MC SYLLABUS 43

EINDIGE GROEPEN

EEN INLEIDENDE CURSUS DOOR

A.M. COHEN EN H.A. WILBRINK

MATHEMATISCH CENTRUM AMSTERDAM 1980

ISBN 90 6196 203 X

INHOUD

HOOFDSTUK V NORMAALDELERS

VOORWOORD

De theorie van de eindige groepen is - afgezien van de elementaire theorie - grofweg te verdelen in drie stromen:

- De lineare representatietheorie, waar de groepen bestudeerd worden via alle mogelijke voorstellingen als groep van matrices;
- de theorie van de permutatiegroepen, waar een groep op verschillende wijzen gezien wordt als groep van permutaties;
- de lokale theorie, waar de struktuur van een groep bestudeerd wordt aan de hand van bepaalde (de zo geheten lokale) ondergroepen.

De elementaire groepentheorie wordt in Hoofdstuk 1 opgezet aan de hand van permutatievoorstellingen. Struktuur-bewarende afbeeldingen (morfismen) worden bestudeerd aan de hand van speciale ondergroepen, de zogenaamde normaaldelers. Bovendien worden er in dit hoofdstuk enige voorbeelden ingevoerd.

De Sylowstellingen vormen het uitgangspunt voor de lokale theorie. Zij komen aan bod in Hoofdstuk 2 en worden daar gevolgd door een stelling van Burnside die informatie geeft over de struktuur van een groep als bepaalde voorwaarden binnen een lokale ondergroep van die groep gelden. De kracht van deze stellingen komt naar voren bij de behandeling van de groepen die minder dan 24 elementen bezitten.

In Hoofdstuk 3 wordt wat uitgebreider aandacht besteed aan permutatiegroepen; de voorbeelden spelen hier een belangrijke rol.

De grondbeginselen van de lineaire representatietheorie worden behandeld in het vierde hoofdstuk. Met name dit deel van de groepentheorie is van belang voor toepassingen in de chemie en de fysika. Wij gaan daar echter niet op in, maar bekijken een enkele toepassing in de groepentheorie zelf.

Het vijfde en tevens laatste hoofdstuk vormt een aanvulling op de abstrakte groepentheorie van de eerste twee hoofdstukken. De struktuur van de normaaldelers krijgt hier met name wat meer aandacht.

De benodigde voorkennis voor deze syllabus gaat de beginselen van de lineaire algebra en het rekenen met permutaties niet te boven. Het is ons doel om een ieder die gewapend is met deze voorkennis, een eerste kennismaking met de theorie van de eindige groepen te verschaffen en om de geïnteresseerde lezer een opstap te geven naar meer geavanceerde leerboeken op dit gebied.

Gepoogd is de toegankelijkheid tot deze syllabus te vergroten door middel van vraagstukken aansluitend aan iedere paragraaf, een index (d.w.z. een lijst van gebruikte termen en begrippen) en een lijst van veel voorkomende symbolen. Bovendien is een literatuurlijst toegevoegd, die zowel boeken voor verdere studie als boeken voor beter begrip van de hier behandelde stof bevat. Men wordt aangeraden bij het doorwerken van deze syllabus goed gebruik te maken van deze lijsten en de "ga na's", "doe zelf's" etcetera serieus op te volgen. De opgaven voorzien van een * worden voor het vervolg van belang geacht, in verband veelal met verwijzingen later in de tekst. De stof zal waarschijnlijk pas echt gaan leven als men met pen en papier probeert te verwerken wat er geschreven staat.

Deze tekst is tot stand gekomen tijdens een oriënterend colloquium voor leraren gegeven in het cursusjaar 1979-1980. Voor hun verbeteringen aangebracht aan eerdere versies willen we graag nog A.E. Brouwer en G.W. de Vries bedanken.

HOOFDSTUK I

FUNDAMENTELE BEGRIPPEN

1.1. Groep en ondergroep

In deze paragraaf voeren we de begrippen groep en ondergroep in. Op de formele definities volgt een serie voorbeelden die in de verdere verhandeling herhaaldelijk terugkeren. De lezer doet er dan ook goed aan met de vanaf 1.1.6 gegeven eindige groepen goed vertrouwd te raken.

1.1.1. DEFINITIE. Een *groep* is een tripel $(G,\cdot,e)$ bestaande uit:
- een verzameling G;
- een binaire operatie: $\left.\begin{array}{l} G \times G \to G \\ (g,h) \mapsto g\cdot h \end{array}\right\}$, de zogenaamde *vermenigvuldiging*;
- een element $e \in G$ (het één-element),

zodanig dat de volgende drie axioma's gelden:

(i) de vermenigvuldiging $\cdot$ is associatief;

(ii) voor iedere $g \in G$ is

linksvermenigvuldiging met g: $\left.\begin{array}{l} G \to G \\ h \mapsto g\cdot h \end{array}\right\}$ zowel als

rechtsvermenigvuldiging met g: $\left.\begin{array}{l} G \to G \\ h \mapsto h\cdot g \end{array}\right\}$ een bijektie van G op zichzelf;

(iii) de links- zowel als de rechtsvermenigvuldiging met het één-element e is de identiteit op G.

Als $\cdot$ en e uit de kontekst duidelijk zijn, wordt $(G,\cdot,e)$ vaak tot G afgekort (hoewel dit strikt genomen slechts een verzameling aangeeft). De vermenigvuldiging $g\cdot h$ zullen we meestal tot gh afkorten. Gebruikmakend van deze schrijfwijze formuleren we de axioma's voor de groep $(G,\cdot,e)$ nog eens, maar nu met kwantoren:

(i) $\forall g,h,k \in G \qquad (gh)k = g(hk)$;

(ii) $\begin{cases} \forall g,h \in G\ \exists k \in G\ gk = h \\ \forall g,h \in G\ \exists k \in G\ kg = h \\ \forall g,h,k \in G \qquad (gh = gk \vee hg = kg) \Rightarrow h = k; \end{cases}$

(iii) $\forall g \in G \qquad ge = eg = g.$

1.1.2. OPMERKINGEN.

- Omdat de plaats van de haakjes in een produkt van elementen uit G er krachtens axioma (i) niet toe doet, worden ze vaak weggelaten. Als $g \in G$ en $n \in \mathbb{N}$, dan schrijven we g^n voor $\underbrace{g \cdot g \ldots . g}_{n \times}$, de n-de macht van g.
- De axioma's hadden zuiniger gekozen kunnen worden. Ga na dat de injektiviteitseisen in (ii) overvloedig zijn. Sterker nog: we kunnen toe met (i), (iii) en (in plaats van (ii)):
  (ii)' $\forall g \in G\ \exists h \in G\ gh = e$.
  Bewijs dit!
- Als $h,g \in G$ met $hg = e$ en $k \in G$ met $gk = e$, dan geldt $h = he = h(gk) = (hg)k = ek = k$. Tezamen met (ii)' volgt nu dat er voor gegeven $g \in G$ precies één $h \in G$ is met $gh = hg = e$. Het element $h \in G$ uit deze formule heet de *inverse van* g en wordt doorgaans aangeduid met g^{-1}. Axioma (ii)' kan nu als volgt worden herschreven:
  (ii)" ieder element in G heeft een inverse.
- De *orde* van een groep G is het aantal elementen $|G|$ van de onderliggende verzameling; als $|G| < \infty$ is, spreken we van een *eindige groep* of een groep van *eindige orde*.

1.1.3. DEFINITIE. Een groep $(H,*,e')$ heet *ondergroep* $(G,\cdot,e)$ als

(i) $H \subseteq G$;

(ii) $* = \cdot|_{H\times H}$, de beperking van $\cdot$ tot $H\times H$;

(iii) $e' = e$.

Als H ondergroep van G is, geven we dat kortweg aan door te schrijven $H \leq G$. Ga na dat G zelf een ondergroep van G is. Als $H \neq G$, dan spreken we van een *echte* ondergroep en noteren we $H < G$. Het is duidelijk dat $\{e\}$ zelf een ondergroep van G is. Een ondergroep H van G heet *niet-triviaal* als $H \neq \{e\}$. Om voor een deelverzameling H van G na te gaan of ze een ondergroep is, moeten we onderzoeken of H voorzien van de vermenigvuldiging van G een groep is.

1.1.4. LEMMA. *Gegeven is een groep* G *en een niet-lege deelverzameling* H *van die groep.* H *is een ondergroep van* G *dan en slechts dan als geldt:*

a) H *is gesloten onder de vermenigvuldiging van* G, *dat wil zeggen*
$(\forall h_1,h_2 \in H)\ (h_1h_2 \in H)$;
b) H *is gesloten onder inverteren in* G, *dat wil zeggen*
$(\forall h \in H)\ (h^{-1} \in H)$.
Als H *eindig veel elementen heeft, dan is* H *een ondergroep dan en slechts dan als* a) *geldt.*

BEWIJS. Gezien de definitie van ondergroep moeten we bewijzen dat $(H,\cdot|_{H\times H},e)$ een groep is dan en slechts dan als a) en b) gelden.
Laat $(H,\cdot|_{H\times H},e)$ een groep zijn. Dan is $\cdot|_{H\times H}$ een afbeelding van $H \times H$ naar H. Dat wil zeggen dat voor willekeurige $h_1,h_2 \in H$ geldt $h_1h_2 \in H$, waarmee a) afgeleid is. b) volgt rechtstreeks uit axioma (ii)" van 1.1.2 voor de groep H. Andersom: als a) en b) gelden, dan is het beeld van $\cdot|_{H\times H}: H \times H \to G$ bevat in H, zodat $\cdot|_{H\times H}$ op te vatten is als een afbeelding van $H \times H$ naar H. Verder bevat H een element h (want $H \neq \emptyset$), dus ook $e = hh^{-1} \in H$.
Axioma's (i) en (iii) van 1.1.1 voor $(H,\cdot|_{H\times H},e)$ volgen nu onmiddellijk uit die voor G, terwijl axioma (ii)" van 1.1.2 uit b) verkregen kan worden. Aldus blijkt $(H,\cdot|_{H\times H},e)$ een groep te zijn.
Wat de laatste uitspraak van het lemma betreft: bedenk dat h^{-1} een macht van h moet zijn als H eindig is. Want voor zekere natuurlijk getal n geldt $h^n = e$, dus ook $h^{-1} = h^{-1}\cdot e = h^{n-1}$. Daarom volgt in dit geval b) uit a) zodat H ondergroep van G is dan en slechts dan als a) geldt. □

1.1.5. GEVOLGEN.
(i) Als $K \leq G$ en $H \leq K$, dan ook $H \leq G$;
(ii) als $H \subseteq K$, $K \leq G$ en $H \leq G$, dan ook $H \leq K$;
(iii) als $H \leq G$ en $K \leq G$, dan ook $H \cap K \leq G$;
(iv) als $\mathcal{H}$ een kollektie ondergroepen van G is, dan geldt $\bigcap_{H\in\mathcal{H}} H \leq G$.

BEWIJS. Doe zelf.

1.1.6. VOORBEELD. Laat $G = \mathbb{R} - \{0\}$ zijn. Als $\cdot$ de gewone vermenigvuldiging der reële getallen $\neq 0$ voorstelt, dan is $(G,\cdot,1)$ een groep; ga zelf de axioma's uit 1.1.1 na. Een bijzondere eigenschap van deze groep is de kommutativiteit van haar vermenigvuldiging: $(\forall g,h \in G)\ (gh = hg)$. Groepen met deze eigenschap heten *kommutatief* of *abels*.
Een eindige ondergroep is $\{1,-1\}$. Het is niet moeilijk in te zien dat dit de enige niet-triviale eindige ondergroep van G is.

De verzameling $H = \{2^a \mid a \in \mathbb{N}\}$ is gesloten onder vermenigvuldiging. Omdat $2 \in H$ en $\frac{1}{2} \notin H$, is H geen ondergroep van G. Hieruit blijkt dat in lemma 1.1.4 eis b) niet overbodig is in het geval dat H oneindige orde heeft.

1.1.7. VOORBEELD. $(\mathbb{R},+,0)$ waar + de gewone optelling der reële getallen voorstelt, is wederom een groep. Deze groep is kommutatief en bezit geen eindige niet-triviale ondergroepen. $(\mathbb{Z},+,0)$ is een voorbeeld van een oneindige ondergroep.

Het zijn juist de twee groepsstrukturen uit 1.1.6 en 1.1.7 die $\mathbb{R}$ tot een lichaam maken.

1.1.8. DEFINITIE. Een *lichaam* is een 5-tupel $(K,\cdot,1,+,0)$ zodanig dat $(K,+,0)$ en $(K-\{0\},\cdot,1)$ abelse groepen zijn en zodat voor alle $a,b,c \in K$ geldt

$$(a+b)\cdot c = (a\cdot c) + (b\cdot c).$$

Doorgaans wordt het lichaam ook met K in plaats van met het omslachtige 5-tupel aangegeven. De bekende voorbeelden zijn $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ en de eindige lichamen $\mathbb{Z}_p$ van de getallen modulo p (priemgetal). Merk op dat voor willekeurige $n \in \mathbb{N} - \{1\}$ het tripel $(\mathbb{Z}_n,+,0)$ wel een groep is, maar dat $(\mathbb{Z}_n - \{0\},\cdot,1)$ dan en slechts dan een groep is als n een priemgetal is. Vandaar dat $\mathbb{Z}_n$ pas een lichaam is als n een priemgetal is.

Vóór we nog meer voorbeelden geven, volgen enkele definities. De definitie van *vektorruimte* (of *lineaire ruimte*) over een lichaam K valt ingeval $K = \mathbb{R}$ samen met de bekende omschrijving. Omdat de algemene versie hier rechtstreeks uit af te leiden is door $\mathbb{R}$ overal door K te vervangen, wordt ze hier achterwege gelaten.

1.1.9. DEFINITIES. Laat $(G,\cdot,e)$ een gegeven groep zijn.

Als $M \subseteq G$, dan heet H de *door* M *voortgebrachte ondergroep* van G als H de kleinste ondergroep (met betrekking tot inklusie) is die M omvat. Zo'n kleinste ondergroep bestaat altijd. Eén manier om dit in te zien is: Laat $\mathcal{H}$ de kollektie ondergroepen van G zijn die M omvatten; dan is $H = \bigcap_{K \in \mathcal{H}} K$ dankzij 1.1.5 (iv) de kleinste ondergroep die M omvat. Een andere manier om in te zien dat H bestaat is een konstruktieve: noteer $M^{-1} = \{m^{-1} \mid m \in M\}$ en definieer $H = \{g_1 g_2 \ldots g_n \mid n \in \mathbb{N};\ g_1,\ldots,g_n \in M \cup M^{-1}\}$. Dan is H gesloten onder vermenigvuldiging en inverteren, dus een ondergroep (vergelijk Lemma 1.1.4). Aan de andere kant bevat iedere groep die M omvat de in H

aanwezige elementen. Derhalve is H de kleinste ondergroep die M omvat. Klaar. Als G eindig is, dan is het voldoende voor de konstruktie van H om produkten van elementen uit M in plaats van uit $M \cup M^{-1}$ te nemen.

We noteren vaak $\langle M \rangle$ voor de door M voortgebrachte ondergroep van G. Als $M = \{g\}$ voor zekere $g \in G$, dan schrijven we vaak $\langle g \rangle$ in plaats van $\langle\{g\}\rangle$. Onder de *orde* van g verstaan we de orde van $\langle g \rangle$. Een door één enkel element voortgebrachte ondergroep heet *cyklisch*. Cyklische groepen zijn kommutatief; ga maar na.

Als K een lichaam is, dan is de additieve ondergroep van K voortgebracht door 1 niet noodzakelijk eindig. De *karakteristiek* van K (notatie kar(K)) is per definitie 0 als deze groep niet eindig is en de orde van deze groep als ze wel eindig is. In het laatste geval is de karakteristiek een priem.

De groep $(\mathbb{C}-\{0\},\cdot,1)$ is kommutatief. We zoeken de eindige ondergroepen van deze groep. Als $x \in \mathbb{C} - \{0\}$ een element van eindige orde is, dan is er een $n \in \mathbb{N}$ zodat $x^n = 1$; bijgevolg is x een n-de machts eenheidswortel. We zullen hieruit afleiden:

1.1.10. STELLING. *De enige eindige ondergroepen van* $G = \mathbb{C} - \{0\}$ *zijn de cyklische groepen* $C_n = \langle \zeta_n \rangle$ *waar* $n \in \mathbb{N}$ *en* $\zeta_n = \exp(2\pi i/n)$.

BEWIJS. Laat H een eindige ondergroep van G zijn. Omdat ieder element van H eindige orde heeft bestaat H uit louter eenheidswortels. Voor we verder gaan bewijzen we een tweetal beweringen:

BEWERING 1. *Als* $x \in \mathbb{C} - \{0\}$ *orde* m *heeft, dan geldt* $\langle x \rangle = C_m$.

BEWIJS. Zo'n x is te schrijven als $x = \exp(2\pi ik/m)$ voor zekere $k \in \mathbb{N}$. Als $\text{ggd}(k,m) = d > 1$, dan is $x = \exp(2\pi i(k/d)/(m/d))$ een (m/d)-de machts wortel, in strijd met het gegeven dat x orde m heeft. Dus geldt $\text{ggd}(k,m) = 1$ en zijn er $a,b \in \mathbb{Z}$ met $ak + bm = 1$. De groep $\langle x \rangle$ bevat derhalve $x^a = \exp(2\pi iak/m) =$ $= \exp(2\pi i(ak+bm)/m) = \exp(2\pi i/m) = \zeta_m$. Er volgt dat $C_m = \langle \zeta_m \rangle \leq \langle x \rangle$. Maar omdat C_m en $\langle x \rangle$ gelijke orde hebben, moeten ze samenvallen.

BEWERING 2. $\langle C_m \cup C_l \rangle = C_{\text{kgv}(m,l)}$.

BEWIJS. Schrijf $r = \text{kgv}(m,l)$. Omdat C_m en C_l uit r-de machts eenheidswortels bestaan, geldt $C_m \cup C_l \subseteq C_r$ en derhalve $\langle C_m \cup C_l \rangle \leq C_r$. Aan de andere kant zijn er $a,b \in \mathbb{Z}$, zodat $lm = r(al+bm)$. Vandaar dat $\zeta_r = \exp(2\pi i(al+bm)/(lm)) =$ $= \zeta_m^a \zeta_l^b$ een element van $\langle C_m \cup C_l \rangle$ is. Omdat hieruit volgt dat $C_r = \langle \zeta_r \rangle \leq$ $\leq \langle C_m \cup C_l \rangle$ hebben we ook de andere inklusie voor de twee onderhavige ondergroepen bewezen; klaar.

VERVOLG BEWIJS STELLING. Laat $x \in H$ een element zijn van de grootst mogelijke orde m. Dan geldt vanwege bewering 1 dat $\langle x \rangle = C_m \leq H$. Stel $y \in H - C_m$ is van orde l. Dan is y geen m-de machts eenheidswortel, dus l is geen deler van m. Met andere woorden $r = kgv(m,l) > m$. Maar dan geldt dankzij bewering 2 dat $\langle \zeta_r \rangle = C_r = \langle C_m \cup C_l \rangle \leq H$. Dus is $\zeta_r \in H$ van orde $r > m$, tegensprekend dat m zo groot mogelijk gekozen was. We konkluderen dat $H - C_m = \emptyset$ ofwel $H = C_m$. □

1.1.11. VOORBEELD. $Gl_n(\mathbb{R})$ = de verzameling van alle inverteerbare (= niet singuliere) n×n-matrices met koëfficiënten in $\mathbb{R}$. Vermenigvuldiging is de bekende matrix-vermenigvuldiging. De notatie $Gl_n(\mathbb{R})$ is afkomstig van de vrij algemeen geaksepteerde benaming General linear group. Het één-element van de groep is de n×n-matrix I_n. Als $n > 1$, dan is de groep niet kommutatief (wijs zelf twee niet kommuterende elementen aan). $Gl_1(\mathbb{R})$ stelt de groep $(\mathbb{R}-\{0\},\cdot,1)$ uit 1.1.6 voor. Het lichaam $\mathbb{R}$ is in de notatie $Gl_n(\mathbb{R})$ opgenomen, omdat vervanging van $\mathbb{R}$ door andere lichamen op analoge wijze groepen van matrices definieert. Ga na dat $Gl_n(K)$ een eindige groep is als K een eindig lichaam is en oneindig als K een oneindig lichaam is. In plaats van $Gl_n(\mathbb{Z}_p)$ voor p priem schrijft men vaak $Gl_n(p)$. Bewijs dat $|Gl_2(p)| = (p^2-1)(p^2-p)$. De groep $Gl_n(\mathbb{R})$ is een ondergroep van $Gl_n(\mathbb{C})$. Als K een lichaam is, dan wordt $Sl_n(K)$ gedefinieerd door $Sl_n(K) = \{g \in Gl_n(K) \mid \det(g) = 1\}$. Zij is de Special linear group.
Bewijs zelf met behulp van de eigenschappen van de determinant dat $Sl_n(K)$ een ondergroep van $Gl_n(K)$ is.

Voorbeeld van een oneindige abelse ondergroep van $Sl_2(\mathbb{R})$ is

$$\left\{ \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \;\middle|\; \alpha \in \mathbb{R} \right\} .$$

1.1.12. VOORBEELD. Onder de eindige ondergroepen van $Gl_2(\mathbb{R})$ bevinden zich weer cyklische groepen van orde n. Ga zelf na dat

$$c_n = \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

voortbrenger van zo'n groep is. Ga na dat c_n een draaiing over $2\pi/n$ in het platte vlak $\mathbb{R}^2$ voorstelt. In tegenstelling tot de situatie bij $Gl_1(\mathbb{C})$ zijn dit echter niet alle eindige ondergroepen. Om deze bewering te staven geven

we een tweede serie eindige groepen D_n, de in vrijwel geen boek over groepentheorie ontbrekende *diëdergroepen*:

$$D_n = \langle c_n, a \rangle,$$

waar c_n als boven en $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. De transformatie a vertegenwoordigt een spiegeling in $\mathbb{R}^2$ ten opzichte van de x-as. Zowel c_n als a laten de regelmatige n-hoek V_n met punten $(\cos(2\pi k/n), \sin(2\pi k/n))$ $(k \in \mathbb{N})$ invariant. We tonen hier aan dat D_n eindig is door te bewijzen dat er voor ieder element $x \in D_n$ getallen $i \in \underline{2}$ en $j \in \underline{n}$ zijn zodat $x = a^i c_n^j$ (Hier en in het vervolg wordt $\underline{k}$ voor $\{1,2,\ldots,k\}$ geschreven). Merk om te beginnen op dat c_n orde n heeft, dat a orde 2 heeft en dat $ac_na^{-1} = c_n^{-1}$. De groep D_n is dus niet abels voor $n > 2$. Uit de laatste gelijkheid leidt men direkt af dat voor iedere $j \in \mathbb{N}$ geldt

$$* \qquad ac_n^j a^{-1} = c_n^{-j} .$$

Met deze formule is snel na te gaan dat de deelverzameling $H = \{c_n^j, ac_n^j \mid j \in \underline{n}\}$ van D_n gesloten is onder de vermenigvuldiging en inverteren. H is dankzij Lemma 1.1.4 dus een ondergroep van D_n. Omdat H de elementen a en c_n bevat, moet $D_n = H$ zijn. D_n is dus eindig en bevat ten hoogste 2n verschillende elementen. Als we nu kunnen bewijzen dat geen tweetal van de produkten $a^i c_n^j$ hetzelfde element in D_n vertegenwoordigt, dan weten we dat D_n uit precies 2n elementen bestaat.

Stel dat voor zekere $i,k \in \underline{2}$ en $j,l \in \underline{n}$ geldt dat $a^i c_n^j = a^k c_n^l$, dan geldt ook $a^{i-k} = c_n^{l-j}$, dus det a^{i-k} = det $c_n^{l-j} = 1$, zodat $i = k \bmod 2$ en $l = j \bmod n$. Vanwege $i,k \in \underline{2}$ en $l,j \in \underline{n}$ volgt $i = k$ en $l = j$. We konkluderen dat alle 2n elementen $a^i c_n^j$ met $i \in \underline{2}$ en $j \in \underline{n}$ verschillend zijn, zodat D_n inderdaad orde 2n heeft.

Een andere manier om in te zien dat D_n eindig is, is na te gaan dat elke transformatie van D_n bepaald wordt door de beelden van de twee onafhankelijke vectoren (1,0) en $(\cos(2\pi/n), \sin(2\pi/n))$ in het vlak $\mathbb{R}^2$. Omdat deze beelden tot de eindige verzameling V_n behoren, zijn er slechts eindig veel van dergelijke transformaties. In deze redenering vatten we D_n als zogenaamde permutatiegroep op. We zullen nu weergeven wat hier precies mee bedoeld wordt, om in 1.3.5 op dit voorbeeld terug te komen.

1.1.13. DEFINITIES. Laat V een eindige verzameling zijn met $|V| = n < \infty$ elementen. Alle bijekties van V op zichzelf vormen een groep met als

vermenigvuldiging de samenstelling van bijekties. Deze groep heet de *symmetrische groep op* V en wordt genoteerd als Sym(V). De groep is eindig, in feite van orde n!, het aantal bijekties van V op V, ook wel *permutaties* van V geheten. Als V = $\underline{n}$, hebben we met Sym($\underline{n}$) van doen, de bekende symmetrische groep, ofwel de groep van alle permutaties van 1,2,...,n. Een ondergroep van Sym(V) heet *permutatiegroep* op V.

Omdat de samenstelling van funkties van een verzameling naar die verzameling zelf een associatieve binaire operatie is, is aan axioma (i) van 1.1.1 'moeiteloos' voldaan. Anders is dat wanneer een groep ingevoerd wordt zoals in het volgende (voor deze paragraaf laatste) voorbeeld.

1.1.14. VOORBEELD. (G,•,e) = ({a,b,c,d,e,f},•,e) met • gegeven door de vermenigvuldigingstabel:

•→ ↑	a	b	c	d	e	f
a	b	e	f	c	a	d
b	e	a	d	f	b	c
c	d	f	e	a	c	b
d	f	c	b	e	d	a
e	a	b	c	d	e	f
f	c	d	a	b	f	e

Om de associativiteit van de vermenigvuldiging te verifiëren moet voor iedere x,y,z ∈ G nagegaan worden dat (xy)z = x(yz) geldt; een omslachtig karwei (op hoeveel gelijkheden komt dit neer?). Het is duidelijk dat voor eindige groepen van grote orde het werk zeer veel tijd zal vergen. Gelukkig is het mogelijk om iedere eindige groep zonder opschrijving van z'n vermenigvuldigingstabel te definiëren. We zullen in het vervolg bewijzen dat iedere eindige groep voorgesteld kan worden als permutatiegroep.

Ter illustratie: de groep uit onderhavig voorbeeld komt in feite overeen met Sym($\underline{3}$), de groep D_4 uit de inleiding komt overeen met een ondergroep van Sym($\underline{4}$). Vóór we dergelijke uitspraken hard kunnen maken, hebben we echter een adekwate wiskundige formulering nodig voor begrippen als 'overeenkomen met'.

OPGAVEN BIJ §1.1.

1. Welke van de volgende deelverzamelingen van $\mathbb{Z}_{11}$ vormen een ondergroep van $(\mathbb{Z}_{11}-\{0\},\cdot,1)$?
   (i) $\{1,3,4,5,9\}$
   (ii) $\{1,3,5,7,8\}$
   (iii) $\{1,8\}$
   (iv) $\{1,10\}$.

2. Bewijs dat een groep van orde ≤ 4 abels is.

*3. Bewijs dat een groep $(G,\cdot,e)$, waarin voor alle $x \in G - \{e\}$ geldt $x^2 = e$, abels is.

4. Welke van onderstaande vermenigvuldigingstabellen beschrijven een groep?

(i)

	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

(ii)

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

5. Laat G een groep zijn en H een niet-lege deelverzameling van G. Bewijs dat H een ondergroep van G is dan en slechts dan als $(\forall x,y \in H)\ (xy^{-1} \in H)$.

*6. Laat $\mathbb{Z}_n^*$ de deelverzameling van die elementen in $\mathbb{Z}_n$ zijn die een inverse hebben ten opzichte van de natuurlijke vermenigvuldiging in $\mathbb{Z}_n$.
Is $(\mathbb{Z}_7^*,\cdot,1)$ cyklisch? Evenzo voor $\mathbb{Z}_8$ resp. $\mathbb{Z}_9$ in plaats van $\mathbb{Z}_7$.

7. Laat K een lichaam zijn. Bewijs dat de deelverzamelingen B en N van $Gl_n(K)$, gegeven door

$$B = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & \ddots & \vdots \\ \emptyset & & & a_{nn} \end{pmatrix} \;\middle|\; a_{ij} \in K;\ a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn} \neq 0 \right\}$$

$$N = \left\{ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ & 1 & & \\ & & \ddots & a_{n-1\,n} \\ \emptyset & & & 1 \end{pmatrix} \;\middle|\; a_{ij} \in K \right\}$$

ondergroepen van $Gl_n(K)$ zijn.
Schrijf in het geval $K = \mathbb{F}_3$ en $n = 2$ de elementen van B en die van N eens uit.

8. (i) Bewijs: als G een groep is met ondergroep H, dan geldt voor iedere $x \in H$ dat $xH = Hx = H$.

   (ii) Laat aan de hand van een voorbeeld zien dat voor $x \in G - H$ de drie verzamelingen xH, Hx, H onderling kunnen verschillen.

*9. Beschouw de verzameling Q der 8 matrices

$$\pm I_2, \quad \pm i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

   (i) Laat zien dat Q een eindige ondergroep van $Sl_2(\mathbb{C})$ vormt.

   (ii) Geef alle ondergroepen van Q.

   Q heet wel de *quaterniongroep*.

* 10. Bewijs:

   (i) Sym(n) wordt voortgebracht door haar 2-kringen.

   (ii) De identiteit kan niet geschreven worden als produkt van een oneven aantal 2-kringen (aanwijzing: Beschouw de positie van de hoogste letter voorkomend in een oneven produkt van 2-kringen van minimale

lengte dat gelijk aan 1 is).

(iii) De afbeelding $sg: Sym(\underline{n}) \to \mathbb{Z}_2$, gegeven door

$$sg(\sigma) = \begin{cases} 0 & \text{als } \sigma \text{ te schrijven is als produkt van een even} \\ & \qquad\qquad \text{aantal 2-kringen,} \\ 1 & \text{anders,} \end{cases}$$

is goed gedefinieerd.

De permutaties σ met $sg(\sigma) = 0$ heten *even* permutaties, terwijl de permutaties σ met $sg(\sigma) = 1$ *oneven* heten.

*11. Bewijs de volgende stelling: *Als* K *een lichaam en* G *een eindige ondergroep van de multiplikatieve groep* $(K-\{0\},\cdot,1)$ *van* K *is, dan is* G *cyklisch*. Dit generaliseert Stelling 1.1.10. Hieronder volgen enkele hints:

We zullen Euler's ϕ-funktie gebruiken, d.w.z. de funktie $\phi: \mathbb{N} \to \mathbb{N}$ die voor $d \in \mathbb{N}$ met $\phi(d)$ het aantal $x \in \underline{d}$ aangeeft, waarvoor $ggd(x,d) = 1$ geldt. Aldus is $\phi(d)$ het aantal elementen in $\mathbb{Z}_d$ van orde d. Bewijs nu achtereenvolgens:

(i) Als $n \in \mathbb{N}$, dan geldt $n = \sum_{d|n} \phi(d)$.

(ii) Voor $d \in \mathbb{N}$ is $\#\{g \in G \mid g^d = 1\} \leq d$. (Gebruik dat de veelterm $x^d - 1 = 0$ hoogstens d nulpunten in K heeft.)

(iii) Als d een deler van $|G|$ is, dan heeft G hetzij 0, hetzij $\phi(d)$ elementen van orde d.

(iv) G bezit een element van orde $|G|$.

*12. Laat $(G,\cdot,e)$ een tripel zijn bestaande uit een verzameling G, een associatieve vermenigvuldiging $\cdot : G \times G \to G$ en een element $e \in G$ zo dat geldt:

(i) $\forall g \in G\ \exists h \in G\ \ hg = e$

(ii) $\forall g \in G \qquad eg = g$

Bewijs dat $(G,\cdot,e)$ een groep is.

1.2. Groepsmorfismen

Afbeeldingen geven een korrespondentie tussen twee verzamelingen aan. Zijn twee verzamelingen voorzien van een gegeven struktuur, dan poogt men korrespondenties tussen die twee verzamelingen aan te geven door afbeeldingen die niet alleen de ene verzameling in de andere overvoeren, maar ook de bijbehorende struktuur behouden. Zulke speciale afbeeldingen worden dan vaak morfismen genoemd. De lineaire afbeeldingen tussen lineaire ruimten bijvoorbeeld zijn de morfismen van lineaire ruimten.

1.2.1. DEFINITIE. Laat $(G,\cdot,e)$ en $(G',\circ,e')$ een tweetal groepen zijn. Een afbeelding $\phi\colon G \to G'$ heet *(groeps)(homo)morfisme* of kortweg *morfisme* als voor alle $g,h \in G$ geldt $\phi(g\cdot h) = \phi(g)\circ\phi(h)$. Omdat $\phi(e) = \phi(e\cdot e) = \phi(e)\circ\phi(e)$, geldt in deze situatie dat $\phi(e) = e'$. Anders gezegd:

$$e \in \phi^{-1}(e').$$

Dit is een speciaal geval van het eerste deel van

1.2.2. LEMMA. *Laat* $\phi\colon G \to G'$ *een groepsmorfisme zijn. Er geldt*
(i) *als* $H' \leq G'$, *dan* $\phi^{-1}(H') \leq G$;
(ii) *als* $H \leq G$, *dan ook* $\phi(H) \leq G'$.

BEWIJS. (i) Als $g,h \in \phi^{-1}(H')$, dan $\phi(g),\phi(h) \in H'$, dus

$$\phi(g\cdot h) = \phi(g)\circ\phi(h) \in H',$$

ofwel

$$g\cdot h \in \phi^{-1}(H').$$

Verder is $e \in \phi^{-1}(e') \subseteq \phi^{-1}(H')$, zodat $\phi^{-1}(H') \neq \emptyset$. Een en ander is volgens Lemma 1.1.4 voldoende opdat $\phi^{-1}(H')$ een ondergroep is ingeval G eindig is. Maak zelf het bewijs af voor een groep G van willekeurige orde.

(ii) te bewijzen is niet moeilijker dan (i). □

1.2.3. DEFINITIES. Het geval $H' = \{e'\}$ van voorgaand lemma geeft dat $\phi^{-1}(e')$ een ondergroep van G is. Deze ondergroep heet de *kern* van het morfisme ϕ en wordt genoteerd als Ker ϕ.

Het volle beeld $\phi(G)$ van G onder ϕ is krachtens (ii) van hetzelfde lemma een ondergroep van G'. Deze ondergroep wordt veelal aangegeven met Im ϕ.

Een *(groeps)monomorfisme* is een injektief groepsmorfisme.

Een *(groeps)epimorfisme* is een surjektief groepsmorfisme.

Een *(groeps)isomorfisme* is een bijektief groepsmorfisme.

Twee groepen G en G' heten *isomorf* als er een groepsisomorfisme van G naar G' is. We schrijven $G \cong G'$.

We hebben nu voldoende definities om te formuleren:

1.2.4. LEMMA. *Laat* ϕ: G $\to$ G' *een groepsmorfisme zijn. Er geldt*

(i) ϕ *is monomorfisme* $\iff$ Ker ϕ = {e};

(ii) ϕ *is epimorfisme* $\iff$ Im ϕ = G';

(iii) ϕ *is isomorfisme* $\iff$ (Ker ϕ = {e} *en* Im ϕ = G').

BEWIJS. (i) "$\Rightarrow$": Stel $x \in$ Ker ϕ. Dan is $\phi(x) = e' = \phi(e)$. Als ϕ monomorfisme is, volgt $x = e$.

"$\Leftarrow$": Laat $x,y \in G$ gegeven zijn met $\phi(x) = \phi(y)$. Omdat

$$e' = \phi(e) = \phi(x^{-1}\cdot x) = \phi(x^{-1})\circ\phi(x) = \phi(x^{-1})\circ\phi(y) = \phi(x^{-1}y),$$

geldt $x^{-1}y \in$ Ker ϕ. Uit Ker ϕ = {e} volgt dus $x^{-1}y = e$, ofwel $x = y$.

(ii) is een direkt gevolg van de definitie van epimorfisme.

(iii) volgt uit (i) en (ii). □

1.2.5. VOORBEELD. Laat $n \in \mathbb{N}$. De afbeelding ϕ: $\mathbb{Z} \to \mathbb{Z}_n$ gedefinieerd door $\phi(z) = z \bmod n$ is een groepsepimorfisme van $(\mathbb{Z},+,0)$ op $(\mathbb{Z}_n,+,0)$ met Ker $\phi = n\mathbb{Z}$, de gehele veelvouden van n. De groep $\mathbb{Z}_n$ is een cyklische groep van orde n. In 1.1.10 hebben we ook een cyklische groep van orde n ontmoet, namelijk C_n, maar:

BEWERING. *Iedere cyklische groep van orde* n *is isomorf met* $\mathbb{Z}_n$.

BEWIJS. Laat C een cyklische groep van orde n met voortbrenger $c \in C$ zijn. De afbeelding α: C $\to \mathbb{Z}_n$ gegeven door $\alpha(c^i) = i$ is goed gedefinieerd, want als $c^i = c^j$, dan is $i = j \bmod n$. Bovendien is α een morfisme; voor $i,j \in \mathbb{N}$ geldt $\alpha(c^i c^j) = \alpha(c^{i+j}) = i + j = \alpha(c^i) + \alpha(c^j)$.
Ga zelf na dat α bijektief is. □

Een gevolg is dat $C_n = \langle \exp(2\pi i/n) \rangle$ isomorf met $\mathbb{Z}_n$ is.

1.2.6. VOORBEELD. Als K een lichaam is, dan is ψ: K $\to Sl_2(K)$ gedefinieerd door

$$\psi(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad (k \in K),$$

een monomorfisme van (K,+,0) naar $Sl_2(K)$.

1.2.7. VOORBEELD. De afbeelding χ: {a,b,c,d,e,f} $\to$ Sym(3), gegeven door

$$\chi(a) = (123), \quad \chi(b) = (132), \quad \chi(c) = (12),$$

$$\chi(d) = (23), \quad \chi(e) = 1 = \text{de identiteit}, \quad \chi(f) = (13),$$

leidt tot een isomorfisme tussen de in 1.1.14 gegeven groep $(G,\cdot,e)$ en $\mathrm{Sym}(\underline{3})$ uit 1.1.13. Aldus hebben we de overeenkomst tussen beide groepen wat preciezer dan in 1.1.14 uit de doeken gedaan.

1.2.8. VOORBEELD. De afbeelding sg: $\mathrm{Sym}(\underline{n}) \to \mathbb{Z}_2$, gedefinieerd als in Opgave 1.1.10, is een epimorfisme met $\mathrm{Ker\ sg} = \mathrm{Alt}(\underline{n})$, de ondergroep van alle even permutaties in $\mathrm{Sym}(\underline{n})$. Als $n = 3$, dan hebben we

$$\mathrm{Ker\ sg} = \{1,(123),(132)\}.$$

Ga na dat deze ondergroep isomorf is met $\mathbb{Z}_3$. De groep $\mathrm{Alt}(\underline{n})$ wordt de *alternerende groep* op n letters genoemd.

1.2.9. LEMMA. *Laat* V *een eindige verzameling van* n *elementen zijn en laat* β *een bijektie van* V *op* $\underline{n}$ *zijn. Dan is de afbeelding* β': $\mathrm{Sym}(V) \to \mathrm{Sym}(\underline{n})$ *gedefinieerd door* $\beta'(\sigma) = \beta\sigma\beta^{-1}$ $(\sigma \in \mathrm{Sym}(V))$ *een isomorfisme.*

BEWIJS. Laat $v_i \in V$ voor $i \in \underline{n}$ het unieke element in V zijn waarvoor $\beta(v_i) = i$. Als $\sigma \in \mathrm{Sym}(V)$ en $\sigma v_i = v_k$, dan is

$$\beta'(\sigma)i = \beta\circ\sigma\circ\beta^{-1}i = \beta\sigma v_i = \beta v_k = k.$$

Dus is $\beta'(\sigma)$ een element van $\mathrm{Sym}(\underline{n})$. Als τ nog een element in $\mathrm{Sym}(V)$ is, dan is

$$\beta'(\sigma\tau) = \beta\circ\sigma\circ\tau\circ\beta^{-1} = \beta\circ\sigma\circ\beta^{-1}\circ\beta\circ\tau\circ\beta^{-1} = \beta'(\sigma)\circ\beta'(\tau),$$

zodat β' inderdaad een morfisme is. Maak zelf het bewijs af. □

Ter afsluiting van deze paragraaf bespreken we nog isomorfismen van een eindige groep op zichzelf (dus met eenzelfde beeld als domein).

1.2.10. DEFINITIES. Een *automorfisme* van een groep G is een isomorfisme van G op zichzelf. De verzameling van alle automorfismen van G noteren we als Aut G.

Laat $(G,\cdot,e)$ een groep zijn. Voor vaste $g \in G$ is de afbeelding

c_g: G → G, gegeven door $c_g(x) = gxg^{-1}$ (x∈G), een automorfisme (ga dit na!). Deze afbeelding c_g wordt *konjugatie met* g genoemd. Een *inwendig automorfisme* φ: G → G is per definitie een afbeelding waarvoor een g ∈ G bestaat zo dat φ = c_g. De verzameling van alle inwendige automorfismen geven we aan met Int G. Als G eindig is, kunnen we schrijven

$$\text{Int } G \subseteq \text{Aut } G \subseteq \text{Sym } G.$$

1.2.11. VOORBEELD. De afbeelding van Sym(3) naar zichzelf, gegeven door:

$$1 \mapsto 1;\ (123) \mapsto (132);\ (132) \mapsto (123),$$

$$(12) \mapsto (32);\ (23) \mapsto (12);\ (13) \mapsto (13),$$

is een inwendig automorfisme, namelijk konjugatie met (13). De ondergroep H = {1,(123),(132)} is invariant onder het automorfisme $c_{(13)}$ van Sym(3). De beperking γ van $c_{(13)}$ tot H is dus goed gedefinieerd. Het is daarom weer een automorfisme van H; van H zelf is het echter geen inwendig automorfisme! Het voorbeeld geeft aan dat niet alle automorfismen van H inwendig zijn.

Omdat H kommutatief is, geldt voor g,h ∈ H dat $c_g(h) = ghg^{-1} = h$. Er volgt dat Int H = $\{id_H\}$. Verder is $\gamma^2 = \gamma\circ\gamma = id_H$. Omdat ieder niet-triviaal automorfisme van H het één-element vasthoudt, verwisselt het de andere twee. Kortom, H kent slechts één automorfisme ≠ id_H, te weten γ. We konkluderen dat Aut H = $\{id_H, \gamma\}$ een groep is. Dit is geen toeval, getuige het volgende resultaat.

1.2.12. PROPOSITIE. *Voor iedere groep* G *zijn* Int G *en* Aut G *groepen van bijekties van de verzameling* G *op zichzelf.*

BEWIJS. Analoog aan 1.1.13 (waar V eindig is) vormen de bijekties van de verzameling V = G op zichzelf een groep K, met als vermenigvuldiging de samenstelling van funkties. Omdat Int G en Aut G bijekties van G op zichzelf zijn, is het voldoende te bewijzen dat Int G en Aut G ondergroepen van K zijn. Omdat de identiteit in Int G en Aut G aanwezig is, zijn beide verzamelingen niet-lege delen van K. We kunnen nu dankzij Lemma 1.1.4 volstaan met te bewijzen dat Int G en Aut G gesloten zijn onder vermenigvuldiging en inverteren. We laten de geslotenheid onder vermenigvuldiging aan uzelf over.

Laat f ∈ Aut G. We bewijzen dat de inverse f^{-1} ∈ K van f weer een

morfisme is. Laat daartoe $x,y \in G$ willekeurig gekozen zijn. Er zijn dan (unieke) $g,h \in G$ met $f(g) = x$ en $f(h) = y$. Omdat $f(gh) = f(g)\cdot f(h) = x\cdot y$, volgt

$$f^{-1}(x)\cdot f^{-1}(y) = gh = (f^{-1}\circ f)(gh) = f^{-1}(f(g)\cdot f(h)) = f^{-1}(xy).$$

We konkluderen dat f^{-1} een bijektief morfisme van G op G is, dus element van Aut G.

Als tenslotte $f \in \text{Int } G$, dan is er een $g \in G$, zodat $f = c_g$. Het is niet moeilijk in te zien dat dan $f^{-1} = c_{g^{-1}} \in \text{Int } G$. Dus ook Int G is gesloten onder inverteren. □

OPGAVEN BIJ §1.2.

1. Welke van de volgende afbeeldingen $\phi_i: \mathbb{C} - \{0\} \to \mathbb{R} - \{0\}$ zijn homomorfismen?
   a. $\phi_1(z) = |z|$
   b. $\phi_2(z) = |z| + 1$
   c. $\phi_3(z) = 1$
   d. $\phi_4(z) = 2$.

*2. Laat K een lichaam zijn. Bewijs dat de determinantafbeelding $\det: Gl_n(K) \to K - \{0\}$ een epimorfisme is.

$$(\det g = \sum_{\sigma\in Sym(\underline{n})} sg(\sigma) \prod_{i=1}^{n} g_{i\sigma(i)}, \quad \text{als } g = (g_{ij}) \in Gl_n(K)).$$

3. Gegeven zijn de permutaties
   $\alpha = (123)(456)(789)$, $\beta = (147)(258)(369)$, $\gamma = (456)(789)$.
   (i) Wat is de orde van α; van β; van γ; van $\beta\gamma$?
   (ii) Bewijs dat α kommuteert met zowel β als γ.
   (iii) Bewijs dat $\alpha \in \langle\beta,\gamma\rangle$.

4. Bepaal Aut D_2 en konstateer dat de automorfismengroep van een kommutatieve groep niet noodzakelijk abels is.

5. De diëdergroep D_4 uit voorbeeld 1.1.12 en de quaterniongroep Q uit Opgave 9 van §1.1 zijn beide eindige groepen van orde 8.
   (i) Hoeveel elementen in D_4 hebben orde 4?
   (ii) Idem voor Q.
   (iii) Bewijs m.b.v. (i) en (ii) dat Q en D_4 niet isomorf zijn.
   (iv) Bereken Aut D_4 en Int D_4.

(iv) Bereken Aut Q en Int Q.

6. $H = \left\{\pm I_2, \pm iI_2, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}\right\}$ is een eindige groep die niet isomorf is met Q uit opgave 1.1.9. Bewijs dit.
Is H isomorf met D_4?

*7. (i) Laat zien dat $\mathrm{Aut}(C_n)$ een abelse groep van orde $\phi(n)$ is, waar ϕ gedefinieerd is als in opgave 1.1.11.

(ii) Bewijs dat $\mathrm{Aut}(C_n)$ isomorf is met $(\mathbb{Z}_n^*, \cdot, 1)$ waar $\mathbb{Z}_n^*$ als in Opgave 1.1.6 gedefinieerd is

(iii) Leid af dat $x^{\phi(n)} = 1 \bmod n$ als $\mathrm{ggd}(x,n) = 1$.

1.3. Permutatievoorstellingen

In stellingen als *Iedere n-dimensionale reële vektorruimte is isomorf met* $\mathbb{R}^n$ worden (iso)morfismen gebruikt om een duidelijker en/of handzamer voorstelling van de gegeven lineaire ruimte te verkrijgen.

We zullen in deze paragraaf een resultaat afleiden dat - hoewel veel minder sterk - dezelfde geest ademt: de reeds eerder aangekondigde, reeds in 1854 door Cayley genoemde stelling.

1.3.1. STELLING (Cayley). *Iedere eindige groep* G *is isomorf met een ondergroep van* Sym(G).

BEWIJS. Beschouw de afbeelding $l: G \mapsto \mathrm{Sym}(G)$ gegeven door $l: g \mapsto l_g$, de linksvermenigvuldiging met $g \in G$. We herinneren eraan dat l_g krachtens axioma (ii) van 1.1.1 een bijektie van G op zichzelf is. l is een groepshomomorfisme, zoals volgt uit de voor alle $g,h,k \in G$ geldige gelijkheid:

$$l_{gh}(k) = (gh)\cdot k = g\cdot(hk) = l_g \circ l_h(k).$$

We zullen aantonen dat G isomorf is met haar beeld onder l in Sym(G). Dankzij Lemma 1.2.4 is het voldoende om te bewijzen dat $\mathrm{Ker}\, l = \{e\}$. Stel $g \in \mathrm{Ker}\, l$. Dan geldt $l_g = \mathrm{id}_G$, dus in het bijzonder $g = g\,e = l_g(e) = \mathrm{id}_G(e) = e$. □

Het hierboven ten tonele gevoerde morfisme l vormt een speciaal geval van een belangrijke klasse morfismen waarop we nu nader ingaan.

1.3.2. DEFINITIES. Laat V een eindige verzameling zijn en laat H een permutatiegroep op V zijn (vergelijk 1.1.13). Onder een *baan van* x *onder* H *in*

V, of kortweg H-baan van x, verstaan we de deelverzameling $Hx = \{h(x) \mid h \in H\}$ van V. "In dezelfde baan zitten" definieert een ekwivalentierelatie op V waarvan de banen juist de ekwivalentieklassen zijn. Het aantal elementen van een baan in V heet de *lengte* van die baan. V bestaat zelf bijvoorbeeld uit één Sym(V)-baan. Als V uit één H-baan bestaat, noemen we H een *transitieve permutatiegroep*. Dat wil zeggen: H is transitief op V precies dan als voor elk tweetal elementen $v,w \in V$ er een $h \in H$ bestaat zodat $h(v) = w$. Voor vaste $v \in V$ vormt de deelverzameling $\{h \in H \mid h(v) = v\}$ een ondergroep van H (bewijs dit!). Deze ondergroep heet de *stabilisator* van v in H of *standondergroep*; de notatie ervoor is H_v. Zo hebben we $\mathrm{Sym}(\underline{n})_n \cong \mathrm{Sym}(\underline{n-1})$. Een *permutatievoorstelling* ϕ *van een groep* G *in een verzameling* V is een groepshomomorfisme $\phi: G \to \mathrm{Sym}(V)$. Merk op dat $\phi(G)$ in zo'n geval een permutatiegroep op V is. Onder de *banen* resp. de *transitiviteit van* ϕ wordt de banen resp. de transitiviteit van $\phi(G)$ verstaan. Voor $v \in V$ is de *standondergroep* of *stabilisator* G_v^ϕ *van* G (*met betrekking tot* ϕ) gedefinieerd door

$$G_v^\phi := \{g \in G \mid \phi(g)(v) = v\}.$$

In andere vorm gegoten luidt dit $G_v^\phi = \phi^{-1}(\phi(G)_v)$. Ga dit na! Als het duidelijk is om welke ϕ het gaat wordt vaak G_v in plaats van G_v^ϕ geschreven.

Een permutatievoorstelling ϕ heet *getrouw* als $\mathrm{Ker}\ \phi = \{e\}$.
De *graad* van een permutatievoorstelling van G in V is het aantal elementen $|V|$ in V.

1.3.3. VOORBEELD. De afbeelding $l: G \to \mathrm{Sym}(G)$ uit het bewijs van Stelling 1.3.1 is een transitieve permutatievoorstelling van G in G, de *linksreguliere permutatievoorstelling* van G geheten. De stelling van Cayley zegt dus dat iedere eindige groep G een getrouwe transitieve permutatievoorstelling van graad $|G|$ heeft. We schrijven deze linksreguliere permutatievoorstelling eens uit voor de groep D_2 uit Voorbeeld 1.1.12. De 4 elementen uit D_2 zijn

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\quad c := c_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

en

$$b := ac = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Schrijf zelf de vermenigvuldigingstabel op. Daaruit is snel af te lezen dat in disjunkte kringsplitsing uitgeschreven de beelden van G onder l in Sym(G) zijn:

$$l_e = id_G;\ l_a = (ea)(bc);\ l_b = (eb)(ac);\quad l_c = (ec)(ab).$$

Aldus blijkt dat D_2 isomorf is met de permutatiegroep

$$\{id_{\underline{4}},\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

Op isomorfie na is dit trouwens de enige niet-cyklische groep van orde 4. Een veelgebruikte benaming voor D_2 is de *vier-groep van Klein*.

1.3.4. OPMERKING. Hoewel we voor een verzameling permutaties geen associativiteit hoeven verifiëren om na te gaan of de verzameling een groep is, is het ook weer niet erg efficiënt om een (grote) groep te schrijven als permutatiegroep van graad gelijk aan z'n orde. Denk aan Sym(n) van orde n!; deze groep is zelf een permutatiegroep van graad n, een heel wat gunstiger graad dan de n! die er via de linksreguliere permutatievoorstelling uit rolt. We trachten hier te motiveren dat voor gegeven abstrakte groep G een getrouwe permutatievoorstelling van minimale of althans kleine graad van belang is.

1.3.5. VOORBEELD. Laat $N \in \mathbb{N} - \{1\}$ gegeven zijn. We schrijven

$$V_n = \{(\cos \tfrac{2\pi k}{n},\ \sin \tfrac{2\pi k}{n}) \mid k \in \mathbb{N}\}.$$

Merk op dat $|V_n| = n$ en dat $gV_n = V_n$ voor iedere $g \in D_n$ (de groep uit Voorbeeld 1.1.12). Teken zelf V_n eens in $\mathbb{R}^2$ voor verschillende waarden van n. De restriktieafbeelding res: $g \mapsto g|_{V_n}$ definieert een homomorfisme res: $D_n \to \mathrm{Sym}(V_n)$. Dit is een permutatievoorstelling van D_n van graad n.

Als $n > 2$, houdt geen enkel element van D_n alle elementen uit V_n puntsgewijs vast; de permutatievoorstelling is dus getrouw. Als $n = 2$, geldt $a|_{V_2} = id_{V_2}$ zodat res geen getrouwe permutatievoorstelling is. Enig rekenwerk verschaft het inzicht dat D_n precies uit alle lineaire transformaties in $Gl_2(\mathbb{R})$ bestaat die V_n in zichzelf overvoeren. Is res transitief?
Nog twee opmerkingen:
- Het platte vlak kan in plaats van als $\mathbb{R}^2$ ook als $\mathbb{C}$ gezien worden.

V_n wordt dan $\{\exp(2\pi ik/n) \mid k \in \mathbb{N}\}$; de afbeelding $c_n \in D_n$ wordt $\exp(2\pi i/n) \in Gl_1(\mathbb{C})$, terwijl a staat voor komplekse konjugatie. Schrijf zelf de finesses van deze opmerking uit door een isomorfisme tussen D_n en een groep van transformaties van $\mathbb{C}$ bestaande uit samenstellingen van lineaire transformaties en komplekse konjugaties te konstrueren.

- In dit voorbeeld is aan een eindige groep van transformaties (i.c. de diëdergroep) van een verzameling (i.c. het reële platte vlak) door restriktie tot een baan (in casu V_n) een transitieve permutatievoorstelling toegevoegd. Ingeval een eindige groep G een permutatievoorstelling in een eindige verzameling V heeft, is "restriktie tot een baan" de aangewezen techniek om de voorstelling in transitieve voorstellingen op te splitsen.

1.3.6. VOORBEELD. $Sl_2(p)$ uit Voorbeeld 1.1.11 is een groep van lineaire transformaties van de lineaire ruimte $\mathbb{Z}_p \times \mathbb{Z}_p$ over het lichaam $\mathbb{Z}_p$. Het eindige platte vlak $\mathbb{Z}_p \times \mathbb{Z}_p$ bestaat uit p^2 punten, zodat $Sl_2(p)$ gezien kan worden als een permutatiegroep van graad p^2. Het punt

$$0 = \begin{pmatrix}0\\0\end{pmatrix} \in \mathbb{Z}_p \times \mathbb{Z}_p$$

vormt een baan op zich. We laten zien dat alle andere punten in één baan zitten. Laat $\binom{x}{y} \in \mathbb{Z}_p \times \mathbb{Z}_p - \{\binom{0}{0}\}$. Als $x = 0$, dan is $y \neq 0$, zodat $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)\binom{x}{y} = \binom{y}{-x}$; omdat $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right) \in Sl_2(p)$ is $\binom{y}{-x}$ in de baan van $\binom{x}{y}$. We mogen dus aannemen dat $x \neq 0$ (zo niet, dan vervangen we namelijk $\binom{x}{y}$ door $\binom{y}{-x}$). Maar

$$\begin{pmatrix}x^{-1}&0\\-y&x\end{pmatrix} \in Sl_2(p)$$

transformeert $\binom{x}{y}$ naar $\binom{1}{0}$. We konkluderen dat ieder element uit $\mathbb{Z}_p \times \mathbb{Z}_p$ - $-\{0\}$in de baan van $\binom{1}{0}$ zit. Bijgevolg werkt $Sl_2(p)$ transitief op $\mathbb{Z}_p \times \mathbb{Z}_p - \{0\}$.

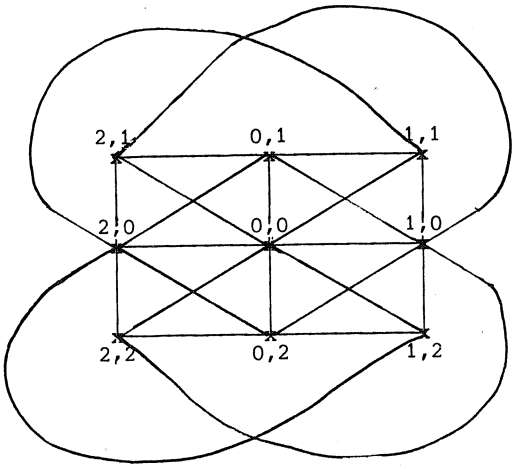
Een lijn in $\mathbb{Z}_p \times \mathbb{Z}_p$ is een verzameling van de vorm

$$a + \mathbb{Z}_p b = \{a+zb \mid z \in \mathbb{Z}_p\}$$

voor gegeven $a,b \in \mathbb{Z}_p \times \mathbb{Z}_p$, $b \neq 0$. Door twee gegeven punten gaat precies één lijn. Op één lijn liggen precies p punten. Omdat $Sl_2(p)$ uit lineaire transformaties van $\mathbb{Z}_p \times \mathbb{Z}_p$ bestaat, worden lijnen in lijnen overgevoerd: voor $a,b \in \mathbb{Z}_p \times \mathbb{Z}_p$ geldt

$$g(a+_{\mathbb{Z}_p} b) = g(a) +_{\mathbb{Z}_p} g(b) .$$

Het platte vlak $\mathbb{Z}_p \times \mathbb{Z}_p$ heeft in totaal $\binom{p^2}{2}/\binom{p}{2} = p(p+1)$ lijnen, waarvan er $(p^2-1)/(p-1) = p+1$ door 0 gaan. Deze p+1 lijnen door 0 vormen één baan. Ga dit zelf na. Bestudeer ook in hoeveel $Sl_2(p)$-banen de resterende p^2-1 lijnen (niet door 0) uiteenvallen. De restriktie van de permutatievoorstelling van $Sl_2(p)$ op de lijnen door 0 is niet getrouw als $p > 2$; dit ziet men in door na te gaan dat $-I_2 \in Sl_2(p)$ de identieke permutatie op de lijnen door 0 teweeg brengt. Tenslotte een tekening van $\mathbb{Z}_3 \times \mathbb{Z}_3$ inklusief zijn 12 lijnen.



1.3.7 VOORBEELD. Laat p priem en $n \in \mathbb{N}$. We bekijken de optelgroep van de vektorruimte $\mathbb{Z}_p^n$, dat wil zeggen $(\mathbb{Z}_p^n,+,0)$. Voor $a \in \mathbb{Z}_p^n$ definiëren we de *translatie* T_a over a als de transformatie gegeven door

$$T_a(x) = x + a \qquad (x \in \mathbb{Z}_p^n) .$$

De translatie T_a komt met de linksvermenigvuldiging l_a uit 1.3.1 overeen; De groep $A = \{T_a \mid a \in \mathbb{Z}_p^n\}$ van alle translaties is dus isomorf met $\mathbb{Z}_p^n$. De ondergroepen $Gl_n(p)$ en A van $Sym(\mathbb{Z}_p^n)$ hebben triviale doorsnede, want

$$A \cap (Sym(\mathbb{Z}_p^n)_0) = \{id\} \quad \text{en} \quad Gl_n(p) \leq Sym(\mathbb{Z}_p^n)_0 .$$

OPGAVEN BIJ §1.3.

1. Laat V_n de verzameling punten in $\mathbb{R}^2$ uit voorbeeld 1.3.5 zijn.
   Beschouw de afbeelding $\beta: V_n \to \underline{n}$ gedefinieerd door
   $\beta(\cos \frac{2\pi k}{n}, \sin \frac{2\pi k}{n}) = t$, waar $t \in \underline{n}$ voldoet aan $t = k \bmod n$.
   Volgens Lemma 1.2.9 induceert β een isomorfisme $\beta': \mathrm{Sym}(V_n) \to \mathrm{Sym}(\underline{n})$.
   (i) Geef de beelden van a respektievelijk c_n onder $\beta' \circ \mathrm{res}: D_n \to \mathrm{Sym}(\underline{n})$.
   (ii) Geef een ondergroep (door uitschrijven van de elementen) van $\mathrm{Sym}(\underline{4})$ die isomorf is met D_4.
   (iii) Bewijs dat D_4 niet isomorf is met een permutatiegroep in $\underline{n}$ als $n < 4$.

2. De groep H uit Opgave 1.2.6 heeft een permutatievoorstelling in $\underline{4}$. Bewijs dit door een baan van H bestaande uit 4 vektoren in $\mathbb{C}^2$ aan te wijzen. Zo'n voorstelling is niet getrouw. Bestaat er een getrouwe permutatievoorstelling van H in $\underline{4}$? Zelfde vraag voor de groep Q uit Opgave 1.1.9.

3. Bewijs dat $\mathrm{Gl}_2(2)$ een getrouwe permutatierepresentatie van graad 3 heeft (namelijk op de vektoren in $\mathbb{Z}_2 \times \mathbb{Z}_2 - \{0\}$).
   Leid hieruit af dat $\mathrm{Gl}_2(2)$ isomorf is met $\mathrm{Sym}(\underline{3})$.

4. Laat $G = \mathrm{Sl}_2(p)$ de groep uit voorbeeld 1.3.6 zijn. Geef de verzameling lijnen in $\mathbb{Z}_p \times \mathbb{Z}_p$ door 0 aan met π en de bijbehorende permutatievoorstelling met $\phi: G \to \mathrm{Sym}(\pi)$.
   (i) Bewijs dat $\mathrm{Ker}\ \phi = \{\pm I_2\}$ als $p > 2$.
   (ii) Als $p = 3$, bewijs dan dat $\phi(G) \cong \mathrm{Alt}(\underline{4})$.
   (iii) Is $\phi(\mathrm{Sl}_2(7))$ isomorf met $\mathrm{Alt}(\underline{7})$?

5. Welke van de volgende permutatiegroepen G_i in $\underline{6}$ zijn transitief?

   $G_1 = \langle (123)(456), (1346) \rangle$;
   $G_2 = \langle (1234)(56), (123) \rangle$.

1.4. Nevenklassen

In deze en de volgende paragraaf maken we gebruik van permutatievoorstellingen van een eindige groep op haar eigen onderliggende verzameling om meer inzicht in de groep zelf te verkrijgen.

1.4.1. DEFINITIE. Laat G een eindige groep zijn en laat H èen willekeurige ondergroep van G zijn. Uit de linksvermenigvuldiging $l_h: G \to G$ met een element $h \in H$ verkrijgen we de permutatievoorstelling

$$l|_H : H \to \mathrm{Sym}(G) \text{ door het voorschrift } l|_H(h) = l_h.$$

De notatie $l|_H$ geeft al aan dat het hier om de restriktie van l tot H gaat. De banen van $l|_H$ in G heten de *rechternevenklassen* van H in G. De rechternevenklasse die $g \in G$ bevat, is $Hg = \{hg \mid h \in H\}$. Door $g = e$ te nemen, zien we dat H zelf ook een rechternevenklasse is. Omdat banen ekwivalentieklassen zijn, vormen de rechternevenklassen een partitie van G, dat wil zeggen

$$G = \bigcup_{g \in G} Hg \text{ en } (\forall g_1, g_2 \in G)(Hg_1 \neq Hg_2 \Rightarrow Hg_1 \cap Hg_2 = \emptyset).$$

De rechternevenklassen hebben echter ook een voor banen niet altijd gebruikelijke eigenschap: ze hebben alle gelijke lengte.

1.4.2. STELLING (Lagrange). *Laat* G *een eindige groep zijn waarvan* H *ondergroep is. Dan is* $t = |G|/|H|$ *een natuurlijk getal en zijn er* $g_1, \ldots, g_t \in G$ *zodat* $Hg_1, Hg_2, \ldots, Hg_t$ *een partitie van* G *vormen. Verder geldt voor iedere* $g \in G$ *dat* $|H| = |Hg|$. *Dus* t *is het aantal rechternevenklassen van* H *in* G.

OPMERKING. Overeenkomstige definitie en uitspraken zijn er natuurlijk ook voor *linkernevenklassen*.

BEWIJS. Rechtsvermenigvuldiging met $g \in G$ geeft een bijektie: $H \to Hg$ vanwege axioma (ii) uit 1.1.1. Vandaar de laatste uitspraak in de stelling.
Laat k het aantal banen van $l|_H$ in G zijn. Nummer deze banen met de getallen 1 t/m k en kies uit de i-de baan een element g_i $(i=1,\ldots,k)$. Uit het voorgaande volgt dat $Hg_1, \ldots, Hg_k$ een partitie van G vormt, bestaande uit deelverzamelingen van kardinaliteit $|H|$. Nu telt G precies $k|H|$ elementen, dus

$$|G| = k|H| = t|H|$$

Omdat we k door t mogen vervangen is het bewijs voltooid. □

1.4.3. KOROLLARIUM. *Als* G *een eindige groep is en* $g \in G$, *dan is de orde van* g *een deler van* $|G|$.

BEWIJS. De orde van g is per definitie de orde van de ondergroep $\langle g \rangle$ van G. □

1.4.4. DEFINITIES. Het getal t uit de stelling heet de *index* van H in G. De kollektie rechternevenklassen van H in G wordt vaak door H\G aangeduid. We hebben gezien dat $t = |H\backslash G| = |G|/|H|$. Voor $t = |G/H|$ schrijven we ook $|G:H|$. De notatie voor de kollektie linkernevenklassen van H in G is G/H. Een stel elementen $g_1, g_2, \ldots, g_t \in G$ als in de stelling heet *representantensysteem* voor de rechternevenklassen van H in G.

1.4.5. VOORBEELD. De ondergroep Alt(n) van Sym(n) bestaande uit alle even permutaties (zie Voorbeeld 1.2.8) heeft één nevenklasse: die der oneven permutaties (hoe bewijst u dit?). De orde van Alt(n) bedraagt dus $\frac{1}{2}n!$. Wat zijn de ordes van elementen van Alt(3), Alt(4) en Alt(5)?
Hoewel de orde van ieder element deler van de orde van de groep is, is niet iedere deler van de orde van de groep orde van een element. Zo dit wel het geval is hebben we met een cyklische groep te doen.

1.4.6. VOORBEELD. $G = Gl_n(p)$. De ondergroep $H = Sl_n(p)$ uit Voorbeeld 1.1.11 heeft $p-1$ rechternevenklassen met representantensysteem

$$g_i = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & i \end{pmatrix},$$

waar $i \in \mathbb{Z}_p$. Voor $g \in G$ geldt dus $\det g = i$ dan en slechts dan als $g \in Hg_i$. Bewijs dit zelf door gebruik te maken van

$$Hg_i = \{g \in G \mid \det g = i\}.$$

Men rekent eenvoudig na dat

$$|Gl_n(p)| = \#\{\text{onafhankelijke geordende bases van } \mathbb{Z}_p^n\}$$
$$= (p^n-1)(p^n-p) \ldots (p^n-p^{n-1}).$$

Vergelijk met 1.1.11 het geval n = 2. Omdat er $p-1$ rechternevenklassen van H in G zijn, is de orde van $Sl_n(p)$

$$|Sl_n(p)| = |Gl_n(p)|/(p-1) = (p^n-1)(p^n-p) \ldots (p^n-p^{n-2})p^{n-1}.$$

1.4.7. LEMMA. *Voor iedere eindige groep* G, *ondergroep* H *van* G *en elementen* $x,y \in G$ *geldt*

$$xH = yH \iff y^{-1}xH = H \iff y^{-1}x \in H.$$

BEWIJS. Beschouw dit als een oefening. □

De linkernevenklassen van een ondergroep H van een gegeven groep G zijn de banen van de permutatievoorstelling $h \mapsto r_{h^{-1}}$, waar r de rechtsvermenigvuldiging met elementen uit H op G voorstelt. Op de kollektie van deze banen werkt de hele groep G weer door linksvermenigvuldiging.

1.4.8. STELLING. *Laat* G *een eindige groep zijn. Als* $H \leq G$, *dan is de afbeelding* $l^H: G \to \mathrm{Sym}(G/H)$ *gedefinieerd door*

$$l^H(g)kH = gkH \qquad (g,k \in G)$$

een transitieve permutatievoorstelling van G *van graad* $|G/H|$.

Andersom, als G *een transitieve permutatievoorstelling van graad* t *heeft, dan heeft* G *een standondergroep* H *van index* t, *dus met* $|G/H| = t$.

BEWIJS. Ga zelf na dat l^H een morfisme is. Als $g,k \in G$, dan geldt

$$l^H(gk^{-1})kH = gH;$$

er volgt dat l^H transitief is.

Omgekeerd, bij gegeven transitieve permutatievoorstelling ϕ van G in een verzameling V met $|V| = t$ kiezen we een $v \in V$ vast en nemen we $H = G_v^{\phi}$, de standondergroep van v in G (zie 1.3.2). We laten zien dat de index van H in G precies t is met behulp van de afbeelding $\psi: G/H \to V$ gedefinieerd door $\psi(gH) = \phi(g)v$ $(g \in G)$. We merken allereerst op dat ψ goed gedefinieerd is: als er $g,k \in G$ zijn met $gH = kH$, dan is $k^{-1}g \in H$ vanwege het voorgaande lemma, dus $\phi(k^{-1}g)v = v$, zodat $\phi(g)v = \phi(k)v$. Verder is ψ surjektief omdat ϕ transitief is (ga na!). ψ is ook injektief, want als voor zekere $g,k \in G$ geldt $\phi(g)v = \phi(k)v$, dan is $\phi(k^{-1}g)v = v$, dus $k^{-1}g \in H$ en (met nogmaals het lemma) $kH = gH$.

We konkluderen dat ψ bijektief is. De verzamelingen G/H en V bestaan dus uit evenveel elementen, te weten $|G/H| = |V| = t$. □

1.4.9. VOORBEELD. Laat $n \in \mathbb{N} - \underline{1}$. De standondergroep bij $n \in \underline{n}$ van $\mathrm{Sym}(\underline{n})$ als permutatiegroep op $\underline{n}$ is de ondergroep $\mathrm{Sym}(\underline{n-1})$. We kunnen aan $\mathrm{Sym}(\underline{n})$ echter ook de permutatievoorstelling op de parenverzameling

$$P_n = \{\{i,j\} \mid i,j \in \underline{n};\ i \neq j\}$$

toekennen. Deze voorstelling π: $\mathrm{Sym}(\underline{n}) \to \mathrm{Sym}(P_n)$ wordt gegeven door

$$\pi(g)\{i,j\} = \{g(i),g(j)\} \quad (i,j \in \underline{n};\ g \in G).$$

Ga zelf na dat π transitief is en van graad $\binom{n}{2}$. Dit impliceert volgens de stelling dat $\mathrm{Sym}(\underline{n})$ een ondergroep van orde $2(n-2)!$ heeft. Geef zo'n ondergroep in de gevallen $n = 4,5$ door uitschrijven van de elementen.

1.4.10. VOORBEELD. $G = \mathrm{Sl}_n(p)$ heeft, zoals we in 1.3.6 gezien hebben, een transitieve permutatievoorstelling op de punten van $\mathbb{Z}_p \times \mathbb{Z}_p - \{0\}$. Uit

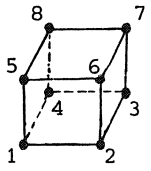
$$|\mathrm{Sl}_2(p)| = p(p^2-1) \quad \text{en} \quad |\mathbb{Z}_p \times \mathbb{Z}_p - \{0\}| = p^2-1$$

leiden we met behulp van de stelling af dat $\mathrm{Sl}_2(p)$ een ondergroep van orde p heeft en dat deze ondergroep de stabilisator van een gegeven vektor $\neq 0$ in $\mathbb{Z}_p \times \mathbb{Z}_p$ is. Als dit de vektor $\binom{1}{0}$ is, dan is de betreffende ondergroep

$$H = \{\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z}_p\}.$$

In 1.3.6 bleek $\mathrm{Sl}_2(p)$ ook een transitieve permutatievoorstelling van graad $p+1$ op de lijnen door 0 te bezitten. Bij gevolg heeft $\mathrm{Sl}_2(p)$ ook een ondergroep van orde $p(p-1)$. Geef zelf zo'n ondergroep aan die H omvat.

1.4.11. VOORBEELD. Groep van isometrieën van de kubus.
Beschouw een kubus in de Euklidische ruimte. We willen de groep G van alle isometrieën bepalen die de kubus in zichzelf overvoeren. Een isometrie is een draaiing of een spiegeling. Het wordt aan uzelf overgelaten om aan te tonen dat G een getrouwe permutatievoorstelling op de 8 hoekpunten van de kubus heeft.



Nummeren we de hoekpunten als in de figuur, dan korrespondeert iedere isometrie die de kubus in zichzelf overvoert dus met één permutatie op $\underline{8}$, terwijl geen twee verschillende isometrieën bij dezelfde permutatie behoren. Verwaarlozen we het bij de getrouwe permutatievoorstelling $G \to \mathrm{Sym}(\underline{8})$ behorende isomorfisme, dan kunnen we G als ondergroep van $\mathrm{Sym}(\underline{8})$ opvatten. Hiervan gebruik makend zien we dat draaiing (*rechtsom*) van 90° om de vertikale as door het midden van het vierkant met hoekpunten 5,6,7,8 de permutatie $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \in G$ oplevert, en dat spiegeling om het horizontale vlak door het midden van de vertikale ribben de permutatie $(1\ 5)(2\ 6)(3\ 7)(4\ 8) \in G$ geeft.

We zullen nu twee methoden schetsen om de orde van G te bepalen. Gezien de twee bovengenoemde transformaties is G transitief op $\underline{8}$. Derhalve weten we dankzij 1.4.8 dat $|G| = |G_1|8$.
Om $|G_1|$ te berekenen, konstateren we allereerst dat G_1 de punten op afstand de lengte van een ribbe (dus de punten 2,4,5) in elkaar moet overvoeren. Draaiing van 120° om de as door de punten 1 en 7 doet inzien dat de permutatie $(2\ 4\ 5)(3\ 8\ 6)$ bevat is in G_1. Restriktie van G_1 tot $\{2,4,5\}$ geeft de permutatievoorstelling $\rho\colon G_1 \to \mathrm{Sym}\{2,4,5\}$, gegeven door

$$\rho(g) = g\big|_{\{2,4,5\}} \qquad (g \in G_1).$$

Zo is $\rho((2\ 4\ 5)(3\ 8\ 6)) = (2\ 4\ 5)$. Hieruit blijkt onmiddellijk dat ρ transitief is op $\{2,4,5\}$. We passen Stelling 1.4.8 nogmaals toe:

$$|G_1| = 3|G_{1,2}|, \quad \text{waar} \quad G_{1,2} = G_1 \cap G_2 = G_1 \cap G_2^{\rho}.$$

Is tenslotte $x \in G_{1,2}$ een niet-triviale isometrie, dan kan x geen draaiing zijn (anders zou de ribbe door 1 en 2 draaiings-as zijn), dus moet x spiegeling zijn met spiegelvlak door de hoekpunten 1 en 2. Zo doorgaande vinden we $x = (4\ 5)(3\ 6)$ en blijkt $|G_{1,2}| = 2$. Dus $|G| = |G_1|8 = |G_{1,2}|24 = 48$.

Voor de tweede methode om de orde te berekenen gebruiken we dat iedere isometrie die de kubus in zichzelf overvoert de tetraëder door de punten 1,3,6,8 hetzij in zichzelf, hetzij in de tetraëder 2,4,5,7 overvoert. Dit induceert een permutatievoorstelling σ: G $\to$ Sym{{1,3,6,8},{2,4,5,7}} die transitief is (immers $\sigma((1\ 5)(2\ 6)(3\ 7)(4\ 8))$ = ({1,3,6,8},{2,4,5,7})).

Maak zelf de berekening af met Stelling 1.4.8.

OPGAVEN BIJ §1.4

1. Laat G een groep zijn en laat X,Y,Z deelverzamelingen van G zijn, Met XY geven we de deelverzameling $\{xy \mid x \in X,\ y \in Y\}$ van G aan.
   (i) Ga na dat als X een ondergroep van G is, XY uit rechternevenklassen van X bestaat.
   (ii) Bewijs (XY)Z = X(YZ).

2. Wat zijn de rechternevenklassen van {1,(12)} in Sym(3)?
   Wat zijn de linkernevenklassen van deze ondergroep?

*3. (i) Bewijs dat C_p (p priem) geen echte niet-triviale ondergroepen heeft.
   (ii) Bewijs dat iedere eindige groep zonder echte niet-triviale ondergroepen isomorf met C_p voor zeker priemgetal p is.

4. Bewijs dat een eindige groep van priemorde noodzakelijk cyklisch is.

5. Bewijs voor een drietal ondergroepen X,Y,Z van een gegeven groep de ekwivalentie van de volgende twee uitspraken
   (i) $(XY) \cap (XZ) = X(Y \cap Z)$
   (ii) $(X \cap Y)(X \cap Z) = X \cap (YZ)$.
   Geef een voorbeeld aan waaruit blijkt dat (i) niet altijd geldt.

1.5. Konjugatie

Laat G een eindige groep zijn. Voor $g \in G$ hebben we de afbeelding c_g: G $\to$ G gedefinieerd door $c_g(x) = gxg^{-1}$ (konjugatie met g; zie 1.2.10). Deze afbeelding induceert een permutatievoorstelling c: G $\to$ Sym(G) door $g \mapsto c_g$. Immers: voor alle $g,h,x \in G$ geldt

$$c_{gh}(x) = ghxh^{-1}g^{-1} = c_g \circ c_h(x),$$

dus c is inderdaad een groepsmorfisme. Het beeld van G onder c in Sym(G) is trouwens Int G. Met Lemma 1.2.2(ii) volgt dus nogmaals dat Int G een ondergroep van Sym(G) is (vergelijk Propositie 1.2.12).

1.5.1. DEFINITIES. De banen van Int G in G heten *konjugatieklassen* of ook wel *inklassen* van G. Twee elementen $x,y \in G$ zitten dus in dezelfde konjugatieklasse precies dan als voor zekere $g \in G$ geldt $y = gxg^{-1}$. We zeggen dan dat x en y *gekonjugeerd* zijn (onder g) in G. In de lineaire voorstellingstheorie voor groepen spelen deze inklassen een belangrijke rol. De permutatievoorstelling c is niet transitief als G niet-triviaal is, omdat $\{e\}$ zelf een konjugatieklasse is. De standondergroep G_x^c van een gegeven $x \in G$ heet *centralisator* van x in G en wordt genoteerd als $C_G(x)$. Er geldt $C_G(x) = \{g \in G \mid gx = xg\}$. Zo is $C_G(e) = G$. Voor $g \in G$ geldt in het algemeen dat $g \in C_G(g)$. De verzameling $\{g \in G \mid C_G(g) = G\}$ heet het *centrum* van G en wordt met Z(G) aangegeven. Z(G) bestaat uit die elementen van G die met alle andere elementen uit de groep kommuteren.

1.5.2. LEMMA. Z(G) *is een ondergroep van* G.

BEWIJS. $Z(G) = \text{Ker } c$. □

1.5.3. PROPOSITIE. *Laat* G *een groep zijn en laat* $K_1, K_2, \ldots, K_r$ *de konjugatieklassen van* G *zijn die meer dan één element bevatten. Kies* $x_i \in K_i$ $(i = 1,2,\ldots,r)$. *Dan geldt:*

(i) $|K_i| = |G|/|C_G(x_i)|$;

(ii) $|G| = |Z(G)| + \sum_{i=1}^{r} |C_G(x_i)|^{-1} \cdot |G|$.

BEWIJS. (i) volgt uit Stelling 1.4.8, terwijl (ii) uit (i) en sommatie over alle banen van c in G te verkrijgen is. □

1.5.4. VOORBEELD. $G = \text{Sym}(\underline{n})$. Als $n = i_1+i_2+\ldots+i_t$ met $i_1 \geq i_2 \geq \ldots \geq i_t > 0$ een partitie van n is, dan is de deelverzameling van $\text{Sym}(\underline{n})$ van alle permutaties met als disjunkte kringsplitsing een produkt van i_j-kringen $(j = 1,2,\ldots,t)$ een inklasse van $\text{Sym}(\underline{n})$. (Bedenk dat voor $g \in \text{Sym}(\underline{n})$ geldt

$$g(x_1x_2 \ldots x_m)g^{-1} = (g(x_1)g(x_2) \ldots g(x_m)).)$$

Ga na dat alle inklassen van $\text{Sym}(\underline{n})$ zo te verkrijgen zijn. In het bijzonder is het aantal inklassen van $\text{Sym}(\underline{n})$ gelijk aan het aantal partities p(n) van n. Er geldt

$$p(n) = \frac{1}{n} \sum_{k=1}^{n} \sigma(k)p(n-k),$$

met

$$p(0) = 1 \quad \text{en} \quad \sigma(k) = \sum_{d|k} d.$$

Geef zelf het bewijs hiervan. Door de betrekking ligt p(n) voor alle $n \in \mathbb{N}$ vast:

$$p(1) = 1, \quad p(2) = 2; \quad p(3) = 3; \quad p(4) = 5; \quad p(5) = 7,$$
$$p(6) = 11, \ \ldots \ .$$

Ter illustratie geven we voor elk van de 5 partities van 4 een element uit de bijbehorende inklasse en de lengte van die inklasse:

partitie	element	lengte
1 + 1 + 1 + 1	1 = (1)(2)(3)(4)	1
2 + 1 + 1	(12)	6
2 + 2	(12)(34)	3
3 + 1	(123)	8
4	(1234)	6

Bereken zelf de lengte van de 6 inklassen $\neq \{1\}$ in het geval n = 5.
Voor welke $n \in \mathbb{N}$ is $Z(\mathrm{Sym}(\underline{n}))$ van orde > 1?

1.5.5. VOORBEELD. $G = Sl_2(7)$. Het centrum van G bestaat uit de twee elementen I_2 en $z = -I_2$. De 11 matrices

$$I_2, \quad z, \quad a = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \quad a^2 = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix},$$

$$b^2 = \begin{pmatrix} 2 & 2 \\ 1 & 5 \end{pmatrix}, \quad b^3 = \begin{pmatrix} 5 & 3 \\ 5 & 6 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad zc,$$

$$d = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \quad \text{en} \quad zd$$

zijn onderling ongekonjugeerd. Dit is onmiddellijk duidelijk voor tweetallen waarvan het spoor of de orde verschillend is. Slechts voor de stellen c, d en zc, zd is een ekspliciete berekening nodig (voer die zelf uit). Bepaal ook de centralisatoren van elk van de 11 gegeven elementen.

Noemen we de lengte van de inklasse van $x \in G$ even k_x, dan volgt dankzij Propositie 1.5.3(i) uit de kennis over de centralisatoren dat k_x zich als volgt gedraagt:

x	k_x
I_2, z	1
a, a^2	56
b, b^2, b^3	42
c, zc, d, zd	24

De betreffende konjugatieklassen bevatten gezamenlijk dus

$$2\cdot 1 + 2\cdot 56 + 3\cdot 42 + 4\cdot 24 = 336 \text{ elementen.}$$

Omdat $|Sl_2(7)| = 336$ (zie Voorbeeld 1.4.6) zijn dit alle konjugatieklassen van $G = Sl_2(7)$. Er volgt ondermeer dat

$$Z(Sl_2(7)) = \{I_2, z\}.$$

Tot nu toe hebben we konjugatieklassen van elementen van een groep G bekeken. We kunnen echter ook deelverzamelingen van G konjugeren. We gaan daarbij uit van het in navolgend lemma geformuleerde principe, dat voor iedere permutatievoorstelling op gaat.

1.5.6. LEMMA. *Als G een eindige groep is, V een eindige verzameling en* $\phi: G \to \mathrm{Sym}(V)$ *een permutatievoorstelling is, dan kunnen we* ϕ *uitbreiden tot de permutatievoorstelling*

$$\phi^V: G \to \mathrm{Sym}(2^V),$$

waar 2^V *de kollektie deelverzamelingen van* V *is.*

BEWIJS. ϕ^V wordt gegeven door $g \in G$ en $M \subseteq V$ gedefinieerd door

$$\phi^V(g)M := \phi(g)(M) = \{\phi(g)m \mid m \in M\}.$$

Werk zelf de details uit. Waarom is er sprake van 'uitbreiding'? □

1.5.7. DEFINITIES. Laat M een deelverzameling van G zijn. De stabilisator $G_M^{c^V}$ van M in G bij de permutatievoorstelling c^V wordt de *normalisator* van M in G genoemd; notatie $N_G(M)$. Dus $N_G(M) = G_M^{c^V} = \{g \in G \mid gMg^{-1} = M\}$.

Uit Stelling 1.4.8 volgt dat M precies $|G|/|N_G(M)|$ gekonjugeerden heeft. Als H een ondergroep van G is, dan is H ondergroep van $N_G(H)$ en

$$c^V(g)H = gHg^{-1}$$

ondergroep van G voor elke $g \in G$ (bewijs dit laatste rechtstreeks of met gebruikmaking van de morfisme-eigenschappen uit Lemma 1.2.2 voor c_g).
De banen van c^V bestaan dus ieder óf uitsluitend uit ondergroepen óf bevatten geen enkele ondergroep van G. De groepen in de c^V-baan van $H \leq G$ zijn precies alle standondergroepen in de permutatievoorstelling 1^H van G in G/H uit Stelling 1.4.8. Bestaat de baan van H onder c^V alléén uit H zelf, dan heet H *normaaldeler* van G; notatie $H \trianglelefteq G$. Anders gezegd, H is normaaldeler als $N_G(H) = G$. In het algemeen geldt $H \trianglelefteq N_G(H)$. De normaaldelers worden in de volgende paragraaf verder besproken.

1.5.8. PROPOSITIE. *Laat* G *een groep zijn. Als* $H,K \leq G$, *dan:*
(i) $|HK| = |KH| = |K|\cdot|H|/|K\cap H|$;
(ii) $HK \leq G \iff HK = KH$;
(iii) $H \leq N_G(K) \Rightarrow HK \leq G$.
(iv) $(H \trianglelefteq G \wedge K \leq G) \Rightarrow HK \leq G$

BEWIJS. (i). De afbeelding $\mu: H\times K \to HK$, gegeven door

$$\mu(x,y) = xy \quad (x \in H,\ y \in K),$$

is surjektief. Het inverse beeld van xy is

$$\mu^{-1}(xy) = \{(xz^{-1},zy) \mid z \in H \cap K\}$$

(verifieer dit zelf) en bestaat dus uit $|H\cap K|$ elementen, ongeacht de keuze van $x \in H$ en $y \in K$. Vandaar dat het beeld van $H \times K$ onder μ kardinaliteit

$$|H\times K|/|H\cap K| = |H|\cdot|K|/|H\cap K|$$

heeft. Aan de andere kant heeft het beeld $|HK|$ elementen omdat μ surjektief is. We hebben dus de gelijkheid $|HK| = |H|\cdot|K|/|H\cap K|$.
Omdat het rechterlid symmetrisch is in H en K, is de uitdrukking ook gelijk aan $|KH|$.

(ii). Stel $HK \leq G$. Dan geldt

$$HK = \{xy \mid x \in H,\ y \in K\} = \{(xy)^{-1} \mid x \in H,\ y \in K\}$$

$$= \{y^{-1}x^{-1} \mid x \in H,\ y \in K\} = \{yx \mid x \in H,\ y \in K\} = KH.$$

Andersom, als $HK = KH$ en $z_1, z_2 \in KH$, dan zijn er $x_i \in H$ en $y_i \in K$ zodat

$$z_i = x_i y_i \quad (i = 1,2).$$

Verder zijn er $a \in H$, $b \in K$ zodat $y_1 x_2 = ab \in HK$, dus

$$z_1 z_2 = x_1 y_1 x_2 y_2 = x_1 aby_2 \in HK.$$

We konkluderen dat HK gesloten is onder vermenigvuldiging. We zijn klaar dankzij Lemma 1.1.4.

(iii). $H \leq N_G(K)$ zegt dat voor alle $h \in H$ geldt $hK = Kh$. Hieruit volgt $HK = KH$ zodat (ii) toegepast kan worden.

(iv) Dit is een direkt gevolg van (iii). □

1.5.9. VOORBEELD. Laat $G = \mathrm{Sym}(\mathbb{Z}_p^n)$ en beschouw $H = Gl_n(p)$. Als permutatiegroep op $\mathbb{Z}_p^n$ is $\mathbb{Z}_p^n$ zelf een groep met als vermenigvuldiging de vektoroptelling. $\mathbb{Z}_p^n$ kent dus ook de getrouwe linksreguliere permutatievoorstelling l van $\mathbb{Z}_p^n$ in zichzelf. Voor $a \in \mathbb{Z}_p^n$ is l_a niet anders dan translatie over a, want voor iedere $x \in \mathbb{Z}_p^n$ geldt $l_a(x) = a + x$. (Vergelijk Voorbeeld 1.3.7). De verzameling beelden van $\mathbb{Z}_p^n$ onder l in G geven we aan met A. Omdat voor alle $g \in H$ en $a \in \mathbb{Z}_p^n$ geldt $gl_a g^{-1} = l_{ga}$ is H ondergroep van $N_G(A)$. Dankzij Stelling 1.5.8(iii) leiden we hieruit af dat $AH = AGl_n(p)$ een permutatiegroep is. Deze groep heet de groep van *affiene transformaties* op $\mathbb{Z}_p^n$. Omdat $A \cap H = \{l_0\} = \{I_n\}$ volgt uit (i) van de voorgaande stelling dat de orde van $AGl_n(p)$ precies

$$p^n(p^n-1)(p^n-p) \ldots (p^n-p^{n-1})$$

is. In het bijzonder is $AGl_1(p)$ de groep van orde $p(p-1)$ bestaande uit alle permutaties van $\mathbb{Z}_p$ van de vorm

$$z \mapsto az + b \quad (a \in \mathbb{Z}_p - \{0\},\quad b \in \mathbb{Z}_p).$$

OPGAVEN BIJ §1.5.

1. (i) Schrijf de konjugatieklassen van D_4 uit Voorbeeld 1.1.12 neer.
   (ii) Geef voor ieder element in D_4 de centralisator van dat element.
   (iii) Schrijf de ondergroepen van D_4 uit in gekonjungeerden.
   (iv) Bepaal $Z(D_4)$.
   (v) Geef alle normaaldelers van D_4.

2. Als opgave 1, maar nu voor Alt(4) in plaats van D_4.

3. Laat zien dat iedere ondergroep N van de groep G bevat in Z(G) normaaldeler in G is.

*4. Laat G een groep zijn en laat $x,y \in G$. Bewijs dat $C_G(xyx^{-1}) = xC_G(y)x^{-1}$.

5. Laat x element zijn van de eindige groep G. Laat zien dat het aantal gekonjungeerden van x^n voor iedere $n \in \mathbb{N}$ een deler is van het aantal gekonjugeerden van x.

6. Gegeven is een tweetal groepen G,H. Bewijs:
   (i) $G \times H = \{(g,h) \mid g \in G, h \in H\}$ is een groep onder de vermenigvuldiging $(g_1,h_1)\cdot(g_2,h_2) = (g_1g_2,h_1h_2)$.
   (ii) $G \times \{e\}$ is normaaldeler van $G \times H$ en isomorf met G. Evenzo is $\{e\} \times H$ normaaldeler van $G \times H$ en isomorf met H.
   (iii) Als G,H eindig zijn, dan is $|G\times H| = |G|\cdot|H|$.

7. Bewijs dat:
   (i) $D_2 \cong C_2 \times C_2$
   (ii) $D_6 \cong D_3 \times C_2$
   (iii) $C_{mn} \cong C_m \times C_n$ als $ggd(m,n) = 1$.

8. Definieer op $G = \mathbb{Z}_2 \times \mathbb{Z}_3$ de vermenigvuldiging

$$(n_1,m_1)\cdot(n_2,m_2) = (n_1+n_2,(-1)^{n_2} m_1+m_2) \quad (n_i \in \mathbb{Z}_2,\ m_i \in \mathbb{Z}_3).$$

   (i) Bewijs dat G een groep vormt onder deze operatie.
   (ii) Bewijs dat $G \ncong C_2 \times C_3$.
   (iii) Geef van ieder element in G de centralisator en het aantal gekonjugeerden.

*9. Bewijs dat:
   (i) Alt(n) wordt voortgebracht door haar 3-kringen.
   (ii) Sym(n) wordt voortgebracht door (12) en (12 ... n).

*10. Laat H een permutatiegroep op een eindige verzameling $\dot{V}$ zijn. Bewijs achtereenvolgens:

(i) Voor elke $h \in H$ is de verzameling vaste punten onder h een vereniging van $C_H(h)$-banen.

(ii) Als H abels is, dan is voor elke $v \in V$ de groep H_v triviaal.

1.6. Normaaldelers en karakteristieke ondergroepen

We hebben gezien dat een morfisme $\phi: G \to G'$ van groepen aanleiding geeft tot een ondergroep Ker ϕ van G. Niet iedere ondergroep van G is als kern van een op G gedefinieerd morfisme te schrijven. Dit is als volgt in te zien: Stel $H = \text{Ker } \phi$, de kern van een groepsmorfisme $\phi: G \to G'$. Dan geldt

$$(\forall x \in H) \quad (\forall g \in G) \quad (gxg^{-1} \in H).$$

Immers, als $\phi(x) = e' \in G'$, dan geldt voor $g \in G$ ook

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(e) = e'.$$

dus $gxg^{-1} \in H$. De kern van een morfisme is dus invariant onder alle inwendige automorfismen van G. Dit betekent dat voor alle $g \in G$ geldt $c_g(H) = gHg^{-1} \subseteq H$. Omdat c_g een bijektie is komt dit overeen met $c_g(H) = H$, zodat H normaaldeler van G is (zie 1.5.7). De konklusie is dat $H \trianglelefteq G$ een noodzakelijke voorwaarde voor $H \leq G$ is opdat H de kern van een morfisme van G is. De ondergroep $\langle(12)\rangle$ van Sym(3) is derhalve voorbeeld van een ondergroep die geen kern van een morfisme zijn kan. De noodzakelijke voorwaarde van hierboven opdat H de kern van een morfisme gedefinieerd op G is, is echter wel voldoende:

1.6.1. STELLING. *Laat G een groep en H een ondergroep van G zijn. De volgende uitspraken zijn ekwivalent:*

(i) *H is normaaldeler van G;*

(ii) $(\forall g \in G)\ (gH = Hg)$;

(iii) $(\forall x \in H)\ (\forall g \in G)\ (gxg^{-1} \in H)$;

(iv) $H = \text{Ker } l^H$ *voor de permutatievoorstelling* l^H *uit* 1.4.8;

(v) *er is een groep* G' *en een morfisme* $\phi: G \to G'$ *zodat* $H = \text{Ker } \phi$.

BEWIJS. (i) $\Leftrightarrow$ (ii) verkrijgt men door op te merken dat rechtsvermenigvuldiging met g een bijektie is.

(ii) $\Longleftrightarrow$ (iii) Doe zelf.

(i) $\Rightarrow$ (iv) Als $H \leq G$, dan is H standondergroep onder 1^H van ieder element uit G/H, getuige 1.5.7. Dit impliceert dat $H = \mathrm{Ker}\ 1^H$.

(iv) $\Rightarrow$ (v) is triviaal.

(v) $\Rightarrow$ (ii) is aangetoond in de opmerking die aan de stelling vooraf gaat. □

1.6.2. KOROLLARIUM. *Als* $H \trianglelefteq G$, *dan is* G/H *voorzien van de vermenigvuldiging*

$$(g_1H)\cdot(g_2H) = g_1g_2H \quad (g_1, g_2 \in G)$$

een groep. Verder is H *kern van het epimorfisme* $\phi\colon G \to G/H$ *gedefinieerd door*

$$\phi(g) = gH \quad (g \in G).$$

BEWIJS. De vermenigvuldiging op G/H is goed gedefinieerd. Als voor $g_1, g_1', g_2, g_2' \in G$ geldt

$$g_1H = g_1'H \quad \text{en} \quad g_2H = g_2'H,$$

dan is

$$(g_1H)(g_2H) = g_1g_2H = g_1(g_2'H) = g_1Hg_2'$$

$$= g_1'Hg_2' = g_1'g_2'H = (g_1'H)(g_2'H).$$

Het één-element van G/H is $eH = H$. Verifieer zelf dat de overige axioma's voor de groep G/H gelden en dat ϕ een epimorfisme is. Tenslotte geldt

$$\mathrm{Ker}\ \phi = \{g \in G \mid gH = H\} = H. \qquad \square$$

1.6.3. KOROLLARIUM. *Voor elke groep* G *is het centrum* $Z(G)$ *normaaldeler van* G.

1.6.4. VOORBEELDEN. $\mathrm{Alt}(\underline{n}) \trianglelefteq \mathrm{Sym}(\underline{n})$. Deze ondergroep is namelijk de kern van het in 1.2.8 beschreven morfisme $\mathrm{sg}\colon \mathrm{Sym}(\underline{n}) \to \mathbb{Z}_2$.

In het algemeen geldt voor $H \leq G$ met $|G/H| = 2$ dat $H \trianglelefteq G$. Ga na waarom! Dus $C_n \trianglelefteq D_n$. Ondergroepen van grotere index zijn in het algemeen niet zonder meer normaaldeler. Alt $(\underline{4})$ heeft een normaaldeler van index 3, namelijk de vier-groep van Klein uit 1.3.3. Daarentegen heeft D_3 uit Voorbeeld 1.1.12 een ondergroep van index 3 die geen normaaldeler is, te weten $\langle a \rangle$.

1.6.5. LEMMA. G *is een groep.*

(i) *Als* $K \leq G$ *en* $H \trianglelefteq G$, *dan* $K \cap H \trianglelefteq K$;

(ii) *als* $K \leq H \leq G$ *en* $K \trianglelefteq G$, *dan* $K \trianglelefteq H$.

BEWIJS. Te beschouwen als een oefening. □

In 1.6.2 hebben we gezien dat G/H op natuurlijke wijze een groep en homomorf beeld van G is. We laten nu zien dat ieder homomorf beeld van G isomorf is met zo'n *faktorgroep*.

1.6.6. (Eerste isomorfie- en korrespondentie-) STELLING. *Laat* $\phi: G \to G'$ *een epimorfisme van eindige groepen zijn. Dan geldt*

(i) $G' \cong G/\mathrm{Ker}\ \phi$.

(ii) *Er is een éénduidige korrespondentie tussen de ondergroepen van* G *die* Ker ϕ *omvatten en de ondergroepen van* G'. *Zo'n ondergroep* H *van* G *korrespondeert met zijn beeld* $H' = \phi(H)$ *in* G'. *Verder is* $H \trianglelefteq G$ *precies dan als* $H' \trianglelefteq G'$.

BEWIJS. (i) Het epimorfisme ϕ induceert een afbeelding $\bar{\phi}$: G/Ker $\phi \to$ G' door $\bar{\phi}(g\ \mathrm{Ker}\ \phi) = \phi(g)$. Ga zelf na dat deze afbeelding goed gedefinieerd is. $\bar{\phi}$ is een morfisme: als $g,h \in G$, dan is in verband met het feit dat Ker ϕ normaaldeler is,

$$\bar{\phi}(g\ \mathrm{Ker}\ \phi \cdot h\ \mathrm{Ker}\ \phi) = \bar{\phi}(gh\ \mathrm{Ker}\ \phi) = \phi(gh) = \phi(g)\phi(h)$$

$$= \bar{\phi}(g\ \mathrm{Ker}\ \phi)\bar{\phi}(h\ \mathrm{Ker}\ \phi).$$

Surjektiviteit van $\bar{\phi}$ volgt uit die van ϕ. Tenslotte is $\bar{\phi}$ injektief, want als $\bar{\phi}(g\ \mathrm{Ker}\ \phi) = e' \in G'$, dan is $\phi(g) = e'$, dus $g \in \mathrm{Ker}\ \phi$, zodat $g\ \mathrm{Ker}\ \phi = \mathrm{Ker}\ \phi$.

(ii). Als $H' \leq G'$, dan omvat $\phi^{-1}(H')$ de kern van ϕ omdat $e' \in H'$. Als verder $H \leq G$ met $\phi(H) = H'$ en $\mathrm{Ker}\ \phi \leq H$, dan geldt $H \leq \phi^{-1}(H')$ en is er voor $x \in \phi^{-1}(H')$ een $h \in H$ zo dat $\phi(x) = \phi(h)$. Er volgt $xh^{-1} \in \mathrm{Ker}\ \phi$, dus $x = (xh^{-1})h \in (\mathrm{Ker}\ \phi)H = H$. De konklusie is dat $H = \phi^{-1}(H')$.

We hebben aangetoond dat de korrespondentie $H \to \phi(H)$ injektief is op de verzameling ondergroepen die Ker ϕ omvatten. Doe de rest zelf. □

1.6.7. VOORBEELDEN. $Q/C_4 \cong C_2$ waar Q de *quaterniongroep* uit Opgave 1.1.9 is.

$Gl_n(k)/Sl_n(k) \cong Gl_1(K)$;

$D_n/C_n \cong Sym(\underline{n})/Alt(\underline{n}) \cong C_2$;

$Alt(\underline{4})/V \cong C_3$, waar $V = \{1,(12)(34),(13)(24),(14)(23)\}$;

$AGl_1(p)/A \cong Gl_1(p)$ met A als in 1.5.9;

$Sl_2(3)/\{\pm I_2\} \cong Alt(\underline{4})$;

$Sl_2(2) \cong Sym(\underline{3})$.

Van elke eindige groep G zijn {e} en G normaaldelers.

1.6.8. DEFINITIE. Een eindige groep G heet *enkelvoudig* als {e} en G de enige normaaldelers van G zijn. Een echte normaaldeler H van G heet *maksimale normaaldeler* als er behalve H geen echte normaaldelers zijn die H omvatten. Ga na dat G tenminste één maksimale normaaldeler heeft, maar mogelijk meerdere.

1.6.9. KOROLLARIUM. *In een groep* G *is* H *een maksimale normaaldeler dan en slechts dan als* G/H *een niettriviale enkelvoudige groep is.*

1.6.10. VOORBEELDEN. C_p (p priem) is enkelvoudig, want C_p kent geen andere ondergroepen dan {e} en C_p. Ook $Alt(\underline{n})$ is enkelvoudig als $n \geq 5$. Dit kan bewezen worden uit het ongerijmde door aan te tonen dat elke niet-triviale normaaldeler een 3-cykel omvat en dat $Alt(\underline{n})$ voortgebracht wordt door de deelverzameling van al haar 3-cykels. Later zullen we echter een ander bewijs geven. Tenslotte vermelden we dat $Sl_n(K)/Z(Sl_n(K))$ enkelvoudig is als K een eindig lichaam is en $n \in \mathbb{N}$ zodanig dat $n > 2$, of $n = 2$ en $|K| > 3$. Ook hier komen we later op terug.

In de rest van deze paragraaf laten we zien dat abelse homomorfe beelden van een gegeven groep korresponderen met normaaldelers die een bepaalde normaaldeler omvatten. We gaan daartoe uit van een morfisme $\phi: G \to G'$ van een groep G naar een andere groep G'.

Als G' abels is, geldt voor iedere $g,h \in G$ dat

$$\phi(ghg^{-1}h^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1}$$

$$= \phi(g)\phi(g)^{-1}\phi(h)\phi(h)^{-1} = e' \in G'.$$

Er volgt dat $A = \{ghg^{-1}h^{-1} \mid g,h \in G\}$ in Ker ϕ bevat is.

Andersom, als deze verzameling A deel van Ker ϕ is en $a,b \in G'$ willekeurige beelden zijn, dan zijn er $g,h \in G$ zodat

$$\phi(g) = a \quad \text{en} \quad \phi(h) = b,$$

terwijl

$$aba^{-1}b^{-1} = \phi(ghg^{-1}h^{-1}) = e'.$$

Hieruit volgt ab = ba. We konkluderen dat G' abels is.

1.6.11. DEFINITIES. De elementen van de verzameling A heten *kommutatoren* van G. Een kommutator is dus een element van G van de vorm

$$ghg^{-1}h^{-1}.$$

Het één-element $e = e \cdot ee^{-1}e^{-1}$ is een kommutator, maar het produkt van twee kommutatoren hoeft in het algemeen geen kommutator te zijn. Met andere woorden, er zijn groepen G waarvoor de verzameling A van kommutatoren geen ondergroep van G is. De door A voortgebrachte ondergroep van G heet *kommutatorgroep* van G en wordt met D(G) aangegeven.

1.6.12. LEMMA. *Laat G een eindige groep zijn. Er geldt:*

(i) $D(G) \trianglelefteq G$;

(ii) $D(G) = \{e\} \iff G$ *is abels*;

(iii) als $H \trianglelefteq G$, *dan* [G/H *abels* $\iff D(G) \leq H$];

(iv) *voor* $H \leq G$ *geldt* [$D(G) \leq H \Rightarrow H \trianglelefteq G$].

BEWIJS. (i) volgt uit de invariantie van A onder Int(G). Werk zelf de details uit.

(ii) wordt aan U overgelaten.

(iii). Laat $H \trianglelefteq G$. De implikatie " $\Rightarrow$ " volgt uit de opmerkingen, voorafgaande aan 1.6.11. Ten aanzien van " $\Leftarrow$ " merken we op dat uit $D(G) \leq H$

volgt dat G/H homomorf beeld van de abelse groep G/D(G) is. Hieruit blijkt dat G/H ook abels is.
(iv). Via $H/D(G) \trianglelefteq G/D(G)$ en toepassing van Stelling 1.6.6(ii) verkrijgt men dat H normaaldeler van G is. □

1.6.13. VOORBEELDEN. Laat V als in 1.6.7 gedefinieerd zijn. Dan is

$$D(\mathrm{Sym}(\underline{n})) = \mathrm{Alt}(\underline{n}); \quad D(\mathrm{Alt}(\underline{4})) = V; \quad D(V) = \{e\}.$$

Omdat $D(D_n) = C_n$, geldt $D(D(D_n)) = \{e\}$.

1.6.14. VOORBEELD. Groep van isometrieën van de kubus. Notatie als in 1.4.11. We berekenen nogmaals de orde van G, de groep van alle isometrieën die de kubus in zichzelf overvoeren, maar nu met behulp van Stelling 1.6.6. De kubus telt 4 lichaamsdiagonalen: één door 1 en 7 die we kortheidshalve met $\overline{17}$ aangeven en op dezelfde wijze genoteerd $\overline{28}$ $\overline{35}$ $\overline{46}$. Een isometrie die de kubus in zichzelf overvoert, voert de 4 lichaamsdiagonalen ook in elkaar over. Dit geeft een permutatievoorstelling

$$\pi: G \to \mathrm{Sym}\{\overline{17},\overline{28},\overline{35},\overline{46}\}.$$

Ga zelf na dat π surjektief is en dat $|\mathrm{Ker}\ \pi| = 2$. Via Stelling 1.6.6 komen we tot

$$\tfrac{1}{2}|G| = |\mathrm{Sym}\{\overline{17},\overline{28},\overline{35},\overline{46}\}| = 24 \quad \text{en} \quad |G| = 48.$$

Ga zelf na dat $Z(G) = \mathrm{Ker}\ \pi$ en bereken $|D(G)|$.

We komen nu toe aan een bijzondere klasse normaaldelers.

1.6.15. DEFINITIE. Een ondergroep N van een gegeven groep G heet *karakteristiek* in G als voor iedere $\alpha \in \mathrm{Aut}(G)$ geldt $\alpha(N) = N$. Notatie $N \trianglelefteq\!\!\trianglelefteq G$, of als $N \neq G$ ook $N \triangleleft\!\triangleleft G$. In elke groep G zijn $\{1\}$ en G karakteristieke ondergroepen. Als dit de enige zijn, dan heet G *karakteristieke enkelvoudig*.

Het volgende lemma geeft aan dat karakteristieke ondergroepen van nut kunnen zijn bij het opsporen van normaaldelers.

1.6.16. LEMMA. *Laat G een eindige ondergroep zijn en K, H ondergroepen van G. Dan geldt*
(i) $K \trianglelefteq\!\!\trianglelefteq G \Rightarrow K \trianglelefteq G$
(ii) $K \trianglelefteq\!\!\trianglelefteq H \trianglelefteq G \Rightarrow K \trianglelefteq\!\!\trianglelefteq G$.

BEWIJS.

(i) Konjugatie met een element uit G is een automorfisme van G en laat K dus invariant.

(ii) Konjugatie met een element uit G laat H invariant, induceert dus een automorfisme van H, zodat K daaronder invariant blijft. □

1.6.17. VOORBEELDEN. Ga na dat in elke groep G zowel Z(G) als D(G) karakteristieke ondergroepen zijn. Ook de doorsnede van alle maximale ondergroepen is een karakteristieke ondergroep (de zogenaamde Frattini-groep, we komen hier in hoofdstuk 5 op terug).
Een minimale normaaldeler van een groep G is een niet-triviale normaaldeler die geen andere niet-triviale normaaldelers van G echt omvat; vanwege 1.6.16(ii) is een minimale normaaldeler karakteristiek enkelvoudig. De viergroep van Klein is een minimale normaaldeler van Sym(4). Karakteristiek enkelvoudige groepen zijn dus niet noodzakelijk enkelvoudig.

In opgave 1.8.12 komt een stelling aan de orde die het begrip karakteristiek enkelvoudig aan het begrip enkelvoudig relateert.

OPGAVEN BIJ §1.6

1. Bewijs:
   (i) Als G een eindige groep is en als G/Z(G) cyklisch is, dan is G abels.
   (ii) Iedere abelse enkelvoudige groep G is isomorf met C_p voor zeker priemgetal p.

2. G is een groep en H,K zijn ondergroepen van G.
   (i) Weerleg aan de hand van een tegenvoorbeeld de uitspraak "$H \trianglelefteq K \trianglelefteq G$, dan $H \trianglelefteq G$".
   (ii) Bewijs; $K \triangleleft H \triangleleft G \Rightarrow K \triangleleft G$.
   (iii) Bewijs dat de uitspraak in (i) waar is als K cyklisch is.
   (iv) Laat zien dat uit $H \trianglelefteq G$ en $|H| = 2$ volgt $H \trianglelefteq Z(G)$.

3. Bepaal alle minimale normaaldelers van Sym(4) en van D_n.

*4. (i) Bewijs dat Int G isomorf is met G/Z(G).
   (ii) Bewijs: Int $G \trianglelefteq$ Aut G.

*5. Kies een symbool $\omega \notin \mathbb{Z}_2$. Laat K de verzameling zijn die bestaat uit de 4 elementen $a + b\omega$ $(a,b \in \mathbb{Z}_2)$. We voorzien K van de optelling

$$(a+b\omega) + (c+d\omega) = (a+c) + (b+d)\omega,$$

en de vermenigvuldiging

$$(a+b\omega)(c+d\omega) = (ac+bd) + (bc+bd+ad)\omega.$$

(i) Laat zien dat K met de gegeven optelling en vermenigvuldiging een lichaam is.

De groep $AGl_n(K)$ wordt gedefinieerd analoog aan $AGl_n(\mathbb{Z}_p)$ uit Voorbeeld 1.5.9 van het diktaat.

(ii) Bereken de ordes van $Gl_n(K)$, $AGl_n(K)$, $Sl_n(K)$, $Z(Gl_n(K))$ en $Z(Sl_n(K))$.

(iii) Is $AGl_1(K)$ isomorf met $Alt(\underline{4})$? Met D_6? Motiveer uw antwoord.

(iv) Bewijs: $Sl_2(K) \cong Alt(\underline{5})$.

6. Laat op $G = \mathbb{Z}_p^4$ de vermenigvuldiging $\cdot$ gegeven zijn door:

$$(a_1,a_2,a_3,a_4) \cdot (b_1,b_2,b_3,b_4) =$$
$$(a_1+b_1+pa_3b_1, a_2+b_2+pa_4b_2, a_3+b_3+pa_3b_2, a_4+b_4+pa_2b_1).$$

(i) Bewijs dat G met deze vermenigvuldiging een groep is.

(ii) Laat zien dat D(G) meer dan de kommutatoren van G alléén bevat.

7. U mag in deze opgave gebruiken dat $Alt(\underline{n})$ enkelvoudig is als $n > 4$.

(i) Bewijs dat $Alt(\underline{n})$ voor $n > 4$ geen echte ondergroep van index $< n$ bezit.

(ii) Bepaal een getrouwe transitieve permutatievoorstelling van $Alt(\underline{5})$ van graad 6. Beargumenteer uw antwoord.

(iii) Wat zijn de verschillende ordes van echte ondergroepen van $Alt(\underline{5})$? Schrijf voor elk van deze ordes alle elementen uit een ondergroep van die orde op.

8. Bewijs dat iedere niet-abelse groep van orde 8 òf isomorf is met Q uit Opgave 9 van §1.1 òf met D_4 (let wel:

$$Q = \{\pm I_2, \pm i\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \pm i\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\}).$$

Aanwijzing: gebruik Opgave 3 van §1.1.

*9. Laat $n \in \mathbb{N}$, $n \geq 2$ en schrijf $\xi = \exp(\pi i/n)$. De groep Q_n is de ondergroep van $Sl_2(\mathbb{C})$ voortgebracht door

$$u = \begin{pmatrix}\xi & 0\\ 0 & \xi^{-1}\end{pmatrix} \quad \text{en} \quad v = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Bewijs achtereenvolgens:

(i) $\langle u \rangle \trianglelefteq Q_n$;

(ii) $Q_n = \langle u \rangle\langle v \rangle$;

(iii) $Q_n/\langle u \rangle \cong C_2$;

(iv) $|Z(Q_n)| = 2$;

(v) $Q_n/Z(Q_n) \cong D_n$ de diëdergroep van orde 2n uit Voorbeeld 1.1.12;

(vi) $Q_2 \cong Q$ uit Opgave 1.1.9;

(vii) $D(D(Q_n)) = \{e\}$.

De groep Q_n wordt wel de *gegeneraliseerde quaterniongroep* van orde 4n genoemd.

*10. Laat $H \leq G$. Bewijs dat de kern K van de permutatievoorstelling

$1^H: G \to \mathrm{Sym}(G/H)$

de grootste normaaldeler van G, bevat in K, is.

(Aanwijzing: $K = \bigcap_{g \in G} gHg^{-1}$.)

*11. Bewijs: $|G| = 6 \Rightarrow G \cong C_6$ of $G \cong \mathrm{Sym}(\underline{3})$.

*12. Bewijs achtereenvolgens voor elk priemgetal p:

(i) $|G| = p^n$ $(n \in \mathbb{N}) \Rightarrow Z(G) \neq 1$.

(Aanwijzing: bekijk de banen onder c_g in G.)

(ii) $|G| = p^2 \Rightarrow$ G is abels.

(iii) $|G| = p^2 \Rightarrow G \cong C_{p^2}$ of $G \cong C_p \times C_p$ (dat wil zeggen de optelgroep van de 2-dimensionale vektorruimte $\mathbb{Z}_p^2$).

13. $G = \mathrm{Sl}_2(p)$ voor een priemgetal p.

(i) Bewijs dat $|Z(\mathrm{Sl}_2(p))| = 2$ als $p \geq 3$.

(ii) Bewijs dat voor $p \geq 3$ er geen echte normaaldeler H van G is die $Z(\mathrm{Sl}_2(p))$ omvat zowel als een element van de vorm $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ voor zekere $c \neq 0$.

(iii) Bewijs dat $\mathrm{Sl}_2(p)/Z(\mathrm{Sl}_2(p))$ enkelvoudig is voor $p \geq 5$.

De groep uit (iii) wordt in het algemeen aangegeven met $\mathrm{PSl}_2(p)$ en is op te vatten als permutatiegroep op de verzameling lijnen door 0 in $\mathbb{Z}_p \times \mathbb{Z}_p$.

(iv) Ga na dat voor $p > 5$ geen der groepen $\mathrm{PSl}_2(p)$ isomorf is met een der groepen $\mathrm{Alt}(\underline{n})$.

(v) Bewijs dat $\mathrm{PSl}_2(5) \cong \mathrm{Alt}(\underline{5})$.

(Aanwijzing: $\mathrm{PSl}_2(5)$ heeft een getrouwe transitieve permutatievoorstelling van graad 6; gebruik Opgave 7 om hetzelfde voor $\mathrm{Alt}(\underline{5})$ te bewijzen; vergelijk beide permutatiegroepen.)

14. Bepaal $Z(AGl_1(p))$ en $D(AGl_1(p))$.

15. Bewijs: Als een groep G een ondergroep H van index n heeft, dan omvat H een normaaldeler K (van G) zodat $|G/K|$ een deler van n! is.
(Aanwijzing: Neem K als in Opgave 10 van §1.6.)

*16. Voor $H \leq G$ geven we met $C_G(H)$ de groep $\bigcap_{h \in H} C_G(h)$ aan.
Bewijs dat $N_G(H)/C_G(H)$ isomorf is met een ondergroep van Aut(H).

17. Bewijs:
(i) $Aut(Sym(\underline{4})) = Int(Sym(\underline{4})) \cong Sym(\underline{4})$.
(ii) Er bestaat geen eindige groep G zodanig dat $D(G) = Sym(\underline{4})$.

18. Laat zien dat als G een groep is zodat $|D(G)| = m$, de lengte van de konjugatieklassen in G hoogstens m is.

*19. Laat m een deler zijn van n. Bewijs dat er precies één ondergroep van C_n is van orde m. Konkludeer dat elke ondergroep van C_n karakteristiek is.

20. Bewijs dat elke ondergroep van een abelse groep normaaldeler is. Geef een voorbeeld waaruit blijkt dat niet elke ondergroep van een abelse groep karakteristiek is.

1.7. Isomorfiestellingen

Met de eerste isomorfiestelling hebben wij in 1.6.6 al kennis gemaakt. Hier volgen de derde en de tweede.

1.7.1. (Derde isomorfie) STELLING. *Laat* G *een eindige groep zijn en laat* K,H *normaaldelers van* G *zijn met* $K \leq H$. *Dan is*

$$G/H \cong (G/K) / (H/K).$$

BEWIJS. In Lemma 1.6.5(ii) hebben we al gezien dat $K \trianglelefteq H$. Uit Stelling 1.6.6(ii) volgt dat $H/K \trianglelefteq G/K$, zodat $(G/K) / (H/K)$ inderdaad een groep is. Definieer nu

$$\phi: G/H \to (G/K) / (H/K)$$

door

$$\phi(gH) = gK(H/K) \quad (g \in G).$$

Bedenk dat ϕ goed gedefinieerd is, want als $g_1, g_2 \in G$ met $g_1H = g_2H$, dan is $g_1 g_2^{-1} \in H$ krachtens Lemma 1.4.7, dus

$$g_1K(g_2K)^{-1} = g_1g_2^{-1}K \in H/K$$

en (weer vanwege Lemma 1.4.7)

$$g_1K(H/K) = g_2K(H/K).$$

Bewijs zelf dat ϕ een epimorfisme is. Ker $\phi = \{e\}$ volgt tenslotte uit de volgende reeks implikaties voor $g \in G$:

$$gK(H/K) = H/K \Rightarrow gK \in H/K \Rightarrow (\exists h \in H)(gK = hK) \Rightarrow$$
$$(\exists h \in H)(gH = hH) \Rightarrow g \in H \Rightarrow gH = H. \qquad \square$$

1.7.2. OPMERKING. Probeer zelf de stelling eens te bewijzen met behulp van de eerste isomorfiestelling door de afbeelding ψ: $G/K \to G/H$, gedefinieerd door

$$\psi(gK) = gH \quad (g \in G),$$

te beschouwen.

1.7.3. KOROLLARIUM. *Laat* G *een groep zijn met een normaaldeler* H *die* D(G) *omvat. Dan is* G/H *een faktorgroep van* G/D(G).

BEWIJS. Neem K = D(G) in de stelling. $\square$

1.7.4. VOORBEELD. Schrijf $G = D_4$. Laat

$$H = \{1, c_4^2, ac_4^2, a\}$$

en

$$K = \{1, c_4^2\}.$$

Ga zelf na dat H en K normaaldelers van D_4 zijn. G/K bestaat uit de nevenklassen K, c_4K, aK, ac_4K, terwijl H/K bestaat uit de nevenklassen K en aK. De groep (G/K) / (H/K) bestaat dus uit de nevenklassen

$$K(H/K) = \{K, aK\} \quad \text{en} \quad c_4K(H/K) = \{c_4K, ac_4K\}.$$

Uit

$$c_4H(H/K)c_4K(H/K) = c_4^2K(H/K) = K(H/K)$$

blijkt (G/K) / (H/K) inderdaad isomorf met C_2 te zijn, zoals ook uit $G/H \cong C_2$ via Stelling 1.7.1 afgeleid kan worden.

Tenslotte bewijzen we nog de

1.7.5. (Tweede isomorfie) STELLING. *Laat* G *een groep zijn èn laat* K,H *een tweetal ondergroepen van* G *zijn met* $K \trianglelefteq G$. *Dan geldt* $HK/K \cong H/H \cap K$.

BEWIJS. Volgens Stelling 1.5.8 is HK een ondergroep van G, terwijl naar Lemma 1.6.5 geldt $K \trianglelefteq HK$. Beschouw de afbeelding $\phi: H \to HK/K$, gedefinieerd door $\phi(h) = hK$. Bewijs zelf dat deze afbeelding een epimorfisme is met Ker $\phi = H \cap K$. Uit de eerste isomorfiestelling volgt dan dat $H/H \cap K$ en HK/K isomorf zijn. □

1.7.6. VOORBEELD. $G = \mathrm{Sym}(\underline{n})$ en $K = \mathrm{Alt}(\underline{n})$. Notatie als in 1.5.4. We willen de inklassen van $\mathrm{Alt}(\underline{n})$ bepalen. $\mathrm{Alt}(\underline{n})$ bestaat uit hele klassen van G en wel die waarvoor de overeenkomstige partitie $i_1 + \ldots + i_t = n$ voldoet aan

$$\sum_{j=1}^{t} i_j = t \bmod 2.$$

Een inklasse van $\mathrm{Sym}(\underline{n})$ binnen $\mathrm{Alt}(\underline{n})$ is ofwel in z'n geheel een inklasse van $\mathrm{Alt}(\underline{n})$ ofwel valt uiteen in twee inklassen van $\mathrm{Alt}(\underline{n})$ met ieder even-veel elementen. Dit laatste geval doet zich precies dan voor als $i_1, i_2, \ldots, i_t$ alle oneven en verschillend zijn.
Toelichting: Voor elke $g \in K$ geldt

$$C_K(g) = C_G(g) \cap \mathrm{Alt}(\underline{n}),$$

dus met de voorgaande stelling: $C_G(g)/C_K(g) \cong C_G(g) \cdot K/K$.
Deze laatste faktorgroep is gelijk aan $G/K \cong C_2$, respektievelijk $K/K \cong \{1\}$, al naar gelang er een oneven permutatie met g kommuteert of niet.

OPGAVEN BIJ §1.7.

1. Ga na wat Stelling 1.7.1 inhoudt in het geval dat

$$G = \mathrm{Sym}(\underline{4}), \quad H = \mathrm{Alt}(\underline{4}) \quad \text{en} \quad K = D(\mathrm{Alt}(\underline{4})).$$

2. Ga na wat Stelling 1.7.5 inhoudt in het geval dat

$$G = \mathrm{AGl}_n(p), \quad H = \mathrm{Sl}_n(p) \quad \text{en} \quad K = A.$$

3. (i) Bewijs: Als G een eindige groep is en K,H zijn normaaldelers van G, dan is

$$(G/H) \,/\, (HK/H) \cong (G/K) \,/\, (HK/K).$$

(ii) Laat zien dat Stelling 1.7.1 een gevolg van (i) is.

1.8. Produkten

Met behulp van produkten van groepen is het mogelijk om, uitgaande van een gegeven stel groepen, een grotere groep te konstrueren. In deze paragraaf voeren we drie soorten van produkt van eindige groepen in, te weten het direkte produkt, het semidirekte produkt en het kransprodukt.

1.8.1. DEFINITIE. Laat G een groep zijn en laat $G_1,G_2,\ldots,G_m$ een stel ondergroepen van G zijn. G heet *direkt produkt* van $G_1,\ldots,G_m$ als

(i) $G_i \trianglelefteq G$ voor alle $i \in \underline{m}$;

(ii) $(\forall g \in G)(\exists!\,(g_1,\ldots,g_m) \in G_1 \times \ldots \times G_m)(g = g_1 \cdot g_2 \cdot \ldots \cdot g_m)$.

In deze situatie is $G_i \cap G_j = \{e\}$ voor $i \neq j$; want als $g \in G_i \cap G_j$, dan is zowel

$$(e,\ldots,e,g,e,\ldots,e) \quad \text{als} \quad (e,\ldots,e,g,e,\ldots,e)$$
$$\uparrow \qquad\qquad\qquad\qquad \uparrow$$
$$\text{i-de plaats} \qquad\qquad\qquad \text{j-de plaats}$$

een m-tupel in $G_1 \times G_2 \times \ldots \times G_m$ als bedoeld in (ii), zodat uit de uniciteit van zo'n tupel volgt dat $i = j$ of $g = e$. Deze eigenschap impliceert dat de elementen van G_i en G_j paarsgewijs verwisselbaar zijn.

1.8.2. LEMMA. *Als G een groep met normaaldelers G_1,G_2 is zodat $G_1 \cap G_2 = \{e\}$, dan geldt*

$$(\forall g_1 \in G_1)(\forall g_2 \in G_2)\ (g_1g_2 = g_2g_1).$$

BEWIJS. Komt er op neer dat voor gegeven $g_1 \in G_1$ en $g_2 \in G_2$ geldt

$$g_1g_2g_1^{-1}g_2^{-1} \in G_1 \cap G_2 = \{e\}. \qquad \square$$

Als G direkt produkt van $G_1,G_2,\ldots,G_m$ is, zijn de elementen uit verschillende faktoren G_i dus paarsgewijs verwisselbaar. We laten nu zien hoe G precies uit de groepen G_i opgebouwd kan worden.

1.8.3. DEFINITIE. Laat $G_1,G_2,\ldots,G_m$ een stel groepen zijn. Het *abstrakte direkte produkt* van $G_1,G_2,\ldots,G_m$ is de verzameling $G_1 \times G_2 \times \ldots \times G_m$ voorzien van de vermenigvuldiging

$$(g_1,g_2,\ldots,g_m)\cdot(h_1,h_2,\ldots,h_m) = (g_1h_1,g_2h_2,\ldots,g_mh_m)$$

$$\text{voor } g_i,h_i \in G_i.$$

Deze vermenigvuldiging is associatief en heeft één-element $(e_1,e_2,\ldots,e_m)$ waar e_i één-element van G_i, terwijl de inverse van

$$(g_1,g_2,\ldots,g_m) \in G_1 \times G_2 \times \ldots \times G_m$$

het element $(g_1^{-1},g_2^{-1},\ldots,g_m^{-1})$ is. Het abstrakte direkte produkt is dus een groep. Ga na dat deze groep direkt produkt van

$$G_1 \times \{e_2\} \times \ldots \times \{e_m\},\{e_1\} \times G_2 \times \{e_3\} \times \ldots \times \{e_m\},\ldots,$$

$$\{e_1\} \times \ldots \times \{e_{m-1}\} \times G_m$$

is. Andersom:

1.8.4. STELLING. *Als G het direkte produkt van* $G_1,G_2,\ldots,G_m$ *is voor zekere* $G_i \trianglelefteq G$, *dan geldt*

$$G \cong G_1 \times G_2 \times \ldots \times G_m.$$

BEWIJS. De afbeelding α: $G_1 \times G_2 \times \ldots \times G_m \to G$, gedefinieerd door

$$\alpha(g_1,g_2,\ldots,g_m) = g_1g_2 \ldots g_m \quad (g_i \in G_i),$$

is een bijektie vanwege axioma (ii) voor direkte produkten. Maar α is ook een morfisme, want voor

$$(g_1,g_2,\ldots,g_m),(h_1,h_2,\ldots,h_m) \in G_1 \times G_2 \times \ldots \times G_m$$

geldt dankzij Lemma 1.8.2. dat

$$\alpha(g_1,g_2,\ldots,g_m)\cdot\alpha(h_1,h_2,\ldots,h_m) =$$

$$g_1g_2 \cdots g_mh_1h_2 \cdots h_m = (g_1h_1)(g_2h_2) \cdots (g_mh_m) =$$

$$\alpha(g_1h_1,g_2h_2,\ldots,g_mh_m).$$

Er volgt dat α een isomorfisme is. □

1.8.5. OPMERKINGEN. Laat G als in Stelling 1.8.4 gegeven zijn.

- Vaak wordt G door middel van α met $G_1 \times G_2 \times \ldots \times G_m$ geïdentificeerd: $G = G_1 \times G_2 \times \ldots \times G_m$.
- De orde van G is $\prod_{i=1}^{m} |G_i|$.
- G is kommutatief dan en slechts dan als iedere G_i kommutatief is.
- Als er eindige verzamelingen $V_1,V_2,\ldots,V_m$ zijn zodat $V_i \cap V_j = \emptyset$ voor $i \neq j$ en zodat $G_i \leq \mathrm{Sym}(V_i)$, dan is $G \leq \mathrm{Sym}(\bigcup_{i=1}^{m} V_i)$ middels het voorschrift $gx = g_ix$ als $x \in V_i$ $(i \in \underline{m})$ voor $g \in G$. Aldus heeft G een getrouwe permutatievoorstelling van graad $\sum_{i=1}^{m} |V_i|$, die slechts transitief is als $m = 1$.

1.8.6. VOORBEELDEN. De groep van isometrieën van de kubus (zie 1.4.11) is isomorf met $\mathrm{Sym}(\underline{4}) \times C_2$. De ondergroep van $\mathrm{Gl}_n(K)$ bestaande uit diagonaalmatrices is isomorf met

$$\underbrace{K^* \times K^* \times \ldots \times K^*}_{n \text{ maal}}, \text{ waar } K^* = (K - \{0\},\cdot,1).$$

De viergroep van Klein D_2 is isomorf met $C_2 \times C_2$. Hoewel D_n voor $n \geq 3$ een normaaldeler C_n en een ondergroep $K \cong C_2$ heeft zodat $C_n \cap K = \{e\}$, is D_n niet isomorf met $C_n \times C_2$ (deze laatste groep is immers abels). Deze situatie vinden we terug in de semi-direkte produkten.

1.8.7. DEFINITIES. Laat G een groep zijn en laat H,K een tweetal ondergroepen van G zijn zodat $H \trianglelefteq G$. De groep G heet *semi-direkt produkt* van H en K als

(i) $G = HK$;

(ii) $H \cap K = \{e\}$.

In dit geval levert konjugatie een morfisme $c: K \to \mathrm{Aut}(H)$, gedefinieerd als in 1.2.10. We kunnen ook omgekeerd te werk gaan. Stel dat twee groepen H,K gegeven zijn alsmede een morfisme $\alpha: K \to \mathrm{Aut}(H)$, dan is de verzameling $H \times K$ voorzien van de vermenigvuldiging

$$(h_1,k_1)(h_2,k_2) = (h_1(\alpha(k_1)h_2),k_1k_2) \qquad (h_i \in H,\ k_i \in K)$$

een groep.

De vermenigvuldiging is namelijk associatief:

$$(h_1,k_1)((h_2,k_2)(h_3,k_3)) = (h_1,k_1)(h_2\alpha(k_2)h_3,k_2k_3) =$$

$$(h_1(\alpha(k_1)(h_2\alpha(k_2)h_3)),k_1k_2k_3) = (h_1\alpha(k_1)h_2\alpha(k_1k_2)h_3,k_1k_2k_3) =$$

$$(h_1\alpha(k_1)h_2,k_1k_2)(h_3,k_3) = ((h_1,k_1)(h_2,k_2))(h_3,k_3).$$

Verder is het één-element (e,e), waar e het één-element van H zowel als van K aanduidt, terwijl de inverse van $(h,k) \in H \times K$ onder de gegeven vermenigvuldiging $(\alpha(k^{-1})h^{-1},k^{-1})$ is. Aldus is een groep gedefinieerd die we het *abstrakte α-semi-direkte produkt* van H en K noemen en die we ter onderscheiding met de groep $H \times K$ noteren als $H \underset{\alpha}{\rtimes} K$. Merk op dat $H \underset{\alpha}{\rtimes} K$ semi-direkt produkt is van $H \times \{e\}$ en $\{e\} \times K$. Andersom:

1.8.8. STELLING. *Laat* G *een groep zijn en* $H \trianglelefteq G$. *Als* $K \leq G$ *zodanig dat* G *semi-direkt produkt van* H *en* K *is, dan is* $G \cong H \underset{c}{\rtimes} K$, *waar* $c: K \to \mathrm{Aut}(H)$ *voor* $k \in K$ *gegeven is door* $c \mapsto c_k$, *konjugatie met* $k \in K$.

BEWIJS. De afbeelding $\phi: H \underset{c}{\rtimes} K \to G$ gedefinieerd door $\phi(h,k) = hk$ is een morfisme: voor $h_1,h_2 \in H$ en $k_1,k_2 \in H$ geldt

$$\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1k_1h_2k_1^{-1},k_1k_2) =$$

$$h_1k_1h_2k_2 = \phi(h_1,k_1)\cdot\phi(h_2,k_2).$$

Bovendien is ϕ injektief vanwege axioma (ii) en surjektief vanwege axioma (i) voor semi-direkte produkten; geef zelf de details aan. □

1.8.9. OPMERKINGEN.

- Als α uit de kontekst duidelijk is, wordt vaak $H \rtimes K$ in plaats van $H \underset{\alpha}{\rtimes} K$ geschreven. Ook schrijven we wel $K \ltimes H = H \rtimes K$.
- De orde van $H \rtimes K$ is $|H|\cdot|K|$.
- $H \rtimes K$ hoeft niet kommutatief te zijn als H en K kommutatief zijn, getuige het eerstvolgende voorbeeld.
- Er zijn groepen G met normale ondergroepen H waarvoor geen K bestaat zodat G semi-direkt produkt van H en K is. Zie de *gegeneraliseerde quaterniongroepen* in Opgave 1.8.5.

1.8.10. VOORBEELDEN. $D_n = C_n \rtimes_c C_2$, waar $c: C_2 \to \mathrm{Aut}(C_n)$ vastligt door de formule * in Voorbeeld 1.1.12. Uitwerking hiervan levert

$$c_a(c_n^j) = ac_n^j a^{-1} = c_n^{-j} \quad (j \in \underline{n}).$$

Als $n = 2$, dan is c_a de identiteit op C_n zodat inderdaad $D_2 = C_2 \times C_2$. Omdat $\mathrm{Sym}(\underline{3}) \cong D_3$ en $\mathrm{Sym}(\underline{4}) = D_2 \rtimes \mathrm{Sym}(\underline{3})$ volgt

$$\mathrm{Sym}(\underline{4}) = (C_2 \times C_2) \rtimes (C_3 \rtimes C_2).$$

Anderzijds volgt uit $\mathrm{Sym}(\underline{n}) = \mathrm{Alt}(\underline{n}) \rtimes C_2$ en $\mathrm{Alt}(\underline{4}) = D_2 \rtimes C_3$ dat

$$\mathrm{Sym}(\underline{4}) = ((C_2 \times C_2) \rtimes C_3) \rtimes C_2.$$

Het semi-direkte produkt is hier (na verontachtzaming van de morfismen α en de identifikatie van isomorfismen) associatief. In het algemeen geldt dit niet zonder meer. Als $n \geq 1$, dan zijn er verschillende morfismen

$$\alpha: \mathbb{Z}_p^* \to \mathrm{Aut}(\mathrm{Sl}_n(p)) \quad (\text{waar } \mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}),$$

zodat $\mathrm{Gl}_n(p) \cong \mathrm{Sl}_n(p) \rtimes_\alpha \mathbb{Z}_p^*$.

De volgende stelling maakt duidelijk dat de ondergroep K in het semi-direkte produkt G de rol van representantensysteem vervult.

1.8.11. STELLING. *Laat* G *een eindige groep zijn, laat* $K \leq G$ *en* $H \trianglelefteq G$. *De volgende uitspraken zijn ekwivalent.*

(i) G *is semi-direkt produkt van* H *en* K;

(ii) K *is representantensysteem van de nevenklassen van* H *in* G;

(iii) *de beperking* $\phi\big|_K$ *van het epimorfisme* $\phi: G \to G/H$ *is bijektief.*

BEWIJS. (i) $\Rightarrow$ (ii). Omdat K en G/H uit evenveel elementen bestaan is het voldoende aan te tonen dat iedere nevenklasse van H in G precies één element met K gemeen heeft. Laat gH een willekeurige nevenklasse zijn. Omdat $G = HK = KH$ (zie 1.5.8), zijn er $k \in K$ en $h \in H$ zodat $g = kh$. Bijgevolg is $kH = gH$, zodat $k \in gH \cap K$. Als echter $k' \in gH \cap K$, dan is er een $h' \in H$ zodat $k' = gh' = khh'$. Er volgt dat $k^{-1}k' = hh' \in K \cap H = \{e\}$ ofwel $k = k'$. De konklusie is dat $gH \cap K = \{k\}$.

(ii) $\Rightarrow$ (iii). Volgt uit de definitie van representantensysteem.

(iii) $\Rightarrow$ (i). Omdat iedere nevenklasse van H precies één element met K gemeen heeft, is de afbeelding ψ: G/H $\to$ K door

$$\psi(gH) = x \iff gH \cap K = \{x\} \quad \text{voor } g \in G$$

goed gedefinieerd. Ga zelf na dat ψ het inverse morfisme van $\phi\big|_K$ is. □

1.8.12. DEFINITIE. Laat K een eindige groep zijn en laat H een permutatiegroep op W van graad t zijn. Onder het *kransprodukt* H $\int$ K van K met H verstaan we de groep bestaande uit de verzameling

$$\{(h,f) \mid h \in H,\ f: W \to K\},$$

voorzien van de vermenigvuldiging

$$(h_1,f_1)(h_2,f_2) = (h_1h_2, w \mapsto f_1(h_2(w))f_2(w))$$

$$(f_1,f_2: W \to K;\ h_1,h_2 \in H).$$

Deze vermenigvuldiging is associatief

$$((h_1,f_1)(h_2,f_2))(h_3,f_3) = (h_1h_2, w \mapsto f_1(h_2(w))f_2(w))(h_3,f_2) =$$

$$(h_1h_2h_3, w \mapsto f_1(h_2h_3(w))f_2(h_3(w))f_3(w)) =$$

$$(h_1,f_1)(h_2h_3, w \mapsto f_2(h_3(w))f_3(w)) = (h_1,f_1)((h_2,f_2)(h_3,f_3)),$$

kent als één-element (1,e'), waar e': W $\to$ K gegeven is door e'(w) = e $\in$ K en als inverse van (h,f) het element (h^{-1},g), waar $g(w) = (f(h^{-1}(w)))^{-1}$ voor w $\in$ W. Dus H $\int$ K is inderdaad een groep.

De volgende stelling geeft enige informatie over de opbouw van H $\int$ K.

1.8.13. STELLING. *Laat* H *permutatiegroep op* $\underline{t}$ *zijn. Het kransprodukt* G = H $\int$ K *omvat de normaaldeler* $N = N_1 \times \ldots \times N_t$, *waar*

$$N_i = \{(e,f) \mid f(j) = e \text{ voor alle } j \neq i\} \cong K.$$

Laat e': $\underline{t} \to$ K *gegeven zijn door* e'(w) = e ($w \in \underline{t}$). *Dan is* H $\int$ K *semidirekt produkt van* N *en*

$$H^* = \{(h,e') \mid h \in H\} \cong H.$$

Dus

$$H \int K = H^* \underset{c}{\ltimes} (N_1 \times N_2 \times \ldots \times N_t),$$

waarbij de faktoren N_i *onder de konjugatie-permutatievoorstelling* c *verwisseld worden volgens* ${}^{c_{(h,e')}}N_i = N_{h(i)}$ $(i \in \underline{t})$.

BEWIJS. Definieer $\pi: H \int K \to H$ door $\pi(h,f) = h$. Dan is π een epimorfisme met kern $N = \{(e,f) \mid f: \underline{t} \to K\}$.
Ga zelf na dat $N = N_1 \times N_2 \times \ldots \times N_t$ en dat $N_i \cong K$.
Nu is de afbeelding $\varepsilon: H \to H^*$ gegeven door $\varepsilon(h) = (h,e')$ ook een morfisme en wel de inverse van $\pi\big|_{H^*}$. Hieruit volgt dat G semi-direkt produkt van N en $H^* = \varepsilon(H)$ is (vergelijk de voorgaande stelling). Voor $(h,e') \in H^*$ en $(e,g) \in N_i$ geldt tenslotte

$$c_{(h,e')}(e,g) = (h,e')(e,g)(h,e')^{-1} = (e, j \mapsto g(h^{-1}(j))),$$

zodat inderdaad ${}^{c_{(h,e')}}N_i = N_{h(i)}$. □

1.8.14. OPMERKINGEN.
- In plaats van $H \int K$ wordt vaak $K \wr H$ geschreven.
- De orde van $H \int K$ bedraagt $|H| \cdot |K|^t$.
- Zelfs als H en K kommutatief zijn, is $H \int K$ dat in het algemeen niet.

Is behalve H ook K voorzien van een permutatievoorstelling, dan is ook $H \int K$ op natuurlijke wijze van een permutatievoorstelling te voorzien:

1.8.15. PROPOSITIE. *Laat* G *een permutatievoorstelling* $\phi: G \to \mathrm{Sym}(V)$ *hebben en laat* H *een permutatiegroep op* $W = \underline{t}$ *zijn. Dan induceert* ϕ *een permutatievoorstelling* $\phi': H \int G \to \mathrm{Sym}(W \times V)$ *middels het voorschrift*

$$\phi'(h,f)(w,v) = (hw, \phi(f(w))v).$$

Als ϕ *getrouw is, dan* ϕ' *ook. Als* ϕ *en* H *transitief zijn, dan* ϕ' *ook.*

BEWIJS. Uit

$$\phi'((h_1,f_1)(h_2,f_2))(w,v) = \phi'(h_1h_2, i \mapsto f_1(h_2(i))f_2(i))(w,v) =$$

$$(h_1h_2w, \phi(f_1(h_2(w))f_2(w))v) = (h_1h_2w, \phi(f_1(h_2(w)))\phi(f_2(w))v) =$$

$$\phi(h_1,f_1)(h_2w,\phi(f_2(w))v) = \phi(h_1,f_1)\phi(h_2,f_2)(w,v)$$

volgt dat ϕ' inderdaad een permutatievoorstelling is. De rest van het bewijs wordt aan u overgelaten. □

Voordat we deze paragraaf met wat voorbeelden afsluiten, laten we nog zien dat het kransprodukt associatief is.

1.8.16. PROPOSITIE. *Laat* G,H,K *permutatiegroepen op respektievelijk* $\underline{r}$, $\underline{s}$ *en* $\underline{t}$ *zijn* $(r,s,t \in \mathbb{N})$. *De groepen* $(G \int H) \int K$ *en* $G \int (H \int K)$ *stellen dezelfde permutatiegroepen op* $\underline{r} \times \underline{s} \times \underline{t} = (\underline{r} \times \underline{s}) \times \underline{t} = \underline{r} \times (\underline{s} \times \underline{t})$ *voor.*

BEWIJS. Laat $(i,j,k) \in \underline{r} \times \underline{s} \times \underline{t}$. Met $m = (g,x \mapsto (h(x),\psi(x))) \in G \int (H \int K)$ korrespondeert $m' = ((g,h),(x,y) \mapsto (\psi(x))y) \in (G \int H) \int K$, want enerzijds geldt

$$m(i,j,k) = m(i,(j,k)) = (g(i),f(i)(j,k)) = (g(i),h(i)j,(\psi(i)j)k),$$

terwijl anderzijds

$$m'(i,j,k) = m'((i,j),k) = ((g,h)(i,j),(\psi(i)(j)k) =$$

$$(g(i),h(i)j,(\psi(i)j)k).$$ □

1.8.17. VOORBEELD. Voor vaste $m,n \in \mathbb{N}$ definiëren we $\Pi(m,n)$ door

$$\Pi(m,n) = \{(a_{ij}) \in Gl_n(\mathbb{C}) \mid \exists \sigma \in Sym(\underline{n})\ \forall i \in \underline{n}\ \exists \theta_i \forall j (\theta_i^m = 1 \wedge a_{ij} = \theta_i \delta_{i\sigma(j)})\}.$$

Dus

$$\Pi(2,2) = \{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}\}.$$

Ga na dat $\Pi(m,n)$ een groep is van orde $(n!)m^n$. De groep $\Pi(1,n)$ is isomorf met $Sym(\underline{n})$, de groep $\Pi(m,1)$ is isomorf met $\underbrace{C_m \times \ldots \times C_m}_{m \text{ keer}}$. Ga na dat $\Pi(m,n)$ zelf isomorf is met $Sym(\underline{n}) \int C_m$.

1.8.18. VOORBEELD. In $Sym(\underline{n})$ gaan we voor willekeurig priemgetal $p \leq n$ een ondergroep konstrueren van orde de hoogste p-macht M_n van $n! = |G|$. Van de getallen $1,2,\ldots,n$ zijn alleen $p,2p,\ldots,[\frac{n}{p}]p$ deelbaar door p (hier is $[\frac{n}{p}]$ het grootste gehele getal $\leq \frac{n}{p}$). Er geldt dus $M_n = [\frac{n}{p}] + M_{[\frac{n}{p}]}$.
Iteratie van de gelijkheid geeft

$$M_n = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \ldots .$$

Schrijven we n als som van p-machten

$$n = a_0 + a_1 p + \ldots + a_k p^k \quad \text{met } 0 \leq a_i < p,$$

dan volgt dat

$$(*) \qquad M_n = \sum_{i=1}^{k} a_i (1 + p + \ldots + p^{i-1}).$$

Laat nu J de cyklische ondergroep $<(12 \ldots p)>$ van orde p in $\mathrm{Sym}(\underline{p})$ zijn. Dan is J een permutatiegroep van orde en graad p, dus $J \int J$ heeft graad p^2 en orde p^{1+p} (vergelijk 1.8.15). Schrijven we

$$\int^r J \quad \text{voor} \quad \underbrace{J \int J \int \ldots \int J}_{r \text{ keer}},$$

dan heeft $\int^r J$ graad p^r en orde $p^{1+p+\ldots+p^{r-1}}$. We spreken nog af dat $\int^0 J = \{1\}$. Voor $n = a_0 + a_1 p + \ldots + a_k p^k$ kunnen we nu (gebruik makend van de laatste opmerking in 1.8.5) voor elke $i \in \{0,1,\ldots,k\}$ precies a_i permutatiegroepen $\int^i J$ van graad p^i vinden, zodat

$$P = \underbrace{(\int^0 J \times \int^0 J \times \ldots \times \int^0 J)}_{a_0 \text{ keer}} \times \underbrace{(\int^1 J \times \int^1 J \times \ldots \times \int^1 J)}_{a_1 \text{ keer}} \times \ldots \times \underbrace{(\int^k J \times \int^k J \times \ldots \times \int^k J)}_{a_k \text{ keer}}$$

een permutatiegroep van graad n en van orde p^{M_n} is.

Ter illustratie: n = 9 en p = 2 geeft $M_2 = 7$, dus P is een ondergroep van orde 2^7. Eén zo'n groep P is

$$<(2\ 3),(2\ 4)(3\ 5),(2\ 6)(3\ 7)(4\ 8)(5\ 9)>.$$

In het volgende hoofdstuk gaan we nader in op de eksistentie van ondergroepen in een gegeven groep G van orde de hoogste p-macht van $|G|$ voor priemgetallen p.

OPGAVEN BIJ §1.8.

*1. Bewijs de associativiteit van het direkte produkt: Als G_1, G_2, G_3 groepen zijn, dan is $(G_1 \times G_2) \times G_3 = G_1 \times (G_2 \times G_3)$.

*2. Bewijs de volgende generalisatie van Lemma 1.8.2. Als G een groep is met normaaldelers $G_1,\ldots,G_m$ zodat $G = G_1G_2 \cdots G_m$ en zodat voor iedere $i \in \underline{m}$ geldt $G_i \cap G_1G_2 \cdots G_{i-1}\, G_{i+1} \cdots G_m = 1$, dan is $G = G_1 \times G_2 \times \ldots \times G_m$.

3. (i) Laat G de ondergroep van Sym($\underline{8}$) zijn voorgebracht door $a = (12345678)$ en $b = (1652)(3478)$. Ga na dat $a^8 = b^4 = 1$ en dat $bab^{-1} = a^3$. Leid hieruit af dat $\langle a\rangle \trianglelefteq G$ en dat $G = \langle a\rangle \rtimes \langle b\rangle$, een groep van orde 32 is.

(ii) Laat H de ondergroep van Sym ($\underline{8}$) zijn voortgebracht door a en b uit (i) en $c = (18)(27)(36)(45)$. Ga na dat $c^2 = 1$ en dat $cac^{-1} = a^{-1}$, terwijl $cbc^{-1} = b$. Leid hieruit af dat $H = G \rtimes \langle c\rangle$, een groep van orde 64 is.

4. Laat a voortbrenger van de cyklische groep C_8 zijn. Door $a \mapsto a^4$ wordt een morfisme $C_8 \to C_2$ gedefinieerd dat als kern de cyklische ondergroep van C_8 voortgebracht door a^2 heeft. Bewijs dat er geen ondergroep K van C_8 bestaat zodat $C_8 = \langle a\rangle \rtimes K$.

*5. Ga na dat de gegeneraliseerde quaterniongroep Q_n uit Opgave 1.6.9 geen semi-direkt produkt van $\langle u\rangle$ en $\langle v\rangle$ is. Bewijs dat als n oneven is, Q_n wel semi-direkt produkt van $\langle u^2\rangle$ en $\langle v\rangle$ is.

6. Bewijs dat de in Opgave 1.2.3 gegeven permutaties β,γ een groep $G = \langle\beta,\gamma\rangle$ voortbrengen die isomorf is met $C_3 \int C_3$.

7. Laat B,N gedefinieerd zijn als in Opgave 1.1.7. Bewijs dat B semi-direkt produkt van N en $\underbrace{K^* \times K^* \times \ldots \times K^*}_{n \text{ keer}}$ is, waar $K^* = K - \{0\}$. Geldt ook $B \cong N \int (K)^*$?

8. Laat zien dat $\mathrm{Aut}(D_k) \cong C_k \rtimes A$, waar A een abelse groep van de orde $\phi(k)$ is; Euler's ϕ-funktie $\phi(k)$ geeft hierin het aantal gehele positieve getallen $\leq k$ dat priem met k is (zie Opgave 1.2.7).

*9. Als de eindige G ondergroepen H,K heeft zodanig dat $K \leq N_G(H)$ en $H \cap K = \{e\}$, dan geldt $H\cdot K = H \rtimes K$. Bewijs dit. Laat ook zien dat $H\cdot K = H \times K$ als bovendien $H \leq N_G(K)$.

*10. Beschouw de groep $K = K_1 \times K_2 \times \ldots \times K_t$ waar K_i ($i \in \underline{t}$) enkelvoudige niet-abelse groepen zijn. Toon aan dat elke normaaldeler van K van de vorm $K_{i_1} \times K_{i_2} \times \cdots \times K_{i_s}$ is voor zekere $i_1,i_2,\ldots,i_s \in \underline{t}$.
Hint: Merk op dat voor elke $i \in \underline{t}$ en elke normaaldeler N geldt hetzij $N \geq K_i$ hetzij $N \leq C_K(K_i) = K_1 \times \cdots \times K_{i-1} \times K_{i+1} \times \cdots \times K_t$.

*11. Stel dat $N_1, N_2 \ldots, N_t$ minimale normaaldelers van de eindige groep G zijn. Laat N de normaaldeler $N_1 N_2 \ldots N_t$ zijn. Bewijs dat er $i_1, i_2, \ldots, i_s \in \underline{t}$ zijn zodat $N = N_{i_1} \times N_{i_2} \times \ldots \times N_{i_s}$.
Hint: voer induktie naar t en gebruik Opgave 1.8.2.

*12. Als G een eindige karakteristiek enkelvoudige groep is (vergelijk 1.6.15), dan bestaan er enkelvoudige onderling isomorfe normaaldelers $N_1, N_2, \ldots, N_t$ in G, zo dat $G = N_1 \times N_2 \times \ldots \times N_t$. Bewijs dit door voor N_1 een minimale normaaldeler te nemen, het produkt over alle $\alpha(N_1)$ voor $\alpha \in \mathrm{Aut}(G)$ te beschouwen en daarop Opgave 1.8.11 toe te passen.

HOOFDSTUK II

LOKALE THEORIE

2.1. Sylowstellingen

Centraal in deze paragraaf zijn de zogeheten Sylowstellingen, waarin onder andere de eksistentie van ondergroepen van een gegeven groep van orde de macht van een priemgetal aangetoond wordt. Deze ondergroepen vormen het uitgangspunt voor dat deel van de ontleding van groepen dat p-lokaal onderzoek heet. Hier en in de rest van dit hoofdstuk stelt p steeds een priemgetal voor.

2.1.1. LEMMA. *Als* G *een groep van orde* $|G| = mp$ *voor* $m \in \mathbb{N}$ *is, dan bevat* G *een element van orde* p.

BEWIJS. Met induktie naar m. Als $m = 1$, dan is het lemma waar. (Waarom?) Laat $m > 1$. Als G een echte ondergroep H bezit zodat p deler van $|H|$ is, volgt de uitspraak uit de induktieveronderstelling. Stel daarom dat iedere echte ondergroep van G een orde heeft die priem met p is. Dan moet vanwege 1.5.3(ii) gelden $Z(G) = G$. Met andere woorden, G is abels. Kies $x \in G - \{e\}$ willekeurig. Laat t de orde van x zijn. Als t een p-veelvoud is, dan heeft $x^{(t/p)}$ de juiste orde. We mogen dus veronderstellen dat $ggd(t,p) = 1$. Omdat G abels is, is $\langle x \rangle$ een normaaldeler. Aldus is $G/\langle x \rangle$ een groep van orde $m_1 p$ voor zekere m_1 deler van m, zodat volgens de induktiehypothese er een $y \in G - \langle x \rangle$ te vinden is met $y^p \in \langle x \rangle$. Het is nu eenvoudig in te zien dat er een geschikte macht van y is die (evenals zojuist voor x) orde p heeft. □

2.1.2. STELLING. *Zij* G *een groep van orde* $p^r q$ $(r \geq 1)$ *en zij* m *het aantal ondergroepen van* G *van orde* p^r. *Als* $ggd(p,q) = 1$, *dan geldt:*

(i) $m = 1 \bmod p$;

(ii) *alle ondergroepen van* G *van orde* p^r *zijn gekonjugeerd;*

(iii) *elke ondergroep van* G *van orde een macht van* p *is bevat in een ondergroep van orde* p^r.

BEWIJS. Laat t maksimaal zijn zodat er een ondergroep in G van orde p^t bestaat. Vanwege 2.1.1 is $t \geq 1$. Geef met M de klasse van alle ondergroepen van G van orde p^t aan. Kies $P \in M$.

Stap 1. $|M| = 1 \bmod p$ *en als* $P,Q \in M$ *met* $P \leq N_G(Q)$, *dan is* $P = Q$.

BEWIJS. P werkt op M via konjugatie. Als $Q \in M$ onder deze werking invariant blijft (dat wil zeggen een P-baan is, bestaande uit $\{Q\}$), dan is $P \leq N_G(Q)$, dus $P \cdot Q$ een ondergroep van G van orde $p^{2t}/|P \cap Q|$ (zie 1.5.8). Uit de maksimaliteit van t volgt dat $|P \cap Q| = p^t$ zodat $Q = P$. Er is dus slechts één P-invariante groep in M, te weten P zelf. Bestaat een P-baan in M uit meer dan één punt, dan is de kardinaliteit van die baan (gezien 1.4.8) een p-voud. Bijgevolg zijn er $m = 1 \bmod p$ groepen in M.

Stap 2. *Alle ondergroepen van* G *in* M *zijn gekonjugeerd.*

BEWIJS. Laat $\mathcal{B}$ een G-baan (onder konjugatie) van P in M zijn. Als $Q \in M - \mathcal{B}$, dan bezit $\mathcal{B}$ enerzijds 0 mod p groepen, omdat $\mathcal{B}$ uit volledige Q-banen bestaat die vanwege stap 1 alle lengte > 1 hebben; anderzijds echter geldt $|\mathcal{B}| = 1 \bmod p$, omdat $\mathcal{B}$ ook uit volledige P-banen bestaat en $P \in \mathcal{B}$. Tegenspraak, dus $\mathcal{B} = M$.

De uitspraken (i) en (ii) volgen nu uit de volgende stap.

Stap 3. $t = r$.

Bewijs. Laat $N = N_G(P)$. Omdat deze groep de stabilisator van P in de genoemde konjugatie-permutatievoorstelling in M is, geldt vanwege Stap 2 en 1.4.8

$$|G|/|N| = 1 \bmod p.$$

Aldus blijkt dat uit $\text{ggd}(|G|/p^t, p) > 1$ zou volgen dat $\text{ggd}(|N/P|, p) > 1$ is. Passen we Lemma 2.1.1 toe op N/P, dan volgt de eksistentie van een $x \in N$, zodat $x^p \in P$. De ondergroep $\langle P,x \rangle$ heeft dan orde p^{t+1}, in tegenspraak met de maksimaliteit van t.

Stap 4. Laat L een ondergroep van G van orde p^s zijn ($s \leq r$). Dan heeft L vanwege $m = 1 \bmod p$ een vast punt, zeg Q, in de konjugatie-permutatievoorstelling op M. Aldus is $L \cdot Q$ een groep van orde een p-macht $\geq p^r$. Derhalve geldt $LQ = Q$, zodat $L \leq Q$ en (iii) bewezen is. □

2.1.3. DEFINITIE. Als G een eindige groep is van orde $|G| = p^s q$ met $\text{ggd}(p,q) = 1$, dan heet een ondergroep van orde p^s een p-*Sylow(onder)groep* van G. Een (onder)groep van orde een macht van p heet een p-*(onder)*groep.

De eerste stelling van deze paragraaf is genoemd naar Sylow. Zij geeft ondermeer aan dat Sylowondergroepen bestaan. Omdat de stelling zo belangrijk is, bewijzen we ook nog de volgende propositie, waaruit de eksistentie van p-ondergroepen van iedere denkbare orde binnen een gegeven groep blijkt.

2.1.4. PROPOSITIE. *Zij* G *een groep van orde* $|G| = p^r q$ $(r \geq 1)$ *en zij* m *het aantal ondergroepen van* G *van orde* p^r. *Dan is* $m \equiv 1 \bmod p$.

BEWIJS. Wordt geleverd in drie stappen:

Stap 1. Laat M de kollektie deelverzamelingen van G van kardinaliteit p^r zijn. We beschouwen de permutatievoorstelling $l\hat{}: G \to \mathrm{Sym}(M)$, gedefinieerd door $l\hat{}(g) = l_g$ met $l\hat{}(g)M = l_g(M) = gM$ $(M \in M)$. Laat $M_1, M_2, \ldots, M_t$ een representantensysteem voor de banen onder $l\hat{}$ in M zijn. Geef met U_i de stabilisator in G van M_i aan, dus

$$U_i = G_{M_i}^{l\hat{}} = \{g \in G \mid gM_i = M_i\} \quad (i \in \underline{t}).$$

Dan zijn er $m_{i1}, m_{i2}, \ldots, m_{ir_i} \in M_i$ zodat

$$M_i = U_i m_{i1} \dot{\cup} U_i m_{i2} \dot{\cup} \ldots \dot{\cup} U_i m_{ir_i}.$$

Hieruit volgt $p^r = |M_i| = r_i |U_i|$; er is dus een $a_i \in \mathbb{N}$ zodat $|U_i| = p^{a_i} | p^r$. Als $a_i < r$, dan geldt $pq \,|\, |G/U_i|$, dus $|G/U_i| \equiv 0 \bmod (pq)$. Als daarentegen $a_i = r$, dan is $|G/U_i| = q$. We konkluderen

$$\binom{p^r q}{p^r} = |M| = \sum_{|U_i| = p^r} |G/U_i| = \sum_{|U_i| = p^r} q \bmod (pq),$$

kortom,

$$\binom{p^r q}{p^r} \equiv q \cdot \#\{i \in \underline{t} \mid |U_i| = p^r\} \bmod (pq).$$

Stap 2. Beweringen:

(i) *Voor elke* $i \in \underline{t}$ *geldt:* $|U_i| = p^r$ *dan en slechts dan als de* G*-baan van* M_i *een ondergroep van* G *(van orde* p^r*) bevat;*

(ii) *géén* G*-baan in* M *bevat méér dan één ondergroep.*

Bewijs. (i) Als $|U_i| = p^r$, dan is er een $x \in M_i$ zodat $U_i x = M_i$. Nu is $x^{-1} M_i$ een element uit de G-baan van M_i. Bovendien is $x^{-1} M_i = x^{-1} U_i x$ een ondergroep (ga na!).

Andersom: Stel dat T een ondergroep van G is en behoort tot de G-baan van M_i. Dan bestaat er een $g \in G$ zodat $T = gM_i$. Volgens Stelling 1.4.8 is dan

$$gU_ig^{-1} = gG^{\hat{1}}_{M_i}g^{-1} = G^{\hat{1}}_{gM_i} = G^{\hat{1}}_{T} = T = gM_i,$$

zodat $|U_i| = |gU_ig^{-1}| = |gM_i| = |M_i| = p^r$.

(ii) Stel dat U,T ondergroepen van G in dezelfde G-baan binnen $\mathcal{M}$ zijn. Dan is er een $g \in G$ met $gU = T$. Hieruit volgt dat voor zekere $u \in U$ geldt $gu = e$ en $g = u^{-1} \in U$, zodat $T = gU = U$, waarmee (ii) bewezen is.

Stap 3. Uit Stap 2 volgt dat $m = \#\{i \in \underline{t} \mid |U_i| = p^r\}$. Tesamen met de formule afgeleid in Stap 1 levert dit

$$\binom{p^rq}{p^r} = mq \bmod pq.$$

Manipulatie met de binomiaalkoëfficient geeft

$$\binom{p^rq}{p^r} = q\binom{p^rq-1}{p^r-1},$$

zodat

$$\binom{p^rq-1}{p^r-1} = m \bmod p.$$

Wij zijn dus klaar zodra we aangetoond hebben dat het linkerlid in deze vergelijking = 1 mod p is. Dit is natuurlijk rechtstreeks te verifiëren, maar er is een ietwat elegantere manier om het bewijs af te maken: Merk op dat het linkerlid in de vergelijking alleen van de orde van G afhangt. We kunnen de waarde m(mod p) dus bepalen door berekening ervan voor het geval $G = C_{p^rq}$, de cyklische groep van die orde. Omdat deze groep precies één ondergroep van orde p^r heeft (zie Opgave 1.6.19), volgt $m = 1 \pmod p$. □

2.1.5. GEVOLGEN. *Laat* G *een eindige groep van orde* p^rq *zijn* ($r \geq 1$). *Dan geldt:*

(i) *Er zijn ondergroepen van orde* p^r;

(ii) G *heeft in de konjugatie-permutatievoorstelling op haar ondergroepen van orde* p^r *minstens een baan* $\mathcal{B}$ *van kardinaliteit* $\neq 0 \bmod p$;

(iii) *laat* $|G| = p^s$ *en laat* n *het aantal normaaldelers van orde* p^r *voor* $r \leq s$ *zijn. Dan is* $n = 1 \bmod p$.

BEWIJS. Doe zelf.

2.1.6. PROPOSITIE. G *als in* 2.1.5.

(i) *Als* P *een* p-*Sylowondergroep van* G *is en* $N_G(P) \leq U \leq G$, *dan is* $N_G(U) = U$.

(ii) *(Frattini-argument). Als* $N \trianglelefteq G$ *en* P *een* p-*Sylowondergroep van* N *is, dan is* $G = N_G(P) \cdot N$;

BEWIJS. (i). Laat $g \in N_G(U)$, dan is $gUg^{-1} = U$, dus $gPg^{-1} \leq gN_G(P)g^{-1} \leq$ $\leq gUg^{-1} = U$. Vandaar dat zowel P als gPg^{-1} ondergroepen van U zijn. Volgens de stelling zijn P en gPg^{-1} gekonjugeerd in U; dit houdt in dat er een $u \in U$ is, zodat $uPu^{-1} = gPg^{-1}$. Er volgt dat $u^{-1}g \in N_G(P) \leq U$, maar dan ook $g = u(u^{-1}g) \in U$.

(ii). Laat $g \in G$. Dan is $g^{-1}Pg \leq g^{-1}Ng = N$, dus P en $g^{-1}Pg$ zijn beide p-Sylowondergroepen van N. Omdat ze dan ook gekonjugeerd zijn in N, is er een $c \in N$, zodat $c^{-1}Pc = g^{-1}Pg$. Anders gezegd: $gc^{-1} \in N_G(P)$. Tenslotte is $g = (gc^{-1})c \in N_G(P) \cdot N$. □

2.1.7. OPMERKING. Uit 2.1.6 volgt in het bijzonder dat $N_G(N_G(P)) = N_G(P)$. De konstruktie $N_G(\cdot)$ levert in dit geval dus geen ondergroep van nog kleinere index. De normalisator van een p-ondergroep van G heet wel p-*lokale* of *lokale ondergroep* van G.

2.1.8. PROPOSITIE. *Als* $N \trianglelefteq G$ *en* P *een* p-*Sylowondergroep van* G, *dan geldt:*

(i) $N \cap P$ *is een* p-*Sylowondergroep van* N;

(ii) PN/N *is een* p-*Sylowondergroep van* G/N.

BEWIJS. (i). Uit 1.5.8(iv) blijkt dat PN een ondergroep van G is. $|N \cap P|$ deelt $|P|$ en is dus een macht van p. Verder is $|N|/|N \cap P| = |NP|/|P|$ een deler van $|G/P|$ en dus verstoken van p-faktoren. Maar dan is $N \cap P$ een p-Sylowgroep van N.

(ii). $|PN/N| = |P/P \cap N|$ is een macht van p, terwijl

$$|G/N|/|PN/N| = |G|/|PN|$$

deler van $|G/P|$ en dus priem met p is. □

2.1.9. VOORBEELD. De Sylowondergroepen van Sym(n) zijn gekonstrueerd in Voorbeeld 1.8.18. Die van Alt(n) zijn hieruit te verkrijgen door met Alt(n)

te doorsnijden (Propositie 2.1.8). Zo is $P = \langle (13), (12)(34) \rangle$ een 2-Sylowondergroep van $\mathrm{Sym}(\underline{4})$.

Ga na dat $N_{\mathrm{Sym}(\underline{n})}(P) = P$. Omdat $P \cong D_4$, is D_4 op isomorfie na de enige permutatiegroep van graad 4 en orde 8. Verder is

$$P' = P \cap \mathrm{Alt}(\underline{4}) = \{1, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$$

2-Sylowondergroep van $\mathrm{Alt}(\underline{4})$. Er geldt $N_{\mathrm{Alt}(\underline{4})}(P') = \mathrm{Alt}(\underline{4})$.

2.1.10. VOORBEELD. Alle p-Sylowondergroepen van zowel $\mathrm{Gl}_n(p)$ als $\mathrm{Sl}_n(p)$ zijn gekonjugeerd met de groep

$$P = \left\{ \begin{pmatrix} 1 & a_{12} & & a_{1n} \\ & 1 & & \\ & & \ddots & \\ 0 & & & a_{n-1,n} \\ & & & 1 \end{pmatrix} \;\middle|\; a_{ij} \in \mathbb{Z}_p \right\}$$

(vergelijk de p-machten in de ordes van de verschillende groepen).
Bepaal zelf $N_{\mathrm{Gl}_n(p)}(P)$.

Tenslotte passen we de Sylowstellingen toe op abelse groepen.

2.1.11. LEMMA. *In iedere abelse groep* A *van orde* $p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}$ *waar* p_i *onderling verschillende priemgetallen zijn, bevinden zich* p_i*-Sylowondergroepen* A_i $(i \in \underline{n})$ *in* A *zodat* $A = A_1 \times A_2 \times \ldots \times A_n$.

BEWIJS. Naar 2.1.2 bestaan er p_i-Sylowondergroepen A_i. Volgens Opgave 1.6.20 zijn deze A_i normaaldelers in A. Maak het bewijs zelf af. □

OPGAVEN BIJ §2.1.

*1. Bewijs dat iedere eindige groep van orde $2p^n$ (p priem > 2; n > 0) een echte niet-triviale normaaldeler heeft.

2. Met welke bekende groep van orde 8 is een 2-Sylowgroep van $\mathrm{PSl}_2(7) = \mathrm{Sl}_2(7)/Z(\mathrm{Sl}_2(7))$ isomorf?

3. Bepaal alle Sylowondergroepen van Alt($\underline{4}$).
   Geef tevens de lokale ondergroepen. Idem voor Alt($\underline{5}$) en Alt($\underline{6}$).

4. Bewijs: Alt($\underline{4}$) = $\langle(123),(234)\rangle$ resp. Alt($\underline{5}$) = $\langle(123),(345)\rangle$ door de beschouwing van het aantal 3-Sylowgroepen in de rechterleden en gebruikmaking van Opgave 1.1.10.

*5. Bewijs dat voor een p-Sylowondergroep P van een groep G geldt $P \trianglelefteq N_G(P)$ (zie 1.6.15). Leid hieruit wederom af dat $N_G(N_G(P)) = N_G(P)$.

*6. Laat zien dat er geen enkelvoudige groep van orde 12 is.

2.2. p-groepen

De Sylow-redeneringen geven een aantal resultaten voor groepen van orde een macht van p (p-groepen) die het waard zijn om apart vermeld te worden.

2.2.1. LEMMA. *Laat* G *een* p*-groep en laat* H *een ondergroep van* G *van index* p *zijn. Dan is* H *normaaldeler van* G.

BEWIJS. Induktie naar s, waar $|G| = p^s$. Als s = 1 is de uitspraak duidelijk. Neem aan dat s > 1 en schrijf Z = Z(G). We weten dat Z > {e}. Als $H \cap Z = \{e\}$, dan is G = ZH dus $H \lhd G$. We mogen dus veronderstellen dat $|H \cap Z| > 1$. Maar $G/(Z \cap H)$ is een groep (vergelijk Opgave 2 van §1.6) van orde $< |G|$ met ondergroep $H/(Z \cap H)$ van index p (ga dit zelf na). Induktie geeft dat $H/(Z \cap H)$ normaaldeler is in $G/(Z \cap H)$. Uit 1.6.6(ii) volgt dat H normaaldeler in G is.

2.2.2. KOROLLARIUM. *De enige enkelvoudige* p*-groepen zijn de priem-cyklische.*

BEWIJS. Laat G een enkelvoudige p-groep zijn. Propositie 2.1.4 geeft dat G minstens één ondergroep H van index p omvat. Uit het vorige lemma volgt dat H normaaldeler is. Uit de enkelvoudigheid van G leiden we af dat H = {e}. □

Aan de hand van de volgende stelling zal blijken dat een niet-priem-cyklische p-groep zelfs erg veel normaaldelers heeft.

2.2.3. STELLING. *Laat* G *een* p*-groep zijn.*

(i) *als* N_1 *en* N_2 *normaaldelers van* G *zijn met* $N_1 < N_2$ *en* $|N_2/N_1| \geq p^2$, *dan heeft* G *nog een normaaldeler* N *zodat* $N_1 < N < N_2$ *en* $|N_2/N| = p$.

(ii) *Als* H *een echte ondergroep van* G *is, dan heeft* G *een ondergroep* K *zodat* $H \lhd K$ *en* $|K/H| = p$.

BEWIJS.

(i) Dankzij 1.6.6(ii) is het voldoende om de uitspraak aan te tonen voor het geval dat $N_1 = \{e\}$. Met V geven we de kollektie ondergroepen van N_2 van index p in N_2 aan. Volgens Propositie 2.1.4 geldt $|V| = 1 \bmod p$. Aan de andere kant bestaat V uit volledige banen onder de konjugatie-permutatievoorstelling van G (immers voor $x \in G$ en $H \in V$ geldt $xHx^{-1} \leq xN_2x^{-1} = N_2$). Omdat iedere baan van lengte > 1 uit $0 \bmod p$ elementen bestaat (gebruik Stelling 1.4.8), volgt dat er minstens één baan binnen V is die bestaat uit precies één element, zeg N. Deze ondergroep $N \in V$ is een normaaldeler van G met de gewenste eigenschappen.

(ii) Induktie naar $|G|$. Als $N_G(H) > H$, dan kunnen we (i) herhaaldelijk toepassen of $N_G(H)$ is zelf al een groep als verlangd. We kunnen ons dus beperken tot het geval $N_G(H) = H$. In het bijzonder is dan $1 < Z(G) \trianglelefteq H$. Pas de induktiehypothese toe op de ondergroep $H/Z(G)$ van $G/Z(G)$. Dit levert een ondergroep K van G zo dat $H \leq K$ en $|K/Z(G) : H/Z(G)| = p$. Maar dan is ook $|K/H| = p$, dus voldoet K. □

2.2.4. KOROLLARIUM. *Iedere groep* G *van orde* p^s *(waar* $s \in \mathbb{N} - \{1\}$*) omvat een stel normaaldelers* $\{e\} = N_0, N_1, \ldots, N_{s-1}, N_s = G$, *waarvoor*

$$\{e\} \triangleleft N_1 \triangleleft N_2 \triangleleft \ldots \triangleleft N_{s-1} \triangleleft G$$

en $N_{i+1}/N_i \cong C_p$ *geldt.*

Dat zo'n opbouw van de groep G met behulp van normaaldelers G nog geenszins volledig bepaalt, blijkt alleen al uit het abelse geval.

2.2.5. PROPOSITIE. *Voor iedere abelse groep* G *van orde* p^s *bestaan* $i_1, i_2, \ldots, i_t \in \mathbb{N}$ *met* $i_1 \geq i_2 \geq \ldots \geq i_t$ *en* $i_1 + i_2 + \ldots + i_t = s$ *(ofwel een ongeordende partitie van* s*) zodat*

$$G \cong C_{p^{i_1}} \times C_{p^{i_2}} \times \ldots \times C_{p^{i_t}}.$$

Deze toevoeging $G \mapsto (i_1, i_2, \ldots, i_t)$ induceert een 1-1 - korrespondentie tussen de isomorfieklassen van eindige abelse groepen van orde p^s en de ongeordende partities van s.

BEWIJS. Laat G een abelse groep van orde p^s zijn. Veronderstel dat G niet cyklisch is (anders is $G \cong C_{p^s}$). Laat $g_1 \in G$ zo gekozen zijn dat $G_1 = \langle g_1 \rangle$ een cyklische groep van maksimale orde, zeg p^{i_1} in G is. Beschouw nu de

groep G/G_1. Laat g_2 zo gekozen zijn dat g_2G_1 een element van maksimale orde, zeg p^{i_2}, in G/G_1 is. Dan is $g_2^{p^{i_2}} = g_1^{np^a}$ voor zekere $a \leq s$ en $n \in \mathbb{N}$ met ggd(n,p) = 1. Maar in g_2G_1 bevindt zich een element van orde p^{i_2}: omdat g_1 maksimale orde p^{i_1} en g_2 orde $p^{i_2}.p^{i_1-a} = p^{i_1-(a-i_2)}$ heeft, is $(a-i_2) \in \mathbb{N}$; de nevenklassevertegenwoordiger $g_2g_1^{-np^{a-i_2}}$ heeft nu orde p^{i_2}. We konkluderen dat $G_2 = \langle g_2g_1^{-np^{a-i_2}} \rangle$ een cyklische groep van orde p^{i_2} met $G_1 \cap G_2 = \{e\}$ is, ofwel $G_1G_2 \cong C_{p^{i_1}} \times C_{p^{i_2}}$. Als G_1G_2 niet alle elementen van G bevat, kiezen we weer een element $g_3 \in G$ zodat $g_3G_1G_2$ maksimale orde in $G/(G_1G_2)$ heeft, enzovoorts. Uiteindelijk hebben we zo een stel ondergroepen $G_1, G_2, \ldots, G_t$ van ordes $p^{i_1} \geq p^{i_2} \geq \ldots \geq p^{i_t}$ verkregen met

$$G_j \cap (G_1G_2 \cdots G_{j-1}) = \{e\}$$

voor iedere $j \in \underline{t}$. Hieruit volgt dat

$$G = (\ldots((G_1 \times G_2) \times G_3) \ldots \times G_t) = G_1 \times G_2 \times \ldots \times G_t$$

$$\cong C_{p^{i_1}} \times C_{p^{i_2}} \times \ldots \times C_{p^{i_t}}.$$

De rest van het bewijs wordt aan u overgelaten. □

2.2.6. OPMERKING. Samengevoegd met 2.1.11 levert de voorgaande propositie de zogenaamde hoofdstelling van de abelse groepen, die er op neer komt dat alle abelse groepen van gegeven orde op isomorfie na bepaald zijn.

2.2.7. VOORBEELD. De groepen van orde 16.
Laat G een groep van orde 16 zijn. Als G abels is, dan wordt G op isomorfie na bepaald door een partitie van 4. De mogelijke ongeordende partities van 4 zijn: 4, $3 \geq 1$, $2 \geq 2$, $2 \geq 1 \geq 1$, $1 \geq 1 \geq 1 \geq 1$. Als G abels is, dan is G dus isomorf met één van de 5 onderling niet isomorfe groepen C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2 \times C_2$, $C_2 \times C_2 \times C_2 \times C_2$.

De methoden geschetst in het voorafgaande (opgaven inkluis) leveren het volgende 8-tal niet-abelse groepen van orde 16.

- D_8, $D_4 \times C_2$ (zie 1.1.12);
- Q_4, $Q \times C_2$ (zie Opgave 9 van §1.6);
- $C_8 \rtimes_\alpha C_2$, $C_8 \rtimes_\beta C_2$, waar $\alpha, \beta: C_2 \to \mathrm{Aut}(C_8)$ gegeven worden door respektievelijk

$$\left.\begin{aligned} \alpha(a)x &= x^3 \\ \text{en } \beta(a)x &= x^5 \end{aligned}\right\} \quad (a \in C_2 - \{e\},\ x \in C_8);$$

- $C_4 \underset{\gamma}{\rtimes} C_4$, $(C_4 \times C_2) \underset{\delta}{\rtimes} C_2$, waar $\gamma\colon C_4 \to \mathrm{Aut}(C_4)$ gegeven wordt door

$$\gamma(a)x = x^3 \qquad (a \in C_4 - C_2,\ x \in C_4),$$

en $\delta\colon C_2 \to \mathrm{Aut}(C_4 \times C_2)$ het morfisme is dat vastgelegd wordt door

$$\delta(a) = (c,bc)(c^{-1},bc^{-1}) \qquad (a \in C_2 - \{e\},\ b \in C_2 - \{e\},\ c \in C_4 - C_2).$$

Dit zijn echter niet alle groepen van orde 16. We geven nog een die met geen der voorafgaande 13 isomorf is: schrijven we

$$u = (1\ 3\ 2\ 4)(5\ 7\ 6\ 8),$$
$$g = (1\ 5\ 2\ 6)(3\ 7\ 4\ 8),$$
$$v = (1\ 7\ 2\ 8)(3\ 5\ 4\ 6),$$

dan is $G_0 = \langle u,g,v\rangle$ een permutatiegroep in $\underline{8}$. De elementen u,g,v voldoen aan de relaties

$$g^4 = u^4 = v^4 = e; \qquad vuv^{-1} = u^{-1}; \qquad u^2 = v^2 = g^2;$$
$$gu = ug; \qquad vg = gv.$$

Hieruit is direkt af te leiden dat ieder element in G_0 te schrijven is als

$$u^i g^j v^k \qquad \text{voor zekere } i \in \underline{2},\ j \in \underline{2},\ k \in \underline{4}.$$

De groep G_0 bevat dus niet meer dan 16 elementen. Door u,g,v als permutaties van de vier paren {1,2}, {3,4}, {5,6}, {7,8} op te vatten, krijgen we een epimorfisme van G_0 op de ondergroep V_4 van $\mathrm{Sym}(\underline{4})$ (zie 1.6.7) met kern van orde ≥ 4. Er volgt dat G_0 (minstens en dus) precies 16 elementen heeft. Ga zelf na dat ieder tweetal van de 14 genoemde groepen van orde 16 onderling niet isomorf is (bekijk daartoe het aantal elementen van gegeven orde, de orde van het centrum, enz.).

Ter illustratie van de voorafgaande theorie sluiten we deze paragraaf af met:

2.2.8. STELLING. *Iedere niet-abelse groep van orde* 16 *is isomorf met één van de* 9 *groepen* $D_4 \times C_2$, D_8, $Q \times C_2$, Q_4, $C_8 \underset{\alpha}{\rtimes} C_2$, $C_8 \underset{\beta}{\rtimes} C_2$, $C_4 \underset{\gamma}{\rtimes} C_4$, $(C_4 \times C_2) \underset{\delta}{\rtimes} C_2$, G_0.

BEWIJS. G bevat geen element van orde 16.

Stap 1. Stel dat G een element c van orde 8 bevat. Volgens Lemma 2.2.1 is $H = \langle c\rangle$ dan een normaaldeler van G. Kies een element $g \in G - H$ van minimale

orde. Dan is $g^2 \in H$. Omdat $c_g(c)$ een element in H van orde 8 is, geldt $c_g(c) \in \{c^3, c^5, c^7\}$. (Merk op dat $c_g(c) = c$ tot gevolg zou hebben dat G abels was.)

- Als g orde 2 heeft, dan is $G = H \rtimes \langle g \rangle$ isomorf met $C_8 \underset{\alpha}{\rtimes} C_2$, $C_8 \underset{\beta}{\rtimes} C_2$ of D_8 al naar gelang $c_g(c) = c^3$, c^5 of c^7. We mogen dus voor de rest van deze stap veronderstellen dat alle elementen in de nevenklasse van H in G orde ≥ 4 hebben.
- Stel dat g orde 4 heeft. Dan is $g^2 = c^4$. Als $c_g(c) = c^3$, dan heeft gc orde 2: als $c_g(c) = c^5$, dan heeft gc^2 orde 2; beide veronderstellingen leiden tot een tegenspraak, dus $c_g(c) = c^7$ en $G \cong Q_4$.
- Rest het geval dat g orde 8 heeft. Er geldt $g^2 \in \{c^2, c^6\}$. Als $c_g(c) = c^5$, dan heeft $(gc)^2 = cg^2$ orde ≤ 2; tegenspraak. Dus $c_g(c) = c^3$ of c^7. In beide gevallen volgt $c_g(c^2) = c^6$, in strijd met $g^2 \in \{c^2, c^6\}$. Het element g kan dus niet van orde 8 zijn.

Aan de orde is het geval dat G geen element van orde 8 bevat. Als G slechts uit elementen van orde 2 bestaat, dan is G abels, getuige Opgave 3 van §1.1. Er is dus een element $c \in G$ van orde 4.

Stap 2. G bevat een ondergroep H van orde 8 met daarin een element van orde 4.

BEWIJS. Dit is Stelling 2.2.3(ii).

Gezien Opgave 8 van §1.6 en Propositie 2.2.5 mogen wij voor de rest van het bewijs van de stelling veronderstellen dat G een ondergroep H bevat isomorf met D_4, Q of $C_4 \times C_2$.

Stap 3. Als $H \cong D_4$, Q, dan omvat H een normaaldeler N in G van orde 4 die isomorf is met C_4. Als $H \cong C_4 \times C_2$, dan omvat H een normaaldeler N in G van orde 4 die isomorf is met $C_2 \times C_2$.

Bewijs. D_4 bevat een unieke normaaldeler $\cong C_4$ en $C_4 \times C_2$ bevat een unieke normaaldeler $\cong C_2 \times C_2$. Omdat voor $g \in G - H$ de beperking H van het automorfisme c_g normaaldelers van H in normaaldelers overvoert, moet de unieke normaaldeler onder c_g vast blijven. (In feite passen we Opgave 1.6.3 toe.) Verder is c_g beperkt tot H een automorfisme van orde een macht van 2. Omdat Q precies 3 (onderling isomorfe) ondergroepen van orde 4 heeft, blijft minstens één daarvan invariant onder c_g. Ga zelf na dat deze c_g-invariante ondergroep dan ook een normaaldeler in G is.

Stap 4. Stel $H \cong D_4$. Vanwege Stap 3 mogen we veronderstellen dat $N = \langle c \rangle$ een ondergroep van orde 4 in D_4 is die normaaldeler in G is. Laat $a \in H$ zo

gekozen zijn dat $a^2 = e$ en $aca^{-1} = c^{-1}$. Dan is $H = \langle c,a \rangle$. Tenslotte kiezen we $g \in G - H$. Omdat $c_g N = N$ moet $c_g(c) \in \{c,c^3\}$ gelden. Als $c_g(c) = c^3$, dan is $c_{ag}(c) = c$. Dus na vervanging van g door ag, mogen we $c_g(c) = c$ veronderstellen. Omdat $c_g N = N$, geldt ook $c_g(H - N) = H - N$. Derhalve is er een $i \in \mathbb{N}$ zodat $c_g(a) = ac^i$. Omdat $c_{gcj}(a) = ac^{i-2j}$ voor $j \in \mathbb{N}$, levert vervanging van g door gc^j voor geschikte j dat we nog slechts twee gevallen hoeven onderscheiden, te weten $c_g(a) = a$ en $c_g(a) = ac$.

- $c_g(a) = a$. Als g van orde 2 is, dan is $G = H \times \langle g \rangle \cong D_4 \times C_2$. Als g van orde 4 is, dan is $g^2 \in H$ van orde 2; maar omdat $g \in C_G(a) \cap G_C(c)$ en $\langle c,a \rangle = H$, geldt $g^2 \in Z(H) = \{e,c^2\}$. Dus $g^2 = c^2$ en G is isomorf met G_0 (zoals men inziet door $u = c$ en $v = ag$ te kiezen).
- $c_g(a) = ac$. De orde van g kan slechts 4 zijn. Uit $c_{g^2}(a) = ac^2$, $c_{g^2}(ac) = ac^3$ en $g^2 \in H$ volgt dat $g^2 \in \{c,c^3\}$, maar dit is in strijd met de orde van g.

Aldus hebben we het geval dat $H \cong D_4$ uitputtend behandeld.

Stap 5. Stel $H \cong Q$. Laat u voortbrenger zijn van de normaaldeler N van G, bevat in H. Kies $v \in H - N$ van orde 4 zodat $u^2 = v^2$ en $vuv^{-1} = u^{-1}$ (ga zelf na dat zo'n v te vinden is). Verder kiezen we $g \in G - H$ willekeurig. Omdat $c_g N = N$, geldt $c_g(u) \in \{u,u^{-1}\}$. Eventuele vervanging van g door gv brengt de te bestuderen gevallen terug tot $c_g(u) = u$. Beschouwing van de elementen van orde 4 in $H - N$ levert $c_g(v) \in \{v,v^{-1},uv,u^3v\}$. Na eventuele vervanging van g door gu hebben we hetzij $c_g(v) = v$, hetzij $c_g(v) = uv$.

- $c_g(v) = v$. Omdat g met ieder element in H kommuteert, geldt $g^2 \in Z(H)$. Ook is g^2 van orde ≤ 2, zodat volgt $g^2 \in \{e,u^2\}$. Als $g^2 = e$, dan is $G = Q \times C_2$. Als $g^2 = u^2$, dan is $G \cong G_0$.
- $c_g(v) = uv$. Hieruit valt af te leiden dat $c_{g^2}(v) = v^{-1}$ en $g_{g^2}(uv) = u^3v$, zodat met $g^2 \in H$ volgt $g^2 \in \{u,u^{-1}\}$, in strijd met de orde van g.

Hiermee is ook het geval $H \cong Q$ afgedaan.

Stap 6. Voor de rest van het bewijs mogen we veronderstellen dat iedere ondergroep in G van index 2 abels is. Laat $H \leq G$ een ondergroep $\cong C_4 \times C_2$ zijn. Kies c van orde 4 en a van orde 2 in H zodat $H = \langle c,a \rangle$. Neem $g \in G - H$. Ga na dat $c_g(c^2) = c^2$. Buiten c^2 kent H nog slechts twee elementen van orde 2, te weten a en ac^2. Als $c_g(a) = ac^2$, dan is $\langle g,a,c^2 \rangle$ een niet-abelse ondergroep in G van orde 8. We houden de mogelijkheid over dat $c_g(a) = a$. Omdat $c_g(c) = c$ tot gevolg zou hebben dat G abels was, geldt $c_g(c) \in \{c^{-1},ac,ac^{-1}\}$, de verzameling van de overige elementen in H van orde 4. Maar als $c_g(c) = ac^{-1}$, kunnen we a vervangen door ac^2 zodat de

gelijkheid teruggebracht wordt tot $c_g(c) = ac$ (ga na waarom). We onderscheiden de twee resterende identiteiten $c_g(c) = c^{-1}$ en $c_g(c) = ac$.

- $c_g(c) = c^{-1}$. Als g orde 2 heeft, of als $g^2 = c^2$, dan is $\langle g,c\rangle$ een niet-abelse groep van orde 8, uitgesloten. Dus $g^2 \in \{a,ac^2\}$. In beide gevallen is G isomorf met $C_4 \underset{\gamma}{\rtimes} C_4$.
- $c_g(c) = ac$. Als g orde 2 heeft, dan is $G \cong (C_4 \times C_2) \underset{\delta}{\rtimes} C_2$.
  Stel g heeft orde 4. Dan is $g^2 \in \{a,ac^2,c^2\}$. Dus $g^2 = ac^2$; dan heeft gc orde 2 en vallen we terug op het voorgaande. Als $g^2 = c^2$, dan geldt $(gc)^2 = a$, zodat na eventuele vervanging van g door gc rest: $g^2 = a$. Via $c_c(g) = ga$ komen we uit op een normaaldeler $\langle g\rangle$ met $G = \langle g\rangle \rtimes \langle c\rangle \cong C_4 \underset{\gamma}{\rtimes} C_4$.

Hiermee zijn alle mogelijkheden uitgeput. □

OPGAVEN BIJ §2.2.

1. Hoeveel onderling niet-isomorfe abelse groepen hebben respektievelijk orde p^2, p^3, p^4 en p^2q^2, waar p en q verschillende priemgetallen zijn?
2. Laat P een p-groep en K een ondergroep van P zijn. Noteer $N_P^1(K) = N_P(K)$ en $N_P^{i+1}(K) = N_P(N_P^i(K))$. Bewijs dat er een natuurlijk getal m bestaat met $N_P^m(K) = P$.
3. Bepaal de verschillende niet-abelse groepen van orde p^3 als p een priemgetal is.
   (Aanwijzing: Behandel $p = 2$ apart. Als voor $p \geq 3$ er een element c van orde p^2 in de groep G van orde p^3 te vinden is, laat dan zien dat $G \cong C_{p^2} \underset{\alpha}{\rtimes} C_p$, waar $\alpha(c) = c^{p+1}$. Zo niet, dan heeft G een ondergroep $\langle a\rangle \times \langle b\rangle$ isomorf met $C_p \times C_p$. Leid af dat dan $G \cong (\langle a\rangle \times \langle b\rangle) \underset{\beta}{\rtimes} C_p$ waar $\beta(a^ib^j) = a^{i+j}b^j$.)

2.3. Een stelling van Burnside

Bij zijn pogingen noodzakelijke voorwaarden voor groepen op te stellen opdat ze enkelvoudig zijn, heeft Burnside onder andere de volgende stelling bewezen.

2.3.1. STELLING. *Laat* G *een eindige groep zijn met* p*-Sylowondergroep* P. *Als* $P \leq Z(N_G(P))$, *dan bezit* G *een normaaldeler* H *met* $H \cap P = \{e\}$ *en* $G = H \rtimes P$.

BEWIJS. In 6 stappen.

Stap 1, waarin een afbeelding v: G → P wordt gedefinieerd.
We noteren n = |G/P|. Laat $x_1, x_2, \ldots, x_n$ een volledig stelsel linksnevenklassevertegenwoordigers van P in G zijn. Voor g ∈ G is er dan een permutatie π ∈ Sym(n), zo dat $gx_iP = x_{\pi(i)}P$ (i ∈ n). Er zijn dus $p_i \in P$, zodat $gx_i = x_{\pi(i)}p_i$. Het voorschrift $v(g) = \prod_{i=1}^{n} p_i$ definieert dus een afbeelding v: G → P.

Stap 2. Ga zelf na dat deze afbeelding v niet afhangt van het gekozen representantensysteem $x_1, x_2, \ldots, x_n$.

Stap 3. Omdat P abels is, is de afbeelding v: G → P een groepsmorfisme:
Als voor h ∈ G er een ρ ∈ Sym(n) en $q_i \in P$ zijn, zo dat $hx_i = x_{\rho(i)}q_i$ (i ∈ n), dan is $ghx_i = gx_{\rho(i)}q_i = x_{\pi\rho(i)}p_{\rho(i)}q_i$, dus volgt
$v(gh) = \prod_{i=1}^{n} p_{\rho(i)}q_i = \prod_{i=1}^{n} p_{\rho(i)} \prod_{i=1}^{n} q_i = \prod_{i=1}^{n} p_i \prod_{i=1}^{n} q_i = v(g)v(h)$.

Stap 4, waarin aangetoond wordt dat voor elke x ∈ G en g ∈ P met $xgx^{-1} \in P$ geldt $g = xgx^{-1}$. Zowel P als $x^{-1}Px$ bevatten g en zijn abels, dus P, $x^{-1}Px \leq C_G(g)$. Volgens Stelling 2.1.5(ii), toegepast op $C_G(g)$ bestaat er een $c \in C_G(g)$, zodat $x^{-1}Px = c^{-1}Pc$. Dit betekent dat $xc^{-1} \in N_G(P)$. Tezamen met $P \leq Z(N_G(P))$ volgt $g \in P \leq C_G(xc^{-1})$. Maar dan ook $xc^{-1} \in C_G(g)$ en $x = (xc^{-1})c \in C_G(g)$, dus $g = xgx^{-1}$; klaar.

Stap 5, waarin v surjektief blijkt te zijn.
Kies g ∈ P. Neem $y_1, y_2, \ldots, y_t \in G$ zodat $y_1P, y_2P, \ldots, y_tP$ een representantensysteem vormt voor de banen in G/P onder $l\big|^{\wedge}_{\langle g\rangle}$: ⟨g⟩ → Sym(G/P) (de linksvermenigvuldiging-permutatievoorstelling beperkt tot ⟨g⟩). We geven voor i ∈ t met n_i de lengte van de baan van y_iP aan. Dan is $n = n_1 + n_2 + \ldots + n_t$. Uitschrijven van v(g) met behulp van de nevenklassen-representanten $g^j y_i$ (i ∈ t; j ∈ n_i) levert dat $y_i^{-1}g^{n_i}y_i \in P$ en $v(g) = \prod_{i=1}^{t} y_i^{-1}g^{n_i}y_i$. Maar uit Stap 4 volgt dat $y_i^{-1}g^{n_i}y_i = g^{n_i}$, dus $v(g) = \prod_{i=1}^{t} g^{n_i} = g^n$. Omdat ggd(n, |P|) = 1, zijn er r,s ∈ ℤ met rn + s|P| = 1. Uit $g^n \in v(G)$ volgt $g = g^{rn+s|P|} = (g^n)^r \in v(G)$.
We hebben bewezen dat voor iedere g ∈ P geldt g ∈ v(G); kortom, v is surjektief.

Stap 6. Slot van het bewijs.
Laat H = Ker v. De eerste isomorfiestelling (1.6.6) geeft G/H ≅ P.
Stelling 1.8.11 doet de rest. □

2.3.2. GEVOLG. Laat p de kleinste priemdeler zijn van de orde van een

gegeven groep G. Als G een cyklische p-Sylowgroep P heeft, dan bezit G een normaaldeler H, zodat $G/H \cong P$.

BEWIJS. Als $g \in N_G(P) - P$ een element van orde, zeg q, is, dan is de beperking van c_g tot P een automorfisme van de orde een deler van q. De orde van een automorfisme van $P \cong C_{p^n}$ voor zekere $n \in \mathbb{N}$ moet vanwege Opgave 8 van §1.8 een deler zijn van $p^n(1 - \frac{1}{p}) = p^{n-1}(p-1)$. Pas de eerste isomorfiestelling toe op het morfisme $g \mapsto c_g|_P$ van $N_G(P)$ naar Aut(P) om in te zien dat $N_G(P)/C_G(P)$ isomorf is met een ondergroep van Aut(P). Dan valt op dat $|N_G(P)|$ een deler is van $|\mathrm{Aut}(P)||C_G(P)|$. Uit Opgave 1.2.7 volgt dat $|\mathrm{Aut}(P)|$ een produkt is van priemgetallen $\leq p$. Omdat p het kleinste priemgetal is dat in $|G|$ en dus ook in $|N_G(P)|$ voorkomt, moet $|N_G(P)|$ deler van $|P||C_G(P)|$ zijn. Omdat $P \trianglelefteq C_G(P)$, $P \trianglelefteq N_G(P)$ en P een p-Sylowgroep is, is $|N_G(P)/P|$ deler van $|C_G(P)/P|$. Maar $C_G(P)/P \leq N_G(P)/P$, zodat nu $C_G(P)/P = N_G(P)/P$. Derhalve $C_G(P) = N_G(P)$.
We passen nu de voorgaande stelling toe om een passende normaaldeler H te vinden. □

De in de stelling en haar gevolg gevonden normaaldeler H is in zoverre een bijzondere normaaldeler, dat hij behalve onder konjugatie met elementen uit G, ook onder ieder ander automorfisme van G invariant is. We bewijzen dit in het navolgende.

2.3.3. PROPOSITIE. *Als G semi-direkt produkt van een normaaldeler N en een p-Sylowgroep P is, dan is* $N \trianglelefteq G$. *In feite is*

$$N = \{x \in G \mid x \text{ is van orde relatief priem met } p\}.$$

BEWIJS. Schrijf $n = |G/P| = |N|$ en laat $q = |P|$. Voor $x \in G$ geldt $x^q \in N$ (immers, $x = yz$ voor zekere $y \in P$ en $z \in N$, zodat er een $z' \in N$ is met $x^q = (yz)^q = y^q z' = z'$).

Andersom: Als $x \in G$ orde m heeft en $\gcd(m,p) = 1$, dan zijn er $r,s \in \mathbb{Z}$, zodat $mr + qs = 1$. Bijgevolg is $x = (x^q)^s \in N$. Hiermee is de laatste uitspraak van de propositie waargemaakt. De eerste volgt hieruit omdat een automorfisme van G de orde van elk van haar elementen behoudt. □

2.3.4. OPMERKING. In gevolg 2.3.2 ligt onder andere besloten dat geen enkelvoudige groep een cyklische 2-Sylowgroep omvat. Een niet-abelse enkelvoudige groep heeft echter altijd een even orde. Dit diepe resultaat was een vermoeden van Burnside, maar is pas in 1963 bewezen. Sindsdien zijn de

enkelvoudige groepen met een gegeven 2-Sylowondergroep voor een aantal 2-groepen bepaald. De kleinste niet-cyklische 2-groep is de viergroep van Klein. Alt(5) heeft een 2-Sylowgroep isomorf met deze groep en is enkelvoudig, naar we nu zullen aantonen.

2.3.5. PROPOSITIE. Alt(5) *is enkelvoudig.*

BEWIJZEN. Laat N een niet-triviale normaaldeler van Alt(5) zijn. We zullen op drie verschillende manieren vaststellen dat N = Alt(5).

Bewijs 1. Uit 1.7.6 volgt dat de lengtes van de konjugatieklassen van Alt(5) respektievelijk 1,15,20,12,12 zijn. N is een vereniging van konjugatieklassen (zie 1.6.1(iii)) en heeft dus een orde die een deler van 60 en een som van 1 en enkele andere lengtes is. Dit leidt tot $|N| = 60$. Klaar □

Bewijs 2.

Stap 1. N *bevat een* 3*-kring.*

Zoniet, dan bevat N (eventueel na verwisseling van enkele letters) hetzij (12)(34) hetzij (12345). Derhalve bevat N ook (125) = (12)(34)(125)(12)(34)$(125)^{-1}$ of (135) = $(12345)^{-1}(123)(12345)(123)^{-1}$. Tegenspraak.

Stap 2. *Als* N *een* 3*-kring bevat, dan geldt* N = Alt(5).

Immers, N bevat één 3-kring, dus alle (ze vormen één konjugatieklasse), en in Opgave 1.5.9 is reeds vastgesteld dat Alt(5) door haar 3-kringen wordt voortgebracht.

Bewijs 3.

Stap 1. N *bevat een* p*-Sylowgroep voor zekere* $p \in \{3,5\}$.

Als het tegendeel zou gelden dan zou N bevat zijn in een 2-Sylowgroep van Alt(5) volgens 2.1.2(iii). In het bijzonder zou N een letter $v \in 5$ fixeren. Maar dan is met v ook g(v) een vast punt van $N = gNg^{-1}$ voor elke $g \in$ Alt(5). Dus elke $w \in 5$ is vast punt van N, ofwel N = 1, wat uitgesloten is.

Stap 2. *Als* N *een* p*-Sylowgroep* P *voor zekere* $p \in \{3,5\}$ *omvat, dan is* N = Alt(5).

Om dit in te zien, mogen we veronderstellen dat N minimaal is met de eigenschap dat ze een P als omschreven omvat. Schrijf G = Alt(5). Nu is $|N_G(P):P| = 2$. Als $|N_N(P):P| = 1$, dan geldt $N_N(P) = P$, dus zelfs $Z(N_N(P)) = P$. De stelling van Burnside (2.3.2 en 2.3.3) levert een karakteristieke ondergroep van N, dus een normaaldeler van G, van orde $|N|/p$. Uit de minimaliteit van N en

Stap 1 volgt dat $|N| = p$, dus $N = P$, in strijd met $|N_G(P):P| = 2$. We konkluderen dat $|N_N(P):P| = 2$, zodat $N_N(P) = N_G(P)$. Uit het Frattini-argument (2.1.6(ii)) volgt nu $G = N_G(P)N = N_N(P)N = N$; het bewijs is voltooid. □

In Opgave 1.6.5 bleek Alt(5) isomorf met $Sl_2(K)$ voor K een lichaam met 4 elementen. In het vervolg (3.1.14) wordt ondermeer bewezen dat $PSl_2(K) = Sl_2(K)$ voor dit lichaam K enkelvoudig is. Dit zou als vierde bewijs voor de enkelvoudigheid van Alt(5) kunnen dienen.

2.3.6. PROPOSITIE. *Als G een enkelvoudige groep van orde 60 is, dan geldt* $G \cong Alt(5)$.

BEWIJS. Laat K een 2-Sylowgroep van zo'n groep G zijn en beschouw $H = N_G(K)$. Vanwege 2.3.2 geldt $H \neq K$ en vanwege de enkelvoudigheid van G is H een echte ondergroep. Bijgevolg is $|G/H| = p$ voor $p \in \{3,5\}$. Nu heeft G een getrouwe transitieve permutatievoorstelling van graad p (zie 1.4.8; waarom getrouw?), met andere woorden, op isomorfie na geldt $G \leq Sym(p)$. Uit overweging van ordes blijkt dat $p = 5$. Verder is $G \cap Alt(5)$ een ondergroep van Alt(5) van index ≤ 2. Was deze index 2, dan zou Alt(5) een echte normaaldeler hebben (zie 1.6.4), in strijd met 2.3.5. Er resulteert dat $G \cap Alt(5) = Alt(5)$, ofwel dat $G = Alt(5)$. □

OPGAVEN BIJ §2.3.

p is steeds een priemgetal.

*1. Schrijf C_p^n voor $\underbrace{C_p \times C_p \times \ldots \times C_p}_{n \text{ keer}}$. Zo'n groep heet *elementair abels*.

Bewijs:

(i) $Aut(C_p^n) \cong Gl_n(p)$.

(ii) Als G een niet-cyklische enkelvoudige groep van oneven orde is en als p de kleinste priemdeler van $|G|$ is, dan is p^3 deler van $|G|$.

(iii) Als G een niet-cyklische enkelvoudige groep van even orde is, dan is 8 of 12 een deler van $|G|$.

2. Bewijs dat Alt(5) de enige enkelvoudige groep van orde p^2qr is voor p,q,r verschillende priemgetallen.

3. Geef de karakteristieke ondergroepen van de twee niet-abelse groepen D_4 en Q_2.

4. Laat zien dat er geen enkelvoudige groep van orde 300 is.

5. (i) Met welke groep van orde 16 is de 2-Sylowgroep van $Sl_2(7)$ isomorf?
   (ii) Idem voor $Sym(\underline{6})$.

6. (i) Met welke groep van orde 16 uit het diktaat is een 2-Sylowgroep van $PSl_2(17)$ isomorf?
   (ii) Bepaal ook het type 3-Sylowgroep van $PSl_2(17)$.

7. Laat zien dat een groep van orde 2n (n oneven) een normaaldeler van index 2 heeft.

8. Bewijs dat er precies één groep van orde n is dan en slechts dan als $(n,\phi(n)) = 1$.

2.4. Groepen van kleine orde

In deze paragraaf zullen we de groepen van orde ≤ 23 behandelen.

2.4.1. LEMMA. *Iedere niet-abelse groep* G *van orde* 2p *(*p *priem* > 2*) is isomorf met* D_p.

BEWIJS. De p-Sylowondergroep van G is een cyklische normaaldeler van orde p. Verder omvat G een 2-Sylowgroep van orde 2, zodat $G \cong C_p \rtimes_\alpha C_2$ voor zeker niet-triviaal morfisme $\alpha: C_2 \to Aut(C_p)$. Aangezien $Aut(C_p) \cong C_{p-1}$ slechts één element van orde 2 heeft, is α uniek bepaald. □

2.4.2. LEMMA. *Laat* G *een niet-abelse groep van orde* 4p *zijn. Geef met* P *een* p*-Sylowondergroep van* G *aan.*

(i) *Als* $p > 4$, *dan is* $P \trianglelefteq G$;

(ii) *als* $P \trianglelefteq G$, *dan is* G *isomorf met* D_{2p}, Q_p *of* $C_p \rtimes_\alpha C_4$, *waar het morfisme* $\alpha: C_4 \to Aut(C_p)$ *gegeven is door* $\alpha(c)(x) = x^a$ $(c \in C_4 - C_2,\ x \in C_p)$, *met* $a \in \mathbb{N}$ *zodanig dat* $a^2 = -1 \bmod p$. *Het laatste geval doet zich uitsluitend voor als* $p = 1 \bmod 4$.

BEWIJS. (i). Omdat er $m = 1 \bmod p$ gekonjugeerden van P zijn, zouden er $m(p-1) \geq p^2 - 1 > 4p - 1 = |G| - 1$ elementen van orde p zijn als P geen normaaldeler was. Maar dan zou er geen element van orde 2 in G aanwezig zijn, in strijd met de Sylowstellingen.

(ii). Laat Q een 2-Sylowondergroep van G zijn. Dan is $G = P \rtimes Q$. Als $Q \cong C_2 \times C_2$, van omvat G een normaaldeler $\cong P \times C_2$ en volgt $G \cong D_{2p}$. Veronderstel daarom voor het vervolg dat $Q \cong C_4$, met voortbrenger $g \in Q$. Aangezien $Aut(C_p) \cong C_{p-1}$, resten er twee gevallen: hetzij

$$c_g(x) = x^{-1} \quad (x \in P) \text{ en } G \cong Q_p,$$

hetzij

$$c_g(x) = x^a \quad (x \in P) \text{ met } a^2 = -1 \bmod p.$$

Omdat de orde van c_g een deler van $|C_{p-1}| = p-1$ is, volgt nog in het laatste geval dat $4 \mid (p-1)$, ofwel dat $p = 1 \bmod 4$. □

VOORBEELD. Een niet-abelse groep van orde 20 is op isomorfie na één van de drie groepen D_{10}, Q_5, $C_5 \rtimes_\alpha C_4$, waar het morfisme $\alpha: C_4 \to \mathrm{Aut}(C_5)$ vastligt door $\alpha(c)x = x^2$ $(x \in C_5)$ voor zekere voortbrenger $c \in C_4$. Om dit in te zien passen we het voorgaande toe en vinden we dat ingeval $G \cong C_5 \rtimes_\alpha C_4$ geldt $a = 2,3$; de notatie is die van het lemma. Als $a = 3$, kiezen we $c = g^{-1} \in Q$ als voortbrenger en als $a = 2$ kunnen we met de keuze $c = g$ volstaan. Welk van de drie is isomorf met $\mathrm{AGl}_1(5)$?

2.4.4. PROPOSITIE. *Iedere niet-abelse groep* G *van orde* 12 *is isomorf met één van de volgende drie onderling niet-isomorfe groepen* D_6, Q_3 *en* $\mathrm{Alt}(\underline{4})$.

BEWIJS. Laat Q een 2-Sylowgroep en P een 3-Sylowgroep in G zijn. Als $P \trianglelefteq G$, dan is $G \cong D_6$ of Q_3 blijkens Lemma 2.4.2. Voor het vervolg kunnen we nu veronderstellen dat P geen normaaldeler is. Gevolg 2.3.2 sluit het geval $Q \cong C_4$ uit, zodat $Q \cong C_2 \times C_2$. Verder voldoet het aantal gekonjugeerden m van P weer aan $m \equiv 1 \bmod 3$ en zijn er 2m elementen van orde 3. Er volgt $2m \leq |G - Q| = 8$ en $m = 1,4$. Maar $m \neq 1$ omdat P geen normaaldeler is. Derhalve geldt $m = 4$. We konkluderen dat $Q \trianglelefteq G$; er is dus een niet-triviaal morfisme $\gamma: C_3 \to \mathrm{Aut}(C_2 \times C_2)$, zodat

$$G = Q \rtimes P \cong (C_2 \times C_2) \rtimes_\gamma C_3.$$

Deze situatie leidt tot een isomorfisme tussen G en $\mathrm{Alt}(\underline{4})$. □

In het voorafgaande hebben we afdoende aandacht besteed aan de groepen van orde 12, 16 en 20. We behandelen nu de overige ordes ≤ 23.

2.4.5. STELLING. *Iedere niet-abelse groep van orde* ≤ 23 $(\neq 12, 16, 20)$ *die niet-isomorf is met* D_m *of* Q_m *voor* $m \in \mathbb{N}$, *is op isomorfie na één der volgende groepen:*

- $(C_3 \times C_3) \rtimes_\alpha C_2$, $(C_3 \times C_3) \rtimes_\beta C_2$, *waar* $\alpha,\beta: C_2 \to \mathrm{Aut}(C_3 \times C_3)$ *morfismen zijn, vastgelegd door respektievelijk*

$$\alpha(c)x = x^{-1},\ \alpha(c)y = y^{-1} \text{ en } \beta(c)x = y,\ \beta(c)y = x$$

voor x,y *een tweetal voortbrengers van* $C_3 \times C_3$ *en* $c \in C_2 \setminus \{e\}$.

- $C_7 \rtimes_\gamma C_3$, *waar* $\gamma: C_3 \to \mathrm{Aut}(C_7)$ *het morfisme is, dat vastligt door*

$$\gamma(c)x = x^2 \quad (x \in C_7)$$

voor c *een vast gekozen voortbrenger van* C_3.

BEWIJS. Gezien de veronderstellingen en de Lemma's 2.4.1 en 2.4.2, komen slechts de volgende ordes nog voorbeschouwing in aanmerking: 8, 9, 15, 18, 21. Ordes 8 en 9 worden afgedaan door Opgave 8 en Opgave 12(ii) van §1.6. Ga zelf na wat er met de ordes 15 en 21 gebeurt.
Stel G heeft orde 18. Als een 3-Sylowgroep isomorf met C_9 is, moet $G \cong D_9$. Stel daarom dat P een ondergroep van G isomorf met $C_3 \times C_3$ is. Laat $a \in G$ een element van orde 2 zijn. Omdat $|G/P| = 2$, is P een normaaldeler in G. Verder omvat P een viertal ondergroepen van orde 3. Als a elke ondergroep van orde 3 invariant laat, moet $G \cong (C_3 \times C_3) \rtimes_\alpha C_2$ (ga na!). Stel dat $x,y \in P$ niet in elkaars inverse zijn en dat $c_a(x) = y$. Dan geldt $c_a(y) = x$ en ligt c_a verder vast op $\langle x,y \rangle = P$. We konkluderen dat G isomorf is met $(C_3 \times C_3) \rtimes_\beta C_2$. □

OPGAVEN BIJ §2.4.

1. Bewijs dat iedere eindige groep van orde pm met $p > m$ (p priem) een normale p-Sylowondergroep heeft.
2. Laat zien dat een niet-cyklische enkelvoudige groep van orde ≤ 100, orde 60 heeft.
3. Bepaal alle groepen van orde 24 (in totaal zijn er 15 niet-isomorfe). Aanwijzing: Maak onderscheid naar het aantal 3-Sylowgroepen. Zo dit aantal 1 is, is de onderhavige groep een semi-direkt produkt met C_3 als normaaldeler. Zo niet, konstrueer dan een permutatievoorstelling van de groep op de verzameling 3-Sylowgroepen en laat zien dat het beeld orde ≥ 12 heeft.
4. Bepaal alle groepen van orde 4p (p priem).

HOOFDSTUK III

PERMUTATIEGROEPEN

3.1. Primitiviteit en meervoudige transitiviteit

In deze paragraaf gaan we wat nader in op de theorie van de permutatiegroepen. Wordt een voor permutatiegroepen bekend begrip gehanteerd voor een permutatievoorstelling ϕ van een groep G, dan zal duidelijk zijn dat bedoeld wordt dat het begrip betrekking heeft op $\phi(G)$.

3.1.1. DEFINITIE. Een permutatiegroep G op een eindige verzameling V heet k-(*voudig-*)*transitief* (waar $k \leq |V|$) als voor ieder tweetal geordende stellen $(x_1,x_2,\ldots,x_k)$ en $(y_1,y_2,\ldots,y_k)$ van elk k verschillende elementen uit V er een $g \in G$ bestaat zodat $gx_i = y_i$ $(i \in \underline{k})$. Is $k \geq 2$, dan spreken we van een *meervoudig transitieve* permutatiegroep.

3.1.2. LEMMA. *Laat* G *een permutatiegroep op* V *zijn en laat* $k \geq 1$ *gegeven zijn met* $k \leq |V|$.

(i) G *is* k*-transitief op* V *dan en slechts dan als* G *transitief is en er een* $x \in V$ *is zodat de stabilisator* G_x (k-1)*-transitief op* $V - \{x\}$ *is.*

(ii) *Als dit het geval is, dan is* $|V|(|V|-1) \ldots (|V|-k+1)$ *een deler van* $|G|$.

BEWIJS. (i). Volgt rechtstreeks uit de definitie. Merk op dat iedere $x \in V$ voldoet voor het bewijs van "dan".

(ii). Komt neer op herhaalde toepassing van Stelling 1.4.8. □

3.1.3. VOORBEELDEN. Sym($\underline{n}$) is n-transitief op $\underline{n}$ en is vanzelfsprekend de enige groep met die eigenschap. Alt($\underline{n}$) is (n-2)-transitief op $\underline{n}$ als $n \geq 3$. De groep $PGl_n(q)$ is 2-transitief op de $(q^n-1)/(q-1)$ lijnen door 0; $PGl_2(q)$ zelfs 3-transitief.

Op soortgelijke wijze als in 1.4.8, waar transitieve permutatievoorstellingen van een groep bleken te corresponderen met ondergroepen, worden

nu de banen van een stabilisatorondergroep van een transitieve permutatiegroep teruggebracht tot een bij die ondergroep behorende partitie van de hele groep.

3.1.4. DEFINITIES. Als G een groep is en H een ondergroep van G, dan wordt voor $g \in G$ de deelverzameling HgH van G de *dubbele nevenklasse van* g *naar* H *in* G genoemd. "In dezelfde dubbele nevenklasse naar H bevat zijn" is een ekwivalentierelatie met als ekwivalentieklassen de dubbele nevenklassen naar H. Deze vormen dus een partitie van G. Het aantal dubbele nevenklassen naar H in G heet de *rang* van H in G. De *rang* van een transitieve permutatievoorstelling van G op een verzameling V is de rang van G_v in G voor zekere $v \in V$ (laat zien dat de definitie niet van v afhangt).

Het is duidelijk dat G zelf de enige ondergroep van G van rang 1 is. De volgende propositie geeft een interpretatie van de rang in termen van transitiviteit.

3.1.5. PROPOSITIE. *Als* G *een transitieve permutatiegroep op* V *is, dan is de rang van de bijbehorende permutatievoorstelling het aantal banen van* G_v *op* V *voor vaste* $v \in V$. *In het bijzonder is* G *2-transitief op* V *dan en slechts dan als voor elke* $g \in G - G_v$ *geldt* $G = G_v \cup G_v g G_v$.

BEWIJS. Laat $H = G_v$ en schrijf $G = H \cup Hg_2H \cup \ldots \cup Hg_tH$, waar t de rang van H in G is. De banen van H op V zijn de deelverzamelingen $B_i = \{gv \mid g \in Hg_iH\}$ van V. Verifieer dit zelf. □

3.1.6. VOORBEELDEN. Laat $k \leq n$. Dan heeft Sym(n) werkend op de ongeordende k-tupels uit n rang $\min(1+k, 1+n-k)$. De diëdergroep D_5 heeft vijf ondergroepen van index 5 en rang 3. (Welke?)

3.1.7. DEFINITIES. Laat G een permutatiegroep op een eindige verzameling V zijn. Een partitie $B_1 \dot\cup B_2 \dot\cup \ldots \dot\cup B_t = V$ heet *imprimitiviteitssysteem* voor G als $(\forall i \in \underline{t})(\forall g \in G)(\exists j \in \underline{t})(g(B_i) = B_j)$. De B_i heten dan *blokken* van het imprimitiviteitssysteem. Een blok B_i heet *triviaal* als $|B_i| = 0,1$ of $|V|$. Een imprimitiviteitssysteem heet *triviaal* als alle blokken ervan triviaal zijn. De groep G heet *imprimitief* op V als V een niet-triviaal imprimitiviteitssysteem voor G kent. Zo niet, dan is G *primitief* op V.

3.1.8. OPMERKINGEN.

- Als G primitief is, dan ook transitief. Immers de banen van de permutatie-

groep vormen een imprimitiviteitssysteem.

- Een transitieve permutatiegroep is niet noodzakelijk primitief. Een tegenvoorbeeld is de viergroep van Klein gezien als permutatiegroep op $\underline{4}$, zie 1.3.3.
- Anderzijds is een transitieve permutatiegroep van priemgraad wel primitief. Het bewijs hiervoor kan rechtstreeks geleverd worden (doe dit eens), maar kan ook via de volgende stelling gaan. Deze stelling brengt het begrip primitiviteit terug tot een uitspraak over een ondergroep.

3.1.9. STELLING. *Stel* G *is een transitieve permutatiegroep op* V *en* $v \in V$. *De groep* G *is primitief dan en slechts dan als* $G_v \leq G$ *een maksimale ondergroep van* G *is.*

BEWIJS. Laat een imprimitiviteitssysteem van G gegeven zijn en laat B het blok zijn dat v bevat. Als het systeem niet-triviaal is, dan is B niet-triviaal (want er is een niet-triviaal blok en G is transitief), en dus geldt met $H = \{g \in G \mid g(B) = B\}$ dat $G_v < H < G$ (ga zelf na waarom $H \neq G_v$ en $H \neq G$).

Als, andersom, een ondergroep H gegeven is met $G_v < H < G$, dan vormt $\{gHv \mid g \in G\}$ een niet-triviaal imprimitiviteitssysteem. Verifieer dit! □

3.1.10. KOROLLARIUM. *Als* G *een 2-voudig-transitieve permutatiegroep op* V *is, dan is* G *primitief op* V.

BEWIJS. Uit 3.1.5 blijkt dat de stabilisatorondergroep van een punt van V een maksimale ondergroep is. □

Voor later gebruik vermelden we

3.1.11. PROPOSITIE. *Laat* G *een primitieve permutatiegroep op* V *zijn en veronderstel* $\{e\} < H \trianglelefteq G$. *Dan is* H *transitief op* V.

BEWIJS. Kies $v \in V$ vast. Omdat $H \trianglelefteq G$, is HG_v een ondergroep van G. Als $HG_v \leq G_v$, dan $H \leq G_v$, dus $H = gHg^{-1} \leq gG_vg^{-1} = G_{gv}$, zodat $H \leq \bigcap_{w \in V} G_w = 1$, tegenspraak. Dus $HG_v \geq G_v$, zodat vanwege de maksimaliteit van G_v volgt $G = HG_v$. Uit de tweede isomorfiestelling (1.7.5) volgt dat $|G|/|H| = |G_v|/|G_v \cap H|$ zodat $|V| = |H|/|G_v \cap H|$, wat betekent dat de H-baan van v lengte $|V|$ heeft. Aldus blijkt H transitief op V. (Kunt u ook een argument geven dat Stelling 1.7.5 niet gebruikt?) □

Voor enkelvoudigheidsbewijzen is het volgende resultaat van Iwasawa erg handig.

3.1.12. PROPOSITIE. *Laat* G *een primitieve permutatiegroep op een eindige verzameling* V *zijn en laat* $v \in V$. *Als* G_v *een abelse normaaldeler* A *bezit zodanig dat* $G = \langle gAg^{-1} \mid g \in G \rangle$, *dan geldt*

(i) $1 < N \trianglelefteq G \Rightarrow N \geq D(G)$;

(ii) $G = D(G) \Rightarrow$ G *is enkelvoudig*.

BEWIJS. (i). Uit Propositie 3.1.11 volgt dat N transitief op V is, zodat $G = NG_v$. Er geldt zelfs $G = NA$, want als $g \in G$, dan zijn er $n \in N$ en $h \in G_v$ met $g = nh$, terwijl $gAg^{-1} = nAn^{-1} \leq NA$, zodat $G = \langle gAg^{-1} \mid g \in G \rangle \leq NA$. Met de tweede isomorfiestelling 1.7.5 volgt dat $G/N = NA/N \cong A/A\cap N$ abels is, waaruit $N \geq D(G)$ volgt (zie 1.6.12(iii)).

(ii). Volgt direkt uit (i). □

3.1.13. VOORBEELD. Alt($\underline{5}$) *is enkelvoudig* (vergelijk 2.3.5).

BEWIJS. $G = \mathrm{Alt}(\underline{5})$ werkt 2- (zelfs 3-)transitief op $\underline{5}$, dus ook primitief. $G_5 \cong \mathrm{Alt}(\underline{4})$ en heeft abelse normaaldeler V_4, de viergroep van Klein (zie 1.6.4). Dankzij (12)(34)(12)(35) = (435) is in te zien dat $\langle g V_4 g^{-1} \mid g \in G \rangle$ 3-kring (435) bevat en dus alle driekringen (we gebruiken hier dat de dubbele 2-kringen en de driekringen ieder slechts één konjugatieklasse opspannen). Omdat Alt($\underline{5}$) - getuige Opgave 1.5.9 - door haar driekringen wordt voortgebracht, is $G = \langle g V_4 g^{-1} \mid g \in G \rangle$. Voor x = (12)(45) en y = (13)(45) geldt $(123) = xyx^{-1}y^{-1} \in D(G)$. Bijgevolg is D(G) = G. De uitspraak volgt nu uit 3.1.12. □

3.1.14. PROPOSITIE. $\mathrm{PSl}_2(K)$ *is enkelvoudig als* $|K| > 3$.

BEWIJS. We maken gebruik van de 2-transitieve en dus primitieve voorstelling van $G = \mathrm{PSl}_2(K)$ op de $|K|+1$ lijnen door 0 in K^2. De stabilisator H in G van de lijn door $\binom{1}{0}$ is van de vorm $H = \left\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in K-\{0\}, b \in K\right\}$ en bevat de abelse normaaldeler $A = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in K\right\}$. Laat nu $N = \langle gAg^{-1} \mid g \in G \rangle$. We zullen eerst N = G bewijzen. Met $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ hebben we $gAg^{-1} \leq N$, dus $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \in N$ voor $b \in K$, zodat voor $a \in K-\{0\}$ volgt

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-1}-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} \in N.$$

Dus H is bevat in N. Maar $H \neq N$ en H is een maksimale ondergroep van G, dus $G = N$.

We zullen nu laten zien dat $G = D(G)$. Beschouw daartoe $g = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ voor willekeurige $b \in K$. Kies $c \in K-\{1\}$ zó dat $c^2 \neq 1$ (ga na dat hiertoe $|K| > 3$ noodzakelijk is) en schrijf $a = b/(c^2-1)$. Dan is

$$g = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} \in D(G).$$

Hieruit blijkt dat $A \leq D(G)$ en $G = \langle gAg^{-1} \mid g \in G \rangle \leq D(G)$. Propositie 3.1.12 doet de rest. □

3.1.15. DEFINITIE. Een permutatiegroep G op V heet *regulier* als G transitief is en voor $v \in V$ geldt $|G_v| = 1$.

Merk op dat de linksreguliere permutatievoorstelling van een willekeurige groep G de groep tot een reguliere permutatiegroep op G maakt.

3.1.16. STELLING. *Laat* G *een* t*-transitieve permutatiegroep op* V *van graad* $n = |V|$ *zijn. Als* N *een reguliere normaaldeler van* G *is, dan is* $t \leq 4$ *en geldt*

(i) $t = 2 \Rightarrow N \cong C_p^k$ *voor zekere* $k \in \mathbb{N}$ *en priem* p *met* $n = p^k$;

(ii) $t = 3 \Rightarrow n = 3$ *of* $n = 2^k$ *met* k *als in* (i);

(iii) $t = 4 \Rightarrow n = 4$.

BEWIJS. Laat $v \in V$ vast gekozen zijn en veronderstel dat $t \geq 2$.

STAP 1. *De permutatievoorstelling van* G_v *op* $V - \{v\}$ *komt overeen met de permutatievoorstelling* $\phi\colon G_v \to \mathrm{Sym}(N - \{e\})$, *gegeven door* $\phi(g)(x) = gxg^{-1}$ ($g \in G_v$, $x \in N - \{e\}$). *De groep* G_v *is dus op te vatten als een* (t-1)*-transitieve permutatiegroep op* $N^* = N - \{e\}$ *werkend door middel van konjugatie.*

BEWIJS. Merk op dat $N - \{e\}$ invariant is onder c_g voor $g \in G$, zodat $\phi(g) = c_g|_{N^*}$ een goed gedefinieerde afbeelding is. De overeenkomst tussen beide permutatievoorstellingen wordt bemiddeld door de bijektie $\beta\colon V - \{v\} \to N^*$, gedefinieerd door $\beta(w) = x \iff w = xv$ ($w \in V - \{v\}$, $x \in N^*$), met dien verstande dat $g(a) = b$ voor $a,b \in V - \{v\}$ en $g \in G_v$ korrespondeert met $\phi(g)\beta(a) = \beta(b)$.

STAP 2. Laat p een priemgetal en deler van de orde van N zijn. Omdat G_v transitief is ($t \geq 2$), heeft ieder element $\neq e \in N$ orde p. Dus N is een p-groep. Verder is $Z(N)$ invariant onder $\mathrm{Int}(G)$ en geldt $1 < |Z(N)|$, dus $N = Z(N)$ oftewel N is abels. (i) volgt nu rechtstreeks uit Propositie 2.2.5.

Als $t \geq 3$ en $p > 2$, kies dan $x \in N^*$ met $x \neq x^{-1}$. Omdat uit $\phi(g)x = x$ volgt dat $\phi(g)x^{-1} = x^{-1}$, geldt $N^* - \{x\} = (G_v)^{\phi}_{x} \cdot x^{-1} = \{x^{-1}\}$. Bijgevolg is $N^* = \{x, x^{-1}\}$, dus $|N| = 3$. Dit geeft (ii). Als $t \geq 4$, dan moet dus $p = 2$ zijn. Laat M een ondergroep van orde 4 van N zijn (ga na dat zo'n M bestaat). Uit de 3-transitiviteit van G_v op $N - \{e\}$ volgt dat ieder drietal elementen uit N^* tezamen met e isomorf beeld van M is en dus weer een ondergroep van N. Dit kan alleen als $M = N$. Vandaar (iii).

Uit $t \geq 4$ volgt krachtens (iii) nu ook $t \leq n = 4$, waarmee het bewijs voltooid is. □

3.1.17. VOORBEELD. Sym(4) heeft de reguliere normaaldeler V_4, de viergroep van Klein. Voorgaande stelling bewijst dat dit het enige voorbeeld is voor $t = 4$.

$AGl_n(K)$ werkt 2-transitief op K^n, met reguliere normaaldeler $A \cong (K^n,+,0) \cong C_p^{mn}$ voor zekere m, waar p de karakteristiek van K is (m heet de graad van het lichaam K over $\mathbb{Z}_p$).

Het belang van de reguliere normaaldelers moge blijken uit het volgende

3.1.18. LEMMA. *Als G een primitieve permutatiegroep op V zonder reguliere normaaldeler en met enkelvoudige stabilisatorondergroep G_v is ($v \in V$), dan is G zelf ook enkelvoudig.*

BEWIJS. Veronderstel dat N een niet-triviale normaaldeler is. Vanwege 3.1.11 is N dan transitief met stabilisator $N_v = N \cap G_v \trianglelefteq G_v$. Enkelvoudigheid van G_v houdt in dat $N_v = \{e\}$ of G_v. In het eerste geval zou N een reguliere normaaldeler zijn; uitgesloten. Dus $N_v = G_v$. Uit $|N/N_v| = |G/G_v| = |V|$ volgt $|N| = |N_v||V| = |G_v||V| = |G|$, zodat $N = G$. □

Het volgende resultaat werd in 1.6.10 reeds aangekondigd.

3.1.19. KOROLLARIUM. *Alt(n) is enkelvoudig voor* $n \geq 5$.

BEWIJS. Voor $n = 5$, zie 2.3.5. We voeren induktie naar n. Stel $n \geq 6$. De induktiehypothese is dat Alt(n-1) enkelvoudig is. Alt(n) is echter 4-transitief van graad > 4 en kan dus geen reguliere normaaldeler bezitten (vergelijk 3.1.16). Pas nu 3.1.18 toe. □

3.1.20. KOROLLARIUM. *De enige normaaldeler van* Sym(n) *voor* $n \geq 5$ *is* Alt(n).

BEWIJS. Als $N \trianglelefteq \mathrm{Sym}(\underline{n})$, bekijk dan $N \cap \mathrm{Alt}(\underline{n})$. Deze normaaldeler van $\mathrm{Alt}(\underline{n})$ kan niet $= \{e\}$ zijn, omdat dan $|N| = 2$, wat in strijd is met 3.1.11. Dus $N \geq \mathrm{Alt}(\underline{n})$, zodat $N = \mathrm{Alt}(\underline{n})$ of $\mathrm{Sym}(\underline{n})$. □

In 3.1.16 is al enige struktuur aangebracht in een 2-transitieve permutatiegroep G voor het geval dat G een reguliere normaaldeler bevat. We zullen ter afsluiting van deze paragraaf bewijzen dat zo G geen reguliere normaaldeler bevat, zij veel met een niet-abelse enkelvoudige groep van doen heeft.

3.1.20. STELLING. *Laat G een 2-transitieve permutatiegroep zonder reguliere normaaldelers zijn. Dan bevat G een niet-abelse enkelvoudige normaaldeler N zo dat op isomorfie na geldt* $N \trianglelefteq G \leq \mathrm{Aut}(N)$.

BEWIJS. We schrijven V voor de eindige verzameling waarop G 2-transitief werkt. Laat N een minimale normaaldeler van G zijn. Uit Opgave 1.8.12 en 1.6.17 volgt dat er enkelvoudige onderling isomorfe normaaldelers $N_1, N_2, \ldots, N_t$ van N bestaan, zo dat $N = N_1 \times N_2 \times \ldots \times N_t$. Uit 3.1.10 en 3.1.11 blijkt dat N transitief op V is. Vanwege Opgave 1.5.10(ii) en de uitsluiting van reguliere normaaldelers is N, en dus ook N_1, niet-abels. Laat H de stabilisator in G van een punt van V zijn. We bewijzen de stelling in 6 stappen.

STAP 1. $G = HN$ *met* $H \cap N > \{1\}$ *en* $H \cap N_i < N_i$ *voor* $i \in \underline{t}$. *Verder werkt* H *via konjugatie transitief op* $\{N_i \mid i \in \underline{t}\}$.

BEWIJS. Omdat HN de maksimale ondergroep H strikt omvat (N is namelijk transitief op V) geldt $G = HN$. Uit $H \cap N = \{1\}$ zou volgen dat N een reguliere normaaldeler is. Uit Opgave 1.8.10 volgt dat $\{N_i \mid i \in \underline{t}\}$ de volledige verzameling minimale normaaldelers van N is. Deze verzameling wordt dus door H onder konjugatie invariant gelaten. Mocht $W \subset \underline{t}$ een echte niet lege deelverzameling van $\underline{t}$ zijn zo dat $\{N_i \mid i \in W\}$ ook invariant onder H is, dan zou het produkt der N_i voor $i \in W$ een niet triviale normaaldeler van G strikt bevat in N zijn, tegenspraak. Dus H werkt transitief op $\{N_i \mid i \in \underline{t}\}$. Rest te bewijzen dat $H \cap N_i < N_i$. Stel van niet, dus $N_i \leq H$ voor zekere $i \in \underline{t}$. Dan volgt na konjugatie met elementen uit H dat $N_i \leq H$ voor alle $i \in \underline{t}$, zodat $N \leq H$. Maar dit is in strijd met $G = HN$. □

STAP 2. *Voor elke* $g \in N - H$ *geldt* $N - (N \cap H) = \bigcup_{h \in H} hgh^{-1}(N \cap H)$.

BEWIJS. Laat $x \in N - N \cap H$. Vanwege Propositie 3.1.5 is dan $x \in (HgH) \cap N$. Er zijn dus $h_1, h_2 \in H$ zo dat $x = h_1 g h_2 \in N$. Omdat $N \trianglelefteq G$ volgt $h_1 h_2 \in N$. Zeg $n = h_1 h_2$. Dan is $n \in N \cap H$ en geldt $x = h_1 g h_1^{-1} n \in h_1 g h_1^{-1} (N \cap H)$. □

STAP 3. *Veronderstel* $t > 1$. *Voor elke* $i \in \underline{t}$ *is de projektie* $\pi_i : H \cap N \to N_i$ *een surjektief morfisme.*

BEWIJS. Stel van niet. Uit Stap 1 volgt dat π_i voor geen $i \in \underline{t}$ surjektief is. Kies $u_i \in N_i - \pi_i(N \cap H)$ voor $i = 1,2$ en beschouw $u = u_1 u_2 \in N$. Pas nu Stap 2 toe op u met $g = u_1$. Dan blijkt dat $u_1 u_2 = h u_1 h^{-1} n$ voor zekere $n \in N \cap H$. Nu is er vanwege Stap 1 een $j \in \underline{t}$ met $h u_1 h^{-1} \in N_j$ zodat $u_1 = \pi_1(n)$ als $j \neq 1$ en $u_2 = \pi_1(n)$ als $j \neq 2$. Elk van beide gevallen levert een tegenspraak met de keuze van u_i. □

STAP 4. *Als* $t > 1$, *dan geldt voor elke* $i \in \underline{t}$ *dat* $H \cap N_i = \{1\}$.

BEWIJS. Stel $x \in N_i \cap H - \{1\}$. Dan volgt uit Stap 3

$$\langle hxh^{-1} \mid h \in N \cap H \rangle = \langle hxh^{-1} \mid h \in N_i \rangle = N_i$$

omdat N_i enkelvoudig is. Maar dit impliceert dat $N_i \leq H$, wat al in stap 1 uitgesloten is. □

STAP 5. $t = 1$.

BEWIJS. Stel van niet. Kies $g_1 \in N_1$ van orde p (priem) en $g_2 \in N_1$ van orde q (priem) met $p \neq q$ (Ga na dat dit kan omdat N_1 niet-abels en enkelvoudig is, zie 2.2.2). Omdat $g_2 \notin H$ (zie stap 4) is er een $h \in H$ en een $n \in N \cap H$ met $g_2 = h g_1 h n^{-1}$ (zie Stap 2). Laat $j \in \underline{t}$ zo zijn dat $h g_1 h^{-1} \in N_j$. Veronderstel dat $j = 1$. Dan is $n \in N_1 \cap H = \{1\}$ volgens Stap 4, zodat $g_2 = h g_1 h^{-1}$ in strijd met de ordes van g_2 respectievelijk g. Dus $j > 1$, zeg $= 2$. Dan is $n = (h g_1^{-1} h^{-1}) g_2 \in N_2 N_1 \cap H$, dus $n^p = g_2^p$ is bevat in $N_1 \cap H$ van orde q; tegenspraak met Stap 4. Dus inderdaad $t = 1$. □

STAP 6. Einde van het bewijs.

We hebben al een niet-abelse enkelvoudige normaaldeler $N = N_1$ van G verkregen. Er rest dus te bewijzen dat het natuurlijke morfisme $G \to Aut(N)$ injektief is. Naar opgave 1.6.16 komt dit neer op het bewijs dat $C_G(N)$ triviaal is. Dit is als volgt in te zien. $C_G(N)$ is een normaaldeler van G. Stel zij bevat een niet-triviaal element h van de stabilisator-ondergroep. Omdat N een transitieve groep op V is en omdat $N \leq C_G(h)$, moet vanwege Opgave 1.5.10(i) elk punt van V vast punt van h zijn, met andere woorden $h = 1$. De konklusie is dat $C_G(N) \neq \{1\}$ betekent dat $C_G(N)$ een reguliere normaaldeler is. Dit is echter uitgesloten door de voorwaarden in de stelling. Klaar. □

OPGAVEN BIJ §3.1.

1. Wat is de maksimale $k \in \mathbb{N}$ waarvoor $Gl_n(p)$ k-transitief op $\mathbb{Z}_p^n - \{0\}$ is? ($p,n \in \mathbb{N}$, p priem.)

2. Bewijs dat als G een enkelvoudige 2-transitieve permutatiegroep van graad 6 is, G isomorf is met $Alt(\underline{5})$ of $Alt(\underline{6})$.

3. Als G een reguliere en primitieve permutatiegroep is, dan is de graad van G een priemgetal.

4. Laat zien dat als G een transitieve permutatiegroep op een gegeven eindige verzameling V is met transitieve ondergroep H, dan geldt $G = G_v H = HG_v$ voor iedere $v \in V$.

5. (i) Wat zijn de graden van de meervoudig-transitieve permutatievoorstellingen van $Alt(\underline{5})$?
   (ii) Wat zijn de graden van de primitieve permutatievoorstellingen van $Alt(\underline{5})$?

6. Als Opgave 5, maar nu voor $PSl_2(7)$.

*7. Laat G een transitieve permutatiegroep op een gegeven eindige verzameling V zijn en geef voor $g \in G$ met $\alpha(g)$ het aantal punten in V aan dat door g vastgehouden wordt (dus $\alpha(g) = \#\{v \in V \mid g(v) = v\}$). Toon aan:
   (i) $\sum_{g \in G} \alpha(g) = |G|$;
   (ii) G is 2-transitief $\iff \sum_{g \in G} \alpha(g)^2 = 2|G|$.

8. Laat G een primitieve permutatiegroep op een eindige verzameling V zijn en laat W een echt deel van V zijn. Bewijs achtereenvolgens:

(i) Als $w \in W$, dan geldt $\bigcap_{\substack{g\in G \\ w\in g(W)}} g(W) = \{w\}$.

(Aanwijzing: het linkerlid is een blok, d.w.z. na transformatie met $h \in G$ (willekeurig) is de doorsnede met het oorspronkelijke linkerlid leeg of het hele linkerlid.)

(ii) Als $v,w \in W$ met $v \neq w$, dan is er een $g \in G$ zodat $g(v) \in W$ en $g(w) \in V - W$.

(iii) Als $|W| > 1$ en $Sym(W) \leq G$, dan is $G = Sym(V)$.

(Aanwijzing: Induktie naar $|V| - |W|$. Als $|W| < |V|$ en $v,w \in W$ met $v \neq w$, dan (met (ii)) $g(v) \in W$, $g(w) \notin W$ voor zekere $g \in G$. Bewijs nu m.b.v. Opgave 1.1.10 dat $Sym(W \cup g(W)) = \langle Sym(W), g\ Sym(W)g^{-1} \rangle \leq G$.)

(iv) Als $|W| > 2$ en $Alt(W) \leq G$, dan is $Alt(V) \leq G$.

(Aanwijzing: Als in (iii); gebruik Opgave 2.1.4.)

(v) Als $(v\ w) \in G$ voor zekere $v,w \in V$ met $v \neq w$, dan geldt $G = Sym(V)$.

(vi) Als $(u\ v\ w) \in G$ voor zekere $u,v,w \in V$ (onderling $\neq$), dan geldt $G \geq Alt(V)$.

9. (i) Laat G een t-transitieve permutatievoorstelling op V van graad $|V| = n$ zijn. Stel dat $H \leq G$ de groep is van alle elementen in G die een gegeven t-tal punten uit V puntsgewijs vasthouden en dat P een p-Sylow-groep van H is. Bewijs dat als P nu w ($\geq t$) punten vasthoudt, dan is $N_G(P)$ t-transitief op deze w punten.

(ii) Bewijs dat er geen 4-transitieve permutatiegroep op 10 punten bestaat van orde $10 \cdot 9 \cdot 8 \cdot 7$.

3.2. De permutatievoorstellingen van $Sl_2(8)$

Bij wijze van voorbeeld zullen we de ondergroepen van $Sl_2(8)$ bepalen. Daarmee zijn (zie 1.4.8) ook de transitieve permutatievoorstellingen van $Sl_2(8)$ bekend.

3.2.1. Het lichaam K van orde 8. Dit lichaam wordt als volgt beschreven. $K = \{a+b\sigma+c\sigma^2 \mid a,b,c \in \mathbb{Z}_2\}$ met σ wortel (= oplossing) van de vergelijking $\sigma^3+\sigma+1 = 0$. Ga zelf na dat deze gelijkheid ook de vermenigvuldiging op K vastlegt. Het element σ is een voortbrenger van de cyklische groep $(K-\{0\},*,1)$ van orde 7; vergelijk Opgave 1.1.11.

3.2.2. De konjugatieklassen van $Sl_2(K)$. Analoog aan 1.5.5 kan men de centralisatoren en de konjugatieklassen van elementen in $Sl_2(K)$ bepalen. We geven hier alleen het resultaat. Laat $x_\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ voor $\alpha \in K$, $y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $d = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}$. Dan hebben we centralisatoren en konjugatieklassen als af te lezen uit onderstaande tabel.

representant	1	x_1	yx_1	yx_σ	yx_{σ^2}	yx_{σ^4}	yx_{σ^3}	yx_{σ^5}	yx_{σ^6}
inklassebenaming	1	2	3	9_1	9_2	9_3	7_1	7_2	7_3
centralisator $\cong$	G	C_2^3	C_9	C_9	C_9	C_9	C_7	C_7	C_7
orde van de inklasse	1	63	56	56	56	56	72	72	72

3.2.3. De lokale ondergroepen van $Sl_2(K)$. Omdat $Sl_2(K)$ orde $7\cdot8\cdot9$ heeft, bevat ze Sylowondergroepen van orde 7, 8 en 9. Die van orde 7 en 9 zijn cyklisch, die van orde 8 zijn isomorf met C_2^3; dit valt immers al uit de tabel in 3.2.2 af te lezen. We zullen eerst de normalisatoren van deze Sylowgroepen bepalen.

Schrijf $G = Sl_2(K)$ en laat P_7 een 7-Sylowgroep van G zijn. Blijkens bovenstaande tabel zijn er $3\times72 = 216$ elementen van orde 7 in G, die elk in slechts één 7-Sylowgroep voorkomen. Er zijn dus $216/6 = 36$ 7-Sylowondergroepen van G. Omdat ze alle gekonjugeerd zijn, heeft de normalisator van zo'n groep orde $7\times8\times9/36 = 14$. De centralisator van een element van orde 7 is van orde 7. Bijgevolg is $N_G(P) \cong C_7 \rtimes C_2$ (gebruik Lemma 2.4.1). Stel zelf vast dat de normalisator van een 3-Sylowondergroep P_9 en van een 2-Sylowondergroep P_8 isomorf is met $C_9 \rtimes C_2$, respektievelijk $C_2^3 \rtimes C_7$ (de laatste groep zijn we ook in 3.1.14 tegengekomen).

Uit de tabel van 3.2.2 valt al te lezen dat $N_G(x_1) = C_G(x_1) \cong C_2^3 \cong P_8$. Nu de normalisator van een element van orde 3, $N_G(\langle yx_1\rangle) \geq N_G(P_9) \cong$ $\cong C_9 \rtimes C_2$, als tenminste $P_9 \ni yx_1$ gekozen is. Anderzijds (zie Opgave 1.6.16) is $N_G(\langle yx_1\rangle)/C_G(yx_1)$ op te vatten als een ondergroep van $\mathrm{Aut}(\langle yx_1\rangle) \cong C_2$, dus $N_G(\langle yx_1\rangle)$ van orde een deler van $2\cdot9 = 18$. Derhalve volgt $N_G(\langle yx_1\rangle) = N_G(P_9)$.

Rest te bepalen $N_G(P)$ voor P een groep van orde 4. Zonder de algemeenheid te schaden mogen we aannemen dat $P \leq P_8$. Maar P_8 is ook uniek met deze eigenschap; dit blijkt bijvoorbeeld uit $P_8 = C_G(g)$ voor $g \in P-\{1\}$. Ga zelf na dat hieruit $N_G(P) = P_8$ volgt.

3.2.4. De niet-lokale ondergroepen van $Sl_2(K)$. Laat H een echte ondergroep van G zijn. Stel eerst dat H de 7-Sylowgroep P_7 ($\cong C_7$) bevat. Dan is het aantal 7-Sylowgroepen in H een deler van $8\cdot9$ en $= 1 \bmod 7$, dus 1, 8 of 36.

Als dit aantal 1 is, dan is P_7 normaal in H, dus $H = P_7$ óf $H = N_G(P_7)$. Als het 36 is, dan bevat H de normaaldeler van G voortgebracht door alle elementen van orde 7, dus is H = G vanwege de enkelvoudigheid van G. We mogen er dus van uitgaan dat H precies 8 7-Sylowgroepen heeft. In dit geval heeft H index ≤ 9 in G. Maar omdat G een element van orde 9 bevat en G enkelvoudig is, heeft iedere niet-triviale transitieve voorstelling van G graad ≥ 9, zodat $|H| = |G|/9 = 7 \cdot 8$. Omdat er $8 \times 6 = 48$ elementen van orde 7 in H zijn, vormen de resterende $56 - 48 = 8$ elementen een normale 2-Sylowondergroep van H. Bijgevolg is H de normalisator van een 2-Sylowondergroep van G en dus lokaal.

Voor de speurtocht naar niet-lokale ondergroepen H van G kunnen we ons dus beperken tot het geval waarin $|H|$ een deler van $8 \cdot 9$ is. Stel $P_8 \leq H$. Uit $N_H(P_8) = N_G(P_8) \cap H = P_8$ volgt met de Stelling 2.3.1 dat er een normale 3-ondergroep Q in H is met $H = Q \rtimes P_8$. Als $|Q| = 9$ dan volgt een tegenspraak met $|N_G(Q)| = 18$, en als $|Q| = 1$, dan is H een 2-Sylowgroep van G. Derhalve resteert $|Q| = 3$. Maar $N_H(Q)/C_H(Q)$ kan ingebed worden in Aut(Q) van orde 2, zodat $C_H(Q)$ een veelvoud van 12 is. Dit is echter in strijd met de orde van $C_G(yx_1)$. We konkluderen dat alle ondergroepen in G, die orde een veelvoud van 8 hebben, bekend zijn.

Stel nu dat een 2-Sylowgroep P van H orde 4 heeft. Dan is P bevat in een 2-Sylowgroep, zeg P_8, van G. Omdat, naar in 3.2.3 bleek, $N_G(P) = P_8$, is $N_H(P) = P$. We passen Stelling 2.3.1 weer toe om af te leiden dat $H = N \rtimes P$ voor een ondergroep N van G van orde een deler van 9. Maar $|N| = 3$; 9 is uitgesloten vanwege $N_G(N) = |N_G(P_9)| = 18$ en $|N| = 1$ levert $H = P$. Er zijn dus geen niet-lokale groepen met $4 \mid |H|$.

Als tenslotte $|H| = 2m$ met m deler van 9, dan heeft H een normaaldeler R van orde m (zie Opgave 2.3.7) en volgt $H = N_G(R)$.

In het licht van 3.1.9 kunnen we het voorgaande als volgt samenvatten:

3.2.5. PROPOSITIE. $Sl_2(8)$ *heeft slechts drie primitieve permutatievoorstellingen, elk behorend bij een lokale ondergroep, te weten:*

1e *de normalisator van een 2-Sylowondergroep, van rang 2 (zelfs 3-transitief) en graad 9;*

2e *de normalisator van een 3-Sylowondergroep, van rang 4 en graad 28;*

3e *de normalisator van een 7-Sylowondergroep, van rang 5 en graad 36.*

Werk zelf de nog niet bewezen details uit.

3.2.6. Een uitbreiding van $Sl_2(8)$. Het lichaam K heeft eèn automorfismengroep van orde 3; met α geven we het Frobenius-automorfisme van K aan dat beschreven wordt door $\alpha(x) = x^2$ $(x \in K)$. Het voorschrift $\alpha^v\binom{x}{y} = \binom{\alpha(x)}{\alpha(y)}$ $(x,y \in K)$ maakt van α een morfisme van de optelgroep van K^2 (ofwel een lineaire transformatie van de 6-dimensionale $\mathbb{Z}_2$-vektorruimte K^2). De groep $Sl_2(8)$ wordt nu uitgebreid door $<\alpha^v>$ toe te voegen. Preciezer: we beschouwen de groep Γ voortgebracht door $Sl_2(8)$ en $<\alpha^v>$. Omdat $\alpha^v\begin{pmatrix}a & b\\ c & d\end{pmatrix}(\alpha^v)^{-1} = \begin{pmatrix}\alpha(a) & \alpha(b)\\ \alpha(c) & \alpha(d)\end{pmatrix}$ voor $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in Sl_2(K)$, is $Sl_2(8)$ een normaaldeler in Γ. Er volgt onmiddellijk dat $\Gamma = Sl_2(K) \rtimes <\alpha^v> \cong Sl_2(K) \rtimes C_3$. Omdat Γ lijnen door O in lijnen door O overvoert, heeft zij ook een 3-transitieve permutatievoorstelling van graad 9. De normalisator van een 3-Sylowgroep van Γ heeft index 28 en is van rang 2. Laat zelf zien dat Γ een primitieve permutatievoorstelling van graad 36 heeft en bereken de rang.

3.2.7. OPMERKINGEN. De ondergroepen van $PSl_2(K)$ voor K een willekeurig eindig lichaam zijn reeds in 1901 uitgerekend door L.E. Dickson.

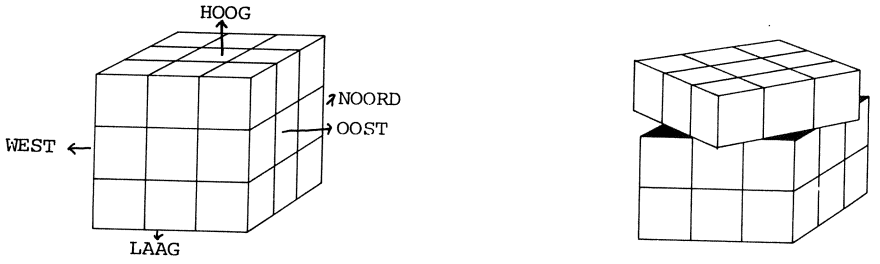
De permutatievoorstellingen van Γ van graad 28 en 36 leiden tot voorbeelden van veel bestudeerde kombinatorische strukturen, te weten 2-designs en (resp.) sterk reguliere grafen (zie § 3.4).

OPGAVEN BIJ §3.2.

1. Bewijs dat Γ uit 2.3.6 isomorf is met $Aut(Sl_2(8))$.
2. Bepaal alle ondergroepen van Γ uit 3.2.6.

3.3. De magische kubus

De magische kubus is een grote kubus die opgebouwd is uit een aantal kleinere kubussen. De lengte van een ribbe van een kleine kubus is 1/3 van de lengte van een ribbe van de grote kubus (zie Figuur 1a). Het "magische" van de kubus is het feit dat ieder van de zes zijvlakken draaibaar is om de middelste kleine kubus van het betreffende zijvlak (zie Figuur 1b), zonder dat de grote kubus bij omhoogwerpen uiteen valt in 27 kleine.



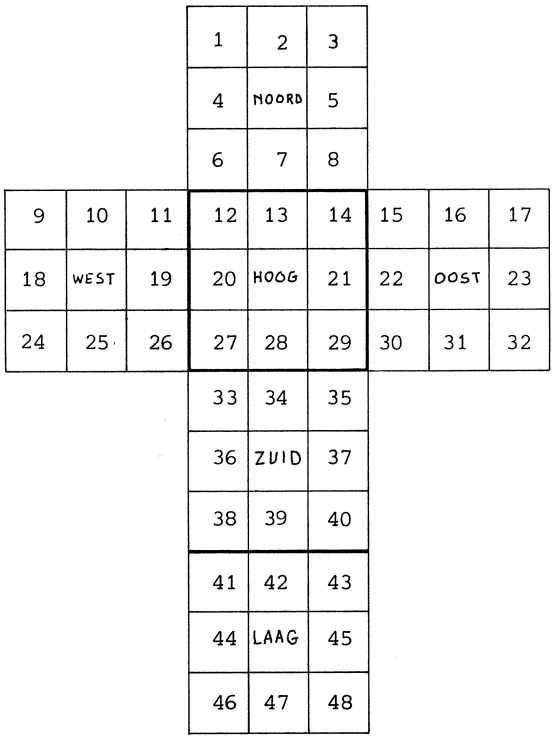
Figuur 1

De zijvlakjes van de kleine kubussen zijn op zodanige wijze gekleurd dat ieder van de zes zijvlakken van de grote kubus één kleur heeft. Het probleem is nu de kubus in deze begintoestand terug te brengen als deze door een aantal onbekende draaiingen verstoord is. Om de procedure die dit bewerkstelligt en de permutatiegroep op de zijvlakjes te kunnen beschrijven, hebben we de zijvlakken van de kubus van namen voorzien (zie Figuur 1a). De permutatie op de zijvlakjes die ontstaat door een bepaald zijvlak in kloksgewijze richting over 90° te draaien zullen we met de naam van het betreffende zijvlak aangeven. Als we de zijvlakjes nummeren zoals in Figuur 2 is aangegeven, dan wordt bijvoorbeeld de permutatie HOOG gegeven door

$$\text{HOOG} = (6,15,35,26)(8,30,33,11)(12,14,29,27)(7,22,34,19)(13,21,28,29).$$

Beschrijf zelf eens op deze manier de permutatie OOST.

Met V geven we de verzameling van de 48 zijvlakjes aan, dus $V = \{1,2,\ldots,48\}$. Met U geven we de verzameling van zijvlakjes van de hoekkubussen aan, $U = \{1,3,6,8,\ldots,48\}$ en met T de verzameling van zijvlakjes van de randkubussen, $T = \{2,5,\ldots,47\}$. We zullen nu eerst de ondergroep G van Sym(V) beschrijven die wordt voortgebracht door de zes basispermutaties HOOG, LAAG, NOORD, OOST, ZUID, WEST.



Figuur 2

3.3.1. De groep van de magische kubus

Het is direkt duidelijk dat G niet transitief is op V, want een zijvlakje van een randkubus kan nooit overgevoerd worden in een zijvlakje van een hoekkubus. Anderzijds gaat men makkelijk na dat G transitief is op zowel U als T, d.w.z. U en T zijn de banen van G op V. De zijvlakjes van een kleine kubus worden overgevoerd in de zijvlakjes van een andere kleine kubus, d.w.z. G is imprimitief op zowel U als T en elke kleine kubus korrespondeert met een blok van het imprimitiviteitssysteem. Laat $\bar{U}$ (resp. $\bar{T}$) de verzameling zijn van de hoekkubussen (resp. randkubussen) en $\bar{G}$ de door G op $\bar{V} := \bar{U} \cup \bar{T}$ geïnduceerde permutatiegroep. Als K de ondergroep van G is die als de identiteit op $\bar{V}$ werkt, dan is volgens 1.6.6

$$\bar{G} \simeq G/K.$$

We beschouwen nu eerst $\bar{G}$. Laat $\bar{G}_{\bar{U}}$ ($\bar{G}_{\bar{T}}$) de ondergroep van $\bar{G}$ zijn die $\bar{U}$ ($\bar{T}$) puntsgewijs vastlaat. Daar $\bar{U} \cap \bar{T} = \emptyset$ kommuteert $\bar{G}_{\bar{U}}$ met $\bar{G}_{\bar{T}}$. Bovendien is $\bar{G}_{\bar{U}} \cap \bar{G}_{\bar{T}} = \bar{G}_{\bar{U}\cup\bar{T}} = \bar{G}_{\bar{V}} = 1$ zodat $\bar{G}_{\bar{U}} \times \bar{G}_{\bar{T}} \lesssim \bar{G}$. Herhaald toepassen van 3.1.2 laat zien dat $\bar{G}$ 3-transitief is op zowel $\bar{U}$ als $\bar{T}$. Achtereenvolgens uitvoeren van HOOG, OOST, HOOG^{-1}, OOST^{-1}, d.w.z. het uitvoeren van $O^{-1}H^{-1}OH$ met H := HOOG etcetera, geeft een 3-cykel op $\bar{T}$ en een produkt van twee 2-cykels op $\bar{U}$. Hieruit volgt dat $\bar{G}_{\bar{U}}$ de 3-cykel $(\bar{O}^{-1}\bar{H}^{-1}\bar{O}\bar{H})^2$ bevat. Met Opgave 3.1.8 volgt nu dat $\text{Alt}(\bar{T}) \lesssim \bar{G}_{\bar{U}}$. Daar H,L,N,O,Z,W op $\bar{V}$ even permutaties induceren, geldt zelfs $\text{Alt}(\bar{T}) \simeq \bar{G}_{\bar{U}}$. Op dezelfde manier volgt $\text{Alt}(\bar{U}) \simeq \bar{G}_{\bar{T}}$ (geef een 3-cykel in $\bar{G}_{\bar{T}}$!). Hiermee is aangetoond dat $\text{Alt}(\bar{U}) \times \text{Alt}(\bar{T}) \lesssim \bar{G}$. Elke basispermutatie induceert op zowel $\bar{U}$ als op $\bar{T}$ een oneven permutatie (namelijk een 4-cykel). De door $\bar{G}$ op $\bar{U}$ ($\bar{T}$) geïnduceerde permutatiegroep $\bar{G}/\bar{G}_{\bar{U}}$ ($\bar{G}/\bar{G}_{\bar{T}}$) is dan ook isomorf met $\text{Sym}(\bar{U})$ ($\text{Sym}(\bar{T})$) en

$$\bar{G} \simeq (\text{Sym}(\bar{U}) \times \text{Sym}(\bar{T})) \cap \text{Alt}(\bar{V}).$$

Meer in het bijzonder volgt dat $|\bar{G}| = \frac{1}{2}\cdot 8!\cdot 12!$

We zullen nu de groep K beschrijven. Laat K_U de ondergroep van K zijn die U puntsgewijs vastlaat, K_T de ondergroep van K die T puntsgewijs vastlaat. Het is direkt duidelijk dat $K_U \lesssim \mathbb{Z}_2^{12}$ en $K_T \lesssim \mathbb{Z}_3^8$. Omdat de basispermutaties op T even permutaties induceren kan K_U geen 2-cykel bevatten, dus $K_U \neq \mathbb{Z}_2^{12}$. We zullen later zien dat K_U een element bevat dat twee randkubussen "omklapt" (de zogenaamde "monoflip"). Daar $\bar{G}$ 2-transitief is op $\bar{T}$ volgt dat voor ieder even aantal randkubussen er een element in K_U is dat die randkubussen omklapt. Dus $K_U \simeq \mathbb{Z}_2^{11}$. Om K_T te bepalen nummeren we de hoekkubussen van 1 t/m 8 en in iedere hoekkubus voorzien we de drie zijvlakjes kloksgewijs van de getallen $1,\omega,\omega^2$ waarbij $\omega = \exp(2\pi i/3)$. Aan iedere door G op U geïnduceerde permutatie a kennen we nu een matrix $M_a := (\delta_{i,a(j)}\omega^{k_i})_{i,j\in\underline{8}}$, toe, waarbij $k_i \in \{0,1,2\}$ gegeven wordt door: na uitvoeren van de permutatie a heeft in hoekpunt i het zijvlakje dat eerst label 1 had nu label ω^{k_i}, i = 1,...,8 (d.w.z. M_a is de permutatiematrix die korrespondeert met de door a op $\bar{U}$ geïnduceerde permutatie, waarbij in rij i de " 1 " vervangen is door ω^{k_i}). Men gaat gemakkelijk na dat de afbeelding $a \mapsto M_a$ een monomorfisme is (d.w.z. deze afbeelding is 1-1 en $M_a \circ M_b = M_{ab}$, waarbij $\circ$ de gewone matrixvermenigvuldiging is). Bovendien geldt voor elk van de basispermutaties a dat $\sum k_i \equiv 0 \pmod 3$, dus $\det(M_a) = \pm 1$. Dus geldt voor iedere permutatie a dat $\det(M_a) = \pm 1$, dus $\sum k_i \equiv 0 \pmod 3$.

Meer in het bijzonder korrespondeert een element $a \in K_T$ met een diagonaalmatrix $M_a = \text{diag}[\omega^{k_1},\omega^{k_2},\ldots,\omega^{k_8}]$ met $\sum k_i = (\text{mod } 3)$. We zullen nog zien dat er een element in K_T is dat precies twee hoekkubussen verdraait, de ene rechtsom en de andere linksom (de zogenaamde "monotwist"). Dus $\text{diag}[\omega,\omega^2,1,1,1,1,1,1] \in K_T$ en daar $\bar{G}$ 2-transitief is op $\bar{U}$ is iedere $\text{diag}[\omega^{k_1},\ldots,\omega^{k_8}]$ met $\sum k_i = 0 \pmod 3$ element van K_T. Dus $K_T \simeq \mathbb{Z}_3^7$ en $K = K_U \times K_T \simeq \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$. Hieruit volgt dat $|K| = 2^{11}\cdot 3^7$ en dus dat $|G| = |\bar{G}||K| = \frac{1}{2}\cdot 8!\cdot 12!\cdot 2^{11}\cdot 3^7$,

$$|G| = 2^{27}\cdot 3^{14}\cdot 5^3\cdot 7^2\cdot 11 = 43252\ 00327\ 44898\ 56000 \approx 4{,}3\cdot 10^{19}.$$

In feite is G het semidirekte produkt van $\bar{G}$ en K. Dit kunnen we als volgt inzien. Label de vlakjes van ieder hoekpunt weer met $1,\omega,\omega^2$ en de vlakjes van iedere randkubus met 1 en -1. Zoals we gezien hebben zijn er $2^{11}\cdot 3^7$ verschillende labelings in een baan van G. Laat H de stabilisator zijn van een labeling; dan heeft H orde $|H| = |G|/2^{11}\cdot 3^7 = |G|/|K|$ en $H \cap K = \{e\}$, want een element dat alle kubussen op hun plaats laat en alle labelings is de identiteit. Dus $G = K \rtimes H$ en $\bar{G} \simeq G/K \simeq H$ volgens 1.8.11.

3.3.2. Een algoritme voor de magische kubus

We geven een van J.H. Conway afkomstig algoritme om de kubus in haar begintoestand terug te brengen.

STAP 1. Breng in één zijvlak alle kleine kubussen op hun plaats (in de juiste oriëntatie!). Dit vereist enige oefening maar mag verder geen probleem opleveren. Het betreffende zijvlak wordt van nu af aan het ondervlak (= LAAG).

STAP 2. Breng de middenlaag in orde. Dit kan met de volgende permutaties:

a) Voer achtereenvolgens uit: HOOG, OOST, HOOG^{-1}, OOST^{-1}, HOOG^{-1}, ZUID^{-1}, HOOG, ZUID. We krijgen dus de permutatie $Z\ H\ Z^{-1}\ H^{-1}\ O^{-1}\ H^{-1}\ O\ H$.

b) Voer achtereenvolgens uit: HOOG^{-1}, ZUID^{-1}, HOOG, ZUID, HOOG, OOST, HOOG^{-1}, OOST^{-1}. We krijgen nu de permutatie $O^{-1}\ H^{-1}\ O\ H\ Z\ H\ Z^{-1}\ H^{-1}$.

Het effekt van a) en b) is dat het ondervlak ongewijzigd blijft, terwijl in de middenlaag één randkubus wordt vervangen door een randkubus uit de bovenste laag, maar verder ongewijzigd blijft (zie Figuur 3).
Merk op dat we steeds, door de juiste keuze van a) of b) kunnen bereiken dat de betreffende randkubus met de juiste oriëntatie in de middenlaag terechtkomt.

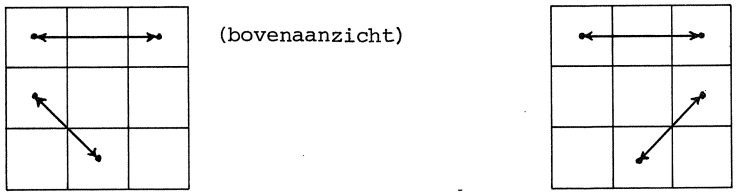
Figuur 3

STAP 3. Breng in de bovenlaag alle kubussen op hun plaats (mogelijk nog niet in de juiste oriëntatie). We kunnen dit bereiken met de volgende permutaties:

a) LINKS $= Z^{-1}\ O^{-1}\ H\ O\ H^{-1}\ O^{-1}\ H^{-1}\ O\ Z\ H^{2}$,

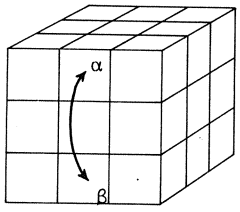
b) RECHTS $= H^{2}\ O^{-1}\ H^{-1}\ O\ Z\ H\ Z^{-1}\ O^{-1}\ H\ O$.

Het effekt van LINKS en RECHTS is dat onder- en middenlaag ongewijzigd blijven en dat in het bovenvlak twee hoekkubussen en twee randkubussen worden verwisseld (zie Figuur 4).



Figuur 4

c) Laat α en $\beta (= \alpha^{-1})$ de draaiingen zijn van de vertikale middenlaag, zoals aangegeven is in Figuur 5.



Figuur 5

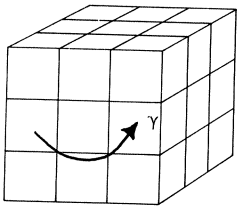
Dan geeft $\alpha H\beta H^2\alpha H\beta$ een 3-cykel op de randkubussen van het bovenvlak (zie Figuur 6), onder- en middenlaag blijven weer ongewijzigd.

Figuur 6

STAP 4. Breng de kubussen in het bovenvlak in de juiste oriëntatie. Voor de randkubussen maken we hierbij gebruik van de zogenaamde dubbele "monoflip":

$$(H)^{-k}Z^{-1}\gamma^{-1}Z^{-2}\gamma^{-2}Z^{-1}(H)^{k}Z\gamma^{2}Z^{2}\gamma Z.$$

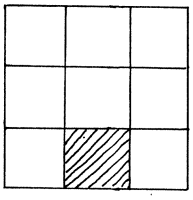
Hierin is γ de draaiing van het horizontale middenvlak, zoals aangegeven in Figuur 7.



Figuur 7

Het effekt van $Z\gamma^2Z^2\gamma Z$ is dat in het bovenvlak alleen de in Figuur 8 aangegeven randkubus van oriëntatie verandert (midden- en ondervlak worden hierbij wel aangetast!). Door nu met $(H)^k$ een andere randkubus op deze plaats te brengen die ook van oriëntatie veranderd moet worden en vervolgens $Z^{-1}\gamma^{-1}Z^{-2}\gamma^{-2}Z^{-1} = (Z\gamma^2Z^2\gamma Z)^{-1}$ uit te voeren, bereiken we dat midden- en ondervlak weer hersteld worden. Door $(H)^{-k}$ wordt het bovenvlak weer op de juiste plaats gebracht. Het uiteindelijke effekt is dat in het bovenvlak twee randkubussen van oriëntatie zijn veranderd.

(boven-aanzicht)



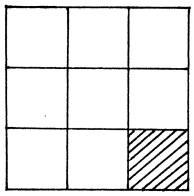
Figuur 8

Bij de hoekkubussen kunnen we op analoge wijze gebruikmaken van de zogenaamde dubbele "monotwist":

$$(H)^{-k}\ O\ L^{-1}\ O^{-1}\ Z^{-1}\ L^{-1}\ Z\ (H)^{k}\ Z^{-1}\ L\ Z\ O\ L\ O^{-1}\ .$$

Hier is het effekt van $Z^{-1}\ L\ Z\ O\ L\ O^{-1}$ dat de in Figuur 9 aangegeven hoekkubus in positieve zin over 120° wordt gedraaid. Met $(H)^{k}$ kunnen we weer een andere hoekkubus op deze plaats brengen, etcetera.

(boven-aanzicht).



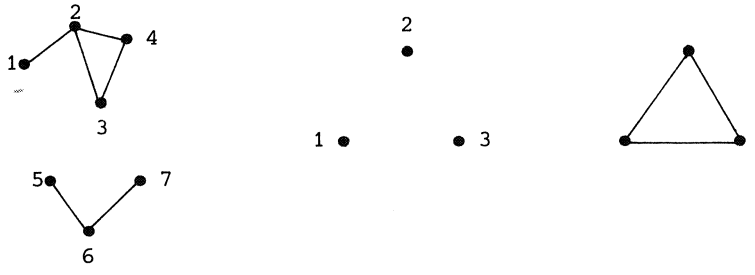
Figuur 9

OPGAVEN BIJ §3.3.

1. Bewijs dat elke stand van de kubus verkregen kan worden door slechts van 5 van de 6 basisdraaiingen gebruik te maken.
2. Wat is de groep voortgebracht door H^2, L^2, N^2, O^2, Z^2, W^2?

3.4. Automorfismengroepen van grafen

3.4.1. DEFINITIES. Een *graaf* is een tweetal (X,Γ) met X een (eindige) verzameling *punten* en $\Gamma \subseteq \binom{X}{2}$ een verzameling *kanten* ($\binom{X}{2} := \{\{x,y\} \mid x,y \in X, x \neq y\}$). Vaak zullen we grafen weergeven met behulp van plaatjes, zoals in Figuur 1.



a b c

Figuur 1.

Zo geeft Figuur 1a de graaf $(\{1,2,3,4,5,6,7\},\{\{1,2\},\{2,4\},\{3,4\},\{5,6\},\{6,7\}\})$ weer, Figuur 1b de graaf $(\{1,2,3\},\emptyset)$ en Figuur 1c de graaf $(\{1,2,3\},\binom{\{1,2,3\}}{2})$.

Het *komplement* van een graaf $G = (X,\Gamma)$ is de graaf $\bar{G} = (X,\Delta)$ met $\Delta := \binom{X}{2} - \Gamma$. Laat $G = (X,\Gamma)$ een graaf zijn. Als $\Gamma = \binom{X}{2}$ dan heet G de *komplete graaf* op $n := |X|$ punten. Als $\{x,y\} \in \Gamma$ dan schrijven we vaak $x \sim y$ en zeggen x is *verbonden* met y. Als $x_1 \sim x_2 \sim x_3 \sim \ldots \sim x_k$ dan heet $(x_1,x_2,\ldots,x_k)$ een *pad* van x_1 naar x_k. Definiëren we $x \approx y$: $\Leftrightarrow$ $x = y$ of er is een pad van x naar y, dan is $\approx$ een ekwivalentierelatie op X. De ekwivalentieklassen heten de *komponenten* G (in Figuur 1a zijn de komponenten $\{1,2,3,4\}$ en $\{5,6,7\}$). De graaf G heet *samenhangend* als er slechts één komponent is.

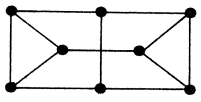
Voor $x \in X$ definiëren we $\Gamma(x) := \{y \in X \mid \{x,y\} \in \Gamma\}$ en $|\Gamma(x)|$ heet de *valentie* van x. Als ieder punt dezelfde valentie heeft, dan heet G *regulier* en de gemeenschappelijke valentie heet de *valentie* van G.

Twee grafen $G = (X,\Gamma)$ en $G' = (X',\Gamma')$ heten *isomorf* (notatie: $G \simeq G'$) als er een bijektie $\phi: X \to X'$ bestaat met $\phi(\Gamma) = \Gamma'$ (ϕ is een *isomorfisme* van G op G'). Een *automorfisme* van G is een isomorfisme van G op zichzelf. De automorfismen van G vormen een groep $\mathrm{Aut}(G) \leq \mathrm{Sym}(X)$, de *automorfismengroep* van G.

3.4.2. PROPOSITIE. *Laat $G = (X,\Gamma)$ een graaf zijn en $\mathrm{Aut}(G)$ transitief op X. Dan is G regulier.*

BEWIJS. Laat $x,y \in X$. Kies $g \in \mathrm{Aut}(G)$ zó dat $g(x) = y$. Dan is $g(\Gamma(x)) = \Gamma(g(x)) = \Gamma(y)$, zodat $|\Gamma(x)| = |\Gamma(y)|$. □

Het omgekeerde van deze bewering is niet waar. Figuur 2 geeft een graaf die regulier is, maar geen transitieve automorfismegroep bezit.



Figuur 2

3.4.3. PROPOSITIE. *Laat $G = (X,\Gamma)$ een graaf zijn en veronderstel dat $\mathrm{Aut}(G)$ primitief werkt op X. Dan zijn G en $\bar{G}$ samenhangend of G of $\bar{G}$ is de complete graaf.*

BEWIJS. Iedere komponent van G of $\bar{G}$ is een imprimitiviteitsblok voor de aktie van $\mathrm{Aut}(G)$ op X. □

Opnieuw geldt de omkering van deze uitspraak niet. Geef zelf een tegenvoorbeeld van een graaf op 6 punten.

Nauw verbonden met de Cayley-representatie van een groep G zijn de zogenaamde Cayley-grafen van de groep G. Zij laten zien dat we iedere groep kunnen opvatten als een groep van automorfismen van een graaf.

3.4.4. DEFINITIE. Laat G een eindige groep zijn met één-element 1. Laat Ω een deelverzameling van G zijn met de eigenschappen

(*) $\quad \forall g \in G(g \in \Omega \to g^{-1} \in \Omega); 1 \notin \Omega;\ G = \langle \Omega \rangle$.

Dan heet de graaf (G,Γ), waar $\Gamma := \{\{x,y\} \mid x^{-1}y \in \Omega\}$, de *Cayley-graaf* van G behorende bij Ω. Zij wordt aangegeven met $C(G,\Omega)$.

3.4.5. PROPOSITIE.

(a) $C(G,\Omega)$ *is samenhangend.*

(b) G *werkt door linksvermenigvuldiging als een reguliere groep van automorfismen van* $C(G,\Omega)$ *op* G.

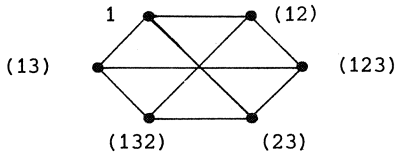
(c) *Als* $\phi \in \mathrm{Aut}(G)$ *voldoet aan* $\phi(\Omega) = \Omega$, *dan is* $\phi \in \mathrm{Aut}(C(G,\Omega))_1$.

BEWIJS. (a). Laat $x \in G$. Er zijn $g_1,\ldots,g_s \in \Omega$ met $x = g_1g_2\ldots g_s$. Laat $x_0 := 1$, $x_1=g_1, x_2=g_1g_2, \ldots, x_s=g_1g_2\ldots g_s=x$. Dan is $(x_0,\ldots,x_s)$ een pad van 1 naar x.

(b). Laat $g \in G$ en $\{x,y\} \in \Gamma$; dan $x^{-1}y \in \Omega$. Dan is $l_g(x)^{-1}l_g(y) = (gx)^{-1}(gy) = x^{-1}y \in \Omega$, dus $\{l_g(x),l_g(y)\} \in \Gamma$. Er volgt $g \in \mathrm{Aut}(C(G,\Omega))$.

(c). Als $\phi \in \mathrm{Aut}(G)$ voldoet aan $\phi(\Omega) = \Omega$, dan volgt voor $x,y \in G$ met $x^{-1}y \in \Omega$ dat $\phi(x)^{-1}\phi(y) = \phi(x^{-1}y) \in \phi(\Omega) = \Omega$. □

Nemen we als voorbeeld $G = \mathrm{Sym}(\underline{3})$ en $\Omega = \{(12),(13),(23)\}$ dan krijgen we de graaf van Figuur 3.



Figuur 3

Daar Ω uit alle 2-kringen bestaat geldt voor elk automorfisme ϕ van G dat $\phi(\Omega) = \Omega$. De orde van de stabilisator van 1 is dan ook tenminste 6. Bovendien geeft $g \mapsto g^{-1}$ nog een automorfisme van de graaf dat 1 stabiliseert. We vinden dat

$$|\mathrm{Aut}(\mathrm{Sym}(3),\Omega)| = 6 \cdot 12 = 72.$$

Nemen we $G' = \mathbb{Z}_6$ en $\Omega' = \{1,3,5\}$ dan vinden we dezelfde graaf. Blijkbaar volgt uit $C(G,\Omega) \simeq C(G',\Omega')$ niet dat $G \simeq G'$.

De volgende uitspraak geeft aan wanneer een graaf G isomorf is met een Cayley graaf $C(G,\Omega)$.

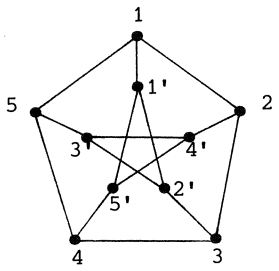
3.4.6. PROPOSITIE. *Laat $G = (X,\Gamma)$ een samenhangende graaf zijn. Als $\mathrm{Aut}(G)$ een op X regulier werkende ondergroep G bevat, dan is $G \simeq C(G,\Omega)$ voor zekere $\Omega \subseteq G$.*

BEWIJS. Kies een punt $x_1 \in X$ vast. Definieer Ω door

$$\Omega := \{g \in G \mid g(x_1) \in \Gamma(x_1)\}.$$

We gaan na dat Ω aan (*) voldoet. Als $g \in \Omega$ dan is $\{x_1, x_1^g\} \in \Gamma$. Daar $g^{-1} \in \mathrm{Aut}(G)$, volgt dat $\{x_1^{g^{-1}}, x_1\} \in \Gamma$, dus $g^{-1} \in \Omega$. Daar $x_1 \notin \Gamma(x_1)$, geldt dat $1 \notin \Omega$. Laat $g \in G$ en laat $(x_1,\ldots,x_s)$ een pad van x_1 naar $x_s := g(x_1)$ zijn en definieer $g_i \in G$ door $x_i = g_i(x_1)$, $i = 1,\ldots,s$. Daar $\{x_i, x_{i+1}\} \in \Gamma$ en $g_i^{-1} \in \mathrm{Aut}(G)$ volgt $g_i^{-1}\{x_i, x_{i+1}\} = \{x_1, g_i^{-1} g_{i+1}(x_1)\} \in \Gamma$, dus ook $g_i^{-1} g_{i+1} \in \Omega$. Dus $g = g_s = (g_1^{-1} g_2)(g_2^{-1} g_3)\ldots(g_{s-1}^{-1} g_s) \in \langle\Omega\rangle$. Men gaat gemakkelijk na dat $\phi: X \to G$ gedefinieerd door $\phi(x) = g$ d.e.s.d. als $g(x_1) = x$ een isomorfisme van G op $C(G,\Omega)$ is. □

Niet iedere graaf G met een transitieve automorfismengroep is isomorf met een Cayley graaf. Een voorbeeld hiervan is de zogenaamde *Petersen-graaf* van Figuur 4. Men gaat gemakkelijk na dat de automorfismengroep transitief is op de punten ((12345)(1',2',3',4',5') en (1,1')(2,2')(5,5')(3',4') zijn geschikte automorfismen). Neem aan dat deze graaf isomorf is met $C(G,\Omega)$ voor zekere groep G van orde 10 en Ω van kardinaliteit 3. Dan is $G \cong G_{10}$ of $G \cong D_5$.

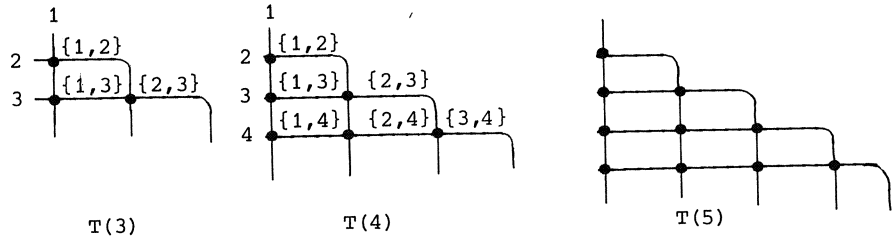


Figuur 4

Laat nu zelf zien dat $C(G,\Omega)$ in alle voorkomende gevallen een vierhoek bevat, in tegenstelling tot de Petersen-graaf.

3.4.7. Triangulaire grafen

Laat $n \in \mathbb{N}$, $n \geq 3$. De *triangulaire graaf* $T(n)$ is de graaf $T(n) = (X,\Gamma)$ met $X = \binom{n}{2}$ en $\Gamma = \{\{x,y\} \mid x,y \in X, |x \cap y| = 1\}$. Meestal geven we de triangulaire grafen weer zoals in Figuur 5: twee punten zijn verbonden als ze op een (geknikte) lijn liggen.



Figuur 5

Het is direkt duidelijk dat $\mathrm{Sym}(\underline{n}) \lesssim \mathrm{Aut}(T(n))$. We zullen aantonen dat voor $n \neq 4$, $\mathrm{Aut}(T(n)) \simeq \mathrm{Sym}(\underline{n})$. Daartoe eerst een definitie. Een *kliek* in een graaf (X,Γ) is een puntverzameling $Y \subseteq X$ met $y_1 \sim y_2$ voor alle $y_1,y_2 \in Y$. In $T(n)$ vormt elke verzameling $X_i := \{\{i,j\} \mid j \neq i\}$, $i = 1,\ldots,n$ een kliek van $(n-1)$ punten. Men gaat gemakkelijk na dat voor $n > 4$ er geen andere klieken zijn met $(n-1)$ punten. Een automorfisme van een graaf voert een kliek over in een kliek met een zelfde aantal punten. Laat $n > 4$, $g \in \mathrm{Aut}(T(n))$ en laat $\pi_g \in \mathrm{Sym}(\underline{n})$ gegeven zijn door $\pi_g(i) = j$ precies dan als $g(X_i) = X_j$. Dan volgt $g(\{i_1,i_2\}) = g(X_{i_1} \cap X_{i_2}) = X_{j_1} \cap X_{j_2} = \{j_1,j_2\} = \pi_g(\{i_1,i_2\})$ als $g(X_{i_1}) = X_{j_1}$, $g(X_{i_2}) = X_{j_2}$. Dit wil zeggen dat g op de

natuurlijke wijze geïnduceerd wordt door $\pi_g \in \mathrm{Sym}(\underline{n})$, dus $\mathrm{Aut}(T(n)) \simeq$ $\simeq \mathrm{Sym}(\underline{n})$.

Voor het geval n = 4 gaan we als volgt te werk. Stel $g \in \mathrm{Aut}(T(4)) - \mathrm{Sym}(\underline{4})$. We mogen aannemen dat $g(\{1,2\}) = \{1,2\}$ omdat $\mathrm{Sym}(\underline{4})$ transitief is op $\binom{4}{2}$. Evenzo mogen we aannemen dat $g(\{1,3\}) = \{1,3\}$ want $\mathrm{Sym}(\underline{4})_{\{1,2\}}$ is transitief op $\Gamma(\{1,2\})$. Als nu ook $g(\{2,3\}) = \{2,3\}$, dan is g de identiteit (waarom?), in tegenspraak met $g \notin \mathrm{Sym}(\underline{4})$. De enige andere mogelijkheid is $g(\{2,3\}) = \{1,4\}$. Dan volgt verder dat $g(\{2,4\}) = \{2,4\}$ en $g(\{3,4\}) = \{3,4\}$ zodat g verder helemaal vast ligt. Onder g gaat de kliek $\{\{1,2\},\{1,3\},\{1,4\}\}$ over in de kliek $\{\{1,2\},\{1,3\},\{2,3\}\}$, dus $g \notin \mathrm{Sym}(\underline{4})$ en $\mathrm{Aut}(T(4)) \simeq \langle \mathrm{Sym}(\underline{4}), g \rangle$ heeft orde $2.4! = 48$.

3.4.8. OPMERKING.

We hebben gezien dat we iedere abstrakte groep op kunnen vatten als een groep van automorfismen van een graaf. Als de groep G gegeven is als transitieve permutatiegroep werkend op de verzameling X, dan is er nog een andere manier om G op te vatten als een groep van automorfismen van een graaf.

Beschouw G werkend op X^2. Daar G transitief op X is, is $I_X := \{(x,x) \in X^2 \mid x \in X\}$ een van de banen van G op X^2. Men gaat gemakkelijk na dat het aantal banen van G op X^2 gelijk is aan het aantal banen van G_x op X ($x \in X$), d.w.z. gelijk aan de rang van G op X.

Met iedere baan $\Gamma \subseteq X^2$ van G op X^2 is ook $\Gamma^U := \{(y,x) \mid (x,y) \in \Gamma\}$ een baan van G op X^2. Als Γ symmetrisch is, d.w.z. als $\Gamma = \Gamma^U$, dan is $\mathcal{G} = (X,\Gamma)$ een graaf en $G \leq \mathrm{Aut}(\mathcal{G})$. Merk op dat G nu niet alleen transitief is op X maar ook op Γ! Nodig en voldoende voorwaarde voor het bestaan van een symmetrische baan $\Gamma \neq I_X$ van G op X^2 is: de orde van G is even. Immers, als $\Gamma = \Gamma^U$ dan is er bij gegeven $(x,y) \in \Gamma$ een $g \in G$ met $g(x) = y$ en $g(y) = x$, en zo'n g heeft even orde. Anderzijds, als G even orde heeft, dan bevat G een element g van orde 2 (Sylow) zodat voor elke x met $g(x) \neq x$ de baan Γ die $(x,g(x))$ bevat symmetrisch is.

Als G rang 2 is op X, dan bestaat X^2 uit de G-banen I_X en X^2-I en vinden we alleen de komplete graaf (X,X^2-I_X) op X, hetgeen vanuit een grafentheoretisch oogpunt gezien niet interessant is (een zg. design aanpak voor de bestudering van G ligt dan meer voor de hand). Interessanter is het geval dat G van even orde is en rang 3 werkt op X. Dit zullen we in deze paragraaf onderzoeken. Een voorbeeld hebben we al gezien, namelijk de triangu-

laire grafen T(n) met G = Sym(n) en X = $\binom{n}{2}$. In dit voorbeeld is X^2 = $= I_X \dot\cup \Gamma \dot\cup \Delta$ met $\Gamma = \{(\{\alpha,\beta\},\{\gamma,\delta\}) \mid |\{\alpha,\beta\} \cap \{\gamma,\delta\}| = 1\}$ en $\Delta = \{(\{\alpha,\beta\},\{\gamma,\delta\}) \mid |\{\alpha,\beta\} \cap \{\gamma,\delta\}| = 0\}$ als de banen $\neq I_X$ van G op X^2.

Laat G van even orde rang 3 werken op X en laat I_X, Γ en Δ de banen van G op X^2 zijn. Dan zijn Γ en Δ beide symmetrisch (waarom?). Daar G transitief is op Γ zijn $\lambda = |\{z \in X \mid (x,z) \in \Gamma, (y,z) \in \Gamma\}|$, $(x,y) \in \Gamma$ en $\mu = |\{w \in X \mid (u,w) \in \Gamma, (v,w) \in \Gamma\}|$, $(u,v) \in \Delta$ onafhankelijk van de keuze van $(x,y) \in \Gamma$ en $(u,v) \in \Delta$.

3.4.9. DEFINITIES. Een reguliere graaf $G = (X,\Gamma)$ heet *sterk regulier* als voor ieder tweetal verbonden punten x en y er precies λ punten z zijn die met zowel x als y verbonden zijn, en voor ieder tweetal niet verbonden punten u en v er precies μ punten w zijn die met zowel u als v verbonden zijn. Als $n = |X|$ en k de valentie van G voorstelt, dan heet het viertal n,k,λ,μ de *parameters* van de sterk reguliere graaf G. Een graaf $G = (X,\Gamma)$ heet *rang 3-graaf* als $\mathrm{Aut}(G)$ rang 3 werkt op X.

Met behulp van deze definities kunnen we nu dus de volgende propositie formuleren.

3.4.10. PROPOSITIE. *Een rang 3-graaf is sterk regulier.*

Meestal zullen we in onze beschouwingen uitsluiten dat de sterk reguliere graaf triviaal is, d.w.z. de vereniging is van een aantal klieks of de vereniging van een aantal koklieks (een kokliek is een deelverzameling Y van punten zó dat $x \not\sim y$ voor alle $x,y \in Y$). De volgende stelling karakteriseert deze grafen in termen van de parameters.

3.4.11. PROPOSITIE. *Laat* $G = (X,\Gamma)$ *een sterk reguliere graaf zijn met parameters* n,k,λ,μ. *Dan geldt* $0 \le \mu \le k$ *en*

$$\mu = 0 \iff X = X_1 \dot\cup X_2 \dot\cup \ldots \dot\cup X_\ell, \quad \Gamma = \binom{X_1}{2} \dot\cup \binom{X_2}{2} \dot\cup \ldots \dot\cup \binom{X_\ell}{2}$$

$$\mu = k \iff X = X_1 \dot\cup X_2 \dot\cup \ldots \dot\cup X_\ell, \quad \Gamma = X^2 \setminus \{I_X \cup \binom{X_1}{2} \cup \binom{X_2}{2} \cup \ldots \cup \binom{X_\ell}{2}\}.$$

BEWIJS. Stel $\mu = 0$. Als $x \sim y$ en $y \sim z$ dan is ook $x \sim z$, want $x \not\sim z$ geeft $\mu \ge 1$ omdat y een gemeenschappelijke buur is van x en z. De relatie $\approx$ gedefinieerd door $x \approx y$: $\iff (x\sim y) \vee (x=y)$ is een ekwivalentierelatie. Neem voor de X_i's de ekwivalentieklassen. Het geval $\mu = k$ gaat precies zo. □

De groep die bij de graaf G van Propositie 3.4.11 hoort, is $\mathrm{Sym}(\ell) \int \mathrm{Sym}(n/\ell)$. Deze groep is rang 3 op X en $X_1,\ldots,X_\ell$ zijn imprimitiviteitsblokken behorende bij de aktie van deze groep op X. De volgende stelling laat zien dat dit het enige geval is waarin een rang 3-werking van een groep imprimitief is.

3.4.12. STELLING. *Laat de groep* G, *van even orde, rang* 3 *werken op* X *en laat* I_X, Γ *en* Δ *de banen zijn van* G *op* X^2. *Als de aktie van* G *op* X *imprimitief is, dan is* (X,Γ) *de vereniging van klieks of van koklieks.*

BEWIJS. Laat $B \subset X$, met $1 < |B| < |X|$, een blok zijn onder de aktie van G op X. Daar $|B| > 1$ zijn er $x,y \in B$ met $x \neq y$. Stel $x \sim y$. Dan is $\Gamma(x) = G_x y \subseteq G_x B = B$. Als er een $z \in B$ is met $x \not\sim z$, dan is ook $\Delta(x) = G_x z \subseteq G_x B = B$, dus $X = \{x\} \cup \Gamma(x) \cup \Delta(x) \subseteq B$ in tegenspraak met $B \neq X$. Dus $x \sim z$ voor alle $z \in B$, d.w.z. $B = \{x\} \cup \Gamma(x)$. Daar G_B transitief is op B, geldt voor alle $u \in B$ dat $B = \{u\} \cup \Gamma(u)$. Daar G transitief is op X geldt $X = X_1 \dot\cup X_2 \dot\cup \ldots \dot\cup X_\ell$, met $X_i = g_i B$ voor geschikt gekozen $g_i \in G$, $i = 1,\ldots,\ell$. Voor $u \in X_i$ geldt $X_i = \{u\} \cup \Gamma(u)$, d.w.z. $\Gamma(u) = X_i \backslash \{u\}$, dus $\Gamma = \binom{X_1}{2} \cup \binom{X_2}{2} \cup \ldots \cup \binom{X_\ell}{2}$. De aanname dat $x \not\sim y$ voert op analoge wijze tot de konklusie dat (X,Γ) de vereniging is van koklieks. □

3.4.13. VOORBEELDEN.

- Beschouw $\mathrm{Sym}(m)$ werkend op $\binom{m}{2}$, $m \geq 5$. Deze werking is rang 3. De bijbehorende graaf is de triangulaire graaf T(m) met $n = \binom{m}{2}$, $k = 2(m-2)$, $\lambda = m-2$, $\mu = 4$. Merk op dat voor $m \geq 5$, $0 < \mu < k$.
- Beschouw $\mathrm{Sym}(2) \int \mathrm{Sym}(m)$ werkend op m^2, $m \geq 3$. Deze werking is rang 3. De bijbehorende graaf is de zg. *Lattice-graaf* L(m) met parameters $n = m^2$, $k = 2(m-1)$, $\lambda = m-2$, $\mu = 2$.
- Laat q een macht van een priemgetal zijn met $q \equiv 1 \pmod 4$. Beschouw de groep G bestaande uit de afbeeldingen $\phi_{a,b}: \mathbb{F}_q \to \mathbb{F}_q$, $a \in (\mathbb{F}_q^*)^2 = \{x^2 \mid x \in \mathbb{F}_q^*\}$, $b \in \mathbb{F}_q$ gedefinieerd door $\phi_{a,b}(x) = ax+b$, $x \in \mathbb{F}_q$. Daar $q \equiv 1 \pmod 4$ is $|G| = \frac{1}{2}q(q-1)$ even. De banen van G_0 op $\mathbb{F}_q$ zijn $\{0\}$, $(\mathbb{F}_q^*)^2$, en de rest: $\mathbb{F}^* - (\{0\} \cup (\mathbb{F}_q^*)^2)$, dus G werkt rang 3 op $\mathbb{F}_q$. De bijbehorende graaf is de *Paley-graaf* $P(q)$ die gegeven wordt door

$$x \sim y: \iff x-y \in (\mathbb{F}_q^*)^2, \qquad x,y \in \mathbb{F}_q.$$

(Merk op dat $\sim$ goed gedefinieerd is, want $q \equiv 1 \pmod 4 \Rightarrow -1 \in (\mathbb{F}_q^*)^2$.) De parameters zijn $n = q$, $k = \frac{1}{2}(q-1)$, $\mu = \frac{1}{4}(q-1)$, $\lambda = \frac{1}{4}(q-1) - 1$ (zie 3.4.16).

- De *Clebsch-graaf*. De puntverzameling is $X = \{(x_1,x_2,x_3,x_4,x_5) \in \mathbb{Z}_2^5 \mid \sum_{i=1}^5 x_i = 0 \pmod 2\}$. Twee punten zijn verbonden d.e.s.d. als ze op precies één koördinaatplaats overeenstemmen (bijv. $(0,0,0,0,0) \sim (0,1,1,1,1), (1,0,1,1,1), \ldots, (1,1,1,1,0)$). De groep is $G = (\mathbb{Z}_2)^4 \rtimes \mathrm{Sym}(\underline{5})$; deze is rang 3 want $G_{(0,0,0,0,0)} \cong \mathrm{Sym}(\underline{5})$ heeft de banen $\{(0,0,0,0,0)\}$, {vektoren met 2 enen}, {vektoren met 4 enen} op X. De parameters zijn $n = 16$, $k = 5$, $\lambda = 0$, $\mu = 2$.

3.4.14. OPMERKING. Niet elke groep G heeft een primitieve rang 3 voorstelling. Geef zelf een tegenvoorbeeld. Tot nu toe zijn we voorbeelden van primitieve rang 3 permutatiegroepen G tegengekomen waarin G een normaaldeler N heeft die aan één van de volgende drie uitspraken voldoet

a) N is regulier

b) N is enkelvoudig en $N \trianglelefteq G \lesssim \mathrm{Aut}(N)$

c) $N \cong K \times K$ voor een enkelvoudige groep K en $N \trianglelefteq G \lesssim \mathrm{Aut}(N)$.

Hier betekent $\lesssim$ "is isomorf met een ondergroep van". Uit Opgave 5.2.7 zal blijken dat elke primitieve groep G van rang 3 noodzakelijkerwijs in één van de kategorieën a), b) of c) valt.

De parameters van sterk reguliere grafen (en dus van rang 3-voorstellingen van groepen) zijn aan sterke beperkingen onderhevig. De eerste is een relatie tussen n, k, λ en μ.

3.4.15. STELLING. Laat $G = (X,\Gamma)$ *een sterk reguliere graaf zijn met parameters* n,k,λ *en* μ. *Dan geldt* $(n-k-1)\mu = k(k-1-\lambda)$.

BEWIJS. Kies een punt $x \in X$ en tel het aantal kanten $(y,z) \in \Gamma$ met $y \in \Gamma(x)$ en $z \in \Delta(x)$ (hierin is zoals steeds $\Delta := X^2 \setminus (I_X \cup \Gamma)$. Enerzijds is dit aantal $|\Gamma(x)|(k-1-\lambda) = k(k-1-\lambda)$ want een punt $y \in \Gamma(x)$ is verbonden met λ punten in $\Gamma(x)$ en met x dus met $k-1-\lambda$ punten in $\Delta(x)$. Anderzijds is dit aantal $\Delta(x) \cdot \mu = (n-k-1) \cdot \mu$ want een punt $z \in \Delta(x)$ is met μ punten in $\Gamma(x)$ verbonden. □

3.4.16. TOEPASSING. We berekenen λ en μ van de Paley-graaf $P(q)$. Merk eerst op dat het komplement van een sterk reguliere graaf met parameters n,k,λ en μ een sterk reguliere graaf met parameters $\bar{n} = n$, $\bar{k} = n-k-1$, $\bar{\lambda} = n-2k+\mu-2$, $\bar{\mu} = n-2k+\lambda$ is. Merk vervolgens op dat de afbeelding $\phi: \mathbb{F}_q \to \mathbb{F}_q$ gegeven door $\phi(x) = \alpha(x)$, met α een vast gekozen niet kwadraat, een isomorfisme is van $P(q)$ op het komplement van $P(q)$. Dus $\lambda = \bar{\lambda} = n-2k+\mu-2 = q-(q-1)+\mu-2 = \mu-1$. Uit $(n-k-1)\mu = k(k-1-\lambda)$ volgt verder $\frac{q-1}{2} \cdot \mu = \frac{q-1}{2}(\frac{q-1}{2} - 1-\lambda)$, dus

$\mu + \lambda = \frac{q-1}{2} - 1$. Dit geeft $\mu = \frac{1}{4}(q-1)$ en $\lambda = \frac{1}{4}(q-1) - 1$.

Iedere graaf $G = (X,\Gamma)$ kunnen we beschrijven met behulp van haar zogenaamde *verbindingsmatrix* $A = A(G)$ die als volgt wordt gedefinieerd: nummer de punten van de graaf van 1 t/m n en definieer

$$A_{ij} = \begin{cases} 1 & \text{als } (i,j) \in \Gamma \\ 0 & \text{anders.} \end{cases}$$

Veel grafentheoretische eigenschappen hebben zo een eenvoudige vertaling in matrixtheoretische eigenschappen van haar verbindingsmatrix; zo ook het sterk regulier zijn.

3.4.17. STELLING. *Een graaf $G = (X,\Gamma)$ is sterk regulier met parameters n,k,λ en μ precies dan als haar verbindingsmatrix A voldoet aan*
(i) $A\underline{j} = k\underline{j}$, *en*
(ii) $A^2 + (\mu-\lambda)A + (\mu-k)I = \mu J$.
Hierin is $\underline{j}$ de (kolom)vektor die bestaat uit louter enen, $\underline{j}^t = (1,1,\ldots,1)$; en J is de $n\times n$ matrix die bestaat uit louter enen.

BEWIJS. (i) is triviaal ekwivalent met: G is regulier van valentie k. Voor (ii) merk op dat $(A^2)_{ij} = \sum_{j=1}^{n} A_{i\ell}A_{\ell j} = \#\{\ell \mid A_{i\ell} = A_{\ell j} = 1\} = \#\{\ell \mid i \sim \ell \sim j\}$. Dus geldt

$$(A^2)_{ij} = \begin{cases} k & \text{als } i = j, \\ \lambda & \text{als } i \sim j, \\ \mu & \text{als } i \not\sim j,\ i \neq j; \end{cases}$$

d.w.z. $A^2 = kI + \lambda A + \mu(J-I-A)$. □

3.4.18. STELLING. *Laat $G = (X,\Gamma)$ een sterk reguliere graaf zijn met parameters n,k,λ en μ zò dat $0 < \mu < k$. Laat r en s de wortels zijn van de vierkantsvergelijking*

$$x^2 + (\mu-\lambda)x + (\mu-k) = 0.$$

Dan geldt:
(a) *r en s zijn reëel en nemen we $r > s$ dan is $r > 0$ en $s < 0$.*
(b) *De getallen $f = (s(n-1)+k)/(s-r)$ en $g = (r(n-1)+k)/(r-s)$ zijn positief en geheel.*
(c) *als r en s niet geheel zijn, dan geldt $k = \frac{1}{2}(n-1)$, $\mu = \frac{1}{4}(n-1)$, $\lambda = \frac{1}{4}(n-1) - 1$.*

BEWIJS. De verbindingsmatrix A van G is symmetrisch. Alle eigenwaarden van A zijn dus reëel en A is diagonaliseerbaar. Laat x een eigenwaarde van A zijn bij de eigenvektor $\underline{\xi}$ met $\underline{\xi}^t = (\xi_1,\xi_2,\ldots,\xi_n)$. Vermenigvuldiging van $A^2 + (\mu-\lambda)A + (\mu-k)I = \mu J$ met $\underline{\xi}$ geeft

$$\xi_j(x^2 + (\mu-\lambda)x + (\mu-k)) = \mu \sum_{i=1}^{n} \xi_i \quad \text{voor alle } j = 1,\ldots,n.$$

Als $\sum_{i=1}^n \xi_i \neq 0$ dan volgt $\xi_1 = \xi_2 = \ldots = \xi_n$, dus $\underline{\xi} = \xi_1\underline{j}$ zodat in dit geval $x = k$ (want $A\underline{j} = k\underline{j}$). Als $\sum_{i=1}^n \xi_i = 0$ dan voldoet x blijkbaar aan $x^2 + (\mu-\lambda)x + (\mu-k) = 0$, d.w.z. $x = r$ of $x = s$. Hieruit volgt dat r en s reëel zijn en daar $rs = \mu-k < 0$ volgt uit $r > s$ dat $r > 0$ en $s < 0$. Laat f de multipliciteit zijn van de eigenwaarde r en g de multipliciteit van de eigenwaarde s. Daar de eigenwaarde k multipliciteit 1 heeft, volgt

$$1 + f + g = n.$$

Daar $0 = \sum_{i=1}^n A_{ii}$ = spoor van A = som van de eigenwaarden van A, vinden we ook

$$1\cdot k + f\cdot r + g\cdot s = 0.$$

Uit deze twee vergelijkingen volgt $f = (s(n-1)+k)/(s-r)$ en $g = (r(n-1)+k)/(r-s)$. Daar r en s de wortels zijn van $x^2 + (\mu-\lambda)x + (\mu-k) = 0$, geldt $r+s = \lambda-\mu$. Met $fr+sg = -k$ geeft dit $r = (-k-(\lambda-\mu)g)/(f-g)$ als $f \neq g$, en dus volgt in dit geval dat r (en dus ook $s = (\lambda-\mu)-r$) geheel is (als $r = p/q$ met $p,q \in \mathbb{Z}$, $(p,q) = 1$ dan volgt uit $(\frac{p}{q})^2 + (\mu-\lambda)\frac{p}{q} + (\mu-k) = 0$ dat $q \mid p^2$, dus $q = 1$).

Als $f = g$ dan is $f = g = \frac{1}{2}(n-1)$. Uit $k = -fr - gs = -f(r+s) = \frac{1}{2}(n-1)(\mu-\lambda)$ en $0 < k < (n-1)$ volgt nu dat $\mu-\lambda = 1$ en $k = \frac{1}{2}(n-1)$. Met $(n-k-1)\mu = k(k-1-\lambda)$ geeft dit $\mu+\lambda = k-1$, dus $\mu = \frac{1}{2}k = \frac{1}{4}(n-1)$ en $\lambda = \frac{1}{4}(n-1) - 1$. □

3.4.19. OPMERKINGEN.

- Gebruikmakend van Stelling 3.4.18 vindt men voor $n \leq 20$ het volgende lijstje van parameters van rang 3-voorstellingen van groepen (met $k \leq \frac{1}{2}(n-1)$).

n	k	λ	μ	r	s	f	g
5	2	0	1	0,618..	-1,618..	2	2
9	4	1	2	1	-2	4	4
10	3	0	1	1	-2	5	4
13	6	2	3	1,30..	-2,30..	6	6
15	6	1	3	1	-3	9	5
16	5	0	2	1	-3	10	5
16	6	2	2	2	-2	6	9
17	8	3	4	1,56..	-2,56	8	8

- Naast 3.4.18 zijn er nog meer nodige voorwaarden voor het bestaan van rang 3-voorstellingen van groepen (zie Opgave 4), maar 3.4.18 is veruit de belangrijkste.

OPGAVEN BIJ §3.4.

1. Laat A een verzameling zijn met ℓ elementen, B een verzameling met m elementen. Definieer $X := A \times B$ en $\Gamma = \{\{(a_1,b_1),(a_2,b_2)\} \mid a_1 = a_2$ of $b_1 = b_2\}$. Laat zien dat $\mathrm{Aut}(X,\Gamma) \simeq \mathrm{Sym}(\underline{\ell}) \times \mathrm{Sym}(\underline{m})$ als $\ell \neq m$ en $\mathrm{Aut}(X,\Gamma) \simeq C_2 \int \mathrm{Sym}(\underline{\ell})$ is rang 3 als $\ell = m$. Als bovendien G een 2-transitieve groep op ℓ is, laat zien dat $C_2 \int G$ dan rang 3 op $X = \underline{\ell} \times \underline{\ell}$ werkt.

   Is (X,Γ) een Cayley-graaf?

2. Toon aan dat $\mathrm{Aut}(T(4))$ isomorf is met de isometriegroep van de kubus.

3. Zoek bij het lijstje van 3.4.19 groepen en grafen.

4. Voor een sterk reguliere graaf met $\mu = 1$ geldt $\lambda \mid k$ en $\lambda(\lambda+1) \mid nk$. Bewijs dit.

5. Voor welke n is T(n) een Cayley-graaf?

6. Is het komplement van een Cayley-graaf weer een Cayley-graaf?

HOOFDSTUK IV

LINEAIRE REPRESENTATIES

4.1. De voorstelling

G is steeds een eindige groep. K is een lichaam (we zijn voornamelijk geïnteresseerd in het geval $K = \mathbb{C}$), V is een n-dimensionale vektorruimte over K, en Gl(V) is de groep van alle inverteerbare lineaire afbeeldingen van V in zichzelf. Iedere basis van V levert een isomorfisme van Gl(V) op $GL_n(K)$ (de groep van inverteerbare n×n-matrices, zie (1.1.11)) dat aan $A \in Gl(V)$ zijn matrix ten opzichte van die basis toevoegt.

4.1.1. DEFINITIES. Een *lineaire representatie* (ofwel *lineaire voorstelling*) van G in V (over K) is een morfisme $f : G \to Gl(V)$ van groepen; n heet de *graad* of *dimensie* van f. Is f injektief, dan heet de voorstelling *getrouw*. We zullen voor $g \in G$ vaak f_g in plaats van f(g) schrijven. Als f en f' twee lineaire voorstellingen van G zijn in de vektorruimten V respektievelijk V' over K dan heten zij *ekwivalent* als er een isomorfisme $t : V \to V'$ van lineaire ruimten bestaat zodanig dat

$$tf_g = f'_g t \qquad \text{voor elke } g \in G.$$

Ga zelf na dat ekwivalentie van voorstellingen over een lichaam voor een vast gekozen groep G inderdaad een ekwivalentie-relatie definieert. Ekwivalente voorstellingen hebben dus gelijke graad. Als F_g en F'_g de matrices van f_g respektievelijk f'_g zijn ten opzichte van vast gekozen bases in V respektievelijk V', dan betekent dit dat er een matrix T met $\det(T) \neq 0$ bestaat zo dat

$$F'_g = TF_gT^{-1} \qquad \text{voor elke } g \in G.$$

Hieruit blijkt wel dat f en f' in wezen niet verschillen; t.o.v. geschikte bases hebben ze gelijke matrices.

We zijn dan ook uitsluitend geïnteresseerd in ekwivalentieklassen van voorstellingen. Voor het gemak zullen we F een bij f horende *matrix-voorstelling* van G noemen.

4.1.2. VOORBEELDEN.

(i) $G = Gl_n(K)$ heeft de identiteit : $G \to Gl(K^n)$ als een getrouwe voorstelling van graad n over K. In (1.1.12) was D_n als ondergroep van $Gl_2(\mathbb{R})$ ingevoerd. De inbedding van D_n in $Gl_2(\mathbb{R})$ is een lineaire voorstelling van graad 2 over $\mathbb{R}$.

(ii) Een voorstelling $f : G \to Gl(\mathbb{C})$ van graad 1 is in feite een morfisme $f : G \to \mathbb{C}^*$. Het beeld f(G) is een ondergroep van $\mathbb{C}^*$ en vanwege (1.1.10) isomorf met C_n voor $n = |f(G)|$. In het bijzonder is f niet getrouw als G niet-cyclisch is. Als f de konstante afbeelding $g \mapsto 1$ ($g \in G$) is, dan noemen we haar de *triviale voorstelling*. Vanzelfsprekend heeft iedere groep een triviale voorstelling.

(iii) Laat G een permutatiegroep op de eindige verzameling X zijn. Laat K een lichaam en $V = \bigoplus_{x \in X} Ke_x$ de vektorruimte over K met basis $(e_x)_{x \in X}$ zijn. Voor $g \in G$ leggen we $f_g^X \in Gl(V)$ vast door

$$f_g^X e_x = e_{g(x)} \qquad (x \in X)$$

Ga na dat f_g^X zo als lineaire transformatie uniek bepaald is. Aldus wordt een lineaire voorstelling f^X van G van graad $|X|$ verkregen; de bijbehorende matrixvoorstelling heeft als beeld een stel permutatiematrices, dat wil zeggen matrices die in elke rij en in elke kolom precies één 1 en verder uitsluitend 0 als koëfficient hebben. In het bijzonder kunnen we X = G nemen en G via de linksreguliere permutatievoorstellling op X laten werken (zie (1.3.3)). De bijbehorende f^G is dan een getrouwe lineaire voorstelling van graad $|G|$, die we de *reguliere voorstelling* van G noemen.

De direkte som $V \oplus V'$ van twee vektorruimtes V, V' over K is de verzameling paren $v \oplus v' = (v,v')$ met $v \in V$ en $v' \in V'$ voorzien van de koördinaatsgewijze vektoroptelling en skalair-vermenigvuldiging (dus $v \oplus v' + w \oplus w' = (v+w) \oplus (v'+w')$ en $\alpha(v \oplus v') = (\alpha v) \oplus (\alpha v')$ voor $v,w \in V$, $v',w' \in V'$ en $\alpha \in K$). De operatie directe som is associatief op de vektorruimtes over K.
Het volgende lemma illustreert hoe van (een) gegeven voorstelling(-en) andere voorstellingen te maken zijn.

4.1.3. LEMMA. *Laat* G *een eindige groep zijn,* V *een vektorruimte over het lichaam* K, *en* $f : G \to Gl(V)$ *een lineaire voorstelling.*

(i) *Als* H *een groep is en* $\phi : H \to G$ *een morfisme, dan is* $f\circ\phi$ *een voorstelling van* H *in* V.

(ii) *Als* W *een lineaire deelruimte van* V, *invariant onder* f, *is (d.w.z.* $(\forall g\in G)(f_g W = W)$*), dan is* f^W gedefinieerd door $f^W_g = (f_g)|_W$ *een lineaire voorstelling van* G *in* W.

(iii) *Als* $f' : G \to Gl(V')$ *een tweede voorstelling van* G *over* K *is, dan is* $f\oplus f' : G \to Gl(V\oplus V')$ *gedefinieerd door* $(f\oplus f')_g(v\oplus v') = f_g(v)\oplus f'_g(v')$ $(v \in V,\ v' \in V',\ g \in G)$ *een lineaire voorstelling van* G *in* $V\oplus V'$.

BEWIJS. (i) en (ii) komen neer op het feit dat het samenstel van twee morfismen er weer een is. (iii) volgt rechtstreeks uit de definities. □

Nemen we in Voorbeeld 4.1.2 (iii) voor W als in 4.1.3 (ii) de 1-dimensionale lineaire ruimte opgespannen door de vektor $\sum_{x\in X} e_x$, dan is $(f^X)^W$ de triviale voorstelling.

4.1.4. DEFINITIE. Laat f een voorstelling van een groep G in een vektorruimte V over K zijn . f heet *irreducibel* als er geen f-invariante deelruimten $\neq 0,V$ in V bestaan. Is W een f-invariante deelruimte van V, dan heet f^W uit Lemma 4.1.3 (ii) de restriktie van f tot w; evenzo heet $f\oplus f'$ uit Lemma 4.1.3 (iii) de direkte som van f en f'.

4.1.5. STELLING (Maschke). *Laat* f *een voorstelling van een groep* G *in een vektorruimte* V *over* K *zijn. Veronderstel verder dat* kar(K) = 0 *of dat* p = kar(K) *geen deler is van* |G|.

(i) *Als* W *een* f*-invariante deelruimte van* V *is, dan bestaat er een* f*-invariant komplement, dat wil zeggen een* f*-invariante deelruimte* W' *van* V, *zo dat* $V = W\oplus W'$.

(ii) *Er zijn irreducibele restricties* $f^1,\ldots,f^t$ *van* f *zo dat* $f = f^1\oplus\ldots\oplus f^t$.

BEWIJS.

(i) Laat $\pi : V \to V$ een projektie van V op W zijn, dus π is lineair, $\pi^2 = \pi$ en $\pi(V) = W$. Merk op dat de voorwaarden omtrent kar(K) impliceren dat |G| als element van $K-\{0\}$ te zien is. Bekijk nu

$$P = \frac{1}{|G|}\sum_{g\in G} f_g \pi f_{g^{-1}}.$$

Dit is een lineaire afbeelding van V in zichzelf. Daar $f_g\pi(V) = f_g(W) = W$, is $P(V)$ bevat in W. Maar voor $w \in W$ geldt $f_{g^{-1}}(w) \in W$ zodat $\pi f_{g^{-1}}(w) = f_{g^{-1}}(w)$ en $f_g \pi f_{g^{-1}}(w) = w$. Bijgevolg is $P(w) = w$ voor elke $w \in W$.

We konkluderen dat $P(V) = W$ en $P^2 = P$, dus dat P een projektie op W is. Verder is $f_g P f_{g^{-1}} = P$, immers

$$f_g P f_{g^{-1}} = \frac{1}{|G|} \sum_{h \in G} f_g f_h \pi f_{h^{-1}} f_{g^{-1}} = \frac{1}{|G|} \sum_{gh \in G} f_{gh} \pi f_{(gh)^{-1}} = P.$$

Derhalve is

$$W' = \{v \in V \mid Pv = 0\} \text{ invariant onder } f.$$

Aangezien V de direkte som van het beeld $W = P(V)$ en de kern W' van P is, volgt het gestelde.

(ii) Met induktie naar dim V. Doe zelf het 1-(of zo u wilt 0-) dimensionale geval. Laat vanaf nu dim $V > 1$. Als f irreducibel is valt er niets te bewijzen. Anders is er een f-invariante deelruimte W van V, waarop (i) van toepassing is. We kunnen dus $f = f' \oplus f''$ schrijven, met f' irreducibel op W en f'' een lineaire voorstelling op een deelruimte van V van dimensie $<$dim V. Pas nu de induktiehypothese op f'' toe: $f'' = f^2 \oplus \ldots \oplus f^t$ met f^i $(2 \leq i \leq t)$ irreducibele restrikties van f'' en dus ook van f. Substitueer tenslotte deze gelijkheid voor f'' in $f = f' \oplus f''$. □

4.1.6. OPMERKINGEN.

(i) In termen van matrixvoorstellingen staat er in 4.1.5. (i) dat er irreducibele matrixvoorstellingen $F^1, \ldots, F^t$ zijn zodat er een matrixvoorstelling bij f is die de vorm

$$\begin{pmatrix} F^1 & & & 0 \\ & F^2 & & \\ & & \ddots & \\ 0 & & & F^t \end{pmatrix}$$

heeft.

(ii) De in de stelling gevonden f^i zijn op ekwivalentie en volgorde na uniek bepaald; dit wordt pas in 4.2.6. bewezen.

(iii) Als $|G|$ een priemdeler $p = kar(K)$ bevat, dan splitst een voorstelling $f : G \to Gl(V)$ niet noodzakelijk in irreducibele delen: denk aan de 2-Sylowgroep $G = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ van $Sl_2(8)$. Van deze groep van orde 8 is de inbedding $i : G \to Gl_2(\mathbb{F}_8)$ reducibel; immers $W = \mathbb{F}_8 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is een invariante deelruimte. Ga na dat er echter geen invariant komplement voor W in $\mathbb{F}_8^2$ bestaat. De eigenschap dat een voorstelling opsplitst in de direkte som van irreducibele voorstellingen noemt men wel *volledige reducibiliteit*.

(iv) Uit de stelling volgt: als $g \in Gl_n(\mathbb{C})$ een element van eindige orde is, dan heeft $\mathbb{C}^n$ een basis $x_1,\ldots,x_n$ van eigenvektoren van g. Het feit dat x_i eigenvektor van g is betekent dat voor elke $i \in \underline{n}$ er een $\lambda_i \in \mathbb{C}$ bestaat waarvoor $gx_i = \lambda_i x_i$. De λ_i zijn hier orde van g-de machts eenheidswortels. In het bijzonder heeft g dan de diagonaalvorm op $x_1,\ldots,x_n$.

4.1.7. LEMMA (van Schur). *Stel* f^1 *en* f^2 *zijn irreducibele voorstellingen van* G *in* V_1 *respectievelijk* V_2. *Laat* $A : V_1 \to V_2$ *een lineaire afbeelding zijn met* $(\forall g \in G)\ (Af_g^1 = f_g^2 A)$. *Dan is ofwel* $A = 0$ *ofwel* A *bijektief en* f^1 *ekwivalent met* f^2. *Als daarenboven* $f^1 = f^2$ *en* $K = \mathbb{C}$ *dan is er een* $\lambda \in K$ *met* $A = \lambda.1_{V_1}$.

BEWIJS. $Ker(A) = \{v \in V_1 \mid Av = 0\}$ en $Im(A) = A(V_1)$ zijn f^i-invariante deelruimten van V_i voor $i = 1$ respektievelijk 2. (Kontroleer dit). Omdat f^1 irreducibel is, volgt $Ker(A) = (0)$ of V_1. Stel $A \neq 0$, dan volgt $Ker(A) = (0)$. Evenzo volgt dan uit de irreducibiliteit van f^2 dat $AV^1 = V^2$. Bijgevolg is A bijektief en is met $t = A$ aan de definitie voor ekwivalentie van f^1 en f^2 voldaan. Om de laatste uitspraak van het lemma te bewijzen, nemen we een eigenwaarde λ van A en konstateren we dat $Ker(A-\lambda I_{V_1})$ een f^1-invariante deelruimte van V_1 van dimensie ≥ 1 is. De irreducibiliteit van f^1 impliceert dat $Ker(A-\lambda I_{V_1}) = V_1$ ofwel dat $A = \lambda I_{V_1}$ is. (Waarom is $K = \mathbb{C}$ genomen?) □

Met bovenstaand lemma kunnen we de sterke relaties van Schur bewijzen.

4.1.8. STELLING. *Stel* f *en* f^1 *zijn twee irreducibele voorstellingen op* V *resp.* V^1 *over* $\mathbb{C}$ *met bijbehorende matrixvoorstellingen* F *en* F^1. *Dan geldt met* n = *graad van* f:

(i) $$\sum_{g \in G} F(g)_{i,s}\, F^1(g^{-1})_{t,j} = 0 \quad \textit{als f en } f^1 \textit{ inekwivalent zijn.}$$

(ii) $$\sum_{g\in G} F(g)_{i,s}\, F(g^{-1})_{t,j} = \frac{\delta_{ij}\delta_{st}|G|}{n}\,.$$

Hierin is $F(g)_{is}$ *de* (i,s)*-koëfficient van de matrix* $F(g)$.

BEWIJS. Laat m nog de graad van f^1 zijn. Aan een lineaire afbeelding $u : V^1 \to V$ voegen we toe $a_u : V^1 \to V$ gedefinieerd door

$$a_u = \sum_{g\in G} f_g u f^1_{g^{-1}}.$$

Deze lineaire afbeelding voldoet voor elke $g \in G$ aan $f_g a_u = a_u f^1_g$.
Nemen we voor u de van $s \in \underline{n}$, $t \in \underline{m}$ afhangende lineaire afbeelding gegeven door $u(y_r) = \delta_{rt}x_s$ $(r = 1,\ldots,m)$, waar $x_1\ldots,x_n$ resp. $y_1\ldots,y_m$ de vast gekozen bases van V' resp. V zijn, dan verschijnt op de (i,j)-plaats in de matrix van a_u de uitdrukking in de linkerkant van (i).
Als f en f^1 inekwivalent zijn, dan volgt uit Lemma 4.1.7.

$$0 = (a_u)_{i,j} = \sum_{g\in G} F(g)_{i,s}\, F^1(g^{-1})_{t,j}\quad ,$$

waarmee (i) bewezen is.
We gaan door met (ii). Daartoe kiezen we $f^1 = f$ en gebruiken we het tweede deel van Lemma 4.1.7. Dit geeft de eksistentie van een $\lambda_{s,t} \in \mathbb{C}$ zodat

$$\lambda_{s,t}\delta_{i,j} = (a_u)_{i,j} = \sum_{g\in G} F(g)_{is}\, F(g^{-1})_{tj} \text{ voor alle } i,j,s,t, \in \underline{m}.$$

Door sommatie over $g \in G$ te vervangen door de gelijkwaardige sommatie over $g^{-1} \in G$ krijgen we

$$\lambda_{s,t}\delta_{i,j} = \sum_{g\in G} F(g)_{tj}\, F(g^{-1})_{is} = \lambda_{j,i}\delta_{s,t}.$$

We konkluderen dat er een $\lambda \in \mathbb{C}$ bestaat zo dat

$$\sum_{g\in G} F(g)_{is}F(g^{-1})_{tj} = \lambda\delta_{i,j}\delta_{s,t}.$$

We zijn dus klaar als we aantonen dat $\lambda = \frac{|G|}{n}$. Voor elke $i,s \in \underline{n}$ geldt blijkens het voorgaande

$$\sum_{g\in G} F(g)_{is}F(g^{-1})_{si} = \lambda,$$

zodat

$$|G| = \sum_{g\in G} F(1)_{ii} = \sum_{g\in G} (F(g)F(g^{-1})_{i,i} = \sum_{g\in G}\sum_{s\in \underline{n}} F(g)_{is}\, F(g^{-1})_{si} =$$

$$= \sum_{s\in \underline{n}}\sum_{g\in G} F(g)_{is}\, F(g^{-1})_{si} = n\lambda. \quad \square$$

4.1.9. NOTATIE. In het hierna volgende korollarium zullen we de voor een willekeurige verzameling X gedefiniëerde vektorruimte $\mathbb{C}^X$ van de funkties $f : X \to \mathbb{C}$ verwerken. (Er wordt daar in het bijzonder X = G genomen.) De optelling en skalair-vermenigvuldiging van die vektorruimte is puntsgewijs gedefiniëerd. Dat betekent voor $\alpha \in \mathbb{C}$, $f,g \in \mathbb{C}^X$:

$$\begin{cases} (f+g)(x) = f(x)+g(x) & (x \in X) \\ (\alpha f)(x) = \alpha.f(x) & (x \in X) \end{cases}$$

Merk op dat de operatie + respektievelijk $\cdot$ in het rechterlid op $\mathbb{C}$ (en dus wel-) gedefiniëerd zijn. De funkties $(\delta_x)_{x\in X}$ in $\mathbb{C}^X$ gegeven door

$$\delta_x(y) = \begin{cases} 0 \text{ als } x \neq y \\ 1 \text{ als } x = y \end{cases} \qquad (y\in X)$$

vormen een basis van $\mathbb{C}^X$. Bijgevolg is de dimensie van $\mathbb{C}^X$ gelijk aan $|X|$.

Ga na dat Stelling 4.1.8. in feite een uitspraak is over de funkties $g \mapsto F(g)_{ij}$ in $\mathbb{C}^G$. We zullen deze funkties met F_{ij} aangeven.

4.1.10. KOROLLARIUM. *Laat G een eindige groep zijn. Veronderstel dat* $f^1,\ldots,f^t$ *onderling niet-ekwivalente irreducibele voorstellingen over* $\mathbb{C}$ *van G zijn. Er geldt:*

(i) *Als* $F^1,\ldots,F^t$ *bij* $f^1,\ldots,f^t$ *horende matrixvoorstellingen zijn, dan zijn de funkties* $F^s_{ij} : G \to \mathbb{C}$ *lineair onafhankelijk in* $\mathbb{C}^G$.

(ii) *Als* n_i *de graad van* f^i *is* $(1 \le i \le t)$, *dan is* $\sum_{i=1}^t n_i^2 \le |G|$.

BEWIJS. Ga zelf na dat (ii) onmiddellijk uit (i) volgt door een dimensieoverweging. Om (i) te bewijzen nemen we aan dat de betreffende funkties aan een lineaire vergelijking voldoen: stel er zijn $\lambda^s_{ij} \in \mathbb{C}$ $(s \in \underline{t};$ $1 \le i,j \le n_s)$, zo dat

$$\sum_{i,j,s} \lambda^s_{ij} F^s_{ij} = 0.$$

Dan volgt na vermenigvuldiging met $g \mapsto F^r_{k\ell}(g^{-1})$ en sommatie over alle $g \in G$

$$\sum_{g\in G} \sum_{i,j,s} \lambda^s_{ij} F^s_{ij}(g) F^r_{k\ell}(g^{-1}) = 0.$$

De stelling geeft na verwisseling van sommatie-indices

$$\frac{\lambda^r_{\ell k} |G|}{n_i} = 0, \text{ dus } \lambda^r_{\ell k} = 0. \quad \square$$

Uit (ii) van dit korollarium volgt dat een eindige groep G slechts eindig veel onderling niet-ekwivalente irreducibele karakters kan hebben. In de volgende paragraaf zullen we zien dat het totale aantal altijd precies zoveel bedraagt dat in (ii) gelijkheid bereikt kan worden.

4.1.11. VOORBEELDEN.

(i) De voorstellingen f^s $(1 \leq s \leq n)$ van $C_n = \langle c \rangle$ in $\mathbb{C}$ gegeven door

$$c^r \mapsto \exp(2\pi irs/n) \quad (r \in \underline{n}),$$

zijn alle onderling verschillend (hoe ziet u dit in?) en van graad 1. Omdat $\sum_{s=1}^{n} 1^2 = n = |C_n|$ volgt uit 4.1.9 dat dit op ekwivalentie na alle irreducibele voorstellingen van C_n zijn. Met behulp van de hoofdstelling van de abelse groepen (zie 2.1.1 en 2.2.5) zullen we zometeen in 4.1.12 zien dat elke irreducibele voorstelling van een abelse groep graad 1 heeft. De moeilijkheden die zich voordoen bij irreducibele voorstellingen over echt in $\mathbb{C}$ bevatte lichamen doemen al op bij het lichaam $\mathbb{R}$ der reële getallen; de voorstelling $f : C_n \to Gl_2(\mathbb{R})$ gegeven door

$$f(c^r) = \begin{pmatrix} \cos \frac{2\pi r}{r} & -\sin \frac{2\pi r}{n} \\ \sin \frac{2\pi r}{n} & \cos \frac{2\pi r}{n} \end{pmatrix}$$

is irreducibel over $\mathbb{R}$ maar reducibel over $\mathbb{C}$.

(ii) Schrijven we $D_n = \langle a,b \mid a^n = b^2 = 1;\ bab = a^{-1} \rangle$, vergelijk 1.1.11, dan wordt voor $s \in \mathbb{N}$ $(1 \leq s \leq \frac{n-1}{2})$

door $\begin{cases} a \mapsto \begin{pmatrix} e^{\frac{2\pi i s}{n}} & 0 \\ 0 & e^{-\frac{2\pi i s}{n}} \end{pmatrix} \\ b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{cases}$

een voorstelling f^s van graad 2 bepaald.
Laat zelf zien dat ze irreducibel zijn voor $n \geq 3$ (ziet U waarom $s \neq 0$?).
Als n even is, dan onderscheiden we 4 voorstellingen $h^{\varepsilon_1,\varepsilon_2}$ van graad 1, geïndiceerd door $(\varepsilon_1,\varepsilon_2)$ met $\varepsilon_1,\varepsilon_2 \in \{\pm 1\}$, te weten

$$h^{\varepsilon_1,\varepsilon_2}(a) = (-1)^{\varepsilon_1}; \quad h^{\varepsilon_1,\varepsilon_2}(b) = (-1)^{\varepsilon_2}.$$

Als n oneven is, dan onderscheiden we 2 voorstellingen h^{ε} van graad 1 (waar $\varepsilon \in \{\pm 1\}$), en wel

$$h^{\varepsilon}(a) = 1; \quad h^{\varepsilon}(b) = (-1)^{\varepsilon}.$$

Beschouwing van de eigenwaarden van a levert dat de aangegeven voorstellingen alle onderling niet ekwivalent zijn (hier speelt de bovengrens voor s een rol!). Als n even is, bedraagt de som van de kwadraten der graden

$$4 + 4.\left[\frac{n-1}{2}\right] = 2n,$$

als n oneven is bedraagt die som

$$2 + 4.\ \frac{n-1}{2} = 2n.$$

Er volgt weer met 4.1.10 (ii) dat we alle voorstellingen van D_n kennen ($n \geq 3$; hoe zit het met D_2?). Merk op dat $f^s(D_n)$ als verzameling slechts afhangt van de restklasse van ggd(s,n) modulo n. Hieruit blijkt

dat automorfismen van $f^s(D_n)$ bestaan die niet inwendig zijn in $Gl_2(\mathbb{C})$. Onderzoek zelf voor welke s de voorstelling getrouw is.

De ekwivalentieklassen van irreducibele voorstellingen van een abelse groep worden nu bepaald. Vanwege 2.1.11 en 2.2.5 kunnen we een abelse groep altijd als een direkt produkt van cyklische groepen schrijven.

4.1.12. PROPOSITIE. *Laat* $A = C_{m_1}\times\ldots\times C_{m_r}$ *een abelse groep zijn. Kies voortbrengers* a_i *van* C_{m_i}. *Dan is elke irreducibele komplexe voorstelling ekwivalent met precies één der voorstellingen* $f^t : A \to \mathbb{C}$ *gegeven door*

$$f^t(a_1^{k_1}\ldots a_r^{k_r}) = \prod_{s=1}^{r} e^{\frac{2\pi i k_s t_s}{m_s}}$$

voor $t = (t_1,t_2,\ldots,t_r)$ *met* $t_s \in \underline{m}_s$.

BEWIJS. Ga zelf na dat alle f^t onderling inekwivalent, irreducibel en van graad 1 zijn. De som van de kwadraten der graden bedraagt het aantal mogelijke vektoren $t = (t_1,t_2,\ldots,t_r)$ met $t_s \in \underline{m}_s$, dus $\prod_{s=1}^{r} m_s = |A|$. De stelling volgt nu uit (4.1.10) (ii). □

We brengen in herinnering dat met D(G) de kommutatorgroep van G aangegeven wordt (zie 1.6.11).

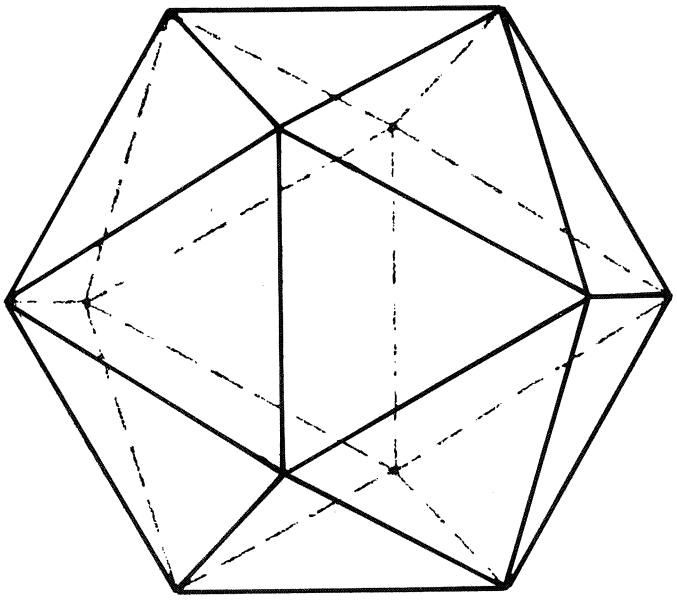
4.1.13. GEVOLG. *Als* G *een eindige groep is, dan is* $|G/D(G)|$ *het aantal ekwivalentieklassen van lineaire voorstellingen van* G *van graad* 1.

BEWIJS. Als f een voorstelling van G van graad 1 is, dan is het beeld f(G) abels (zelfs cyklisch, zie 1.1.10); dus omvat de kern Ker f vanwege 1.6.12 de kommutatorgroep D(G) van G. Er volgt dat f opgevat kan worden als een voorstelling van G/D(G). Andersom kan elke irreducibele voorstelling van G/D(G) (vanwege 4.1.12 steeds van graad 1) middels het in Lemma 4.1.3 (i) beschreven proces als voorstelling van G gezien worden. We hebben een 1-1 korrespondentie verkregen tussen de voorstellingen van G van graad 1 en alle irreducibele voorstellingen van G/D(G). De uitspraak volgt nu uit 4.1.12 omdat G/D(G) abels is en dus $|G/D(G)|$ irreducibele voorstellingen heeft. □

Tot slot van deze paragraaf bekijken we een lineaire voorstelling van een welbekende groep als groep van isometrieën van een icosaeder.

4.1.14. VOORBEELD. Beschouw de icosaeder: het regelmatige 20-vlak met 30 ribben en 12 hoekpunten in de Euclidische ruimte $\mathbb{R}^3$. Figuur 1 bevat er een

schets van. We stellen ons ten doel de groep G van alle isometrieën van de ruimte te bepalen die deze icosaeder in zichzelf overvoeren.



Figuur 1

Het zwaartepunt van de icosaeder moet op zijn plaats blijven; dit kiezen we dan ook als oorsprong. Bijgevolg hebben we te maken met een groep van lineaire transformaties. Het is natuurlijk mogelijk de punten van de icosaeder te koördinatiseren (alleen de afstand van een punt tot de oorsprong is nog vrij te kiezen), maar we zullen hier zonder zo'n koördinatisering te werk gaan. G bevat spiegelingen: neem twee overstaande (evenwijdige) ribben; de spiegeling aan het vlak opgespannen door die twee ribben is een isometrie die de icosaeder in zichzelf overvoert. Laat N de ondergroep van G zijn die bestaat uit alle draaiïngen. Omdat het product van een even aantal spiegelingen een draaiïng is, heeft N index 2 in G. Er zijn drie soorten draaiingen te onderscheiden: hun assen gaan respektievelijk door twee overstaande hoekpunten, door de zwaartepunten van twee overstaande zijvlakken en door de middens van twee overstaande ribben. Hun ordes zijn respektievelijk

5,3,2. Met behulp van deze elementen is het niet moeilijk aan te tonen dat N drie transitieve permutatievoorstellingen heeft: op de 12 punten, op de 30 ribben en op de 20 zijvlakken. Beschouw zelf de stabilisator in G van een element uit een van deze verzamelingen om af te leiden dat $|G| = 120$ (gebruik 1.4.8.). Alle drie permutatievoorstellingen zijn imprimitief, immers de paren overstaande punten, ribben resp. zijvlakken vormen blokken voor een imprimitiviteitssysteem. Maar in het geval van de ribben zijn de blokken nog groter te kiezen: de 15 "richtingen" (= paren overstaande ribben) vallen uiteen in 5 assenkruizen (=3-tallen onderling loodrechte richtingen). G en N hebben dus homomorfe beelden in $\mathrm{Sym}(\underline{5})$. Door na te gaan door wat voor permutatie een draaiing (van orde 5,3,2) en een spiegeling op deze 5 assenkruizen induceert, is snel in te zien dat het beeld van zowel N als G de hele groep $\mathrm{Alt}(\underline{5})$ is. Vergelijking van ordes geeft tenslotte dat deze permutatievoorstelling van N getrouw is. Met andere woorden, $N \cong \mathrm{Alt}(\underline{5})$. We hebben dus een lineaire voorstelling d van $\mathrm{Alt}(\underline{5})$ van graad 3 verkregen. Ga zelf na dat d irreducibel is. Als u nog in de struktuur van G geïnteresseerd bent, bekijk dan de puntspiegeling s aan de oorsprong (het niet-triviale element dat de richtingen vasthoudt) en leid af dat $G = N \times \langle s \rangle \cong \mathrm{Alt}(\underline{5}) \times C_2$.

OPGAVEN BIJ §4.1.

1. Leid af dat een abelse groep dan en slechts dan een getrouwe irreducibele komplexe voorstelling heeft als ze cyklisch is.

*2. Bepaal alle ekwivalentieklassen van irreducibele voorstellingen over $\mathbb{C}$ van de quaterniongroep Q uit Vraagstuk 1.1.9.

3. Bewijs de omgekeerde implikatie van een deel van het lemma van Schur: Als f een voorstelling in V over $\mathbb{C}$ van een eindige groep G is waarvoor geldt

$$\{A \in \mathrm{Gl}(V) \mid Af_g = f_g A\} \subseteq \{\lambda 1_V \mid \lambda \in \mathbb{C}\},$$

dan is f irreducibel.

*4. Bewijs: Als f, h, f', h' voorstellingen van G zijn zo dat f ekwivalent met f' en h ekwivalent met h' is, dan is $f \oplus h$ ekwivalent met $f' \oplus h'$.

*5. Laat V een lineaire ruimte over een lichaam K zijn. Met $P_m(V)$ geven we de

verzameling van alle homogene m-de graads polynoomfunkties op V over K aan, dat wil zeggen $P \in P_m(V)$ dan en slechts dan als er een basis $x_1,\ldots,x_n$ van V is en er $a_{i_1\ldots i_n} \in K$ met $i_1+i_2+\ldots+i_n = m$ zijn zo dat

$$P(\alpha_1x_1+\alpha_2x_2+\ldots\alpha_nx_n) = \sum_{\substack{(i_1,\ldots,i_n)\\ i_1+i_2+\ldots+i_n=m}} a_{i_1,\ldots,i_n}\,\alpha_1^{i_1}\ldots\alpha_n^{i_n}$$

voor alle $\alpha_i \in K \quad (i=1,\ldots,n)$.

(i) Laat $x_1,\ldots,x_n$ een basis van V zijn. Bewijs dat $P \in P_m(V)$ dan en slechts dan als f een polynoomfunktie ten opzichte van de basis $x_1,\ldots,x_n$ is (Met andere woorden, het begrip polynoomfunktie hangt niet van de gekozen basis af.

(ii) Laat zien dat $P_m(V)$ een lineaire deelruimte over K is.

(iii) Laat f een lineaire voorstelling van een groep G in V zijn. Toon aan dat $f^{(m)} : G \to Gl(P_m(V))$ gedefiniëerd door

$$(f_g^{(m)}(P))(x) = P(f_{g^{-1}}(x)) \qquad (P \in P_m(V),\ g \in G,\ x \in V)$$

een lineaire voorstelling van G in $P_m(V)$ is.

(iv) Bewijs dat de dimensie $d_{m,n}$ van $P_m(V)$ en dus de graad van $f^{(m)}$ het aantal n-tupels $(i_1,i_2,\ldots,i_n)$ met $m = i_1+i_2+\ldots+i_n$ is, door aan tonen dat de funkties

$$\alpha_1x_1+\alpha_2x_2+\ldots+\alpha_nx_n \mapsto \alpha_1^{i_1}\ldots\alpha_n^{i_n}$$

(ten opzichte van een vaste gekozen basis $x_1,\ldots,x_n$ van V) een basis van $P_m(V)$ vormen.
Kunt U ook nog afleiden dat dit getal $d_{m,n}$ gegeven wordt door

$$d_{m,n} = \sum_{\substack{(p_1,\ldots,p_m)\\ m=p_1+2p_2+\ldots+mp_m}} \frac{n^{p_1+p_2+\ldots+p_m}}{p_1!\ldots p_m!\ 1^{p_1}\ 2^{p_2}\ldots m^{p_m}} \qquad \text{of door}$$

$$d_{m,n} = \binom{m+n-1}{m}, \qquad \text{of door}$$

$$d_{m,n} = \sum_{k=1}^{m} \frac{d_{m-k,n}\ .\ n}{m}, \qquad \text{als we nog } d_{0,n} = 1 \text{ schrijven?}$$

*6. Als de eindige groep G voorstellingen f resp. f' in de lineaire ruimtes V resp. V' over K heeft, dan kunnen we een voorstelling $f * f'$ van G in de lineaire ruimte M(V',V) van alle lineaire afbeeldingen van V' naar V definiëren door

$$((f * f')_g A)(x) = f_g A(f'^{-1}_g(x))$$

voor $g \in G$, $A \in M(V',V)$, $x \in V'$.
Bewijs dit. Ga na dat de graad van $f * f'$ het produkt van de graad van f en die van f' is.

7. Laat G een eindige groep zijn en $\alpha \in \mathrm{Aut}(G)$ en laat f een lineaire voorstelling van G zijn.
   (i) Bewijs dat f^α gedefiniëerd door $f^\alpha(g) = f(g^\alpha)$ voor $g \in G$ weer een lineaire voorstelling van G is.
   (ii) Laat zien dat f^α dan en slechts dan irreducibel is als f irreducibel is.

4.2. Het karakter van een voorstelling

Vanaf nu zullen we ons beperken tot de studie van komplexe lineaire voorstellingen (dus $K = \mathbb{C}$). Om in te zien of twee voorstellingen inekwivalent zijn, kan kennis van eigenwaarden van de verschillende matrices van pas komen. Dit vond plaats in Voorbeeld 4.1.11 (ii). Voor het probleem welke voorstellingen ekwivalent zijn is de kennis van het spoor, dat is de som van de eigenwaarden, van elke optredende matrix echter al toereikend.

4.2.1. DEFINITIE. Het *spoor* van een m×m - matrix A (notatie: sp(A)), is de som van de hoofddiagonaalelementen: $\sum_{i=1}^{m} A_{ii}$. Bijvoorbeeld door uitschrijven met behulp van de definitie, verifiëert men eenvoudig dat voor twee m×m - matrices A,B geldt sp(AB) = sp(BA). In het bijzonder volgt als A inverteerbaar is: $sp(B) = sp(ABA^{-1})$. Men kan dan spreken van het *spoor van een lineaire afbeelding* a: V → V (V is hier een eindige vektorruimte). Immers, door sp(a) = sp(A) als A de matrix van a ten opzichte van de basis van V is, is het spoor sp(a) goed gedefiniëerd. Laat nu f een voorstelling van een groep G in een vektorruimte V over het lichaam K zijn. Onder het *karakter* χ_f van f verstaan we de afbeelding $\chi_f : G \to K$ gegeven door $\chi_f(g) = sp(f_g)$. We noemen χ_f ook wel een karakter van G. Een *irreducibel karakter* is een karakter van een irreducibele voorstelling. Met Irr(G) geven we de verzameling irreduci-

bele karakters van G aan. Uit 4.1.10 blijkt dat dit een eindige verzameling is.

4.2.2. PROPOSITIE.
(i) *Twee ekwivalente voorstellingen over* $\mathbb{C}$ *hebben hetzelfde karakter.*
(ii) *Als* $f = f_1 \oplus f_2$, *dan* $\chi_f = \chi_{f_1} + \chi_{f_2}$.

BEWIJS. (i) volgt rechtstreeks uit het voorafgaande, terwijl (ii) ook neer komt op een eenvoudige eigenschap van het spoor. □

Deel (i) van de propositie betekent dat het voldoende is opdat twee voorstellingen inekwivalent zijn dat hun karakters ongelijk zijn. Het volgende resultaat laat niet alleen zien dat dit ook noodzakelijk is, maar geeft ook een snelle manier om na te gaan of aan deze gelijkheid voldaan wordt.

4.2.3. LEMMA. *Laat* χ *een karakter van* G *zijn, afkomstig van de komplexe voorstelling* f *en laat* $g \in G$. *Dan geldt:*
(i) $\chi(1)$ *is de graad van* f;
(ii) $\chi(g)$ *is de som van* $\chi(1)$ m*de-eenheidswortels waar* m *de orde van* g *is;*
(iii) $\overline{\chi(g)} = \chi(g^{-1})$
(iv) *Voor* $h \in G$ *is* $\chi(ghg^{-1}) = \chi(h)$; *met andere woorden,* χ *is konstant op de konjugatieklassen van* G.

BEWIJS. Laat n de graad van f zijn. Volgens 4.1.6. (iv) is $\chi(g)$ de som van n eigenwaarden $\lambda_1,\ldots,\lambda_n$ van g. Als $g = 1$ zijn deze alle $= 1$, zodat $n = \chi(1)$. Dit geeft (i) en (ii). Omdat g^{-1} eigenwaarden $\lambda_1^{-1},\ldots,\lambda_n^{-1}$ heeft geldt $\overline{\chi(g)} = \sum_{i=1}^{n} \overline{\lambda}_i = \sum_{i=1}^{m} \lambda_i^{-1} = \chi(g^{-1})$, zodat (iii) verkregen is. Tenslotte volgt (iv) uit de formule $sp(B) = sp(ABA^{-1})$ voor het spoor van een lineaire afbeelding B bij gegeven lineaire transformatie A. □

4.2.4. NOTATIE. Een funktie $\phi \in \mathbb{C}^G$ (zoals een karakter) die konstant is op de konjugatieklassen van G, kunnen we opvatten als een funktie op de verzameling konjugatieklassen $K(G)$ (of kortweg K) van G door het voorschrift $\phi(K) = \phi(g)$ voor $g \in K \in K$. Andersom, is iedere $\phi \in \mathbb{C}^K$ eenduidig te zien als funktie $\phi \in \mathbb{C}^G$ die konstant is op de konjugatieklassen van G. We kunnen dus $\mathbb{C}^K$ naar willekeur opvatten als een lineaire deelruimte van $\mathbb{C}^G$ dan wel als de vektorruimte van komplexwaardige funkties op K. Op $\mathbb{C}^G$ definiëren we de binaire operator $\langle \cdot | \cdot \rangle : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}$ door

$$\langle \phi | \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\, \overline{\psi(g)}, \qquad (\phi, \psi \in \mathbb{C}^G),$$

waarin de streep op komplexe konjugatie slaat. Deze operator wordt een hermiets inprodukt genoemd omdat hij voldoet aan de volgende eigenschappen. Voor elke $\phi,\chi,\psi \in \mathbb{C}^G$ geldt:

(i) $\langle\phi|\phi\rangle = 0 \Leftrightarrow \phi = 0$.

(ii) $\langle\alpha\phi+\beta\psi|\chi\rangle = \alpha\langle\phi|\chi\rangle+\beta\langle\psi|\chi\rangle \qquad (\alpha,\beta \in \mathbb{C})$.

(iii) $\langle\phi|\chi\rangle = \overline{\langle\chi|\phi\rangle}$.

(iv) $\langle\chi|\alpha\phi + \beta\psi\rangle = \overline{\alpha}\,\langle\chi|\phi\rangle + \overline{\beta}\,\langle\chi|\psi\rangle \qquad (\alpha,\beta \in \mathbb{C})$.

Ga zelf na dat (iv) uit (ii) en (iii) volgt.

4.2.5. STELLING. *Laat f^1,f^2 een tweetal lineaire voorstellingen van een eindige groep G over $\mathbb{C}$ zijn, met karakter χ_1 respektievelijk χ_2. Veronderstel dat f^2 irreducibel is. Dan geldt:*

(i) $\langle\chi_1|\chi_2\rangle$ *is het aantal met f^2 ekwivalente voorstellingen dat in een direkte-som-splitsing van f^1 voorkomt.*

(ii) $\langle\chi_1|\chi_1\rangle = 1 \Leftrightarrow f^1$ *is irreducibel.*

(iii) *Als f^1 ook irreducibel is, dan is $\langle\chi_1|\chi_2\rangle = 0$ tenzij f^1 ekwivalent met f^2 is.*

(iv) $\overline{\chi}_2$ *is een irreducibel karakter van* G.

BEWIJS. Laat F^1 resp. F^2 een matrixvoorstelling van f^1 resp. f^2 zijn

$$\begin{aligned}\langle\chi_1|\chi_2\rangle &= \frac{1}{|G|}\sum_{g\in G}\chi_1(g)\,\overline{\chi_2(g)}\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_1(g)\,\chi_2(g^{-1})\\ &= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{i=1}^{\chi_1(1)}(F^1(g))_{ii}\Big)\Big(\sum_{j=1}^{\chi_2(1)}(F^2(g^{-1}))_{jj}\Big)\\ &= \frac{1}{|G|}\sum_{i,j,g}F^1(g)_{ii}F^2(g^{-1})_{jj}.\end{aligned}$$

Stel nu dat f^1 ook irreducibel is. Dan geldt volgens Stelling 4.1.8.

$$\langle\chi_1|\chi_2\rangle = \begin{cases} 0 \text{ als } f^1 \text{ en } f^2 \text{ inekwivalent zijn} \\ \dfrac{1}{|G|}\displaystyle\sum_{i,g}F^1(g)_{ii}F^2(g^{-1})_{ii} = 1 \text{ als } f^1 = f^2 \end{cases}$$

Dit bewijst (iii) en de helft van (ii).

Als χ_1 echter reducibel is, dan geldt vanwege Propositie 4.2.2. (iii) en 4.1.5. dat $\chi_1 = \sum_{\psi\in Irr(G)} n_\psi \psi$, waarin n_ψ de multipliciteit van ψ in χ_1 is. De eigenschappen van het unitair inprodukt leiden nu tot

$$\langle \chi_1 | \chi_2 \rangle = \sum_{\psi\in Irr(G)} n_\psi \langle \psi | \chi_2 \rangle = n_{\chi_2},$$

wat (i) bewijst. Rest de andere helft van (ii) te bewijzen. Stel $\langle \chi_1 | \chi_1 \rangle = 1$. Dan met voorgaande splitsing en bedenkend dat $\langle \psi | \chi_1 \rangle = n_\psi$ omdat n_ψ reëel is:

$$\sum_{\psi\in Irr(G)} n_\psi^2 = 1,$$

waaruit volgt dat $n_\psi = 1$ voor precies één $\psi \in Irr(G)$, terwijl $n_\phi = 0$ voor $\phi \neq \psi$. Dit betekent dan $\chi_1 = \psi \in Irr(G)$.
(iv) Ga zelf na dat de getransponeerde matrix van $(F_g^2)^{-1}$, genoteerd $((F_g^2)^{-1})^t$, toegevoegd aan $g \in G$ tot een voorstelling leidt. Uit spoor $(((F_g^2)^{-1})^t)$ = spoor $((f_g^2)^{-1})$ = spoor $(f_{g^{-1}}^2) = \chi_2(g^{-1}) = \overline{\chi_2(g)} = \bar{\chi}_2(g)$ volgt dat $\bar{\chi}_2$ het spoor van de voorstelling is. Irreducibiliteit wordt verkregen door $\langle \bar{\chi}_2 | \chi_2 \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_2(g)}\ \overline{\chi_2(g^{-1})} = \langle \chi_2 | \chi_2 \rangle = 1$.

4.2.6. KOROLLARIUM. *Als* f *een lineaire voorstelling van* G *over* $\mathbb{C}$ *is, dan hangt de direkte somsplitsing* $f = f^1 \oplus \ldots \oplus f^t$ *van* f *in irreducibele voorstellingen slechts tot op volgorde en ekwivalentie van de* f^i $(1 \leq i \leq t)$ af.

BEWIJS. De uitspraak zegt dat het aantal met een gegeven irreducibele voorstelling van G ekwivalente deelvoorstellingen van f niet van de gekozen direkte somsplitsing afhangt. Volgens de stelling is dit aantal een inprodukt van twee karakters dus inderdaad daarvan onafhankelijk. □

4.2.7. KOROLLARIUM. *Als* f^1, f^2 *lineaire komplexe voorstellingen zijn van* G *met karakters* χ_1 *respektievelijk* χ_2, *dan zijn* f^1 *en* f^2 *ekwivalent dan en slechts dan als* $\chi_1 = \chi_2$.

BEWIJS. In 4.2.2. (i) is al bewezen dat $\chi_1 = \chi_2$ als f^1 en f^2 ekwivalent zijn. Stel $\chi_1 = \chi_2$. Als f^2 irreducibel is, dan volgt uit 4.2.5. (i) en (iii) dat f^1 en f^2 ekwivalent zijn. Het algemene geval volgt nu omdat f^1, f^2 beide een direkte somsplitsing met onderling overeenstemmende karakters hebben (vergelijk Opgave 4.1.4.). □

4.2.8. PROPOSITIE. *Laat* G *een eindige groep zijn. Dan geldt:*

(i) $\sum_{\phi\in Irr(G)} \phi(1)^2 = |G|$

(ii) $Irr(G)$ vormt een basis van $\mathbb{C}^K$

(iii) $|Irr(G)| = |K(G)|$.

BEWIJS.

(i) Schrijf het *reguliere karakter* ρ van de reguliere voorstelling f^G uit 4.1.2 (iii) als som van irreducibele:

$$\rho = \sum_{\psi\in Irr(G)} n_\psi \psi.$$

Dan volgt voor $\phi \in Irr(G)$ enerzijds met de stelling dat $\langle\rho|\phi\rangle = n_\phi$, anderzijds met behulp van de definitie

$$\langle\rho|\phi\rangle = \frac{1}{|G|} \sum_{g\in G} \rho(g)\,\overline{\phi(g)} = \overline{\phi(1)} = \phi(1).$$

Derhalve is $n_\phi = \phi(1)$, zodat

$$|G| = \rho(1) = \sum_{\psi\in Irr(G)} n_\psi \psi(1) = \sum_{\psi\in Irr(G)} \psi(1)^2 .$$

(ii) We zullen eerst aantonen dat $Irr(G)$ uit onafhankelijke funkties in $\mathbb{C}^K$ bestaat. Laat daartoe $\lambda_\psi \in \mathbb{C}$ voor $\psi \in Irr(G)$ gegeven zijn zo dat

$$\sum_{\psi\in Irr(G)} \lambda_\psi \psi = 0.$$

Dan volgt na het nemen van het hermiets inprodukt met $\phi \in Irr(G)$ vanwege 4.2.5

$$0 = \langle \sum_{\psi\in Irr(G)} \lambda_\psi \psi, \phi\rangle = \lambda_\phi ; \text{ klaar.}$$

Laat nu $\phi \in \mathbb{C}^K$ gegeven zijn. We bewijzen de gelijkheid $\phi = \sum_{\psi\in Irr(G)} \langle\phi|\psi\rangle\psi$. Schrijf $\chi = \phi - \sum_{\psi\in Irr(G)} \langle\phi|\psi\rangle\psi$. Dit is een funktie in $\mathbb{C}^K$ waarvoor $\langle\chi|\zeta\rangle = 0$ $(\zeta\in Irr(G))$. Beschouw nu de lineaire afbeelding t van $V = \bigoplus_{g\in G} \mathbb{C}e_g$ naar zichzelf (vergelijk 4.1.2 (iii)) gegeven door

$$t = \sum_{g\in G} \chi(g^{-1}) f^G_g \quad \text{met } f^G \text{ als in 4.1.2 (iii).}$$

Er geldt $f_h^G t = t f_h^G$ voor elke $h \in G$, immers

$$f_h^G t = \sum_{g\in G} \chi(g^{-1}) f_h^G f_g^G = \sum_{g\in G} \chi(g^{-1}) f_{hgh^{-1}}^G f_h^G =$$

$$= \sum_{g\in G} \chi(h^{-1}g^{-1}h) f_g^G f_h^G = t\, f_h^G$$

(waar in de op een na laatste gelijkheid van sommatie over $g \in G$ op sommatie over h $gh^{-1} \in G$ is overgegaan en in de laatste gelijkheid $\phi \in \mathbb{C}^K$ gebruikt wordt). Toepassing van het Lemma van Schur (4.1.7) levert dat de beperking $t|_W$ van t tot een onder f^G irreducibele deelruimte W van V voor zekere $\lambda_W \in \mathbb{C}$ de vorm $t|_W = \lambda_W . id_W$ heeft. Zij ψ het karakter van G behorend bij $f^G|W$. Dan geldt

$$(\dim W).\lambda_W = \text{spoor}(t|_W) = \sum_{g\in G} \chi(g^{-1}) \text{spoor}(f_g^G|_W) =$$

$$= \sum_{g\in G} \chi(g^{-1})\psi(g) = |G|\ \langle\psi|\chi\rangle = \overline{|G|\ \langle\chi|\psi\rangle} = 0\ .$$

Aldus blijkt $t|_W = 0$ voor elke irreducibele deelruimte W van V. Met Maschke's stelling (4.1.5) volgt dan dat $t = 0$. In het bijzonder is

$$0 = t(e_1) = \sum_{g\in G} \chi(g^{-1}) f_g^G(e_1) = \sum_{g\in G} \chi(g^{-1}) e_g .$$

Omdat $(e_g)_{g\in G}$ een basis van V vormt, is dus $\chi(g) = 0$ voor elke $g \in G$, met andere woorden $\chi = 0$. De konklusie is dat elk element $\phi \in \mathbb{C}^K$ te schrijven is als lineaire kombinatie der $\psi \in \text{Irr}(G)$. Tezamen met de onafhankelijkheid van de elementen van $\text{Irr}(G)$, bewijst dit dat $\text{Irr}(G)$ een basis van $\mathbb{C}^K$ is.

(iii) De dimensie van $\mathbb{C}^K$ is enerzijds $|K|$, anderzijds vanwege (ii) gelijk aan $|\text{Irr}(G)|$. □

4.2.9. DEFINITIE. Voor een eindige groep G bestaat $\text{Irr}(G)$ dus uit precies $t = |K|$ funkties op K. We kunnen $\text{Irr}(G)$ dus beschrijven door een $t \times t$ matrix, waarin de rijen geindiceerd worden door de irreducibele karakters van G en de kolommen door de konjugatieklassen van G, terwijl de (χ,K)-plaats voor $\chi \in \text{Irr}(G)$, $K \in K(G)$ gevuld wordt met $\chi(K)$. Deze matrix, die voor

gegeven G op permutaties van rijen en kolommen na vast ligt, noemen we de *karaktertabel* van G. Het is een goed gebruik om het triviale karakter (vergelijk 4.1.2. (ii)) in de eerste rij en de inklasse {1} in de eerste kolom te zetten.

4.2.10. VOORBEELDEN.

(i) G = Sym(3). Aangezien Sym(3) = D_3, kennen we uit 4.1.10 (ii) reeds alle voorstellingen van Sym(3). Zoals te doen gebruikelijk geven we de inklassen aan door representanten:

Sym(3)	1	(12)	(123)	← inklassen
triviale karakter	1	1	1	
"teken"	1	-1	1	
dieder-voorstelling	2	0	-1	

↑
irreducibele
karakters

(ii) G = D_4 en G = Q. Uit 4.1.11 (ii) is eenvoudig af te leiden dat de karaktertabel voor D_4 er als volgt uitziet:

1	a^2	a	b	ab
1	1	1	1	1
1	1	-1	1	-1
1	1	1	-1	-1
1	1	-1	-1	1
2	-2	0	0	0

In Opgave 4.1.2. is gevraagd alle irreducibele voorstellingen van Q (op ekwivalentie na) te bepalen. De konjugatieklassen van Q bestaan uit {1}, $\{u^2\}$, $\{u,u^{-1}\}$, $\{v,v^{-1}\}$, $\{uv,v^{-1}u^{-1}\}$, waar u en v als in Opgave 1.6.9 gekozen zijn. Nu is D(Q) = Z(Q) en geldt $Q/Z(Q) \cong C_2 \times C_2$. Er zijn dus vier verschillende irreducibele karakters van graad 1. Er rest één irreducibel karakter van graad 2. Dit karakter hoort bij de 2×2-matrix-voorstelling van Q in Opgave 1.6.9. De tabel is nu eenvoudig op te

stellen: hij is dezelfde als die voor D_4! De irreducibele karakters van G voldoen volgens 4.2.4 aan de *orthogonaliteitsrelaties*:

$$\langle \phi | \psi \rangle = \begin{cases} 0 & \text{als } \phi \neq \psi \\ 1 & \text{als } \phi = \psi \end{cases} \qquad (\phi, \psi \in \mathrm{Irr}(G))$$

$\langle \cdot | \cdot \rangle$ is dus een inprodukt op de rijen van de karaktertabel ten opzichte waarvan ze orthogonaal zijn. Zo'n inprodukt is er ook voor de kolommen van de tabel, zoals we nu zullen afleiden. Voor de volledigheid vermelden we de oude orthogonaliteitsrelaties ook nog een keer.

4.2.11. PROPOSITIE. *Laat voor* G (*een eindige groep*)

$$K = \{K_1, \ldots, K_t\} \text{ en } \mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_t\}.$$

Dan geldt

(i) $$\sum_{r=1}^{t} |K_r| \, \chi_i(K_r)\bar{\chi}_j(K_r) = |G|\delta_{ij}$$

(ii) $$\sum_{r=1}^{t} \chi_r(K_i)\bar{\chi}_r(K_j) = \frac{|G|}{|K_i|}\delta_{ij}.$$

BEWIJS.

(i) is een herschrijving van Stelling 4.2.5 (ii) en (iii).

(ii) volgt uit (i): Beschouw de "op schaal gebrachte karaktertabel" U, waarvan de (i,j) koëfficiënt $U_{ij} = \chi_i(K_j)\sqrt{\frac{|K_j|}{|G|}}$ is. De uitspraak (i) komt in matrixvorm neer op $UU^* = I$, waar U^* de komplex gekonjugeerde van de getransponeerde matrix van U is; dat wil zeggen:

$$U^*_{i,j} = \overline{U_{j,i}} \quad (i,j \in \underline{t})$$

Maar $UU^* = I$ is ekwivalent met $U^*U = I$, immers linksinverse en rechtsinverse vallen samen. Uitschrijven van de (i,j)koëfficiënt geeft

$$\delta_{ij} = (U^*U)_{ij} = \sum_{r=1}^{t} \bar{\chi}_r(K_i)\sqrt{\frac{|K_i|}{|G|}}\,\chi_r(K_j)\sqrt{\frac{|K_j|}{|G|}} =$$

$$= \frac{\sqrt{|K_i||K_j|}}{|G|}\sum_{r=1}^{t}\chi_r(K_j)\bar{\chi}_r(K_i).$$

Hieruit volgt het gestelde onmiddellijk. □

In 4.2.11 (i) respektievelijk (ii) staat het zogenaamde *eerste* respektievelijk *tweede stelsel orthogonaliteitsrelaties*. Ze komen goed van pas bij het opstellen van een karaktertabel.

Andersom, als de tabel eenmaal gegeven is, kan men zich afvragen welke informatie zo'n tabel over de groep bevat. Getuige Voorbeeld 4.2.10 (ii), wordt een groep niet eenduidig door haar karaktertabel bepaald. Dat er toch nog veel vastgesteld kan worden uit de tabel blijkt wel uit de volgende propositie.

4.2.12. PROPOSITIE. *Zij* G *een eindige groep, laat* $K(G) = \{K_1,\ldots,K_t\}$ *en* $\mathrm{Irr}(G) = \{\chi_1,\ldots,\chi_t\}$ *zijn. Kies* $g \in K_k$ *en laat* $a_{ijk} = \#\{(g_i,g_j) \in K_i \times K_j \mid g_i g_j = g\}$. *Dan hangt* a_{ijk} *niet van de gekozen* $g \in K_k$ *af en geldt*

$$a_{ijk} = \frac{|K_i|\,|K_j|}{|G|} \sum_{r=1}^{t} \frac{\chi_r(K_i)\chi_r(K_j)\overline{\chi_r(K_k)}}{\chi_r(1)}$$

BEWIJS. Merk allereerst op dat als $(g_i,g_j) \in K_i \times K_j$ voldoet aan $g_i g_j = g$ voor $h \in G$ het paar $(h^{-1}g_i h, h^{-1}g_j h) \in K_i \times K_j$ voldoet aan $(h^{-1}g_i h)(h^{-1}g_j h) = h^{-1}gh$. Dit impliceert dat de definitie van a_{ijk} inderdaad niet afhangt van de keuze van $g \in K_k$. Beschouw nu om een formule voor a_{ijk} af te leiden, de uitdrukking

$$S_j = \sum_{g \in K_j} f_g,$$

waarin f een irreducibele voorstelling over $\mathbb{C}$ van G is, met karakter $\chi \in \mathrm{Irr}(G)$. Uit

$$f_h S_j = \sum_{g \in K_j} f_{hgh^{-1}} f_h = S_j f_h$$

volgt met 4.1.7 dat $S_j = \lambda_j I$ voor zekere $\lambda_j \in \mathbb{C}$. Maar het spoor van S_j kunnen we op twee manieren berekenen:

$$\chi(1)\lambda_j = \mathrm{sp}(S_j) = \mathrm{sp}\Big(\sum_{g \in K_j} f_g\Big) = \sum_{g \in K_j} \chi(g) = |K_j|\chi(K_j).$$

Er volgt dat

$$\lambda_j = \frac{|K_j|\chi(K_j)}{\chi(1)} \quad .$$

Uit de definitie van a_{ijk} volgt

$$\lambda_i\lambda_j I = S_i.S_j = \Big(\sum_{g_i\in K_i} f_{g_i}\Big)\Big(\sum_{g_j\in K_j} f_{g_j}\Big) = \sum_{(g_i,g_j)\in K_i\times K_j} f_{g_ig_j}$$

$$= \sum_{k=1}^{t} a_{ijk} \sum_{g\in K_k} f_g = \sum_{k=1}^{t} a_{ijk}\, S_k = \sum_{k=1}^{t} a_{ijk}\, \lambda_k I,$$

ofwel

$$\frac{|K_i|\ |K_j|\chi(K_i)\chi(K_j)}{\chi(1)} = \sum_{k=1}^{t} a_{ijk}|K_k|\chi(K_k).$$

Om het tweede stel orthogonaliteitsrelaties uit 4.2.11 (ii) toe te kunnen passen, vermenigvuldigen we beide zijden met $\overline{\chi(K_m)}$ en sommeren over $\chi \in \mathrm{Irr}(G)$. Dit geeft

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{|K_i||K_j|\chi(K_i)\chi(K_j)\overline{\chi(K_m)}}{\chi(1)} = \sum_{\chi\in\mathrm{Irr}(G)} \sum_{k=1}^{t} a_{ijk}|K_k|\chi(K_k)\overline{\chi(K_m)}$$

$$= \sum_{k=1}^{t} a_{ijk}|K_k| \sum_{\chi\in\mathrm{Irr}(G)} \chi(K_k)\overline{\chi(K_m)}$$

$$= \sum_{k=1}^{t} a_{ijk}|K_k| \frac{|G|}{|K_k|}\delta_{k,m} = a_{ijm}|G|,$$

waaruit de te bewijzen formule onmiddellijk volgt. □

Ga zelf na dat het tweede stel orthogonaliteitsrelaties een speciaal geval van de net bewezen propositie vormt. Met gebruikmaking van de theorie van algebraïsch gehelen kan bewezen worden dat de graad van een irreducibele voorstelling de orde van de groep (zelfs het quotient van de orde naar die van het centrum) deelt. We gaan hier nog wat nader op in.

4.2.13. DEFINITIE. Een veelterm

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad (a_i \in \mathbb{C})$$

heet *monisch* als zijn hoogste koëfficient aan $a_n = 1$ voldoet. Een komplex getal α heet *algebraisch geheel* als er een monische veelterm $f(x) = \sum_{i=0}^{n} a_i x^i$ bestaat met koëfficiënten $a_i \in \mathbb{Z}$ zodanig dat $f(\alpha) = 0$ (dat wil zeggen α is een *wortel* van $f(x)$).

De volgende eigenschappen van algebraïsch gehelen vermelden we zonder bewijs. Voor meer informatie over algebraïsch gehelen (waaronder de hier ontbrekende bewijzen) zij verwezen naar de boeken van Lang.

4.2.14. PROPOSITIE. *Laat* $\alpha,\beta \in \mathbb{C}$ *algebraïsch gehelen zijn.*

(i) $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ *zijn ook algebraïsch gehelen.*

(ii) *Laat* $f(x)$ *een monisch polynoom met koëfficienten in* $\mathbb{Q}$ *zijn van minimale graad zo dat* $f(\alpha) = 0$. *Dan liggen de koëfficiënten van* $f(x)$ in $\mathbb{Z}$.

(iii) *De veelterm* $f(x)$ *van* (ii) *is uniek bepaald door* α.

(iv) *Als* $\alpha \in \mathbb{Q}$, *dan* $\alpha \in \mathbb{Z}$.

(Ga na dat (iii) en (iv) uit (ii) volgen).

4.2.15. DEFINITIES. Het polynoom $f(x)$ als in (iii) van bovenstaande propositie heet de *minimum-veelterm* van de algebraïsche gehele α. De wortels van $f(x)$ heten de *algebraïsch gekonjugeerden* van α. Het produkt van de algebraïsch gekonjugeerden van α is de konstante term $f(0)$ van $f(x)$ en is dus een geheel getal. Dit getal heet de *norm* van α. Notatie $N(\alpha)$. Voor later gebruik (zie 5.2.8) vermelden we nog een hulpresultaat.

4.2.16. LEMMA. *Als* $\alpha \in \mathbb{C}$ *algebraisch geheel is met minimum-veelterm* $f(x)$ *en* $h(x)$ *een monische veelterm met wortel* α *en gehele koëfficiënten, dan geldt:*

(i) *er is een monische veelterm* $g(x)$ *met gehele koëfficiënten zo dat* $h(x) = f(x)g(x)$;

(ii) $N(\alpha)$ *is een deler van* $h(0)$.

Omdat n-de machts eenheidswortels wortels zijn van de monische veelterm x^n-1 zijn ze algebraïsch geheel. Gezien Propositie 4.2.14 (i) is dus ook een som van komplexe eenheidswortels algebraïsch geheel. 4.2.3 (ii) impliceert dat de waarden die het karakter aanneemt algebraïsch geheel zijn.

4.2.17. PROPOSITIE. *Laat* G *een eindige groep zijn. Dan geldt:*

(i) $\chi(g)$ *is een algebraisch gehele voor elk karakter* χ *van* G *en elke* $g \in G$.

(ii) *Als* $\chi \in \mathrm{Irr}(G)$ *en* $K \in \mathcal{K}(G)$, *dan is* $|K|\chi(K)/\chi(1)$ *een algebraïsch gehele.*

BEWIJS. (i) Is hierboven al behandeld. (ii) We gebruiken de notatie van 4.2.12. We moeten bewijzen dat de in het bewijs van die propositie voorkomende getallen λ_j algebraïsch geheel zijn. In dat bewijs was onderstaande gelijkheid afgeleid

$$\lambda_i\lambda_j I = \sum_{k=1}^{t} a_{ijk}\,\lambda_k I.$$

Als we de matrix $(a_{ijk})_{j,k\in \underline{t}}$ met A_i aangeven, valt de formule te herschrijven als

$$(A_i - \lambda_i I)\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_t\end{pmatrix} = 0.$$

Omdat $\lambda_1 = 1 \neq 0$ als $K_1 = \{1\}$, is λ_i een eigenwaarde van de matrix A_i (met eigenvektor de getransponeerde van $(\lambda_1,\ldots,\lambda_t)$). Er volgt $\det(\lambda_i I - A_i) = 0$. Dit betekent dat $\det(xI - A_i)$ een monische veelterm is met gehele koëfficiënten waarvan λ_i een wortel is. De konklusie is dat λ_i een algebraïsch gehele is. □

Tenslotte bewijzen we een al eerder aangekondigd resultaat over de graad van een irreducibele voorstelling.

4.2.18. PROPOSITIE. *Als* n *de graad van een irreducibele voorstelling van een eindige groep* G *is, dan geldt* $n \mid |G|$.

BEWIJS. Laat $\chi \in \mathrm{Irr}(G)$ met $n = \chi(1)$ en schrijf $K(G) = \{K_1,\ldots,K_t\}$. Uit

$$\frac{|G|}{n} = \frac{|G|}{n}\langle\chi|\chi\rangle = \sum_{i=1}^{t}\left(\frac{|K_i|\chi(K_i)}{n}\right)\overline{\chi(K_i)}$$

volgt dat $|G|/n$ een algebraïsch geheel is. Omdat het ook rationaal is, volgt met 4.2.14 (iv) dat $|G|/n$ zelfs geheel is. □

Ga zelf na dat dit resultaat te verscherpen is tot $n \mid |G/Z(G)|$ door aan te tonen dat $\chi(K_i) = 0$ voor een irreducibel getrouw karakter χ als $zK_i = K_i$ voor zekere $z \in Z(G)-\{1\}$.

OPGAVEN BIJ §4.2.

1. Stel de karaktertabel op van de groep G_0 van orde 16 uit Voorbeeld 2.2.7.

2. Bepaal de karaktertabel van Sym(4).

3. Beschouw Opgave 4.1.7. Druk het karakter van f^{α} uit in dat van f.

4. Laat f een komplexe lineaire voorstelling van G op een lineaire ruimte V zijn. Als $\chi \in \mathrm{Irr}(G)$, dan is

$$t = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})\,f_g.$$

een projektie van V op de lineaire deelruimte U bestaande uit de som van alle onder f invariante lineaire deelruimtes W van V waarvoor $\chi_{f^W} = \chi$ (met andere woorden, waarvoor de gerestringeerde voorstelling f^W van G tot W karakter χ heeft). Bewijs dit.
Toelichting: zie het bewijs van 4.1.5 (i) voor het begrip projektie.
Aanwijzing: Ga met t te werk als gedaan is in 4.2.8.

*5. Laat zien dat $\chi_f \cdot \bar{\chi}_{f'}$ het karakter is van de lineaire voorstelling f*f' van G uit opgave 4.1.6.

6. Laat G een lineaire voorstelling f in V hebben, en geef met $\chi^{(m)}$ het karakter van de voorstelling $f^{(m)}$ uit Opgave 4.1.5 aan. Schrijf χ_m voor de funktie in $\mathbb{C}^K$ gegeven door $\chi_m(g) = \chi(g^m)$. Bewijs dat

$$\chi^{(m)} = \sum_{k=1}^{m} \frac{\chi^{(m-k)} \cdot \chi_k}{m} \qquad \text{voor } m \geq 1,$$

als $\chi^{(0)} = 1$ (dat wil zeggen $\chi^{(0)}(g) = 1$ voor alle $g \in G$).

7. Bepaal alle isomorfieklassen van groepen die de volgende karaktertabel hebben

1	1	1	1	1	1	1	1
1	1	1	1	1	-1	-1	-1
2	2	2	-1	-1	0	0	0
3	3	-1	0	0	1	-1	-1
3	3	-1	0	0	-1	1	1
2	-2	0	-1	1	0	$\sqrt{2}i$	$-\sqrt{2}i$
2	-2	0	-1	1	0	$-\sqrt{2}i$	$\sqrt{2}i$
4	-4	0	1	-1	0	0	0

8. (i) Bewijs dat de irreducibele karakters van graad 1 van een groep G een groep vormen onder puntsgewijze vermenigvuldiging. Aanwijzing: gebruik 4.2.5 (iv) en Opgave 5.
(ii) Laat zien dat de onder (i) genoemde groep isomorf is met G/D(G).

Aanwijzing: Breng het probleem terug tot het geval waarin G abels is (zie 4.1.13) en laat zien dat de afbeelding $(a_1^{k_1},\ldots,a_r^{k_r}) \mapsto f^{t_1}\ldots^{t_r}$ met notatie als in 4.1.12 en $t_s \in \underline{m}_s$ zodanig dat $t_s = k_s \bmod m_s$ een isomorfisme van $G = C_{m_1}\times\ldots\times C_{m_r}$ op de karakters van G van graad 1 definieert.

*9. Laat G een eindige groep zijn met $\mathrm{Irr}(G) = \{\phi_1,\ldots,\phi_t\}$. Een funktie $\phi \in \mathbb{C}^{K(G)}$ heet *gegeneraliseerd karakter* als er gehele getallen $a_1,\ldots,a_t$ zijn zodat $\phi = \sum_{i=1}^{t} a_i\phi_i$. Ga na dat zo'n ϕ een (gewoon) karakter is als $a_i \geq 0$ voor alle $i \in \underline{t}$. Bewijs dat als ϕ een gegeneraliseerd karakter van G is zo dat $\langle\phi|\phi\rangle = 1$ en $\phi(1) > 0$, dan ϕ een echt karakter is.

*10. (i) Laat $\varepsilon_1,\ldots,\varepsilon_n \in \mathbb{C}$ een n-tal eenheidswortels zijn. Bewijs dat

$$\left|\sum_{i=1}^{n} \varepsilon_i\right| = n$$

dan en slechts dan als $\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_n$.

(ii) Leid hieruit af dat als f een lineaire voorstelling van G is, met karakter χ, dan $\mathrm{Ker}\, f = \{g \in G \mid \chi(g) = \chi(1)\}$.

(iii) Toon aan dat als $f = f^1\oplus\ldots\oplus f^t$ met f^i irreducibele voorstellingen van G, dan $\mathrm{Ker}\, f = \bigcap_{i=1}^{t} \mathrm{Ker}\, f^i$.

4.3. Geïnduceerde voorstellingen

Laat H een ondergroep van index s van de eindige groep G zijn. Kies een representantensysteem $1 = g_1,g_2,\ldots,g_s$ van rechter nevenklassen. Dan is $H\backslash G = \{Hg_1,\ldots,Hg_s\}$. We zullen nu een willekeurige voorstelling f van H in een komplexe vektorruimte W uitbreiden tot een voorstelling f^G van G in een grotere vektorruimte. De te gebruiken techniek heet induktie. We definiëren eerst nog $F^* : G \to Gl_n(\mathbb{C})$ voor een matrixvoorstelling F van H van graad n over $\mathbb{C}$ door $F^*(g) = \begin{cases} 0 & \text{als } g \notin H \\ F(g) & \text{als } g \in H \end{cases}$.

4.3.1. DEFINITIE. De naar G *geïnduceerde voorstelling* f^G van f met matrixvoorstelling F is de voorstelling f^G behorend bij de matrixvoorstelling F^G gegeven door

$$F^G(g) = (F^*(g_i^{-1}gg_j))_{i,j \in \underline{s}}$$

Hierin hoort bij elk paar indices een n×n deelmatrix. De graad van f^G is dus sn als n de graad van f is. De vektorruimte V waarin G voorgesteld wordt, bestaat uit de direkte som van s kopieen van W. We moeten nog nagaan dat dit inderdaad een voorstelling definieert. Laat daartoe g,h $\in$ G. Dan is

$$(F^G(g)\ F^G(h))_{ij} = \sum_{r=1}^{s} F^*(g_i^{-1}gg_r)F^*(g_r^{-1}hg_j).$$

Maar voor gegeven i is er slechts één r zodat $g_i^{-1}gg_r \in H$. Voor deze r geldt

$$(F^G(g)F^G(h))_{ij} = F^*(g_i^{-1}gg_r)F^*(g_r^{-1}hg_j).$$

Als nu ook $g_r^{-1}hg_j \in H$ dan volgt

$$(F^G(g)F^G(h))_{ij} = F^*(g_i^{-1}(gh)g_j) = (F^G(gh))_{ij}.$$

Zoniet, dus in geval $g_r hg_j^{-1} \notin H$, dan is $(F^G(g)F^G(h))_{ij} = 0$. Anderzijds is dan $g_i^{-1}(gh)g_j = (g_i^{-1}gg_r)(g_r^{-1}hg_j) \notin H$, (want $g_i^{-1}gg_r \in H$), zodat ook $(F^G(gh))_{ij} = 0$. Er volgt dat $F^G(g)F^G(h) = F^G(gh)$ en dus ook $f_g^G f_h^G = f_{gh}^G$. Uit $f_1^G = id_V$ blijkt verder dat $f_g^G \in Gl(V)$ voor elke $g \in G$ en dat $f^G : G \to Gl(V)$ een morfisme is.

4.3.2. VOORBEELDEN.

(i) Neem $H = C_n = \langle a \rangle$ ondergroep van $G = D_n = \langle a,b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$, en laat $f : H \to \mathbb{C}^*$ een voorstelling van H van graad 1 zijn. Dan is $f(a) = e^{\frac{2\pi im}{n}}$ voor zekere $m \in \mathbb{N}$.

Kies als nevenklassenrepresentanten g_1, g_2 voor H in G de elementen $g_1 = 1$, $g_2 = b$.

Dan geldt

$$(f_a^G) = \begin{pmatrix} f_a^* & f_{ab}^* \\ f_{ba}^* & f_{a^{-1}}^* \end{pmatrix} = \begin{pmatrix} e^{\frac{2\pi im}{n}} & 0 \\ 0 & e^{-\frac{2\pi im}{n}} \end{pmatrix}$$

en

$$(f_b^G) = \begin{pmatrix} f_b^* & f_1^* \\ f_1^* & f_b^* \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

waaruit blijkt dat de voorstellingen van graad 2 in 4.1.10 (ii) alle van H geïnduceerd zijn.

(ii) Laat $H \leq G$ en neem voor f de triviale voorstelling 1_H. De voorstelling f^G komt overeen met f^X uit 4.1.2 (iii) als $X = G/H$ en G op X werkt via de gebruikelijke linksvermenigvuldiging. Immers als $X = \{g_1H,\ldots,g_sH\}$ dan is

$$(1_H^*)(g_i^{-1}gg_j) \in \{0,1\} \text{ voor elke } g \in G,$$

terwijl

$$(1_H^*)(g_i^{-1}gg_j) = 1$$

dan en slechts dan als $gg_j \in g_iH$, dus precies dan als $g(g_jH) = g_iH$. De konklusie is dat

$$(f^G)_{ij} = (f^X)_{ij}\ .$$

Vanwege 1.4.8 geldt het omgekeerde ook voor transitieve permutatievoorstellingen: Als G een transitieve permutatievoorstelling in X heeft, dan is f^X equivalent met $(1_H)^G$ voor H de stabilisatorgroep binnen G van een punt in X. De definitie van geïnduceerde voorstelling hangt af van het gekozen representantensysteem. Dat een ander representantensysteem tot op ekwivalentie na dezelfde geïnduceerde voorstelling geeft, blijkt uit de volgende propositie. Als H een ondergroep van G is en $\theta \in \mathfrak{C}^H$, dan geven we met $\theta^* \in \mathfrak{C}^G$ de voortzetting van θ gegeven door $\theta^*(g) = 0$ voor $g \in G-H$ aan.

4.3.3. PROPOSITIE. *Laat* f *een lineaire voorstelling van een ondergroep* H *van een eindige groep* G *zijn, met karakter* χ.

(i) *Dan heeft een geïnduceerde voorstelling* f^G *karakter* χ^G *gegeven door*

$$\chi^G(g) = \frac{1}{|H|} \sum_{h \in G} \chi^*(h^{-1}gh).$$

In het bijzonder zijn alle van f *geïnduceerde voorstellingen ekwivalent.*

(ii) *Als bovendien* K *een ondergroep van* G *is die* H *omvat, dan is*

$$(\chi^K)^G = \chi^G.$$

BEWIJS.

(i) Laat $g_1,\ldots,g_s$ een stelsel representanten van rechternevenklassen van H in G zijn. Laat verder F de matrixvoorstelling bij f zijn.

$$\chi^G(g) = sp(F^*(g_i^{-1}gg_i)) = \sum_{i=1}^{s} \chi^*(g_i^{-1}gg_i) =$$

$$= \frac{1}{|H|} \sum_{i=1}^{s} \sum_{h\in H} \chi^*(h^{-1}g_i^{-1}gg_ih)$$

$$= \frac{1}{|H|} \sum_{h\in G} \chi^*(h^{-1}gh).$$

Het tweede deel van (i) volgt uit 4.2.5.

(ii) $$(\chi^K)^G(g) = \frac{1}{|K|} \sum_{k\in G} (\chi^K)^*(k^{-1}gk) = \frac{1}{|K|} \sum_{\substack{k\in G \\ k^{-1}gk\in K}} \chi^K(k^{-1}gk) =$$

$$= \frac{1}{|K|}\frac{1}{|H|} \sum_{\substack{k\in G \\ k^{-1}gk\in K}} \sum_{\substack{h\in K \\ h^{-1}k^{-1}gkh\in H}} \chi^*(h^{-1}k^{-1}gkh) =$$

$$= \frac{1}{|K|\,|H|} \sum_{k\in G} \sum_{\substack{h\in K \\ h^{-1}k^{-1}gkh\in H}} \chi(h^{-1}k^{-1}gkh) =$$

$$= \frac{1}{|K|\,|H|} \sum_{h\in K} \sum_{\substack{(kh)\in G \\ (kh)^{-1}g(kh)\in H}} \chi((kh)^{-1}g(kh))$$

$$= \frac{1}{|K|\,|H|} \sum_{h\in K} \sum_{k\in G} \chi^*(k^{-1}gk) =$$

$$= \frac{1}{|H|} \sum_{k\in G} \chi^*(k^{-1}gk) = \chi^G(g). \quad \square$$

Uitgaande van een lineaire voorstelling f van H, levert de beperking ("reduktie") $f^G|_H$ van de geïnduceerde voorstelling f^G tot H weer een voorstelling van H, echter met een graad die een veelvoud is van de graad van f. De voorstellingen f en $f^G|_H$ zijn dus zeker niet ekwivalent. Een verband tussen de twee wordt gegeven door de zogenaamde *Frobenius reciprociteitswet*.

4.3.4. STELLING. *Laat* H *een ondergroep van* G *zijn en veronderstel dat* χ,ϕ *een karakter van* H *respectievelijk* G *is. Dan geldt*

$$\langle \chi^G | \phi \rangle = \langle \chi | \phi_{|H} \rangle.$$

BEWIJS.

$$\langle \chi^G | \phi \rangle = \frac{1}{|G|}\frac{1}{|H|} \sum_{g,h\in G} \chi^*(h^{-1}gh)\overline{\phi(g)}$$

$$= \frac{1}{|G|}\frac{1}{|H|} \sum_{h\in G}\sum_{g\in G} \chi^*(h^{-1}gh)\overline{\phi(h^{-1}gh)}$$

$$= \frac{1}{|G|}\frac{1}{|H|} \sum_{h\in G}\sum_{g\in G} \chi^*(g)\overline{\phi(g)}$$

$$= \frac{1}{|H|} \sum_{g\in H} \chi(g)\overline{\phi(g)} = \langle \chi | \phi_{|H} \rangle. \quad \square$$

4.3.5. GEVOLG. *Laat* G *een permutatiegroep op* X *en* χ^X *het karakter van de bijbehorende lineaire voorstelling zijn.*

(i) $\langle \chi^X | 1 \rangle$ *is het aantal banen van* G *in* X.

(ii) *Als* G *transitief is, dan is* $\langle \chi^X | \chi^X \rangle$ *de rang van* G *op* X.

(iii) *Als* $|X| > 1$, *dan is* G *2-transitief op* X *dan en slechts dan als* $\langle \chi^X | \chi^X \rangle = 2$.

BEWIJS.

(i) Stel dat $O_1,\ldots,O_s$ de banen van G in X zijn. Dan is $f^X = f^{O_1}\oplus\ldots\oplus f^{O_s}$, wat bewezen kan worden door de directe somsplitsing

$$\bigoplus_{x\in X} \mathbb{C}e_x = \bigoplus_{i=1}^{s} \Big(\bigoplus_{x\in O_i} \mathbb{C}e_x\Big)$$

te beschouwen. Laat H_i de stabilisator in G van een punt uit O_i zijn.

Er volgt dat

$$\chi^X = \sum_{i=1}^{s} \chi^{O_i}$$

en met Voorbeeld 4.3.2 (ii)

$$\langle \chi^X | 1_G \rangle = \sum_{i=1}^{s} \langle \chi^{O_i} | 1_G \rangle$$

$$= \sum_{i=1}^{s} \langle (1_{H_i})^{O_i} | 1_G \rangle = \sum_{i=1}^{s} \langle 1_{H_i} | 1_{H_i} \rangle = s$$

vanwege de Frobenius-reciprociteit (4.3.4).

(ii) Stel G werkt transitief van rang n op X. Dan heeft G in haar werking op X×X middels $g(x,y) = (gx,gy)$ ($g \in G$, $x,y \in X$) precies n banen, waarvan $I_X = \{(x,y) \in X \times X | x=y\}$ er één is (vergelijk 3.4.6). Ga zelf na dat de lineaire voorstelling $f^{X\times X}$ bij G werkend op X×X karakter $\chi^{X\times X} = (\chi^X)^2$ heeft. Er volgt met (i) dat

$$n = \langle (\chi^X)^2 | 1 \rangle = \frac{1}{|G|} \sum_{g\in G} (\chi^X)^2(g) =$$

$$= \frac{1}{|G|} \sum_{g\in G} \chi^X(g) \overline{\chi^X(g)} = \langle \chi^X | \chi^X \rangle.$$

(iii) Uit (ii) volgt $\langle \chi^X | \chi^X \rangle = 2$ als G 2-transitief is op X. Andersom: Stel $\langle \chi^X | \chi^X \rangle = 2$. Dan heeft G precies 2 banen op X×X (dit volgt uit het bewijs van (ii). Maar I_X uit (ii) is een vereniging van banen; dus als $|X| > 1$ dan bestaat I_X uit precies één baan (en is $X\times X - I_X$ de tweede). Dit bewijst dat G transitief is op X.
De rest volgt uit (ii). □

Vergelijk deze resultaten eens met die uit Opgave 3.1.7!

4.3.6. VOORBEELDEN.

(i) $PSl_2(\mathbb{F}_q)$ werkt 2-transitief op de q+1 lijnen in $\mathbb{F}_q^{\,2}$ door 0. Met 4.3.5. volgt dat er een karakter χ van $PSl_2(\mathbb{F}_q)$ bestaat zodanig dat χ_g het aantal lijnen is dat onder g vast blijft (in het bijzonder $\chi(1) = q+1$), $\langle \chi | \chi \rangle = 2$ en $\langle \chi | 1 \rangle = 1$. Er volgt dat $\psi = \chi - 1$ een irreducibel karakter van $PSl_2(\mathbb{F}_q)$ is.

(ii) Als G een transitieve rang 3 permutatiegroep op X is, dan volgt voor het bijbehorende permutatiekarakter $\chi = \chi^X$, dat er twee irreducibele karakters ϕ,ψ van G zijn met $\chi = 1+\phi+\psi$. Als G nu van even orde is, dan bestaat er krachtens Stelling 3.4.9 een sterk reguliere graaf (X,Γ) zodanig dat $G \leq \mathrm{Aut}(X,\Gamma)$. Laat A de verbindingsmatrix van (X,Γ) zijn. Het feit dat G uit automorfismen van (X,Γ) bestaat, betekent dat voor elke $g \in G$ geldt:

$$Af_g^X = f_g^X A.$$

Beperking tot een f^X-irreducibel deel W van $V = \bigoplus_{x\in X} \mathbb{C}e_x$ levert

$$A|_W (f^X)_g^W = (f^X)_g^W A|_W.$$

Met Lemma 4.1.7 van Schur geeft dat $A|_W = \lambda 1_W$ voor zekere $\lambda \in \mathbb{C}$. Omdat f^X karakter $1+\phi+\psi$ heeft, zijn er precies drie f-invariante irreducibele deelruimten van V, (korresponderend met $1,\phi,\psi$) zodat A hooguit 3 verschillende eigenwaarden heeft. In Stelling 3.4.15 zijn deze eigenwaarden berekend, en tevens hun multipliciteiten. Er volgt dat de graden $1,\phi(1),\psi(1)$ van $1_G,\phi,\psi$ berekend kunnen worden als de multipliciteiten 1,f,g van de eigenwaarden van A via de in 3.4.15 gegeven formules.

OPGAVEN BIJ §4.3.

G is steeds een eindige groep.

1. Bereken de graden van de irreducibele konstituenten (= deelvoorstellingen) van Sym(n) die horen bij de rang 3 permutatievoorstelling op de paren $\{i,j\}$ met $i,j \in n$ en $i \neq j$. (vergelijk 3.4.10.)

2. Laat $\chi = (1_H)^G$ het karakter van een transitieve permutatievoorstelling van G met stabilisatorondergroep H zijn. Toon aan:
   (i) $\chi(1)$ deelt $|G|$
   (ii) $\chi(g) \in \mathbb{N} \cup \{0\}$ voor elke $g \in G$
   (iii) $\chi(g) \leq \chi(g^m)$ voor elke $g \in G$ en elke $m \in \mathbb{N}$
   (iv) $\langle\chi|\psi\rangle \leq \psi(1)$ voor elke $\psi \in \mathrm{Irr}(G)$
   (v) $\chi(g) = 0$ als g een orde heeft die $|G|/\chi(1)$ niet deelt.

3. Laat f een lineaire voorstelling van G in de komplexe lineaire ruimte V zijn die geïnduceerd is van een echte ondergroep H van G. Ga na dat er een directe somsplitsing $V = W_1 \oplus \ldots \oplus W_t$ van V in $f|_H$-invariante lineaire deelruimten W_i van V bestaat (met $t = |G/H|$) zodanig dat voor elke $g \in G$ en $i \in \underline{t}$ er een $j \in \underline{t}$ is waarvoor $f_g W_i = W_j$.

4. Bewijs dat Alt($\underline{5}$) een irreducibele voorstelling van graad 3 heeft die niet geïnduceerd kan zijn van een echte ondergroep (gebruik 4.1.14 en de vorige opgave).

4.4. Enkele karaktertabellen

Aan de hand van hierboven afgeleide resultaten, zullen we nu enkele konkrete voorbeelden uitwerken.

4.4.1. VOORBEELD. Alt($\underline{5}$). Het is wel bekend dat Alt($\underline{5}$) precies 5 konjugatieklassen heeft. We kiezen als representanten 1, (123), (12) (34), (12345) en (21345). We beweren dat de karaktertabel er als volgt uit ziet

	1	(123)	(12)(34)	(12345)	(21345)
1	1	1	1	1	1
χ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
$\pi-1$	4	1	0	-1	-1
λ^G	5	-1	1	0	0

De karakters van graad 1 en 4 uit de tabel zijn respektievelijk het triviale karakter en het irreducibele van graad >1 dat van de 2-transitieve permutatievoorstelling van graad 5 af komt. Het karakter λ^G van graad 5 is te verkrijgen als geïnduceerde van een niet-triviaal karakter van Alt($\underline{4}$) van graad 1, en wel als volgt. Alt($\underline{4}$) heeft de viergroep V_4 als normaaldeler, met quotient $\text{Alt}(\underline{4})/V_4 \cong C_3$. Laat λ de lineaire voorstelling van Alt($\underline{4}$) zijn met V_4 in de kern en $\lambda((123)) = e^{2\pi i/3}$. We berekenen nu het geïnduceerde karakter λ^G aan de hand van de definitie:

$$\lambda^G(1) = |G:\mathrm{Alt}(\underline{4})| = 5$$

$$\lambda^G((123)) = \frac{1}{|\mathrm{Alt}(\underline{4})|} \sum_{h\in G} \lambda^*(h^{-1}(123)h) =$$

$$= \sum_{i=1}^{5} \lambda^*((12345)^{-i}(123)(12345)^i)$$

$$= \lambda((123)) + \lambda((234)) = \lambda((123)) + \lambda((321))$$

$$= e^{2\pi i/3} + e^{-2\pi i/3} = -1.$$

$$\lambda^G((12)(34)) = \sum_{i=1}^{5} \lambda^*((12345)^{-i}\ (12)(34)(12345)^i)$$

$$= \lambda((12)(34)) = 1.$$

$$\lambda^G((12345)) = 0.$$

Dat λ^G irreducibel is volgt uit $\langle\lambda^G|\lambda^G\rangle = 1$. Merk op dat dit karakter eenvoudiger te krijgen is. Het komt namelijk af van de 2-transitieve permutatievoorstelling van graad 6 gegeven in Opgave 1.6.13; equivalent: het is $(1_H)^G$ voor H de normalisator van een 5-Sylowgroep (vergelijk 4.3.2 (ii)).
We zullen nu irreducibele diëderkarakters ψ van $H = N_G(\langle 12345\rangle) = \langle(12345), (15)(24)\rangle$ induceren. Als ψ graad 2 heeft, komt dit getuige 4.3.2 (i) en 4.3.3 (ii) op hetzelfde neer als induktie vanaf $\langle(12345)\rangle$. We zullen voor de berekeningen gebruiken dat $(21345)^i$ $(1\le i\le 5)$, (524) een volledig stelsel nevenklasserepresentanten van H in G is.

$$\psi^G(1) = 6\psi(1)$$

$$\psi^G((123)) = 0$$

$$\psi^G((15)(24)) = \psi((15)(24)) + \psi^*((24)(53)) + \psi^*((53)(41))$$

$$+ \psi^*((41)(32)) + \psi^*((32)(15)) + \psi^*((14)(52))$$

$$= \psi((15)(24)) + \psi((14)(23)).$$

$$\psi^G((12345)) = \psi((12345)).$$

Nemen we voor ψ het karakter ψ_s behorende bij de voorstelling (vergelijk 4.1.10 (ii)) bepaald door de volgende beelden:

$$(12345) \mapsto \begin{pmatrix} e^{2\pi is/5} & 0 \\ 0 & e^{-2\pi is/5} \end{pmatrix},$$

$$(15)(24) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

dan ligt ψ_s^G vast door:

	1	(123)	(12)(34)	(12345)	(21345)
ψ_s^G	12	0	0	$2\cos\frac{2\pi s}{5}$	$2\cos\frac{4\pi s}{5}$

Uit berekening volgt $\langle\psi^G|\lambda^G\rangle = \langle\psi^G|\pi\rangle = 1$ (want $2\cos\frac{2\pi s}{5} + 2\cos\frac{4\pi s}{5} = -1$). Derhalve is $\chi_s = \psi^G - \lambda^G - \pi$ een karakter (behorend bij het komplement van de deelvoorstelling bij ψ^G die karakter $\lambda^G+\pi$ heeft). Uit $\langle\chi_s|\chi_s\rangle = 1$ volgt dat χ_s irreducibel is. Ga zelf na dat χ_1, χ_2 de resterende karakters uit de tabel leveren (maak gebruik van de gelijkheid $\cos 2\pi/5 = \frac{-1+\sqrt{5}}{4}$).

Het spreekt vanzelf dat er vele andere manieren zijn waarop de karaktertabel verkregen kan worden. Zo komen de karakters χ_1, χ_2 van de in 4.1.14 besproken voorstelling van Alt(5) als rotatiegroep van de icosaeder in de euclidische ruimte $\mathbb{R}^3$ (het is niet moeilijk het spoor van een draaiing te bepalen!). Ook is λ^G nog een konstituent van het karakter van de permutatievoorstelling van Alt(5) op de 10 3-Sylowgroepen. Opvallend is echter dat we alle irreducibele karakters hebben verkregen uit kombinaties van geïnduceerde karakters van graad 1 op echte ondergroepen. Volgens stellingen van Brauer en Artin is dit altijd mogelijk: elk karakter van een groep is te schrijven als lineaire kombinatie met gehele koëfficienten van geïnduceerde karakters van graad 1 op ondergroepen. We zullen deze stelling niet bewijzen.

4.4.2. VOORBEELD $Sl_2(8)$. De konjugatieklassen van $Sl_2(8)$ zijn in 3.2.2 te vinden. We houden de notatie daarvan aan. Uit de in 3.2.5 gevonden permutatievoorstellingen verkrijgen we de volgende permutatiekarakters

	1	2	3	9_1	9_2	9_3	7_1	7_2	7_3
π_1	9	1	0	0	0	0	2	2	2
π_2	28	4	1	1	1	1	0	0	0
π_3	36	4	0	0	0	0	1	1	1

De waarden van π_i zijn gemakkelijk te vinden met behulp van $\langle\pi_i|1\rangle = 1$. Voor π_1 bijvoorbeeld volgt $\pi_1(z) = 0$ als z een element van orde 3 of 9 is, omdat zo'n element geen 2-Sylowgroep normaliseert. Verder is $Sl_2(8)$ enkelvoudig, dus kan een element w van orde 7 niet in de kern zitten van de permutatievoorstelling. Derhalve is het beeld van zo'n element w in de symmetrische groep op de 9 2-Sylowgroepen een 7-kring, die 2 vaste punten heeft. Er volgt $\pi_1(w) = 2$. Uit $\langle\pi_1|1\rangle = 1$ volgt tenslotte $\pi_1(u) = 1$ voor u een element van orde 2.

Nu is (π_1-1) irreducibel en $\langle\pi_1-1|\pi_3-1\rangle = 1$, zodat $\pi_3-\pi_1$ weer een karakter is. Het blijkt π_2-1 te zijn, dus beschouwing van π_3 naast π_2 heeft voor de karaktertabel verder geen zin. Uit 3.2.5 weten we dat π_2-1 een som van 3 irreducibele karakters is. Om meer karakters te krijgen, induceren we de 1-dimensionale karakters van de normalisator H van de 2-Sylowgroep $P = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Zoals bekend is H/P van orde 7 en dus isomorf met C_7. Schrijf $d = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma^{-1} \end{pmatrix}$. Dan is $d \in H$. Laat nu $\lambda_s : H \to \mathbb{C}$ voor $s \in \underline{6}$ het karakter van H van graad 1 zijn dat bepaald wordt door

$$\lambda_s(d) = e^{\frac{2\pi is}{7}}$$

en

$$\lambda_s(P) = \{1\}.$$

We stellen ons tot taak λ_s^G te berekenen:

klasse	1	2	3	9_1	9_2	9_3	7_1	7_2	7_3
λ_s^G	9	1	0	0	0	0	$2\cos\frac{4\pi s}{7}$	$2\cos\frac{2\pi s}{7}$	$2\cos\frac{6\pi s}{7}$

$$\lambda_s^G(x_1) = \frac{1}{|H|} \sum_{g\in G} \lambda_s^*(gx_1g^{-1}) = \lambda_s^*(x_1) = 1,$$

met x_1 als in 3.2.3.

Omdat de normalisator van een 7-Sylowgroep een diëdergroep van orde 14 is (zie 3.2.3) volgt

$$\lambda_s^G(d^r) = \frac{1}{|H|}\sum_{g\in G}\lambda_s^*(gd^rg^{-1}) = \lambda_s^*(d^r) + \lambda_s(d^{-r}) =$$

$$= \exp\left(\frac{2\pi irs}{7}\right) + \exp\left(\frac{-2\pi irs}{7}\right).$$

Merk op dat d, d^2, d^3 representanten van de inklassen 7_2, 7_1, 7_3 zijn. Vanzelfsprekend levert s = 0 ons het al bekende karakter π_1. Verder blijkt $\lambda_s^G = \lambda_{7-s}^G$, dus kunnen we ons beperken tot de waarden s = 1,2,3. Ga zelf na dat λ_s^G irreducibel is voor deze waarden.

Tenslotte induceren we nog 1-dimensionale karakters van een 3-Sylowondergroep. Beschouw de groep $P_9 = \langle yx_\sigma \rangle$. De normalisator $N(P_9)$ is blijkens 3.2.3 een diëdergroep van orde 18. Derhalve heeft voor $s \in \underline{9}$ het karakter $\mu_s : P_9 \to \mathbb{C}$ bepaald door $\mu_s(yx_\sigma) = e^{\frac{2\pi is}{9}}$ de waarden:

	1	2	3	9_1	9_2	9_3	7_1	7_2	7_2
μ_s^G	56	0	$2\cos\frac{6\pi s}{9}$	$2\cos\frac{2\pi s}{9}$	$2\cos\frac{4\pi s}{9}$	$2\cos\frac{8\pi s}{9}$	0	0	0

Uit berekeningen van inprodukten volgt dat $\chi_s = \mu_s^G - \sum_{r=0}^{3}\lambda_{r+1}^G$ een karakter is dat inprodukt 0 heeft met de tot nu toe gevonden irreducibele karakters. We tabelleren χ_s:

	1	2	3	9_1	9_2	9_3	7_1	7_2	7_3
χ_s	21	-3	$2\cos\frac{6\pi s}{9}+1$	$2\cos\frac{2\pi s}{9}+1$	$2\cos\frac{4\pi s}{9}+1$	$2\cos\frac{8\pi s}{9}+1$	0	0	0

Er zijn nog 4 irreducibele karakters ψ_1, ψ_2, ψ_3, ψ_4 die ontbreken aan de tabel (zie 4.2.8 (iii)). Uit het feit dat de al bekende irreducibele karakters geen konstituenten van χ_s (s = 1,2,3,4) zijn, volgt dat elk der χ_s een som van de ψ_i is. Uit de inprodukt-waarden $\langle\chi_s|\chi_s\rangle = 3$ en $\langle\chi_s|\chi_t\rangle = 2$ voor $s,t \in \underline{4}$; $s \neq t$ konkluderen we dat op permutatie van indices na, de ψ_i voldoen aan

$$\chi_1 = \psi_2 + \psi_3 + \psi_4$$
$$\chi_2 = \psi_1 + \psi_3 + \psi_4$$
$$\chi_3 = \psi_1 + \psi_2 + \psi_4$$
$$\chi_4 = \psi_1 + \psi_2 + \psi_3.$$

Uit deze 4 vergelijkingen zijn de 4 onbekenden ψ_i te berekenen door

$$\psi_i = \frac{1}{3}\left(\sum_{j\neq i} \chi_j - 2\chi_i\right).$$

Er resulteren 4 irreducibele karakters van graad 7. De karaktertabel voor $Sl_2(8)$ ziet er dus als volgt uit

	1	2	3	9_1	9_2	9_3	7_1	7_2	7_3
1	1	1	1	1	1	1	1	1	1
π_1-1	8	0	-1	-1	-1	-1	1	1	1
λ_1^G	9	1	0	0	0	0	$2\cos\frac{4\pi}{7}$	$2\cos\frac{2\pi}{7}$	$2\cos\frac{6\pi}{7}$
λ_2^G	9	1	0	0	0	0	$2\cos\frac{6\pi}{7}$	$2\cos\frac{4\pi}{7}$	$2\cos\frac{2\pi}{7}$
λ_3^G	9	1	0	0	0	0	$2\cos\frac{2\pi}{7}$	$2\cos\frac{6\pi}{7}$	$2\cos\frac{4\pi}{7}$
ψ_1	7	-1	+2	$-2\cos\frac{2\pi}{9}$	$-2\cos\frac{4\pi}{9}$	$-2\cos\frac{8\pi}{9}$	0	0	0
ψ_2	7	-1	+2	$-2\cos\frac{4\pi}{9}$	$-2\cos\frac{8\pi}{9}$	$-2\cos\frac{2\pi}{9}$	0	0	0
ψ_3	7	-1	-2	1	1	1	0	0	0
ψ_4	7	-1	+2	$-2\cos\frac{8\pi}{9}$	$-2\cos\frac{2\pi}{9}$	$-2\cos\frac{4\pi}{9}$	0	0	0

OPGAVEN BIJ §4.4.

1. Stel de karaktertabel van $Sl_2(7)$ op (gebruik Voorbeeld 1.5.5).

2. Idem voor Sym(5).

3. Geef de karaktertabellen voor de twee niet-abelse groepen van orde 27 uit opgave 2.2.3.

4.5. Een stelling van Frobenius

De karaktertheorie kan in bepaalde gevallen toegepast worden om de eksistentie van een niettriviale normaaldeler af te leiden. In dit diktaat zullen we twee zeer klassieke stellingen van deze strekking behandelen, te weten (in het volgende hoofdstuk) de p^aq^b-stelling van Burnside en (in deze paragraaf) een stelling over de zogenaamde Frobeniusgroepen.

4.5.1. DEFINITIE. Een eindige groep G van permutaties op een eindige verzameling V heet een *Frobeniusgroep* op V als G transitief is op V, $G_x > 1$ en $G_{xy} = 1$ voor elke $x,y \in V$ $(x \neq y)$.

4.5.2. VOORBEELDEN. De diëdergroep D_n van orde 2n in haar natuurlijke permutatievoorstelling op n elementen is een Frobeniusgroep. Ook de groep $AGl_1(q)$ uit 1.3.7 in haar gewone werking op $\mathbb{F}_q$ is een Frobeniusgroep.
Voor het bewijs hebben we het volgende lemma nodig. We brengen van Opgave 4.2.9 in herinnering dat een *gegeneraliseerd karakter* van een eindige groep H een lineaire combinatie $\lambda = \sum_{\chi \in Irr(H)} a_\chi \chi$ met gehele koëfficiënten a_χ is. Als H een ondergroep van G is, dan geven we met λ^G de eindige kombinatie $\sum_{\chi \in Irr(H)} a_\chi \chi^G$ aan.

4.5.3. LEMMA. *Laat ϕ,χ een tweetal gegeneraliseerde karakters van een ondergroep H van een eindige groep G zijn, en veronderstel dat $\phi(1) = 0$ en $gHg^{-1} \cap H = \{1\}$ voor $g \notin H$. Dan geldt*

(i) $\phi^G(g) = \phi(g)$ *voor* $g \in H$.

(ii) $\langle \phi | \chi \rangle = \langle \phi^G | \chi^G \rangle$.

(iii) *Als* $\chi \in Irr(H)$, *dan is* $\chi^G - \chi(1)((1_H)^G - 1_G) \in Irr(G)$.

BEWIJS.

(i) Definiëer ϕ^* als in 4.3.2. Dan is voor $h \in H-\{1\}$:

$$\phi^G(h) = \frac{1}{|H|} \sum_{g \in G} \phi^*(ghg^{-1}) = \frac{1}{|H|} \sum_{g \in H} \phi(ghg^{-1}) =$$

$$= \frac{1}{|H|} \sum_{g \in H} \phi(h) = \phi(h).$$

(ii) $$\langle\phi|\chi^G{}_{|H}\rangle = \frac{1}{|H|}\sum_{h\in H}\phi(h)\,\overline{\chi^G(h)} =$$

$$= \frac{1}{|H|^2}\sum_{h\in H-\{1\}}\sum_{g\in G}\phi(h)\,\overline{\chi^*(g^{-1}hg)} =$$

$$= \frac{1}{|H|^2}\sum_{h\in H-\{1\}}\sum_{g\in H}\phi(h)\overline{\chi(g^{-1}hg)} =$$

$$= \frac{1}{|H|}\sum_{h\in H-\{1\}}\phi(h)\overline{\chi(h)} = \langle\phi|\chi\rangle. \quad \square$$

(iii) Vanwege Frobenius-reciprociteit (4.3.4) en de voorgaande uitspraak geldt:

$$\langle\chi^G-\chi(1)((1_H)^G-1)\,|\,\chi^G-\chi(1)((1_H)^G-1)\rangle =$$

$$= \langle\chi^G-\chi(1)(1_H)^G|\chi^G-\chi(1)(1_H)^G\rangle+\chi(1)\langle 1|\chi^G\rangle-\chi(1)^2\langle 1|(1_H)^G\rangle+\chi(1)^2$$

$$-\chi(1)\langle\chi^G|1\rangle-\chi(1)^2\langle(1_H)^G|1\rangle =$$

$$= \langle\chi-\chi(1).1|\chi-\chi(1).1\rangle+\chi(1)\langle 1_H|\chi\rangle-\chi(1)^2\langle 1_H|1_H\rangle+\chi(1)^2-\chi(1)\langle\chi|1_H\rangle$$

$$-\chi(1)^2\langle 1_H|1_H\rangle = \langle\chi|\chi\rangle = 1.$$

Ga zelf na dat $\chi^G-\chi(1)((1_H)^G-1)$ een gegeneraliseerd karakter van G is met waarde $\chi(1)$ op 1. We kunnen dus Opgave 4.2.9 toepassen om het bewijs af te ronden.

4.5.4. STELLING. *Stel* G *is een Frobeniusgroep op* V. *Dan is* $N = \{1\} \cup (G-(\bigcup_{x\in V} G_x))$ *een normaaldeler van* G *van orde* $|V|$.

BEWIJS. Uit de definitie van N volgt dat N onder konjugatie van G in zichzelf overgaat. Het is dus zaak te bewijzen dat N een groep is. We zullen hiervoor gebruik maken van Opgave 4.2.10 waarin $\{x\in G\,|\,\phi(x) = \phi(1)\}$ voor een willekeurig karakter ϕ van G een normaaldeler bleek te zijn. Kies nu

$$\phi = \sum_{\chi\in Irr(H)}\chi(1)(\chi^G-\chi(1)((1_H)^G-1_G)), \text{ waarin } H = G_x.$$

Uit Lemma 4.5.3 (iii) volgt dat ϕ een karakter is van graad $\phi(1) = \sum_{\chi\in Irr(H)} \chi(1)^2 = |H|$. We bepalen de waarden van ϕ op een element uit N respektievelijk uit $\bigcup_{x\in G} G_x$. Voor $g \in N$ geldt:

$$\phi(g) = \sum_{\chi\in Irr(H)} \chi(1)(\chi^G(g)-\chi(1)((1_H)^G(g)-1_G(g)))$$

$$= \sum_{\chi\in Irr(H)} \chi(1)^2 = |H|.$$

Stel $h \in G_y$ voor zekere $y \in V$. Dan is er een $g \in G$ zo dat $y = g(x)$ en $g^{-1}hg \in G_x$. We mogen ons dus beperken tot het geval $h \in G_x$.

Nu is $$\phi(h) = \sum_{\chi\in Irr(H)} \chi(1)(\chi^G(h)-\chi(1)((1_H)^G(h)-1_G(h))$$

$$= \sum_{\chi\in Irr(H)} \chi(1)(\chi(h)-\chi(1)(1-1))$$

$$= \sum_{\chi\in Irr(H)} \chi(1)\chi(h) = \begin{cases} 0 & \text{als } h \neq 1 \\ |H| & \text{als } h = 1 \end{cases}$$

(zie bijvoorbeeld Propositie 4.2.11). We concluderen dat $\phi(g) = 0$ voor $g \in \bigcup_{x\in V} G_x - \{1\}$ en dat $N = \{g \in G \mid \phi(g) = \phi(1)\}$. □

De normaaldeler N heet wel de *Frobeniuskern van* G. Ga zelf na hoe de normaaldeler eruit ziet in de voorbeelden van 4.5.2.

OPGAVEN BIJ §4.5.

1. Bewijs dat de Frobeniusgroep G op V het semidirekte produkt van haar Frobeniuskern N en een stabilisatorondergroep G_x (voor zekere $x \in V$) is. Ga na dat N een reguliere normaaldeler van G op V is.

2. Laat G een (niet-noodzakelijk transitieve) permutatiegroep op de eindige verzameling V zijn met banen ter lengte > 1 en veronderstel dat $G_{xy} = 1$ voor elke $x,y \in V$, $x \neq y$. Ga na dat de restriktie van G tot elke baan van V een getrouwe permutatievoorstelling van G levert. Bewijs dat er ten hoogste één baan van V is waarop G niet-regulier werkt.

Aanwijzing: Laat x,y twee punten in verschillende banen zijn zodanig dat $G_x, G_y > 1$. Gebruik Stelling 4.5.4 om normaaldelers A en B van G te verkrijgen waarvoor $G = A \cup \bigcup_{z\in Gx} (G_z-\{1\}) = B \cup \bigcup_{z\in Gy} (G_z-\{1\})$ (disjunkte verenigingen!) en ga na dat $\bigcup_{z\in Gx} (G_z-\{1\})$ bevat is in B (en andersom).
Leid hieruit af dat $(|G|/|A| - 1)|A| \leq |B|$ (en andersom). Dit geeft een tegenspraak.

3. Geef de karaktertabel van $AGl_1(p)$ voor willekeurige p priem (Lemma 4.5.3 is van nut).

4. Laat G het semidirekte produkt van een normaaldeler N en een ondergroep K zijn, zó dat elk element van G-N met een element uit K gekonjugeerd is. Bewijs dat G een Frobenius-groep is.

HOOFDSTUK V

NORMAALDELERS

5.1. De Stelling van Jordan-Hölder

Een natuurlijk getal kan, op volgorde na uniek geschreven worden als het produkt van een aantal priemgetallen. Zoiets geldt ook voor een eindige groep. We kunnen met elke eindige groep een aantal enkelvoudige groepen associëren waaruit deze groep is opgebouwd. Dit is de inhoud van de Stelling van Jordan-Hölder, die we in deze paragraaf zullen bewijzen.

5.1.1. DEFINITIE. Laat G een groep zijn. Een *kompositierij* van G is een rij $G_0, G_1, \ldots, G_r$ van ondergroepen van G met

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

zo dat voor elke $i \in \underline{r}$ de groep G_i een maksimale normale ondergroep van G_{i-1} is.

Merk op dat de eis dat G_i een maksimale normale ondergroep van G_{i-1} is, volgens 1.6.9 ekwivalent is met de eis dat G_{i-1}/G_i een niet-triviale enkelvoudige groep is.

5.1.2. PROPOSITIE. *Elke eindige groep heeft minstens één kompositierij.*

BEWIJS. Laat G een eindige groep zijn. Het bewijs gaat met induktie naar $|G|$. Als $|G| = 1$ dan is $G = G_0 = \{1\}$ een kompositierij. Stel $|G| > 1$ en laat G_1 een maksimale normaaldeler van G zijn. Daar $|G_1| < |G|$ heeft G_1 vanwege de induktie-hypothese een kompositierij $G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$. Nu is $G = G_0 \rhd G_1 \rhd \ldots G_r = \{1\}$ een kompositierij van G. □

5.1.3. STELLING (Jordan-Hölder). *Laat G een eindige groep zijn en laat* $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$ *en* $G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$ *twee kompositierijen van G zijn. Dan is* $r = s$ *en is er een permutatie* $\pi \in \mathrm{Sym}(\underline{r})$ *zo*

dat $G_{i-1}/G_i \simeq H_{\pi(i)-1}/H_{\pi(i)}$ $(i = 1,\ldots,r)$.

BEWIJS. Voor $i \in \underline{r}$ en $j \in \underline{s}$ schrijven we $G_{i,j} = G_i(G_{i-1} \cap H_j)$ en $H_{i,j} = H_j(H_{j-1} \cap G_i)$. Omdat $G_i \lhd G_{i-1}$ en $H_j \lhd H_{j-1}$ zijn de $G_{i,j}$ en $H_{i,j}$ ondergroepen van G. Uit $H_j \lhd H_{j-1}$ volgt verder nog dat $G_{i-1} \cap H_j \trianglelefteq G_{i-1} \cap H_{j-1}$ zodat $G_{i,j-1} \trianglerighteq G_{i,j}$ voor $i = 0,\ldots,r$, $j = 1,\ldots,s$. Evenzo volgt dat $H_{i-1,j} \trianglerighteq H_{i,j}$ voor $i = 1,\ldots,r$, $j = 0,\ldots,s$. We beweren nu dat voor $i \in \underline{r}$ en $j \in \underline{s}$ geldt

$$G_{i,j-1}/G_{i,j} \simeq H_{i-1,j}/H_{i,j}.$$

Kies $i \in \underline{r}$ en $j \in \underline{s}$. Volgens 1.7.5 is $G_i(G_{i-1} \cap H_{j-1})/G_i \simeq (G_{i-1} \cap H_{j-1})/G_i \cap (G_{i-1} \cap H_{j-1}) = (G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1})$.
In dit isomorfisme wordt de ondergroep $G_i(G_{i-1} \cap H_j)/G_i$ van $G_i(G_{i-1} \cap H_{j-1})/G_i$ afgebeeld op de ondergroep $G_i(G_{i-1} \cap H_j) \cap (G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1})$ van $(G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1})$. Nu is $G_i(G_{i-1} \cap H_j) \cap (G_{i-1} \cap H_{j-1}) = G_i(G_{i-1} \cap H_j) \cap H_{j-1} = (G_i \cap H_{j-1})(G_{i-1} \cap H_j) \trianglelefteq G_{i-1} \cap H_{j-1}$ zodat geldt

$$(G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1})(G_{i-1} \cap H_j) \simeq$$

$$(G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1}) \Big/ (G_i \cap H_{j-1})(G_{i-1} \cap H_j)/(G_i \cap H_{j-1})$$

$$G_i(G_{i-1} \cap H_{j-1})/G_i \Big/ G_i(G_{i-1} \cap H_j)/G_i \simeq$$

$$G_i(G_{i-1} \cap H_{j-1})/G_i(G_{i-1} \cap H_j) = G_{i,j-1}/G_{i,j}.$$

Verwisselen we de rol van G en H en i en j dan vinden we ook $(G_{i-1} \cap H_{j-1})/(G_i \cap H_{j-1})(G_{i-1} \cap H_j) \simeq H_{i-1,j}/H_{i,j}$, waarmee onze bewering bewezen is. Daar voor alle $i \in \underline{r}$ geldt $G_{i-1} = G_{i,0} \trianglerighteq G_{i,1} \trianglerighteq \ldots \trianglerighteq G_{i,s} = G_i$ en G_i een maksimale normale ondergroep van G_{i-1} is, is er voor elke $i \in \underline{r}$ een unieke $j = \pi(i) \in \underline{s}$ met $G_{i-1} = G_{i,0} = \ldots = G_{i,j-1} \rhd G_{i,j} = G_{i,j+1} = \ldots = G_{i,s} = G_i$ waarbij $\pi(i)$ gegeven wordt door $G_{i-1} \cap H_{\pi(i)-1} \not\leq G_i$ en $G_{i-1} \cap H_{\pi(i)} \leq G_i$. Evenzo is er voor elke $j \in \underline{s}$ een $i = \sigma(j) \in \underline{r}$ met $G_{\sigma(j)-1} \cap H_{j-1} \not\leq H_j$ en $G_{\sigma(j)} \cap H_{j-1} \leq H_j$.
Nu volgt

$$1 \neq G_{i-1}/G_i = G_{i,\pi(i)-1}/G_{i,\pi(i)} \simeq H_{i-1,\pi(i)}/H_{i,\pi(i)},$$

zodat $\sigma\pi(i) = i$ voor $i \in \underline{r}$. Daar ook $\pi\sigma(j) = j$ voor alle $j \in \underline{s}$ vinden we $r = s$ en

$$G_{i-1}/G_i \simeq H_{\pi(i)-1}/H_{\pi(i)}$$

voor alle $i \in \underline{r}$, waarmee de stelling bewezen is. □

Dankzij de stelling van Jordan-Hölder kunnen we de nu volgende definitie geven

5.1.4. DEFINITIE. Als G een eindige groep is met een kompositierij $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r$ dan heten de enkelvoudige groepen G_{i-1}/G_i $(i = 1,\ldots,r)$ de *kompositie-faktoren van* G.

Opgaven bij §5.1

1. Bepaal alle groepen met kompositie-faktoren C_2, C_3.
2. Geef kompositierijen voor de quaterniongroep en Sym(4).
3. Geef een eindige groep aan met een kompositierij die niet uitsluitend uit normaaldelers van die groep bestaat.
4. Leid uit de stelling van Jordan-Hölder de eenduidigheid van de priemontbinding van de natuurlijke getallen af.
5. Bepaal alle groepen met kompositiefaktoren C_2 en Alt(5).

*6. Laat de groep G een keten $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$ van ondergroepen hebben met G_i normaaldeler in G_{i-1} voor $i \in \underline{r}$. Ga na dat deze keten te verfijnen is tot een kompositie-rij, d.w.z. dat er een kompositierij $G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$ bestaat zó dat er $j_1 < \ldots < j_r = s$ zijn met $G_i = H_{j_i}$ $(i \in \underline{r})$

5.2. Oplosbare groepen

We zullen nu aandacht besteden aan groepen waarvan alle kompositiefaktoren abels zijn. We zullen laten zien dat groepen waarvan de orde door slechts twee verschillende priemgetallen deelbaar is deze eigenschap hebben.

5.2.1. DEFINITIES. Als G een groep is dan definiëren we de k-de *kommutatorgroep van* G, notatie $D^k(G)$, rekursief door $D^0(G) = G$ en $D^k(G) = D(D^{k-1}(G))$ voor $k \in \mathbb{N}$. In het bijzonder is dus $D^1(G) = D(G)$. Een groep G heet *oplosbaar* als er een $k \in \mathbb{N} \cup \{0\}$ is zó dat $D^k(G) = \{1\}$.

5.2.2. VOORBEELDEN. Volgens Lemma 1.6.12.(ii) is iedere abelse groep oplosbaar. Uit 1.6.13 volgt dat Sym(4) en D_n oplosbaar zijn. Een enkelvoudige groep is slechts oplosbaar als ze abels is. Sym(5) is een niet-enkelvoudige

niet-oplosbare groep.

5.2.3. STELLING. *Iedere ondergroep en iedere faktorgroep van een oplosbare groep is oplosbaar.*

BEWIJS. Laat G een oplosbare groep zijn met ondergroep H. Triviaal geldt $D(H) \leq D(G)$ en met induktie volgt hieruit $D^k(H) \leq D^k(G)$ voor $k \in \mathbb{N}$. Uit $D^k(G) = \{1\}$ volgt dus $D^k(H) = \{1\}$, dat wil zeggen H is oplosbaar.
Als $\phi: G \to K$ een epimorfisme is van G op de groep K, dan is $\phi(D(G)) = D(\phi(G)) = D(K)$ en met induktie volgt $\phi(D^k(G)) = D^k(K)$. Uit $D^k(G) = \{1\}$ volgt dus $D^k(K) = \{1\}$ en daarmee de oplosbaarheid van K. ⌐

We zullen nu enkele karakteriseringen geven van het begrip oplosbaarheid.

5.2.4. STELLING. *Een groep* G *is oplosbaar dan en slechts dan als* G *een keten van ondergroepen* $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = \{1\}$ *heeft, met* G_{i-1}/G_i *abels voor* $i = 1,2,\ldots,r$.

BEWIJS. Als G oplosbaar is met $D^r(G) = \{1\}$, neem dan $G_i := D^i(G)$ voor $i = 0,1,\ldots,r$.
Als G een keten van ondergroepen $G = G_0 \trianglerighteq \ldots \trianglerighteq G_r = \{1\}$ bevat met G_{i-1}/G_i abels, dan is $D(G_{i-1}) \leq G_i$ volgens Lemma 1.6.12(iii).
Hieruit volgt met induktie $D^r(G) \leq G_r = \{1\}$. □

5.2.5. KOROLLARIUM. *Elke* p*-groep is oplosbaar.*

BEWIJS. Dit volgt nu direkt uit Korollarium 2.2.4. □

5.2.6. STELLING. *Een eindige groep* G *is oplosbaar dan en slechts dan als alle kompositiefaktoren van* G *cyklische groepen van priemorde zijn.*

BEWIJS. Laat $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{1\}$ een kompositierij zijn van G met $G_{i-1}/G_i \simeq C_{p_i}$ voor priemgetallen p_i $(i \in \underline{r})$. Dan is G_{i-1}/G_i abels voor $i = 1,\ldots,r$ en G dus oplosbaar volgens 5.2.4. Als G oplosbaar is, dan is G_{i-1} oplosbaar $(i \in \underline{r})$ volgens 5.2.3. Dan is ook G_{i-1}/G_i oplosbaar (weer 5.2.3) voor $i = 1,\ldots,r$. Daar G_{i-1}/G_i enkelvoudig is en $D(G_{i-1}/G_i) \lhd G_{i-1}/G_i$ geldt, volgt $G_{i-1}/G_i \simeq C_{p_i}$ voor een priemgetal p_i met $i \in \underline{r}$. □

Ga zelf na dat deze karakteriseringen van oplosbare groepen de aankondiging in het begin van deze paragraaf waar maken. Dankzij de nu volgende

stelling en 5.2.3 is het mogelijk om bij veel bewijzen waarin oplosbaarheid een rol speelt, induktie te gebruiken.

5.2.7. STELLING. *Laat* G *een groep zijn met een normaaldeler* N. *Als* N *en* G/N *oplosbaar zijn, dan is ook* G *oplosbaar.*

BEWIJS. Volgens Stelling 5.2.4 zijn er ketens $G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq G_2/N \trianglerighteq \trianglerighteq \ldots \trianglerighteq G_s/N = N/N$ en $N = G_s \trianglerighteq G_{s+1} \trianglerighteq \ldots \trianglerighteq G_r = \{1\}$ met $(G_{i-1}/N)/(G_i/N)$ voor $i = 1,2,\ldots,s$ en G_{j-1}/G_j voor $j = s+1,s+2,\ldots,r$ abels. Vanwege $(G_{i-1}/N)/(G_i/N) \simeq G_{i-1}/G_i$ $(i \in \underline{s})$ is $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_r = \{1\}$ een keten van ondergroepen van G met G_{i-1}/G_i een abelse groep voor $i \in \underline{r}$. Uit Stelling 5.2.4 volgt dat G oplosbaar is. □

Volgens Korollarium 5.2.5 is elke groep G met een orde $|G| = p^a$, p priem oplosbaar. We zullen nu een bekende stelling van Burnside bewijzen die zegt dat ook groepen met een orde $|G| = p^a q^b$, p en q priem, oplosbaar zijn. Daartoe bewijzen we eerst het nu volgende lemma.

5.2.8. LEMMA. *Laat* G *een eindige groep zijn en* f *een irreducible komplexe voorstelling van* G *van de graad* n *met karakter* χ. *Als* K *een konjugatieklasse is met* $\text{ggd}(|K|,n) = 1$ *dan is* $\chi(K) = 0$ *of* $f(K) = \{\lambda I\}$ *voor zekere* $\lambda \in \mathbb{C}$.

BEWIJS. Volgens 4.2.17 zijn $\chi(K)$ en $\frac{|K| \cdot \chi(K)}{n}$ algebraïsch geheel. Daar $\text{ggd}(|K|,n) = 1$ zijn er $a,b \in \mathbb{Z}$ zó dat $a|K| + bn = 1$. Hieruit volgt dat $a\frac{|K|\chi(K)}{n} + b\chi(K) = \frac{\chi(K)}{n}$ algebraisch geheel is. Laat m de orde van f(x) voor x uit K zijn en laat ω een primitieve m-de machtseenheidswortel zijn. De eigenwaarden van f(x) zijn dan $\omega = \omega^{k_1}, \omega^{k_2}, \ldots, \omega^{k_n}$ (zeg), zodat

$$\left|\frac{\chi(K)}{n}\right| = \left|\frac{1}{n}\sum_{i=1}^{n} \omega^{k_i}\right| \leq \frac{1}{n}\sum_{i=1}^{n} \left|\omega^{k_i}\right| = 1,$$

met gelijkheid dan en slechts dan als $\omega = \omega^{k_1} = \omega^{k_2} = \ldots = \omega^{k_n}$, d.w.z. dan en slechts dan als $f(x) = \omega I$. Maar dan is $f(K) = \{\omega I\}$. Als $n^{-1}|\chi(K)| < 1$ dan geldt ook voor algebraïsch gekonjugeerden $n^{-1}|\sum_{i=1}^{n} \omega^{jk_i}| < 1$ $(\text{ggd}(j,m) = 1)$ en daarmee ook

$$\left|\prod_{\text{ggd}(j,m)=1} (n^{-1}\sum_{i=1}^{n} \omega^{jk_i})\right| < 1.$$

Maar het linkerlid in deze ongelijkheid is een geheel getal en veelvoud van de norm $N(n^{-1}\chi(K))$ (zie 4.2.16), zodat $N(n^{-1}\chi(K)) = 0$ en daarmee ook $\chi(K) = 0$. □

5.2.9. STELLING (Burnside). *Laat* G *een eindige enkelvoudige groep zijn en* $K \neq \{1\}$ *een konjugatieklasse met* $|K| = p^a$ *voor zekere priem* p *en* $a \in \mathbb{N} \cup \{0\}$. *Dan is* G *abels.*

BEWIJS. Veronderstel dat G een enkelvoudige niet-abelse groep is en laat $K \subseteq G$ gegeven zijn als in de stelling. Stel dat f een niet triviale voorstelling is met karakter χ zo dat $\chi(K) \neq 0$ en $p \nmid \chi(1)$. Dan is er volgens het vorige lemma een $\lambda \in \mathbb{C}$ zo dat $f(k) = \lambda I$ voor alle $k \in K$. Dus geldt $\{1\} \neq f(K) \subseteq Z(f(G)) \trianglelefteq f(G)$, zodat $f(G) = Z(f(G))$ abels is en $G = D(G) \leq \text{Kern}(f)$. Dit is een tegenspraak want f is niet-triviaal. We hebben nu bewezen dat voor elk niet-triviaal irreducibel karakter χ met $p \nmid \chi(1)$ geldt $\chi(K) = 0$.

Laat ρ het karakter zijn behorende bij de reguliere voorstelling van G. Volgens het bewijs van Propositie 4.2.8 geldt

$$0 = \rho(K) = \sum_{\chi \in \text{Irr } G} \chi(1)\chi(K) = 1 + p \sum_{\substack{\chi \in \text{Irr } G \\ \chi \neq 1}} \frac{\chi(1)}{p} \chi(K),$$

zodat

$$-\frac{1}{p} = \sum_{\substack{\chi \in \text{Irr } G \\ \chi \neq 1}} \chi(K)$$

algebraïsch geheel is.
Met deze laatste tegenspraak is de stelling bewezen. □

5.2.10. STELLING (Burnside). *Een groep* G *van orde* $|G| = p^a q^b$, p *en* q *priem, is oplosbaar.*

BEWIJS. Volgens Stelling 5.2.7 is een kleinste tegenvoorbeeld G enkelvoudig. Laat P een p-Sylowondergroep van G zijn en kies $z \in Z(P) - \{1\}$. Dan geldt $C_G(z) \geq P$ zodat de konjugatieklasse die z bevat, lengte $|G : C_G(z)| = q^c$ met $c \leq b$ heeft. Volgens Stelling 5.2.9 is $G \simeq C_p$ en dus oplosbaar. Dit is in tegenspraak met onze aanname dat G niet oplosbaar is. □

Opgaven bij §5.2

1. Bewijs (zonder gebruik te maken van Stelling 5.2.10) dat groepen van orde pq met p en q priem, oplosbaar zijn.
2. Bewijs dat groepen van orde pqr met p,q en r priem, oplosbaar zijn.
3. Geef een niet-oplosbare groep aan waarvan de orde bestaat uit een produkt van machten van drie verschillende priemgetallen.

4. Laat zien dat het direkte produkt van een stel oplosbare groepen oplosbaar is. Hoe zit dat met het semidirekte produkt van twee oplosbare groepen?

5. Bewijs dat er in elke eindige oplosbare groep G een niet-triviale normaaldeler te vinden is die een p-groep voor zekere priem p is.

*6. Laat G een groep zijn van orde $p_1^{m_1} p_2^{m_2} \ldots p_t^{m_t}$ voor p_i ($i \in \underline{t}$) onderling verschillende priemgetallen. Stel dat er voor alle $i \in \underline{t}$ een ondergroep H_i van G is met $|G: H_i| = p_i^{m_i}$. Bewijs dat G oplosbaar is.

Aanwijzingen: Laat G een minimaal tegenvoorbeeld zijn. Leid af dat $K = \bigcap_{i=3}^{t} H_i$ orde $|K| = p_1^{m_1} p_2^{m_2}$ heeft en dus oplosbaar is. Gebruik Opgave 5 om een niet-triviale normale p-ondergroep P (waar $p = p_1$ of p_2) van K te vinden.

Toon vervolgens aan dat P bevat is in $N = \bigcap_{g \in G} gH_i g^{-1}$ waar i = 1 of 2 al naar gelang $p = p_2$ of p_1.

Pas tenslotte de induktiehypothese toe op N en G/N (vergelijk 5.2.7).

7. Bewijs voor een rang 3 permutatiegroep G zonder reguliere normaaldelers dat G een minimale normaaldeler N bezit met $G \lesssim \mathrm{Aut}(N)$ zodanig dat $N \cong N_1$ of $N \cong N_1 \times N_1$ voor een niet-abelse enkelvoudige ondergroep N_1 van G.

Aanwijzing: Pas het bewijs van 3.1.20 aan. Gebruik in Stap 5 de stelling van Burnside 5.2.10 om 3 verschillende priemgetallen te vinden die de orde van N_1 (uit 3.1.20) delen.

5.3. Nilpotente groepen

In deze paragraaf zullen we een bekende deelklasse van de klasse van oplosbare groepen beschouwen die veel eigenschappen gemeen heeft met de klasse van abelse groepen.

5.3.1. DEFINITIE. Een eindige groep heet *nilpotent* als zij het direkte produkt is van haar Sylow-ondergroepen.

5.3.2. PROPOSITIE. *Een nilpotente groep is oplosbaar.*

BEWIJS. Volgens 5.2.5 zijn p-groepen oplosbaar. Volgens Opgave 5.2.4 is het direkte produkt van oplosbare groepen oplosbaar. □

5.3.3. PROPOSITIE. *Een groep* G *is nilpotent dan en slechts dan als elke Sylow-ondergroep van* G *een normaaldeler is.*

BEWIJS. Dit is opgave 1.8.3. □

5.3.4. STELLING. *Elke ondergroep en elk homomorf beeld van een nilpotente groep is nilpotent.*

BEWIJS. Laat H een ondergroep van de nilpotente groep G zijn, en P een p-Sylow-ondergroep van G. Uit $HP/P \simeq H/(H \cap P)$ volgt dat $H \cap P$ een normale p-Sylow-ondergroep van H is. Nu volgt uit 5.3.3. dat H nilpotent is. Laat $\bar{G}$ een homomorf beeld zijn van $G = P_1 \times P_2 \ldots \times P_k$, waarbij de P_i de p_i-Sylow-ondergroepen van G voorstellen ($i \in \underline{k}$). Dan is $\bar{G} = \bar{P}_1 \times \bar{P}_2 \times \ldots \times \bar{P}_k$, waarin $\bar{P}_i$ het homomorfe beeld is van P_i onder het betreffende morfisme van G op $\bar{G}$. Dus $P_i = \{1\}$ of een p_i-Sylow-ondergroep van $\bar{G}$ en daarmee is $\bar{G}$ nilpotent. □

5.3.5. PROPOSITIE. *Laat G een nilpotente groep zijn. Als* $H < G$ *dan ook* $H < N_G(H)$.

BEWIJS. Daar $H < G$ is er een p-Sylow-ondergroep P van G met $H \cap P < P$. Volgens Stelling 2.2.36 (ii) is er een groep R met $H \cap P < R \leq P$ en $|R: H \cap P| = p$. Volgens Lemma 2.2.1 geldt $H \cap P \lhd R$ en dus normaliseert R de p-Sylow ondergroep $H \cap P$ van H. Daar $R \leq P$ en G nilpotent is, centraliseert R alle andere Sylow-ondergroepen van H. Dus geldt $H \lhd RH \leq N_G(H)$. □

5.3.6. PROPOSITIE. *Iedere maksimale ondergroep van een nilpotente groep* G *is een normale ondergroep van priemindex en bevat dus* D(G).

BEWIJS. Laat M een maksimale ondergroep van G zijn. Dan geldt volgens 5.3.5 dat $M < N_G(M)$, en dus, daar M maksimaal is, $N_G(M) = G$. Anders gezegd $M \lhd G$. Uit de maksimaliteit van M volgt verder nog dat G/M geen echte ondergroepen bevat zodat $G/M \simeq C_p$ voor zekere priem p. Daar C_p abels is volgt nog $D(G) \leq M$. □

5.3.7. LEMMA. *Laat* G *een nilpotente groep zijn en* H *een ondergroep van* G *die voldoet aan* $G = HD(G)$. *Dan is* $H = G$.

BEWIJS. Stel dat $H < G$. Laat M een maksimale ondergroep van G zijn die H bevat. Dan geldt volgens Propositie 5.3.6 dat $M \geq D(G)$ dus $M \geq D(G)H = G$, een tegenspraak. □

5.3.8. STELLING. *Een eindige groep is nilpotent precies dan als alle maksimale ondergroepen normaal zijn.*

BEWIJS. Laat G een eindige groep zijn waarvan alle maksimale ondergroepen normaal zijn. Uit Propositie 2.1.6 (i) volgt direkt dat iedere Sylow-ondergroep een normaaldeler van G is, zodat G nilpotent is volgens 5.3.3. De rest volgt uit 5.3.6. □

5.3.9. STELLING. *Een eindige groep* G *is nilpotent precies dan als voor elke ondergroep* $H < G$ *geldt* $H < N_G(H)$.

BEWIJS. Laat $H < N_G(H)$ voor elke $H < G$ en laat P een Sylow-ondergroep van G zijn. Als $P = G$ dan is G nilpotent. Als $P < G$ dan is $P \lhd G$ want $N_G(P) < G$ impliceert $N_G(N_G(P)) > N_G(P)$ wat in tegenspraak is met Propositie 2.1.6(i). Dus G is nilpotent volgens Propositie 5.3.3. De rest staat in 5.3.5. □

5.3.10. STELLING. *Laat* G *een eindige groep zijn. Definieer ondergroepen* $\{1\} = Z_0(G) \leq Z_1(G) \leq \ldots$ *van* G *door* $Z_0(G) = \{1\}$ *en door voor* $Z_{i+1}(G)$ *het volledig origineel in* G *van* $Z(G/Z_i(G))$ *onder het natuurlijk morfisme* $G \to G/Z_i(G)$ *te nemen. Precies dan is* G *nilpotent als* $Z_r(G) = G$ *voor zekere* $r \in \mathbb{N}$.

BEWIJS. Merk op dat iedere $Z_i(G)$ een karakteristieke (en dus normale) ondergroep van G is. Als G een p-groep is, dan is er een $r \in \mathbb{N}$ met $Z_r(G) = G$ volgens Opgave 1.6.12. Dus geldt voor nilpotente groepen dat er een $r \in \mathbb{N}$ is met $Z_r(G) = G$.
Anderzijds, laat G een groep zijn met $Z_r(G) = G$ voor zekere r. Als $r = 1$, dan is $G = Z(G)$ abels en dus nilpotent. Neem aan $r > 1$ en laat $H < G$. Als $H \not\leq Z(G)$ dan is $N_G(H) > H$. Als $H \geq Z(G)$, dan geldt op grond van induktie dat $G/Z(G)$ nilpotent is, dus met 5.3.9, $N_{G/Z(G)}(H/Z(G)) > H/Z(G)$ en daarmee ook in dit geval $N_G(H) > H$. Volgens Stelling 5.3.9 is G nilpotent. □

Een soortgelijke karakterisering van nilpotentie, maar nu met een dalende rij karakteristieke ondergroepen in plaats van een stijgende rij, geeft de volgende stelling. Hiertoe eerst enige notatie. Als A en B deelverzamelingen zijn van een groep G dan definiëren we $[a,b] = aba^{-1}b^{-1}$ voor $a \in A, b \in B$ en $[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$. Dus $[G,G] = D(G)$.

5.3.11. STELLING. *Laat* G *een eindige groep zijn. Definieer* $K_i(G)$ *rekursief door* $K_0(G) = G$ *en* $K_{i+1}(G) = [K_i(G),G]$ *voor* $i \in \mathbb{N} \cup \{0\}$. *Dan is* $K_i(G)$ *een karakteristieke ondergroep van* G; $G = K_0(G) \geq K_1(G) \geq \ldots$ *en* G *is nilpotent precies dan als er een* $r \in \mathbb{N}$ *is zo dat* $K_r(G) = \{1\}$.

BEWIJS. Laat ϕ een homomorfisme van G op een groep $\bar{G}$ zijn. Uit de definitie van $K_i(G)$ volgt direkt (met induktie) $K_i(G)^\phi = K_i(G^\phi)$, zodat de $K_i(G)$ karakteristieke ondergroepen zijn. Laat $i \in \mathbb{N}$, $k \in K_i(G)$ en $g \in G$. Daar $K_i(G) \trianglelefteq G$ geldt $[k,g] = k^{-1}g^{-1}kg \in K_i(G)$, dus $K_{i+1}(G) \leq K_i(G)$.
Met $Z_i(G)$ gedefinieerd als in 5.3.10 gaat men eenvoudig na dat $K_j(G) \leq Z_i(G)$ equivalent is met $[K_{j-1}(G),G] \leq Z_i(G)$, of wel met $K_{j-1}(G)Z_i(G)/Z_i(G) \leq$ $\leq Z(G/Z_i(G))$, dus met $K_{j-1}(G) \leq Z_{i+1}(G)$. Als G nilpotent is dan is er een $r \in \mathbb{N}$ met $Z_r(G) = G = K_0(G)$ en dan volgt $\{1\} = Z_0(G) \geq K_r(G)$, dus $K_r(G) =$ $= \{1\}$. Als er een $r \in \mathbb{N}$ is met $K_r(G) = \{1\}$ dan volgt uit $K_r(G) = \{1\} = Z_0(G)$ dat $Z_r(G) \geq K_0(G) = G$, dus G is nilpotent volgens 5.3.10. □

Opgaven bij §5.3

1. Laat G een eindige groep zijn. Definieer de groepen $I_i(G)$, $i \in \mathbb{N}$ door $I_1(G) := \mathrm{Int}(G)$ en $I_{i+1}(G) = \mathrm{Int}(I_i(G))$, $i \in \mathbb{N}$. Als er een $r \in \mathbb{N}$ is met $I_r(G) = \{1\}$ dan is G nilpotent. Bewijs dit.

*2. Geef een voorbeeld van een niet-nilpotente groep G met een nilpotente normaaldeler N zo dat G/N ook nilpotent is.

3. Laat N een normaaldeler van de eindige groep G zijn die bevat is in Z(G). Toon aan: G/N nilpotent impliceert G nilpotent.

4. Een eindige groep G is nilpotent dan en slechts dan als voor iedere normaaldeler $N \neq G$ geldt $Z(G/N) \neq 1$. Toon dit aan.

*5. Als de eindige groep G nilpotent is en $N \trianglelefteq G$, dan is $N \cap Z(G) \neq \{1\}$. (Aanwijzing: bewijs dit eerst voor G een p-groep.)

*6. Bewijs dat het direkte produkt van een eindig stel nilpotente groepen weer nilpotent is.

7. Laat zien dat een eindige groep G dan en slechts dan nilpotent is als voor elk tweetal $x,y \in G$ geldt: $\mathrm{ggd}(|\langle x\rangle|, |\langle y\rangle|) = 1 \Rightarrow |\langle xy\rangle| =$ $= |\langle x\rangle||\langle y\rangle|$.
Hint voor het "als"-deel: Laat $P_1,P_2,\ldots,P_t$ Sylow-ondergroepen van G bij de verschillende priemdelers van $|G|$ zijn. Laat zien dat de verzameling $P_1P_2\ldots P_t$ uit precies $|G|$ elementen bestaat.

5.4. De Frattini- en Fitting-ondergroep

Naast de kommutatorondergroep en het centrum van een groep zijn er nog andere karakteristieke ondergroepen in een groep aan te wijzen. Voorbeelden hiervan staan aan het eind van de vorige paragraaf. In deze paragraaf zullen we nog twee van zulke ondergroepen bestuderen: de Frattini-ondergroep en de Fitting-ondergroep.

5.4.1. DEFINITIE. Laat G een eindige niet-triviale groep zijn. De *Frattini-ondergroep van* G, notatie $\Phi(G)$, is de doorsnede van alle maksimale ondergroepen van G. Verder is $\Phi(\{1\}) := \{1\}$.

Een automorfisme van G permuteert de maksimale ondergroepen van G, zodat $\Phi(G) \trianglelefteq G$ (als $|G| > 1$). De volgende stelling geeft een beschrijving van $\Phi(G)$ als verzameling van voor voortbrenging van G overbodige elementen.

5.4.2. STELLING. *Laat* $G \neq \{1\}$ *een eindige groep zijn. Dan is* $\Phi(G) = \{x \in G \mid \forall S \subseteq G\ [\langle S,x\rangle = G \Rightarrow \langle S\rangle = G]\}$.

BEWIJS. Laat $x \in G$ de eigenschap hebben dat voor elke deelverzameling $S \subseteq G$ geldt: $\langle S,x\rangle = G$ impliceert $\langle S\rangle = G$. Als M een maksimale ondergroep van G is en $x \notin M$, dan is $\langle M,x\rangle = G$ en dus $M = G$ hetgeen absurd is. Dus $x \in M$ voor iedere maksimale ondergroep M van G, zodat $x \in \Phi(G)$. Anderzijds, laat $x \in \Phi(G)$ en laat $S \subseteq G$ zo dat $\langle x,S\rangle = G$. Als $\langle S\rangle < G$ dan is er een maximale ondergroep $M \geq \langle S\rangle$. Daar $x \in \Phi(G) \leq M$ krijgen we nu de tegenspraak $G = \langle x,S\rangle \leq \langle x,M\rangle = M$. Dus $\langle S\rangle = G$. □

5.4.3. STELLING. *Laat* G *een eindige groep zijn en laat* N *een normaaldeler van* G *zijn die* $\Phi(G)$ *omvat. Als* $N/\Phi(G)$ *nilpotent is, dan is ook* N *nilpotent.*

BEWIJS. Laat P een Sylow-ondergroep van N zijn. Dan is omdat $N/\Phi(G)$ nilpotent is, $P\Phi(G)$ een normaaldeler van N. De groep $P\Phi(G)$ is vanzelfsprekend ook normaal in $N_G(P)N$. Maar vanwege het Frattini-argument (2.1.6(ii)) is laatstgenoemde groep gelijk G. Passen we het Frattini-argument andermaal toe, maar nu op de normaaldeler $P\Phi(G)$ van G en haar Sylow-ondergroep P, dan krijgen we

$$G = N_G(P)P\Phi(G) = N_G(P)\Phi(G).$$

Volgens 5.4.2 volgt $N_G(P) = G$, ofwel $P \trianglelefteq G$. Er volgt $P \trianglelefteq N$. Hiermee is de stelling volgens Propositie 5.3.3. bewezen. □

5.4.4. GEVOLGEN. *Laat* G *een eindige groep zijn. Er geldt*

(i) $\Phi(G)$ *is nilpotent.*

(ii) G *is nilpotent dan en slechts dan als* $G/\Phi(G)$ *nilpotent is.*

BEWIJS.

(i) Pas de stelling toe met $N = \Phi(G)$.

(ii) Pas de stelling toe met $N = G$ voor de ene implikatie en citeer Stelling 5.3.4 voor de andere.

In de volgende stellingen beschouwen we de Frattini-ondergroep van een p-groep. We brengen in herinnering dat een elementair abelse groep een groep van de vorm C_p^n is (zie Opgave 2.3.1).

5.4.5. STELLING. *Laat* P *een* p*-groep zijn* (p *priem*). *Dan geldt*

$$\Phi(P) = D(P)\,Q \text{ met } Q := \langle x^p \mid x \in P \rangle .$$

Verder is $P/\Phi(P)$ *elementair abels en is* $\Phi(P)$ *de kleinste normaaldeler van* P *met elementair abelse faktorgroep.*

BEWIJS. Laat M een maksimale ondergroep van P zijn. Volgens Stelling 2.2.3 geldt $|P:M| = p$ zodat $M \lhd P$ (Lemma 2.2.1). Dus geldt $P/M \simeq C_p$, zodat $M \geq D(P)$ (omdat C_p abels is) en $M \geq Q$ (omdat ieder element in C_p orde 1 of p heeft). De konklusie is $D(P)Q \leq \Phi(P)$. Laat $N \trianglelefteq P$ met P/N elementair abels en kies $x \in P-N$. Daar P/N isomorf is met de optelgroep van een eindig dimensionale vektorruimte over $\mathbb{F}_p$ zijn er $x_1 = x, x_2, \ldots, x_d \in P$ zó dat $\{x_1N, x_2N, \ldots, x_dN\}$ een basis is voor P/N. Dus geldt $P = \langle x_1, x_2, \ldots, x_d, N\rangle \neq \langle x_2, x_3, \ldots, x_d, N\rangle$. Uit Stelling 5.4.2 volgt nu dat $x = x_1 \notin \Phi(P)$, en hebben we $\Phi(P) \leq N$ bewezen. Omdat $D(P)Q \trianglelefteq P$ en $P/D(P)Q$ elementair abels is volgt in het bijzonder $\Phi(P) \leq D(P)Q$. Hiermee is het gestelde aangetoond. □

5.4.6. STELLING (Basisstelling van Burnside). *Laat* P *een* p*-groep zijn* (p *priem*) *met* $|P/\Phi(P)| = p^d$. *Iedere kleinste verzameling van voortbrengers van* P *bevat* d *elementen en elk element van* $P-\Phi(P)$ *is bevat in een kleinste verzameling van voortbrengers.*

BEWIJS. Er geldt $\langle x_1, x_2, \ldots, x_k\rangle = P \iff \langle x_1, x_2, \ldots, x_k, \Phi(P)\rangle = P$ $\iff \langle x_1\Phi(P), x_2\Phi(P), \ldots, x_k\Phi(P)\rangle = P/\Phi(P)$, en volgens de vorige stelling kunnen we $P/\Phi(P)$ opvatten als een d-dimensionale vektorruimte over $\mathbb{F}_p$. Elke basis van een d-dimensionale vektorruimte bevat d vektoren $\neq 0$ en elke vektor $\neq 0$ zit in een basis. □

We zullen nu de Fitting-ondergroep van een groep beschouwen.

5.4.7. DEFINITIE. Laat G een eindige groep zijn. Het produkt van alle nilpotente normaaldelers van G heet de *Fitting-ondergroep* van G. Met F(G) geven we deze ondergroep aan.

Het is direkt duidelijk dat F(G) een karakteristieke ondergroep van G is.

5.4.8. STELLING. *Laat* G *een eindige groep zijn. Dan is* F(G) *nilpotent.*

BEWIJS. Laat N en M nilpotente normaaldelers van G zijn en laat L = NM. Het is voldoende aan te tonen dat L nilpotent is. Laat P een p-Sylow-ondergroep zijn van L. Volgens Propositie 1.5.8 is

$$|L| = |NM| = \frac{|N||M|}{|N\cap M|} \quad \text{en} \quad |(P\cap N)(P\cap M)| = \frac{|P\cap N||P\cap M|}{|P\cap N\cap M|}.$$

Volgens Propositie 2.1.8 zijn $P \cap N$, $P \cap M$, $P \cap N \cap M$ p-Sylow-ondergroepen van respektievelijk N,M en $N \cap M$. Hieruit volgt dat $(P\cap N)(P\cap M)$ een p-Sylow-ondergroep van L is. Dus $P = (P\cap N)(P\cap M)$. Daar N en M nilpotent zijn geldt $P \cap N \trianglelefteq N$ en $P \cap M \trianglelefteq M$, dus volgt uit $N,M \trianglelefteq G$ dat $P \cap N, P \cap M \trianglelefteq G$. Nu volgt $P = (P\cap N)(P\cap M) \trianglelefteq L$, zodat L nilpotent is volgens 5.3.3. □

Op grond van deze stelling kunnen we de Fitting-ondergroep van een groep dus ook definiëren als de grootste nilpotente normaaldeler van de groep.

5.4.9. STELLING. *Laat* G *een eindige groep zijn. Dan bevat* $C_G(F(G))F(G)/F(G)$ *geen niet-triviale oplosbare normaaldeler van* G/F(G). *Meer in het bijzonder geldt voor oplosbare* G *dat* $C_G(F(g)) \leq F(G)$.

BEWIJS. Laat N/F(G) een abelse normaaldeler van G/F(G) zijn met $N \leq C_G(F(G))F(G)$. Schrijf $C = N \cap C_G(F(G))$; dan is

$$N/C \leq CF(G)/C \simeq F(G)/(F(G)\cap C), \text{ dus is } N/G$$

nilpotent (5.3.4). Uit Stelling 5.3.11 volgt de eksistentie van een $r \in \mathbb{N}$ met $K_r(N/C) = C/C$, d.w.z. $K_r(N) \leq C$. Daar $K_r(N) \leq K_1(N) = D(N) \leq F(G)$ (de laatste inklusie vanwege het feit dat N/F(G) abels is) vinden we $K_r(N) \leq C \cap F(G) \leq Z(F(G)) \leq Z(N)$ (in de laatste inklusie is $N \leq C_G(F(G))F(G)$ gebruikt) zodat $K_{r+1}(N) = \{1\}$ geldt. Dus is N nilpotent volgens Stelling 5.3.11 en $N \leq F(G)$. Daar iedere niet-triviale oplosbare normaaldeler van

een groep een niet-triviale abelse normaaldeler van die groep heeft (waarom?) is hiermee de stelling bewezen. □

5.4.10. STELLING. *Als* G *een eindige groep is dan geldt* $F(G/\Phi(G)) = F(G)/\Phi(G)$.

BEWIJS. Uit 5.4.4(i) volgt dat $\Phi(G) \leq F(G)$. Laat $F' \leq G$ zo gekozen zijn dat $F'/\Phi(G)$ de Fitting-ondergroep $F(G/\Phi(G))$ van $G/\Phi(G)$ is. Omdat $F(G)/\Phi(G)$ nilpotent is geldt $F'/\Phi(G) \geq F(G)/\Phi(G)$, dus $F' \geq F(G)$. Daar $F'/\Phi(G)$ wegens 5.4.8 nilpotent is, is F' nilpotent (zie 5.4.3). Dus geldt ook $F' \leq F(G)$, zodat nu $F(G) = F'$ volgt. □

Opgaven bij §5.4.

1. Bepaal $\Phi(G)$ voor $G = \mathbb{Z}_n$, Sym(3), Q.
2. Laat K een normaaldeler en laat H een ondergroep zijn van de eindige groep G. Toon aan dat uit $K \leq \Phi(H)$ volgt dat $K \leq \Phi(G)$.
3. Laat G,H een tweetal eindige groepen zijn. Bewijs achtereenvolgens:
   (i) $\Phi(G\times H) = \Phi(G) \times \Phi(H)$
   (ii) $H \trianglelefteq G \Rightarrow \Phi(H) \trianglelefteq \Phi(G)$
   (iii) $H \trianglelefteq G \Rightarrow \Phi(G)H/H \leq \Phi(G/H)$
4. (i) Toon aan dat een eindige groep G precies dan nilpotent is als $D(G) \leq \Phi(G)$.
   (ii) Bewijs dat een normaaldeler H van G precies dan nilpotent is als $D(H) \leq \Phi(G)$.
5. (i) Voor een eindige groep G geldt $D(G) \cap Z(G) \leq \Phi(G)$. Toon dit aan.
   (ii) Bewijs dat zelfs $D(G) \cap Z_i(G) \leq \Phi(G)$ voor $i \in \mathbb{N}$.
6. Bepaal F(G) voor G = Sym(3), Sym(4)
7. Bewijs: Als de eindige groep $G \neq \{1\}$ oplosbaar is, dan geldt $\Phi(G) < F(G)$.
8. Als N een minimale normaaldeler van de eindige groep G is, dan geldt $F(G) \leq C_G(N)$. Als N bovendien abels is, dan is $N \leq Z(F(G))$
   (aanwijzing: Volgens Opgave 5.3.5 is een minimale normaaldeler van een nilpotente groep bevat in het centrum van de groep).

5.5. De stelling van Schur-Zassenhaus

We besluiten dit hoofdstuk met een voldoende voorwaarde opdat een groep G met gegeven normaaldeler een semi-direkt produkt is.

5.5.1. DEFINITIE. Als G een groep is, $N \trianglelefteq G$, $K \leq G$, $G = NK$ en $N \cap K = \{1\}$ (d.w.z. als G het semi-direkt produkt is van N en K) dan heet K een *komplement* van N in G.

5.5.2. STELLING (Schur-Zassenhaus). *Laat* G *een eindige groep met een normaaldeler* N *die voldoet aan* ggd $(|N|,|G/N|) = 1$. *Dan heeft* N *een komplement in* G.

BEWIJS. Laat de groep G een minimaal tegenvoorbeeld zijn. Het bewijs gaat in een aantal stappen.

STAP 1. N is nilpotent.

Laat P een Sylow-ondergroep van N zijn. Volgens het Frattini-argument (Propositie 2.1.6 (ii)) geldt $G = N_G(P)N$ zodat $|G/N| = |N_G(P)/N_N(P)|$. Dus zijn $|N_N(P)|$ en $|N_G(P)/N_N(P)|$ relatief priem. Stel nu dat $N_G(P) < G$ dan is er een komplement K van $N_N(P)$ in $N_G(P)$. Daar $|K| = |N_G(P)/N_N(P)| = |G/N|$ is K ook een komplement van N in G. Dus geldt $N_G(P) = G$, met andere woorden $P \trianglelefteq G$ en N is nilpotent op grond van 5.3.3.

STAP 2. N is abels. Uit Stap 1 en 5.3.2 volgt dat $D(N) < N$. Neem aan dat N niet abels is, d.w.z. neem aan dat $D(N) > 1$. Dan is $|G/D(N)| < |G|$ en kunnen we dus in G/D(N) een komplement H/D(N) van N/D(N) vinden (immers ggd $(|N/D(N)|, |G/D(N)/N/D(N)|) = 1$). Nu is $|H/D(N)| = |G/D(N)/N/D(N)| = |G/N|$ relatief priem met $|N|$ en dus ook met $|D(N)|$. Bovendien geldt $|H| = |G/N| \cdot |D(N)| < |G|$. Er is dus in H een komplement K van D(N). Maar $|K| = |H/D(N)| = |G/N|$ zodat K ook een komplement van N in G is. Dus $D(N) = 1$ en N is abels.

STAP 3. Slot van het bewijs.

We konstrueren een homomorfisme h van G in G met kern N. Kies hiertoe representanten $r_\alpha \in G$ voor de verschillende rechts-nevenklassen α van N in G. Dan geldt $x \in r_{(xN)}N$ voor alle $x \in G$ en $r_\alpha r_\beta N = r_{\alpha\beta}N$ voor alle $\alpha,\beta \in G/N$. Definieer de afbeelding $f: G \times (G/N) \to N$ door

$$f(x,\alpha) := x r_\alpha r_{(xN)\alpha}^{-1}, \qquad x \in G,\ \alpha \in G/N.$$

(Dat $f(x,\alpha) \in N$ volgt uit $x r_\alpha r_{(xN)\alpha}^{-1} \in r_{(xN)} r_\alpha r_{(xN)\alpha}^{-1} N = N$.) De afbeelding f voldoet aan

(a) $f(xy,\alpha) = xf(y,\alpha)x^{-1}f(x,(yN)\alpha)$ voor alle $x,y \in G$, $\alpha \in G/N$, en

(b) $f(n,\alpha) = n$ voor alle $n \in N$, $\alpha \in G/N$.

Immers, voor $x,y \in G$ en $\alpha \in G/N$ geldt $f(xy,\alpha) = xyr_\alpha r_{(xyN)\alpha}^{-1} = xyr_\alpha r_{(yN)\alpha}^{-1} x^{-1} x r_{(yN)\alpha} r_{(yN\alpha)}^{-1} = xf(y,\alpha)x^{-1}f(x,(yN)\alpha)$, en voor $n \in N$ geldt $f(n,\alpha) = nr_\alpha r_{nN\alpha}^{-1} = nr_\alpha r_\alpha^{-1} = n$.

Daar $|G/N|$ relatief priem is met $|N|$, is er een $m \in \mathbb{N}$ met $|G/N|m = 1 \bmod |N|$. Definieer nu de afbeelding $g: G \to N$ door middel van

$$g(x) = \Big(\prod_{\alpha\in G/N} f(x,\alpha)\Big)^m .$$

(Volgens Stap 2 is N abels en is g dus goed gedefinieerd.) Voor g gelden dan de eigenschappen $g(xy) = xg(y)x^{-1}g(x)$ en $g(n) = n$ voor alle $x,y \in G$, $n \in N$ want

$$g(xy) = \Big(\prod_{\alpha\in G/N} f(xy,\alpha)\Big)^m = \Big(\prod_{\alpha\in G/N} (xf(y,\alpha)x^{-1})\Big)^m\Big(\prod_{\alpha\in G/N} f(x,(yN)\alpha)\Big)^m =$$

$$= xg(y)x^{-1}g(x), \quad \text{en} \quad g(n) = \Big(\prod_{\alpha\in G/N} f(n,\alpha)\Big)^m = \Big(\prod_{\alpha\in G/N} n\Big)^m = n^{|G/N|m} = n,$$

als $x,y \in G$ en $n \in N$.
Tenslotte definieren we de afbeelding $h: G \to G$ door $h(x) = g(x)^{-1}x$ voor alle $x \in G$. Voor $x,y \in G$ geldt dan

$$h(xy) = g(xy)^{-1}(xy) = g(x)^{-1}xg(y)^{-1}x^{-1}xy = g(x)^{-1}xg(y)^{-1}y = h(x)h(y).$$

Dus is h een homomorfisme van G in G. Als $n \in N$ dan is $h(n) = g(n)^{-1}n =$ $= n^{-1}n = 1$, en als $x \notin N$ dan is $h(x) = g(x)^{-1}x \in xN \neq N$ zodat $h(x) \neq 1$. Dus geldt $N = \mathrm{Ker}\,(h)$. Laat nu K het h-beeld zijn van G dan is $K \leq G$ en $K \simeq G/N$. Dus K is een komplement van N in G. Met deze laatste tegenspraak is de stelling bewezen. □

Opgaven bij §5.5.

1. Merk op dat voor G als in de stelling elke ondergroep K met $|K| = |G/N|$ een komplement van N is.
2. Als G een eindige groep is en als $p \mid\mid \Phi(G)$ dan ook $p \mid\mid G/\Phi(G)$. Bewijs dit.
3. Als p een priemdeler van de orde van een eindige groep G met normaaldeler N is zodat p geen deler van $|G/N|$ is, dan bestaat er een ondergroep H waarvan de orde niet door p deelbaar is, zodat $G = HN$. Bewijs dit.

LITERATUURLIJST

- Een zeer leesbare, maar ietwat elementaire introduktie:

BAUMSCHLAG, B. & B. CHANDLER, *Theory and Problems of Group Theory*, McGraw-Hill, New York, 1968.

- Goed bij hoofdstukken 1, 2 en 5 te gebruiken:

HALL, M. Jr., *The Theory of Groups*, McMillan, New York, 1959.

ROSE, J.S., *A course on Group Theory*, Cambridge University Pres Cambridge, 1978.

- Over permutatiegroepen, veel verder gaand dan hoofdstuk 3:

PASSMAN, D., *Permutation Groups*, Benjamin, New York, 1968.

WIELANDT, H., *Finite Permutation Groups*, Academic Press, New York, 1964.

- Over de lineaire representatietheorie (hoofdstuk 4):

DORNHOFF, L., *Group Representation Theory*, Marcel Dekker, New York, 1971.

FEIT, W., *Characters of Finite Groups*, Benjamin, New York, 1967.

SERRE, J.P., *Représentations lineaires des groupes finis*, Hermann, Parijs, 1967.

ISAACS, I.M., *Character Theory of Finite Groups*, Academic Press, New York, 1976.

- Gedegen standaardwerken:

GORENSTEIN, D., *Finite Groups*, Harper & Row, New York, 1968.

HUPPERT, B., *Endliche Gruppen I*, Springer, Berlijn, 1967.

- Voor de algebraïsche benodigdheden kan men vele boeken raadplegen. We noemen er een paar bij wijze van voorbeeld.

LANG, S., *Algebra*, Addison-Wesley, Reading, 1965.

LANG, S., *Algebraic Numbers*, Addison-Wesley, Reading, 1964.

JACOBSON, N., *Lectures in Abstract Algebra*, van Nostrand, 1951.

SYMBOLEN

$\underline{n}$	$\{1,2,\ldots,n\}$
$\{\ldots.\}$	verzameling
$\cap$	doorsnede
$\cup$	vereniging
$\dot{\cup}$	disjunkte vereniging
$\in$	is element van
$\notin$	is geen element van
$\subseteq$	is deelverzameling van
$\not\subseteq$	is geen deelverzameling van
$\emptyset$	lege verzameling
X^Y	verzameling van funkties $f : X \to Y$
$\binom{X}{k}$	$\{Y \subseteq X \mid \lvert Y\rvert = k\}$
$\lvert X\rvert$ (#X)	kardinaliteit van X
$\forall$	al - kwantor
$\exists$	er is - kwantor
$\exists!$	er is precies één
$\wedge$	en
$\vee$	of
$\Rightarrow$	implikatie
$\mid_X$	restriktie tot X
$\mathbb{N}$	natuurlijke getallen
$\mathbb{Z}$	gehele getallen
$\mathbb{Q}$	rationale getallen
$\mathbb{R}$	reële getallen
$\mathbb{C}$	komplexe getallen
$\mathbb{F}_q$	(Galois)lichaam met q elementen
$\mathbb{Z}_n$	gehele getallen mod n
$\mathbb{Z}_n^*$	Opgave 1.1.6
$p \mid n$	p deelt n
$p \nmid n$	p is geen deler van n
kgv	kleinste gemene veelvoud
ggd	grootste gemene deler
$[x]$	entier van $x = \max\{n \in \mathbb{N} \mid n \leq x\}$
$\lvert z\rvert$	absolute waarde van z
cos	cosinus

sin	sinus
exp	exponentiele afbeelding, dus $\exp(x) = e^x$
$n!$	n fakulteit = 1.2.3...n
$\binom{n}{k}$	binomiaal-koëfficient
$p(n)$	1.5.4
$\sigma(n)$	1.5.4
mod	modulo
ϕ	Euler's ϕ-funktie
A^t	getransponeerde van de matrix A
$\underline{j}$	vektor met alle koordinaten gelijk 1
I (I_n)	(n×n) - eenheidsmatrix
J	matrix met alle koëfficienten gelijk 1
sp	spoor (4.2.1)
$\oplus$	4.1.2
$<\cdot\,|\,\cdot>$	inprodukt
dim V	dimensie van V
Kar(F)	karakteristiek van het lichaam F

$\sim$		3.4.1	$\Gamma(x)$		3.4.1
Aut(G)		3.4.1	$C(G,\Omega)$		3.4.4
T(n)		3.4.7	$P(q)$		3.4.10
$H \leq G$		1.1.3	$Gl_n(K)$		1.1.11
$H < G$		1.1.3	$SL_n(K)$		1.1.11
$H \trianglelefteq G$		1.5.7	$GL_n(p)$		1.1.11
$H \trianglelefteq G$		1.6.15	$SL_n(p)$		1.1.11
$H \cong G$		1.2.3	$AGL_n(K)$	Opgave	1.6.5
$N_G(H)$		1.5.7	$PSL_2(p)$	Opgave	1.6.13
$C_G(x)$		1.5.1	C_n		1.1.10
$C_G(H)$	Opgave	1.6.16	D_n		1.1.12
Z(G)		1.5.1	Q	Opgave	1.1.9
$Z_i(G)$		5.3.10	Q_n	Opgave	1.6.9
D(G)		1.6.11	Ker ϕ		1.2.3

INDEX

UITGAVEN IN DE SERIE MC SYLLABUS

Onderstaande uitgaven zijn verkrijgbaar bij het Mathematisch Centrum, 2e Boerhaavestraat 49 te Amsterdam-1005, tel. 020-947272.

MCS 1.1 F. GÖBEL & J. VAN DE LUNE, *Leergang Besliskunde, deel 1: Wiskundige basiskennis*, 1965. ISBN 90 6196 014 2.

MCS 1.2 J. HEMELRIJK & J. KRIENS, *Leergang Besliskunde, deel 2: Kansberekening*, 1965. ISBN 90 6196 015 0.

MCS 1.3 J. HEMELRIJK & J. KRIENS, *Leergang Besliskunde, deel 3: Statistiek*, 1966. ISBN 90 6196 016 9.

MCS 1.4 G. DE LEVE & W. MOLENAAR, *Leergang Besliskunde, deel 4: Markovketens en wachttijden*, 1966. ISBN 90 6196 017 7.

MCS 1.5 J. KRIENS & G. DE LEVE, *Leergang Besliskunde, deel 5: Inleiding tot de mathematische besliskunde*, 1966. ISBN 90 6196 018 5.

MCS 1.6a B. DORHOUT & J. KRIENS, *Leergang Besliskunde, deel 6a: Wiskundige programmering 1*, 1968. ISBN 90 6196 032 0.

MCS 1.6b B. DORHOUT, J. KRIENS & J.TH. VAN LIESHOUT, *Leergang Besliskunde, deel 6b: Wiskundige programmering 2*, 1977. ISBN 90 6196 150 5.

MCS 1.7a G. DE LEVE, *Leergang Besliskunde, deel 7a: Dynamische programmering 1*, 1968. ISBN 90 6196 033 9.

MCS 1.7b G. DE LEVE & H.C. TIJMS, *Leergang Besliskunde, deel 7b: Dynamische programmering 2*, 1970. ISBN 90 6196 055 X.

MCS 1.7c G. DE LEVE & H.C. TIJMS, *Leergang Besliskunde, deel 7c: Dynamische programmering 3*, 1971. ISBN 90 6196 066 5.

MCS 1.8 J. KRIENS, F. GÖBEL & W. MOLENAAR, *Leergang Besliskunde, deel 8: Minimaxmethode, netwerkplanning, simulatie*, 1968. ISBN 90 6196 034 7.

MCS 2.1 G.J.R. FÖRCH, P.J. VAN DER HOUWEN & R.P. VAN DE RIET, *Colloquium Stabiliteit van differentieschema's, deel 1*, 1967. ISBN 90 6196 023 1.

MCS 2.2 L. DEKKER, T.J. DEKKER, P.J. VAN DER HOUWEN & M.N. SPIJKER, *Colloquium Stabiliteit van differentieschema's, deel 2*, 1968. ISBN 90 6196 035 5.

MCS 3.1 H.A. LAUWERIER, *Randwaardeproblemen, deel 1*, 1967. ISBN 90 6196 024 X.

MCS 3.2 H.A. LAUWERIER, *Randwaardeproblemen, deel 2*, 1968. ISBN 90 6196 036 3.

MCS 3.3 H.A. LAUWERIER, *Randwaardeproblemen, deel 3*, 1968. ISBN 90 6196 043 6.

MCS 4 H.A. LAUWERIER, *Representaties van groepen*, 1968. ISBN 90 6196 037 1.

MCS 5 J.H. VAN LINT, J.J. SEIDEL & P.C. BAAYEN, *Colloquium Discrete wiskunde*, 1968.
ISBN 90 6196 044 4.

MCS 6 K.K. KOKSMA, *Cursus ALGOL 60*, 1969. ISBN 90 6196 045 2.

MCS 7.1 *Colloquium Moderne rekenmachines, deel 1*, 1969. ISBN 90 6196 046 0.

MCS 7.2 *Colloquium Moderne rekenmachines, deel 2*, 1969. ISBN 90 6196 047 9.

MCS 8 H. BAVINCK & J. GRASMAN, *Relaxatietrillingen*, 1969.
ISBN 90 6196 056 8.

MCS 9.1 T.M.T. COOLEN, G.J.R. FÖRCH, E.M. DE JAGER & H.G.J. PIJLS, *Elliptische differentiaalvergelijkingen, deel 1*, 1970.
ISBN 90 6196 048 7.

MCS 9.2 W.P. VAN DEN BRINK, T.M.T. COOLEN, B. DIJKHUIS, P.P.N. DE GROEN, P.J. VAN DER HOUWEN, E.M. DE JAGER, N.M. TEMME & R.J. DE VOGELAERE, *Colloquium Elliptische differentiaalvergelijkingen, deel 2*, 1970.
ISBN 90 6196 049 5.

MCS 10 J. FABIUS & W.R. VAN ZWET, *Grondbegrippen van de waarschijnlijkheidsrekening*, 1970. ISBN 90 6196 057 6.

MCS 11 H. BART, M.A. KAASHOEK, H.G.J. PIJLS, W.J. DE SCHIPPER & J. DE VRIES, *Colloquium Halfalgebra's en positieve operatoren*, 1971.
ISBN 90 6196 067 3.

MCS 12 T.J. DEKKER, *Numerieke algebra*, 1971. ISBN 90 6196 068 1.

MCS 13 F.E.J. KRUSEMAN ARETZ, *Programmeren voor rekenautomaten; De MC ALGOL 60 vertaler voor de EL X8*, 1971. ISBN 90 6196 069 X.

MCS 14 H. BAVINCK, W. GAUTSCHI & G.M. WILLEMS, *Colloquium Approximatietheorie*, 1971. ISBN 90 6196 070 3.

MCS 15.1 T.J. DEKKER, P.W. HEMKER & P.J. VAN DER HOUWEN, *Colloquium Stijve differentiaalvergelijkingen, deel 1*, 1972. ISBN 90 6196 078 9.

MCS 15.2 P.A. BEENTJES, K. DEKKER, H.C. HEMKER, S.P.N. VAN KAMPEN & G.M. WILLEMS, *Colloquium Stijve differentiaalvergelijkingen, deel 2*, 1973. ISBN 90 6196 079 7.

MCS 15.3 P.A. BEENTJES, K. DEKKER, P.W. HEMKER & M. VAN VELDHUIZEN, *Colloquium Stijve differentiaalvergelijkingen, deel 3*, 1975.
ISBN 90 6196 118 1.

MCS 16.1 L. GEURTS, *Cursus Programmeren, deel 1: De elementen van het programmeren*, 1973. ISBN 90 6196 080 0.

MCS 16.2 L. GEURTS, *Cursus Programmeren, deel 2: De programmeertaal ALGOL 60*, 1973. ISBN 90 6196 087 8.

MCS 17.1 P.S. STOBBE, *Lineaire algebra, deel 1*, 1974. ISBN 90 6196 090 8.

MCS 17.2 P.S. STOBBE, *Lineaire algebra, deel 2*, 1974. ISBN 90 6196 091 6.

MCS 17.3 N.M. TEMME, *Lineaire algebra , deel 3*, 1976. ISBN 90 6196 123 8.

MCS 18 F. VAN DER BLIJ, H. FREUDENTHAL, J.J. DE IONGH, J.J. SEIDEL & A. VAN WIJNGAARDEN, *Een kwart eeuw wiskunde 1946-1971, Syllabus van de Vakantiecursus 1971*, 1974. ISBN 90 6196 092 4.

MCS 19 A. HORDIJK, R. POTHARST & J.Th. RUNNENBURG, *Optimaal stoppen van Markovketens*, 1974. ISBN 90 6196 093 2.

MCS 20 T.M.T. COOLEN, P.W. HEMKER, P.J. VAN DER HOUWEN & E. SLAGT, *ALGOL 60 procedures voor begin- en randwaardeproblemen*, 1976. ISBN 90 6196 094 0.

MCS 21 J.W. DE BAKKER (red.), *Colloquium Programmacorrectheid*, 1975. ISBN 90 6196 103 3.

MCS 22 R. HELMERS, F.H. RUYMGAART, M.C.A. VAN ZUYLEN & J. OOSTERHOFF, *Asymptotische methoden in de toetsingstheorie; Toepassingen van naburigheid*, 1976. ISBN 90 6196 104 1.

MCS 23.1 J.W. DE ROEVER (red.), *Colloquium Onderwerpen uit de bicmathematica, deel 1*, 1976. ISBN 90 6196 105 X.

MCS 23.2 J.W. DE ROEVER (red.), *Colloquium Onderwerpen uit de biomathematica, deel 2*, 1976. ISBN 90 6196 115 7.

MCS 24.1 P.J. VAN DER HOUWEN, *Numerieke integratie van differentiaalvergelijkingen, deel 1: Eenstapsmethoden*, 1974. ISBN 90 6196 106 8.

MCS 25 *Colloquium Structuur van programmeertalen*, 1976. ISBN 90 6196 116 5.

MCS 26.1 N.M. TEMME (ed.), *Nonlinear analysis, volume 1*, 1976. ISBN 90 6196 117 3.

MCS 26.2 N.M. TEMME (ed.), *Nonlinear analysis, volume 2*, 1976. ISBN 90 6196 121 1.

MCS 27 M. BAKKER, P.W. HEMKER, P.J. VAN DER HOUWEN, S.J. POLAK & M. VAN VELDHUIZEN, *Colloquium Discretiseringsmethoden*, 1976. ISBN 90 6196 124 6.

MCS 28 O. DIEKMANN, N.M. TEMME (EDS), *Nonlinear Diffusion Problems*, 1976. ISBN 90 6196 126 2.

MCS 29.1 J.C.P. BUS (red.), *Colloquium Numerieke programmatuur, deel 1A, deel 1B*, 1976. ISBN 90 6196 128 9.

MCS 29.2 H.J.J. TE RIELE (red.), *Colloquium Numerieke programmatuur, deel 2*, 1976. ISBN 144 0.

* MCS 30 P. GROENEBOOM, R. HELMERS, J. OOSTERHOFF & R. POTHARST, *Efficiency begrippen in de statistiek*, . ISBN 90 6196 149 1.

MCS 31 J.H. VAN LINT (red.), *Inleiding in de coderingstheorie*, 1976. ISBN 90 6196 136 X.

MCS 32 L. GEURTS (red.), *Colloquium Bedrijfssystemen*, 1976. ISBN 90 6196 137 8.

MCS 33 P.J. VAN DER HOUWEN, *Differentieschema's voor de berekening van waterstanden in zeeën en rivieren*, 1977. ISBN 90 6196 138 6.

MCS 34 J. HEMELRIJK, *Oriënterende cursus mathematische statistiek*, ISBN 90 6196 139 4.

MCS 35 P.J.W. TEN HAGEN (red.), *Colloquium Computer Graphics*, 1977. ISBN 90 6196 142 4.

MCS 36 J.M. AARTS, J. DE VRIES, *Colloquium Topologische Dynamische Systemen*, 1977. ISBN 90 6196 143 2.

MCS 37 J.C. van Vliet (red.), *Colloquium Capita Datastructuren*, 1978. ISBN 90 6196 159 9.

MCS 38.1 T.H. KOORNWINDER (ED.), *Representations of locally compact groups with applications*, 1979. ISBN 90 6196 161 0.

MCS 38.2 T.H. KOORNWINDER (ED.), *Representations of locally compact groups with applications*, 1979. ISBN 90 6196 181 5.

MCS 39 O.J. VRIEZE & G.L. WANROOY, *Colloquium Stochastische Spelen*, 1978. ISBN 90 6196 167 X.

MCS 40 J. VAN TIEL, *Convexe Analyse*, 1979. ISBN 90 6196 187 4.

MCS 41 H.J.J. TE RIELE (ED.), *Colloquium Numerical Treatment of Integral Equations*, 1979. ISBN 90 6196 189 0.

MCS 42 J.C. VAN VLIET (RED.), *Colloquium Capita Implementatie van Programmeertalen*, 1980. ISBN 90 6196 191 2.

MCS 43 A.M. COHEN & H.A. WILBRINK, *Eindige groepen (Een inleidende cursus)*, 1980. ISBN 90 6196 203 X

MCS 44 J.G. VERWER (ED.), *Numerical solution of partial differential equations*, 1980. ISBN 90 6196 205 6.

MCS 45 P. KLINT (red.), *Colloquium hogere programmeertalen en computerarchitectuur*, 1980. ISBN 90 6196 206 4.

De met een * gemerkte uitgaven moeten nog verschijnen.