A.M. Schouten
Wollebrand 19
2642 JH Pijnacker
afkeschouten@gmail.com

Competities, schuifpuzzels en automorfismen van S_6

Bachelorscriptie, 9 juni 2009

Scriptiebegeleider: Dr. L. Taelman

Mathematisch Instituut, Universiteit Leiden

Inhoudsopgave

1 Inleiding

Deze scriptie is geschreven naar aanleiding van het Bachelor Seminarium. Het onderwerp betreft de automorfismengroep van S_6. Voor we hier verder over uitweiden zullen we eerst een aantal definities en de Hoofdstelling van deze scriptie geven.

Definitie 1.1. *Zij X de verzameling $\{1, 2, \ldots, n\}$. De verzameling S_n van alle bijecties $X \to X$ met als groepsoperatie samenstelling noemen we de symmetrische groep op n elementen.*

Een groepsautomorfisme is een groepsisomorfisme van een groep G naar zichzelf. De verzameling van alle automorfismen van een groep G vormt een groep onder samenstelling. Deze groep noteren we als $Aut(G)$. Het homomorfisme $f : G \longrightarrow Aut(G)$ gegeven door $\gamma \longmapsto (\sigma_\gamma : x \mapsto \gamma x \gamma^{-1})$ geeft aan $\gamma \in G$ de conjugatieafbeeldingen $\sigma_\gamma : G \xrightarrow{\sim} G$ gedefinieerd door $\sigma_\gamma(x) = \gamma x \gamma^{-1}$. Het beeld van f noteren we als $Inn(G)$. Elementen van $Inn(G)$ noemen we inwendige automorfismen. $Inn(G)$ is een normaaldeler van $Aut(G)$; volgens propositie 4.12 in [1]. Dus we kunnen de quotiëntgroep nemen. Hiermee komen we op de twee hoofdstellingen van deze scriptie:

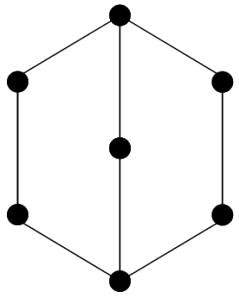
Hoofdstelling 1.2. *Als $n \geq 2$ en $n \neq 6$, dan is elk automorfisme van S_n inwendig.*

Hoofdstelling 1.3. $\#Aut(S_6)/Inn(S_6) = 2$.

In hoofdstuk 2 zullen we bewijzen dat als $n \geq 2$ en $n \neq 6$ dat elk automorfisme in S_n inwendig is en dus dat $\#Aut(S_n)/Inn(S_n)$ gelijk is aan 1 en dat $\#Aut(S_6)/Inn(S_6) \leq 2$.

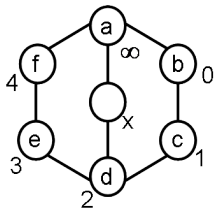
Om de tweede hoofdstelling te bewijzen volstaat het nu om een niet-inwendig automorfisme te construeren. We zullen twee combinatorische constructies geven. De eerste constructie staat in hoofdstuk 3: via teams en competities definiëren we een werking van de symmetrische groep op een verzameling van zes elementen, doormiddel van een werking construeren we een niet-inwendig automorfisme. Met de constructie van een niet-inwendig automorfisme volgt dat $\#Aut(S_6)/Inn(S_6) \neq 1$ en dus gelijk aan 2.

In hoofdstuk 4 zullen we de graaf in Figuur 1 beschouwen.



Figuur 1: De graaf bij de schuifpuzzel

Deze graaf hoort bij de schuifpuzzel in Figuur 2, in deze puzzel kunnen we zes stenen over de zeven posities schuiven. We zullen in dit hoofdstuk een



Figuur 2: Schuifpuzzel

puzzelgroep definiëren. Deze puzzelgroep bevat alle mogelijke zetten van de schuifpuzzel. Deze puzzelgroep zullen we gebruiken om een alternatieve constructie van een niet-inwendig automorfisme van S_6 te geven. We doen dit door opnieuw een werking te definiëren. Dit zal opnieuw een werking zijn van S_6 op een verzameling van zes elementen.

2 Automorfismengroep van S_n

In dit hoofdstuk laten we zien dat automorfismen die transposities bewaren precies de inwendige automorfismen van S_n zijn. We zullen met behulp van een telargument laten zien dat voor $n \neq 6$ alle automorfismen van S_n transposities behouden, daarmee zijn alle automorfismen van S_n inwendig. Als $n = 6$ is het echter niet zeker voor een automorfisme $\theta \in Aut(S_6)$ of het beeld van een transpositie opnieuw een transpositie is. Dit duidt op een mogelijke aanwezigheid van een niet-inwendig automorfisme.

Lemma 2.1. *Een automorfisme ϕ van S_n behoudt transposities dan en slechts dan als ϕ een inwendig automorfisme is.*

Het volgende bewijs is gebaseerd op het bewijs van Lemma 7.4 uit [2].

Bewijs. $\Leftarrow$ Zij ϕ een inwendig automorfisme. ϕ bewaart de cykelstructuur van elke permutatie (Stelling 3.5 in [2]), dus ϕ behoudt ook transposities.

$\Rightarrow$ Zij ϕ een automorfisme van S_n dat transposities behoudt. We zullen bewijzen dat ϕ een inwendig automorfisme is met behulp van inductie. We laten zien dat er conjugaties $\gamma_2, \ldots, \gamma_t$ bestaan zodanig dat $\gamma_t^{-1} \cdots \gamma_2^{-1}\phi$ de transposities $(1\ 2), \ldots, (1\ t)$ vasthoudt.

Voor $t = 2$ hebben we een conjugatie γ_2 nodig zodanig dat $\gamma_2^{-1}\phi$ de transpositie $(1\ 2)$ vasthoudt. Per definitie geldt dat $\phi(1\ 2) = (a\ b)$ voor zekere a en b. Laat $\gamma_2 = (a\ 1)(b\ 2)$ zodat $\gamma_2^{-1}\phi(1\ 2) = (1\ 2)$. Dus er bestaat een conjugatie γ_2 zodanig dat $\gamma_2^{-1}\phi$ de transpositie $(1\ 2)$ vasthoudt.

Voor $t = 3$ hebben we conjugaties γ_2, γ_3 nodig zodanig dat $\gamma_3^{-1}\gamma_2^{-1}\phi$ de transposities $(1\ 2)$ en $(1\ 3)$ vasthoudt. Beschouw $\phi(1\ 3)$, dat is een transpositie, dus er bestaat een $(a\ b)$ zodat $\gamma_2\gamma_3(a\ b) = \phi(1\ 3)$. Er geldt $(a\ b) \neq (1\ 2)$, want stel dat $(a\ b)$ wel gelijk is aan $(1\ 2)$, dan moet gelden dat $\gamma_2\gamma_3(a\ b) = \phi(a\ b)$ maar ook moet gelden dat $\gamma_2\gamma_3(a\ b) = \phi(1\ 2)$, wat in tegenspraak is met de injectiviteit van ϕ. Dus $(a\ b) \neq (1\ 2)$. Ook geldt dat $(a\ b)$ niet disjunct is met $(1\ 2)$: stel dat $(a\ b)$ wel disjunct is met $(1\ 2)$, dan is de orde van $(a\ b)(1\ 2)$ gelijk 2. Dus het beeld van $(a\ b)(1\ 2)$ onder $\gamma_2\gamma_3$ ook: $\gamma_2\gamma_3(a\ b)(1\ 2) = \gamma_2\gamma_3(a\ b)\gamma_2\gamma_3(1\ 2) = \phi(1\ 3)\phi(1\ 2) = \phi(1\ 2\ 3)$, maar $\phi(1\ 2\ 3)$ is van orde 3 en dat levert een tegenspraak op. Dus $(a\ b)$ en $(1\ 2)$ zijn niet disjunct. Er volgt $(a\ b) = (1\ c)$ of $(a\ b) = (2\ c)$, we onderscheiden deze twee gevallen. *Geval 1:* Als $(a\ b) = (1\ c)$ laat dan γ_3 conjugatie met $(3\ c)$ zijn, dan volgt $\gamma_3^{-1}\gamma_2^{-1}\phi(1\ 3) = \gamma_3(1\ c) = (3\ c)(1\ c)(3\ c) = (1\ 3)$, en ook $\gamma_3^{-1}\gamma_2^{-1}\phi(1\ 2) = \gamma_3^{-1}(1\ 2) = (3\ c)(1\ 2)(3\ c) = (1\ 2)$. *Geval 2:* Als $(a\ b) = (2\ c)$ laat dan γ_3 conjugatie met $(1\ 2)(3\ c)$ zijn, dan volgt $\gamma_3^{-1}\gamma_2^{-1}\phi(1\ 3) = (1\ 2)(3\ c)(2\ c)(1\ 2)(3\ c) = (1\ 3)$, en ook $\gamma_3^{-1}\gamma_2^{-1}\phi(1\ 2) = \gamma_3^{-1}(1\ 2) = (1\ 2)(3\ c)(1\ 2)(1\ 2)(3\ c) = (1\ 2)$. Dus er bestaan conjugaties γ_2, γ_3 zodanig dat $\gamma_3^{-1}\gamma_2^{-1}\phi$ de transposities $(1\ 2)$ en $(1\ 3)$ vasthoudt.

Zij nu $t \geq 3$ en laat $\gamma_2, \ldots, \gamma_t$ gegeven door de inductiehypothese: $\psi = \gamma_t^{-1} \cdots \gamma_2^{-1}\phi$ houdt de transposities $(1\ 2), \ldots, (1\ t)$ vast. Omdat ψ transposities behoudt, geldt $\psi(1\ t{+}1) = (l\ k)$ voor zekere l en k. We claimen dat voor $m \leq t$ geldt dat $(1\ m)$ en $(l\ k)$ niet disjunct zijn, en in het bijzonder dat $(1\ 2)$ en $(l\ k)$ en ook $(1\ 3)$ en $(l\ k)$ niet disjunct zijn. Inderdaad, de orde van $(1\ m)(1\ t{+}1) = (m\ t{+}1\ 1)$ is 3, de orde van $\psi(1\ m)(1\ t{+}1) = \psi(1\ m)\psi(1\ t{+}1) = (1\ m)(l\ k)$ is 2 als $(l\ k)$ disjunct is met $(1\ m)$. Dus $(1\ m)$ en $(l\ k)$ zijn niet disjunct. Laat $m = 2$ respectievelijk $m = 3$ en er volgt direct dat $(1\ 2)$ en $(l\ k)$ respectievelijk $(1\ 3)$ en $(l\ k)$ niet disjunct zijn. We kunnen concluderen dat $\psi(1\ t{+}1) = (1\ k)$.

Stel nu dat $k \leq t$, dan betekent dat $\psi(1\ t{+}1) \in \langle (1\ 2), \ldots, (1\ t) \rangle$, en dus dat $(1\ t{+}1)$ vastgehouden wordt door ψ. Dit is in tegenspraak met het gegeven dat ψ injectief is voor $\psi(1\ t{+}1) = (1\ k) = \psi(1\ k)$, dus $k \geq t{+}1$. Definieer γ_{t+1} als de conjugatie met $(k\ t{+}1)$. Nu houdt γ_{t+1} de transposities $(1\ 2), \ldots, (1\ t)$ en $\gamma_{t+1}(1\ t{+}1) = \psi(1\ t{+}1)$ vast. Dus $\gamma_{t+1}^{-1} \cdots \gamma_2^{-1}\phi$ houdt $(1\ 2) \cdots (1\ t{+}1)$ vast, en daarmee is de inductie is compleet.

$\gamma_n^{-1} \cdots \gamma_2^{-1}\phi$ houdt de transposities $(1\ 2), \ldots, (1\ n)$ vast. Deze transposities brengen samen de S_n voor, dus $\gamma_n^{-1} \cdots \gamma_2^{-1}\phi$ is de identiteit. We kunnen nu concluderen dat $\phi = \gamma_2 \cdots \gamma_n \in Inn(S_n)$. Dus een automorfisme ϕ dat transposities behoudt is een inwendig automorfisme. □

Stelling 2.2. *Als $n \geq 2$ en $n \neq 6$, dan is elk automorfisme van S_n inwendig.*

Het volgende bewijs is gebaseerd op het bewijs van Stelling 7.5 uit [2].

Bewijs. Laat T_k de conjugatieklasse in S_n zijn, bestaande uit alle producten van k disjuncte transposities. Een element in S_n is van orde 2 dan en slechts dan als deze in een T_k ligt. Hieruit volgt dat als $\phi \in Aut(S_n)$, dan $\phi(T_1) = T_k$ voor een zekere k. We zullen laten zien dat als $n \neq 6$, dat dan $\#T_k \neq \#T_1$ voor k ongelijk aan 1. Stel $\#T_k \neq \#T_1$ voor k ongelijk aan 1 dan moet het beeld van T_1 onder ϕ weer in T_1 terechtkomen: met andere woorden dan moet gelden dat $\phi(T_1) = T_1$. Dat betekent dat een automorfisme ϕ transposities behoudt en uit Lemma 2.1 volgt dan dat ϕ inwendig is.

Het aantal elementen van T_1 is gelijk aan $n(n-1)/2$. Om de elementen van T_k te tellen merken weeerst op dat er $\frac{1}{2}n(n-1) \times \frac{1}{2}(n-2)(n-3) \times \cdots \times \frac{1}{2}(n-2k+2)(n-2k+1)$ k-tupels van disjuncte transposities zijn. Omdat disjuncte transposities commuteren en er $k!$ ordeningen verkregen kunnen worden van een willekeurige k-tupel, volgt dat het aantal elementen van T_k gelijk is aan $n(n-1)(n-2)\cdots(n-2k+1)/k!2^k$. De vraag of het aantal elementen van T_1 gelijk is aan het aantal elementen van T_k. En dus de vraag of $n(n-1)/2 = n(n-1)(n-2)\cdots(n-2k+1)/k!2^k$ voor een zekere $k > 1$. Is equivalent aan de vraag of er een $k > 1$ bestaat zodanig dat

$$(n-2)(n-3)\cdots(n-2k+1) = k!2^{k-1}. \tag{1}$$

Omdat het rechterlid van vergelijking (1) positief is, moet er gelden dat $n \geq 2k$. Daarom geldt voor vaste n dat $(n-2)(n-3)\cdots(n-2k+1) \geq (2k-2)(2k-3)\cdots(2k-2k+1) = (2k-2)!$.

We zullen door inductie laten zien dat als $k \geq 4$, dat dan $(2k-2)! > k!2^{k-1}$. Zij nu $(2k-2)! > k!2^{k-1}$ gegeven door de inductiehypothese: we laten zien dat als $(2(k{+}1){-}2)! > (k{+}1)!2^{(k+1)-1}$ dat dan ook $(2(k{+}1){-}2)! > (k{+}1)!2^{(k+1)-1}$: $2(k+1)(2k-2)! > (k+1)!2 \cdot 2^{k-1} \Rightarrow 2(k+1)(2k-2)! > 2 \cdot (k+1)!2^{-1} \Rightarrow (2k-2)! > k!2^{k-1}$. Dus voor $k \geq 4$ geldt $(2k-2)! > k!2^{k-1}$.

De enige mogelijkheid voor (1) om te voldoen is als $k = 2$ of $k = 3$. Als $k = 2$ is het rechterlid gelijk aan 4, en het is gemakkelijk om te zien dat er nooit gelijkheid is. We mogen daarom aannemen dat $k = 3$. We weten dat $n \geq 2k$ en omdat $k = 3$ volgt dat $n \geq 6$. Als $n > 6$ dan is het linkerlid van (1) minstens $\times 4 \times 3 \times 2 = 120$. Het rechterlid is altijd gelijk aan 24, dus gelijkheid kan voor geen enkele n optreden. We hebben nu laten zien dat als $n \neq 6$, dat dan het aantal elementen van T_1 ongelijk is aan het aantal elementen van T_k voor alle $k > 1$. Dus als $n \geq 2$ en $n \neq 6$ dan is elk automorfisme van S_n inwendig. □

Als $n = 6$ dan is het aantal elementen van T_1 gelijk aan het aantal elementen van T_3 en ongelijk aan het aantal elementen van T_2. Uit het bewijs van Stelling 2.2 volgt:

Lemma 2.3. *Als θ een niet-inwendig automorfisme is van S_6, en als $\tau \in S_6$ een transpositie is, dan is $\theta(\tau)$ een product van drie disjuncte transposities.*

Propositie 2.4. $\#Aut(S_6)/Inn(S_6) \leq 2$.

Bewijs. Beschouw de afbeelding $f : Aut(S_6) \to S_{\{T_1,T_3\}}$. In Lemma 2.1 zagen we dat $ker(f) = Inn(S_6)$. Hieruit volgt dat de afbeelding $g : Aut(S_6)/Inn(S_6) \to S_{\{T_1,T_3\}}$ injectief is en dus dat $\#Aut(S_6)/Inn(S_6) \leq 2$. □

In de volgende hoofdstukken laten we met twee verschillende constructies zien dat er inderdaad een niet-inwendig automorfisme in S_n bestaat.

3 Eerste constructie: teams en competities

In dit hoofdstuk zullen we de volgende Stelling bewijzen:

Stelling 3.1. $\#Aut(S_6)/Inn(S_6) = 2$

We hebben in Propositie 2.4 gezien dat $\#Aut(S_6)/Inn(S_6) \leq 2$. Als $Aut(S_6)$ enkel uit inwendige automorfismen bestaat geldt dat $\#Aut(S_6)/Inn(S_6) = 1$. Het is dus voldoende om een niet-inwendig automorfisme aan te wijzen, dan volgt direct dat $\#Aut(S_6)/Inn(S_6) = 2$.

Zij $A := \{1, 2, 3, 4, 5, 6\}$, we noemen de elementen van A teams. Zij $B := \{X \subset A | \#X = 2\}$, we noemen de elementen van B wedstrijden, een voorbeeld van een wedstrijd is $X = \{1, 2\}$. Zij $C := \{Y \subset B | \#Y = 3, \cup_{X \in Y} X = A\}$, we noemen de elementen van C zondagen. Een voorbeeld van een zondag is $Y = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$. Op een zondag worden er drie wedstrijden gespeeld en elk team speelt precies één wedstrijd. Zij $D := \{Z \subset C | \#Z = 5, \cup_{Y \in Z} Y = B\}$, we noemen de elementen van D roosters. Een voorbeeld van een rooster is:

$$\begin{aligned} Z = \{&\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}, \\ &\{\{1, 3\}, \{2, 5\}, \{4, 6\}\}, \\ &\{\{1, 4\}, \{2, 6\}, \{3, 5\}\}, \\ &\{\{1, 5\}, \{2, 4\}, \{3, 6\}\}, \\ &\{\{1, 6\}, \{2, 3\}, \{4, 5\}\}\} \end{aligned}$$

Merk op dat in een rooster elke mogelijke wedstrijd precies één keer voorkomt.

Propositie 3.2. $\#A = 6, \#B = 15, \#C = 15, \#D = 6$.

Bewijs. Dat het aantal elementen van A gelijk is aan zes is evident.

Elk team speelt precies één wedstrijd tegen elk ander team, dat betekent $5 + 4 + 3 + 2 + 1 = 15$ wedstrijden, dus het aantal elementen van B is vijftien.

Voor $\#C = 15$ is iets meer nodig. Op elke zondag zijn er drie wedstrijden. De eerste wedstrijd is een willekeurige wedstrijd ($1\ i$), voor deze wedstrijd zijn vijf mogelijkheden. Voor de overige twee wedstrijden zijn dan nog drie mogelijkheden over: $\{j, k\}, \{l, m\}$ en $\{j, l\}, \{k, m\}$ en $\{j, m\}, \{l, k\}$ voor j, k, m, en i ongelijk aan 1. Er volgt dan dat het aantal elementen van C gelijk is aan $5 \cdot 3 = 15$.

Er zijn vijf zondagen van drie wedstrijden, elke zondag ligt in hoogstens twee roosters, want stel er is een zondag die in drie roosters ligt. Zeg de zondag $\{\{1, a\}, \{b, c\}, \{d, e\}\}$, dan hebben we voor deze roosters de volgende opties voor de zondag waarin de wedstrijd $\{1, b\}$ ligt: $\{\{1, b\}, \{a, c\}, \{d, e\}\}$, $\{\{1, b\}, \{a, d\}, \{c, e\}\}$ en $\{\{1, b\}, \{a, e\}, \{c, d\}\}$. Maar merk op dat de eerste van de tweede zondagen, de wedstrijd $\{d, e\}$ bevat, maar op de eerste zondag wordt deze wedstrijd al gespeeld. Dit is in tegenspraak met het feit dat $\cup_{Y \in Z} = B$, dus elke zondag ligt in hoogstens twee roosters. Er zijn dus hoogstens zes roosters. Voor elk rooster kan de eerste zondag $\{\{1, a\}, \{b, c\}, \{d, e\}\}$ gekozen worden, hiervoor zijn vijftien mogelijkheden, want er zijn vijftien zondagen. Voor de zondag waarin dan de wedstrijd $\{1, b\}$ ligt kunnen $\{\{1, b\}, \{a, d\}, \{c, e\}\}$ en $\{\{1, b\}, \{a, e\}, \{c, d\}\}$ gekozen worden, dat betekent dat er minstens $15 \cdot 2 = 30$ verschillende combinaties zijn. Er kunnen immers eventueel nog meer verschillende zondagen gekozen worden. Dat betekent ook dat er minstens $\frac{30}{5} = 6$ roosters zijn. Dus zijn er precies zes roosters. $\square$

De groep S_6 werkt per definitie op A en ook op B en op C dus uiteindelijk krijgen we een werking van S_6 op de verzameling D met zes elementen. Dus S_6 werkt op D, deze werking geeft een homomorfisme $f : S_6 \to S_D$.

Propositie 3.3. *$f : S_6 \to S_D$ is een isomorfisme.*

Bewijs. De kern van deze afbeelding is een normaaldeler van S_6. De groep S_6 heeft precies drie normaaldelers: $\{1\}, A_6$ en S_6. Beschouw $(1\ 2\ 3) \in A_6 \subset S_6$. Stel $(1\ 2\ 3)$ zit in de kern. Voor de zondag $Y \in Z$ waarin de wedstrijd $\{1, 3\}$ ligt, zeg de zondag $Y = \{\{1, 3\}, \{2, i\}, \{a, b\}\}$ geldt dan dat onder de werking van $(1\ 2\ 3)$ deze zondag Y in zichzelf over gaat, maar dan geldt $Y' = \{\{3, 2\}, \{1, i\}, \{a, b\}\} \in Z$. Dit geeft een tegenspraak met $\cup_{Y \in Z} = B$ dus er is geen rooster wat onder de werking van $(1\ 2\ 3)$ in zichzelf overgaat. Met andere woorden: de kern van de afbeelding is triviaal. Omdat de kern triviaal is volgt direct dat f injectief is. Uit de isomorfiestelling volgt nu $S_6 \cong f[S_6]$. Omdat $\#S_D = \#f[S_6]$ volgt dat $f : S_6 \to S_D$ een isomorfisme is. □

Kies nu een willekeurige bijectie $\alpha : D \to \{1, \ldots, 6\}$. Deze bijectie induceert een isomorfisme $g : S_D \to S_6$. Merk op dat g transposities bewaart. Zij θ de samenstelling $g \circ f$. Dit is een automorfisme van S_6.

Stelling 3.4. *$\theta(1\ 2)$ is geen transpositie.*

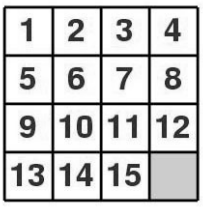
Bewijs. Stel $\theta(1\ 2)$ is wel een transpositie. Omdat g transposities behoudt, geldt dan dat $f(1\ 2)$ ook een transpositie is. Dat wil zeggen dat er een rooster Z door $(1\ 2)$ wordt vastgehouden. Beschouw een zondag $Y \in Z$ met $\{1, 3\} \in Y$, stel $Y = \{\{1, 3\}, \{2, i\}, \{a, b\}\}$. Omdat Z door $(1\ 2)$ wordt vastgehouden volgt dat er een Y' in Z is met $Y' = \{\{2, 3\}, \{1, i\}, \{a, b\}\}$. Dit geeft een tegenspraak met $\cup_{Y \in Z} = B$, want dan geldt $\# \cup_{Y \in Z} Y \leq 14$ en dus niet gelijk aan $\cup_{Y \in Z} Y \neq B$. Er is dus geen rooster dat door $(1\ 2)$ vastgehouden wordt. Daarmee is bewezen dat $\theta(1\ 2)$ geen transpositie is. □

Gevolg 3.5. *θ is een niet-inwendig automorfisme.*

Bewijs. Een inwendig automorfisme behoudt transposities, uit Stelling 4.12 volgt dat θ geen transposities behoudt, dus θ is een niet-inwendig automorfisme. □

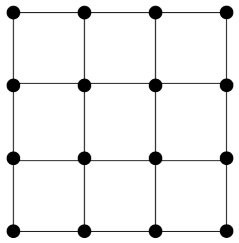
Er bestaat dus een niet-inwendig automorfisme van S_6. Dat betekent dat het aantal elementen van $Aut(S_6)/Inn(S_6)$ ongelijk is aan 1. Uit Propositie 2.4 volgt nu dat $\#Aut(S_6)/Inn(S_6) = 2$ en hiermee hebben we Stelling 3.1 bewezen.

4 Tweede constructie: schuifpuzzel



Figuur 3: Schuifpuzzel van Loyd

De constructie in dit hoofdstuk is gebaseerd op een constructie van Alex Fink en Richard Guy [3]. De schuifpuzzel van Loyd, te zien in Figuur 3, zal bij de meeste lezers wel bekend zijn. De vijftien blokjes in de schuifpuzzel moeten door te schuiven in de juiste volgorde worden gebracht, een 'zet' in deze schuifpuzzel bestaat uit verwisseling van het lege 'blokje x' en een naburig blokje. Bij deze schuifpuzzel kunnen we de graaf tekenen zoals in Figuur 4. In deze graaf staan de knooppunten voor de posities waarop de stenen kunnen liggen en de takken staan voor de routes waarlangs de stenen geschoven kunnen worden.

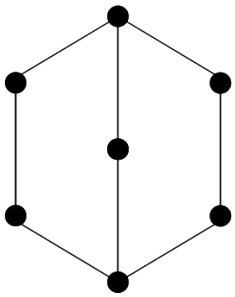


Figuur 4: De graaf bij de schuifpuzzel van Loyd

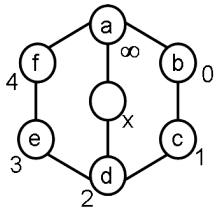
We kunnen ook het algemene geval van zo'n schuifpuzzel beschouwen. Laat Γ een graaf met $n+1$ knooppunten genummerd $x, 1, \ldots, n$. We kunnen deze graaf zien als een schuifpuzzel met n stenen die we over de takken van Γ schuiven. Definieer een legale zet in een puzzel als: de positie waarop zich geen steen bevindt verplaatsen naar een naburige positie en het verplaatsen van de steen op de naburige positie naar de lege positie. Zij $P_\Gamma \subseteq S_n$ de verzameling van permutaties van de beginpositie die te verkrijgen zijn met een reeks legale zetten, waarbij het lege vakje op zijn beginpositie eindigt.

Stelling 4.1. *P_Γ is een ondergroep van S_n.*

Bewijs. Niks doen is een legale zet, dus $\{id\} \in P_\Gamma$. Als we twee afzonderlijke reeksen legale zetten hebben beide met het lege vakje eindigend op zijn beginpositie, en deze na elkaar uitvoeren, hebben we weer een reeks legale zetten. Als we een reeks legale zetten hebben, het lege vakje eindigend op zijn beginpositie, en deze in omgekeerde volgorde uitvoeren, hebben we weer een reeks legale zetten. Dus P_Γ is een ondergroep van S_n. □

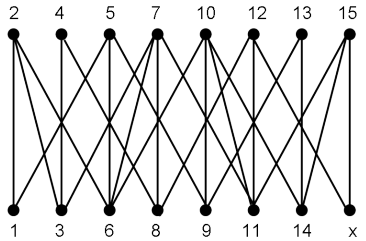


Figuur 5: De graaf bij de Schuifpuzzel



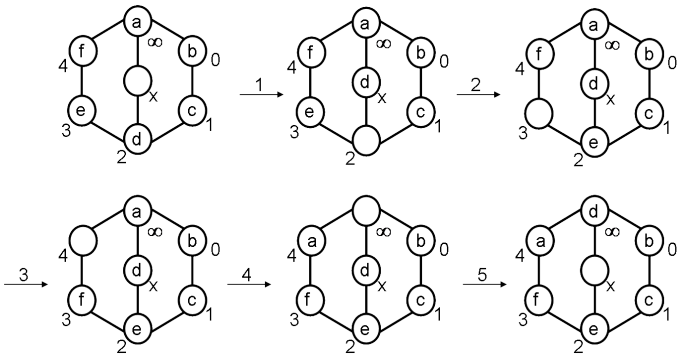
Figuur 6: Schuifpuzzel

De Stelling van Richard Wilson [4] zegt dat, behalve enkelvoudige veelhoeken en de graaf in Figuur 5, de groep van permutaties van verkrijgbare posities ofwel de S_n is, als de graaf een oneven kring bevat, ofwel de A_n is, als de graaf enkel even kringen bevat. In het laatste geval is de graaf een bipartiete graaf: want de knooppunten splitsen in twee verzamelingen en er zijn geen takken tussen leden van dezelfde verzameling. De schuifpuzzel van Loyd is hiervan een klassiek voorbeeld. We kunnen de graaf in Figuur 4 ook tekenen zoals in Figuur 7 en zo zien we direct dat de graaf bij de schuifpuzzel van Loyd inderdaad een bipartiete graaf is.



Figuur 7: De graaf bij de schuifpuzzel van Loyd in bipartiete vorm

We hebben al opgemerkt dat de graaf in Figuur 5 een bijzonder geval is. Zij nu P de ondergroep van S_6 behorende bij de schuifpuzzel van de graaf in Figuur 5 en laat $x, \infty, 0, 1, 2, 3, 4$ de posities op de schuifpuzzel zijn, zoals in Figuur 6 waar bij x de 'lege' beginpositie is, en op de andere posities een steen ligt. We zullen later zien waarom het handig is de posities op deze manier te nummeren en niet met $1, 2, 3, 4, 5, 6$. De permutatie $(\infty\ 4\ 3\ 2)$ zit bijvoorbeeld in P zoals te zien is in Figuur 8 en wegens symmetrie zit ook $(\infty\ 0\ 1\ 2)$ in P.



Figuur 8: De permutatie $(\infty\ 4\ 3\ 2)$

Propositie 4.2. *De permutaties* $a = (\infty\ 4\ 3\ 2)$ *en* $b = (\infty\ 0\ 1\ 2)$ *brengen samen de puzzelgroep voort.*

Bewijs. Beschouw de volgende partitie van de knopen in de graaf: $\{\{\infty, x, 2\}, \{0, 1\}, \{3, 4\}\}$. Het lege vakje begint altijd op positie x. Een reeks legale zetten kunnen we zien als het volgen van het lege vakje. Het is belangrijk te onthouden dat aan het eind van een reeks legale zetten het lege vakje altijd weer terugkomt op positie x. Als het lege vakje in een reeks legale zetten in de deelverzameling $\{\infty, x, 2\}$ blijft, is er in feite niks gebeurd, want het lege vakje komt altijd weer terug op positie x. Als het lege vakje de deelverzameling $\{\infty, x, 2\}$ verlaat en via dezelfde positie als waar $\{\infty, x, 2\}$ verlaten is weer terugkomt, is er in feite ook niets gebeurd. Als het lege vakje de deelverzameling $\{\infty, x, 2\}$ verlaat en via de andere kant weer binnenkomt, is er wel iets gebeurd. We onderscheiden hierin vier gevallen. Als het lege vakje de deelverzameling $\{\infty, x, 2\}$ verlaat aan de bovenkant en via rechts aan de onderkant weer binnenkomt dan is dit gelijk aan b. Als dit gebeurt via links, dan is dit gelijk aan a. Als het lege vakje de deelverzameling $\{\infty, x, 2\}$ verlaat aan de onderkant en via rechts aan de bovenkant weer naar binnenkomt dan is dit gelijk aan b^{-1}. Als dit gebeurt via links, dan is dit gelijk aan a^{-1}. Op deze manier kunnen we alle mogelijke zetten schrijven als een woord in a en b, dus a en b brengen samen de puzzelgroep voort. □

We zullen een andere bruikbare beschrijving van de groep P geven door $P = f[G]$ voor een zekere afbeelding f en groep G. Definieer de projectieve lijn over $\mathbb{F}_5$ als $\mathbb{P}^1(\mathbb{F}_5) := \{(x : y) | x, y \in \mathbb{F}_5; (x, y) \neq (0, 0)\}/\sim$ waarbij $\sim$ wordt gegeven door: $(x_1 : y_1) \sim (x_2 : y_2)$ dan en slechts dan als $(\lambda x_1 : \lambda y_1) = (x_2 : y_2)$ voor een zekere $\lambda \in \mathbb{F}_5^*$ We identificeren $\{\infty, 0, 1, 2, 3, 4\}$ met $\mathbb{P}^1(\mathbb{F}_5)$ door $\infty \leftrightarrow (1 : 0)$ en $x \leftrightarrow (x : 1)$. Merk op dat $\frac{x}{y} \in \mathbb{F}_5$ als $y \neq 0$ en dat $(x : 0) \sim (1 : 0)$.

Definitie 4.3. $GL(2, \mathbb{F}_5)$ *is de groep van* 2×2 *matrices over het lichaam* $\mathbb{F}_5$ *met determinant ongelijk aan 0.*

Er zijn $5^2 - 1 = 24$ mogelijke niet-nul vectoren (a, c) voor de linkerkolom van een matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $GL(2, \mathbb{F}_5)$. Er zijn 5 lineair afhankelijke vectoren van (a, c), dus $5^2 - 5 = 20$ mogelijke vectoren voor (b, d). Dat geeft ons $24 \times 20 = 480$ matrices met determinant ongelijk aan nul.

Definitie 4.4. *$PGL(2,\mathbb{F}_5)$ is de groep $GL(2,\mathbb{F}_5)/\mathbb{F}_5^*$ waarbij $\mathbb{F}_5^*$ de scalaire matrices zijn over $\mathbb{F}_5^*$.*

Het aantal elementen in $PGL(2,\mathbb{F}_5)$ is gelijk aan $\frac{480}{4} = 120$. Merk op dat in $PGL(2,\mathbb{F}_5)$ geldt dat $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a\cdot x & b\cdot x \\ c\cdot x & d\cdot x \end{bmatrix}$ als $x \neq 0$. Definieer nu een werking van $PGL(2,\mathbb{F}_5)$ op $\mathbb{P}^1(\mathbb{F}_5)$ voor $A \in PGL(2,\mathbb{F}_5)$ en $(x:y) \in \mathbb{P}^1(\mathbb{F}_5)$, door $A\cdot(x:y) := (x':y')$ waarbij $\begin{bmatrix} x' \\ y' \end{bmatrix} = A \cdot \begin{bmatrix} x \\ y \end{bmatrix}$. Merk op dat de werking goed gedefinieerd is, want deze is onafhankelijk van de gekozen representant in $PGL(2,\mathbb{F}_5)$, en ook onafhankelijk van de gekozen representant $(x:y)$ in $\mathbb{P}^1(\mathbb{F}_5)$. Als we $\mathbb{P}^1(\mathbb{F}_5)$ zien als $\mathbb{F}_5 \cup \{\infty\}$ dan werkt A op x door $x \mapsto \frac{ax+b}{cx+d}$. Deze werking vatten we samen in het homomorfisme $f : PGL(2,\mathbb{F}_5) \to S_{\mathbb{P}^1(\mathbb{F}_5)}$.

Propositie 4.5. *f is injectief.*

Bewijs. Zij $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in ker(f)$. Deze matrix houdt de punten $0, 1$ en ∞ vast. Uit $0 \mapsto 0$ volgt $b = 0$, uit $\infty \mapsto \infty$ volgt $c = 0$, en omdat $b = c = 0$ en $1 \mapsto 1$ volgt $a = d$. Dus de kern bestaat uit de scalaire matrices en daarmee is f injectief. □

Lemma 4.6. *$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ en $B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ brengen samen een ondergroep van $PGL(2,\mathbb{F}_5)$ van orde 8 voort.*

Bewijs. $G = \left\{ \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix} \right\}$ vormt een groep. Elk element $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ van $PGL(2,\mathbb{F}_5)$ is uniek te schrijven als $\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}$. En elk element $\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}$ is uniek te schrijven als $\begin{bmatrix} 0 & 1 \\ * & 0 \end{bmatrix}$. Van beide vormen bestaan vier matrices en dus is het aantal elementen van G gelijk aan acht. We laten nu zien dat $G = \langle A, B\rangle$: er geldt dat $A, B \in G$ en dus is $\langle A, B\rangle$ in ieder geval een ondegroep van G. Er geldt dat $\langle A, B\rangle > 4$; want $\#\langle B\rangle = 4$ en $A \notin \langle B\rangle$. Er volgt nu dat A en B samen voortbrengers zijn van een ondergroep van $PGL(2,\mathbb{F}_5)$ van orde 8. □

Propositie 4.7. *$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ en $\begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix}$ brengen samen $PGL(2,\mathbb{F}_5)$ voort.*

Bewijs. Uit Lemma 4.6 weten we dat $\left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle$ een ondergroep van $PGL(2,\mathbb{F}_5)$ is van orde 8. $G = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix} \right\rangle$ bevat elementen van orde 3 en 5: $\begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix}$ is van orde 3 en $\begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ is van orde 5. Dus de orde van G is deelbaar door 8,3 en 5. Omdat de orde van $PGL(2,\mathbb{F}_5)$ gelijk is aan $120 = 2^3 \cdot 3 \cdot 5$ volgt automatisch dat $PGL(2,\mathbb{F}_5) = G$. Hiermee is bewezen dat $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ en $\begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix}$ samen $\#PGL(2,\mathbb{F}_5)$ voortbrengen. □

Stelling 4.8. *$P = f[PGL(2,\mathbb{F}_5)]$ in $S_{\mathbb{P}^1(\mathbb{F}_5)}$.*

Bewijs. $f[PGL(2,\mathbb{F}_5)]$ wordt voortgebracht door

$$\begin{aligned} f\left(\begin{bmatrix} 4 & 1 \\ 4 & 0 \end{bmatrix}\right) &= (0\ \infty\ 1)(2\ 3\ 4); \\ f\left(\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}\right) &= (1\ 2\ 4\ 3); \\ f\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) &= (0\ \infty)(2\ 3). \end{aligned}$$

Het is gemakkelijk na te gaan dat de volgende gelijkheden voldoen.

$$\begin{aligned} (0\ \infty\ 1)(2\ 3\ 4) &= a^{-1}bab^{-1}ab^{-1}a^{-1}ba^{-1}ba^{-1}; \\ (1\ 2\ 4\ 3) &= ab^{-1}ab^{-1}a^{-1}ba^{-1}; \\ (0\ \infty)(2\ 3) &= ab^{-1}a^{-1}b. \end{aligned}$$

Daaruit volgt dat $(0\ \infty\ 1)(2\ 3\ 4)$,$(1\ 2\ 4\ 3), (0\ \infty)(2\ 3) \in P$ en dus dat $f[PGL(2,\mathbb{F}_5)] \subseteq P$.

We weten uit Propositie 4.2 dat $(\infty\ 4\ 3\ 2)$ en $(\infty\ 0\ 1\ 2)$ voortbrengers zijn van de ondergroep $P \subset S_{\mathbb{P}^1(\mathbb{F}_5)}$. Om te bewijzen dat $P \subset f[PGL(2,\mathbb{F}_5)]$ volstaat het te verifiëren dat $f\left(\begin{bmatrix} 4 & 0 \\ 1 & 3 \end{bmatrix}\right) = (\infty\ 4\ 3\ 2)$ en $f\left(\begin{bmatrix} 0 & 3 \\ 1 & 3 \end{bmatrix}\right) = (\infty\ 0\ 1\ 2)$ dus dat $(\infty\ 4\ 3\ 2), (\infty\ 0\ 1\ 2) \in f[PGL(2,\mathbb{F}_5)]$ en dus $P \subseteq f[PGL(2,\mathbb{F}_5)]$. We kunnen nu concluderen dat $P = f\,[PGL(2,\mathbb{F}_5)]$. □

We zullen de schuifpuzzel gebruiken om op ongeveer dezelfde wijze als in hoofdstuk 3 een niet-inwendig automorfisme construeren. Zij $\{x, \infty, 0, 1, 2, 3, 4\}$ de verzameling puzzelposities en zij $A := \{a, b, c, d, e, f\}$ de verzameling van stenen. Laat X de verzameling bijecties van A naar de zes posities op de schuifpuzzel zijn. Zo een bijectie kunnen we zien als het plaatsen van de stenen op de puzzel. Definieer een werking van S_A op X voor $\sigma \in S_A$ en $x \in X$, als $\sigma x = x \circ \sigma^{-1}$. We zullen nu net als in hoofdstuk 3 een verzameling D definiëren die bestaat uit zes elementen. Laat $D := X/\sim$, waarbij de equivalentie relatie $\sim$ wordt gegeven door: $x \sim y$ dan en slechts dan als er een reeks legale zetten $\rho \in P$ bestaat zodanig dat $\rho \circ x = y$.

Stelling 4.9. *Voor alle $\sigma \in S_A$ geldt $x \sim y$ dan en slechts dan als $\sigma x \sim \sigma y$*

Bewijs. Gegeven $x \sim y$, dat wil zeggen er bestaat een reeks legale zetten $\rho \in P$ zodanig dat $\rho \circ x = y$. Beschouw nu $\sigma y = y \circ \sigma^{-1} = (\rho \circ x) \circ \sigma^{-1} = \rho \circ (x \circ \sigma^{-1}) = \rho \circ \sigma x$. Omdat $\rho \in P$ een reeks legale zetten is volgt nu direct dat $\sigma x \sim \sigma y$. □

Er volgt nu dat een equivalentieklasse onder de werking van S_A in zijn geheel overgaat in dezelfde of een andere equivalentieklasse. Er zijn $\#D = \frac{720}{120} = 6$ equivalentieklassen in X.

Stelling 4.10. *De zes equivalentieklassen zijn de klassen van posities verkregen uit de volgende beginposities: $abcdef, abcdfe, abcedf, abcefd, abcfde$ en $abcfed$, waarbij we de posities met de klok mee lezen, beginnend bij twaalf uur.*

Bewijs. Het is voldoende te laten zien dat er geen reeks van legale zetten bestaat om een representant in een andere representant om te zetten. Stel dat er wel een reeks legale zetten bestaat om een representant in een andere representant om te zetten, dan is het mogelijk een matrix in $PGL(2, \mathbb{F}_5)$ te vinden die dit doet. Om zo'n matix te bepalen weten we al dat die moet voldoen aan $\infty \mapsto \infty, 0 \mapsto 0$ en $1 \mapsto 1$, voor elke representant geldt immers dat de steen op positie ∞ terug op positie ∞ moet komen en hetzelfde geldt voor de steen op positie 0 en de steen op positie 1. In het bewijs van Propositie 4.5 hebben we gezien dat dit een scalaire matrix geeft. Dus de identiteit. Het volgt dat een representant enkel op zichzelf afgebeeld kan worden en dus op geen enkele andere representant. Zodoende zijn $abcdef, abcdfe, abcedf, abdefd, abcfde$ en $abcfed$ de representanten van de equivalentieklassen.

□

We hadden al opgemerkt dat S_A op D werkt; deze werking geeft een homomorfisme $f : S_A \to S_D$.

Propositie 4.11. *$f : S_A \to S_D$ is een isomorfisme.*

Bewijs. De kern van deze afbeelding is een normaaldeler van S_A. De groep S_A heeft precies drie normaaldelers: $\{1\}, A_A$ en S_A. Beschouw $(d\ e\ f) \in A_A \subset S_A$. Stel $(d\ e\ f)$ zit in de kern. Voor een willekeurige equivalentieklasse, zeg $abcdef$, geldt dan dat onder de werking van $(d\ e\ f)$ deze equivalentieklasse in zichzelf over gaat, maar er geldt $f((d\ e\ f)) = abdefd$. Dit geeft een tegenspraak. We kunnen concluderen dat de kern van de afbeelding gelijk is aan de identiteit. Omdat de kern triviaal is volgt direct dat f injectief is. Uit de isomorfiestelling volgt nu $S_A \cong f[S_A]$. Omdat $\#S_A = \#f[S_A]$ volgt dat $f : S_A \to S_D$ een isomorfisme is. □

Kies nu een willekeurige bijectie $\alpha : D \to A$, deze bijectie induceert een isomorfisme $g : S_D \to S_A$, merk op dat g transposities bewaart. Zij θ de samenstelling $g \circ f$, dit is een automorfisme van S_A.

Stelling 4.12. *$\theta(e\ f)$ is geen transpositie.*

Bewijs. Onder de werking geldt onder andere dat $abcdef \mapsto abcdfe$, $abcedf \mapsto abcfde$ en $abcfed \mapsto abcefd$, het is duidelijk dat $\theta(e\ f)$ geen transpositie is. □

Gevolg 4.13. *θ is een niet-inwendig automorfisme.*

Bewijs. Een inwendig automorfisme behoudt transposities, uit Stelling 4.12 volgt dat θ geen transposities behoudt, dus θ is een niet-inwendig automorfisme. □

Referenties

[1] P. Stevenhagen, Algebra I, 2007.

[2] Joseph J Rotman. An introduction to the theory of groups. Fourth edition. Graduate Texts in Mathematics 148. SpringerVerlag

[3] Ricks Tricky Six Puzzle: S_5 Sits Specially in S_6, Alex Fink University of California, Berkeley Berkeley, CA 94720, Richard Guy The University of Calgary Calgary, Alberta, Canada T2N 1N4

[4] Richard M.Wilson, Graph puzzles, homotopy, and the alternating group, J. Combin. Theory Ser. B 16 (1974) 86-96; MR 48 #10882