1}{1}$ - 1 mogelijkheden. Dan moeten we nog tellen hoeveel mogelijkheden er zijn om twee streepjes naast elkaar te zetten. Merk op dat we dit in het vorige geval al geteld hebben als er een streepje helemaal links of rechts staat. Als we de twee streepjes nu als één beschouwen en het zetten over n-1 bolletjes, hebben we $\binom{n-1}{1}$ mogelijkheden. Ook hier hebben we voor onze voortbrengers weer telkens de keuze om de voortbrenger of zijn inverse te nemen. In totaal hebben we dus

$$2^3 \binom{3}{3} \left[\binom{n+2}{2} - \binom{n+1}{1} - \binom{n+1}{1} + \binom{n}{0} - \binom{n-1}{1} \right]$$

woorden van lengte n voor drie voortbrengers.

We besluiten dat de groeifunctie van $\mathbb{Z}_3$ gelijk is aan

$$\begin{aligned} \gamma_{\mathbb{Z}_3,\{s_1,s_2,s_3\}}(n) = \sum_{p=0}^{n} & 2 \binom{3}{1} \binom{p}{0} + 2^2 \binom{3}{2} \left[\binom{p+1}{1} - \binom{p}{0} - \binom{p}{0} \right] \\ & + 2^3 \binom{3}{3} \left[\binom{p+2}{2} - \binom{p+1}{1} - \binom{p+1}{1} + \binom{p}{0} - \binom{p-1}{1} \right]. \end{aligned}$$

□

Nu geven we een algemeen bewijs.

Bewijs. We hebben nu m voortbrengers. We tellen weer het aantal woorden van exact lengte n. Voor één, twee en drie voortbrengers kunnen we het vorige bewijs overnemen en krijgen we respectievelijk

$$\begin{aligned} & 2 \binom{m}{1} \binom{n}{0}, 2^2 \binom{m}{2} \left[\binom{n+1}{1} - \binom{n}{0} - \binom{n}{0} \right] \text{ en} \\ & 2^3 \binom{m}{3} \left[\binom{n+2}{2} - \binom{n+1}{1} - \binom{n+1}{1} + \binom{n}{0} - \binom{n-1}{1} \right]. \end{aligned}$$

We tellen nu het aantal mogelijkheden voor woorden van lengte n met vier voortbrengers. We beschouwen $n+3$ bolletjes. Het totaal aantal mogelijke manieren om drie streepjes te zetten is $\binom{n+3}{3}$. Hier trekken we dan weer het aantal mogelijkheden dat een streepje op de eerste of de laatste plaats staat af. Dit zijn er in totaal $\binom{n+2}{2} + \binom{n+2}{2} - \binom{n+1}{1}$. Wat ook nog kan voorkomen is dat er twee of drie streepjes naast elkaar staan, zonder op de eerste of laatste plaats te zijn. Het aantal mogelijkheden hiervoor is $\binom{n}{2} + \binom{n}{2} - \binom{n-1}{1}$, waarbij we in de eerste term de eerste twee streepjes samen nemen en bij de tweede term de

laatste twee streepjes samen nemen. Hierbij hebben we de mogelijkheden op drie streepjes naast elkaar dubbel geteld. In totaal hebben we

$$2^4 \binom{m}{4} \left[\binom{n+3}{3} - \binom{n+2}{2} - \binom{n+2}{2} + \binom{n+1}{1} - \binom{n}{2} - \binom{n}{2} + \binom{n-1}{1} \right]$$

woorden van lengte n voor vier voortbrengers.

Nu veralgemenen we dit denkpatroon voor i voortbrengers. We hebben in totaal

$$2^i \binom{m}{i} \left[\binom{n+(i-1)}{i-1} - \sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} 2 \binom{n+(i-1)-(2j-1)}{i-2} + \sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{n+(i-1)-2j}{i-3} \right.$$
$$\left. - \begin{cases} 0 & \text{als i even} \\ \binom{n+(i-1)-(2\lfloor \frac{i}{2} \rfloor + 1)}{i-2} & \text{als i oneven} \end{cases} \right]$$

mogelijkheden voor woorden van lengte n voor i voortbrengers. We kunnen dit laatste herschrijven tot

$$2^i \binom{m}{i} \left[\binom{n+(i-1)}{i-1} - \left(\sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{n+(i-1)-(2j-1)}{i-2} + \binom{n+(i-1)-(2j-1)}{i-3} \right) \right.$$
$$\left. - \begin{cases} 0 & \text{als i even} \\ \binom{n+(i-1)-(2\lfloor \frac{i}{2} \rfloor + 1)}{i-2} & \text{als i oneven} \end{cases} \right],$$

wat ook gelijk is aan

$$2^i \binom{m}{i} \left[\binom{n+(i-1)}{i-1} - \left(\sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{n+(i-1)-(2j-1)+1}{i-2} \right) \right.$$
$$\left. - \begin{cases} 0 & \text{als i even} \\ \binom{n+(i-1)-(2\lfloor \frac{i}{2} \rfloor + 1)}{i-2} & \text{als i oneven} \end{cases} \right].$$

We besluiten dat de groeifunctie van $\mathbb{Z}_m$ gelijk is aan

$$\gamma_{\mathbb{Z}_m,\{s_1,\cdots,s_m\}}(n) = \sum_{p=0}^{n} \sum_{i=1}^{m} 2^i \binom{m}{i} \left[\binom{p+(i-1)}{i-1} \right.$$
$$- \left(\sum_{j=1}^{\lfloor \frac{i}{2} \rfloor} \binom{p+(i-1)-(2j-1)+1}{i-2} \right)$$
$$\left. - \begin{cases} 0 & \text{als i even} \\ \binom{p+(i-1)-(2\lfloor \frac{i}{2} \rfloor + 1)}{i-2} & \text{als i oneven} \end{cases} \right].$$

□

Referenties

[1] H. Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. London Math. Soc. s3-25 nr. 4 (1972), 603-614.

[2] E. Breuillard, *On uniform exponential growth for solvable groups*, Pure Appl. Math. Q. 3 (2007), 949-967.

[3] E. Colebunders, *Topologie*, VUB, 2015-2016.

[4] P. De La Harpe, *Uniform growth in groups of exponential growth*, Geometriae Dedicata 95 (2002), 1-17.

[5] W. Feit, J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math 13 nr. 3 (1963), 775-1029.

[6] M. Gromov, *Groups of polynomial growth and expanding maps*, Publ. Math. IHES 53 (1981), 53-78.

[7] J. Groves, *Soluble groups with every proper quotient polycyclic*, Illinois Journal of Mathematics 22 nr. 1 (1978), 90-95.

[8] E. Jespers, *Galoistheorie*, VUB, 2013-2014, `http://homepages.vub.ac.be/~efjesper/alg3.pdf`.

[9] E. Jespers, *Inleiding groepentheorie*, VUB, 2013-2014, `http://homepages.vub.ac.be/~efjesper/cursus.pdf`.

[10] E. Jespers, *Ring- en moduultheorie*, VUB, 2014-2015, `http://homepages.vub.ac.be/~efjesper/AlgebraII.pdf`.

[11] A. Mann, *How groups grow*, London Mathematical Society Lecture Note Series 395, Cambridge University Press, 2012.

[12] C. Löh, *Geometric group theory, an introduction*, 2011, `http://www.mathematik.uni-regensburg.de/loeh/teaching/ggt_ws1011/lecture_notes.pdf`.

[13] D.J.S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics 80, Springer-Verslag, New York, 1982.

[14] D.J.S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics 80, 2nd edition, Springer-Verslag, New York, 1996.

[15] I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk SSSR (NS), 57 (1947), 657–659.

[16] J. Tits, *Free subgroups in linear groups*, J. Algebra 20 (1972), 250-270.

[17] A. Weil, *Basic number theory*, Springer-Verlag, Berlin, 1967.

[18] *F2 Cayley graph*, geraadpleegd op 31 oktober 2015, `http://www.math.cornell.edu/~mec/2008-2009/Victor/part4.htm`.