Inhoudsopgave

1 De gehele getallen

In dit hoofdstuk houden we ons bezig met de verzameling van alle gehele getallen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$. Veel elementaire eigenschappen daarvan zijn ons welbekend uit het lager– en middelbaar onderwijs. Wat daar evenwel in de meeste gevallen *niet* gedaan wordt, is zulke eigenschappen ook echt bewijzen. Dat doen we hier wel, en in latere hoofdstukken zal blijken hoe dat weer te gebruiken is voor bijvoorbeeld een beter begrip van het rekenen met resten bij deling door een vast getal. Dat laatste kan dan op zijn beurt gebruikt worden voor bijvoorbeeld het vinden van criteria die zeggen of een gegeven groot getal een priemgetal is of niet. En zo zullen we hier en in verdere hoofdstukken veel meer voorbeelden zien van soms vrij abstracte definities en bewijzen, die later in concrete situaties heel goed toepasbaar blijken te zijn.

1.1 Deling (met rest)

Al op de lagere school komen we sommen als $100 : 7 = 14$ rest 2 tegen. Achter dit soort opgaven ligt het volgende.

Stelling 1.1.1 *(Deling met rest.) Laat $a, b \in \mathbb{Z}$ met $b > 0$. Dan bestaan er $q, r \in \mathbb{Z}$ waarvoor*

$$a = qb + r \quad en \quad 0 \leq r < b.$$

Bovendien zijn deze q, r uniek.

Bewijs. We tonen eerst het bestaan van zulke $q, r \in \mathbb{Z}$ aan. Voor niet-negatieve a kan dat bijvoorbeeld met volledige inductie: is $a = 0$ dan kunnen we $q = r = 0$ nemen. Weten we dat $a - 1 \geq 0$ te schrijven is als $a - 1 = \tilde{q}b + \tilde{r}$ met $0 \leq \tilde{r} < b$, dan volgt $a = \tilde{q}b + \tilde{r} + 1$. Er geldt uiteraard $0 \leq \tilde{r} + 1 \leq b$. In het geval $\tilde{r} + 1 < b$ kunnen we dus $q = \tilde{q}$ en $r = \tilde{r} + 1$ nemen. In het resterende geval $\tilde{r} + 1 = b$ hebben we $a = \tilde{q}b + \tilde{r} + 1 = \tilde{q}b + b = (\tilde{q} + 1)b + 0$, dus $q = \tilde{q} + 1$ en $r = 0$ voldoen. Hiermee is volgens het principe van volledige inductie voor $a \geq 0$ de existentie van q, r aangetoond.

Is $a < 0$, dan is $-a > 0$, dus uit wat we zojuist bewezen hebben volgt dat er q', r' zijn met $-a = q'b + r'$ en $0 \leq r' < b$. Dan is $a = (-q')b - r' = (-q' - 1)b + (b - r')$, dus we concluderen dat $q = -q'$ en $r = 0$ voldoen in het geval dat $r' = 0$, en als $r' \neq 0$ dan kunnen we $q = -q' - 1$ en $r = b - r'$ nemen.

Nu nog de uniciteit. Stel dat $a = q_1 b + r_1 = q_2 b + r_2$ waarbij $0 \leq r_1 \leq r_2 < b$. Dan volgt $0 \leq r_2 - r_1 \leq r_2 < b$, maar ook $r_2 - r_1 = b(q_1 - q_2)$. Dus moet $r_1 = r_2$, want anders zou het een positief veelvoud van b zijn en we

hebben al gezien dat $r_2 - r_1 < b$. We concluderen dat ook $b(q_1 - q_2) = 0$, en omdat $b \neq 0$ impliceert dit $q_1 = q_2$. Hiermee is de stelling bewezen. □

Opmerking 1.1.2 Als we wat kennis over reële getallen gebruiken, dan kan een heel ander bewijs gegeven worden: deel de reële lijn op in intervallen met lengte b, dus

$$\mathbb{R} = \ldots \cup [-2b, -b) \cup [-b, 0) \cup [0, b) \cup \ldots\ldots$$

Het getal $a \in \mathbb{R}$ ligt dan in één zo'n interval $[qb, (q+1)b)$, en is dus te schrijven als $a = qb + r$ waarin $0 \leq r < b$.

Definitie 1.1.3 Laat $a, b \in \mathbb{Z}$. We zeggen dat a het getal b *deelt*, als er een $q \in \mathbb{Z}$ bestaat waarvoor geldt $b = qa$. Dit noteren we als $a|b$. Bestaat zo'n q niet, dan schrijven we $a \not| b$ (en we zeggen: a deelt b *niet*).

In plaats van a deelt b wordt ook wel gezegd dat a een *deler* van b is, of dat b een *veelvoud* van a is, of dat b *deelbaar* is door a. Bijvoorbeeld geldt $17|-153$ en $0|0$ en $-2 \not| 101$ en $0 \not| 3$.

We geven een aantal eenvoudige eigenschappen van deelbaarheid.

Propositie 1.1.4 *Voor $a, b, c \in \mathbb{Z}$ geldt*

1. *Als $a|b$ en $b|c$ dan ook $a|c$.*
2. *Als $a|b$ en $a|c$ dan ook $a|b \pm c$.*
3. *$a|0$ en $1|a$.*
4. *$0|a$ dan en slechts dan als $a = 0$.*
5. *Als voor $b \neq 0$ geldt dat $a|b$, dan is $|a| \leq |b|$.*

Bewijs. Al deze eigenschappen volgen direct uit de definitie. Bijvoorbeeld impliceert $a|b$ en $a|c$ dat er $p, q \in \mathbb{Z}$ bestaan waarvoor $b = pa$ en $c = qa$, en daaruit volgt dat $b \pm c = pa \pm qa = (p \pm q)a$, met andere woorden $a|b \pm c$. □

Uit de laatste in Propositie 1.1.4 genoemde eigenschap volgt, dat een geheel getal $a \neq 0$ slechts eindig veel delers heeft; de grootste daarvan is uiteraard $|a|$. Hebben we nog een getal, zeg b, dan hebben dus in het bijzonder a en b slechts eindig veel delers gemeenschappelijk (twee van die gemeenschappelijke delers zijn natuurlijk 1 en -1). Iets dergelijks geldt wanneer we kijken naar gemeenschappelijke veelvouden van twee gehele getallen a, b. Als a of b nul is, dan volgt uit de vierde in Propositie 1.1.4 gegeven eigenschap dat 0 het enige gemeenschappelijke veelvoud is. Geldt daarentegen $ab \neq 0$, dan hebben a en b gemeenschappelijke positieve veelvouden, bijvoorbeeld $|ab|$. Dit leidt tot de volgende definitie:

Definitie 1.1.5 Laat $a, b \in \mathbb{Z}$. Als a en b niet allebei gelijk aan 0 zijn, dan wordt de *grootste gemene deler* van a en b gedefiniëerd als het grootste getal dat zowel een deler van a als van b is. Dit wordt genoteerd als $\text{ggd}(a, b)$. Verder spreken we af dat $\text{ggd}(0, 0) = 0$.

Het *kleinste gemene veelvoud*, notatie $\text{kgv}(a, b)$ van a en b is per definitie 0 als $ab = 0$, en het is het kleinste positieve getal k met de eigenschap $a|k$ en $b|k$ als zowel a als b ongelijk aan nul zijn.

Twee getallen a, b noemen we *relatief priem* of ook wel *onderling ondeelbaar* als $\text{ggd}(a, b) = 1$.

Voorbeeld 1.1.6 Er geldt $\text{ggd}(a, b) = \text{ggd}(b, a)$ en $\text{ggd}(a, 0) = |a|$. Omdat de delers van a en die van $|a|$ dezelfde zijn, geldt ook $\text{ggd}(a, b) = \text{ggd}(|a|, b) = \text{ggd}(a, |b|) = \text{ggd}(|a|, |b|)$. Het is in het algemeen lastig om met behulp van de definitie grootste gemene delers uit te rekenen. Probeer bijvoorbeeld maar eens na te gaan dat $\text{ggd}(35581, 46189) = 221$.

Dergelijke voorbeelden voor kgv zijn eenvoudig zelf te maken; bijvoorbeeld komen we ze tegen op de lagere school bij het gelijknamig maken van breuken. In de rest van deze paragraaf houden we ons alleen met de ggd bezig; in Sectie 1.2 komen we dan op het begrip kgv terug.

Er blijkt een verrassend eenvoudig en efficiënt algoritme te bestaan voor het bepalen van $\text{ggd}(a, b)$. Dit is afkomstig van de Griekse wiskundige Euclides die rond 300 B.C. leefde. Het algoritme werkt als volgt.

Stelling 1.1.7 *(Het Euclidische algoritme.) Het volgende algoritme bepaalt in eindig veel stappen de grootste gemene deler van twee getallen a, b:*

```
ggd:=proc(a::integer,b::integer)::integer;
        local rn,ro,hulp;
        ro:=max(abs(a),abs(b)); rn:=min(abs(a),abs(b));
        while rn<>0 do
            do hulp:=ro; ro:=rn; rn:=hulp mod rn end do;
        return ro
    end proc;
```

Bewijs. Om te begrijpen wat dit programma doet, gaan we na wat er in de 'while-loop' gebeurt. Telkens wordt het paar getallen (ro, rn) vervangen door (rn, ro mod rn). Zoals bekend is ro mod rn precies de rest die overblijft wanneer we ro door rn delen. (NB. pas overigens op: in veel programmeertalen is voor *negatieve* a de uitkomst van a mod b *niet* de rest r zoals die in Stelling 1.1.1 gegeven wordt, maar juist $r - |b|$. Bovenstaande code is geschreven in Maple; daar doet dit probleem zich niet voor.) In het bijzonder geldt dus

dat steeds aan het begin van de 'loop' geldt ro, rn ≥ 0, en iedere keer dat deze doorlopen wordt, wordt rn strikt kleiner. Dus termineert het programma. Om te laten zien dat met het programma ook inderdaad de grootste gemene deler van a en b wordt berekend, zullen we nagaan dat bovendien bij het ingaan van de 'loop' steeds geldt $\text{ggd}(\text{ro}, \text{rn}) = \text{ggd}(a, b)$. In Lemma 1.1.8 hierna wordt dat gedaan. Is dit bewezen, dan volgt dat wanneer de 'loop' voor het laatst doorlopen is dat $\text{rn} = 0$ en $\text{ggd}(a, b) = \text{ggd}(\text{ro}, \text{rn}) = \text{ggd}(\text{ro}, 0) = \text{ro}$, met andere woorden het algoritme levert inderdaad de grootste gemene deler van a en b op. □

Lemma 1.1.8 *Voor $a, b, q, r \in \mathbb{Z}$ met $a = qb + r$ geldt $ggd(a, b) = ggd(b, r)$.*

Bewijs. We zullen laten zien dat de verzameling gemeenschappelijke delers van a en b dezelfde zijn als die van b en r. Uit de definitie van grootste gemene deler volgt dan het lemma.

Geldt $d|a$ en $d|b$, dan ook $d|a - qb = r$. Dus gemeenschappelijke delers van a en b zijn ook gemeenschappelijke delers van b en r.

Omgekeerd, als $d|b$ en $d|r$, dan ook $d|qb + r = a$. Dus zijn de delers van zowel b als r ook gemeenschappelijke delers van a en b. Hiermee is het lemma bewezen. □

Voorbeeld 1.1.9

$$\begin{array}{lll} \text{ggd}(1057, 315) & = \text{ggd}(3 \cdot 315 + 112, 315) & = \\ & = \text{ggd}(315, 112) & = \text{ggd}(2 \cdot 112 + 91, 112) = \\ & = \text{ggd}(112, 91) & = \text{ggd}(91 + 21, 91) = \\ & = \text{ggd}(91, 21) & = \text{ggd}(4 \cdot 21 + 7, 21) = \\ & = \text{ggd}(21, 7) & = \text{ggd}(7, 0) = 7. \end{array}$$

We zullen nu nagaan hoe efficient het Euclidische algoritme is.

Stelling 1.1.10 *(G. Lamé, 1844, Frans wiskundige.) Is $a > b > 0$, dan is het aantal delingen met rest in het Euclidische algoritme voor het bepalen van $ggd(a, b)$ hoogstens gelijk aan 5 maal het aantal cijfers van b (in het gewone tientallig stelsel).*

Bewijs. Schrijf $r_0 = a$ en $r_1 = b$. In het algoritme wordt dan achtereenvolgend uitgerekend

$$\begin{array}{lcll} r_0 & = & q_0 r_1 + r_2 & (0 < r_2 < r_1) \\ r_1 & = & q_1 r_2 + r_3 & (0 < r_3 < r_2) \\ r_2 & = & q_2 r_3 + r_4 & (0 < r_4 < r_3) \\ & & \vdots & \\ r_{n-2} & = & q_{n-2} r_{n-1} + r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} & = & q_{n-1} r_n + 0. & \end{array}$$

Het aantal delingen met rest is dus precies n.

Om een schatting voor n te vinden maken we gebruik van de zogeheten Fibonacci rij $(f_i)_{i\geq 0}$, die gedefiniëerd wordt door $f_0 = f_1 = 1$ en $f_{i+2} = f_{i+1} + f_i$ voor $i \geq 0$. Dus dit is de rij $1, 1, 2, 3, 5, 8, 13, 21, \ldots\ldots$.

Omdat $0 < r_n < r_{n-1}$, volgt dat $q_{n-1} > 1$ en dus $r_{n-1} \geq 2r_n \geq f_2$. Met het principe van volledige inductie volgt zo voor iedere i met $1 \leq i \leq n-1$ dat $r_{n-i} \geq f_{i+1}$. Voor $i = 1$ hebben we dit namelijk zojuist aangetoond. Is $i > 1$ en weten we deze ongelijkheid al voor $1 \leq j < i$, dan volgt $r_{n-i} = q_{n-i}r_{n-(i-1)} + r_{n-(i-2)} \geq r_{n-(i-1)} + r_{n-(i-2)} \geq f_i + f_{i-1} = f_{i+1}$.

In het bijzonder blijkt hieruit dat $b = r_1 \geq f_n$.

Om het bewijs te voltooien, laten we zien dat $f_{5i+1} > 10^i$ voor $i \geq 1$. Voor $i = 1$ klopt dit, want $f_6 = 13 > 10$. Is het juist voor $i \geq 1$, dan volgt $f_{5(i+1)+1} = f_{5i+6} = f_{5i+5} + f_{5i+4} = f_{5i+4} + 2f_{5i+3} + f_{5i+2} = f_{5i+3} + 3f_{5i+2} + 3f_{5i+1} + f_{5i} = f_{5i+2} + 7f_{5i+1} + 4f_{5i} = 8f_{5i+1} + 5f_{5i} > 8f_{5i+1} + 2f_{5i} + 2f_{5i-1} = 10f_{5i+1} > 10 \cdot 10^i = 10^{i+1}$.

Schrijf nu $n = 5m + k$ met $1 \leq k \leq 5$. Dan volgt dat $b \geq f_n \geq f_{5m+1} > 10^m$. Met andere woorden, het aantal cijfers van b is minstens gelijk aan $m+1 \geq n/5$, oftewel n is kleiner dan of gelijk aan 5 maal het aantal decimale cijfers van b, hetgeen we wilden bewijzen. □

Een toepassing van het Euclidische algoritme die verderop bij het 'rekenen modulo N' van groot belang zal blijken, is dat we er oplossingen in gehele getallen van bepaalde lineaire vergelijkingen mee kunnen vinden:

Stelling 1.1.11 *(Bachet-Bézout; vernoemd naar de Franse wiskundigen Claude Gaspard Bachet 1581–1638 en Étienne Bézout 1730–1783.) Voor $a, b \in \mathbb{Z}$ bestaan er $x, y \in \mathbb{Z}$ met $ax + by = ggd(a, b)$.*

Bewijs. Dit volgt direct uit de definitie van ggd in het geval dat $ab = 0$. We nemen nu aan $a \neq 0 \neq b$. Schrijf $r_0 = |a|$ en $r_1 = |b|$. Als het Euclidisch algoritme precies n delingen met rest uitvoert, dan levert dit een rij

$$\begin{array}{lcll} r_0 & = & q_0 r_1 + r_2 & (0 < r_2 < r_1) \\ r_1 & = & q_1 r_2 + r_3 & (0 < r_3 < r_2) \\ r_2 & = & q_2 r_3 + r_4 & (0 < r_4 < r_3) \\ & & \vdots & \\ r_{n-2} & = & q_{n-2} r_{n-1} + r_n & (0 < r_n < r_{n-1}) \\ r_{n-1} & = & q_{n-1} r_n + 0 & \end{array}$$

zoals we in het voorgaande bewijs al gebruikt hebben. De voorlaatste gelijkheid hier geeft $r_n = \text{ggd}(a, b)$ als gehele lineaire combinatie van r_{n-1} en r_{n-2}. Met behulp van de gelijkheid daarboven kunnen we r_{n-1} hierin schrijven als

combinatie van r_{n-2} en r_{n-3}, dus dat levert een schrijfwijze van $\text{ggd}(a,b)$ op als gehele lineaire combinatie van r_{n-2} en r_{n-3}. Zo verder naar boven werkend elimineren we achtereenvolgens $r_{n-2}, r_{n-3}, \ldots, r_3, r_2$. Wat overblijft is een relatie $\text{ggd}(a,b) = xr_1 + yr_0$, en door eventueel hierin x en/of y van teken te wisselen geeft dit een gelijkheid $ax + by = \text{ggd}(a,b)$, zoals verlangd. □

Het bovenstaand bewijs is volledig constructief, zoals blijkt uit het volgende algoritme waarmee tegelijk de grootste gemene deler van $a, b \in \mathbb{Z}$ gevonden wordt, en x, y berekend wordt waarvoor $ax + by = \text{ggd}(a,b)$. In feite is dit algoritme niet gebaseerd op het van beneden naar boven doorlopen van de hiervoor gegeven rij gelijkheden voor de r_i's, maar juist van boven naar beneden. Er wordt namelijk bij iedere nieuw berekende r_i meteen $x_i, y_i \in \mathbb{Z}$ gevonden waarvoor $x_i a + y_i b = r_i$. De in de n-de stap gevonden x_n, y_n zijn dan de gevraagde x, y. Ga zelf na dat het algoritme inderdaad werkt.

```
# Hier gaan we ggd(a,b) vinden, en schrijven als xa+yb.
if a=0
then x:=0; y:=1; ggd:=abs(b)
else if b=0
    then x:=1; y:=0; ggd:=abs(a)
    else # a en b zijn nu beide niet 0
        ro:=abs(a); xo:=sign(a); yo:=0;
        rn:=abs(b); x:=0; y:=sign(b);
        while rn<>0
            do
               q:=floor(ro/rn); hulp:=rn; rn:=ro-q*rn; ro:=hulp;
               hulp:=x; x:=xo-q*x; xo:=hulp;
               hulp:=y; y:=yo-q*y; yo:=hulp
            end do;
        ggd:=ro; x:=xo; y:=yo
    end if
end if; print(ggd,x,y);
```

Voorbeeld 1.1.12 In Voorbeeld 1.1.9 zagen we dat $\text{ggd}(1057, 315) = 7$. We construeren nu volgens bovenstaand algoritme gehele getallen x, y waarvoor $1057x + 315y = 7$. Beschouw daartoe de volgende gelijkheden:

$$\begin{aligned}
1 \cdot 1057 &+ 0 \cdot 315 = 1057 \\
0 \cdot 1057 &+ 1 \cdot 315 = 315 \quad \text{(deze 3 keer van de vorige af:)} \\
1 \cdot 1057 &+ -3 \cdot 315 = 112 \quad \text{(deze 2 keer van de vorige af:)} \\
-2 \cdot 1057 &+ 7 \cdot 315 = 91 \quad \text{(deze 1 keer van de vorige af:)} \\
3 \cdot 1057 &+ -10 \cdot 315 = 21 \quad \text{(deze 4 keer van de vorige af:)} \\
-14 \cdot 1057 &+ 47 \cdot 315 = 7.
\end{aligned}$$

De hier gevonden oplossing is zeker niet de enige. Is bijvoorbeeld ook (x', y') een oplossing, dan geldt met betrekking tot het standaardinproduct op $\mathbb{R}^2$ dat $\langle \begin{pmatrix} 1057 \\ 315 \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \rangle = 7 = \langle \begin{pmatrix} 1057 \\ 315 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \rangle$, en dus staat de vector $\begin{pmatrix} x - x' \\ y - y' \end{pmatrix}$ loodrecht op $\begin{pmatrix} 1057 \\ 315 \end{pmatrix}$. Hiermee zijn eenvoudig alle geheeltallige oplossingen van $1057x + 315y = 7$ te vinden.

Met behulp van het bestaan van getallen $x, y \in \mathbb{Z}$ waarvoor geldt $ax+by = \text{ggd}(a, b)$ zijn gemakkelijk een paar verdere resultaten af te leiden:

Gevolg 1.1.13 *Laat $a, b \in \mathbb{Z}$ en $d = ggd(a, b)$. Elk getal dat zowel a als b deelt is ook een deler van d, en omgekeerd is elke deler van d een gemeenschappelijke deler van a en b.*

Bewijs. Omdat d zowel a als b deelt, volgt uit de eerste eigenschap in Propositie 1.1.4 dat iedere deler van d dat ook doet.

Omgekeerd, schrijf $d = ax + by$ voor zekere $x, y \in \mathbb{Z}$. Als $c|a$ en $c|b$ dan ook $c|ax + by = d$. Dit bewijst het gevolg. □

Gevolg 1.1.14 *Laat $a, b \in \mathbb{Z}$. Dan zijn a, b onderling ondeelbaar precies dan als er $x, y \in \mathbb{Z}$ bestaan waarvoor geldt $ax + by = 1$.*

Bewijs. Zijn a, b onderling ondeelbaar, dan houdt dat per definitie in dat $\text{ggd}(a, b) = 1$. Uit Stelling 1.1.11 volgt dan het bestaan van $x, y \in \mathbb{Z}$ met $ax + by = 1$.

Omgekeerd, als $ax + by = 1$ voor zekere $x, y \in \mathbb{Z}$ en $d = \text{ggd}(a, b)$, dan $d|a$ en $d|b$, dus $d|ax + by = 1$, dus $d = 1$. □

Gevolg 1.1.15 *Voor $a, b, c \in \mathbb{Z}$ met $ggd(a, b) = 1$ geldt: als $a|bc$, dan $a|c$.*

Bewijs. Neem $x, y \in \mathbb{Z}$ met $ax + by = 1$. Als $a|bc$, dan ook $a|axc + byc = (ax + by)c = c$. □

1.2 Priemfactorontbinding

Definitie 1.2.1 Een *priemgetal* is een geheel getal groter dan 1, dat alleen 1 en zichzelf als positieve delers heeft.

Voorbeeld 1.2.2 Kleine priemgetallen als $2, 3, 5, \ldots$ zijn welbekend. Voor grotere getallen is het heel lastig om na te gaan of het priemgetallen zijn. Zo weten we bijvoorbeeld dat $2^{524288} + 1$ *geen* priemgetal is, en $2^{859433} -$

1 is er *wel* één, en $2^{1048576}+1$ weer niet. Dit zijn getallen die decimaal uitgeschreven uit resp. 157827, 258716 en 315653 cijfers bestaan. Van het eerstgenoemde grote getal (de exponent van 2 is precies 2^{19}) vond in 1962 de Zweedse wiskundige Hans Riesel een deler, namelijk $33629 \cdot 2^{21}+1$. Voor het tweede getal (de exponent 859433 is zelf een priemgetal) werd in januari 1994 door twee Amerikanen, David Slowinski en Paul Gage, bewezen dat het een priemgetal is. Momenteel (februari 2012) kennen we nog veel grotere priemgetallen, bijvoorbeeld $2^{43112609}-1$, een getal van maar liefst 12978189 decimale cijfers, in 2008 gevonden door Edson Smith, een systeembeheerder van de universiteit van Californië in Los Angeles (UCLA). Van het derde getal (de exponent is, net als voor het eerste, een macht van 2, namelijk 2^{20}) werd in 1987 door de Amerikanen Jeff Young en Duncan Buell bewezen dat het geen priemgetal is. Echter, tot nu toe heeft nog niemand een deler van dit getal gevonden. Het kleinste getal van de vorm $1+2^m$ waarvoor op dit moment nog niet bekend is of het een priemgetal is, is dat met $m = 2^{22}$.

Stelling 1.2.3 *Is p een priemgetal, en zijn $a, b \in \mathbb{Z}$ getallen zodat $p|ab$, dan $p|a$ of $p|b$.*

Bewijs. Noem $d = \text{ggd}(a,p)$. Omdat $p \neq 0$ is, geldt dat d positief is. Bovendien is het een deler van p. Uit de definitie van priemgetal volgt nu dat $d = 1$ of $d = p$. In het eerste geval levert dan Gevolg 1.1.15 dat $p|b$. In het tweede geval geldt $p = d|a$. □

Gevolg 1.2.4 *Is p een priemgetal, en zijn $a_1, \ldots, a_n$ gehele getallen zodat $p|a_1a_2 \cdot \ldots \cdot a_n$, dan is er een index k met $1 \leq k \leq n$ zodat $p|a_k$.*

Bewijs. Dit kan met volledige inductie naar n bewezen worden. Voor $n = 1$ is er niets te bewijzen (en voor $n = 2$ hebben we zojuist in Stelling 1.2.3 dit bewezen). Neem aan dat $n \geq 3$ en dat we het gevraagde voor een product van $< n$ factoren al weten. Als $p|a_1a_2 \cdot \ldots \cdot a_n = (a_1) \cdot (a_2 \cdot \ldots \cdot a_n)$, dan volgt uit Stelling 1.2.3 dat $p|a_1$ of $p|a_2 \cdot \ldots \cdot a_n$. In het eerste geval zijn we direct klaar, en in het tweede geval vanwege onze inductiehypothese ook. □

Met behulp van bovenstaande eigenschappen van priemgetallen kan een resultaat bewezen worden dat wel de 'hoofdstelling van de rekenkunde' wordt genoemd:

Stelling 1.2.5 *(unieke priemfactorisatie) Ieder geheel getal groter dan 1 is, op de volgorde van de factoren na, op precies één manier te schrijven als een product van priemgetallen.*

Bewijs. Eerst tonen we aan dat iedere $n \in \mathbb{Z}$ met $n > 1$ als product van priemgetallen te schrijven is. Dit gaat met inductie naar n: het geval $n = 2$ is duidelijk. Stel $n > 2$ en neem aan dat elk getal groter dan 1 en kleiner dan n als product van priemgetallen te schrijven is. Is n een priemgetal, dan zijn we klaar. Zoniet, dan is $n = n_1 n_2$, met $1 < n_1, n_2 < n$. Uit de inductiehypothese volgt dat zowel n_1 als n_2 als product van priemgetallen te schrijven zijn, en dus is n dat ook.

Vervolgens tonen we de uniciteit van deze schrijfwijze aan. Stel dat de schrijfwijze *niet* uniek is. Neem n het kleinste getal > 1 dat meerdere factorisaties heeft, zeg

$$n = p_1 p_2 \cdot \ldots \cdot p_t = q_1 q_2 \cdot \ldots \cdot q_s,$$

voor priemgetallen p_i, q_j zijn twee verschillende factorisaties. Dan geldt $p_1 | n = q_1 q_2 \cdot \ldots \cdot q_s$. Omdat n meerdere factorisaties heeft, kan n zelf geen priemgetal zijn, dus $s, t > 1$ en in het bijzonder $n/p_1 > 1$. Uit Gevolg 1.2.4 blijkt dat $p_1 | q_k$ voor zekere k. Omdat q_k een priemgetal is, concluderen we dat $p_1 = q_k$. Delen we de beide gegeven factorisaties door hun gemeenschappelijke factor $p_1 = q_k$, dan blijkt dat ook n/p_1 twee verschillende factorisaties heeft. Dit is in tegenspraak met de minimaliteit van n. Hiermee is dus de stelling bewezen. □

Hoewel we in Voorbeeld 1.2.2 al zagen dat het vinden van grote priemgetallen lastig is, is toch de volgende stelling al heel oud.

Stelling 1.2.6 *(Euclides) Er bestaan oneindig veel priemgetallen.*

Bewijs. Stel we hebben $n \geq 1$ onderling verschillende priemgetallen $p_1, \ldots, p_n$. Bezie het getal $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Kies een priemgetal q uit de priemfactorisatie van N. Dan is q verschillend van elke p_i, want anders zou q zowel N als $N - 1 = p_1 \cdot \ldots \cdot p_n$ delen, en dus ook het verschil $N - (N - 1) = 1$ hetgeen onmogelijk is. We concluderen dus uit het bestaan van n priemgetallen, dat er ook $n + 1$ priemgetallen bestaan. Hieruit volgt de stelling. □

Opmerking 1.2.7 Het is *niet* het geval dat de N in het bewijs van Stelling 1.2.6 zelf noodzakelijkerwijs een priemgetal is. Bijvoorbeeld is voor een eindige verzameling *oneven* priemgetallen hun product plus 1 altijd even. En beginnen we bijvoorbeeld bij de verzameling $\{2\}$, dan levert herhaaldelijk 1 plus het product van alle gegeven priemgetallen nemen achtereenvolgend $2, 3, 7, 43, 1807$ op. Dit laatste getal is deelbaar door 13.

Definitie 1.2.8 Is p een priemgetal en $a \in \mathbb{Z}$ ongelijk aan 0 of ± 1, dan schrijven we $v_p(a)$ voor het aantal keren dat p voorkomt in de priemfactorisatie van $|a|$. Verder schrijven we $v_p(1) = v_p(-1) = 0$ en $v_p(0) = \infty$.

Het getal $v_p(a)$ wordt wel de *valuatie* of ook wel de *orde* van a bij p genoemd. Omdat de priemfactorisatie op volgorde na uniek is, is $v_p(a)$ goed gedefiniëerd. Is $a \in \mathbb{Z}$ niet nul, dan volgt uit de definitie dat $|a| = \prod p^{v_p(a)}$. Hier nemen we het product over *alle* priemgetallen p, en hoewel dat er blijkens Stelling 1.2.6 oneindig veel zijn, is dit product toch goed gedefiniëerd. Er geldt namelijk dat slechts eindig veel priemgetallen voorkomen in de priemfactorisatie van $|a|$. Voor alle overige is $v_p(a) = 0$ en dus $p^{v_p(a)} = 1$.

Gevolg 1.2.9 *Laat a, b gehele getallen zijn.*

1. *Voor elk priemgetal p is $v_p(ab) = v_p(a) + v_p(b)$.*
2. *$a|b$ dan en slechts dan als voor ieder priemgetal p geldt $v_p(a) \leq v_p(b)$.*
3. *Als a en b niet allebei nul zijn, dan is*
$$ggd(a, b) = \prod_{p\ priem} p^{min\{v_p(a), v_p(b)\}}.$$
4. *Als $a \neq 0$ én $b \neq 0$, dan is*
$$kgv(a, b) = \prod_{p\ priem} p^{max\{v_p(a), v_p(b)\}}.$$
5. *Als $a|c$ en $b|c$, dan $kgv(a, b)|c$.*
6. *$ggd(a, b) \cdot kgv(a, b) = |ab|$.*

Bewijs. 1: De uitspraak is waar indien a en/of b nul is, want oneindig plus oneindig en ook oneindig plus een geheel getal is weer oneindig. Het resterende geval volgt uit de gelijkheid
$$|ab| = |a| \cdot |b| = \prod_p p^{v_p(a)} \cdot \prod_p p^{v_p(b)} = \prod_p p^{v_p(a)+v_p(b)}.$$
2: Als $a|b$, dan $b = qa$ voor een $q \in \mathbb{Z}$, en uit wat zojuist bewezen is volgt dan $v_p(a) \leq v_p(a) + v_p(q) = v_p(qa) = v_p(b)$, voor ieder priemgetal p.

Omgekeerd, als voor ieder priemgetal p geldt $v_p(a) \leq v_p(b)$, dan geldt zeker $a|b$ in het geval $b = 0$. In het geval $a = 0$ volgt dat $v_p(b) = \infty$, dus $b = 0$, dus opnieuw $a|b$. Zijn zowel a als b ongelijk aan nul, dan is $q = \prod_p p^{v_p(b)-v_p(a)}$ een goed gedefiniëerd geheel getal. Per definitie hebben $|b|$ en $|qa|$ dezelfde priemfactorisatie, dus $b = \pm qa$, met andere woorden $a|b$.
3: Uit wat zojuist bewezen is volgt dat de getallen d die zowel a als b delen, precies die getallen met de eigenschap $v_p(d) \leq v_p(a)$ én $v_p(d) \leq v_p(b)$

voor elk priemgetal p. Omdat $a \neq 0$ of $b \neq 0$, is $\min\{v_p(a), v_p(b)\}$ eindig voor ieder priemgetal, en ongelijk aan nul voor slechts eindig veel p's. Dus $\prod_p p^{\min\{v_p(a),v_p(b)\}}$ is een goed gedefiniëerd getal, dat zowel a als b deelt en bovendien minstens zo groot is als iedere andere gemeenschappelijke deler. Dus is dit $\text{ggd}(a, b)$.
4: a en b zijn beide niet nul, dus voor elk priemgetal p zijn $v_p(a)$ en $v_p(b)$ eindig terwijl deze getallen voor slechts eindig veel p's $\neq 0$ zijn. Dus is $k = \prod_p p^{\max\{v_p(a),v_p(b)\}}$ welgedefiniëerd en positief, en vanwege de tweede eigenschap hierboven is k een veelvoud van zowel a als b. Ieder gemeenschappelijk veelvoud c voldoet blijkens deze zelfde eigenschap aan $v_p(c) \geq v_p(a)$ én $v_p(c) \geq v_p(b)$, dus volgt dat k het kleinste positieve gemeenschappelijke veelvoud is, oftewel $k = \text{kgv}(a, b)$.
5: Is $ab = 0$ en $a|c$ en $b|c$, dan volgt dat $c = 0$ dus in dit geval is de bewering bewezen. Is $ab \neq 0$ dan volgt de bewering door de reeds bewezen 2de en 4de uitspraak hier te combineren.
6: Dit klopt wanneer $ab = 0$ omdat dan ook per definitie $\text{kgv}(a, b) = 0$. Indien $ab \neq 0$, dan is

$$\begin{aligned} |ab| &= \prod_p p^{v_p(a)} \cdot \prod_p p^{v_p(b)} = \prod_p p^{v_p(a)+v_p(b)} \\ &= \prod_p p^{\min\{v_p(a),v_p(b)\}+\max\{v_p(a),v_p(b)\}} \end{aligned}$$

hetgeen vanwege 3) en 4) gelijk is aan $\text{ggd}(a, b) \cdot \text{kgv}(a, b)$. □

Opmerking 1.2.10 De in Gevolg 1.2.9 gegeven formules voor $\text{ggd}(a, b)$ en $\text{kgv}(a, b)$ leveren een methode om deze getallen te vinden op voorwaarde dat we de priemfactorisatie van a en b kennen. In het algemeen kennen we deze natuurlijk niet, en het berekenen ervan blijkt vaak veel lastiger dan direct met het Euclidische algoritme de ggd te bepalen, en vervolgens het kgv met behulp van de formule $\text{kgv}(a, b) = |ab|/\text{ggd}(a, b)$. Merk op dat we om deze formule te *bewijzen* wel gebruikt hebben dat unieke priemfactorisatie bestaat. Evenwel in het *gebruiken* van de formule hebben we dat verder niet nodig.

1.3 Opgaven

1. ('Het b-tallig stelsel'). Laat $a, b \in \mathbb{Z}$ met $a \geq 1$ en $b \geq 2$. Toon aan dat er een $t \in \mathbb{Z}$ bestaat met $t \geq 0$, en verder getallen $c_0, c_1, \ldots, c_t \in \{0, 1, \ldots, b-1\}$ zodat $c_t \neq 0$ en

$$a = c_t b^t + \ldots + c_2 b^2 + c_1 b + c_0.$$

   Laat ook zien dat deze $t, c_0, \ldots, c_t$ *uniek* bepaald zijn.

2. Bewijs dat als $a, b \in \mathbb{Z}$ niet *allebei* gelijk zijn aan nul, dan zijn $a/\text{ggd}(a,b)$ en $b/\text{ggd}(a,b)$ relatief priem.

3. Bepaal $d = \text{ggd}(3354, 3081)$ en vind $x, y \in \mathbb{Z}$ waarvoor $3354x + 3081y = d$. Geef vervolgens *alle* gehele oplossingen van deze vergelijking.

4. Gegeven de Fibonacci rij $(f_n)_{n \geq 0}$, gedefiniëerd door $f_0 = f_1 = 1$ en $f_{n+2} = f_{n+1} + f_n$ voor $n \geq 0$. Hoeveel delingen met rest voert het Euclidische algoritme uit bij het bepalen van $\text{ggd}(f_n, f_{n+1})$? Laat zien dat $\text{ggd}(f_n, f_{n+1}) = 1$ voor elke $n \geq 0$.

5. Laat $n \in \mathbb{Z}$, $n \geq 2$. Toon aan dat n een priemgetal is precies dan als n *geen* deler d heeft met $1 < d \leq \sqrt{n}$.

6. Bewijs dat er oneindig veel priemgetallen zijn die bij deling door 4 rest 3 opleveren.

7. Bewijs dat er oneindig veel priemgetallen p zijn met de eigenschap dat $p - 2$ geen priemgetal is.

8. Bewijs dat voor $a, b, c \in \mathbb{Z}$ geldt:

   (a) Als $\text{ggd}(a,b) = \text{ggd}(a,c) = 1$, dan is $\text{ggd}(a, bc) = 1$.

   (b) Als a en b relatief priem zijn en beide delen c, dan deelt hun product c.

   (c) Is $c \geq 0$, dan geldt $\text{ggd}(ac, bc) = c \cdot \text{ggd}(a,b)$.

9. Neem $a, b \in \mathbb{Z}$ beide positief.

   (a) Laat r de rest van a bij deling door b zijn. Toon aan dat $2^r - 1$ de rest van $2^a - 1$ bij deling door $2^b - 1$ is.

   (b) Laat zien dat $2^b - 1 | 2^a - 1$ dan en slechts dan als $b | a$.

   (c) Bewijs dat $\text{ggd}(2^a - 1, 2^b - 1) = 2^{\text{ggd}(a,b)} - 1$.

(d) Zijn bovenstaande uitspraken ook waar indien we '2' vervangen door een geheel getal $c > 2$?

10. Gegeven zijn $a, b, n \in \mathbb{Z}$ met $n \geq 0$.

    (a) Toon aan dat $a - b | a^n - b^n$.

    (b) Bewijs dat als n oneven is, dan geldt $a + b | a^n + b^n$.

    (c) Kies nu $b = 1$ en neem aan $a > 1$ en $n > 1$. Bewijs dat als $a^n - 1$ een priemgetal is, dan geldt $a = 2$ en n is een priemgetal.

    (d) Neem $a = 2$ en $n = 11$, en ga na dat $a^n - 1$ geen priemgetal is. Kennelijk geldt de omkering van bovenstaande bewering dus niet.

11. Laat zien dat als $2^n + 1$ een priemgetal is, dan geldt $n = 2^k$ voor een geheel getal $k \geq 0$.

12. Bewijs dat als voor $n \in \mathbb{Z}, n \geq 1$ geldt dat $n^4 + 4^n$ een priemgetal is, dan is $n = 1$.

13. (a) Laat zien dat voor een priemgetal $p > 3$ geldt dat $24 | p^2 - 1$.

    (b) Laat zien dat als p_1, p_2, p_3, p_4, p_5 (niet noodzakelijk verschillende) priemgetallen zijn, en $p_1 p_2 p_3 p_4 p_5 + 1 = p^2$ voor een priemgetal p, dan is $p = 7$ of $p = 11$ of $p = 13$.

14. Stel dat $p_1, \ldots, p_n$ onderling verschillende priemgetallen zijn. Toon aan dat $\log(p_1), \ldots, \log(p_n)$ lineair onafhankelijk zijn over $\mathbb{Q}$, dwz. er bestaan geen $a_1, \ldots, a_n \in \mathbb{Q}$ die niet allemaal gelijk aan nul zijn, zodat $a_1 \log(p_1) + \ldots + a_n \log(p_n) = 0$.

2 Rekenen modulo N

In dit hoofdstuk gaan we in op de basiseigenschappen van het rekenen met resten.

2.1 Restklassen modulo N

Laat N een willekeurig positief geheel getal zijn.

Definitie 2.1.1 Twee gehele getallen a, b heten *congruent modulo* N wanneer $N|a-b$. Dit wordt genoteerd als $a \equiv b \bmod N$.

Er geldt dat gehele getallen a, b congruent zijn modulo N precies dan als ze dezelfde rest opleveren bij deling door N. Immers, is $a = q_1N + r_1$ en $b = q_2N + r_2$ met $0 \leq r_1, r_2 < N$, dan is $N|a-b$ gelijkwaardig met $N|r_1 - r_2$. Omdat $r_1 - r_2$ strikt tussen $-N$ en $+N$ ligt kan dat alleen maar deelbaar door N zijn als $r_1 - r_2 = 0$ oftewel $r_1 = r_2$.

De relatie 'congruent zijn modulo N' is een equivalentierelatie op $\mathbb{Z}$. Immers, als a en b dezelfde rest hebben bij deling door N dan hebben b en a dat ook, dus de relatie is symmetrisch. Ook is de relatie reflexief, want dat wil in dit geval precies zeggen dat a dezelfde rest bij deling door N heeft als a. Tenslotte geldt dat als a en b dezelfde rest opleveren, en b en c doen dat ook, dan uiteraard ook a en c, oftewel de relatie is transitief.

Zoals bekend deelt een equivalentierelatie een verzameling op in een vereniging van disjuncte deelverzamelingen. In ons geval heten die deelverzamelingen restklassen modulo N. Expliciet:

Definitie 2.1.2 Voor $a \in \mathbb{Z}$ wordt de *restklasse van a modulo N* gegeven door

$$\{b \in \mathbb{Z} \mid \ b \equiv a \bmod N\}.$$

We noteren deze restklasse als $a \bmod N$ of ook wel, als er geen verwarring mogelijk is over wat N is, als $\overline{a}$.

Per definitie is $a \bmod N$ dus een *deelverzameling* van $\mathbb{Z}$. Als $a = qN + r$, dan geldt $a \equiv r \bmod N$, en de restklasse $r \bmod N$ is dezelfde als $a \bmod N$. Er zijn dus evenveel restklassen modulo N als er mogelijke resten bij deling door N zijn, en dat zijn er precies N. De restklasse van a modulo N bestaat precies uit alle getallen van de vorm $a + Nk$ voor een $k \in \mathbb{Z}$, dus we kunnen ook schrijven

$$a \bmod N = \overline{a} = a + N\mathbb{Z}.$$

Voorbeeld 2.1.3 Voor $N = 4$ zijn er zoals uit het bovenstaande blijkt 4 verschillende restklassen, namelijk 0 mod 4 en 1 mod 4 en 2 mod 4 en 3 mod 4. Zoals gezegd zijn dit 4 deelverzamelingen van $\mathbb{Z}$ die verenigd heel $\mathbb{Z}$ opleveren. Uitgeschreven:

$$\begin{aligned}
\{ \quad &\ldots\ldots, -284, \ldots, -8, -4, 0, 4, \ldots, 1016, \ldots\ldots \quad \} = 0 \bmod 4,\\
\{ \quad &\ldots\ldots, -283, \ldots, -7, -3, 1, \ldots, 1017, \ldots\ldots \quad \} = 1 \bmod 4,\\
\{ \quad &\ldots\ldots, -282, \ldots, -6, -2, 2, \ldots, 1018, \ldots\ldots \quad \} = 2 \bmod 4,\\
\{ \quad &\ldots\ldots, -281, \ldots, -5, -1, 3, \ldots, 1019, \ldots\ldots \quad \} = 3 \bmod 4.
\end{aligned}$$

De restklasse 17 mod 4 is dezelfde als 1 mod 4, of, in de notatie $\overline{a} = a \bmod 4$: er geldt $\overline{17} = \overline{1}$, en evenzo $\overline{-1001} = \overline{3}$.

De volgende elementaire eigenschap volgt direct uit algemeenheden over equivalentierelaties. We geven toch een bewijs, als oefening met de gegeven definities.

Lemma 2.1.4 *Voor $a, b \in \mathbb{Z}$ geldt $a \bmod N = b \bmod N$ precies dan als $a \equiv b \bmod N$.*

Bewijs. Neem aan dat $a \bmod N = b \bmod N$. Omdat a een element is van de restklasse $a \bmod N = b \bmod N$, geldt per definitie $a \equiv b \bmod N$.

Omgekeerd, stel $a \equiv b \bmod N$. Zoals we gezien hebben betekent dit dat a en b dezelfde rest opleveren bij deling door N. Dan volgt voor een $c \in \mathbb{Z}$ dat c in de restklasse $a \bmod N$ zit precies dan als c dezelfde rest bij deling door N heeft als a, hetgeen gelijkwaardig is met de uitspraak dat c dezelfde rest oplevert als b, ofwel dat c in $b \bmod N$ zit. Dit bewijst dat $a \bmod N = b \bmod N$. □

Stelling 2.1.5 *Als $\overline{a_1}, \overline{a_2}, \overline{b_1}, \overline{b_2}$ restklassen modulo N zijn bij zekere $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, en $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$, dan volgt $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ en $\overline{a_1 b_1} = \overline{a_2 b_2}$.*

Bewijs. Uit $\overline{a_1} = \overline{a_2}$ en $\overline{b_1} = \overline{b_2}$ volgt vanwege Lemma 2.1.4 dat er $q, q' \in \mathbb{Z}$ zijn zodat $a_2 = a_1 + Nq$ en $b_2 = b_1 + Nq'$. Dan volgt dat $a_2 + b_2 = a_1 + b_1 + N(q + q')$, oftewel, opnieuw vanwege Lemma 2.1.4, $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Ook is $a_2 b_2 = (a_1 + Nq)(a_2 + Nq') = a_1 a_2 + N(a_1 q' + q a_2 + Nqq')$, en dit impliceert dat $\overline{a_1 b_1} = \overline{a_2 b_2}$. □

Definitie 2.1.6 (*Optellen en vermenigvuldigen van restklassen.) De verzameling restklassen modulo N noteren we als $\mathbb{Z}/N\mathbb{Z}$. Zijn $a \bmod N, b \bmod N \in \mathbb{Z}/N\mathbb{Z}$, dan definiëren we*

$$(a \bmod N) + (b \bmod N) = (r_1 + r_2) \bmod N$$

en

$$(a \bmod N) \cdot (b \bmod N) = r_1 r_2 \bmod N,$$

waarbij r_1 een willekeurig element van $a \bmod N$ is en r_2 een willekeurig element van $b \bmod N$. Uit Stelling 2.1.5 blijkt dat het niet uitmaakt welke r_1, r_2 we kiezen.

Opmerking 2.1.7 Als we in de bovenstaande definitie $r_1 = a$ en $r_2 = b$ kiezen (dat mag, want a, b zitten in resp. $a \bmod N, b \bmod N$), dan staat er $\overline{a} + \overline{b} = \overline{a+b}$ en $\overline{a} \cdot \overline{b} = \overline{ab}$.

Voorbeeld 2.1.8 We kiezen $N = 17$. Er geldt $\overline{-1} = \overline{67}$, want het verschil van -1 en 67 is deelbaar door 17. Dus volgt dat ook $\overline{1} = \overline{(-1)(-1)} = \overline{-1} \cdot \overline{-1} = \overline{67} \cdot \overline{67} = \overline{67^2}$. Kennelijk geldt dus dat 67^2 en 1 dezelfde rest opleveren bij deling door 17, oftewel dat $67^2 - 1$ deelbaar is door 17. (Dat hadden we natuurlijk ook zonder restklassen kunnen inzien: $67^2 - 1 = (67+1)(67-1)$.)

Nu we restklassen modulo N kunnen optellen en vermenigvuldigen, kunnen we ze natuurlijk ook tot een positieve macht n verheffen.

Definitie 2.1.9 Voor een natuurlijk getal n wordt de $n$de macht van een restklasse $\overline{a}$, notatie $\overline{a}^n$, inductief als volgt gedefiniëerd. $\overline{a}^1 = \overline{a}$ en hebben we voor $n \geq 1$ al $\overline{a}^n$ gedefiniëerd, dan is $\overline{a}^{n+1} = \overline{a}^n \cdot \overline{a}$.

Met deze definitie geldt $\overline{a}^m = \overline{a^m}$ en $\overline{a}^{n+m} = \overline{a}^n \cdot \overline{a}^m$, zoals men gemakkelijk met inductie naar m nagaat. Ook volgt dus $\overline{ab}^m = \overline{(ab)^m} = \overline{a^m b^m} = \overline{a^m} \cdot \overline{b^m} = \overline{a}^m \cdot \overline{b}^m$.

Voorbeeld 2.1.10 Om te illustreren hoe deze definities te gebruiken zijn, laten we zien dat $2^{1000} + 1$ deelbaar is door 257. Schrijf $\overline{a}$ voor de restklasse van a modulo 257. Er geldt

$$\overline{2^{1000}} = \overline{(2^8)^{125}} = \overline{256}^{125} = \overline{-1}^{125} = \overline{-1}.$$

Omdat 2^{1000} en -1 dezelfde restklasse modulo 257 opleveren, is hun verschil deelbaar door 257 en dat is precies wat we wilden laten zien. Merk op dat $2^{1000} + 1$ decimaal uitgeschreven een getal van 302 cijfers is, dus deze deelbaarheid controleren door gewoon te delen door 257 is een hele klus.

Voorbeeld 2.1.11 We berekenen de laatste twee cijfers van 2^{1000} (decimaal uitgeschreven). Dit is hetzelfde als de rest van 2^{1000} bij deling door 100. In $\mathbb{Z}/100\mathbb{Z}$ geldt, omdat $4^6 = 2^{12} = 4096$, dat

$$\overline{16}^6 = \overline{4}^6 \cdot \overline{4}^6 = \overline{4096} \cdot \overline{4096} = \overline{-4} \cdot \overline{-4} = \overline{16}.$$

Verder is $1000 = 4 \cdot 250$ en $250 = 6 \cdot 41 + 4$ en $41 = 6 \cdot 6 + 5$, dus

$$\begin{aligned}\overline{2^{1000}} = \overline{2}^{250} &= \overline{16}^4 \cdot (\overline{16}^6)^{41} \\ &= \overline{16}^4 \cdot \overline{16}^{41} \qquad = \overline{16}^4 \cdot (\overline{16}^6)^6 \cdot \overline{16}^5 \\ &\qquad\qquad = \overline{16}^4 \cdot \overline{16} \cdot \overline{16}^5 \\ &\qquad\qquad = \overline{16}^4 \cdot \overline{16}^6 = \overline{16}^4 \cdot \overline{16} \\ &\qquad\qquad = \overline{16}^5 = (\overline{2^{10}})^2 = \overline{24}^2 = \overline{76}.\end{aligned}$$

De gevraagde laatste 2 cijfers zijn dus 76.

2.2 Eenheden modulo N

Definitie 2.2.1 Een restklasse a mod N heet een *eenheid modulo* N wanneer er een restklasse b mod N bestaat waarvoor geldt $(a \bmod N) \cdot (b \bmod N) = 1 \bmod N$.

De deelverzameling van $\mathbb{Z}/N\mathbb{Z}$ bestaande uit alle restklassen die eenheden modulo N zijn, noteren we als $(\mathbb{Z}/N\mathbb{Z})^*$.

Voorbeeld 2.2.2 Neem $N = 12$. Dan $\mathbb{Z}/12\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{10}, \overline{11}\right\}$. We gaan na welke van deze restklassen in $(\mathbb{Z}/12\mathbb{Z})^*$ zitten. Als $a, b \in \mathbb{Z}$ en $\overline{a} \cdot \overline{b} = \overline{1}$, dan wil dat zeggen dat $ab = 1 + 12k$ voor zekere $k \in \mathbb{Z}$. In het bijzonder zien we dat als $\overline{a}$ een eenheid modulo 12 is, dan is a niet deelbaar door 2 en ook niet deelbaar door 3. Hieruit volgt

$$(\mathbb{Z}/12\mathbb{Z})^* \subset \left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}.$$

Omdat $\overline{1}^2 = \overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$, zijn de vier genoemde restklassen inderdaad eenheden modulo 12. Dus

$$(\mathbb{Z}/12\mathbb{Z})^* = \left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}.$$

We geven een eenvoudig criterium om ook in het algemeen alle eenheden modulo N te vinden.

Stelling 2.2.3 *Voor $a \in \mathbb{Z}$ geldt dat $a \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$ dan en slechts dan als $ggd(a, N) = 1$.*

Bewijs. Laat $a \in \mathbb{Z}$. De uitspraak '$a \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$' houdt per definitie in dat er een $b \in \mathbb{Z}$ is zodat $(ab) \bmod N = (a \bmod N) \cdot (b \bmod N) = 1 \bmod N$. Dit is equivalent met het bestaan van een $q, b \in \mathbb{Z}$ zodat $ab - 1 = Nq$. Anders geschreven: $ab - Nq = 1$. In Gevolg 1.1.14 is al aangetoond dat zulke getallen bestaan precies dan als $\text{ggd}(a, N) = 1$. □

Definitie 2.2.4 (De Euler Phi functie; Leonhard Euler, Zwitsers wiskundige, 1707–1783) Het aantal elementen van $(\mathbb{Z}/N\mathbb{Z})^*$ duiden we aan met $\varphi(N)$.

Gevolg 2.2.5 *$\varphi(N)$ is gelijk aan het aantal getallen $a \in \mathbb{Z}$ met $1 \leq a \leq N$ en $ggd(a, N) = 1$. In het bijzonder geldt voor ieder priemgetal p dat $\varphi(p) = p - 1$.*

Bewijs. Dit volgt direct uit de definities en uit Stelling 2.2.3. □

Een aantal eigenschappen van $(\mathbb{Z}/N\mathbb{Z})^*$ sommen we nu op.

Stelling 2.2.6 *1. Als $a \bmod N$ en $b \bmod N$ eenheden modulo N zijn, dan is hun product dat ook.*

2. Als $a \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$, dan is een restklasse $b \bmod N$ waarvoor $(a \bmod N) \cdot (b \bmod N) = 1 \bmod N$ zelf ook weer een eenheid modulo N.

3. Voor elke $a \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$ bestaat er precies één klasse $b \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$ zodat $(a \bmod N) \cdot (b \bmod N) = 1 \bmod N$.

Bewijs. 1: Vanwege Stelling 2.2.3 is de te bewijzen uitspraak gelijkwaardig met: als $\text{ggd}(a, N) = \text{ggd}(b, N) = 1$, dan ook $\text{ggd}(ab, N) = 1$. Welnu, zou $\text{ggd}(ab, N) \neq 1$ zijn, dan bestaat er een priemgetal p dat $\text{ggd}(ab, N)$ deelt. Dit priemgetal deelt N, en ab, dus vanwege Stelling 1.2.3 ook $p|a$ of $p|b$. Dit levert een tegenspraak met $\text{ggd}(a, N) = \text{ggd}(b, N) = 1$.

Ander bewijs: omdat $\overline{a}, \overline{b}$ eenheden modulo N zijn, bestaan er $\overline{c}, \overline{d}$ zodat $\overline{c} \cdot \overline{a} = \overline{db} = \overline{1}$. Noem $\overline{e} = \overline{d} \cdot \overline{c}$, dan is $\overline{e} \cdot \overline{ab} = \overline{dcab} = \overline{d} \cdot \overline{ca} \cdot \overline{b} = \overline{db} = \overline{1}$, dus is $\overline{ab} \in (\mathbb{Z}/N\mathbb{Z})^*$.
2: Dit volgt direct uit het feit dat $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.
3: Als $\overline{a} \cdot \overline{b_1} = \overline{1} = \overline{a} \cdot \overline{b_2}$, dan volgt dat $\overline{b_1} = \overline{b_1} \cdot \overline{1} = \overline{b_1} \cdot \overline{ab_2} = \overline{b_1 ab_2} = \overline{ab_1} \cdot \overline{b_2} = \overline{b_2}$.
Dit bewijst Stelling 2.2.6. □

Definitie 2.2.7 Voor $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ noemen we de unieke $\overline{b} \in (\mathbb{Z}/N\mathbb{Z})^*$ met de eigenschap $\overline{a} \cdot \overline{b} = \overline{1}$ de *inverse* van $\overline{a}$, notatie $\overline{a}^{-1}$.

Opmerking 2.2.8 Is $a \in \mathbb{Z}$ zo, dat $a \bmod N$ een eenheid modulo N is, dan kan de inverse van $a \bmod N$ met behulp van het Euclidische algorithme berekend worden.Er geldt namelijk omdat $a \bmod N$ een eenheid is, dat $\text{ggd}(a, N) = 1$. Dus bestaan er $x, y \in \mathbb{Z}$ met $xa + yN = 1$, en voor zo'n x geldt $\overline{x} \cdot \overline{a} = \overline{1}$, met andere woorden, $x \bmod N$ is de inverse van $\overline{a}$ modulo N.

De belangrijkste bewerkingen die we tot nu toe met restklassen modulo N gedaan hebben, zijn naast natuurlijk optellen, aftrekken en vermenigvuldigen, het machtsverheffen en in het geval van eenheden modulo N, het inverse nemen.

In computeralgebra systemen als MAGMA, Maple, Mathematica en PARI, en zelfs in WolframAlpha, zijn standaardroutines ingebouwd voor dit soort bewerkingen. Bijvoorbeeld in Maple ziet dat er als volgt uit:

```
100^(-1) mod 420001;
7 &^ (420!) mod 100;
```

Het symbool & in de tweede regel hier, zorgt ervoor dat Maple niet eerst 7 tot de macht 420! gaat verheffen, maar op een efficientere manier het antwoord vindt.

Voorbeeld 2.2.9 Er geldt $(13 \bmod 37)^{-1} = 20 \bmod 37$ (ga na).

Stelling 2.2.10 *Voor elke* $a \bmod N \in (\mathbb{Z}/N\mathbb{Z})^*$ *geldt* $(a \bmod N)^{\varphi(N)} = 1 \bmod N$.

Dit resultaat werd voor het eerst door Euler bewezen. Een andere manier om de stelling te formuleren is: als $a, N \in \mathbb{Z}$ getallen zijn met $N > 0$ en $\text{ggd}(a, N) = 1$, dan geldt $N | a^{\varphi(N)} - 1$. Het resultaat en allerlei gevolgen ervan zijn tegenwoordig toegepast in o.a. cryptografie en in het testen of een (heel groot) getal een priemgetal is. We komen hier nog op terug.

Bewijs. Schrijf $(\mathbb{Z}/N\mathbb{Z})^* = \left\{\overline{a_1}, \ldots, \overline{a_{\varphi(N)}}\right\}$. In Stelling 2.2.6 zagen we dat een product van eenheden modulo N weer een eenheid is, dus is

$$\epsilon := \overline{a_1} \cdot \overline{a_2} \cdot \ldots \cdot \overline{a_{\varphi(N)}}$$

ook een eenheid modulo N. Bekijk nu de afbeelding 'vermenigvuldigen met $\overline{a}$'. Dit beeldt $(\mathbb{Z}/N\mathbb{Z})^*$ naar zichzelf af, want $\overline{a}$ is een eenheid. We laten nu zien dat de afbeelding zelfs een bijectie op $(\mathbb{Z}/N\mathbb{Z})^*$ is. Immers, als $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c}$, dan volgt door beide uitdrukkingen met de inverse van $\overline{a}$ te vermenigvuldigen, dat $\overline{b} = \overline{c}$. Dus is de afbeelding injectief. Dit betekent dat verschillende elementen ook naar verschillende elementen worden afgebeeld, dus bestaat het beeld uit evenveel elementen als het origineel, en dat zijn er $\varphi(N)$. Dit impliceert dat de afbeelding ook surjectief is. Uitgeschreven levert dit de gelijkheid

$$(\mathbb{Z}/N\mathbb{Z})^* = \left\{\overline{a} \cdot \overline{a_1}, \overline{a} \cdot \overline{a_2}, \ldots, \overline{a} \cdot \overline{a_{\varphi(N)}}\right\}.$$

Vermenigvuldigen we al deze elementen, dan krijgen we zoals we al zagen ϵ. Anderzijds zien we dat het product gelijk is aan

$$(\overline{a} \cdot \overline{a_1}) \cdot (\overline{a} \cdot \overline{a_2}) \cdot \ldots \cdot (\overline{a} \cdot \overline{a_{\varphi(N)}}) = \overline{a}^{\varphi(N)} \cdot \overline{a_1} \cdot \overline{a_2} \cdot \ldots \cdot \overline{a_{\varphi(N)}} = \overline{a}^{\varphi(N)} \cdot \epsilon.$$

Dus volgt $\epsilon = \overline{a}^{\varphi(N)} \cdot \epsilon$, en door beide kanten met de inverse van ϵ te vermenigvuldigen volgt $\overline{a}^{\varphi(N)} = \overline{1}$, wat we wilden bewijzen. □

Gevolg 2.2.11 *(De kleine stelling van Fermat; Pierre de Fermat, Frans amateurwiskundige, 1601–1665) Is p een priemgetal, dan geldt voor elke restklasse $a \bmod p$ dat $(a \bmod p)^p = a \bmod p$.*

Bewijs. Als $a \bmod p$ geen eenheid modulo p is, dan volgt vanwege het feit dat p priem is, dat $a \bmod p = 0 \bmod p$, en in dit geval is het Gevolg dus duidelijk. Verder is voor p een priemgetal $\varphi(p) = p - 1$, zoals we al in Gevolg 2.2.5 zagen. Is dus $a \bmod p$ wel een eenheid, dan geldt vanwege Stelling 2.2.10 dat $(a \bmod p)^p = (a \bmod p) \cdot (a \bmod p)^{p-1} = (a \bmod p) \cdot \overline{1} = a \bmod p$. □

De kleine stelling van Fermat levert een zeer snel te implementeren criterium op om na te gaan dat veel grote getallen geen priemgetallen zijn. Willen we namelijk nagaan of N priem is, dan kiezen we (bijvoorbeeld) $a = 2$, en berekenen $(2 \bmod N)^N$. Komt daar iets anders uit dan $2 \bmod N$, dan mogen we uit Fermat's kleine stelling concluderen dat N geen priemgetal is. Merk op dat dit machtsverheffen gedaan kan worden door in de orde van grootte van $\log(N)$ vermenigvuldigingen/ delingen met rest uit te voeren. Bovendien gaat het hierbij steeds om getallen tussen 0 en N. Deze 'samengesteldheids test' is dus heel veel sneller dan domweg proberen of N ergens tussen 1 en $\sqrt{N}$ een deler heeft! Hier staat evenwel tegenover, dat ons algorithme minder informatie geeft: bijvoorbeeld weten we als het algorithme concludeert dat een gegeven N niet priem is, nog niets over eventuele delers van N. En wat veel erger is: er bestaan getallen die geen priemgetal zijn, zoals $341 = 11 \cdot 31$, waarvoor geldt dat toch $(2 \bmod 341)^{341} = 2 \bmod 341$. In dit voorbeeld kunnen we door naar $3 \bmod 341$ in plaats van naar $2 \bmod 341$ te kijken, toch nog inzien dat 341 geen priemgetal is. Helemaal vervelend zijn in dit opzicht de zogeheten Carmichael getallen. Dit zijn getallen N die niet priem zijn, maar waarvoor toch voor elke $a \in \mathbb{Z}$ geldt dat $(a \bmod N)^N = a \bmod N$. Het kleinste Carmichael getal is $N = 561 = 3 \cdot 11 \cdot 17$. In 1992 bewezen Alford, Granville en Pomerance dat er oneindig veel van deze getallen bestaan.

2.3 De Chinese reststelling

Om na te gaan dat bijvoorbeeld $N = 561 = 3 \cdot 11 \cdot 17$ de zojuist genoemde eigenschap heeft, namelijk dat elk getal a voldoet aan $561|a^{561} - a$, ligt het voor de hand in plaats van direct naar deelbaarheid door 561, naar deelbaarheid door 3, 11 en 17 te kijken. Op die manier volgt de eigenschap betrekkelijk eenvoudig: is a niet deelbaar door 3, dan volgt uit Stelling 2.2.10 dat $(a \bmod 3)^2 = 1 \bmod 3$, dus voor een *even* exponent $m = 2k$ geldt $(a \bmod 3)^m = (1 \bmod 3)^k = 1 \bmod 3$, met andere woorden $3|a^{2k} - 1$. Door met a te vermenigvuldigen, volgt $3|a^{2k+1} - a$, en deze eigenschap is ook waar voor een a die door 3 deelbaar is, dus voor elke $a \in \mathbb{Z}$.

Op dezelfde manier volgt dat voor een exponent $m = 10\ell$ die een veelvoud van 10 is geldt, dat $11|a^{10\ell} - 1$ (mits a niet deelbaar is door 11). Dus krijgen we voor iedere $a \in \mathbb{Z}$ dat $11|a^{10\ell+1} - a$. En tenslotte geldt evenzo voor $a \in \mathbb{Z}$ dat $17|a^{16n+1} - a$. Combineren we deze drie deelbaarheidseigenschappen, dan blijkt dat voor elke exponent m die één plus een veelvoud van zowel 16 als 10 als 2 is, met andere woorden die één plus een veelvoud van $\text{kgv}(16, 10, 2) = 80$ is, geldt dat $3 \cdot 11 \cdot 17 = 561|a^m - a$. In het bijzonder geldt dus voor zulke a dat $561|a^{561} - a$, want $561 = 1 + 80 * 7$.

Een dergelijk resultaat vinden we dus door twee hulpmiddelen te combineren: het rekenen modulo priemgetallen p (dat leverde het benodigde speciale geval van Stelling 2.2.10), en het combineren van deelbaarheid modulo priemgetallen tot deelbaarheid modulo hun product. Dit laatste gaan we nu wat algemener bekijken; in het bijzonder niet alleen voor priemgetallen.

Lemma 2.3.1 *Laat $N, M \in \mathbb{Z}$ positieve getallen zijn. Het voorschrift 'Beeldt de restklasse van a modulo N af op de restklasse van a modulo M' geeft een goed gedefiniëerde afbeelding: $\mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/M\mathbb{Z}$ precies dan als $M|N$.*

Bewijs. We moeten nagaan wanneer het genoemde voorschrift een afbeelding definiëert; met ander woorden, wanneer elk origineel in $\mathbb{Z}/N\mathbb{Z}$ precies één beeld in $\mathbb{Z}/M\mathbb{Z}$ heeft. Neem een restklasse in $\mathbb{Z}/N\mathbb{Z}$; zeg dat dit de restklasse van een $a \in \mathbb{Z}$ is. Deze wordt dan afgebeeld op $a \bmod M$, maar ook, voor elke andere $b \in \mathbb{Z}$ die dezelfde restklasse modulo N oplevert als a, op $b \bmod M$. Wat we dus willen is kennelijk precies, dat voor elke $a, b \in \mathbb{Z}$ met $a \bmod N = b \bmod N$ ook geldt dat $a \bmod M = b \bmod M$. Anders gezegd: als $N|a-b$, dan moet ook $M|a-b$. Dit willen we voor alle $a, b \in \mathbb{Z}$; dus door $a = N$ en $b = 0$ te kiezen zien we, dat om een goed gedefiniëerde afbeelding te krijgen noodzakelijk is, dat $M|N$. Omgekeerd, als $M|N$, dan volgt voor alle $a, b \in \mathbb{Z}$ met $N|a - b$ dat $M|N|a - b$, dus in het bijzonder dat $M|a - b$. Dit bewijst het gevraagde. □

Opmerking 2.3.1 Bovenstaand lemma komt wellicht wat merkwaardig over. Het laat evenwel iets heel essentieels van het rekenen met restklassen zien. Namelijk, restklassen zijn verzamelingen, en als we daar zomaar een element uit kiezen en daar weer iets mee doen, dan hoeft het natuurlijk helemaal niet zo te zijn dat als we een ander element uit de restklasse gekozen hadden, dit uiteindelijk hetzelfde had opgeleverd.

Voorbeeld 2.3.2 $a \bmod 4 \mapsto a \bmod 2$ definiëert een afbeelding van $\mathbb{Z}/4\mathbb{Z}$ naar $\mathbb{Z}/2\mathbb{Z}$. Deze afbeelding beeldt $1 \bmod 4$ en $3 \bmod 4$ af op $1 \bmod 2$, en $0 \bmod 4$ en $2 \bmod 4$ op $0 \bmod 2$.

Echter $a \bmod 2 \mapsto a \bmod 4$ definiëert geen afbeelding. Want bijvoorbeeld $1 \bmod 2$ is hetzelfde als $3 \bmod 2$, maar $1 \bmod 4$ en $3 \bmod 4$ zijn uiteraard verschillend.

Anders gezegd: als we van een getal z'n rest bij deling door 4 weten, dan kennen we ook de rest bij deling door 2. Maar omgekeerd, uit de informatie wat de rest bij deling door 2 is, weten we nog niet wat we overhouden bij deling door 4.

Om de belangrijkste resultaten van deze sectie te kunnen formuleren, brengen we nog even een notatie uit de verzamelingentheorie in herinnering. Voor verzamelingen V en W, noteren we het cartesisch product van V en W als $V \times W$. Per definitie bestaat dit uit alle geordende paren van een element uit V gevolgd door een element uit W:

$$V \times W = \{(v, w) \mid \ v \in V \text{ en } w \in W\}.$$

Stelling 2.3.3 *(De Chinese reststelling)*
Laat N, M positieve gehele getallen zijn met ggd$(N, M) = 1$. Dan bestaat de afbeelding

$$a \bmod NM \mapsto (a \bmod N, a \bmod M) \ : \ \mathbb{Z}/NM\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}.$$

Deze afbeelding is bijectief.

Bovendien beeldt de afbeelding $(\mathbb{Z}/NM\mathbb{Z})^*$ af naar $(\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/M\mathbb{Z})^*$, en ook dit is een bijectie.

Bewijs. Het bestaan van de afbeelding volgt uit Lemma 2.3.1. We tonen nu eerst aan dat de afbeelding injectief is. Als $a, b \in \mathbb{Z}$ en $(a \bmod N, a \bmod M) = (b \bmod N, b \bmod M)$, dan houdt dat per definitie in dat $N|a - b$ en $M|a - b$. Uit Gevolg 1.2.9 volgt dan dat $\text{kgv}(N, M)|a - b$. Verder impliceert ditzelfde gevolg, omdat $\text{ggd}(N, M) = 1$, dat $NM = \text{ggd}(N, M) \cdot \text{kgv}(N, M) = \text{kgv}(N, M)$. Conclusie: $NM|a - b$ oftewel $a \bmod NM = b \bmod NM$. De

afbeelding is dus injectief, en omdat zowel $\mathbb{Z}/NM\mathbb{Z}$ als $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$ uit precies NM elementen bestaan, is de afbeelding dan ook surjectief.

Verder, als voor $a \in \mathbb{Z}$ geldt dat $a \bmod NM \in (\mathbb{Z}/NM\mathbb{Z})^*$, dan is $\gcd(a, NM) = 1$, dus in het bijzonder ook $\gcd(a, N) = 1 = \gcd(a, M)$. Dit wil precies zeggen dat dan ook $(a \bmod N, a \bmod M) \in (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/M\mathbb{Z})^*$. Dus inderdaad beeldt de afbeelding $(\mathbb{Z}/NM\mathbb{Z})^*$ af op $(\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/M\mathbb{Z})^*$.

Omgekeerd, als $(a \bmod N, b \bmod M) \in (\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/M\mathbb{Z})^*$, dan geldt $\gcd(a, N) = 1 = \gcd(b, N)$. Omdat de afbeelding surjectief is, bestaat $c \in \mathbb{Z}$ waarvoor $(c \bmod N, c \bmod M) = (a \bmod N, b \bmod M)$. Bij gevolg is $c = q_1 N + a$ en $c = q_2 M + b$, dus vanwege Lemma 1.1.8 geldt $\gcd(c, N) = \gcd(a, N) = 1$ en evenzo $\gcd(c, M) = \gcd(b, M) = 1$. Maar dan is ook $\gcd(c, NM) = 1$ oftewel $c \bmod NM \in (\mathbb{Z}/NM\mathbb{Z})^*$. De beperking van de afbeelding tot $(\mathbb{Z}/NM\mathbb{Z})^*$ heeft dus als beeld precies $(\mathbb{Z}/N\mathbb{Z})^* \times (\mathbb{Z}/M\mathbb{Z})^*$, en uiteraard is deze beperking ook weer injectief. Hiermee is de Chinese reststelling bewezen. □

Voorbeeld 2.3.4 De Chinese reststelling kan gezien worden als een criterium voor oplosbaarheid van een stel simultane congruenties: voor gegeven a, b, N, M zoeken we $x \in \mathbb{Z}$ met zowel $x \equiv a \bmod N$ als $x \equiv b \bmod M$. De stelling zegt dat als $\gcd(N, M) = 1$, dan zijn er altijd zulke x, en bovendien is de verzameling van alle oplossingen precies een restklasse modulo NM.

Voorbeeld: we bepalen alle $x \in \mathbb{Z}$ met $x \equiv 4 \bmod 9$ en $x \equiv 5 \bmod 11$. Zulke x moeten van de vorm $x = 4 + 9y$ zijn, met $y \in \mathbb{Z}$. Verder dient $4 + 9y \equiv 5 \bmod 11$ te gelden, oftewel $9y \equiv 1 \bmod 11$. Dit wil precies zeggen dat $9 \bmod 11$ de inverse van $y \bmod 11$ in $(\mathbb{Z}/11\mathbb{Z})^*$ moet zijn, dus $y \bmod 11 = 5 \bmod 11$. We concluderen $y = 5 + 11z$ en dus $x = 4 + 9(5 + 11z) = 49 + 99z$ met $z \in \mathbb{Z}$ willekeurig. Anders gezegd: de oplossing bestaat precies uit de restklasse van 49 modulo 99. Het enige getal tussen 1 en 99 dat rest 4 bij deling door 9 en rest 5 bij deling door 11 oplevert, is dus 49.

Opmerking 2.3.5 Met inductie naar n laat zich de Chinese reststelling eenvoudig als volgt generaliseren. Stel $N_1, \ldots, N_n$ zijn positieve gehele getallen met $\gcd(N_i, N_j) = 1$ voor elk paar i, j met $1 \leq i < j \leq n$. Dan is

$$\mathbb{Z}/N_1 \ldots N_n\mathbb{Z} \longrightarrow \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \ldots \times \mathbb{Z}/N_n\mathbb{Z}$$

gegeven door $a \bmod N_1 \ldots N_n \mapsto (a \bmod N_1, \ldots, a \bmod N_n)$ een bijectie. Hetzelfde geldt als we de afbeelding beperken tot eenheden.

Een voorbeeld: $7, 11$ en 13 zijn paarsgewijs relatief priem, en hun product is $7 \cdot 11 \cdot 13 = 1001$. Voor elk drietal gehele getallen $a, b, c \in \mathbb{Z}$ bestaat er dus precies één $x \in \mathbb{Z}$ met $0 \leq x \leq 1000$ waarvoor $x \equiv a \bmod 7$ en $x \equiv b \bmod 11$ en $x \equiv c \bmod 13$. Probeer zelf maar eens voor bepaalde drietallen a, b, c deze x te vinden.

Gevolg 2.3.6 *Voor Euler's φ-functie geldt, dat als N, M positieve gehele getallen zijn met ggd$(N, M) = 1$, dan is $\varphi(NM) = \varphi(N) \cdot \varphi(M)$.*

Bewijs. Per definitie is $\varphi(n)$ gelijk aan het aantal elementen van $(\mathbb{Z}/n\mathbb{Z})^*$. De bewering volgt direct uit Stelling 2.3.3 plus het feit dat voor eindige verzamelingen V, W het aantal elementen van $V \times W$ gelijk is aan het product van de aantallen elementen van V en W. □

Met behulp van dit gevolg zullen we een formule voor $\varphi(n)$ in termen van de priemfactorisatie van n afleiden. Hiervoor is eerst een hulpresultaat nodig.

Lemma 2.3.7 *Voor p een priemgetal en k een geheel getal ≥ 1 geldt*

$$\varphi(p^k) = (p-1)p^{k-1} = p^k - p^{k-1}.$$

Bewijs. We weten al dat $\varphi(p^k)$ gelijk is aan het aantal gehele getallen a met $0 \leq a \leq p^k - 1$ en $\text{ggd}(a, p^k) = 1$. Het genoemde interval bevat precies p^k gehele getallen, en zo'n getal heeft precies dan *niet* grootste gemene deler 1 met p^k, wanneer het door p deelbaar is. De door p deelbare getallen in het interval zijn $0 \cdot p, 1 \cdot p, \ldots, m \cdot p$, waarbij m het grootste gehele getal kleiner dan p^{k-1} is. Het interval bevat dus precies p^{k-1} door p deelbare getallen, en daarom is $\varphi(p^k) = p^k - p^{k-1}$. □

Stelling 2.3.8 *De Euler φ-functie kan voor $n \geq 2$ berekend worden met behulp van de formule*

$$\varphi(n) = \prod_{p|n} (p-1)p^{v_p(n)-1} = n \prod_{p|n} (1 - \frac{1}{p})$$

waar het product over de priemdelers van n wordt genomen.

Bewijs. De tweede gelijkheid volgt uit het feit dat $n = \prod_{p|n} p^{v_p(n)}$.

Voor de eerste gelijkheid zullen we met inductie naar N aantonen dat voor elke n met $2 \leq n \leq N$ de gelijkheid geldt. Voor $N = 2$ is dit juist. Geldt het voor $N \geq 2$, dan hoeven we om het ook voor $N + 1$ te bewijzen alleen maar te verifiëren dat de gelijkheid waar is voor $n = N + 1$. Is deze n een macht van een priemgetal, dan zijn we klaar vanwege Lemma 2.3.7. In het resterende geval kunnen we schrijven $n = p^{v_p(n)} \cdot n'$, met $2 \leq n' \leq N$. Er geldt $\text{ggd}(p^{v_p(n)}, n') = 1$, dus vanwege Gevolg 2.3.6 is $\varphi(n) = \varphi(p^{v_p(n)})\varphi(n')$. Met behulp van de inductiehypothese toegepast op n' volgt dus de gelijkheid voor n. □

Voorbeeld 2.3.9 $\varphi(1000000) = 2^5 \cdot 4 \cdot 5^5 = 400000$. Er zijn dus 400000 positieve oneven getallen onder miljoen die niet op een 5 eindigen.

2.4 Opgaven

1. Bewijs dat voor een oneven $n \in \mathbb{Z}$ geldt $n^2 \equiv 1 \bmod 8$, en voor een oneven priemgetal $p \neq 3$ zelfs $p^2 \equiv 1 \bmod 24$.

2. Gegeven een positief geheel getal $n = \sum a_i 10^i$.

   (a) Laat zien: voor $p = 2$ en voor $p = 5$ geldt dat $p|n$ dan en slechts dan als $p|a_0$.

   (b) Laat zien: voor $m = 3$ en voor $m = 9$ is $m|n$ precies dan als $m|\sum a_i$.

   (c) Bewijs dat $11|n$ precies dan als $11|\sum(-1)^i a_i$.

3. Bepaal de inverse van $\overline{100}$ in $(\mathbb{Z}/257\mathbb{Z})^*$.

4. Laat zien dat $2^{341} \equiv 2 \bmod 341$. Is 341 een priemgetal? Bereken ook $3^{341} \bmod 341$.

5. Laat zien dat voor elke $n \in \mathbb{Z}$ geldt dat $n^{13} \equiv n \bmod 2730$.

6. Welke rest houden we over wanneer $(177 + 10^{15})^{116}$ gedeeld wordt door $1003 = 17 \times 59$?

7. Bepaal alle gehele getallen die rest 3 bij deling door 7, rest 6 bij deling door 11 en rest 1 bij deling door 13 opleveren.

8. (a) Bepaal voor $n = 4$ de restklasse $(n-1)! \bmod 4$.

   (b) Laat zien dat voor $n > 4$ geen priemgetal geldt, dat $(n-1)! \equiv 0 \bmod n$.

   (c) Neem nu $n = p$ een priemgetal. Bepaal alle restklassen $a \bmod p \in (\mathbb{Z}/p\mathbb{Z})^*$ die voldoen aan $(a \bmod p)^{-1} = a \bmod p$.

   (d) Laat zien dat voor $n = p$ een priemgetal geldt $(n-1)! \equiv -1 \bmod n$.

   (e) Laat zien dat $n \geq 2$ priem is dan en slechts dan als $(n-1)! \equiv -1 \bmod n$. Is dit een praktische manier om primaliteit te testen?

9. (a) Laat zien dat een Carmichael getal niet deelbaar is door een kwadraat > 1.

   (b) Bewijs dat als $n = p_1 \cdot \ldots \cdot p_t$ een product is van $t > 1$ onderling verschillende priemgetallen, met de eigenschap dat $p_i - 1|n-1$ voor elke i, dan is n een Carmichael getal.

10. Vind alle oplossingen n van $\varphi(n) = 24$. Idem voor $\varphi(n) = 14$.

11. Laat $N, a \in \mathbb{Z}$ met $N > 0$.

    (a) Bewijs dat $\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ dan en slechts dan als $\overline{-a} \in (\mathbb{Z}/N\mathbb{Z})^*$.

    (b) Voor welke restklassen a mod N geldt dat a mod $N = -a$ mod N? (Onderscheid de gevallen N even en N oneven.)

    (c) Laat zien dat $\varphi(N)$ even is als $N \geq 3$.

12. Laat zien dat als $p_1, \ldots, p_t$ de eerste t priemgetallen zijn, en $n_j = p_1 \cdots p_t - p_1 \cdots p_t / p_j$, dan $\varphi(n_j) = \varphi(n_k)$ voor $1 \leq j, k \leq t$. Concludeer hieruit dat de vergelijking $\varphi(x) = m$ voor vaste m willekeurig veel oplossingen kan hebben.

13. Bepaal alle n waarvoor $\varphi(n) | n$.

3 Groepen en homomorfismen

Een aantal eigenschappen die $\mathbb{Z}$ heeft ten aanzien van de optelling, heeft $(\mathbb{Z}/N\mathbb{Z})^*$ juist ten aanzien van het vermenigvuldigen. We zullen verderop zien dat er nog veel meer verzamelingen zijn met een bewerking erop, die allemaal zo'n zelfde collectie gemeenschappelijke eigenschappen hebben. Het is typerend voor (abstracte) algebra, zoiets in een definitie te gaan vangen. In plaats van voor alle gevallen weer opnieuw, kan dan in één keer voor alles wat aan de definitie voldoet een reeks eigenschappen bewezen worden. Dit hebben we al gezien bij de colleges lineaire algebra: daar wordt heel abstract het begrip 'lineaire ruimte' ingevoerd, en vervolgens blijkt dat allerlei eigenschappen daarvan niet alleen voor de vertrouwde ruimten $\mathbb{R}^2$ en $\mathbb{R}^3$ gelden, maar ook bijvoorbeeld voor allerlei 'scheefliggende' deelruimten van $\mathbb{R}^n$, of zelfs voor ruimten van functies of veeltermen of rijtjes of matrices, enz. enz.

In het geval van 'groepen' waar we het hier over zullen hebben, werd zo'n abstracte definitie voor het eerst opgesteld door de in Duitsland werkende W.F.A. von Dyck (1856–1934). Algebra colleges opbouwen vanuit dit soort abstracte definities werd voor het eerst gedaan in Göttingen rond 1920, met name door een beroemde vrouwelijke wiskundige: Emmy Noether (1882–1935). Onder haar studenten zat een nog jonge Amsterdammer, B.L. van der Waerden. Deze werd in 1928 toen hij nog maar 25 jaar oud was benoemd tot professor in de wiskunde in Groningen, en daar schreef hij een nog steeds veel gebruikt leerboek over algebra, geheel in deze abstracte 'moderne' stijl. Dit was het eerste boek van deze soort ooit geschreven. Van der Waerden, overleden in 1996, werd er wereldberoemd door. De algebra is dankzij dit werk sindsdien over de hele wereld steeds meer uitsluitend op deze wijze gedoceerd.

3.1 Groepen

Definitie 3.1.1 Een *groep* is een tripel $(G, \cdot, e)$ met G een verzameling , $e \in G$, en $\cdot$ een afbeelding van $G \times G$ naar G, die we schrijven als $(x, y) \mapsto x \cdot y$, waarvoor geldt dat

G1 (associativiteit) Voor alle $x, y, z \in G$ geldt $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

G2 (eenheidselement) Voor alle $x \in G$ geldt $e \cdot x = x = x \cdot e$.

G3 (inverses) Voor elke $x \in G$ bestaat een $y \in G$ zodat $x \cdot y = e = y \cdot x$.

Een groep $(G, \cdot, e)$ noemen we *commutatief* of ook wel (naar de Noorse wiskundige Niels Henrik Abel, 1802–1829) *abels*, wanneer bovendien geldt

G4 Voor alle $x, y \in G$ geldt $x \cdot y = y \cdot x$.

Opmerking 3.1.2 In plaats van $(G, \cdot, e)$ hebben we het meestal kortweg over de groep G. De afbeelding $\cdot$ wordt de vermenigvuldiging op G genoemd; ook wel de groepswet op G. In plaats van $x \cdot y$ worden afhankelijk van de context ook wel andere notaties gebruikt, bijvoorbeeld $x \circ y$ of $x * y$ of $x \times y$ of $x + y$ of zelfs xy.

Voorbeeld 3.1.3 $(\mathbb{Z}, +, 0)$ is een groep, en $(\mathbb{Z}/N\mathbb{Z}, +, 0 \bmod N)$ en $((\mathbb{Z}/N\mathbb{Z})^*, \cdot, 1 \bmod N)$ eveneens. Dit zijn allemaal voorbeelden van commutatieve groepen. We kennen al veel meer commutatieve groepen: neem $G = V$ een lineaire ruimte, neem '+' de optelling van vectoren uit V, en $0 \in V$ de nulvector. Dan is $(V, +, 0)$ een abelse groep.

Voorbeeld 3.1.4 De verzameling inverteerbare $n \times n$ matrices met coëfficiënten in $F = \mathbb{R}$ of $F = \mathbb{C}$ of $F = \mathbb{Q}$ (of meer algemeen: F is een *lichaam*) wordt een groep, wanneer we als bewerking matrixvermenigvuldiging nemen, en als eenheidselement de eenheidsmatrix. Deze groep wordt aangeduid als $\mathrm{GL}_n(F)$. Voor $n \geq 2$ is deze groep *niet* commutatief, omdat (bijvoorbeeld) geldt

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \vdots \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \vdots \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix}$$
$$\neq$$
$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \vdots \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \vdots \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix}.$$

Zijn $a_1, a_2, \ldots, a_n$ elementen van een groep G, dan wordt hun product $a_1 a_2 \ldots a_n$ met inductie naar n gedefiniëerd als volgt: voor $n = 2$ is het gewoon de bewerking in de groep. Is het product voor $n-1 \geq 2$ al gedefiniëerd, dan is verder $a_1 a_2 \ldots a_n = (a_1 \ldots a_{n-1}) \cdot a_n$. Met behulp van de associativiteit en inductie naar n blijkt dan dat $(a_1 a_2 \ldots a_k) \cdot (a_{k+1} \ldots a_n) = (a_1 a_2 \ldots a_n)$. Dit product van n factoren wordt vaak afgekort als $\prod_{i=1}^{n} a_i$, en in het geval van een abelse groep als $\sum_{i=1}^{n} a_i$. Zijn alle a_i hierin gelijk, zeg $a_i = a$, dan

schrijven we $a^n = \prod_{i=1}^{n} a_i$. De zojuist genoemde eigenschap vertaalt zich, wanneer we schrijven $\ell = n - k$, in $a^k \cdot a^\ell = a^{k+\ell}$. Let op dat machtsverheffen in een groep zich in het algemeen toch wat minder mooi gedraagt als machtsverheffen met bijvoorbeeld gehele getallen. Bijvoorbeeld geldt in het voorbeeld van inverteerbare matrices i.h.a. *niet* dat $(AB)^2 = A^2B^2$ (maak zelf een voorbeeld).

We geven nu eerst een paar elementaire eigenschappen van groepen.

Stelling 3.1.5 *Gegeven is een groep $(G, \cdot, e)$.*

1. *Het enige element $e' \in G$ met de eigenschap $e'x = x$ voor elke $x \in G$, is $e' = e$. Hetzelfde is waar met de eigenschap $xe' = x$ voor elke $x \in G$.*

2. *Voor elke $x \in G$ bestaat er precies één $y \in G$ met $xy = e = yx$.*

3. *Kies $a \in G$ vast, dan is de afbeelding $x \mapsto ax$ een bijectie van G naar zichzelf. Evenzo is $x \mapsto xa$ een bijectie.*

Bewijs. 1: Als voor elke $x \in G$ geldt $e'x = x$, dan geldt dit in het bijzonder voor $x = e$. Dus volgt $e = e'e = e'$, de tweede gelijkheid vanwege groepseigenschap G2. Het geval $ee' = e$ leidt op dezelfde wijze tot $e = e'$.
2: Als $xy = e = yx$ en ook $xz = e = zx$, dan volgt $z = ze = z(xy) = (zx)y = ey = y$, dus $y = z$.
3: Neem $a \in G$ willekeurig. De afbeelding $x \mapsto ax$ is injectief, want stel $ax = ay$. Kies $b \in G$ met $ba = e$, dan volgt $x = ex = (ba)x = b(ax) = b(ay) = (ba)y = ey = y$, dus $x = y$. Ook is de afbeelding surjectief, want als $z \in G$ willekeurig, neem dan b als boven en $x = bz$, dan wordt deze x afgebeeld op $ax = a(bz) = (ab)z = ez = z$, dus z zit in het beeld. De afbeelding 'van links met a vermenigvuldigen' is dus zowel injectief als surjectief, dus bijectief. Het geval 'van rechts met a vermenigvuldigen' wordt geheel analoog bewezen. □

Definitie 3.1.6 Laat $(G, \cdot, e)$ een groep zijn en $x \in G$. Het vanwege Stelling 3.1.5 unieke element $y \in G$ met de eigenschap $xy = e = yx$ noemen we de *inverse* van x in G. Dit wordt genoteerd als x^{-1}.

In het geval van een abelse groep waar de groepswet als $+$ genoteerd wordt, noemen we dit element y de *tegengestelde* van x in G, en het wordt genoteerd als $-x$.

Opmerking 3.1.7 Om na te gaan of een zeker element y in een groep de inverse is van een element x, is het voldoende na te gaan dat $xy = e = yx$, want Stelling 3.1.5 zegt dat er slechts één element bestaat met deze eigenschap, en dat is per definitie x^{-1}.

Gevolg 3.1.8 *Laat G een groep zijn en $a, a_1, a_2, \ldots, a_n \in G$.*

1. $(a^{-1})^{-1} = a$.
2. $(a_1 \ldots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdot \ldots \cdot a_1^{-1}$. *(Bij inverse nemen draait dus de volgorde om!)*
3. $(a^n)^{-1} = (a^{-1})^n$.

Bewijs. 1: Er geldt $aa^{-1} = e = a^{-1}a$, en dat zegt precies dat a de inverse van a^{-1} is, oftewel $(a^{-1})^{-1} = a$.
2: Dit bewijzen we met inductie naar n. Voor $n = 1$ klopt de bewering, en als $n \geq 2$ en we nemen aan $(a_1 \ldots a_{n-1})^{-1} = a_{n-1}^{-1} \cdot \ldots \cdot a_1^{-1}$, dan volgt $(a_n^{-1} \cdot a_{n-1}^{-1} \cdot \ldots \cdot a_1^{-1}) \cdot (a_1 \ldots a_n) = a_n^{-1}((a_{n-1}^{-1} \cdot \ldots \cdot a_1^{-1}) \cdot (a_1 \ldots a_{n-1}))a_n = a_n^{-1}ea_n = e$ en evenzo $(a_1 \ldots a_n) \cdot (a_n^{-1} \cdot a_{n-1}^{-1} \cdot \ldots \cdot a_1^{-1}) = e$. Hiermee is met inductie het bewijs geleverd.
3: Dit volgt uit de voorgaande bewering door alle a_i gelijk aan a te kiezen. □

Is x een element van een groep G en $n \in \mathbb{Z}$, dan hebben we voor positieve n al gedefiniëerd wat we onder x^n verstaan. Voor $n = 0$ is per definitie $x^0 = e$, en voor negatieve n is $x^n = (x^{-1})^{-n}$. Met deze definitie en wat zojuist bewezen is, volgt dat $x^n \cdot x^{-n} = e$, dus x^{-n} is de inverse van x^n. Ook volgt eenvoudig met behulp van volledige inductie naar $|n|$ dat voor $n, m \in \mathbb{Z}$ geldt dat $x^{n+m} = x^n \cdot x^m$.

Definitie 3.1.9 De vermenigvuldigtabel
We kunnen een groep G die uit slechts *eindig* veel elementen bestaat volledig beschrijven door in een tabel alle uitkomsten van vermenigvuldigingen van twee elementen van G weer te geven. Dit geven we weer in een matrix $(a_{i,j})$. Op plek $a_{1,1}$ schrijven we niets, of zo je wilt de naam van de groep. In de rest van de eerste rij schrijven we alle elementen van G, en evenzo in de eerste kolom. Op plek $a_{i,j}$ voor $i, j \geq 2$ noteren we het produkt $a_{i,1} \cdot a_{1,j}$. (Dus het element uit de eerste kolom schrijven we links, dat uit de eerste rij rechts! Dit maakt natuurlijk uit in het geval van niet-abelse groepen.)

Voorbeeld 3.1.10 Hier volgt de vermenigvuldigtabel voor $\mathbb{Z}/3\mathbb{Z}$:

$\mathbb{Z}/3\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Het feit dat van links met een vast element vermenigvuldigen een bijectie is, wil precies zeggen dat in iedere rij elk element van de groep een keer voorkomt (na de eerste plek). Evenzo is van rechts met een vast element vermenigvuldigen bijectief, en dat betekent dat in iedere kolom vanaf de tweede plek elk element een keer voorkomt.

Nagaan of een groep commutatief is betekent in termen van de tabel dat we moeten nagaan of $a_{i,j} = a_{j,i}$ voor alle i, j. Met andere woorden, we moeten kijken of de tabel symmetrisch is langs de hoofddiagonaal.

Voorbeeld 3.1.11 Hier volgt een groepentabel voor een niet-abelse groep bestaande uit 6 elementen:

G	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

3.2 Ondergroepen

Analoog aan het begrip "lineaire deelruimte" in een vectorruimte, hebben we ook iets bij groepen.

Definitie 3.2.1 Een *ondergroep* H van een groep $(G, \cdot, e)$ is een deelverzameling van G die, met hetzelfde element e en dezelfde groepsbewerking $\cdot$, zelf weer een groep is.

Voorbeeld 3.2.2 In $(\mathbb{Z}, +, 0)$ is de verzameling bestaande uit alle even getallen een ondergroep.

De verzameling bestaande uit alle niet-negatieve gehele getallen is *geen* ondergroep van $\mathbb{Z}$. Immers, ten aanzien van de groepsbewerking op $\mathbb{Z}$ (de optelling) is niet voor ieder element x uit deze deelverzameling aan G3 voldaan.

In de groep $\mathrm{GL}_n(\mathbb{Q})$ vormen de matrices waarvan de determinant gelijk is aan 1 een ondergroep. Dit volgt uit de formule $\det(AB) = \det(A)\det(B)$ voor $n \times n$-matrices A, B. De zo verkregen ondergroep wordt aangeduid met $\mathrm{SL}_n(\mathbb{Q})$. Hetzelfde geldt als we $\mathbb{Q}$ door $\mathbb{R}$ of door $\mathbb{C}$ of algemener, door een willekeurig lichaam F vervangen. De ondergroep van matrices met determinant 1 heet dan $\mathrm{SL}_n(F)$.

Om op een efficiënte manier na te gaan of een gegeven deelverzameling van een groep een ondergroep is, kan je gebruik maken van het volgende criterium.

Stelling 3.2.3 *Is $(G, \cdot, e)$ een groep en $H \subset G$, dan geldt dat H een ondergroep is precies dan als*

H1 *$e \in H$;*

H2 *Voor elke $x, y \in H$ geldt $x \cdot y \in H$;*

H3 *Voor elke $x \in H$ geldt $x^{-1} \in H$.*

Bewijs. Is H een ondergroep van $(G, \cdot, e)$, dan wil dat per definitie zeggen dat $(H, \cdot, e)$ een groep is. De definitie van een groep impliceert dan direct de eigenschappen H1, H2 en H3.

Omgekeerd, stel dat voor een deelverzameling H de eigenschappen H1, H2 en H3 gelden. We moeten dan nagaan dat $(H, \cdot, e)$ een groep is. H1 zegt dat inderdaad $e \in H$, en H2 zegt dat de beperking tot H van de groepsbewerking op G inderdaad een afbeelding van $H \times H$ naar H is. Aan G1 en G2 is door het tripel $(H, \cdot, e)$ voldaan, want deze eigenschappen gelden voor alle elementen van G dus zeker voor de elementen in de deelverzameling H. Tenslotte is vanwege H3 ook aan G3 voldaan. □

Voorbeeld 3.2.4 Is G een groep en $x \in G$, dan is de verzameling van alle machten van x (zowel positieve als negatieve machten, en ook x^0 wat per definitie gelijk is aan e) een ondergroep. Immers deze verzameling voldoet aan H1, H2 en H3. We noteren de zo verkregen ondergroep als $\langle x \rangle$; in sommige boeken wordt er ook wel de notatie $x^{\mathbb{Z}}$ voor gebruikt.

Voorbeeld 3.2.5 In $(\mathbb{Z}/24\mathbb{Z})^*$ kunnen we een heleboel ondergroepen van de gedaante $\langle x \bmod 24 \rangle = \langle \overline{x} \rangle$ vinden, namelijk $\langle \overline{1} \rangle$ bestaande uit slechts één element, en $\langle \overline{5} \rangle, \langle \overline{7} \rangle, \langle \overline{11} \rangle, \langle \overline{13} \rangle, \langle \overline{17} \rangle, \langle \overline{19} \rangle, \langle \overline{23} \rangle$ die ieder uit precies twee elementen bestaan.

$(\mathbb{Z}/24\mathbb{Z})^*$ heeft overigens nog veel meer ondergroepen; bijvoorbeeld ook $\{\overline{\pm 1}, \overline{\pm x}\}$ voor $x = 5, 7, 11$, bestaande uit 4 elementen.

Voorbeeld 3.2.6 We gaan alle ondergroepen van $(\mathbb{Z}, +, 0)$ beschrijven. Om te beginnen is $\{0\} = 0\mathbb{Z}$ een ondergroep. Is H een ondergroep met $H \neq 0\mathbb{Z}$, dan bevat H een element $x \neq 0$. Omdat H een groep is voor de gewone optelling, is dan ook $-x \in H$. Dus kunnen we concluderen dat H tenminste één positief geheel getal bevat. Het kleinste positieve gehele getal dat in H zit noemen we a.

Bewering: $H = \langle a \rangle = a\mathbb{Z}$. Immers, de tweede gelijkheid is gewoon de definitie van $\langle a \rangle$ die in Voorbeeld 3.2.4 gegeven is. Om te laten zien dat $H \supset \langle a \rangle$, moet bewezen worden dat voor elke $n \in \mathbb{Z}$ geldt dat $an \in H$. Dit gaat met inductie naar $|n|$, gebruik makend van de eigenschappen H2 en H3 voor H (vul zelf de details in!). Omgekeerd moeten we laten zien dat $H \subset a\mathbb{Z}$. Neem $b \in H$ willekeurig. Noem $d = \text{ggd}(a, b)$. Ook d zit in H, want er bestaan $x, y \in \mathbb{Z}$ waarvoor $d = ax + by$, en omdat $a \in H$ geldt ook $ax \in H$ (dat argument is zojuist uitgelegd); evenzo is $b \in H$ en dus ook $by \in H$. Uit H2 volgt dan dat de som $d = ax + by \in H$. We weten $1 \leq d \leq a$, en omdat a per definitie het kleinste positieve getal in H is, moet dus gelden $d = a$. Maar dat impliceert dat $a = d|b$, oftewel $b \in a\mathbb{Z}$. Hiermee zijn beide inclusies aangetoond, dus we hebben bewezen dat $H = \langle a \rangle$.

Een willekeurige ondergroep van $\mathbb{Z}$ is dus van de gedaante $a\mathbb{Z}$, met eventueel $a = 0$. Omgekeerd is iedere deelverzameling van $\mathbb{Z}$ die van deze vorm is, een ondergroep. Hiermee zijn alle ondergroepen van $\mathbb{Z}$ beschreven.

Een belangrijke eigenschap van ondergroepen van *eindige* groepen (dwz. groepen $(G, \cdot, e)$ waarvoor geldt dat de verzameling G uit slechts eindig veel elementen bestaat) wordt in de volgende stelling gegeven. Het in het bewijs gebruikte telargument verdient de nodige aandacht: we zullen deze techniek later nog meerdere malen tegenkomen.

Stelling 3.2.7 *(Stelling van Lagrange; Joseph Louis Lagrange, Frans wiskundige, 1736–1813) Is H een ondergroep van een eindige groep G, dan is het aantal elementen van H een deler van het aantal elementen van G (notatie: $\#H|\#G$).*

Bewijs. Voor $x \in G$ bezien we de deelverzameling $xH = \{xy \mid y \in H\}$ van G. De vereniging van alle deelverzamelingen van dit type is heel G, immers $x \in G$ is een element van xH, want $e \in H$ en $x = xe$.

Verder geldt dat al deze deelverzamelingen hetzelfde aantal elementen hebben, oftewel $\#xH = \#yH$ voor alle $x, y \in G$. Dit volgt uit het feit dat er een bijectie tussen xH en yH bestaat, namelijk $f : xH \to yH$ gegeven door $f(z) = yx^{-1}z$. Deze afbeelding beeldt namelijk inderdaad xH op yH af, want is $z \in xH$, dan geldt $z = xh$ voor een $h \in H$, dus $f(z) = yx^{-1}z = yx^{-1}xh = yh \in yH$. De afbeelding is bijectief, want $g : yH \to xH$ gegeven door $g(z) = xy^{-1}z$ is een inverse zoals eenvoudig na te rekenen is. Het bestaan van een bijectie tussen twee eindige verzamelingen impliceert, dat deze verzamelingen evenveel elementen hebben.

We gaan vervolgens na dat als $xH \cap yH \neq \emptyset$, dan zijn ze gelijk: $xH = yH$. Immers, stel $z \in xH \cap yH$. Dan $z \in xH$, dus we kunnen schrijven $z = xh_1$ voor zekere $h_1 \in H$. Evenzo $z = yh_2$ voor een $h_2 \in H$. Dus is $xh_1 = yh_2$, en

door beide kanten van rechts met h_1^{-1} of met h_2^{-1} te vermenigvuldigen, volgt dat $x = yh_2h_1^{-1}$ en $y = xh_1h_2^{-1}$. Een willekeurige $xh \in xH$ is dus te schrijven als $xh = yh_2h_1^{-1}h = y(h_2h_1^{-1}h) \in yH$ en evenzo is een willekeurige $yh \in yH$ te schrijven als $yh = xh_1h_2^{-1}h \in xH$. Dit bewijst dat $xH = yH$.

We hebben dus G gegeven als vereniging van deelverzamelingen met allemaal evenveel elementen. Door zoveel mogelijk overbodige deelverzamelingen xH weg te gooien, mogen we aannemen dat hierbij deze verzamelingen twee aan twee lege doorsnede hebben. Dan volgt dat $\#G$ gelijk is aan het aantal resterende deelverzamelingen vermenigvuldigd met $\#xH$, en $\#xH = \#eH = \#H$. Dit impliceert $\#H|\#G$, hetgeen we wilden bewijzen. □

We willen dit resultaat in het bijzonder gebruiken voor ondergroepen van de vorm $\langle x \rangle$. Daartoe eerst het volgende.

Definitie 3.2.8 Is x een element van een groep G, dan definiëren we de *orde* van x, notatie $\mathrm{ord}(x)$, als volgt. Als er een $m > 0$ bestaat met $x^m = e$, dan is $\mathrm{ord}(x)$ het kleinste positieve gehele getal n met de eigenschap $x^n = e$. Als voor elke $m > 0$ geldt $x^m \neq e$, dan is $\mathrm{ord}(x) = \infty$.

Voorbeeld 3.2.9 In elke groep $(G, \cdot, e)$ geldt $\mathrm{ord}(e) = 1$. Bovendien, als voor een $x \in G$ geldt dat $\mathrm{ord}(x) = 1$, dan $x = e$, want $\mathrm{ord}(x) = 1$ impliceert dat $x = x^1 = e$.

In $(\mathbb{Z}/5\mathbb{Z})^*$ geldt $\mathrm{ord}(\overline{1}) = 1$ en $\mathrm{ord}(\overline{4}) = 2$ en $\mathrm{ord}(\overline{2}) = \mathrm{ord}(\overline{3}) = 4$.

Stelling 3.2.10 *Gegeven een groep G en een element $x \in G$.*

1. *$ord(x) = ord(x^{-1})$.*
2. *Als $ord(x) < \infty$, dan $\langle x \rangle = \{x, x^2, \ldots, x^{ord(x)} = e\}$.*
3. *$ord(x) = \#\langle x \rangle$.*
4. *Als $\#G < \infty$, dan ook $ord(x) < \infty$ en bovendien $ord(x)|\#G$.*
5. *Als $x^n = e$, dan is $ord(x)|n$.*

Bewijs. 1: Is $x^m = e$, dan ook $(x^{-1})^m = x^{-m} = (x^m)^{-1} = e$. Door deze regel ook voor de inverse van x te gebruiken, zien we dat de verzameling getallen m waarvoor geldt $x^m = e$ dezelfde verzameling is als de getallen n waarvoor $(x^{-1})^n = e$. (NB deze verzameling zou leeg kunnen zijn!) In het bijzonder volgt dus $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$.
2: Schrijf $d = \mathrm{ord}(x)$. Is $m \in \mathbb{Z}$, schrijf dan $m = qd + r$ met $0 \leq r < d$. Dan is $x^m = (x^d)^q \cdot x^r = e^q x^r = x^r$. Hieruit volgt dat $\langle x \rangle \subset \{e, x, \ldots, x^{d-1}\}$.

3: De bewering is juist als $\mathrm{ord}(x) = \infty$, dus we mogen vanaf nu aannemen dat de orde van x eindig is. In dit geval volgt het uit 2) als we aangetoond hebben dat de elementen van $\{e, x, \ldots, x^{\mathrm{ord}(x)-1}\}$ twee aan twee verschillend zijn. Welnu, stel $x^m = x^n$ met $0 \leq m \leq n < \mathrm{ord}(x)$. Vermenigvuldigen met de inverse van x^m levert $e = x^{n-m}$, waarin $0 \leq n - m < \mathrm{ord}(x)$. Omdat per definitie $\mathrm{ord}(x)$ de kleinste positieve d is waarvoor $x^d = e$, moet wel $n - m = 0$. Dus $x^m = x^n$ voor niet-negatieve $n, m < ord(x)$ kan alleen als $n = m$. Hiermee is 3) bewezen.
4: $\langle x \rangle$ is een ondergroep van G, en omdat G eindig is, is deze ondergroep dat ook. Uit 3) en uit Stelling 3.2.7 volgt dan $\mathrm{ord}(x) = \#\langle x \rangle$ is eindig, en zelfs $\mathrm{ord}(x) = \#\langle x \rangle | \#G$.
5: Uit $x^n = e$ volgt dat $\mathrm{ord}(x) < \infty$. Noem $d = \mathrm{ggd}(n, \mathrm{ord}(x))$. Dan zijn er k, ℓ met $nk + \mathrm{ord}(x)\ell = d$. Dus volgt $x^d = (x^n)^k (x^{\mathrm{ord}(x)})^\ell = e$. Omdat $1 \leq d \leq \mathrm{ord}(x)$, moet vanwege de definitie van $\mathrm{ord}(x)$ wel gelden $d = \mathrm{ord}(x)$. In het bijzonder dus $d = \mathrm{ggd}(n, \mathrm{ord}(x)) | n$. □

Voorbeeld 3.2.11 Voor een eindige groep geldt dus dat zowel het aantal elementen van een ondergroep als de orde van elk element een deler moet zijn van het aantal elementen van de groep.

Echter, niet iedere deler van het aantal elementen van de groep komt ook voor als orde van een element. Bijvoorbeeld hebben we al gezien dat alle 8 elementen van $(\mathbb{Z}/24\mathbb{Z})^*$ orde 1 of 2 hebben. In een later hoofdstuk komen we op deze kwestie terug.

Definitie 3.2.12 Het produkt van groepen
Hebben we twee groepen $(G_1, \cdot, e_1)$ en $(G_2, *, e_2)$, dan kan ook op de produktverzameling $G_1 \times G_2$ de structuur van een groep gezet worden. Dit heet het produkt van groepen, en het werkt als volgt. Per definitie zijn elementen van $G_1 \times G_2$ geordende paren (x_1, x_2) met $x_i \in G_i$. Het eenheidselement in de produktgroep is het paar (e_1, e_2). De groepsbewerking wordt gegeven door $(x_1, x_2) \circ (y_1, y_2) = (x_1 \cdot y_1, x_2 * y_2)$. Ga zelf na dat met deze definities inderdaad $(G_1 \times G_2, \circ, (e_1, e_2))$ een groep is.

Geheel analoog wordt het produkt van meer dan twee groepen gemaakt.

Voorbeeld 3.2.13 De groepen $\mathbb{Z}/8\mathbb{Z}$ en $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ hebben alle drie precies 8 elementen. Toch zijn ze in zekere zin echt verschillend: de eerste heeft 4 elementen van orde 8 en de andere twee geen enkel element van die orde. De tweede heeft 4 elementen van orde 4, terwijl in de derde elk element orde 1 of 2 heeft. Wel zijn deze groepen alle drie commutatief. Er bestaan overigens ook nog twee niet-commutatieve groepen met precies 8 elementen (zie Opgave 14).

3.3 Homomorfismen

Na groepen en ondergroepen bekijken we nu afbeeldingen tussen groepen. In de lineaire algebra zijn de afbeeldingen tussen vectorruimten die bekeken worden de lineaire afbeeldingen, oftewel de afbeeldingen die de op vectoren gedefiniëerde bewerkingen behouden. Iets dergelijks doen we nu voor groepen (en in vele andere structuren binnen de wiskunde gebeurt iets geheel analoogs):

Definitie 3.3.1 Gegeven twee groepen $(G_1, \cdot, e_1)$ en $(G_2, *, e_2)$. Een *homomorfisme* van G_1 naar G_2 is een afbeelding $f : G_1 \to G_2$ die voldoet aan $f(x \cdot y) = f(x) * f(y)$ voor alle $x, y \in G_1$.

Een *isomorfisme* van G_1 naar G_2 is een homomorfisme dat bovendien bijectief is.

We noemen G_1 en G_2 *isomorf* (notatie $G_1 \cong G_2$) precies dan, als er een isomorfisme van G_1 naar G_2 bestaat.

Voorbeeld 3.3.2

1. Met $\mathbb{R}^*_{>0}$ duiden we de positieve reële getallen aan. Dit is een groep onder de normale vermenigvuldiging. De afbeelding $\exp : \mathbb{R} \to \mathbb{R}^*_{>0}$ gegeven door $x \mapsto e^x$ is een homomorfisme van $(\mathbb{R}, +, 0)$ naar $(\mathbb{R}^*_{>0}, \cdot, 1)$. Immers, $\exp(x + y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$. Deze afbeelding is zelfs bijectief, dus zijn beide groepen isomorf.

2. $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ is een homomorfisme, omdat $\det(AB) = \det(A)\det(B)$. Dit is voor $n \neq 1$ geen isomorfisme, want het is voor $n > 1$ eenvoudig twee inverteerbare matrices op te schrijven met dezelfde determinant.

3. Is G een willekeurige groep en $x \in G$, dan is $f_x : \mathbb{Z} \to G$ gegeven door $f(n) = x^n$ een homomorfisme. Immers, $f(n + m) = x^{n+m} = x^n x^m = f(n)f(m)$.

   In het speciale geval $G = \mathbb{Z}/N\mathbb{Z}$ en $x = \overline{1}$ is dit precies de afbeelding "reductie modulo N": $n \mapsto n \bmod N$.

4. De in de Chinese Reststelling 2.3.3 gebruikte afbeelding $a \bmod NM \mapsto a \bmod N$ is een homomorfisme, zowel opgevat als afbeelding van $(\mathbb{Z}/NM\mathbb{Z}, +, 0 \bmod NM)$ naar $(\mathbb{Z}/N\mathbb{Z}, +, 0 \bmod N)$, als als afbeelding van $((\mathbb{Z}/NM\mathbb{Z})^*, *, 1 \bmod NM)$ naar $((\mathbb{Z}/N\mathbb{Z})^*, *, 1 \bmod N)$. In het bijzonder volgt dus dat wanneer $\mathrm{ggd}(N, M) = 1$, dan geldt

$$(\mathbb{Z}/NM\mathbb{Z}, +, 0 \bmod NM) \cong (\mathbb{Z}/N\mathbb{Z}, +, 0 \bmod N) \times (\mathbb{Z}/M\mathbb{Z}, +, 0 \bmod M)$$

en

$$((\mathbb{Z}/NM\mathbb{Z})^*, *, 1 \bmod NM) \cong ((\mathbb{Z}/N\mathbb{Z})^*, *, 1 \bmod N) \times ((\mathbb{Z}/M\mathbb{Z})^*, *, 1 \bmod M).$$

We geven een paar basiseigenschappen van homomorfismen.

Stelling 3.3.3 *Gegeven een homomorfisme* $f : (G_1, \cdot, e_1) \to (G_2, *, e_2)$.

1. $f(e_1) = e_2$.
2. *Voor alle* $x \in G_1$ *geldt* $f(x^{-1}) = (f(x))^{-1}$.
3. *Is* f *een isomorfisme, dan is de inverse van* f *dat ook.*
4. *Als ook* $g : (G_2, *, e_2) \to (G_3, \star, e_3)$ *een homomorfisme is, dan is de samenstelling* $g \circ f$ *het ook.*

Bewijs. 1: Schrijf $x = f(e_1)$. Dan geldt in G_2 dat $x * x = f(e_1) * f(e_1) = f(e_1 \cdot e_1) = f(e_1) = x$. Links en rechts met de inverse van x vermenigvuldigen levert dus $x = e_2$.
2: Noem $y = f(x^{-1})$. Er geldt $y * f(x) = f(x^{-1}) * f(x) = f(x^{-1} \cdot x) = f(e_1) = e_2$. Dus is y de inverse van $f(x)$, hetgeen we wilden bewijzen.
3: Schrijf h voor de inverse van f. Zijn $x, y \in G_2$, dan geldt $f(h(x * y)) = x * y = f(h(x)) * f(h(y)) = f(h(x) \cdot h(y))$. Omdat f bijectief is volgt hieruit $h(x * y) = h(x) \cdot h(y)$. Dus h is een homomorfisme, en omdat f bijectief is, is z'n inverse h dat ook. Hieruit volgt dat h een isomorfisme is.
4: Voor $x, y \in G_1$ geldt $g \circ f(x \cdot y) = g(f(x \cdot y)) = g(f(x) * f(y) = g(f(x)) \star g(f(y)) = g \circ f(x) \star g \circ f(y)$. □

Een isomorfisme van groepen kunnen we opvatten als een soort naamsverandering in de groep: we noemen alle elementen anders, we schrijven misschien zelfs de bewerking op een andere manier. Maar in zekere zin is er toch niets veranderd. In het bijzonder verandert de orde van een element niet (al krijgt het element een andere naam). Dit kan soms gebruikt worden om aan te tonen dat bepaalde groepen niet isomorf zijn.

In het algemeen wordt bij een functie φ van een verzameling S_1 naar een verzameling S_2 de volgende notatie gebruikt: is $T_1 \subset S_1$, dan is het *beeld* van T_1, notatie $\varphi(T_1)$, gegeven door

$$\varphi(T_1) = \{y \in S_2 \mid \text{er bestaat een } x \in S_1 \text{ met } y = \varphi(x)\}.$$

Evenzo is voor $T_2 \subset S_2$ het *volledig origineel* van T_2, notatie $\varphi^{-1}(T_2)$, gegeven door

$$\varphi^{-1}(T_2) = \{x \in S_1 \mid \varphi(x) \in T_2\}.$$

Het speciale geval dat in de theorie van groepen van belang is, is dat $\varphi = f$ een homomorfisme tussen groepen is, en de T_i ondergroepen.

Stelling 3.3.4 *Gegeven is een homomorfisme* $f : (G_1, \circ, e_1) \to (G_2, *, e_2)$ *en voor* $i = 1, 2$ *ondergroepen* $H_i \subset G_i$. *Er geldt dat* $f(H_1)$ *een ondergroep van* G_2 *is, en evenzo dat* $f^{-1}(H_2)$ *een ondergroep is van* G_1.

Bewijs. In beide gevallen dient nagegaan te worden dat aan de eisen H1, H2 en H3 is voldaan. H1: $e_2 \in f(H_1)$, want $e_1 \in H_1$ en $f(e_1) = e_2$. Ook $e_1 \in f^{-1}(H_2)$, want $f(e_1) = e_2 \in H_2$. Nu de eis H2: laat $x, y \in f^{-1}(H_2)$. Dan is $f(x), f(y) \in H_2$, dus omdat H_2 een groep is, ook $f(x \cdot y) = f(x) * f(y) \in H_2$. Dit wil precies zeggen dat $x \cdot y \in f^{-1}(H_2)$. Is $w, z \in f(H_1)$, dan wil dat zeggen dat er $u, v \in H_1$ zijn met $f(u) = w$ en $f(v) = z$. Daar H_1 een groep is, is ook $u \cdot v \in H_1$, en dus $w * z = f(u) * f(v) = f(u \cdot v) \in f(H_1)$. Tenslotte H3: voor $x \in f^{-1}(H_2)$ is $f(x^{-1}) = (f(x))^{-1} \in H_2$, want $f(x) \in H_2$ en H_2 is een groep. Dit impliceert dat $x^{-1} \in f^{-1}(H_2)$. Is $z \in f(H_1)$, schrijf dan $z = f(v)$ met $v \in H_1$. Dan volgt $z^{-1} = (f(v))^{-1} = f(v^{-1}) \in f(H_1)$, omdat ook $v^{-1} \in H_1$. Hiermee is de stelling bewezen. □

Definitie 3.3.5 Is $f : (G_1, \cdot, e_1) \to (G_2, *, e_2)$ een homomorfisme, dan definiëren we de *kern* van f, notatie: $\mathrm{Ker}(f)$, door

$$\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\}.$$

Stelling 3.3.6 *Gegeven is een homomorfisme* $f : (G_1, \circ, e_1) \to (G_2, *, e_2)$.

1. *Ker*(f) *is een ondergroep van* G_1.
2. f *is injectief dan en slechts dan als Ker*$(f) = \{e_1\}$.

Bewijs. 1: Dit volgt uit Stelling 3.3.4 omdat $\{e_2\}$ een ondergroep van G_2 is, en $\mathrm{Ker}(f) = f^{-1}(\{e_2\})$.
2: Er geldt altijd $f(e_1) = e_2$. Is f injectief, en $f(x) = e_2$, dan volgt $f(x) = f(e_1)$. Vanwege de injectiviteit impliceert dit $x = e_1$, dus $\mathrm{Ker}(f) = \{e_1\}$. Omgekeerd, als $\mathrm{Ker}(f) = \{e_1\}$ en $f(x) = f(y)$ voor zekere $x, y \in G_1$, dan $e_2 = f(x) * (f(x))^{-1} = f(y) * f(x^{-1}) = f(y \cdot x^{-1})$. Dus $y \cdot x^{-1} \in \mathrm{Ker}(f)$, oftewel $y \cdot x^{-1} = e_1$. Dit impliceert $x = y$, oftewel f is injectief. □

Opmerking 3.3.7 Elke ondergroep van een groep G is te schrijven als $f(G')$ voor een homomorfisme f van een andere groep G' naar G. Immers, voor G' kunnen we simpelweg die ondergroep zelf nemen, en voor f de inclusieafbeelding.

Het is echter *niet* mogelijk, elke ondergroep van G te realiseren als de kern van een homomorfisme van G naar een andere groep G''. Geldt namelijk $H = \mathrm{Ker}(f)$ voor een homomorfisme f, dan heeft H een eigenschap die ondergroepen in het algemeen niet hebben: is $h \in H$, en is $x \in G$ willekeurig, dan is ook $x \cdot h \cdot x^{-1} \in H$. Een kern heeft deze eigenschap, want $f(x \cdot h \cdot x^{-1}) = f(x) * f(h) * (f(x))^{-1} = f(x) * e_2 * ((f(x))^{-1} = e_2$. We zullen later zien dat alle ondergroepen die deze eigenschap hebben, *wel* als kern van een homomorfisme te schrijven zijn.

3.4 Opgaven

1. Ga na welke van de volgende tripels een groep definiëren:
   (a) $(\mathbb{N}, +, 0)$;
   (b) $(\mathbb{Q}^*_{>0}, \cdot, 1)$;
   (c) $(\mathbb{R}, \star, 1)$ waarbij $x \star y = x + y - 1$;
   (d) $(\{x \in \mathbb{R} \mid -\pi/2 < x < \pi/2\}, \circ, 0)$ waarbij $x \circ y = \arctan(\tan(x) + \tan(y))$;
   (e) $(\mathbb{Z}_{>0}, \bullet, 1)$ met $n \bullet m = n^m$.

2. Bewijs (analoog aan de beschrijving van alle ondergroepen van $\mathbb{Z}$) dat de ondergroepen van $\mathbb{Z}/N\mathbb{Z}$ precies alle $\langle a \bmod N \rangle$ zijn, waarbij $a|N$.

3. Geef alle ondergroepen van $(\mathbb{Z}/24\mathbb{Z})^*$.

4. Geef de 2×2 matrices die (t.a.v. de standaardbasis van $\mathbb{R}^2$) roteren over 120 graden en spiegelen in de x-as voorstellen. Maak een zo klein mogelijke ondergroep van $\mathrm{GL}_2(\mathbb{R})$ die deze twee matrices bevat. Is de zo verkregen groep abels? Bereken van elk element van deze groep de orde.

5. Bepaal alle ondergroepen van de in Opgave 4 beschouwde groep. Ga voor deze ondergroepen na of ze te schrijven zijn als kern van een geschikt gekozen homomorfisme.

6. Voor een groep G wordt het *centrum* $\mathcal{Z}(G)$ gegeven door $\mathcal{Z}(G) = \{x \in G \mid \text{voor elke } y \in G \text{ geldt } xy = yx\}$.
   (a) Bewijs dat $\mathcal{Z}(G)$ een abelse ondergroep van G is.
   (b) Bepaal $\mathcal{Z}(\mathrm{GL}_2(\mathbb{R}))$.

7. Gegeven twee eindige groepen G_1 en G_2. Toon aan dat voor $(x, y) \in G_1 \times G_2$ geldt $\mathrm{ord}(x, y) = \mathrm{kgv}(\mathrm{ord}(x), \mathrm{ord}(y))$.

8. In $\mathbb{C}$ definiëren we de deelverzameling $\mathbf{T} = \{a + bi \in \mathbb{C} \mid a^2 + b^2 = 1\}$. Verder noteren we $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
   (a) Laat zien dat $(\mathbf{T}, \cdot, 1)$ een ondergroep van $(\mathbb{C}^*, \cdot, 1)$ is.
   (b) Bewijs dat $(\mathbb{C}^*, \cdot, 1) \cong (\mathbf{T}, \cdot, 1) \times (\mathbb{R}_{>0}, \cdot, 1)$.

9. Stel G is een groep, en $f : G \to G$ is de afbeelding $x \mapsto x \cdot x$. Bewijs dat f een homomorfisme is dan en slechts dan als G abels is.

10. Stel $f : G_1 \to G_2$ is een homomorfisme van groepen, en f is surjectief. Laat zien dat als G_1 commutatief is, dan is G_2 dat ook. Geef een voorbeeld waarbij G_2 abels is maar G_1 niet.

11. (a) Laat zien dat voor een element x van een groep G geldt $x = x^{-1}$ precies dan als $\mathrm{ord}(x) = 2$ of $\mathrm{ord}(x) = 1$.

    (b) Bewijs dat een eindige groep een even aantal elementen heeft, dan en slechts dan als de groep een element van orde 2 bevat.

12. Laat zien dat er op isomorfie na precies twee groepen met precies 4 elementen bestaan (dit is een beetje puzzelwerk; kijk bijv. wat de mogelijke ordes zijn van elementen in zo'n groep, en probeer alle mogelijke vermenigvuldigtabellen te maken).

13. Gegeven een priemgetal p en een groep G met precies p elementen. Neem $x \in G$ met $x \neq e$. Wat is de orde van x? Bewijs dat $G \cong \mathbb{Z}/p\mathbb{Z}$. Er bestaat dus op isomorfie na slechts één groep van orde p (namelijk de abelse groep $\mathbb{Z}/p\mathbb{Z}$).

14. In de groep $\mathrm{GL}_2(\mathbb{C})$ bestaande uit alle inverteerbare 2×2 matrices met complexe coëfficiënten, beschouwen we twee ondergroepen: H_1 is de kleinste ondergroep waar zowel de matrix $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ als de matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ inzit. Verder is H_2 de kleinste ondergroep die zowel $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ als $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ bevat. Ga na dat beide ondergroepen niet-commutatieve groepen bestaande uit 8 elementen zijn, en dat ze niet isomorf zijn (bijvoorbeeld omdat de ene meer elementen met orde 2 bevat dan de andere).

15. Laat x een element zijn van een groep G, en beschouw het homomorfisme $f_x : \mathbb{Z} \to G$ gegeven door $f(n) = x^n$. Geef een verband tussen de orde van x en de kern van f_x.

16. Gegeven een priemgetal $p \neq 3$ en een $n \in \mathbb{Z}$ waarvoor $p | n^2 + n + 1$.

    (a) Ga na dat $n \bmod p \neq 1 \bmod p$ en dat $n \bmod p \in (\mathbb{Z}/p\mathbb{Z})^*$.

    (b) Toon aan dat $\mathrm{ord}(n \bmod p) = 3$ in de groep $(\mathbb{Z}/p\mathbb{Z})^*$.

    (c) Laat zien dat $p \equiv 1 \bmod 3$.

    (d) Bewijs dat er oneindig veel priemgetallen $\equiv 1 \bmod 3$ bestaan. (Aanwijzing: zijn $p_1, \ldots, p_t$ zulke priemgetallen, schrijf dan $n = 3 \cdot p_1 \cdots p_t$ en beschouw priemdelers van $n^2 + n + 1$.)

    (e) (Vergelijk met Opgave 7 in Hoofdstuk 1): Bewijs dat er oneindig veel priemgetallen p zijn waarvoor $p + 2$ niet priem is.

17. Gegeven een priemgetal $p \neq 2$ en een $n \in \mathbb{Z}$ waarvoor $p|n^2 + 1$.

    (a) Ga na (analoog aan de methode gevolgd in Opgave 16) dat $p \equiv 1 \bmod 4$.

    (b) Bewijs dat er oneindig veel priemgetallen $\equiv 1 \bmod 4$ bestaan.

4 Permutatie-groepen

In dit hoofdstuk bestuderen we een belangrijke klasse van groepen, namelijk de groepen bestaande uit alle bijectieve afbeeldingen van een verzameling naar zichzelf.

4.1 Bijecties op een verzameling

Zij Σ een niet-lege verzameling. Een bijectie van Σ naar zichzelf is zoals we weten een afbeelding $\sigma : \Sigma \to \Sigma$ die zowel injectief als surjectief is. Zo'n σ heeft dan een unieke inverse, zeg $\tau : \Sigma \to \Sigma$, die voldoet aan $\sigma \circ \tau = \tau \circ \sigma = id_\Sigma$. Hier is $\circ$ de samenstelling van afbeeldingen, en $id_\Sigma : \Sigma \to \Sigma$ is de identieke afbeelding, gegeven door $id_\Sigma(x) = x$ voor elke $x \in \Sigma$. De samenstelling van bijecties is weer een bijectie.

Definitie 4.1.1 Voor een niet-lege verzameling Σ duiden we met S_Σ de verzameling van alle bijecties van Σ naar zichzelf aan. De *symmetrische groep* op de verzameling Σ is per definitie de groep gegeven door $(S_\Sigma, \circ, id_\Sigma)$.

Het is eenvoudig na te gaan dat de symmetrische groep inderdaad een groep is.

Voorbeeld 4.1.2 Als Σ een verzameling bestaande uit precies één element is, dan is de enige bijectie op Σ de identiteit. In dit geval krijgen we dus een groep S_Σ die uit slechts één element bestaat (de "triviale" groep).

Bestaat Σ uit precies twee elementen, dan zijn er precies twee bijecties mogelijk: degene die beide elementen vasthoudt (dat is id_Σ), en degene die de twee elementen verwisselt (die noemen we even τ). Er geldt $\tau^2 = \tau \circ \tau = id_\Sigma$. De groep S_Σ is dus in dit geval isomorf met $\mathbb{Z}/2\mathbb{Z}$.

Voor Σ met $\#\Sigma > 2$ is de groep S_Σ niet commutatief. Immers, kies drie verschillende elementen $x, y, z \in \Sigma$. Construeer twee bijecties $\sigma, \tau \in S_\Sigma$ als volgt. σ verwisselt x en y en houdt alle overige elementen van Σ vast. τ verwisselt y en z en houdt de overige elementen vast. Dit definiëert inderdaad twee bijecties, en er geldt $\sigma \circ \tau(x) = y$ terwijl $\tau \circ \sigma(x) = z$. Dus $\sigma \circ \tau \neq \tau \circ \sigma$. In het bijzonder is dus S_Σ niet commutatief.

Hebben we twee "even grote" verzamelingen Σ en Σ' (preciezer gezegd: twee verzamelingen met een bijectie $f : \Sigma \xrightarrow{\sim} \Sigma'$ ertussen), dan is waarschijnlijk intuïtief wel duidelijk dat de groepen S_Σ en $S_{\Sigma'}$ hetzelfde (dwz. isomorf) zullen zijn. Immers, zo'n bijectie tussen de verzamelingen wil eigenlijk niets anders zeggen dan dat alle elementen van Σ een nieuwe naam krijgen, en het geven van bijecties in termen van de oude of de nieuwe namen komt natuurlijk

op hetzelfde neer. Wordt dit argument omgesmeed tot een formeel bewijs, dan ziet het er als volgt uit:

Stelling 4.1.3 *Stel $f : \Sigma \to \Sigma'$ is een bijectie en $g : \Sigma' \to \Sigma$ is de inverse van f (dus $f \circ g = id_{\Sigma'}$ en $g \circ f = id_{\Sigma}$). Dan zijn S_Σ en $S_{\Sigma'}$ isomorfe groepen; een expliciet isomorfisme $\varphi : S_\Sigma \to S_{\Sigma'}$ wordt gegeven door $\varphi(\sigma) = f \circ \sigma \circ g$, met als inverse $\psi : S_{\Sigma'} \to S_\Sigma$ gegeven door $\psi(\tau) = g \circ \tau \circ f$.*

Bewijs. Dit is een goede oefening in het formeel rekenen met samenstellingen van afbeeldingen, en het test meteen een aantal definities. We laten het daarom graag aan de lezer over! □

Een speciaal geval wordt gekregen door alleen naar eindige verzamelingen Σ te kijken. Tussen twee zulke verzamelingen bestaat een bijectie dan en slechts dan als ze evenveel elementen hebben. Vanwege bovenstaande stelling blijkt dus, dat wanneer symmetriegroepen van eindige verzamelingen beschouwd worden, dan is het voldoende te kijken naar $S_{\{1,2,\ldots,n\}}$. We geven nog een voorbeeld van een abstracte stelling over dit soort algemene groepen van bijecties.

Stelling 4.1.4 *(Stelling van Cayley; Arthur Cayley, engels wiskundige, 1821–1895) Elke groep G is isomorf met een ondergroep van S_G. In het speciale geval dat $\#G = n < \infty$, is dus G isomorf met een ondergroep van $S_{\{1,\ldots,n\}}$.*

Bewijs. Voor vaste $a \in G$ is de afbeelding $\lambda_a : G \to G$ gegeven door $\lambda_a(x) = ax$ een bijectie (zie Stelling 3.1.5). Dus $\lambda_a \in S_G$. Dit gebruiken we om een afbeelding

$$\varphi : G \longrightarrow S_G$$

te definiëren, namelijk $\varphi(a) = \lambda_a$. Men gaat eenvoudig na dat φ een homomorfisme is, oftewel dat $\varphi(ab) = \lambda_{ab} = \lambda_a \circ \lambda_b = \varphi(a) \circ \varphi(b)$ voor $a, b \in G$.

Verder is φ injectief, want als $a \in \mathrm{Ker}(\varphi)$, dan geldt $\lambda_a = id_G$, dus $a = ae = \lambda_a(e) = id_G(e) = e$. De conclusie is dat G isomorf is met $\varphi(G)$, en de laatstgenoemde groep is inderdaad een ondergroep van S_G.

De extra bewering voor het geval $\#G = n$ volgt direct uit het bovenstaande, samen met Stelling 4.1.3. □

4.2 Permutaties op n getallen

Definitie 4.2.1 Laat $n \in \mathbb{Z}_{\geq 1}$. De *symmetrische groep op n getallen*, notatie S_n, is per definitie de groep $S_{\{1,2,\ldots,n\}}$. Elementen van deze groep noemen we *permutaties*. S_n heet ook wel de permutatiegroep op n elementen.

Stelling 4.2.2 *De groep S_n heeft $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$ elementen.*

Bewijs. Een element van S_n is per definitie een bijectie op de verzameling $\{1, \ldots, n\}$. Zo'n bijectie wordt volledig beschreven door een rijtje van lengte n, waarin elk van de getallen $1, \ldots, n$ precies één keer voorkomt. Men gaat eenvoudig na dat er precies $n!$ zulke mogelijke rijtjes zijn. □

Definitie 4.2.3 Een permutatie $\sigma \in S_n$ heet een *cykel* van lengte k (ook wel k-cykel), als er k verschillende getallen $a_1, \ldots, a_k \in \{1, \ldots, n\}$ zijn met $\sigma(a_i) = a_{i+1}$ voor $1 \leq i < k$ en $\sigma(a_k) = a_1$ en $\sigma(x) = x$ voor $x \notin \{a_1, \ldots, a_k\}$.

Dit wordt genoteerd als $\sigma = (a_1\ a_2\ \ldots\ a_k)$.

Een 2-cykel heet ook wel een transpositie of een verwisseling.

Twee cykels $(a_1\ a_2\ \ldots\ a_k)$ en $(b_1\ b_2\ \ldots\ b_\ell)$ heten *disjunct* als $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_\ell\} = \emptyset$.

Voorbeeld 4.2.4 Er geldt $(1\ 2\ 3\ 4\ 5) = (2\ 3\ 4\ 5\ 1) = \ldots = (5\ 1\ 2\ 3\ 4)$, want deze 5-cykels sturen 5 naar 1, en i naar $i+1$ voor $1 \leq i < 5$, en ze houden de getallen ≥ 6 vast. Op dezelfde wijze geldt algemeen voor k-cykels dat $(a_1\ a_2\ \ldots\ a_k) = (a_2\ \ldots\ a_k\ a_1)$.

Twee disjuncte cykels commuteren, want zijn $(a_1\ a_2\ \ldots\ a_k)$ en $(b_1\ b_2\ \ldots\ b_\ell)$ disjunct, dan doet de ene alleen iets met de getallen $a_1, \ldots, a_k$ en de andere alleen met $b_1, \ldots, b_\ell$. Het doet er dan niet toe in welke volgorde deze cykels toegepast worden.

Voor niet-disjuncte cykels ligt dit anders: bijvoorbeeld $(1\ 2\ 3) \circ (2\ 3\ 4) \neq (2\ 3\ 4) \circ (1\ 2\ 3)$, want het eerste product beeldt 2 af op 1 en het tweede beeldt 2 af op 4. (Let op, dit is het samenstellen van functies, en daarbij wordt eerst de meest rechtse functie toegepast!)

Stelling 4.2.5 *Elk element $\sigma \in S_n$ is te schrijven als product $\sigma = \sigma_1 \ldots \sigma_r$, waarin de σ_i onderling disjuncte cykels zijn. Deze schrijfwijze is bovendien uniek op de volgorde van de cykels na.*

Bewijs. De existentie van zo'n schrijfwijze kan met inductie naar n bewezen worden. Voor $n = 1$ is de bewering duidelijk, want de enige permutatie is in dat geval $\sigma = (1)$. Laat $n > 1$, en veronderstel dat het voor alle S_m met $m < n$ waar is. Is dan $\sigma \in S_n$, dan is $\{1, \sigma(1), \sigma^2(1), \ldots\}$ een deelverzameling van $\{1, \ldots, n\}$, en dus bestaan er k, ℓ met $k < \ell$ en $\sigma^k(1) = \sigma^\ell(1)$. Bijgevolg is $\sigma^{\ell-k}(1) = 1$. Er bestaat dus een positief geheel getal s met $\sigma^s(1) = 1$. Het kleinste getal met die eigenschap noemen we q. Omdat q de kleinste is, zijn de getallen $1, \sigma(1), \ldots, \sigma^{q-1}(1)$ allemaal verschillend, en het effect van σ op deze getallen wordt precies gegeven door de k-cykel $\sigma_1 = (1\ \sigma(1)\ \ldots\ \sigma^{q-1}(1))$.

Bekijk vervolgens de overige getallen in $\{1, \ldots, n\}$. Is dit de lege verzameling dan geldt $\sigma = \sigma_1$ en we zijn klaar. Is de verzameling niet leeg, dan werkt σ er als een permutatie op. Uit de inductiehypothese volgt dat de beperking van σ tot deze verzameling te schrijven is als product van disjuncte cykels $\sigma_2 \ldots \sigma_r$. Vatten we deze cykels op als permutaties op $\{1, \ldots, n\}$, dan geldt dus $\sigma = \sigma_1 \ldots \sigma_r$.

De uniciteit is niet moeilijk te bewijzen: kan zo'n schrijfwijze op twee manieren, dan houdt dat in dat in de ene een zekere i naar een $j \neq i$ gestuurd wordt, terwijl in de andere schrijfwijze ofwel i niet voorkomt (en dan zou i op i worden afgebeeld, hetgeen niet zo is), ofwel i komt wel voor maar in de cykel waarin dat gebeurt staat achter i iets anders als j. Ook dat is niet mogelijk, want het beeld van i is j. □

Voorbeeld 4.2.6 Het bovenstaande bewijs is in feite een algorithme. Bijvoorbeeld stel we willen (1 2 3 4)(2 3 4 5)(4 5 1) als product van disjuncte cykels schrijven. Hier staat een samenstelling van afbeeldingen. We gaan eerst na wat er met 1 gebeurt. De laatstgeschreven permutatie stuurt 1 naar 4, en deze 4 wordt door de permutatie daarvóór op 5 afgebeeld. De voorste permutatie houdt 5 vast, dus het beeld van 1 is 5. Vervolgens gaan we na wat er met 5 gebeurt. De achterste stuurt 5 naar 1; deze 1 blijft vast onder de middelste en gaat dan onder de voorste naar 2. Zo voortgaande vinden we dat 4 het beeld van 2 is, en 4 wordt op 3 afgebeeld, en 3 weer op 1. Hiermee hebben we dan een 5-cykel gevonden, en omdat alleen de getallen 1 t/m 5 in de permutaties waarmee we begonnen voorkomen, zijn we dan klaar: (1 2 3 4)(2 3 4 5)(4 5 1) = (1 5 2 4 3).

De schrijfwijze van een permutatie als product van disjuncte cykels is onder andere nuttig wanneer we de orde van een permutatie willen bepalen:

Stelling 4.2.7 *1.* $(i_1\ i_2\ \ldots\ i_k)^{-1} = (i_k\ i_{k-1}\ \ldots i_1)$.

2. Een k-cykel $(i_1\ i_2\ \ldots\ i_k)$ heeft orde k.

3. Is $\sigma_1 \ldots \sigma_r$ een product van disjuncte cykels, dan geldt voor elke $n \in \mathbb{Z}$ dat $(\sigma_1 \ldots \sigma_r)^n = \sigma_1^n \ldots \sigma_r^n$.

4. Is $\sigma_1 \ldots \sigma_r$ een product van disjuncte cykels, waarbij σ_i lengte ℓ_i heeft, dan is $ord(\sigma_1 \ldots \sigma_r) = kgv(\ell_1, \ldots, \ell_r)$.

Bewijs. 1: Dit volgt direct uit de definitie van een cykel.
2: Voor $0 < n < k$ is het beeld van i_1 onder $(i_1\ i_2\ \ldots\ i_k)^n$ gelijk aan i_n. Omdat $i_n \neq i_1$ is dus de orde $\geq k$. Verder is $(i_1\ i_2\ \ldots\ i_k)^k = (1)$, dus de orde is gelijk aan k.

3: Dit volgt direct uit het feit dat disjuncte cykels onderling commuteren.
4: Er geldt vanwege 3) dat $(\sigma_1 \dots \sigma_r)^n = (1)$ precies dan als $\sigma_1^n = \dots = \sigma_r^n = (1)$. Dit is vanwege Stelling 3.2.10 het geval precies dan als n een veelvoud is van ieder van $\mathrm{ord}(\sigma_1), \dots, \mathrm{ord}(\sigma_r)$. □

Voorbeeld 4.2.8 Het is niet altijd zo dat een n-de macht van een k-cykel, met $1 < n < k$, zelf ook weer een k-cykel is. Bijvoorbeeld geldt $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$.

Voorbeeld 4.2.9 We gaan na welke getallen als ordes van een element van S_5 kunnen voorkomen. Er geldt $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Dit zijn alle schrijfwijzen van 5 als som van positieve gehele getallen. We zien hieraan dan een product van disjuncte cykels in S_5 op 7 manieren tot stand kan komen: een 5-cykel, of een 4-cykel (maal een 1-cykel, maar die laten we weg), of ... enz. Uit Stelling 4.2.7 volgt dat de ordes van deze producten respectievelijk $5, 4, 6, 3, 2$ en 1 zijn. Het is voor elk van die ordes een eenvoudig combinatorisch probleem om te bepalen hoeveel elementen er precies met die orde zijn.

Stelling 4.2.10 *Elke $\sigma \in S_n$ is te schrijven als product van 2-cykels.*

Bewijs. We weten al dat we σ als product van cykels kunnen schrijven. Het is dus voldoende te bewijzen, dat een cykel te schrijven is als product van 2-cykels. Welnu, er geldt

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_2\ a_3)\dots(a_{k-1}\ a_k)$$

zoals men eenvoudig narekent. □

Opmerking 4.2.11 Stelling 4.2.10 zegt eigenlijk, dat we door herhaald paren getallen te verwisselen, een rij van n getallen in een willekeurige volgorde kunnen plaatsen. Uit het bewijs krijgen we zelfs een bovengrens voor het aantal verwisselingen waarmee dit bereikt wordt: ga uit van een schrijfwijze van onze permutatie als product van r disjuncte ℓ_i-cykels, met $\ell_i \geq 1$ en $\sum \ell_i = n$. Dan zijn voor zo'n ℓ_i-cykel blijkens het bewijs van Stelling 4.2.10 niet meer dan $\ell_i - 1$ verwisselingen nodig. In totaal kunnen we dus volstaan met $\sum(\ell_i - 1) = n - r$ verwisselingen.

Opmerking 4.2.12 Men kan zelfs eenvoudig laten zien dat elke permutatie te schrijven is als product van verwisselingen van een bepaalde eenvoudige gedaante. Bijvoorbeeld, als product van zogenaamde 'buurverwisselingen'. Dit zijn 2-cykels van de gedaante $(i\ i+1)$. Is $i < j$, dan is

$$(i\ j) = (i\ i+1)(i+1\ i+2)\dots(j-1\ j)(j-2\ j-1)\dots(i\ i+1).$$

Hieruit volgt de schrijfwijze direct.

Men kan ook elke permutatie schrijven als product van 2-cykels van de vorm $(1\ i)$. Dit volgt voor $1 \neq i \neq j \neq 1$ uit het feit dat $(i\ j) = (1\ i)(1\ j)(1\ i)$. In de overige gevallen is er niets te bewijzen. Anders gezegd: door alleen maar één vast element met andere(n) te verwisselen, kan een rij getallen in een willekeurige volgorde worden gezet.

Merk op dat de schrijfwijze als product van 2-cykels beslist niet uniek is! We zullen echter zien, dat het aantal benodigde 2-cykels voor een gegeven permutatie hooguit een *even* aantal verschilt. Met andere woorden, is σ een product van k verwisselingen en ook een product van ℓ verwisselingen, dan geldt $2|(k-\ell)$. We bewijzen dit in de nu volgende §.

4.3 Even en oneven permutaties

Definitie 4.3.1 Met X duiden we de verzamelingen paren gehele getallen (i,j) aan waarvoor geldt $1 \leq i < j \leq n$. Verder noteren we voor $\sigma \in S_n$ de afbeelding $f_\sigma : X \to X$, gegeven door $f_\sigma(i,j) = (\sigma(i), \sigma(j))$ als $\sigma(i) < \sigma(j)$, terwijl $f_\sigma(i,j) = (\sigma(j), \sigma(i))$ als $\sigma(i) > \sigma(j)$.

Tenslotte definiëren we $h_\sigma : X \to \mathbb{Q}$ door $h_\sigma(i,j) = \dfrac{\sigma(j) - \sigma(i)}{j - i}$.

De eigenschappen van de hier gegeven functies die we zullen gebruiken staan opgesomd in:

Lemma 4.3.2 *1. Voor $\sigma, \tau \in S_n$ geldt $f_{\sigma\tau} = f_\sigma \circ f_\tau$.*

2. f_σ is een bijectie op X.

3. $\displaystyle\prod_{(i,j)\in X} h_\sigma(i,j) = \pm 1.$

Bewijs. 1: Beide functies sturen een willekeurige $(i,j) \in X$ naar ofwel $(\sigma\tau(i), \sigma\tau(j))$, ofwel $(\sigma\tau(j), \sigma\tau(i))$ (afhankelijk welke van deze twee in X zit). Dus zijn de functies gelijk.
2: Er geldt $f_\sigma \circ f_{\sigma^{-1}} = f_{\sigma^{-1}} \circ f_\sigma = f_{id} = id$.
3: In absolute waarde is het gegeven product gelijk aan

$$\left(\prod_{(i,j)\in X} |\sigma(j) - \sigma(i)| \right) \ / \ \left(\prod_{(i,j)\in X} (j-i) \right).$$

De teller hier is precies gelijk aan het product van alle $(\ell - k)$, voor $(k,\ell) = f_\sigma(i,j) \in f_\sigma(X) = X$. Dus teller en noemer zijn gelijk. Omdat het product in absolute waarde dus gelijk is aan 1, is het zelf ± 1. □

Definitie 4.3.3 Het *teken* van een permutatie $\sigma \in S_n$, notatie $\epsilon(\sigma)$, is per definitie

$$\epsilon(\sigma) = \prod_{(i,j)\in X} h_\sigma(i,j) = \prod_{1\le i<j\le n)} \frac{\sigma(j)-\sigma(i)}{j-i} = \pm 1.$$

We noemen σ *even* als $\epsilon(\sigma) = 1$ en *oneven* als $\epsilon(\sigma) = -1$.

Opmerking 4.3.4 We zullen hierna een efficiënte manier afleiden om het teken van een permutatie te vinden. Met de gegeven definitie is dat in het algemeen een heel werk; probeer bijvoorbeeld maar eens met de definitie het teken van de 3-cykel (1 3 5) te vinden!

We kunnen het teken van een permutatie als volgt interpreteren: in de noemer van de uitdrukking waarmee het teken wordt gedefiniëerd, staat een product van positieve getallen. De getallen in de teller zijn van de vorm $\sigma(j) - \sigma(i)$, en zo'n getal is negatief precies dan als σ de getallen i en j overbrengt naar een paar dat ten aanzien van de gewone 'kleiner dan'-relatie op $\{1,\ldots,n\}$ in de andere volgorde staat dan i, j. Gebeurt dit voor een *even* aantal $(i,j) \in X$, dan is het teken $\epsilon(\sigma) = 1$; gebeurt het een *oneven* aantal keren, dan heeft σ teken -1.

De verzameling $\{+1,-1\}$ is ten aanzien van de gewone vermenigvuldiging een groep. Dus ϵ is een afbeelding van de groep S_n naar de groep ± 1.

Stelling 4.3.5 *Het teken $\epsilon : S_n \longrightarrow \pm 1$ is een homomorfisme.*

Bewijs. Laat $\sigma, \tau \in S_n$. Er geldt

$$\prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} = \prod_{(i,j)\in X} h_\sigma(f_\tau(i,j)) = \prod_{(i,j)\in X} h_\sigma(i,j) = \epsilon(\sigma),$$

omdat f_σ op X bijectief is (Lemma 4.3.2). Dus volgt

$$\begin{aligned}\epsilon(\sigma\tau) &= \textstyle\prod_{(i,j)\in X} \frac{(\sigma\tau)(j)-(\sigma\tau)(i)}{j-i} \\ &= \left(\textstyle\prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\right)\left(\textstyle\prod_{(i,j)\in X} \frac{\tau(j)-\tau(i)}{j-i}\right) \\ &= \epsilon(\sigma)\epsilon(\tau).\end{aligned}$$

Dit bewijst de stelling. □

Om met behulp van dit resultaat het teken van permutaties te kunnen berekenen, bewijzen we eerst een lemma. Het eerste deel van dit lemma is ook voor het aantonen van heel andere eigenschappen van permutaties later nog van belang.

Lemma 4.3.6 *1. Is* $\tau, (a_1 \ a_2 \ \ldots \ a_\ell) \in S_n$, *dan geldt* $\tau(a_1 \ a_2 \ \ldots \ a_\ell)\tau^{-1} = (\tau(a_1) \ \tau(a_2) \ \ldots \ \tau(a_\ell))$.

2. Voor een 2-cykel $(a_1 \ a_2)$ *geldt* $\epsilon((a_1 \ a_2)) = -1$.

Bewijs. 1: Neem $i \in \{1, \ldots, n\}$. Als $i = \tau(a_\ell)$, dan $(\tau(a_1 \ a_2 \ \ldots \ a_\ell)\tau^{-1})(i) = (\tau(a_1 \ a_2 \ \ldots \ a_\ell))(a_\ell) = \tau(a_1)$. Evenzo, als $i = \tau(a_k)$ met $1 \leq k < \ell$, dan volgt $(\tau(a_1 \ a_2 \ \ldots \ a_\ell)\tau^{-1})(i) = \tau(a_{k+1})$. Voor alle overige i geldt $(\tau(a_1 \ a_2 \ \ldots \ a_\ell)\tau^{-1})(i) = i$. Dit bewijst de gevraagde gelijkheid.
2: Kies een permutatie τ waarvoor geldt $\tau(a_1) = 1$ en $\tau(a_2) = 2$. Dan $\epsilon((1 \ 2)) = \epsilon(\tau(a_1 \ a_2)\tau^{-1})$. Omdat ϵ een homomorfisme is, is verder $\epsilon(\tau(a_1 \ a_2)\tau^{-1}) = \epsilon(\tau)\epsilon((a_1 \ a_2))\epsilon(\tau)^{-1} = \epsilon((a_1 \ a_2))$. Dus iedere 2-cykel heeft hetzelfde teken. Voor (1 2) is dat eenvoudig met de definitie te berekenen: $\epsilon((1 \ 2)) = -1$, want het enige paar $(i, j) \in X$ dat onder (1 2) van volgorde wisselt, is $(1, 2)$. □

Gevolg 4.3.7 *1. Een* ℓ*-cykel* σ *heeft teken* $\epsilon(\sigma) = (-1)^{\ell-1}$.

2. Is σ *een product van cykels van lengte* $\ell_1, \ldots, \ell_r$, *dan* $\epsilon(\sigma) = (-1)^{\sum_{i=1}^{r}(\ell_i - 1)}$.

3. Een permutatie σ *is even dan en slechts dan als* σ *te schrijven is als een product van een even aantal 2-cykels.*

Bewijs. 1: Er geldt $(a_1 \ a_2 \ \ldots \ a_\ell) = (a_1 \ a_2)(a_2 \ a_3) \ldots (a_{\ell-1} \ a_\ell)$. Het aantal 2-cykels hier is $\ell - 1$, dus omdat ieder van deze teken -1 heeft en omdat ϵ een homomorfisme is, volgt het gevraagde.
2: Volgt direct uit 1) vanwege het feit dat ϵ een homomorfisme is.
3: Laat $\sigma \in S_n$. Wegens Stelling 4.2.10 is σ te schrijven als product van 2-cykels. De bewering volgt dan uit wat zojuist in 2) bewezen is. □

4.4 De alternerende groep

Definitie 4.4.1 Voor $n \geq 1$ is de *alternerende groep* (notatie: A_n) de ondergroep van S_n bestaande uit alle even permutaties.

Dat A_n inderdaad een groep is, volgt bijvoorbeeld uit het feit dat $A_n = \mathrm{Ker}(\epsilon)$, en ϵ is een homomorfisme (Stellingen 4.3.5 en 3.3.6).

Voorbeeld 4.4.2 In S_2 hebben we alleen de permutaties (1) en (1 2). Dus A_2 bestaat uit alleen maar de identiteit.

S_3 bestaat uit de identiteit, 2-cykels en 3-cykels. Alleen de 2-cykels zitten niet in A_3, dus $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$. Deze groep is isomorf met $\mathbb{Z}/3\mathbb{Z}$.

In A_4 zitten naast de identiteit de 3-cykels (dat zijn er 8) en de producten van twee disjuncte 2-cykels (dat zijn er 3). De zo verkregen groep is niet abels, en bestaat uit 12 elementen.

Stelling 4.4.3 *Voor $n \geq 2$ heeft A_n precies $n!/2$ elementen.*

Bewijs. De verzamelingen A_n en $(S_n \setminus A_n)$ zijn per definitie disjunct, en ze vormen samen de hele S_n. Verder hebben ze evenveel elementen, want de afbeelding $\tau \mapsto (1\ 2)\tau$ is een bijectie van de ene naar de andere. Hieruit volgt de stelling. □

Stelling 4.4.4 *Elk element van A_n is te schrijven als een product van 3-cykels.*

Bewijs. Neem $\sigma \in A_n$. Vanwege Gevolg 4.3.7 is σ te schrijven als product van een even aantal 2-cykels. In het bijzonder dus als product van permutaties van de vorm $(a\ b)(c\ d)$. Vanwege $(a\ c\ b)(c\ d\ a) = (a\ b)(c\ d)$ volgt dan de stelling (ga zelf na hoe dit argument aangepast dient te worden als bijvoorbeeld $a = c$). □

Voorbeeld 4.4.5 We geven tenslotte een voorbeeld bij de stelling van Cayley die aan het begin van dit hoofdstuk werd bewezen (Stelling 4.1.4). Neem $G = (\mathbb{Z}/8\mathbb{Z})^*$. Omdat $\#G = \varphi(8) = 4$, is G isomorf met een ondergroep van S_4. We gaan na welke ondergroep het bewijs van Stelling 4.1.4 ons daarvoor geeft, en we zien dan meteen dat zelfs G als ondergroep van A_4 is op te vatten. In het genoemde bewijs wordt $a \in G$ geïdentificeerd met λ_a, het van links met a vermenigvuldigen. Bovendien wordt S_G met S_4 geïdentificeerd, en dat gaat door gewoon een bijectie tussen G en $\{1, 2, 3, 4\}$ te kiezen. Welnu, voor deze bijectie nemen we $\overline{1} \mapsto 1, \overline{3} \mapsto 2, \overline{5} \mapsto 3$ en $\overline{7} \mapsto 4$.

Het element $\overline{1} \in G$ levert $\lambda_{\overline{1}} = id_G$, dus dat wordt de permutatie (1). Het element $\overline{3}$ levert de bijectie op G die $\overline{1}$ naar $\overline{3}$, $\overline{3}$ naar $\overline{3}\cdot\overline{3} = \overline{1}$, $\overline{5}$ naar $\overline{3}\cdot\overline{5} = \overline{7}$ en $\overline{7}$ naar $\overline{5}$ stuurt. Met onze bijectie tussen G en $\{1, 2, 3, 4\}$ wordt dat dus de permutatie $(1\ 2)(3\ 4)$.

Een zelfde berekening stuurt $\overline{5}$ naar de permutatie $(1\ 3)(2\ 4)$ en $\overline{7}$ naar $(1\ 4)(2\ 3)$. Dus kennelijk is $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ een ondergroep van S_4, isomorf met $(\mathbb{Z}/8\mathbb{Z})^*$. Het is duidelijk dat deze ondergroep zelfs in A_4 zit.

4.5 Opgaven

1. Schrijf de volgende permutaties als product van disjuncte cykels:
   (a) $(3\ 1\ 4)(1\ 5\ 9\ 2\ 6)(5\ 3)$
   (b) σ^{-1}, waarbij $\sigma = (5\ 6\ 2)(1\ 3)(1\ 4)$.

2. (a) Vind alle $\sigma \in S_4$ die voldoen aan $\sigma^2 = (1\ 2)(3\ 4)$.
   (b) Laat $n > 1$. Bestaat er een $\sigma \in S_n$ met $\sigma^2 = (1\ 2)$?
   (c) Laat $n \geq 6$. Bestaat er een $\sigma \in S_n$ waarvoor $\sigma^2 = (1\ 2)(3\ 4\ 5\ 6)$?

3. Stel dat σ een k-cykel is. Bewijs dat σ^n ook een k-cykel is dan en slechts dan als $\text{ggd}(k, n) = 1$.

4. Bepaal welke getallen voorkomen als de orde van een element van S_6, en ga voor elk van deze getallen na hoeveel elementen met die orde er in S_6 zitten.

5. Wat is de kleinste n waarvoor $\#S_n$ deelbaar is door 30? En wat is de kleinste n waarvoor S_n een element van orde 30 bevat?

6. Bepaal de orde van $(5\ 6\ 7\ 8\ 9)(3\ 4\ 5\ 6)(2\ 3\ 4)(1\ 2)$ in de groep S_9. Is dit een even of een oneven permutatie?

7. (a) Bepaal σ^{1999} voor $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10)$.
   (b) Bereken ook τ^{1995} voor $\tau = (1\ 2\ 3)(3\ 4)(4\ 5\ 6\ 7)$.

8. Laat $\sigma \in S_n$. Bewijs dat als $\sigma(1\ 2\ \ldots\ n) = (1\ 2\ \ldots\ n)\sigma$, dan is $\sigma = (1\ 2\ \ldots\ n)^i$ voor zekere i.

9. Bepaal voor $n \geq 1$ het centrum $\mathcal{Z}(S_n)$ van S_n (dat zijn de permutaties τ met de eigenschap $\sigma\tau = \tau\sigma$ voor elke $\sigma \in S_n$).

10. Laat $\sigma, \tau \in S_n$. Toon aan dat als σ een product is van disjuncte cykels van lengtes $\ell_1, \ldots, \ell_r$, dan is $\tau\sigma\tau^{-1}$ dat ook.

11. (a) Laat $a \neq 1 \neq b$ en bereken $(1\ a)(1\ b)(1\ a)(1\ b)$.
    (b) Toon aan dat elk element van A_n te schrijven is als een product van elementen van de vorm $\sigma\tau\sigma^{-1}\tau^{-1}$, voor $\sigma, \tau \in S_n$.
    (c) Bewijs dat als G een abelse groep is, en $f : S_n \to G$ een homomorfisme, dan geldt $A_n \subset \text{Ker}(f)$.
    (d) Bewijs dat als $g : S_n \to S_m$ een homomorfisme is, dan is $g(A_n) \subset A_m$.

12. Een ondergroep H van S_n heet *transitief* als er voor elk paar $\{i, j\} \subset \{1, 2, \ldots, n\}$ een $\tau \in H$ is met $\tau(i) = j$.

    (a) Toon aan dat voor $n \geq 3$ de groep A_n een transitieve ondergroep van S_n is.

    (b) Toon aan dat als G een groep is met $\#G = n$, dan is de ondergroep van S_n die in het bewijs van de stelling van Cayley wordt geconstrueerd en waarmee G isomorf is, een transitieve ondergroep van S_n.

    (c) Vind met behulp van de stelling van Cayley een transitieve ondergroep van S_6 die isomorf is met S_3.

5 Groepen van symmetrieën

In dit hoofdstuk worden bepaalde soorten groepen van bijecties beschouwd. Steeds zal het gaan om bijecties waaraan bepaalde extra eisen zijn opgelegd. Het is vooral dit type groepen dat in de natuurkunde, maar ook in bijvoorbeeld de discrete wiskunde een rol speelt. De begrippen uit de lineaire algebra die in dit hoofdstuk gebruikt worden, zijn in vrijwel ieder boek over dat onderwerp terug te vinden. Bijvoorbeeld komen ze aan de orde in Hoofdstuk 6 van het boek S.H. Friedberg, A.J. Insel en L.E. Spence, Linear Algebra (2nd edition), London etc.: Prentice-Hall, 1989.

5.1 een aantal matrixgroepen

De ruimte $\mathbb{R}^2$ kunnen we visualiseren als een plat vlak. De standaardmanier om dit te doen wordt al heel vroeg op de middelbare school aangeleerd. Met behulp van de stelling van Pythagoras stelt deze standaard-interpretatie ons vervolgens in staat, een afstandbegrip d op $\mathbb{R}^2$ in te voeren:

$$d(\ (a,b)\ ,\ (c,d)\ ) = \sqrt{(a-c)^2 + (b-d)^2}.$$

Iets analoogs leren we dan voor $\mathbb{R}^3$, en later in de lineaire algebra wordt dit ineens vergaand gegeneraliseerd tot de situatie van een (reële of complexe) lineaire ruimte V voorzien van een inproduct $\langle\ \cdot\ ,\ \cdot\ \rangle$. In dit laatste geval wordt de afstand $d(v,w)$ tussen twee vectoren $v, w \in V$ gedefiniëerd als

$$d(v,w) = ||v-w|| = \sqrt{\langle v-w, v-w\rangle}.$$

Bij een dergelijke inproductruimte hoort, althans in het eindig-dimensionale geval, een groep:

Definitie 5.1.1 Laat V een eindig-dimensionale lineaire ruimte over $\mathbb{R}$ of $\mathbb{C}$ zijn, voorzien van een inproduct $\langle\ \cdot\ ,\ \cdot\ \rangle$. Met $O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ duiden we de verzameling van alle lineaire afbeeldingen $\varphi\ :\ V \to V$ aan, die voldoen aan $\langle v,w\rangle = \langle \varphi(v), \varphi(w)\rangle$ voor elk paar $v, w \in V$.

Stelling 5.1.2 *In de situatie van Definitie 5.1.1 is $O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ ten aanzien van het samenstellen van lineaire afbeeldingen een groep, met als eenheidselement id_V.*

Bewijs. We tonen eerst aan dat $O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ een deelverzameling is van de groep van *alle* inverteerbare lineaire afbeeldingen van V naar zichzelf $\mathrm{GL}(V)$. Daarvoor is het voldoende, aan te tonen dat de elementen van

$O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ inverteerbaar zijn. Stel $\varphi \in O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$. Is $\varphi(v) = 0$, dan volgt $\langle v, v\rangle = \langle \varphi(v), \varphi(v)\rangle = 0$, en dus $v = 0$. Dit impliceert dat φ injectief is, en dus, omdat injectieve lineaire afbeeldingen van een eindig-dimensionale ruimte naar zichzelf automatisch ook surjectief zijn, is φ inverteerbaar.

Om nu aan te tonen dat $O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ een groep als boven beschreven is, volstaat het om te laten zien dat het een ondergroep van $\mathrm{GL}(V)$ is. Dit laten we met behulp van Stelling 3.2.3 als oefening aan de lezer over. □

Is $A = (a_{i,j})$ een (vierkante) matrix met reële of complexe coëfficiënten, dan wordt in de lineaire algebra de geadjungeerde van A, notatie A^*, gedefiniëerd als $A^* = (b_{i,j})$, met $b_{i,j} = \overline{a_{j,i}}$. Dus, om A^* te krijgen worden alle getallen in de matrix gespiegeld ten aanzien van de hoofddiagonaal, en vervolgens complex geconjugeerd. Wordt een $\varphi \in \mathrm{GL}(V)$ ten aanzien van een orthonormale basis voor V gegeven door een matrix A, dan geldt $\varphi \in O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ dan en slechts dan als $A^*A = I$, waarin I de eenheidsmatrix voorstelt. Dit vertaalt dus de groep $O(V, \langle\ \cdot\ ,\ \cdot\ \rangle)$ in een groep van matrices, om precies te zijn, een ondergroep van $\mathrm{GL}_n(\mathbb{R})$ of $\mathrm{GL}_n(\mathbb{C})$, voor $n = \dim(V)$. Een opsomming van de zo gegeven groepen van matrices, en wat relevante ondergroepen, volgt nu.

Definitie 5.1.3 Laat $n \in \mathbb{Z}, n > 0$.

1. De *orthogonale* groep $\mathrm{O}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^*A = I\}$.
2. De *unitaire* groep $\mathrm{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^*A = I\}$.
3. De *speciale orthogonale* groep $\mathrm{SO}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^*A = I \text{ en } \det(A) = 1\}$.
4. De *speciale unitaire* groep $\mathrm{SU}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^*A = I \text{ en } \det(A) = 1\}$.

Voorbeeld 5.1.4 Is $n = 1$, dan krijgen we $\mathrm{O}(1) = \{a \in \mathbb{R} \setminus \{0\} \mid a^2 = 1\} = \{\pm 1\}$. Als groep van afbeeldingen op $\mathbb{R}$ stelt dit de identiteit, en 'tegengestelde nemen' voor. De groepen $\mathrm{SO}(1)$ en $\mathrm{SU}(1)$ zijn beide de triviale groep bestaande uit slechts één element. $\mathrm{U}(1)$ is al interessanter: dit is de groep van punten op de eenheidscirkel in $\mathbb{C}$, met als groepswet de vermenigvuldiging.

Voor $n = 2$ bestaat $\mathrm{SO}(2)$ precies uit alle matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, met $a, b, c, d \in \mathbb{R}$ en $a^2 + c^2 = b^2 + d^2 = ad - bc = 1$ en $ab + cd = 0$. Schrijven we $a = \cos\alpha$ en $c = \sin\alpha$, dan volgt $d = \cos\alpha$ en $b = -\sin\alpha$. Met andere woorden, als afbeelding van $\mathbb{R}^2$ naar zichzelf stelt onze matrix een rotatie over de

hoek α met als centrum de oorsprong voor. De groep SO(2) is precies de groep van al deze rotaties.

In de groep O(2) komen naast de matrices uit SO(2) ook degenen van de gedaante $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ -\sin\alpha & -\cos\alpha \end{pmatrix}$ voor. Meetkundig representeert dit een spiegeling in de lijn door de oorsprong, die de positieve x-as snijdt onder een hoek $-\alpha/2$. We concluderen dus dat O(2) gezien als groep van meetkundige afbeeldingen bestaat uit alle rotaties met de oorsprong als centrum, plus alle spiegelingen in lijnen door de oorsprong. Deze groep is dus niet commutatief, want als we bijvoorbeeld eerst spiegelen in de x-as en dan draaien over een hoek van 90 graden, dan is $(0,1)$ het beeld van $(1,0)$. Passen we deze twee afbeeldingen evenwel in de omgekeerde volgorde toe, dan wordt $(1,0)$ afgebeeld op $(0,-1)$.

Al de in Definitie 5.1.3 genoemde groepen kunnen worden gezien als groepen bestaande uit inverteerbare lineaire afbeeldingen van $\mathbb{R}^n$ of $\mathbb{C}^n$ naar zichzelf, met de eigenschap dat ze het standaardinproduct, en dus ook de afstanden tussen punten, vast houden.

We zullen ons vanaf nu beperken tot het reële geval, en met name tot $\mathbb{R}^2$ en $\mathbb{R}^3$. Meetkundig betekent het feit dat een afbeelding afstandbehoudend is, dat bijvoorbeeld een driehoek wordt overgevoerd in een daarmee congruente driehoek. Immers, de drie hoekpunten worden afgebeeld op drie nieuwe punten met onderling dezelfde afstand, en een punt op een zijde moet gaan naar een punt dat dezelfde afstanden tot de nieuwe hoekpunten heeft, als het oorspronkelijke punt tot de oude hoekpunten. Daaruit volgt dat zijden van de driehoek op zijden worden afgebeeld. Dit argument laat zien dat in het algemeen afstandbehoudende afbeeldingen (we hoeven geen lineariteit te eisen) lijnen in lijnen en hoeken in even grote hoeken overvoeren.

5.2 groepen van isometrieën

Zoals al gezegd, werken we steeds met de ruimte $\mathbb{R}^n$, voorzien van de 'gewone' norm $||(a_1,\ldots,a_n)|| = \sqrt{a_1^2 + \ldots a_n^2}$ en het gewone afstandsbegrip $d(v,w) = ||v-w||$ voor $v,w \in \mathbb{R}^n$.

Definitie 5.2.1 Een *isometrie* op $\mathbb{R}^n$ is een afbeelding $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ die voldoet aan $d(v,w) = d(\varphi(v),\varphi(w))$ voor alle $v,w \in \mathbb{R}^n$.

Voorbeeld 5.2.2 Voorbeelden van isometrieën zijn translaties, rotaties, spiegelingen in een punt of in een lijn of in een vlak.

Stelling 5.2.3 *1. Een isometrie op $\mathbb{R}^n$ die $0 \in \mathbb{R}^n$ op 0 afbeeldt, is een lineaire afbeelding.*

2. *Elke isometrie is te schrijven als samenstelling van translatie met een lineaire isometrie.*

3. *Isometrieën zijn inverteerbaar.*

Bewijs. 1: Er geldt $||u-v||^2 = \langle u-v, u-v\rangle = ||u||^2 + ||v||^2 - 2\langle u, v\rangle$ voor $u, v \in \mathbb{R}^n$. Is φ een isometrie en $\varphi(0) = 0$, dan volgt

$$\begin{aligned} 2\langle u, v\rangle &= ||u-0||^2 + ||v-0||^2 - ||u-v||^2 \\ &= ||\varphi(u)-\varphi(0)||^2 + ||\varphi(v)-\varphi(0)||^2 - ||\varphi(u)-\varphi(v)||^2 \\ &= 2\langle \varphi(u), \varphi(v)\rangle. \end{aligned}$$

Hieruit volgt met wat rekenwerk dat $||\varphi(u+av) - \varphi(u) - a\varphi(v)||^2 = 0$ voor $a \in \mathbb{R}$, en dat impliceert dat φ lineair is.
2: Laat φ een isometrie zijn. Schrijf $v = \varphi(0)$. Definieer $\tau_v : \mathbb{R}^n \to \mathbb{R}^n$ als transleren over v, dus $\tau_v(w) = v + w$ voor $w \in \mathbb{R}^n$. Definieer tenslotte $\psi : \mathbb{R}^n \to \mathbb{R}^n$ door $\psi(w) = \varphi(w) - v$. Dan zijn τ_v, ψ isometrieën, en omdat $\psi(0) = 0$, volgt uit 1) dat ψ lineair is. Er geldt $\varphi(w) = \varphi(w) - v + v = \psi(w) + v = \tau_v(\psi(w))$ voor elke $w \in \mathbb{R}^n$, met andere woorden $\varphi = \tau_v \circ \psi$.
3: Wegens 2) en het feit dat een samenstelling van bijecties weer een bijectie is, is het voldoende om aan te tonen dat zowel translaties als lineaire isometrieën inverteerbaar zijn. Voor translaties is dit duidelijk, en voor lineaire isometrieën is dit in het bewijs van Stelling 5.1.2 al aangetoond. □

De lineaire isometrieën genoemd in bovenstaande stelling worden in de lineaire algebra meestal orthogonale (lineaire) afbeeldingen genoemd. In het geval van $\mathbb{R}^2$ hebben we al deze afbeeldingen al in Voorbeeld 5.1.4 bepaald: het zijn de spiegelingen in een lijn door de oorsprong, en de rotaties om de oorsprong. We gaan nu bepalen hoe dit voor $\mathbb{R}^3$ zit. In feite werkt het hierna gegeven bewijs voor willekeurige reële inproductruimten.

Stelling 5.2.4 *Is φ een orthogonale afbeelding op $\mathbb{R}^3$ met $\det(\varphi) = \epsilon$, dan geldt $\epsilon = \pm 1$.*

Verder zijn er een lijn L door de oorsprong, en een vlak V door de oorsprong loodrecht op L, waarvoor geldt dat φ zowel L als V naar zichzelf afbeeldt.

φ werkt op V als een rotatie, en op L als vermenigvuldiging met ϵ.

Meetkundig gezien zegt dit resultaat heel precies hoe een orthogonale afbeelding op $\mathbb{R}^3$ eruitziet: is de determinant 1, dan is het een draaiing 'om een lijn L'. Is de determinant -1, dan draaien we niet alleen om een lijn L, maar bovendien spiegelen we in het vlak V loodrecht op L. Hoe we dat vlak V en

die lijn L en de hoek waarover geroteerd wordt kunnen bepalen, zal blijken uit het bewijs dat nu gegeven wordt.

Bewijs. Ten aanzien van de standaardbasis voor $\mathbb{R}^3$ wordt de orthogonale afbeelding φ gegeven door een 3×3-matrix A. Deze matrix voldoet aan $A^*A = I$. Omdat $\det(A) = \det(A^*)$, volgt dan $\epsilon^2 = \det(A)^2 = \det(A^*A) = \det(I) = 1$ en dus $\epsilon = \pm 1$.

Het eigenwaardenpolynoom van A heeft graad 3, en dus heeft dit polynoom minstens één reëel nulpunt, dat we λ noemen. Dit is dan een eigenwaarde van φ bij een eigenvector v. Omdat φ afstandbehoudend is, geldt $||v|| = ||\varphi(v)|| = ||\lambda v|| = |\lambda| \cdot ||v||$, dus $\lambda = \pm 1$. Laat W het vlak door de oorsprong loodrecht op v zijn. We beweren dat φ dit vlak op zichzelf afbeeldt. Immers, laat $w \in W$ willekeurig. We moeten aantonen dat $\varphi(w) \in W$, hetgeen precies wil zeggen dat $\varphi(w) \perp v$. Welnu, $\varphi^*\varphi = id$ en $\lambda = \pm 1$, en dus volgt door φ^* toe te passen op $v = \lambda\varphi(v)$ dat $\varphi^*(v) = \lambda v$. Dus $\langle \varphi(w), v \rangle = \langle w, \varphi^*(v) \rangle = \lambda \langle w, v \rangle = 0$, hetgeen we wilden laten zien.

De beperking van φ tot W is natuurlijk evenals φ zelf weer afstandbehoudend. Er zijn nu twee mogelijkheden voor deze beperking: het kan een rotatie zijn, en een spiegeling in een lijn in W door de oorsprong. In het geval van een rotatie zijn we direct klaar: ten aanzien van een basis van $\mathbb{R}^3$ bestaande uit de vector v samen met twee onderling loodrechte vectoren in W met lengte 1 wordt φ dan namelijk gegeven door een matrix $B = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$. Dan is $\epsilon = \det(A) = \det(B) = \lambda$ en we nemen $L =$ de lijn door v en de oorsprong, en $V = W$.

Is de beperking van φ tot W een spiegeling, neem dan w_1 een vector met lengte 1 op de lijn waarin gespiegeld wordt, en w_2 een vector in W met lengte 1 loodrecht op w_1. Dan ziet ten aanzien van de basis v, w_1, w_2 voor $\mathbb{R}^3$ de matrix van φ eruit als $C = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Dus is $\epsilon = -\lambda$. Is $\lambda = 1$, dan kiezen we voor V het vlak door v en w_1, en voor L de lijn door w_2. (Dit correspondeert dus met de spiegeling in V.) Is $\lambda = -1$, dan wordt V het vlak door v en w_2, en L de lijn door w_1. (Dit levert dan draaien over 180 graden 'om de lijn L'.) □

Definitie 5.2.5 Is F een deelverzameling van $\mathbb{R}^n$, dan is de verzameling van alle isometrieën op $\mathbb{R}^n$ die de eigenschap hebben dat ze F weer naar F afbeelden een groep. Immers, men gaat eenvoudig na dat het een ondergroep is van de groep van *alle* isometrieën. Dit heet *de symmetriegroep van F*.

Het blijkt dat op isomorfie na de symmetriegroep van een verzameling F niet afhangt van *waar* F in $\mathbb{R}^n$ ligt, alleen maar van 'hoe F eruitziet':

Stelling 5.2.6 *Is $F \subset \mathbb{R}^n$, $a \in \mathbb{R}_{>0}$ en φ een isometrie op $\mathbb{R}^n$, dan is de symmetriegroep van $a\varphi(F)$ isomorf met die van F.*

Bewijs. De afbeelding $\sigma \mapsto a\varphi\sigma\varphi^{-1}\frac{1}{a}$ beeldt de symmetriegroep van F af op die van $a\varphi(F)$ (vergelijk ook Opgave 4), en deze afbeelding is een homomorfisme. De afbeelding is bovendien bijectief, want een inverse wordt gegeven door $\tau \mapsto \varphi^{-1}\frac{1}{a}\tau a\varphi$ zoals men eenvoudig narekent. □

We zullen nu voor een aantal deelverzamelingen van $\mathbb{R}^2$ en $\mathbb{R}^3$ de zo verkregen groep van symmetrieën beschrijven. Het volgende hulpresultaat speelt daarbij een rol:

Lemma 5.2.7 *Is G een ondergroep van $SO(2)$ bestaande uit precies N elementen, dan bestaat G precies uit alle rotaties over een veelvoud van $2\pi/N$ radialen. In het bijzonder geldt dus $G \cong \mathbb{Z}/N\mathbb{Z}$.*

Bewijs. Ieder element van SO(2), en dus in het bijzonder ook ieder element van G, is een rotatie. Laat σ het element van G zijn dat draaien over een zo klein mogelijke positieve hoek $2\pi\alpha$ voorstelt. Omdat G eindig is, geldt $\sigma^n = id$ voor zekere $n > 0$, en dus is $n \cdot 2\pi\alpha$ een geheel veelvoud van 2π. Dit impliceert dat $\alpha \in \mathbb{Q}$, dus we kunnen schrijven $\alpha = a/b$ voor gehele, positieve a, b met $\mathrm{ggd}(a, b) = 1$. Kies $c, d \in \mathbb{Z}$ met $ac + bd = 1$, dan is σ^c de rotatie over $2\pi ac/b = 2\pi(1 - bd)/b$, oftewel over een hoek $2\pi/b$. Omdat $2\pi a/b$ de kleinste positieve hoek is waarover door een element van G geroteerd wordt, moet dus $a = 1$. We laten nu zien dat $b = N$. Neem een willekeurige draaiing $\tau' \in G$ over een hoek $2\pi\ell/m$. Precies zoals we dat zojuist voor σ gedaan hebben, vinden we een macht τ van τ' die roteren over $2\pi/m$ weergeeft. Er geldt dat τ' een macht van σ is dan en slechts dan als dat zo is voor τ. Door een geschikte combinatie $\sigma^p\tau^q$ te nemen, vinden we een element van G dat een rotatie over $2\pi/\mathrm{kgv}(b, \ell)$ is. De minimaliteit van $2\pi/b$ levert dan dat $\mathrm{kgv}(b, \ell) \leq b$, en dus $\ell | b$. Dit toont aan dat ieder element van G een macht van σ is. Dus $N = \#G = \mathrm{ord}(\sigma) = b$, en het lemma is bewezen.

Een alternatief, veel meetkundiger bewijs kan als volgt gevonden worden. Neem een cirkel met als middelpunt de oorsprong, en een punt daarop. De beelden van dit punt onder alle elementen van G levert dan N punten op de cirkel. Door te gebruiken dat de elementen van G isometrieën zijn, kan worden nagegaan dat deze N punten precies de hoekpunten van een regelmatige N-hoek zijn. De rotaties die deze hoekpunten in elkaar overvoeren vormen precies de gevraagde groep. □

5.3 De diëdergroepen.

Laat C_r de cirkel in $\mathbb{R}^2$ zijn met als middelpunt de oorsprong en straal $r \geq 0$. Een isometrie die de cirkel op zichzelf afbeeldt moet het middelpunt van de cirkel vasthouden. Immers, voor elk punt van de cirkel geldt dat er slechts één punt op de cirkel ligt dat afstand $2r$ heeft tot het gegeven punt, namelijk het tegenoverliggende punt. Dit laat zien dat lijnen door het middelpunt naar lijnen door het middelpunt worden afgebeeld, en dus moet het snijpunt van deze lijnen vast blijven. We concluderen dat de symmetriegroep van de cirkel isomorf is met de groep $\mathrm{O}(2)$.

Definitie 5.3.1 De symmetriegroep van de cirkel C_r noemen we de *oneindige diëdergroep*. Deze groep noteren we als D_∞.

Stelling 5.3.2 *De groep D_∞ is isomorf met $O(2)$, en bestaat uit spiegelingen σ in een willekeurige lijn door het middelpunt van de cirkel, en rotaties ρ om het middelpunt van de cirkel.*

Hierbij geldt dat de deelverzameling $R \subset D_\infty$ bestaande uit alle rotaties een commutatieve ondergroep is van D_∞.

Is $\sigma \in D_\infty$ een willekeurige spiegeling, dan geldt

$$D_\infty = R \cup R \cdot \sigma.$$

Nemen we σ de spiegeling in de x-as, dan geldt voor willekeurige $\rho \in R$ dat $\sigma\rho\sigma = \rho^{-1}$.

Bewijs. Dat $D_\infty \cong \mathrm{O}(2)$ en dat deze matrixgroep uit spiegelingen en rotaties bestaat, weten we al. De rotaties zijn precies de matrices in $\mathrm{O}(2)$ die determinant 1 hebben, en dus is R de kern van het homomorfisme "determinant": $\mathrm{O}(2) \to \{\pm 1\}$.

De elementen van $\mathrm{O}(2)$ die determinant -1 hebben zijn allemaal spiegelingen (want ze hebben een eigenwaardenpolynoom van de vorm $X^2 - t*X - 1$ voor zekere $t \in \mathbb{R}$, dus twee reële eigenwaarden. Die hebben absolute waarde 1 en product -1. De matrix stelt dan spiegelen in de eigenrichting bij eigenwaarde $+1$ voor).

De opdeling $D_\infty = R \cup R \cdot \sigma$ is precies de opdeling van D_∞ in rotaties en spiegelingen.

Nemen we voor σ de spiegeling in de x-as, dan komt dit overeen met de matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Voor een willekeurige rotatie $\rho = \left(\begin{smallmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{smallmatrix}\right)$ geldt dan

$$\sigma\rho\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \rho^{-1}$$

want $\cos(-\alpha) = \cos(\alpha)$ en $\sin(-\alpha) = -\sin(\alpha)$. Dit bewijst de stelling. $\square$

Voor het rekenen met de groep D_∞ is het soms handig om de rotaties en spiegelingen op te vatten als afbeeldingen van het complexe vlak $\mathbb{C}$ naar zichzelf. De "spiegeling in de x-as" wordt dan de complexe conjugatie

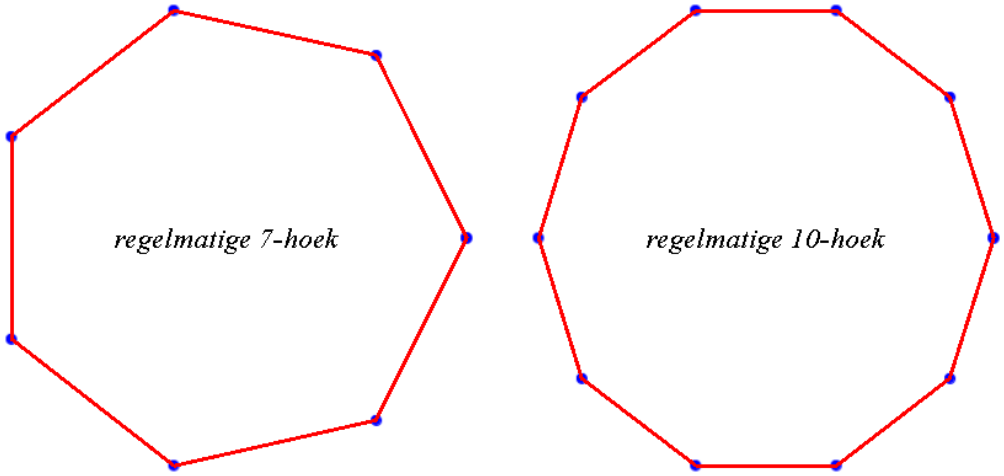
$$c \ : \ \ z \mapsto \overline{z}$$

en "roteren over α" wordt vermenigvuldigen met $e^{\alpha i}$, dus

$$v \ : \ \ z \mapsto e^{\alpha i} \cdot z.$$

Bijvoorbeeld cvc is dan de afbeelding die een $z \in \mathbb{C}$ stuurt naar $cvc(z) = cv(\overline{z}) = c(e^{\alpha i}\overline{z}) = \overline{e^{\alpha i}\overline{z}} = e^{-\alpha i}z$, dus $cvc = v^{-1}$ zoals we al wisten.

Delen we de cirkel met positieve straal in $n \geq 2$ even grote segmenten, dan levert dat n punten op die we gebruiken als hoekpunten van een regelmatige n-hoek F_n.



Definitie 5.3.3 De groep van alle symmetrieën van F_n wordt de n-de diëdergroep D_n genoemd.

Het middelpunt van F_n blijft weer vast onder alle symmetrieën, dus D_n is een ondergroep van $D_\infty = \mathrm{O}(2)$. Ook de groep D_n bestaat dus uit rotaties en spiegelingen; de rotaties die in D_n zitten zijn precies die over een hoek $k \cdot 2\pi/n$, voor $0 \leq k < n$. Dat zijn er dus n. De rotatie over de kleinste van deze hoeken, dus over $2\pi/n$, noemen we ρ. De spiegelingen die F_n in zichzelf overvoeren, zijn precies de spiegelingen in lijnen door de oorsprong en een

hoekpunt, en die in de lijnen door de oorsprong en het midden van een zijde van F_n. Eén van die spiegelingen is de spiegeling in de x-as, die we vanaf nu σ noemen. Er zijn precies n spiegelingen, namelijk alle $\sigma\rho^k$ voor $0 \leq k < n$. Dus D_n is een eindige groep, bestaande uit $n + n = 2n$ elementen.

We vatten deze discussie samen als volgt.

Stelling 5.3.4 *De groep D_n bestaat uit $2n$ elementen. Voor $n > 2$ is D_n een niet-commutatieve groep.*

In D_n zit de rotatie ρ over een hoek $2\pi/n$ en de spiegeling σ in de x-as. Elk element van D_n is op een unieke manier te schrijven als ρ^k of als $\sigma\rho^k$ met $0 \leq k < n$.

Er geldt orde$(\rho) = n$ en orde$(\sigma) = 2$, dus in het bijzonder $\rho^n = \sigma^2 = id$. Verder geldt $\sigma\rho\sigma = \rho^{-1}$.

De ondergroep R_n van D_n bestaande uit alle rotaties is isomorf met $\mathbb{Z}/n\mathbb{Z}$.

Bewijs. De inverse ρ^{-1} is een rotatie over een hoek $(n-1)2\pi/n$. Voor $n > 2$ is dat verschillend van een rotatie over $2\pi/n$, dus dan is $\sigma\rho\sigma = \rho^{-1} \neq \rho$. Dit impliceert dat D_n niet commutatief is als $n > 2$.

De overige uitspraken in de stelling zijn evident, en/of volgen direct uit Stelling 5.3.2. □

Voorbeeld 5.3.5 Voor $n = 2$ hebben we de groep D_2 bestaande uit 4 elementen. In dit geval is ρ de afbeelding "roteren over 180 graden", dus $\rho(x, y) = (-x, -y)$. In het bijzonder is dan $\rho^{-1} = \rho$, dus ook $\sigma\rho = \rho\sigma$. En dus is D_2 commutatief. Dat wisten we natuurlijk al, omdat elke groep bestaande uit slechts 4 elementen commutatief is. Hier is $\sigma\rho$ de spiegeling in de y-as. Alle elementen $\neq id$ in D_2 hebben orde 2, en $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Merk op dat dit voorbeeld een beetje vreemd is: een regelmatige 2-hoek is in feite een lijnstuk. De spiegeling in de lijn die dit lijnstuk bevat, is een element van orde 2 in D_2. Maar deze spiegeling houdt elk punt van het lijnstuk vast.

Voorbeeld 5.3.6 We gaan na voor welke n de rotatie r over 180 graden, dus gegeven door $r(x, y) = (-x, -y)$, een element is van D_n.

Daarvoor merken we allereerst op dat orde$(r) = 2$. Als $r \in D_n$, dan $r = \rho^k$ voor zekere k, want elke rotatie is een macht van ρ. Bijgevolg is $r^n = \rho^{nk} = id$. Hieruit volgt dat $2 =$ orde(r) een deler is van n. Dus n is even; schrijf $n = 2m$ met m geheel. Dan is ρ^m een rotatie die orde 2 heeft, oftewel $\rho^m = r$. Conclusie:

$$r \in D_n \Leftrightarrow n \text{ is even.}$$

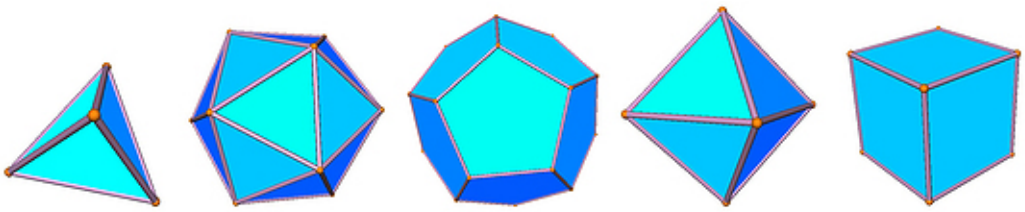
5.4 Symmetriegroepen van de platonische lichamen.

Precies zoals we dat hiervoor in het geval van een cirkel in $\mathbb{R}^2$ deden, beschouwen we nu een bol in $\mathbb{R}^3$. De symmetriegroep van de bol is de hele $\mathrm{O}(3)$ die zoals we zagen bestaat uit draaiingen en draaispiegelingen. Dit is een heel grote, niet-commutatieve groep.

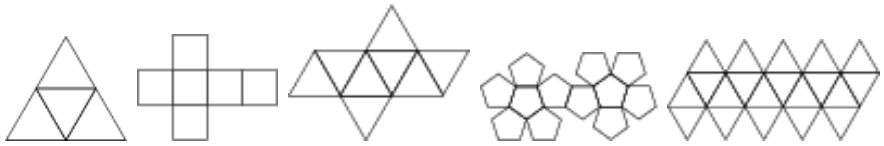
Analoog aan de regelmatige n-hoeken in het vlak kan men vervolgens proberen regelmatige veelvlakken in de ruimte te maken. Dit gaat door op de bol n punten te kiezen zo, dat het figuur opgespannen door deze punten als zijvlakken steeds dezelfde regelmatige m-hoek heeft. We zullen een bewijs schetsen voor het feit dat dit slechts voor een paar combinaties (n, m) mogelijk is. Preciezer geformuleerd:

De enige ruimtelijke regelmatige n-vlakken zijn

- *De tetraeder, met* 4 *gelijkzijdige driehoeken als zijvlakken en met* 4 *hoekpunten en* 6 *ribben;*
- *De kubus, met* 6 *vierkanten als zijvlakken en met* 8 *hoekpunten en* 12 *ribben;*
- *De octaeder, met* 8 *gelijkzijdige driehoeken als zijvlakken en met* 6 *hoekpunten en* 8 *ribben;*
- *De dodecaeder, met* 12 *regelmatige vijfhoeken als zijvlakken en met* 20 *hoekpunten en* 30 *ribben;*
- *De icosaeder, met* 20 *gelijkzijdige driehoeken als zijvlakken en met* 12 *hoekpunten en* 30 *ribben.*



Schets van een bewijs. De symmetriegroep van een willekeurig regelmatig veelvlak is eindig. Immers, zo'n symmetrie wordt volledig bepaald door wat er met de hoekpunten van de figuur gebeurt (die hoekpunten corresponderen



met vectoren die tezamen $\mathbb{R}^3$ opspannen). Dus er bestaan hooguit zoveel symmetrieën als er permutaties van de hoekpunten zijn, en dat aantal is eindig. Dit argument laat in feite zien dat de symmetriegroep van zo'n figuur isomorf is met een ondergroep van S_n, waarbij n het aantal hoekpunten is. Verder geldt, dat ieder hoekpunt door een geschikt element van de symmetriegroep op ieder willekeurig ander hoekpunt kan worden afgebeeld. Dit kan zelfs al met een rotatie. Immers, stellen we ons de hoekpunten voor als punten op een bol, dan is door het draaien van die bol elk hoekpunt op de noordpool te leggen, en door de bol dan nog om de noord-zuid as te draaien 'behoudt het veelvlak z'n oorspronkelijke stand'. Ook merken we op, dat er bij een hoekpunt altijd rotaties zijn, die dat hoekpunt vasthouden. En vanwege Lemma 5.2.7, toegepast op de rotaties van een vlak loodrecht op de lijn door de oorsprong en het gegeven hoekpunt, vormen die een groep isomorf met $\mathbb{Z}/m\mathbb{Z}$ voor zekere m. Deze draaiingen voeren de zijvlakken die in het gegeven hoekpunt bij elkaar komen cyklisch in elkaar over; in het bijzonder zijn er dus precies m zulke zijvlakken.

Bovenstaande observaties leiden tot de volgende strategie voor het bepalen van alle regelmatige veelvlakken. Bepaal eerst alle eindige ondergroepen van de groep van draaiingen SO(3). Voor de gevonden groepen bepalen we alle punten op een boloppervlak die door meerdere elementen van de groep worden vastgehouden. Dat levert alle mogelijke hoekpunten, en door uitgaande van één ervan alle beelden onder de groep te bepalen vinden we dan alle mogelijke regelmatige veelvlakken. We voeren dat nu in iets meer detail uit.

Laat G een willekeurige eindige ondergroep van SO(3) zijn bestaande uit precies $N \geq 2$ elementen. Met B duiden we de verzameling punten in $\mathbb{R}^3$ aan die op afstand 1 van de oorsprong liggen; dus B is het boloppervlak. Is $\sigma \in G$, en $\sigma \neq id$, dan is σ vanwege Stelling 5.2.4 een rotatie om een lijn L. Er zijn dus precies twee punten van B die door σ op zichzelf worden afgebeeld, namelijk de snijpunten van L met B. In totaal vinden we zo een verzameling van precies $2(N-1)$ paren (σ, P), waarbij $\sigma \in G, \sigma \neq id, P \in B$ en $\sigma(P) = P$.

We bekijken vervolgens de zo verkregen punten $P \in B$. Bij zo'n P hebben we minstens één draaiing $\sigma \neq id$ met $\sigma \in G$ en $\sigma(P) = P$. Alle rotaties in G die P vasthouden, houden ook de lijn door P en de oorsprong O vast.

Bijgevolg kunnen we ze opvatten als eindige groep van rotaties van het vlak door de oorsprong loodrecht op de lijn door OP; vanwege Lemma 5.2.7 is dit een groep G_P isomorf met $\mathbb{Z}/m_P\mathbb{Z}$, voor zekere $m_P \geq 2$. Omdat G_P een ondergroep is van G, geldt $m_P = \#G_P | \#G = N$. Schrijf $N = m_P \cdot n_P$. Uit het bewijs van Stelling 3.2.7 concluderen we dat er $\sigma_1, \ldots, \sigma_{n_P} \in G$ zijn zodat $G = \sigma_1 G_P \cup \ldots \cup \sigma_{n_P} G_P$, waarbij geldt dat $\sigma_i G_P \cap \sigma_j G_P = \emptyset$ voor $i \neq j$. Ieder element van $\sigma_i G_P$ is te schrijven als $\sigma_i \tau$ voor een $\tau \in G_P$, en dus $\sigma_i \tau(P) = \sigma_i(P)$. Schrijf $P_i = \sigma_i(P)$. Er geldt $P_i \neq P_j$ als $i \neq j$. Immers, anders zou $\sigma_i(P) = \sigma_j(P)$ en dus $\sigma_i^{-1}\sigma_j \in G_P$, hetgeen impliceert dat $\sigma_i G_P$ en $\sigma_j G_P$ geen lege doorsnede zouden hebben. Dus P wordt door de elementen van G op in totaal n_P verschillende punten afgebeeld. De zo verkregen verzameling van n_P punten noteren we als C_P.

Neem P als boven, $\sigma \in G$ willekeurig, en $Q = \sigma(P)$. Dan geldt $m_P = m_Q$. Immers, is $\tau \in G_P$, dan is $\sigma\tau\sigma^{-1} \in G_Q$ en omgekeerd is voor $\rho \in G_Q$ het element $\sigma^{-1}\rho\sigma \in G_P$. Dit levert een bijectie (zelfs een isomorfisme van groepen) tussen G_P en G_Q, dus in het bijzonder hebben beide hetzelfde aantal elementen oftewel $m_P = m_Q$. Dit levert een tweede manier om het aantal paren (σ, P) met $\sigma \in G, \sigma \neq id, P \in B$ en $\sigma(P) = P$ te tellen: het is gelijk aan $\sum_C n_C(m_C - 1)$. Hier sommeren we over alle verschillende verzamelingen $C = C_P$, en voor zo'n C_P is n_C het aantal punten $Q \in C_P$ en m_C het aantal elementen in G_Q voor elke $Q \in C_P$.

De twee uitdrukkingen voor het aantal paren leveren de gelijkheid

$$2N - 2 = \sum_C (N - \frac{N}{m_C}).$$

Dit delen door N geeft $2 - \frac{2}{N} = \sum_C (1 - 1/m_C)$. De rest van het bewijs bestaat voornamelijk uit het analyseren van deze vergelijking. Het linkerlid is groter dan 1, dus moet de som in het rechterlid uit minstens twee termen bestaan. Omdat het linkerlid kleiner is dan 2, en het rechterlid bestaat uit termen die minstens $1/2$ zijn, bestaat de som daar dus óf uit 2, óf uit drie termen. Eerst zullen we het geval dat de som eruitziet als $2 - 2/N = (1 - 1/m_1) + (1 - 1/m_2)$ beschouwen. Met N vermenigvuldigen levert $2 = N/m_1 + N/m_2$. Omdat m_1 en m_2 positieve delers van N zijn, moet gelden $m_1 = m_2 = N$. Elk van de twee verzamelingen C_i bestaat in dit geval uit $n_i = N/m_i = 1$ punt. Omdat de elementen van G rotaties zijn en allemaal deze twee punten vasthouden, is G een eindige groep van rotaties om een vaste lijn, dus met behulp van Lemma 5.2.7 volgt dat $G \cong \mathbb{Z}/N\mathbb{Z}$. Ook concluderen we dat dit geval ons geen regelmatig veelvlak oplevert, want we zouden slechts één hoekpunt krijgen.

In het resterende geval zijn er drie verzamelingen C_i. We schrijven weer $m_i = m_{C_i}$ en ook $n_i = \#C_i = N/m_i$. De volgorde van de C_i's kiezen we zo,

dat $m_1 \leq m_2 \leq m_3$. De vergelijking die we hebben kan geschreven worden als

$$1 + \frac{2}{N} = \frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3}.$$

Zouden alle m_i minstens 3 zijn, dan was het rechterlid van deze gelijkheid ≤ 1 en dat kan niet. Dus geldt $m_1 = 2$. Met andere woorden,

$$\frac{1}{2} + \frac{2}{N} = \frac{1}{m_2} + \frac{1}{m_3}.$$

Hetzelfde argument als zojuist levert dat m_2, m_3 niet beide minstens 4 kunnen zijn. Dus is $m_2 = 2$ of $m_2 = 3$. Eerst analyseren we de mogelijkheid $m_2 = 2$. In dit geval geldt $N = 2m_3$, en m_3 mag willekeurig ≥ 2 zijn, zeg $m_3 = n$. De verzamelingen C_1, C_2 bestaan hier elk uit $N/m_1 = n$ punten, en ieder van die punten wordt vastgehouden door een ondergroep van G bestaande uit $m_1 = 2$ rotaties. In zo'n ondergroep zit dus een draaiing over 180 graden om de lijn door de oorsprong en dat punt. Hieruit volgt dat bijvoorbeeld de n punten in C_1 alle in één vlak V door de oorsprong liggen. De doorsnede van V met B is een cirkel, en omdat G uit isometrieën bestaat, vormen de punten in C_1 dan een regelmatige n-hoek. De groep G beeldt V op zichzelf af en in het bijzonder deze n-hoek ook. 'Beperken tot V' is een homomorfisme van G naar de symmetriegroep van de n-hoek, en dat is D_n. Dit homomorfisme is injectief, want als voor een draaiing geldt dat z'n beperking tot een vlak de identiteit is, dan is de draaiing zelf de identiteit. Dus het beperkingshomomorfisme heeft als kern alleen de identiteit en is bijgevolg injectief. Daar zowel G als D_n uit $2n$ elementen bestaan, volgt $G \cong D_n$. Als ondergroep van SO(3) ziet D_n er volgens bovenstaande analyse als volgt uit. Kies een vlak V door de oorsprong en een regelmatige n-hoek om O in V. De rotaties in D_n zijn dan rotaties om de lijn door O loodrecht op V, en de spiegelingen zijn de draaiingen over 180 graden om een lijn door O en een hoekpunt van de n-hoek.

De resterende mogelijk is $m_1 = 2$ en $m_2 = 3$. In dat geval geldt $m_3 \geq m_2 = 3$ en $1/6 + 2/N = 1/m_3$. Dus kan m_3 niet meer dan 5 zijn. Er resteren drie mogelijkheden, namelijk $m_3 = 3$ en $m_3 = 4$ en $m_3 = 5$. Is $m_3 = 3$, dan geldt $N = 12$. De verzamelingen C_2 en C_3 bestaan in dit geval elk uit 4 punten. Ieder van deze punten wordt door een groep van orde 3, dus door rotatie over 120 graden vastgehouden. Dit leidt tot een regelmatig figuur bestaande uit 4 hoekpunten, waar steeds 3 ribben en 3 zijvlakken samenkomen. Dit is precies de tetraeder.

Wanneer $m_3 = 4$, dan is $N = 24$. De verzameling C_2 spant dan een figuur op met $24/3 = 8$ hoekpunten. In elk van deze punten komen 3 zijden en 3 ribben bij elkaar. Deze worden in elkaar overgevoerd door rotaties over

veelvouden van 120 graden. Dit bepaalt weer precies een regelmatig veelvlak, namelijk de kubus. Bezien we de verzameling C_3, dan geeft dat $24/4 = 6$ punten waarin 4 ribben/zijvlakken samenkomen. C_3 spant dus een octaeder op.

Tenslotte $m_3 = 5$, wat leidt tot $N = 60$. Het figuur opgespannen door C_2 heeft nu 20 hoekpunten. In ieder ervan komen 3 ribben/vlakken samen, en we krijgen een dodecaeder. Op dezelfde manier geeft C_3 hier aanleiding tot een icosaeder. Hiermee zijn de regelmatige veelvlakken geklassificeerd, en we hebben zelfs voor ieder ervan het aantal elementen van de ondergroep van hun symmetriegroep bestaande uit alle rotaties bepaald. □

We gaan nu voor elk van de regelmatige veelvlakken een beschrijving van de symmetriegroep geven. Allereerst merken we op dat (met uitzondering van het geval van de tetraeder) de afbeelding -1 (puntspiegelen in de oorsprong) hier een element van is. Verder is het een eindige ondergroep van O(3). Is τ zo'n symmetrie, dan $\det(\tau) = \pm 1$. In het geval $\det(\tau) = 1$ is τ een rotatie. Is $\det(\tau) = -1$, dan is $-\tau$ een rotatie. Hieruit concluderen we dat de symmetriegroep precies bestaat uit alle rotaties τ, en alle afbeeldingen $-\tau$.

Voor de tetraeder bestaat eenzelfde soort redenering: neem een spiegeling σ in de symmetriegroep ervan. Dan geldt $\det(\sigma) = -1$ en $\sigma^2 = id$. Is een τ in de symmetriegroep *geen* rotatie, dan $\det(\tau) = -1$ en $\tau = \sigma \cdot \sigma\tau$ waarbij $\sigma\tau$ *wel* een rotatie is, omdat immers $\det(\sigma\tau) = \det(\sigma)\det(\tau) = -1 \cdot -1 = 1$. Dus de hele symmetriegroep bestaat uit de rotaties, en σ maal deze rotaties.

In het bijzonder bestaat de symmetriegroep van een regelmatig veelvlak uit resp. $24, 48, 48, 120, 120$ elementen.

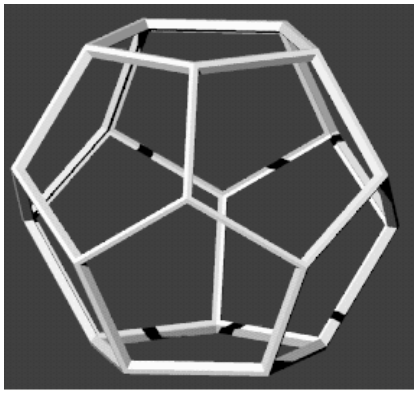
De tetraeder. De symmetriegroep is isomorf met S_4. Immers, gezien als permutatiegroep op de hoekpunten is het een ondergroep van S_4, en omdat de groep uit 24 elementen bestaat is het dan de hele S_4.

De kubus en de octaeder. Deze twee figuren hebben dezelfde symmetriegroep. Immers, leggen we binnen de kubus een bol die precies aan de zijvlakken raakt, dan vormen de 6 raakpunten precies de hoekpunten van een octaeder. Hieruit volgt dat een symmetrie van de kubus ook een symmetrie van de octaeder oplevert. Dit argument kan vervolgens omgedraaid worden: een ingeschreven bol aan de octaeder raakt deze weer precies in de hoekpunten van een kubus. Dus beide figuren hebben precies dezelfde symmetrieën.

Zoals we gezien hebben heeft deze symmetriegroep 48 elementen. De groep is isomorf met $S_4 \times \{\pm 1\}$. Dit kan als volgt bewezen worden. Een

kubus heeft 4 hoofddiagonalen, en deze worden door de symmetriegroep gepermuteerd. Verder heeft elke symmetrie een determinant ± 1. Aldus wordt een homomorfisme naar $S_4 \times \{\pm 1\}$ verkregen. Zit τ in de kern van dit homomorfisme, dan houdt τ alle hoofddiagonalen vast en $\det(\tau) = 1$. τ is dan een rotatie om één van de hoofddiagonalen, en het is niet moeilijk om na te gaan dat het feit dat τ de drie andere diagonalen naar zichzelf moet sturen impliceert dat $\tau = id$. Dus het gegeven homomorfisme is injectief, en omdat zowel de symmetriegroep als $S_4 \times \{\pm 1\}$ uit 48 elementen bestaan, zijn beide groepen isomorf.

De dodecaeder en de icosaeder. Hetzelfde argument dat voor de kubus en de octaeder gegeven werd toont aan dat deze twee dezelfde symmetriegroep hebben. In dit geval is de symmetriegroep isomorf met $A_5 \times \{\pm 1\}$. We gebruiken de dodecaeder om dit aan te tonen.



Nummer de ribben van het bovenvlak $1, 2, 3, 4, 5$. Voor i met $1 \leq i \leq 5$ definiëren we V_i als de verzameling ribben van de dodecaeder die in een richting wijzen die óf evenwijdig is, óf loodrecht staat op de richting van ribbe i. Elke V_i bestaat dan uit precies 6 ribben. Omdat symmetrieën hoeken in even grote hoeken overvoeren, werkt de symmetriegroep van de dodecaeder als permutaties op de verzameling $\{V_1, V_2, V_3, V_4, V_5\}$. De symmetrie 'puntspiegelen in de oorsprong' houdt elk van de V_i's op z'n plaats, dus om na te gaan welke permutaties voorkomen als beeld van een symmetrie hoeven we alleen maar naar draaiingen te kijken. Men ziet dan eenvoudig in dat alleen *even* permutaties voorkomen. Door ook nog een symmetrie te sturen naar z'n determinant krijgen we een homomorfisme naar $A_5 \times \{\pm 1\}$. De kern blijkt alleen uit de identiteit te bestaan, dus omdat zowel de symmetriegroep als

$A_5 \times \{\pm 1\}$ precies 120 elementen heeft zijn ze isomorf.

5.5 Automorfismen van een graaf

We zullen ons hier niet met de meest algemene soort grafen bezighouden. In het bijzonder beperken we ons tot eindige grafen, waarbij tussen twee punten hooguit één verbindingslijn bestaat:

Definitie 5.5.1 Een graaf Γ bestaat uit een paar (P, L), waarin P een niet-lege eindige verzameling is (de 'punten' van de graaf), en L een (evt. lege) verzameling is bestaande uit paren $\{a, b\}$ met $a, b \in P$ (de 'lijnen' van de graaf).

Opmerking 5.5.2 In veel literatuur over grafen heten de punten 'vertices' en de lijnen 'edges'. Wat wij hier 'graaf' noemen heet elders meestal een 'simpele' of 'enkelvoudige' graaf (zie bijvoorbeeld het boekje P.W.H. Lemmens en T.A. Springer, Hoofdstukken uit de Combinatoriek, Utrecht: Epsilon Uitgaven, 1992, blzn. 57 en 64). Een graaf kan worden weergegeven door een plaatje: we tekenen de punten, en verbinden twee punten a, b door een lijnstukje (of een lusje indien $a = b$) precies dan als $\{a, b\}$ in de verzameling lijnen van de graaf zit. In de regel is zo'n plaatje niet mogelijk zonder dat de getekende lijnstukjes elkaar ook in andere punten dan de punten van de graaf snijden. Door de punten van de graaf wat dikker te tekenen leidt dit vrijwel nooit tot verwarring.

Bij een graaf hoort een eindige groep als volgt.

Definitie 5.5.3 Een automorfisme van een graaf $\Gamma = (P, L)$ is een permutatie σ van z'n punten P, met de eigenschap dat voor elke $\{a, b\} \in L$ geldt dat ook $\{\sigma(a), \sigma(b)\} \in L$.

De verzameling van alle automorfismen van Γ noteren we als $\mathrm{Aut}(\Gamma)$.

Stelling 5.5.4 *Voor elke graaf Γ bestaande uit n punten is $Aut(\Gamma)$ een ondergroep van S_n.*

Bewijs. Nummer de punten van de graaf Γ als $1, 2, \ldots, n$. Het is evident dat elke $\sigma \in \mathrm{Aut}(\Gamma)$ correspondeert met een permutatie in S_n, dus is $\mathrm{Aut}(\Gamma)$ een deelverzameling van S_n. We tonen aan dat deze deelverzameling een ondergroep is. De identiteit zit er in. Als $\sigma \in \mathrm{Aut}(\Gamma)$, dan stuurt σ elementen van L naar elementen van L door $\sigma(\{i, j\}) = \{\sigma(i), \sigma(j)\}$. Dit geeft een injectieve afbeelding van L naar L, en omdat L eindig is, is deze dan ook surjectief. Dit betekent dat als $\sigma(k) = i$ en $\sigma(\ell) = j$ en $\{i, j\} \in L$, dan is ook

$\{k, \ell\} \in L$. Uit de definitie van $\mathrm{Aut}(\Gamma)$ volgt hiermee dat als $\sigma \in \mathrm{Aut}(\Gamma)$, dan ook $\sigma^{-1} \in \mathrm{Aut}(\Gamma)$. Het bewijs dat een product van elementen uit $\mathrm{Aut}(\Gamma)$ weer een element van $\mathrm{Aut}(\Gamma)$ oplevert is veel eenvoudiger en dat laten we aan de lezer over. Hieruit volgt de stelling. □

Voorbeeld 5.5.5 De *volle* graaf Γ_n op n punten is per definitie de graaf bestaande uit n punten $1, 2, \ldots, n$, met als lijnen alle $\{i, j\}$ voor $1 \leq i \leq j \leq n$. De eis dat een automorfisme lijnen in lijnen moet overvoeren legt in dit geval geen enkele beperking op, dus er geldt $\mathrm{Aut}(\Gamma_n) = S_n$.

Voorbeeld 5.5.6 Nummer de hoekpunten van een regelmatige n-hoek als $1, 2, \ldots, n$. Deze n-hoek vatten we op als graaf F_n met als punten $1, 2, \ldots n$ en als lijnen $\{1, 2\}, \{2, 3\}, \ldots, \{n-1, n\}, \{n, 1\}$. Er geldt $\mathrm{Aut}(F_n) \cong D_n$. Immers, elke symmetrie van de regelmatige n-hoek kan worden opgevat als element van $\mathrm{Aut}(F_n)$, dus $D_n \subset \mathrm{Aut}(F_n)$. Verder geldt dat als $\tau \in \mathrm{Aut}(F_n)$ het element 1 naar i stuurt, dan wordt 2 naar één van de twee buren van i gestuurd, en daarmee ligt τ vast. Hieruit zien we dat er slechts $n \cdot 2 = 2n$ mogelijkheden zijn voor τ. Zoveel elementen heeft D_n al, dus $\mathrm{Aut}(F_n) \cong D_n$.

5.6 Opgaven

1. Toon aan dat $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ en dat $D_3 \cong S_3$.

2. Laat zien dat D_n niet-commutatief is precies dan als $n > 2$.

3. Door de elementen van D_n op te vatten als permutaties op de hoekpunten van een regelmatige n-hoek krijgen we een afbeelding van D_n naar S_n. Ga na dat dit een injectief homomorfisme is. Welke elementen van D_n hebben als beeld een even permutatie?

4. Neem $v \in \mathbb{R}^n$ en noteer transleren over v als τ_v. Laat $a \in \mathbb{R}$ met $a \neq 0$.

   (a) Ga na dat $a\tau_v\frac{1}{a}$ ook weer een translatie is.

   (b) Toon aan dat als φ een willekeurige isometrie op $\mathbb{R}^n$ is, dan is $a\varphi\frac{1}{a}$ er ook één.

5. Deze opgave is bedoeld om de draaiingshoek die voorkomt in orthogonale afbeeldingen op $\mathbb{R}^3$ te bepalen. Zie het bewijs van Stelling 5.2.4 voor de gebruikte notaties. De matrix A in dat bewijs vatten we hier op als complexe 3×3-matrix.

   (a) Laat zien dat de eigenwaarden van A van de vorm $\lambda = \pm 1, e^{i\alpha}$ en $e^{-i\alpha}$ zijn, met $0 \leq \alpha < 2\pi$.

   (b) Is $e^{i\alpha}$ een niet-reële eigenwaarde van A, bewijs dan dat een eigenvector hierbij te schrijven is als $x + iy$ voor reële vectoren x, y en dat x, y en de eigenvector bij λ een basis van $\mathbb{R}^3$ vormen van onderling loodrechte vectoren.

   (c) Ga na dat A de ruimte opgespannen door x, y naar zichzelf afbeeldt, en dat A op die ruimte werkt als een draaiing over de hoek α.

6. Lees de beschrijving van de symmetriegroep van de dodecaeder in dit dictaat. Kies vervolgens een hoekpunt P, en ga na welke permutaties in A_5 de rotaties om de lijn OP opleveren. Doe hetzelfde voor de rotaties om de lijn door een middelpunt van een zijvlak, en ook voor de rotatie (over 180 graden) om de lijn door het midden van een ribbe.

7. De tetraeder bevat precies 3 paren R_1, R_2, R_3 van elkaar niet snijdende ribben, en de symmetriegroep permuteert deze drie. Geef het homomorfisme: $S_4 \to S_3$ waartoe dit aanleiding geeft expliciet. Laat zien dat het een surjectie is, en beschrijf de kern.

8. Ga na dat er 20 verschillende grafen bestaande uit 3 punten bestaan, en dat geen van deze A_3 als automorfismengroep heeft.

9. Bepaal het aantal automorfismen en de groep $\mathrm{Aut}(H)$, waarbij H de graaf is met 6 punten en 5 lijnen die de vorm heeft van de hoofdletter 'H'.

10. Door de hoekpunten als punten te nemen en de ribben als lijnen, kan een kubus worden opgevat als een graaf K. Bepaal de automorfismengroep van K.

6 Conjugatie, index en Sylow-groepen

In dit hoofdstuk gaan we wat dieper in op ondergroepen van met name eindige groepen. Ook bestuderen we het van links of van rechts vermenigvuldigen met een vast element in meer detail.

6.1 conjugatie en index

We gaan uit van een willekeurige groep G en vastgekozen elementen $a, b \in G$. De afbeeldingen van G naar G 'van links vermenigvuldigen met a' (dus $x \mapsto ax$) en 'van rechts met b vermenigvuldigen' ($x \mapsto xb$) zijn dan bijecties. Hun samenstelling, gegeven door $x \mapsto axb$, is dan ook bijectief. In het algemeen is deze bijectie geen homomorfisme. Immers, een homomorfisme heeft in het bijzonder de eigenschap dat het eenheidselement op het eenheidselement wordt afgebeeld. De hier gegeven bijectie stuurt $e \in G$ naar $aeb = ab$. Dit is precies dan gelijk aan het eenheidselement e, als b de inverse van a is: $b = a^{-1}$.

Definitie 6.1.1 Is G een groep en $a \in G$, dan noemen we de bijectie $\gamma_a : G \to G$ gegeven door $\gamma_a(x) = axa^{-1}$ de *conjugatie* met a.

Stelling 6.1.2 *Gegeven is een groep G en $a, b \in G$.*

1. *De conjugatie γ_a met a is een isomorfisme : $G \cong G$.*
2. *Voor conjugaties γ_a, γ_b geldt $\gamma_a\gamma_b = \gamma_{ab}$.*
3. *De inverse van γ_a is $\gamma_{a^{-1}}$.*
4. *Is H een ondergroep van G, dan is $\gamma_a(H) = aHa^{-1}$ dat ook en $H \cong aHa^{-1}$.*

Bewijs. 1: Voor $x, y \in G$ geldt $\gamma_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \gamma_a(x)\gamma_a(y)$. Dus γ_a is een homomorfisme. We hadden al opgemerkt dat γ_a bijectief is, dus is het een isomorfisme.
2: Is $x \in G$, dan $\gamma_a\gamma_b(x) = \gamma_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \gamma_{ab}(x)$. Met andere woorden, $\gamma_a\gamma_b = \gamma_{ab}$.
3: Uit 2) volgt $\gamma_a\gamma_{a^{-1}} = \gamma_e = \gamma_{a^{-1}}\gamma_a$. Ook geldt voor elke $x \in G$ dat $\gamma_e(x) = exe^{-1} = x$, dus $\gamma_e = id$. Dit impliceert de bewering.
4: Omdat γ_a een homomorfisme is en H een groep, is $\gamma_a(H)$ dat ook. γ_a is injectief, dus z'n beperking tot H is dat ook. Bovendien heeft deze beperking per definitie als beeld $\gamma_a(H)$, en dus $H \cong \gamma_a(H)$. □

Voorbeeld 6.1.3 Is G een commutatieve groep, dan is conjugeren met een willekeurig element van G de identiteit. Conjugaties zijn dus alleen interessant in het geval van niet-commutatieve groepen.

In de lineaire algebra speelt het conjugeren van matrices een grote rol bij het overgaan op een andere basis.

Definitie 6.1.4 Twee elementen x, y in een groep G heten *geconjugeerd* wanneer er een conjugatie γ_a met $a \in G$ bestaat zodat $\gamma_a(x) = y$.

De *conjugatieklasse* van $x \in G$ is per definitie de deelverzameling

$$C_x = \{y \in G \mid \text{er bestaat een } a \in G \text{ met } \gamma_a(x) = y\}\,.$$

Voorbeeld 6.1.5 In een commutatieve groep G geldt voor elke $x \in G$ dat $C_x = \{x\}$.

Voor S_3 geldt dat $(1\ 2)$ en $(1\ 2\ 3)$ *niet* geconjugeerd zijn. Immers, voor elke $\tau \in S_3$ geldt dat $\tau(1\ 2)\tau^{-1} = (\tau(1)\ \tau(2))$ en $\tau(1\ 2\ 3)\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3))$. Hieruit volgt dat $(1\ 2)$ met elke andere 2-cykel geconjugeerd is, en $(1\ 2\ 3)$ met elke andere 3-cykel, maar ze zijn het niet met elkaar.

Voorbeeld 6.1.6 Met behulp van de theorie over Jordan-normaalvormen wordt in de lineaire algebra aangetoond dat twee matrices $A, B \in \mathrm{GL}_n(\mathbb{C})$ geconjugeerd zijn dan en slechts dan als ze aanleiding geven tot dezelfde Jordan-normaalgedaante. Dus bijvoorbeeld $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ en $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ zijn *niet* geconjugeerd, maar $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ en $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ zijn het wel.

Stelling 6.1.7 *In een groep G is 'geconjugeerd zijn' een equivalentierelatie. Dit houdt precies in dat:*

1. *Elke $x \in G$ is met zichzelf geconjugeerd, oftewel $x \in C_x$.*
2. *Als x met y geconjugeerd is, dan ook y met x (anders gezegd: als $x \in C_y$, dan ook $y \in C_x$).*
3. *Als $x \in C_y$ en $y \in C_z$, dan ook $x \in C_z$.*
4. *G is de disjuncte vereniging van verzamelingen C_x. Dat wil zeggen dat elk element van G in een C_x zit, en zit een element zowel in C_x als in C_y, dan geldt $C_x = C_y$.*

Bewijs. 1: Er geldt $x = \gamma_e(x)$, dus $x \in C_x$ voor elke $x \in G$.
2: Voor $x, y \in G$ geldt $x = \gamma_a(y)$ precies dan als $y = \gamma_{a^{-1}}(x)$. Hieruit volgt de bewering.
3: Ons gegeven hier is, dat er $a, b \in G$ bestaan waarvoor $\gamma_a(y) = x$ en $\gamma_b(z) = y$. Dit impliceert dat $\gamma_{ab}(z) = \gamma_a\gamma_b(z) = \gamma_a(y) = x$, dus $x \in C_z$.
4: Elk element $a \in G$ zit in een C_x, want $a \in C_a$ vanwege 1). Geldt $a \in C_x$ en $a \in C_y$, dan zijn er $c, d \in G$ met $a = \gamma_c(x)$ en $a = \gamma_d(y)$. Een $z \in C_x$ is dan te schrijven als $z = \gamma_f(x) = \gamma_{fc^{-1}d}(y)$, dus $z \in C_y$. Omgekeerd werkt hetzelfde argument met x, y verwisseld. Dus $C_x = C_y$. □

Voorbeeld 6.1.8 We proberen S_n te schrijven als disjuncte vereniging van conjugatieklassen. Neem $\sigma \in S_n$ willekeurig. Dan is σ te schrijven als product van disjuncte cykels: $\sigma = (a_1 \ \dots \ a_{\ell_1})(a_{\ell_1+1} \ \dots \ a_{\ell_2}) \dots (a_{\ell_{s-1}+1} \ \dots \ a_{\ell_s})$. Elke permutatie τ die a_i naar i stuurt (en de overige getallen in $\{1, \dots, n\}$ bijectief naar $\{\ell_s + 1, \dots, n\}$ afbeeldt) levert $\tau\sigma\tau^{-1} = (1 \ 2 \ \dots \ \ell_1)(\ell_1 + 1 \ \dots \ \ell_2) \dots (\ell_{s-1}+1 \ \dots \ell_s)$. Hieruit zien we dat alle producten van disjuncte $\ell_1, \ell_2 - \ell_1, \dots, \ell_s - \ell_{s-1}$-cykels geconjugeerd zijn. De conjugatieklasse hangt dus alleen maar af van de verzameling $\{\ell_1, \ell_2 - \ell_1, \dots, \ell_s - \ell_{s-1}\}$. In het bijzonder is het aantal onderling verschillende conjugatieklassen gelijk aan het aantal *partities* van n; dat is het aantal mogelijke schrijfwijzen $n = \sum n_i$, met n_i positief en geheel, waarbij we niet letten op de volgorde van de n_i's. Dit aantal wordt met $p(n)$ aangeduid. Dus $p(2) = 2$ want $2 = 2$ en $2 = 1+1$, en $p(4) = 5$ $(4, 3+1, 2+2, 2+1+1, 1+1+1+1)$.

Voorbeeld 6.1.9 Voor de alternerende groep A_n is het bepalen van alle conjugatieklassen beduidend moeilijker dan voor S_n. We bekijken het geval $n \leq 5$. Voor $n \leq 3$ is A_n commutatief. Dus in die gevallen geldt $\tau\sigma\tau^{-1} = \sigma$ voor elke $\sigma, \tau \in A_n$, oftewel $C_\sigma = \{\sigma\}$ voor elke σ.

De groep A_4 bestaat uit (1), drie producten van twee disjuncte 2-cykels, en acht 3-cykels. Schrijf $\{3, 4\} = \{a, b\}$, dan geldt voor $\tau = (2 \ a \ b) \in A_4$ dat $\tau(1 \ 2)(3 \ 4)\tau^{-1} = (1 \ a)(b \ 2)$. Dus de producten van twee 2-cykels zijn onderling geconjugeerd. Door bijvoorbeeld (1 2 3) te conjugeren met alle 12 elementen van A_4 volgt dat $C_{(1\,2\,3)} = \{(1 \ 2 \ 3), (1 \ 3 \ 4), (1 \ 4 \ 2), (2 \ 4 \ 3)\}$. De overige 4 cykels van lengte 3 vormen ook precies een conjugatieklasse.

De groep A_5 bestaat uit 3-cykels, 5-cykels, producten van 2 disjuncte 2-cykels en de identiteit. Alle 3-cykels vormen samen één conjugatieklasse. Immers, is $\sigma = (a_1 \ a_2 \ a_3)$, en is τ een permutatie die a_i naar i stuurt, dan $\tau\sigma\tau^{-1} = (1 \ 2 \ 3)$. Onze enige zorg hier is, dat we zo'n τ in A_5 moeten kiezen. Dat is echter altijd mogelijk, door namelijk evt. τ te laten volgen door de 2-cykel (4 5). De producten van twee disjuncte 2-cykels zijn ook allemaal geconjugeerd. Zo'n product σ houdt namelijk precies één getal i vast, en een

$\tau\sigma\tau^{-1}$ houdt dan het getal $\tau(i)$ vast. Op deze wijze zien we door een geschikte τ te kiezen, dat σ geconjugeeerd is met een product dat 5 vasthoudt. Echter dit levert precies de producten op die we al bij A_4 bekeken hebben, en die zijn allemaal geconjugeerd. Wat nog overblijft zijn de 5-cykels. Elke 5-cykel σ is te schrijven als $\sigma = (1\ a\ b\ c\ d)$, dus er zijn 24 zulke 5-cykels. Er geldt $\tau\sigma\tau^{-1} = \sigma$ precies dan als $(\tau(1)\ \tau(a)\ \tau(b)\ \tau(c)\ \tau(d)) = (1\ a\ b\ c\ d)$, en dus precies dan als τ een macht is van σ. De machten van σ vormen een ondergroep H van A_n, bestaande uit 5 elementen. Schrijf A_n als disjuncte vereniging van deelverzamelingen $H\pi$, voor $\pi \in A_n$. Is $\tau \in H\pi$, dan $\tau\sigma\tau^{-1} = \pi\sigma\pi^{-1}$. Verder geldt dat $\pi_1\sigma\pi_1^{-1} = \pi_2\sigma\pi_2^{-1}$ precies dan, als $\pi_2^{-1}\pi_1 \in H$, oftewel, als $\pi_1 \in H\pi_2$. Dus er zijn voor een vaste 5-cykel σ precies evenveel onderling verschillende elementen $\tau\sigma\tau^{-1}$, als er verschillende verzamelingen $H\pi$ zijn. Dat zijn er $\#A_5/\#H = 12$. Hieruit volgt dat de verzameling 5-cykels in twee disjuncte conjugatieklassen van elk 12 elementen uiteenvalt. In totaal vinden we hier dus 5 conjugatieklassen, bestaande uit resp. $1, 20, 15, 12$ en 12 elementen.

In bovenstaand voorbeeld hebben we voor A_5 een resultaat gebruikt dat veel algemener waar is:

Stelling 6.1.10 *Is G een groep en $a \in G$, dan is $N(a) = \{x \in G \mid \gamma_x(a) = a\}$ een ondergroep van G. Is G eindig, dan geldt*

$$\#G = \#N(a) \cdot \#C_a.$$

Bewijs. Omdat $\gamma_e = id$ en $\gamma_{x^{-1}} = \gamma_x^{-1}$ en $\gamma_{xy} = \gamma_x\gamma_y$, is $N(a)$ een ondergroep. Het bewijs van Stelling 3.2.7 laat zien, dat G een disjuncte vereniging is van deelverzamelingen $g_iN(a)$, voor zekere $g_i \in G$. Elk van deze deelverzamelingen heeft $\#N(a)$ elementen, dus we zijn klaar als we hebben aangetoond dat het aantal g_i's hier gelijk is aan $\#C_a$. Welnu, elke g_i levert een element $x_i = \gamma_{g_i}(a) \in C_a$. Is $x \in C_a$ willekeurig, dan $x = \gamma_g(a)$ voor een $g \in G$. Dan $g \in g_iN(a)$ voor zekere i, dus $g = g_ih$ met $h \in N(a)$, en $x = \gamma_g(a) = \gamma_{g_i}\gamma_h(a) = \gamma_{g_i}(a) = x_i$. Is $x_i = x_j$, dan $g_j^{-1}g_iag_i^{-1}g_j = a$, dus $g_j^{-1}g_i \in N(a)$. Hieruit volgt $g_iN(a) = g_jN(a)$, en dus $g_i = g_j$. Hiermee is de stelling bewezen. □

Als toepassing bepalen we een paar conjugatieklassen in A_n.

Stelling 6.1.11 *Laat $n \geq 5$.*

1. *In A_n zijn alle 3-cykels onderling geconjugeerd.*
2. *In A_n zijn alle producten van twee disjuncte 2-cykels onderling geconjugeerd.*

Bewijs. Laat $\sigma = (1\ 2\ 3) \in A_n$. De ondergroep $N(\sigma) \subset A_n$ bestaat per definitie uit alle even permutaties τ die voldoen aan $\tau\sigma\tau^{-1} = \sigma$, oftewel $(\tau(1)\ \tau(2)\ \tau(3)) = (1\ 2\ 3)$. Hieruit volgt dat zo'n τ een macht van $(1\ 2\ 3)$ maal een even permutatie op $\{4, 5, \ldots, n\}$ moet zijn. Dus $\#N(\sigma) = 3 \cdot (n-3)!/2$. Merk op dat we hier gebruik maken van het feit dat $n \geq 5$. Stelling 6.1.10 impliceert dat $\#C_\sigma = (n!/2)/(3 \cdot (n-3)!/2) = 2\binom{n}{3}$. Dit is precies het aantal 3-cykels in A_n, dus omdat C_σ uit 3-cykels bestaat concluderen we dat alle 3-cykels geconjugeerd zijn.

Een alternatief bewijs werkt als volgt. Laat $(a\ b\ c)$ een 3-cykel zijn. Kies een permutatie τ met $\tau(1) = a, \tau(2) = b$ en $\tau(3) = c$. Zowel conjugeren met τ als met $\tau \cdot (4\ 5)$ beeldt $(1\ 2\ 3)$ op $(a\ b\ c)$ af. Omdat óf τ, óf $\tau \cdot (4\ 5)$ een element is van A_n, zijn dus $(1\ 2\ 3)$ en $(a\ b\ c)$ geconjugeerd binnen A_n.

Beide hier gegeven bewijzen werken met de voor de hand liggende aanpassingen ook voor de tweede bewering in de stelling; de details laten we als een nuttige oefening aan de lezer over. □

Is G een groep en $H \subset G$ een ondergroep, dan is voor $g_1, g_2 \in G$ de verzameling g_1H resp. Hg_2 bijectief op H af te beelden, namelijk door van links resp. van rechts te vermenigvuldigen met de inverse van g_1 resp. g_2. Dus alle verzamelingen van dit soort zijn onderling bijectief. In het bijzonder hebben ze, zoals al vaker is opgemerkt, in het geval dat H eindig is allemaal evenveel elementen. Verder hebben we al eerder opgemerkt dat het feit dat H een ondergroep is impliceert, dat óf $g_1H = g_2H$ (en dat is het geval precies dan, als $g_1g_2^{-1} \in H$), óf $g_1H \cap g_2H = \emptyset$. Ga zelf na hoe deze beweringen bewezen kunnen worden!

Definitie 6.1.12 Is H een ondergroep van een groep G, dan is de *index* van H in G gelijk aan het totaal aantal disjuncte deelverzamelingen van de vorm Hg in G. De index noteren we als $[G : H]$. Is dit aantal niet eindig, dan schrijven we $[G : H] = \infty$.

Opmerking 6.1.13 Omdat 'inverse nemen' $\iota : G \to G$ een bijectie is, en $\iota(Hg) = \iota(g)H$, geldt dat we de index evengoed in termen van deelverzamelingen van de vorm gH hadden kunnen definiëren.

Stelling 6.1.14 *Is G een eindige groep, dan is $[G : H]$ ook eindig voor elke ondergroep H. Er geldt bovendien dat*

$$\#G = [G : H] \cdot \#H.$$

Bewijs. Dit is precies wat in het bewijs van Stelling 3.2.7 al is aangetoond. □

Voorbeeld 6.1.15 Ook voor een oneindige groep G kan de index van een ondergroep eindig zijn. Bijvoorbeeld geldt voor $G = \mathbb{Z}$ dat de ondergroepen precies de groepen $n\mathbb{Z}$ zijn. Omdat voor $n \neq 0$ geldt $\mathbb{Z} = n\mathbb{Z} \cup 1 + n\mathbb{Z} \cup \ldots \cup n - 1 + n\mathbb{Z}$, is $[\mathbb{Z} : n\mathbb{Z}] = n$, en $[\mathbb{Z} : 0\mathbb{Z}] = \infty$.

6.2 Sylow ondergroepen

Definitie 6.2.1 (Genoemd naar P.L.M. Sylow, Noors wiskundige, 1832–1918.)
Laat G een eindige groep zijn met $\#G = p^n \cdot m$ waarbij p een priemgetal is, $n \geq 1$ en $\text{ggd}(p, m) = 1$. Een *Sylow p-groep* in G is een ondergroep $H \subset G$ met $\#H = p^n$.

Voorbeeld 6.2.2 Neem een priemgetal p en $n, m \geq 1$ met $\text{ggd}(p, m) = 1$. Dan is $G = \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ een groep met precies $p^n m$ elementen. Er bestaat precies één Sylow p-groep in G, namelijk $H = \mathbb{Z}/p^n\mathbb{Z} \times \{\overline{0}\}$. Dit is namelijk inderdaad een Sylow p-groep in G. Is ook $H' \subset G$ zo'n groep, bekijk dan een willekeurige $h = (a \bmod p^n, b \bmod m) \in H'$. Er geldt $\text{ord}(h) | \#H' = p^n$. Zou $b \bmod m \neq \overline{0}$, dan zou $1 < \text{ord}(b \bmod m) | \#\mathbb{Z}/m\mathbb{Z} = m$. Omdat $\text{ggd}(p, m) = 1$, bevat $\text{ord}(b \bmod m)$ dan een priemdeler $\ell \neq p$. Maar dan ook $\ell | \text{ord}(h) | p^m$, en dat is niet het geval. Dus geldt $b \bmod m = 0 \bmod m$, oftewel $H' \subset H$. Omdat $\#H' = p^n = \#H$, volgt hieruit $H' = H$.

Stelling 6.2.3 *Laat G een groep zijn met $\#G = p^n m$ waarbij p een priemgetal is en $n, m > 0$ en ggd$(p, m) = 1$.*

1. *G bevat een Sylow p-groep.*
2. *Het aantal onderling verschillende Sylow p-groepen in G is $\equiv 1 \bmod p$.*
3. *Zijn H en H' Sylow p-groepen in G, dan geldt $H' = \gamma_a(H)$ voor een $a \in G$.*
4. *Het aantal onderling verschillende Sylow p-groepen in G is een deler van m.*

Bewijs. Schrijf N voor het totale aantal onderling verschillende Sylow p-groepen in G. We moeten onder andere aantonen dat $N \neq 0$; dit volgt zeker als we de bewering in 2) die zegt dat $N \equiv 1 \bmod p$ bewezen hebben. Dit zullen we laten zien door de collectie van alle deelverzamelingen in G die uit precies p^n elementen bestaan te bestuderen.

Is $H \subset G$ een Sylow p-groep, dan heeft voor elke $g \in G$ de verzameling Hg precies p^n elementen. Vanwege Stelling 6.1.14 zijn er voor gegeven H

precies $\#G/\#H = m$ zulke verzamelingen Hg. Er geldt voor $x \in G$ dat $xHg = Hg$ precies dan als $xH = H$, en dat is het geval dan en slechts dan als $x \in H$. Dus uit $V = Hg$ vinden we H terug als de elementen $x \in G$ met $xV = V$. Bezie nu een willekeurige verzameling $V \subset G$ die uit p^n elementen bestaat, en die de eigenschap heeft dat $\{x \in G \mid xV = V\}$ een ondergroep H van G is met p^n elementen. Is $v \in V$ en $x \in H$, dan volgt vanwege $xV = V$ dat ook $xv \in V$. Dus $Hv \subset V$, en omdat $\#Hv = p^n = \#V$, volgt $V = Hv$. Conclusie: elke verzameling V met de genoemde eigenschappen is van de vorm Hg, voor een $g \in G$ en een Sylow p-groep H. Er bestaan dus in totaal precies $N \cdot m$ zulke verzamelingen.

We bekijken vervolgens alle overige deelverzamelingen $V \subset G$ met $\#V = p^n$. Voor zo'n deelverzameling noteren we $G_V = \{x \in G \mid xV = V\}$. Men gaat eenvoudig na dat G_V een ondergroep is van G. Omdat $V \subset G$ te schrijven is als disjuncte vereniging van deelverzamelingen van de vorm $G_V \cdot v$, die elk uit $\#G_V$ elementen bestaan, volgt $\#G_V | \#V = p^n$. De V's met $\#G_V = p^n$ zijn precies degenen die we hierboven al gezien hebben; daarvan zijn er Nm. Schrijf

$$\mathcal{P} = \left\{V \subset G \mid \#V = p^n \text{ en } \#G_V = p^k \text{ voor een } k < n\right\}.$$

Dan geldt

$$\binom{p^n m}{p^n} = Nm + \#\mathcal{P}.$$

We zullen laten zien dat $\#\mathcal{P} \equiv 0 \bmod p$. Laat $V \in \mathcal{P}$. Voor elke $x \in G$ is dan ook $xV \in \mathcal{P}$, want xV bevat p^n elementen, en $g \cdot (xV) = xV$ precies dan als $x^{-1}gxV = V$. Dus $G_{xV} = \gamma_{x^{-1}}(G_V)$, en dus hebben G_V en G_{xV} in het bijzonder evenveel elementen. Dit toont aan dat als $V \in \mathcal{P}$ dan ook $xV \in \mathcal{P}$. Schrijf $G = \cup g_i G_V$, met $[G : G_V]$ verschillende g_i's. Elke xV is dan gelijk aan een $V_i = g_i V$, want $x = g_i g$ voor zekere g_i en zekere $g \in G_V$, en dus $xV = g_i g V = g_i V = V_i$. De V_i's zijn onderling verschillend omdat $V_i = V_j$ zou impliceren dat $g_i^{-1} g_j \in G_V$ en dus $g_i G_V = g_j G_V$. Er geldt $[G : G_V] \equiv 0 \bmod p$, dus op deze wijze wordt $\mathcal{P}$ opgedeeld in deelverzamelingen die elk uit een veelvoud van p elementen bestaan. Dit bewijst dat $\#\mathcal{P} \equiv 0 \bmod p$.

De conclusie hieruit is, dat

$$\binom{p^n m}{p^n} = Nm + \#\mathcal{P} \equiv Nm \bmod p.$$

Omdat $\text{ggd}(m, p) = 1$ is $\overline{m} = m \bmod p$ een eenheid in $\mathbb{Z}/p\mathbb{Z}$, en de formule geeft dan

$$N \bmod p = \overline{m}^{-1} \cdot \binom{p^n m}{p^n} \bmod p.$$

Dit toont aan dat $N \bmod p$ alleen maar afhangt van p, n en m, en niet van de groep G zelf! In het bijzonder kunnen we voor G de groep $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ kiezen. In Voorbeeld 6.2.2 zagen we dat dan geldt $N = 1$. Hieruit volgt dat voor *iedere* groep G met $\#G = p^n m$ geldt dat $N \bmod p = 1 \bmod p$. Dit bewijst 1) en 2).

Nu het bewijs van 3) en 4). Stel H en H' zijn allebei Sylow p-groepen in G. Zoals we weten zijn er precies $[G : H] = m$ verschillende verzamelingen van de vorm gH in G, en G is hun vereniging. We delen deze collectie verzamelingen gH op in twee klassen $\mathcal{H}_1, \mathcal{H}_2$ als volgt: $gH \in \mathcal{H}_1$ precies dan, als voor elke $h \in H'$ geldt dat $hgH = gH$. En $gH \in \mathcal{H}_2$ precies dan, als er een $h \in H'$ bestaat met $hgH \neq gH$. Dan geldt $m = \#\mathcal{H}_1 + \#\mathcal{H}_2$. We gaan, in feite op precies dezelfde manier als we dat hiervoor voor de verzameling $\mathcal{P}$ gedaan hebben, laten zien dat $\#\mathcal{H}_2 \equiv 0 \bmod p$. Laat $gH \in \mathcal{H}_2$. Dan is $H'' = \{h \in H' \mid hgH = gH\}$ een ondergroep van H'. Uit de definitie van $\mathcal{H}_2$ volgt dat $H'' \neq H'$, dus $p|[H' : H'']$. Door $h \in H'$ te laten variëren krijgen we zo $[H' : H'']$ onderling verschillende verzamelingen hgH. Men rekent eenvoudig na dat elk van deze hgH's weer een element van $\mathcal{H}_2$ is. Op deze manier krijgen we een opdeling van heel $\mathcal{H}_2$ in steeds een veelvoud van p elementen, dus $\#\mathcal{H}_2 \equiv 0 \bmod p$. Dit impliceert

$$\#\mathcal{H}_1 \equiv m \bmod p \neq 0 \bmod p,$$

dus in het bijzonder volgt dat $\mathcal{H}_1$ niet leeg is. Dit levert een gH met de eigenschap $hgH = gH$ voor elke $h \in H'$. Anders gezegd: $g^{-1}hg \in H$ voor elke $h \in H'$, oftewel $H' \subset \gamma_g(H)$. Hieruit volgt 3).

Tenslotte nog 4). Zij H een willekeurige Sylow p-groep in G. Er zijn in totaal N zulke groepen, en we hebben al aangetoond dat ze allemaal te schrijven zijn als $\gamma_g(H)$ voor een $g \in G$. Definieer

$$N(H) = \{g \in G \mid \gamma_g(H) = H\}.$$

Dit is een ondergroep van G, en door te schrijven $G = \cup g_i N(H)$ vinden we op de gebruikelijke manier dat alle Sylow p-ondergroepen in G precies de $\gamma_{g_i}(H)$ zijn. Dus volgt $N = [G : N(H)]$. Omdat H een ondergroep is van $N(H)$, volgt nu dat $N|m$. Immers, $\#N(H) = [N(H) : H] \cdot \#H$ en

$$N = [G : N(H)] = \#G/\#N(H) = \#G/([N(H) : H] \cdot \#H)|\#G/\#H = m.$$

Hiermee is de stelling volledig bewezen. □

Gevolg 6.2.4 *Voor p een priemgetal en $n, m > 0$ met $ggd(p, m) = 1$ geldt*

$$\binom{p^n m}{p^n} \equiv m \bmod p.$$

Bewijs. In het bewijs van Stelling 6.2.3 hebben we gezien dat $\binom{p^n m}{p^n} \equiv Nm \bmod p$, waarbij $N \equiv 1 \bmod p$. Dit impliceert het gevolg. □

Voorbeeld 6.2.5 De groep S_4 heeft $24 = 3 \cdot 8$ elementen. Het aantal Sylow 3-groepen in S_4 is blijkens Stelling 6.2.3 een deler van 8, en het is van de vorm $3k + 1$. Het moeten er dus 1 of 4 zijn. Elke deelverzameling van de vorm $\{(1), (a\ b\ c), (a\ c\ b)\}$ met $a \neq b, b \neq c, c \neq a$ is inderdaad een ondergroep, en dit levert er precies 4.

Het aantal Sylow 2-groepen in S_4 is oneven en een deler van 3. Dat kunnen er dus 1 of 3 zijn. Is H zo'n groep, dan $\#H = 8$, dus elk element in H heeft een orde die 8 deelt. Hieruit volgt dat H bestaat uit 4-cykels, 2-cykels, producten van twee disjuncte 2-cykels en de identiteit. Er kunnen hoogstens twee 2-cykels in H zitten en deze moeten dan disjunct zijn. Immers, anders zou er een product $(a\ b)(b\ c) = (a\ b\ c)$ in H zitten, en dat is niet het geval. Het is niet mogelijk dat er precies één 2-cykel in H zit. Immers, dat zou betekenen dat elke ondergroep $\sigma H \sigma^{-1}$ precies één 2-cykel bevat, en omdat we op deze manier alle mogelijke 2-cykels kunnen krijgen, zijn er dan minstens evenveel Sylow 2-groepen in S_4 als er 2-cykels zijn, wat niet mogelijk is. Dus bevat H óf geen, óf precies twee (onderling disjuncte) 2-cykels. Het aantal 4-cykels in H is even, want een 4-cykel is niet gelijk aan z'n inverse, en met elk ervan moet ook de inverse in H zitten. Verder is het kwadraat van een 4-cykel gelijk aan een product van twee disjuncte 2-cykels, en elk paar bestaande uit een 4-cykel en z'n inverse geeft aanleiding tot hetzelfde kwadraat terwijl een ander zo'n paar ook weer een ander kwadraat oplevert. Hieruit volgt dat er precies één zo'n paar 4-cykels in H moet zitten. Immers, zijn het er twee of meer, dan volgt door deze onderling te conjugeren dat *alle* 4-cykels in H zitten, en dus ook alle producten van disjuncte 2-cykels. Dat zou betekenen dat $\#H \geq 1 + 6 + 3 = 10$ hetgeen niet het geval is. Het is ook niet mogelijk dat er helemaal geen 4-cykels in H zitten, want met de hooguit twee 2-cykels en de drie producten van twee disjuncte 2-cykels en de identiteit hebben we samen nog geen 8 elementen. Dus moet H uit precies twee disjuncte 2-cykels, alle drie producten van disjuncte 2-cykels, en nog één paar bestaande uit een 4-cykel en z'n inverse (plus de identiteit) bestaan. Wat rekenwerk levert inderdaad drie zulke ondergroepen die onderling geconjugeerd zijn. Eén ervan bestaat uit $(1), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3)$ en $(2\ 4)$.

We hadden onszelf overigens al dit werk kunnen besparen: de symmetriegroep van het vierkant, D_4, bestaat uit precies 8 elementen. Deze elementen permuteren de hoekpunten van het vierkant. Dus D_4 kan worden opgevat als ondergroep van S_4. Helemaal expliciet: neem het vierkant in het x, y-vlak met hoekpunten $(\pm 1, \pm 1)$. Noem het hoekpunt in het i-de kwadrant i.

Roteren over 90 graden tegen de wijzers van de klok levert dan de permutatie (1 2 3 4) op de hoekpunten. Spiegelen in de x-as correspondeert met (1 4)(2 3). Spiegelen in de diagonaal $x + y = 0$ levert (1 3), enzovoort.

We laten aan een tweetal voorbeelden zien hoe Stelling 6.2.3 gebruikt kan worden.

Stelling 6.2.6 *Gegeven is een groep G met $\#G = pq$, waarbij p en q onderling verschillende priemgetallen zijn met de eigenschap $p \not\equiv 1 \bmod q$ en $q \not\equiv 1 \bmod p$. Dan geldt $G \cong \mathbb{Z}/pq\mathbb{Z}$.*

Bewijs. Een element $g \in G$ heeft een orde die een deler is van pq. Dus $\mathrm{ord}(g) \in \{1, p, q, pq\}$. Het enige element van orde 1 is $e \in G$. Geldt $\mathrm{ord}(g) = p$, dan is $\langle g \rangle$ een Sylow p-groep in G. Het aantal zulke groepen is een deler van q, dus het is 1 of q. Verder is dit aantal $\equiv 1 \bmod p$. Omdat $q \not\equiv 1 \bmod p$ moet het aantal Sylow p-groepen dus wel precies gelijk zijn aan 1. Elk element in G met orde p zit in deze Sylow p-groep, dus er zijn hoogstens $p - 1$ zulke elementen. (In feite precies $p - 1$, maar dat hebben we niet eens nodig.)

Precies hetzelfde argument toont aan, dat er hoogstens $q - 1$ elementen in G zijn waarvan de orde q is. Omdat $1 + p - 1 + q - 1 < pq = \#G$, bevat G dus elementen met orde pq. Is $g \in G$ zo'n element, dan $\langle g \rangle = G$, en $g \mapsto 1 \bmod pq$ levert een isomorfisme: $G \cong \mathbb{Z}/pq\mathbb{Z}$. □

Voorbeeld 6.2.7 Passen we Stelling 6.2.6 toe met $p = 3$ en $q = 5$, dan volgt dat er op isomorfie na slechts 1 groep met 15 elementen bestaat, en dat is $\mathbb{Z}/15\mathbb{Z}$.

Stelling 6.2.8 *(Augustin-Louis Cauchy, Frans wiskundige, 1789–1857)*
Is G een eindige groep, en is p een priemgetal dat het aantal elementen van G deelt, dan bestaat er een element $g \in G$ met $\mathrm{ord}(g) = p$.

Bewijs. Kies een Sylow p-groep $H \subset G$. Die bestaat vanwege Stelling 6.2.3, en $\#H = p^k$ met $k \geq 1$. Neem $x \in H$ met $x \neq e$ willekeurig. Dan $\mathrm{ord}(x) \neq 1$, en $\mathrm{ord}(x) | p^k$. Dit impliceert dat $\mathrm{ord}(x) = p^\ell$, met $1 \leq \ell \leq k$. Voor $g = x^{p^{\ell-1}}$ geldt dan $\mathrm{ord}(g) = p$, zoals verlangd. □

6.3 Opgaven

1. Bepaal van iedere conjugatieklasse in S_6 uit hoeveel elementen deze bestaat.

2. Bepaal het aantal conjugatieklassen in A_6, en geef voor elk ervan het aantal elementen.

3. Geef een bewijs voor de tweede uitspraak in Stelling 6.1.11.

4. In de groep D_n hebben we twee elementen ρ, σ, gegeven door $\rho =$ 'draaien over $2\pi/n$ radialen tegen de richting van de klok', en $\sigma =$ 'spiegelen in de x-as'.

   (a) Laat zien dat $\sigma\rho\sigma = \rho^{-1}$.

   (b) Toon aan dat elke $\tau \in D_n$ te schrijven is als $\rho^a\sigma^b$, met $0 \leq a < n$ en $0 \leq b \leq 1$.

   (c) Neem n oneven, en bewijs dat er één conjugatieklasse in D_n bestaande uit n elementen is, ook één bestaande uit 1 element, en verder $(n-1)/2$ met ieder 2 elementen.

   (d) Bewijs dat voor even n de groep D_n uiteenvalt in 2 conjugatieklassen met 1 element, $(n-2)/2$ conjugatieklassen met 2 elementen, en 2 met $n/2$ elementen.

5. Stel G is een eindige groep met $\#G = n$, en G bestaat uit precies 3 conjugatieklassen.

   (a) Laat zien dat $n = 1 + a + b$, met $1 \leq a \leq b$ en $a|n$ en $b|n$.

   (b) Bepaal alle mogelijke oplossingen van de in (a) gevonden gelijkheid. (Deel bijv. door n, en ga na dat $a \leq 3$ moet gelden.)

   (c) Gebruik dat een niet-commutatieve groep met 6 elementen isomorf is met S_3, en bewijs dan dat $G \cong \mathbb{Z}/3\mathbb{Z}$ of $G \cong S_3$. Ga na dat deze twee groepen inderdaad uit precies 3 conjugatieklassen bestaan.

6. Bewijs dat voor een groep G, een ondergroep $H \subset G$ en een element $g \in G$ geldt dat $[G : H] = [G : \gamma_g(H)]$.

7. Toon aan dat een eindige *abelse* groep G voor elk priemgetal p met $p|\#G$ precies één Sylow p-groep heeft.

8. Bepaal voor elke p het aantal Sylow p-groepen in S_5.

9. We beschrijven alle Sylow p-groepen in S_6.

(a) Laat zien dat de Sylow 2-groepen isomorf zijn met $D_4 \times \mathbb{Z}/2\mathbb{Z}$, en dat er $\binom{6}{2} \cdot 3 = 45$ zulke groepen zijn. (Denk aan een Sylow 2-groep in S_4, samen met de permutatie (5 6).)

(b) Laat zien dat de Sylow 3-groepen isomorf zijn met $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, en dat er $\binom{6}{3}/2 = 10$ zulke groepen zijn. (Denk aan disjuncte 3-cykels.)

(c) Laat zien dat de Sylow 5-groepen isomorf zijn met $\mathbb{Z}/5\mathbb{Z}$, en dat er daarvan 36 zijn.

10. In deze opgave geven we een ander bewijs voor het feit dat als 3 het aantal elementen van een eindige groep G deelt, dan heeft die groep een element met orde 3. Het bewijs in deze opgave is afkomstig van J. McKay, en het kan gegeneraliseerd worden tot een willekeurig priemgetal in plaats van '3'.

    Laat G een eindige groep zijn met $\#G = n \equiv 0 \bmod 3$. Neem $\mathcal{D} = \{(a,b,c) \in G \times G \times G \mid abc = e\}$ en $\mathcal{D}_1 = \{(a,b,c) \in \mathcal{D} \mid a = b = c\}$ en $\mathcal{D}_2 = \mathcal{D} \setminus \mathcal{D}_1$.

    (a) Laat zien dat $\#\mathcal{D} = n^2 \equiv 0 \bmod 3$.

    (b) Toon aan dat als $(a,b,c) \in \mathcal{D}$, dan ook $(b,c,a) \in \mathcal{D}$ en $(c,a,b) \in \mathcal{D}$.

    (c) Toon aan dat als $(a,b,c) \in \mathcal{D}_2$, dan zijn (a,b,c) en (b,c,a) en (c,a,b) alle drie verschillend.

    (d) Bewijs dat $\#\mathcal{D}_2 \equiv 0 \bmod 3$.

    (e) Bewijs dat $\#\mathcal{D}_1 \geq 3$, en dat het aantal elementen in G met orde 3 een drievoud plus twee is.

11. Laat G een groep zijn met $\#G = 6$.

    (a) Beargumenteer dat er een $a \in G$ is met $\mathrm{ord}(a) = 2$ en ook een $b \in G$ met $\mathrm{ord}(b) = 3$.

    (b) Laat zien dat als a, b als in (a), en $\gamma_b(a) = a$, dan $\mathrm{ord}(ab) = 6$ en $G \cong \mathbb{Z}/6\mathbb{Z}$.

    (c) Laat zien dat als a, b als in (a), en $\gamma_b(a) \neq a$, dan bevat C_a precies 3 elementen die allemaal orde 2 hebben in G, en $G \cong S_3$.

7 Normaaldelers en factorgroepen

Terugblikkend naar Hoofdstuk 2 kunnen we achteraf zeggen, dat we daar uitgaande van de groep $\mathbb{Z}$ en de ondergroep $N\mathbb{Z}$ een nieuwe groep geconstrueerd hebben. Namelijk, de *elementen* van die nieuwe groep zijn precies de *restklassen* $a + N\mathbb{Z}$. En in Stelling 2.1.5 met de daarop volgende definitie en opmerking werd aangetoond, dat de groepsbewerking op $\mathbb{Z}$ (optellen) aanleiding geeft tot een groepsbewerking (ook optellen) op die restklassen. We zullen in dit hoofdstuk precies hetzelfde gaan proberen voor een willekeurige groep G in plaats van $\mathbb{Z}$, en een willekeurige ondergroep $H \subset G$. Het zal blijken dat alleen voor bepaalde ondergroepen, de zogeheten 'normaaldelers', zo'n constructie mogelijk is. Het is wellicht goed, vóór het bestuderen van dit hoofdstuk nog even Sectie 2.1 door te lezen.

7.1 Normaaldelers

Voor een groep G en een ondergroep H hebben we in Stelling 6.1.2 gezien dat als $a \in G$, dan is de geconjugeerde $\gamma_a(H) = aHa^{-1}$ ook een ondergroep van G. Zelfs zijn H en $\gamma_a(H)$ isomorf. In het algemeen geldt *niet* dat $H = \gamma_a(H)$. Bijvoorbeeld is $H = \{(1), (1\ 2)\}$ een ondergroep van S_3. Nemen we $a = (1\ 3)$, dan $\gamma_a(H) = \{(1), (2\ 3)\} \neq H$.

Definitie 7.1.1 Een ondergroep H van een groep G heet een *normaaldeler* als voor elke $a \in G$ geldt dat $H = aHa^{-1}$.

Voorbeeld 7.1.2 In een commutatieve groep G is elke ondergroep H een normaaldeler. Immers, $aha^{-1} = aa^{-1}h = h$ voor alle a, h in zo'n commutatieve groep, dus in het bijzonder is $aHa^{-1} = H$.

Voorbeeld 7.1.3 In de diëdergroep D_n vormen de rotaties een ondergroep, die een normaaldeler is. Immers, gezien als lineaire afbeeldingen op $\mathbb{R}^2$ zijn de rotaties in D_n precies die elementen van D_n die determinant 1 hebben. Is ρ zo'n rotatie en $a \in D_n$ willekeurig, dan $\det(a\rho a^{-1}) = \det(a)\det(\rho)\det(a^{-1}) = \det(a)\det(a)^{-1} = 1$, dus $a\rho a^{-1}$ is ook een rotatie.

Voorbeeld 7.1.4 We gaan alle normaaldelers in S_4 bepalen. Stel H is zo'n normaaldeler en $\sigma \in H$. Omdat $H = \tau H \tau^{-1}$ voor elke $\tau \in S_n$, bevat H dan ook de hele conjugatieklasse C_σ. Vanwege het feit dat S_4 een disjuncte vereniging van conjugatieklassen is (Stelling 6.1.7), is dus ook H een disjuncte vereniging van conjugatieklassen in S_4. Deze klassen hebben resp. $1, 6, 8$ en 3 elementen. Er geldt $(1) \in H$, dus $\#H$ is een som van sommige van deze getallen, waarbij zeker 1 als term voorkomt. Ook geldt $\#H | \#S_4 = 24$

vanwege Stelling 3.2.7. Hiermee blijven nog maar een paar mogelijkheden over:

1. $\#H = 1$, dus H bestaat uit alleen het eenheidselement in S_4. Dit is inderdaad een ondergroep, en zelfs een normaaldeler.

2. $\#H = 1 + 3 = 4$, dus H bestaat uit het eenheidselement plus de drie producten van twee disjuncte 2-cykels. Dit levert inderdaad een normaaldeler in S_4.

3. $\#H = 1 + 3 + 8 = 12$. In dit geval bestaat H uit de identiteit, de producten van twee disjuncte 2-cykels, en alle 3-cykels. Dus $H = A_4$, en dat is een normaaldeler in S_4.

4. $\#H = 1 + 3 + 8 + 12 = 24$, dus $H = S_4$.

We zien dus dat hoewel S_4 heel veel ondergroepen heeft, toch behalve S_4 zelf en (1) er slechts twee 'echte' normaaldelers in S_4 zijn.

Voorbeeld 7.1.5 We zagen al dat A_4 een normaaldeler in S_4 is. Er geldt zelfs algemeen dat A_n een normaaldeler in S_n is. Dit volgt uit het feit dat voor permutaties σ, τ geldt dat $\epsilon(\sigma) = \epsilon(\tau\sigma\tau^{-1})$. (We kunnen ook direct inzien dat conjugeren een product van disjuncte cykels overvoert in precies zo'n product van disjuncte cykels. Dus in het bijzonder verandert het teken niet bij conjugatie, hetgeen impliceert dat $\tau A_n \tau^{-1} = A_n$.)

Voorbeeld 7.1.6 Stel G is een eindige groep met $\#G = p^n m$ waarbij p priem, $n \geq 1$ en $\text{ggd}(p, m) = 1$. Laat H een Sylow p-groep in G zijn. Alle geconjugeerde groepen aHa^{-1} voor $a \in G$ zijn dan ook Sylow p-groepen, en in Stelling 6.2.3 hebben we afgeleid dat we ze op deze manier allemaal krijgen. We concluderen dat H een normaaldeler is precies dan als er slechts één Sylow p-groep in G is. Deze voorwaarde is vaak te verifiëren met behulp van de twee deelbaarheidseigenschappen die in Stelling 6.2.3 voor het aantal Sylow p-groepen zijn gegeven.

Het volgende lemma zal in het vervolg nuttig blijken te zijn. In feite hebben we dit allang in allerlei situaties afgeleid en gebruikt.

Lemma 7.1.7 *Is H een ondergroep van een groep G, en $a, b \in G$, dan geldt $aH = bH$ precies dan als $b^{-1}a \in H$.*

Bewijs. In het bewijs van Stelling 3.2.7 is al aangetoond dat twee zulke verzamelingen aH, bH óf gelijk, óf disjunct zijn. Omdat $e \in H$, geldt $a = ae \in aH$, dus $aH = bH$ is equivalent met $a \in bH$. Anders gezegd: $aH = bH$ precies dan als $a = bh$ voor een $h \in H$, dus precies dan als $b^{-1}a = h \in H$. □

Stelling 7.1.8 *Laat G een groep zijn en $H \subset G$ een ondergroep. De volgende drie uitspraken zijn equivalent:*

1. *H is een normaaldeler.*
2. *Voor elke $a \in G$ geldt $aH = Ha$.*
3. *Voor elke $a \in G$ en elke $h \in H$ geldt dat $aha^{-1} \in H$.*
4. *Voor alle $a, b, c, d \in G$ met $aH = cH$ en $bH = dH$ geldt dat ook $abH = cdH$.*

Bewijs. 1) impliceert 2): Is $a \in G$, dan geldt $aHa^{-1} = H$. Door deze gelijkheid aan de rechterkant met a te vermenigvuldigen volgt dat $aH = Ha$.
2) impliceert 3): Neem willekeurige $a \in G$ en $h \in H$. De aanname $aH = Ha$ levert dat $ah = h_1 a$ voor zekere $h_1 \in H$, en dus is $aha^{-1} = h_1 \in H$ hetgeen we wilden bewijzen.
3) impliceert 4): Gezien Lemma 7.1.7 moeten we laten zien dat als $c^{-1}a \in H$ en $d^{-1}b \in H$, dan ook $(cd)^{-1}(ab) = d^{-1}c^{-1}ab \in H$. Schrijf $c^{-1}a = h_1 \in H$. Aanname 3) levert in het bijzonder dat $h_2 := d^{-1}h_1 d \in H$. Dus volgt $d^{-1}c^{-1}ab = d^{-1}h_1 dd^{-1}b = h_2 d^{-1}b \in H$, wat we wilden bewijzen.
4) impliceert 1): Laat $h \in H$ en $a \in G$ willekeurig. Er geldt $hH = eH$, dus vanwege 4) ook $ha^{-1}H = ea^{-1}H = a^{-1}H$. Volgens Lemma 7.1.7 wil dit precies zeggen dat $aha^{-1} \in H$. Dus conjugatie met een willekeurige $a \in G$ beeldt H weer op H af, oftewel H is een normaaldeler.
Hiermee is aangetoond dat de vier uitspraken gelijkwaardig zijn. □

Het feit dat bijvoorbeeld de rotaties binnen D_n, en de even permutaties binnen S_n normaaldelers zijn, is een speciaal geval van het volgende resultaat.

Stelling 7.1.9 *Is G een groep en $H \subset G$ een ondergroep waarvoor geldt $[G : H] = 2$, dan is H een normaaldeler van G.*

Bewijs. De voorwaarde $[G : H] = 2$ wil precies zeggen dat er een $a \in G$ is zodat G de disjuncte vereniging is van H en Ha. Maar dan volgt $Ha = G \setminus H$. Omdat $a \notin H$, zijn ook H en aH disjuncte deelverzamelingen van G. Opnieuw gebruik makend van $[G : H] = 2$ volgt vanwege Opmerking 6.1.13 dat ook $aH = G \setminus H$, dus $aH = Ha$. Elke verzameling van de vorm bH binnen G is ofwel gelijk aan H, of aan aH. Dus volgt $bH = Hb$ voor elke $b \in G$, dus met behulp van Stelling 7.1.8 concluderen we dat H een normaaldeler van G is. □

7.2 Factorgroepen

Stelling 7.1.8 laat onder meer zien, dat als een ondergroep H van een groep G een normaaldeler is, dan is het voorschrift $(aH) \cdot (bH) = abH$ goed gedefinieerd. Dat wil zeggen: schrijven we $aH = cH$ of $bH = dH$ voor zekere andere elementen $c, d \in G$, dan levert dit dezelfde uitkomst $abH = cdH$. (En omgekeerd, is H *geen* normaaldeler, dan maakt het in het algemeen *wel* uit welk element van G we gebruiken om een verzameling aH mee aan te geven.)

Voorbeeld 7.2.1 Neem $G = S_3$ en $H = \{(1), (1\ 2)\} \subset S_3$. Zoals al wel vaker is opgemerkt, is H een ondergroep van G, maar H is geen normaaldeler in G. Bezie $a = (1\ 3)$ en $b = (1\ 2\ 3)$. Dan is $aH = \{(1\ 3)(1), (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$ en evenzo $bH = \{(1\ 2\ 3)(1), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}$. Dus $aH = bH$ (allicht: er geldt immers $b^{-1}a = (1\ 2) \in H$, dus ook vanwege Lemma 7.1.7 zien we dat $aH = bH$). Echter $a^2H = H$ en $b^2H = (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\} \neq a^2H$.

Definitie 7.2.2 Gegeven een groep G en een normaaldeler $H \subset G$. De *factorgroep* G modulo H die we noteren als G/H is de groep met als elementen de verzamelingen van de vorm aH, voor $a \in G$. Het eenheidselement is $H = eH$, en de groepsbewerking wordt gegeven door $(aH) \cdot (bH) = abH$.

Opmerking 7.2.3 Dat de bovenstaande manier om een groepsbewerking op G/H te geven werkt, volgt vanwege Stelling 7.1.8 precies uit het feit dat H een normaaldeler is. Omdat G een groep is, volgt eenvoudig dat dan ook G/H op deze manier een groep wordt. Zo is bijvoorbeeld de inverse $(aH)^{-1}$ van een element $aH \in G/H$ gelijk aan $a^{-1}H$. Immers, $(aH) \cdot a^{-1}H = eH$, en dat is per definitie het eenheidselement in G/H.

Opmerking 7.2.4 Per definitie van het begrip index is het aantal onderling verschillende verzamelingen van de vorm aH gelijk aan $[G : H]$. Is G een eindige groep, dan zegt Stelling 6.1.14 dat $[G : H] = \#G/\#H$. In het bijzonder is dus voor een normaaldeler H in een groep G het aantal elementen van de factorgroep G/H gelijk aan $[G : H]$.

Voorbeeld 7.2.5 $H = N\mathbb{Z}$ is een normaaldeler in $G = \mathbb{Z}$. De factorgroep is precies de groep $\mathbb{Z}/N\mathbb{Z}$. In het bijzonder zien we aan dit voorbeeld dat een factorgroep van een oneindige groep best een eindige groep kan zijn.

Voorbeeld 7.2.6 Laat $n \geq 2$ en neem $H = A_n$ als normaaldeler in $G = S_n$. Omdat A_n index 2 in S_n heeft, bestaat S_n/A_n uit precies twee elementen. In het bijzonder geldt dus dat $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, want dat is op isomorfie na

de enige groep bestaande uit precies twee elementen. We zien dus dat een factorgroep van een niet-abelse groep best commutatief kan zijn.

De twee elementen van S_n/A_n zijn per definitie twee deelverzamelingen van S_n. De ene bestaat uit alle *even* permutaties (A_n), en de andere uit alle *oneven* permutaties (dus $(1\ 2)A_n$). De groepsbewerking in S_n/A_n gaat volgens de regels 'even maal even is even' en 'oneven maal even is oneven' en 'even maal oneven is oneven' en 'oneven maal oneven is even'.

Stelling 7.2.7 *Is H een normaaldeler in een groep G, dan geldt dat de factorgroep G/H commutatief is dan en slechts dan als voor elke $a, b \in G$ het element $a^{-1}b^{-1}ab$ in H zit.*

Bewijs. Er geldt dat G/H abels is precies dan als $(aH)\cdot(bH) = (bH)\cdot(aH)$ voor alle $a, b \in G$. En dit is het geval dan en slechts dan als $abH = baH$ voor elke $a, b \in G$. Vanwege Lemma 7.1.7 is deze laatste eis gelijkwaardig met $a^{-1}b^{-1}ab = (ba)^{-1}ab \in H$, voor alle $a, b \in G$. Dit bewijst de stelling. □

Voorbeeld 7.2.8 Laat $n \geq 3$. Zoals we al gezien hebben, is S_n/A_n een commutatieve groep. Vanwege Stelling 7.2.7 is dus voor elk paar permutaties σ, τ het product $\sigma^{-1}\tau^{-1}\sigma\tau$ even. Dit volgt natuurlijk ook uit het feit dat het teken ϵ een homomorfisme van S_n naar een commutatieve groep (± 1) is. Omdat $(a\ b)^{-1}(a\ c)^{-1}(a\ b)(a\ c) = (a\ b\ c)$ voor onderling verschillende a, b, c en omdat elk element van A_n als product van 3-cykels te schrijven is, volgt dat als $H \subset S_n$ een normaaldeler is met de eigenschap dat S_n/H abels, dan $A_n \subset H$, en dus $H = A_n$ of $H = S_n$.

Stelling 7.2.9 *Laat H een normaaldeler in een groep G zijn. Het voorschrift*

$$\pi \ : \ G \longrightarrow G/H \quad : \quad g \mapsto gH$$

levert een surjectief homomorfisme van G naar G/H met $Ker(\pi) = H$.

Bewijs. Er geldt voor $a, b \in G$ dat $\pi(ab) = abH = (aH)\cdot(bH) = \pi(a)\pi(b)$. Dus inderdaad is π een homomorfisme. Een willekeurig element van G/H is te schrijven als aH, voor een $a \in G$. Dan is $\pi(a) = aH$, met andere woorden, π is surjectief. Tenslotte geldt voor $a \in G$ dat $a \in \mathrm{Ker}(\pi)$ precies dan als $aH = eH$, oftewel volgens Lemma 7.1.7 precies dan als $a \in H$. Dus $\mathrm{Ker}(\pi) = H$, en daarmee is de stelling bewezen. □

Opmerking 7.2.10 Het homomorfisme π genoemd in Stelling 7.2.9 wordt vaak het *kanonieke* homomorfisme naar een factorgroep genoemd.

Stelling 7.2.11 *Een ondergroep H van een groep G is een normaaldeler precies dan als H de kern is van een homomorfisme van G naar een andere groep.*

Bewijs. Is H de kern van een homomorfisme, dan is het een aardige oefening in de hier gegeven definities om na te gaan dat H inderdaad een normaaldeler is.

Omgekeerd, is H een normaaldeler, dan is H vanwege Stelling 7.2.9 de kern van het kanonieke homomorfisme van G naar G/H. □

7.3 Normaaldelers in de alternerende groep

Definitie 7.3.1 Een groep G heet *simpel* (of ook wel *enkelvoudig*) als $\{e\}$ en G de enige normaaldelers in G zijn.

Opmerking 7.3.2 Is G een simpele groep, G' een willekeurige groep en $f : G \to G'$ een homomorfisme, dan is f óf injectief, óf er geldt dat f ieder element van G op het eenheidselement van G' afbeeldt. Immers, de kern van f is een normaaldeler in G, dus $\mathrm{Ker}(f) = \{e\}$ (en dan is f injectief) of $\mathrm{Ker}(f) = G$ (en dan wordt alles op het eenheidselement afgebeeld). Deze eigenschap van simpele groepen geeft al aan, dat 'simpel zijn' een sterke eigenschap is.

Voorbeeld 7.3.3 We gaan na welke niet-triviale eindige, abelse groepen G simpel zijn. Is p een priemgetal dat het aantal elementen van zo'n groep G deelt, dan bestaat er vanwege Stelling 6.2.8 een $a \in G$ met $\mathrm{ord}(a) = p$. De ondergroep $\langle a \rangle$ is dan een normaaldeler $\neq \{e\}$ (want elke ondergroep van een abelse groep is een normaaldeler). Dus als G simpel is, dan $G = \langle a \rangle \cong \mathbb{Z}/p\mathbb{Z}$. Inderdaad is $\mathbb{Z}/p\mathbb{Z}$ simpel, want een ondergroep heeft als aantal elementen een deler van p en p is een priemgetal. We concluderen dat op isomorfie na de groepen $\mathbb{Z}/p\mathbb{Z}$ de enige niet-triviale simpele eindige abelse groepen zijn.

Opmerking 7.3.4 Eén van de belangrijkste resultaten uit de moderne theorie van eindige groepen is, dat de volledige lijst van alle simpele eindige groepen bekend is. Deze lijst bestaat uit een paar 'families van simpele groepen' (zoals de $\mathbb{Z}/p\mathbb{Z}$'s voor p een priemgetal), en 26 losse exemplaren die 'sporadische groepen' worden genoemd. De lijst is te vinden in J. Conway etc., Atlas of finite simple groups. Oxford: Clarendon Press, 1985. Aan het bewijs dat de lijst volledig is hebben vele wiskundigen bijgedragen; met name dient daarbij de Amerikaan Daniel Gorenstein (1923–1992) genoemd te worden.

De grootste sporadische simpele eindige groep heeft de fraaie naam 'Het Monster' gekregen. Deze groep heeft

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

elementen.

Andere eindige simpele groepen zijn bijvoorbeeld de groepen $\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$, voor $n \geq 2$ en p een priemgetal en $(n,p) \neq (2,2)$ en $(n,p) \neq (2,3)$. Dit zijn factorgroepen G/H, waarin G de groep van $n \times n$ matrices met coëfficiënten in $\mathbb{Z}/p\mathbb{Z}$ en determinant $\overline{1}$ is, en H de ondergroep bestaande uit alle matrices $\overline{a}I$, met $\overline{a}^n = \overline{1}$. Het bewijs dat deze groepen inderdaad simpel zijn valt buiten het bestek van dit college. Wat we echter *wel* zullen aantonen is dat de groepen A_n, voor $n \geq 5$ simpel zijn.

Voorbeeld 7.3.5 We tonen aan dat A_5 een simpele groep is. Laat $H \subset A_5$ een normaaldeler zijn. Is $\sigma \in H$, dan is voor elke $\tau \in A_5$ ook $\tau\sigma\tau^{-1} \in \tau H\tau^{-1} = H$. Dus H bevat de gehele conjugatieklasse C_σ van σ in A_5. Er volgt dat H een vereniging is van zulke conjugatieklassen. Deze klassen zijn onderling disjunct en hebben respectievelijk $1, 12, 12, 15$ en 20 elementen (vergelijk Voorbeeld 6.1.9). Dus

$$\#H = 1 + 12a + 15b + 20c$$

met $a = 0, 1$ of 2 en $b, c \in \{0, 1\}$. Verder $\#H | \#A_5 = 60$, en het is niet moeilijk om na te gaan dat hieruit volgt $\#H = 1$ of $\#H = 60$. Dus A_5 heeft geen normaaldelers behalve $\{(1)\}$ en A_5 zelf.

Stelling 7.3.6 *Voor $n \geq 5$ is A_n een simpele groep.*

Bewijs. Het idee van onderstaand bewijs is dat we gaan aantonen dat voor $n \geq 5$ een normaaldeler $H \neq \{(1)\}$ in A_n altijd een 3-cykel bevat. Er volgt dan dat H de conjugatieklasse in A_n van die 3-cykel bevat, en die bestaat vanwege Stelling 6.1.11 uit *alle* 3-cykels. Vanwege Stelling 4.4.4 volgt dan tenslotte $H = A_n$.

Laat $n \geq 5$ en stel $H \neq \{(1)\}$ is een normaaldeler. We willen bewijzen dat $H = A_n$, en bovenstaand argument laat zien dat we daarvoor alleen maar hoeven aan te tonen dat H een 3-cykel bevat. Stel $\sigma \neq (1)$ is een element van H. Schrijf $\sigma = \sigma_1\sigma_2 \ldots \sigma_r$, met de σ_i disjuncte ℓ_i-cykels, en $\ell_1 \geq \ell_2 \geq \ldots \geq \ell_r$.

Als $\ell_1 \geq 4$, schrijf dan $\sigma_1 = (a_1\ a_2\ \ldots\ a_{\ell_1})$ en neem $\tau = (a_1\ a_2\ a_3) \in A_n$. Omdat H een normaaldeler is, geldt dat $\sigma' = \tau\sigma\tau^{-1} \in H$. We gaan na hoe σ'

eruit ziet. De getallen a_1, a_2, a_3 komen in σ_1 voor en niet in $\sigma_2, \ldots, \sigma_r$. Bijgevolg is $\tau\sigma_i\tau^{-1} = \sigma_i$ voor $i \geq 2$. Verder is $\tau\sigma_1\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \ldots\ \tau(a_{\ell_1})) = (a_2\ a_3\ a_1\ a_4\ \ldots\ a_{\ell_1})$. Dus

$$\sigma' = \tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1})\ldots(\tau\sigma_r\tau^{-1}) = (a_2\ a_3\ a_1\ a_4\ \ldots\ a_{\ell_1})\sigma_2\ldots\sigma_r.$$

Er volgt dat ook $\sigma^{-1}\sigma' = (a_{\ell_1}\ \ldots\ a_1)(a_2\ a_3\ a_1\ a_4\ \ldots\ a_{\ell_1}) = (a_1\ a_3\ a_{\ell_1}) \in H$. Dus in dit geval bevat H een 3-cykel, en zijn we klaar.

Als $\ell_1 = \ell_2 = 3$, schrijf dan $\sigma_1 = (a_1\ a_2\ a_3)$ en $\sigma_2 = (b_1\ b_2\ b_3)$. Conjugeren met $\tau = (a_1\ a_2\ b_1) \in A_n$ levert dan $\sigma' = (a_2\ b_1\ a_3)(a_1\ b_2\ b_3)\sigma_3\ldots\sigma_r \in H$. Daarmee is ook $\sigma^{-1}\sigma' = (a_1\ b_1\ a_2\ b_3\ a_3) \in H$. Het argument dat we voor $\ell_1 \geq 4$ gebruikten kan hierop worden toegepast, en de conclusie is dat ook in dit geval er een 3-cykel in H zit.

Als $\ell_1 = 3$ en $\ell_i < 3$ voor $i \neq 1$, dan is σ^2 een 3-cykel in H, dus ook dit geval is daarmee klaar.

Het resterende geval is dat σ een product is van disjuncte 2-cykels. Omdat $\sigma \in H \subset A_n$, bestaat σ dan uit een even aantal 2-cykels. Schrijf $\sigma = (a\ b)(c\ d)\sigma_3\ldots\sigma_r$. Conjugeren met $(a\ b\ c)$ levert dat ook $\sigma' = (b\ c)(a\ d)\sigma_3\ldots\sigma_r \in H$, en dus ook $\sigma\sigma' = (a\ c)(b\ d) \in H$. Daarmee bevat H dan ook de hele conjugatieklasse in A_n van dit product van twee disjuncte 2-cykels. Stelling 6.1.11 zegt dat dus *ieder* product van twee disjuncte 2-cykels in H zit, dus in het bijzonder ook $(1\ 2)(4\ 5)\cdot(4\ 5)(2\ 3) = (1\ 2\ 3) \in H$. Hiermee is ook dit laatste geval afgehandeld.

We concluderen dat $H = A_n$, hetgeen we wilden bewijzen. □

7.4 Opgaven

1. Gegeven twee groepen G_1 en G_2 en een homomorfisme $\varphi : G_1 \to G_2$. Laat zien dat $\mathrm{Ker}(\varphi)$ een normaaldeler in G_1 is.

2. Toon aan dat als G een groep is, $H \subset G$ een ondergroep en $N \subset G$ een normaaldeler, dan is $N \cap H$ een normaaldeler van H.

3. Gegeven de verzameling $H \subset A_4$ bestaande uit het eenheidselement en alle producten van twee disjuncte 2-cykels. Laat zien dat H een normaaldeler is in A_4. Geef expliciet alle elementen van A_4/H, en maak een vermenigvuldigtabel voor de groep A_4/H.

4. Geef een normaaldeler in $\mathbb{Z}/2\mathbb{Z} \times A_n$ bestaande uit precies twee elementen. Bewijs dat $\mathbb{Z}/2\mathbb{Z} \times A_n \ncong S_n$ wanneer $n \neq 2$.

5. Bewijs dat er op isomorfie na, slechts één groep met precies 1001 elementen bestaat, als volgt:

   (a) Zo'n groep G bevat normaaldelers N_7, N_{11} en N_{13} met resp. $7, 11$ en 13 elementen;

   (b) Er bestaat een injectief homomorfisme $G \to G/N_7 \times G/N_{11}$;

   (c) Met behulp van Stelling 6.2.6 volgt, dat G commutatief is.

   (d) G bevat een element met orde 1001, en dus $G \cong \mathbb{Z}/1001\mathbb{Z}$.

6. Bepaal alle ondergroepen van D_4 en beschrijf voor de normaaldelers daaronder de bijbehorende factorgroepen.

7. Gegeven twee groepen G_1, G_2 met eenheidselementen respectievelijk e_1, e_2. Laat zien dat $H = G_1 \times \{e_2\}$ een normaaldeler is van $G_1 \times G_2$, en dat $(G_1 \times G_2)/H \cong G_2$.

8. Beschouw $G = \{\left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) \mid b \neq 0\} \subset \mathrm{GL}_2(\mathbb{R})$.

   (a) Laat zien dat G een ondergroep is van $\mathrm{GL}_2(\mathbb{R})$, maar geen normaaldeler.

   (b) Laat zien dat $H_1 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) \mid b \neq 0\}$ een ondergroep is van G, maar geen normaaldeler.

   (c) Laat zien dat $H_2 = \{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{R}\}$ wel een normaaldeler in G is.

   (d) Laat zien dat $b \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & b \end{smallmatrix}\right) H_2$ een isomorfisme tussen de vermenigvuldiggroep
   $\mathbb{R} \setminus \{0\}$ en G/H_2 oplevert.

9. Laat G een groep zijn en N een normaaldeler in G. Zij verder H een ondergroep van G waarvoor geldt $N \subset H$.

   (a) Toon aan dat N ook een normaaldeler van H is.

   (b) Toon aan dat H/N een ondergroep is van G/N.

   (c) Laat zien dat als $X \subset G/N$ een ondergroep is, dan is $Y = \{a \in G \mid aN \in X\}$ een ondergroep van G, en $N \subset Y$, en $X = Y/N$.

   (d) Bewijs dat als $Y \subset G$ een ondergroep is die N bevat, dan geldt dat Y/N een normaaldeler in G/N is dan en slechts dan als Y een normaaldeler is in G.

10. Neem $k \geq 2$ vast. In een groep G nemen we de deelverzameling H bestaande uit alle eindige producten $a_1^k a_2^k \dots a_n^k$, voor $a_1, \dots, a_n \in G$. Laat zien dat H een normaaldeler in G is, en dat elk element van G/H een orde heeft die een deler is van k.

11. In een *abelse* groep G nemen we $H = \{a \in G \mid \text{ord}(a) < \infty\}$. Laat zien dat H een normaaldeler is in G. Bewijs dat het eenheidselement eH het enige element van G/H is dat een eindige orde heeft.

12. Laat $n \geq 5$, en neem een *oneven* k met $3 \leq k \leq n$.

    (a) Gegeven een groep G en een niet lege verzameling $X \subset G$ met de eigenschap dat voor elke $x \in X$ en elke $a \in G$ ook $axa^{-1} \in X$. Bewijs dat
    $$H = \{x_1^{\pm 1} \cdot \ldots \cdot x_r^{\pm 1} \mid x_i \in X\}$$
    een normaaldeler in G is.

    (b) Laat zien dat A_n een element van orde k bevat.

    (c) Laat zien dat A_5 geen element van orde 4 of 6 bevat.

    (d) Bewijs m.b.v. a) dat elk element van A_n te schrijven is als product van elementen van orde k.

8 Homomorfie– en isomorfiestellingen

In dit hoofdstuk komen een aantal rekenregels voor het omgaan met factorgroepen G/H aan de orde. Een centraal thema daarbij is, hoe een homomorfisme van G/H naar een andere groep gegeven dient te worden. Het probleem daarbij is, dat een element gH van G/H op verschillende manieren gegeven kan worden: er kan gelden $gH = g'H$ terwijl toch $g \neq g'$. Een belangrijk voorbeeld van dit fenomeen kwam al in Lemma 2.3.1 aan de orde. Wie dat lemma goed begrijpt zal ook weinig moeite hebben met de hieronder in Criterium 8.1.2 gegeven algemenere situatie.

8.1 homomorfismen vanuit een factorgroep

We geven om te beginnen een eigenschap die elk homomorfisme vanuit een factorgroep heeft. Daarna zullen we die eigenschap gebruiken voor het maken van zulke homomorfismen.

Stelling 8.1.1 *Laat G en G' groepen zijn, H een normaaldeler in G, en*

$$\varphi \ : \ G/H \longrightarrow G'$$

een homomorfisme. Dan is, met $\pi \ : \ G \to G/H$ het kanonieke homomorfisme gegeven door $\pi(g) = gH$, de samenstelling $\psi = \varphi \circ \pi$ een homomorfisme van G naar G'.

Dit homomorfisme ψ heeft de eigenschap dat $H \subset Ker(\psi)$.

Bewijs. Ga zelf na dat algemeen geldt dat een samenstelling van homomorfismen weer een homomorfisme is. In het bijzonder is dus ψ hier een homomorfisme van G naar G'.

Ook de tweede uitspraak in de stelling berust op een algemeenheid: omdat $\psi = \varphi \circ \pi$, volgt $\mathrm{Ker}(\pi) \subset \mathrm{Ker}(\psi)$, en we weten dat $\mathrm{Ker}(\pi) = H$. □

Criterium 8.1.2 *Laat H een normaaldeler in een groep G zijn, en G' een willekeurige groep. Het construeren van een homomorfisme $\varphi \ : \ G/H \to G'$ gaat volgens het volgende recept:*

1. *Geef eerst een homomorfisme $\psi \ : \ G \to G'$ met de eigenschap dat $H \subset Ker(\psi)$.*

2. *Voor ψ als in (1) geldt dan dat $\psi(g_1) = \psi(g_2)$ voor alle $g_1, g_2 \in G$ met de eigenschap $g_1H = g_2H$. Met andere woorden: het voorschrift $\varphi(gH) = \psi(g)$ levert een goed gedefiniëerde afbeelding van G/H naar G'.*

3. *$\varphi : G/H \to G'$ als in (2) is een homomorfisme, en er geldt $\psi = \varphi \circ \pi$ met π het kanonieke homomorfisme van G naar G/H.*

Bewijs. We laten eerst zien dat een ψ als in (1) voldoet aan $\psi(g_1) = \psi(g_2)$ indien $g_1H = g_2H$. Dit volgt uit het feit dat $g_1H = g_2H$ wegens Lemma 7.1.7 impliceert dat $g_2^{-1}g_1 \in H$. Omdat $H \subset \mathrm{Ker}(\psi)$ concluderen we dan dat $g_2^{-1}g_1 \in \mathrm{Ker}(\psi)$, met andere woorden $\psi(g_2^{-1}g_1) = e'$, het eenheidselement van G'. Hieruit volgt $\psi(g_2)^{-1}\psi(g_1) = e'$, en dus $\psi(g_1) = \psi(g_2)$ wat we wilden aantonen.

Vervolgens moeten we laten zien dat de gegeven φ een homomorfisme is. Laat g_1H, g_2H elementen van G/H zijn. Dan geldt $\varphi(g_1H \cdot g_2H) = \varphi(g_1g_2H)$ (dit vanwege de definitie van de groepsbewerking in G/H), en verder $\varphi(g_1g_2H) = \psi(g_1g_2)$ (dat is de definitie van φ). Omdat ψ een homomorfisme is, geldt verder $\psi(g_1g_2) = \psi(g_1)\psi(g_2)$, en dat is wegens de definitie van φ gelijk aan $\varphi(g_1H)\varphi(g_2H)$. Dus we zien dat $\varphi(g_1H \cdot g_2H) = \varphi(g_1H)\varphi(g_2H)$, wat we wilden bewijzen.

Tenslotte geldt voor willekeurige $g \in G$ dat $(\varphi \circ \pi)(g) = \varphi(gH) = \psi(g)$, dus inderdaad $\psi = \varphi \circ \pi$. □

Voorbeeld 8.1.3 We gaan alle homomorfismen van $\mathbb{Z}/12\mathbb{Z}$ naar $\mathbb{Z}/4\mathbb{Z}$ bepalen. Uit Stelling 8.1.1 en Criterium 8.1.2 blijkt, dat dit neerkomt op het vinden van alle homomorfismen van $\mathbb{Z}$ naar $\mathbb{Z}/4\mathbb{Z}$ die de eigenschap hebben dat $12\mathbb{Z}$ in de kern zit. Die eigenschap legt echter geen enkele beperking op. Immers, is $f : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ een willekeurig homomorfisme, en $n \in 12\mathbb{Z}$, dan geldt $n = 12m$ met $m \in \mathbb{Z}$, en dus in het bijzonder $n = 3m + 3m + 3m + 3m$, hetgeen impliceert dat $f(n) = f(3m) + f(3m) + f(3m) + f(3m) = \overline{0}$.

Dus wat we zoeken, zijn gewoon alle homomorfismen van $\mathbb{Z}$ naar $\mathbb{Z}/4\mathbb{Z}$. Zo'n homomorfisme stuurt het eenheidselement naar het eenheidselement, dwz. 0 naar $\overline{0}$. Stel $\overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ is het beeld van 1. Dan ligt hiermee de afbeelding vast, want $1 + \ldots + 1$ moet op $\overline{a} + \ldots + \overline{a}$ worden afgebeeld, en de tegengestelde van $1 + \ldots + 1$ naar de tegengestelde van $\overline{a} + \ldots + \overline{a}$. Ga zelf na dat op deze wijze inderdaad een homomorfisme verkregen wordt.

In totaal vinden we dus 4 onderling verschillende homomorfismen van $\mathbb{Z}/12\mathbb{Z}$ naar $\mathbb{Z}/4\mathbb{Z}$. Elk ervan wordt volledig vastgelegd door het beeld van 1 mod 12.

Voorbeeld 8.1.4 De groep D_4 bestaande uit alle symmetrieën van het vierkant bestaat zoals bekend uit 8 elementen. We leggen dit vierkant in het vlak zo, dat het middelpunt de oorsprong is. Dan worden de 8 symmetrieën gegeven door lineaire afbeeldingen van $\mathbb{R}^2$ naar $\mathbb{R}^2$. De symmetrie 'puntspiegelen in de oorsprong' vormt samen met de identiteit een ondergroep

$H = \{\pm 1\} \subset D_4$. Het is eenvoudig na te gaan dat dit een normaaldeler van D_4 is. We gaan een isomorfisme $D_4/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ geven.

Volgens Criterium 8.1.2 moeten we dan beginnen met het maken van een homomorfisme van D_4 naar $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De determinant levert een homomorfisme van D_4 naar $\pm 1 \cong \mathbb{Z}/2\mathbb{Z}$. Verder heeft een vierkant 2 diagonalen, en elk element van D_4 permuteert deze twee. Dat geeft aanleiding tot een tweede homomorfisme $f : D_4 \to S_2 \cong \mathbb{Z}/2\mathbb{Z}$. Het paar $(\det, f)$ is het gevraagde homomorfisme:

$$\psi : D_4 \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : \sigma \mapsto (\det(\sigma), f(\sigma)) \in \pm 1 \times S_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Er geldt dat ψ surjectief is (geef zelf expliciet elementen van D_4 die naar elk van de elementen van $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ worden afgebeeld). De kern van ψ bestaat per definitie uit alle symmetrieën die de beide diagonalen elk op zichzelf afbeelden, en die bovendien determinant 1 hebben, dus die een draaiing zijn. Hieruit volgt dat de kern precies onze ondergroep H is. Er is hier dus voldaan aan de voorwaarde $H \subset \mathrm{Ker}(\psi)$ van Criterium 8.1.2. De conclusie hieruit is, dat er een homomorfisme $\varphi : D_4/H \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is, gegeven door $\varphi(\sigma H) = \psi(\sigma)$. Omdat $\psi(\sigma)$ alle elementen van $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ doorloopt, geldt dat φ surjectief is. Het aantal elementen van D_4/H is gelijk aan $[D_4 : H] = \#D_4/\#H = 8/2 = 4$ en dat is gelijk aan het aantal elementen van $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dit samen met de surjectiviteit van φ impliceert dat φ een bijectie en dus een isomorfisme is. Dus geldt $D_4/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, zoals we beweerden.

8.2 isomorfismen vanuit een factorgroep

De meest gebruikte rekenregel voor het omgaan met factorgroepen is de volgende.

Stelling 8.2.1 *Is $\psi : G \to G'$ een homomorfisme van groepen, en $H = Ker(\psi)$, dan is H een normaaldeler in G en er geldt*

$$G/H \cong \psi(G) \subset G'.$$

In het bijzonder volgt dat indien ψ surjectief is dan $G/H \cong G'$.

Bewijs. Het feit dat H een normaaldeler is, staat al vermeld in Stelling 7.2.11. Verder wordt vanwege Criterium 8.1.2 door $\varphi(gH) = \psi(g)$ in ons geval een goed gedefiniëerd homomorfisme φ van G/H naar G' gegeven.

We bepalen de kern van φ. Er geldt $gH \in \mathrm{Ker}(\varphi)$ precies dan als $\varphi(gH)$ het eenheidselement van G' is. Omdat $\varphi(gH) = \psi(g)$, is dit het geval dan en

slechts dan als $g \in \mathrm{Ker}(\psi) = H$. Echter $g \in H$ is equivalent met $gH = eH$, oftewel gH is het eenheidselement van G/H. De conclusie is dat $\mathrm{Ker}(\varphi)$ alleen uit het eenheidselement van G/H bestaat. Stelling 3.3.6 impliceert dus dat φ injectief is.

De injectiviteit van φ levert dat G/H isomorf is met het beeld van φ, en dat is per definitie gelijk aan het beeld van ψ. Dus $G/\mathrm{Ker}(\psi) \cong \psi(G)$, zoals verlangd. Is ψ surjectief, dan geldt $\psi(G) = G'$ en dus $G/\mathrm{Ker}(\psi) \cong G'$. □

Voorbeeld 8.2.2 De determinant is een surjectief homomorfisme van $\mathrm{GL}_n(\mathbb{R})$ naar de vermenigvuldiggroep $\mathbb{R} \setminus \{0\}$. De kern hiervan is precies $\mathrm{SL}_n(\mathbb{R})$, en dus impliceert Stelling 8.2.1 dat

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R} \setminus \{0\}.$$

Voorbeeld 8.2.3 De complexe getallen $a+bi$ met de eigenschap $a^2+b^2 = 1$ vormen een ondergroep $\mathbf{T}$ van de vermenigvuldiggroep $\mathbb{C} \setminus \{0\}$. Deze ondergroep is isomorf met de factorgroep $\mathbb{R}/\mathbb{Z}$. Immers, $x \mapsto e^{2\pi ix}$ definiëert een surjectief homomorfisme van $\mathbb{R}$ naar $\mathbf{T}$ waarvan de kern precies $\mathbb{Z}$ is.

De nu volgende twee isomorfiestellingen voor factorgroepen zijn in feite gevolgen van Stelling 8.2.1.

Stelling 8.2.4 *Gegeven is een groep G, een willekeurige ondergroep $H \subset G$, en een normaaldeler $N \subset G$. Dan geldt*

1. *$HN = \{hn \mid h \in H \ \text{ en } \ n \in N\}$ is een ondergroep van G.*
2. *N is een normaaldeler van HN.*
3. *$H \cap N$ is een normaaldeler van H.*
4. *$H/(H \cap N) \cong HN/N$.*

Bewijs. 1: Volgens Stelling 3.2.3 moeten we een drietal eisen (H1, H2, H3) nagaan. H1: er geldt $e = e \cdot e$ en $e \in H, e \in N$, dus $e \in HN$. H3: voor willekeurige $h \in H$ en $n \in N$ weten we dat $hn^{-1}h^{-1} \in N$ omdat N een normaaldeler in G is. Dus is $(hn)^{-1} = n^{-1}h^{-1} = h^{-1} \cdot (hn^{-1}h^{-1}) \in HN$. Tenslotte H2: als $h_1, h_2 \in H$ en $n_1, n_2 \in N$, dan is $h_2^{-1}n_1h_2 \in N$ omdat N een normaaldeler is. Bijgevolg geldt $(h_1n_1) \cdot (h_2n_2) = h_1h_2(h_2^{-1}n_1h_2)n_2 \in HN$. Dus HN is inderdaad een ondergroep.
2: Omdat $e \in H$, is $N = eN \subset HN$. Dus N is een deelverzameling van HN, en omdat N een groep is is het dan ook een ondergroep van HN. Er geldt $gNg^{-1} = N$ voor alle $g \in G$, dus zeker voor de $g \in G$ die in HN zitten. Dus

N is een normaaldeler van HN.
3 en 4: definiëer $\psi : H \to G/N$ door $\psi(h) = hN \in G/N$. Dit is de beperking tot H van het kanonieke homomorfisme van G naar G/N, dus ψ is zelf ook een homomorfisme. Er geldt dat $h \in \mathrm{Ker}(\psi)$ precies dan als $hN = N$, ofwel als $h \in N$. Dus $\mathrm{Ker}(\psi) = H \cap N$, en dit impliceert vanwege Stelling 7.2.11 dat $H \cap N$ een normaaldeler in H is. Uit Stelling 8.2.1 weten we dan dat $H/(H \cap N)$ isomorf is met het beeld van ψ. We zijn dus klaar wanneer is aangetoond dat $\psi(H) = HN/N$. Dit is niet moeilijk: een element van $\psi(H)$ is van de vorm $hN \in G/N$, en omdat hierin $h \in H \subset HN$, zit dat element dan in HN/N. Omgekeerd, een element in HN/N zier eruit als hnN met $h \in H$ en $n \in N$. Dan is $nN = N$ en dus $hnN = hN$, en dat is het beeld van $h \in H$ onder ψ. Hiermee is het bewijs voltooid. □

Voorbeeld 8.2.5 Neem $G = \mathbb{Z}$, $n, h \in \mathbb{Z}$ en $H = h\mathbb{Z}$ en $N = n\mathbb{Z}$. Merk op dat de groepswet op $\mathbb{Z}$ 'optellen' is; dus Stelling 8.2.4 zegt in dit geval dat $h\mathbb{Z}/(h\mathbb{Z} \cap n\mathbb{Z}) \cong (h\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z}$. Dit kan nog wat verder worden uitgewerkt. Merk op dat $h\mathbb{Z} \cap n\mathbb{Z}$ bestaat uit precies alle getallen die zowel een veelvoud van h als een veelvoud van n zijn. Uit Gevolg 1.2.9 (5) weten we dat dit precies de veelvouden van $\mathrm{kgv}(h, n)$ zijn. Dus $h\mathbb{Z} \cap n\mathbb{Z} = \mathrm{kgv}(h, n)\mathbb{Z}$. Evenzo volgt met behulp van Stelling 1.1.11 dat $h\mathbb{Z} + n\mathbb{Z} = \mathrm{ggd}(h, n)\mathbb{Z}$. We concluderen

$$h\mathbb{Z}/\mathrm{kgv}(h, n)\mathbb{Z} \cong \mathrm{ggd}(h, n)\mathbb{Z}/n\mathbb{Z}.$$

In het speciale geval dat $\mathrm{ggd}(h, n) = 1$ staat hier $h\mathbb{Z}/hn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$. Overigens geldt deze isomorfie ook wanneer $\mathrm{ggd}(h, n) \neq 1$, zoals met behulp van bijvoorbeeld Stelling 8.2.1 te bewijzen is.

Voorbeeld 8.2.6 Kies $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ als ondergroep van $G = S_4$ en $H =$ alle permutaties in S_4 die het getal 4 vasthouden (dus $H = S_3 \subset S_4$). Dan is N een normaaldeler in G. Verder geldt $HN = S_4$, want zowel H als N zijn ondergroepen van HN, dus $\#HN$ is zowel door $\#H = 4$ als door $\#N = 6$ deelbaar. Dus $12|\#HN$. Hieruit volgt dat $[S_4 : HN] = 1$ of $= 2$. In het bijzonder is dan HN een normaaldeler in S_4. Daar S_4/HN hooguit twee elementen heeft, is deze factorgroep abels, en dit impliceert dat $A_4 \subset HN$. Echter HN bevat ook oneven permutaties, dus volgt $HN = S_4$. (Dit kan ook wel op allerlei andere manieren worden ingezien, maar bovenstaand argument illustreert een aantal technieken die we inmiddels tot onze beschikking hebben.) Omdat $H \cap N = \{(1)\}$, volgt uit Stelling 8.2.4 dat

$$S_4/H = HN/H \cong H/(H \cap N) = S_3/\{(1)\} = S_3.$$

Een gedeelte van de volgende stelling zijn we al in Opgave 9 van Hoofdstuk 7 tegengekomen.

Stelling 8.2.7 *Gegeven is een groep G en een normaaldeler N in G.*

1. *Elke normaaldeler in G/N is van de vorm H/N, waarbij H een normaaldeler in G is die N omvat.*

2. *Is $N \subset H$ voor een normaaldeler H in G, dan geldt*

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

Bewijs. Voor (1) verwijzen we naar Opgave 9 in Hoofdstuk 7; dit is een nuttige oefening.
(2): Beschouw het kanonieke homomorfisme $\pi : G \to G/H$. Er geldt $N \subset H$ en vanwege Stelling 7.2.9 is $H = \mathrm{Ker}(\pi)$, dus $N \subset \mathrm{Ker}(\pi)$. Vanwege Criterium 8.1.2 wordt dan door $\psi(gN) = \pi(g) = gH$ een homomorfisme $\psi : G/N \to G/H$ gedefinieerd. Dit homomorfisme ψ is surjectief, want π is surjectief. Verder geldt $gN \in \mathrm{Ker}(\psi)$ precies dan als $\psi(gN) = gH = eH$, dus $\mathrm{Ker}(\psi)$ bestaat uit alle klassen gN met $g \in H$. We concluderen dat $\mathrm{Ker}(\psi) = H/N$. Uit Stelling 8.2.1 volgt dan

$$(G/N)/(H/N) = (G/N)/\mathrm{Ker}(\psi) \cong \psi(G/N) = G/H,$$

hetgeen we wilden bewijzen. □

Voorbeeld 8.2.8 De restklassen $2a \bmod 6$ voor $a \in \mathbb{Z}$ vormen samen een normaaldeler in $\mathbb{Z}/6\mathbb{Z}$. Dit is precies $2\mathbb{Z}/6\mathbb{Z}$, en Stelling 8.2.7 met in dit geval $G = \mathbb{Z}$ en $N = 6\mathbb{Z}$ en $H = 2\mathbb{Z}$ zegt dat $(\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

8.3 Opgaven

1. Bepaal alle homomorfismen van $\mathbb{Z}/4\mathbb{Z}$ naar $\mathbb{Z}/6\mathbb{Z}$.

2. Bewijs dat $\mathbb{C}/\mathbb{Z}$ isomorf is met de vermenigvuldiggroep $\mathbb{C} \setminus \{0\}$.

3. Toon aan dat voor $n, h \in \mathbb{Z}$ met $h \neq 0$ geldt dat $h\mathbb{Z}/hn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$.

4. Met $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset S_4$, toon aan dat
$$(S_4/N)/(A_4/N) \cong \mathbb{Z}/2\mathbb{Z}.$$

5. Bewijs dat als k een deler is van N, dan is
$$(\mathbb{Z}/N\mathbb{Z})/(k\mathbb{Z}/N\mathbb{Z}) \cong \mathbb{Z}/k\mathbb{Z}.$$
Is het hier wel nodig te eisen dat $k|N$?

6. Laat $n, m \in \mathbb{Z}$ beide positief zijn. In de groep D_{nm} noteren we de draaiing over $2\pi/nm$ tegen de richting van de klok als ρ. Verder nemen we $\sigma =$ 'spiegelen in de x-as' als element van D_{nm}; zoals bekend is $\sigma\rho\sigma = \rho^{-1}$. We beschouwen $H = \{id, \sigma\}$ en $N = \{id, \rho^m, \rho^{2m}, \ldots, \rho^{(n-1)m}\}$.
   (a) Laat zien dat H een ondergroep is van D_{nm} en dat N een normaaldeler is in D_{nm}.
   (b) Beargumenteer dat $HN \cong D_n$.
   (c) Bewijs dat $D_m \cong D_{nm}/N$.

7. Laat G een groep zijn en H_1, H_2 normaaldelers in G. Definiëer $\psi : G \to G/H_1 \times G/H_2$ door $\psi(g) = (gH_1, gH_2)$.
   (a) Toon aan dat ψ een homomorfisme is en dat $H_1 \cap H_2$ een normaaldeler in G is.
   (b) Bewijs dat $G/(H_1 \cap H_2)$ isomorf is met een ondergroep van $G/H_1 \times G/H_2$.
   (c) Gebruik (b) om de Chinese Reststelling nog eens opnieuw te bewijzen.

8. We gaan bewijzen dat voor $n \geq 5$ de enige normaaldeler in S_n ongelijk aan $\{(1)\}$ of de hele groep, A_n is. Laat hiertoe N zo'n niet-triviale normaaldeler in S_n zijn.
   (a) Gebruik dat A_n simpel is om aan te tonen dat $A_n \subset N$ of $N \cap A_n = \{(1)\}$.

(b) Laat zien dat als $A_n \subset N$, dan volgt $N = A_n$.

(c) Laat zien dat als $N \neq \{(1)\}$ en $N \cap A_n = \{(1)\}$, dan $NA_n = S_n$ en $S_n/N \cong A_n$.

(d) Concludeer dat in de situatie van onderdeel (c) moet gelden dat $\#N = 2$, en bewijs dat dit in tegenspraak is met het gegeven dat N een normaaldeler is.

9 Eindig voortgebrachte abelse groepen

In dit hoofdstuk houden we ons vooral bezig met commutatieve groepen. Ons belangrijkste doel daarbij zal zijn, een beschrijving te geven van alle zogeheten eindig voortgebrachte commutatieve groepen.

9.1 Eindig voortgebrachte groepen

Definitie 9.1.1 Een groep G heet *eindig voortgebracht*, wanneer er elementen $g_1, \ldots, g_n \in G$ bestaan met de eigenschap dat elke $g \in G$ te schrijven is als

$$g = g_{i_1}^{\pm 1} \cdot \ldots \cdot g_{i_t}^{\pm 1}$$

voor indices i_j met $1 \leq i_j \leq n$ (N.B. het is hierbij toegestaan dat $i_k = i_\ell$, met andere woorden, dat een g_i meerdere malen gebruikt wordt).

Voorbeeld 9.1.2

1. Iedere eindige groep G is eindig voortgebracht, want we kunnen (bijvoorbeeld) voor $\{g_1, \ldots, g_n\}$ in dit geval de verzameling bestaande uit alle elementen van G nemen.

2. De groep $\mathbb{Z}^r = \mathbb{Z} \times \ldots \times \mathbb{Z}$ (het product van r kopieën van $\mathbb{Z}$) is eindig voortgebracht. Immers, neem $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0), \ldots\ldots, e_r = (0, \ldots, 0, 1) \in \mathbb{Z}^r$. Een willekeurige $(m_1, \ldots, m_r) \in \mathbb{Z}^r$ is dan te schrijven als $m_1 e_1 + \ldots + m_r e_r$. (In dit voorbeeld is deze schrijfwijze bovendien uniek bepaald; de groep $\mathbb{Z}^r$ is daarmee een voorbeeld van een zogeheten *vrije abelse groep*, met basis $e_1, \ldots, e_r$.)

3. De optelgroep $(\mathbb{Q}, +, 0)$ is *niet* eindig voortgebracht. Immers, als $g_1, \ldots, g_n \in \mathbb{Q}$ willekeurig genomen zijn, dan kan een eindige som $\pm g_{i_1} \pm \ldots \pm g_{i_t}$ geschreven worden als a/b met $a \in \mathbb{Z}$ en b gelijk aan het kleinste gemene veelvoud van de noemers van g_1 t/m g_n. Dus een getal $c/d \in \mathbb{Q}$ met $c, d \in \mathbb{Z}$ en $\mathrm{ggd}(c, d) = 1$ en d groter dan dit kleinste gemene veelvoud is niet als zo'n som te schrijven. Hieruit volgt dat geen enkele eindige verzameling $\{g_1, \ldots, g_n\} \subset \mathbb{Q}$ de hele groep voortbrengt.

4. Het is mogelijk dat een groep G eindig voortgebracht wordt, terwijl een ondergroep $H \subset G$ toch niet eindig voortgebracht is. Een aardig voorbeeld van dit fenomeen wordt beschreven in het artikel B.L. van der Waerden, *Example d'un groupe avec deux générateurs, contenant un*

sous-groupe commutatif sans système fini de générateurs, verschenen in het Nieuw Archief voor Wiskunde, Vol. **23** (1951), p. 190.

Evenzo is het mogelijk dat een eindig voortgebrachte groep wordt voortgebracht door elementen met eindige orde, terwijl toch de groep elementen van oneindige orde bevat. Als voorbeeld hierbij nemen we σ_1 de spiegeling in de x-as en σ_2 = spiegelen in de lijn gegeven door $y = ax$. Dan is $\sigma_2\sigma_1$ een rotatie over een hoek α met $\tan(\alpha/2) = a$. Bij geschikte keuze van a heeft deze rotatie oneindige orde. Echter zowel σ_1 als σ_2 hebben orde 2.

5. De groep $\mathrm{SL}_2(\mathbb{Z})$ is eindig voortgebracht. Als voortbrengers kan men bijvoorbeeld de matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ en $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ nemen. Om te bewijzen dat deze matrices inderdaad de groep voortbrengen, nemen we $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ willekeurig. Merk op dat $T^q = \left(\begin{smallmatrix} 1 & q \\ 0 & 1 \end{smallmatrix}\right)$ en $S^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Als $c = 0$, dan $1 = \det(A) = ad$, dus $a = d = 1$ (en dan $A = T^b$), of $a = d = -1$ (en dan $A = S^2T^{-b}$). We gaan er dus verder vanuit dat $c \neq 0$. Er geldt $T^qA = \left(\begin{smallmatrix} a+qc & * \\ c & * \end{smallmatrix}\right)$, dus voor geschikte keuze van q krijgen we hier linksboven de rest r van a bij deling door c. Voor die q is dan $ST^qA = \left(\begin{smallmatrix} -c & * \\ r & * \end{smallmatrix}\right)$. Dit proces van vermenigvuldigen met een geschikte macht van T en vervolgens met S herhalend, worden de getallen in de eerste kolom in absolute waarde steeds kleiner. Dus na eindig veel stappen vinden we een matrix van de vorm $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ en daarvan zagen we reeds dat deze als combinatie van machten van S en T te schrijven is. Hieruit volgt dat ook A zo'n schrijfwijze heeft.

In de rest van dit hoofdstuk zullen we ons beperken tot commutatieve groepen. De groepswet duiden we aan met $+$.

Stelling 9.1.3 *Een eindig voortgebrachte commutatieve groep $(A, +, 0)$ is isomorf met een factorgroep $\mathbb{Z}^n/H$ voor een ondergroep $H \subset \mathbb{Z}^n$.*

Bewijs. Stel dat de verzameling $\{a_1, \ldots, a_n\}$ de groep A voortbrengt. Definiëer

$$\varphi \;:\; \mathbb{Z}^n \longrightarrow A$$

door $\varphi(m_1, \ldots, m_n) = m_1a_1 + \ldots + m_na_n$. Men ziet eenvoudig in dat φ een homomorfisme is. Bovendien is φ surjectief, want $a_1, \ldots, a_n$ brengen A voort, dus elk element van A is als combinatie van deze elementen te schrijven. En omdat A commutatief is, is daarbij de volgorde van de a_i's niet van belang. Met andere woorden, een willekeurige $a \in A$ is te schrijven als $a = n_1a_1 + \ldots + n_na_n$, en dat is het beeld van $(n_1, \ldots, n_n)$ onder φ.

Schrijf $H = \mathrm{Ker}(\varphi)$. Dit is een ondergroep van $\mathbb{Z}^n$. Uit Stelling 8.2.1 volgt nu

$$\mathbb{Z}^n/H = \mathbb{Z}^n/\mathrm{Ker}(\varphi) \cong \varphi(\mathbb{Z}^n) = A.$$

□

9.2 Ondergroepen van vrije abelse groepen

Stelling 9.1.3 laat zien, dat het beschrijven van alle eindig voortgebrachte commutatieve groepen nerkomt op het beschrijven van alle ondergroepen van $\mathbb{Z}^n$ en de bijbehorende factorgroepen $\mathbb{Z}^n/H$. Het geval $n = 1$ kennen we al (vgl. Voorbeeld 3.2.6): dan is $H = m\mathbb{Z}$ voor een $m \geq 0$. Dus $\mathbb{Z}/H \cong \mathbb{Z}$ als $m = 0$ en $\mathbb{Z}/H = (0)$ als $m = 1$, en $\mathbb{Z}/H = \mathbb{Z}/m\mathbb{Z}$ in het algemeen.

Stelling 9.2.1 *Als $H \subset \mathbb{Z}^n$ een ondergroep is, dan is $H \cong \mathbb{Z}^k$ voor een k met $0 \leq k \leq n$.*

Bewijs. We zullen dit met volledige inductie naar n bewijzen. Het geval $n = 0$ is triviaal, en het geval $n = 1$ volgt uit Voorbeeld 3.2.6: dan is namelijk $H = m\mathbb{Z}$ met $m \geq 0$. Voor $m = 0$ is dus $H = (0) \cong \mathbb{Z}^0$, en voor $m > 0$ is $\mathbb{Z} \cong m\mathbb{Z}$, met als expliciet isomorfisme het vermenigvuldigen met m.

Neem nu aan dat de stelling geldt voor $n \geq 1$, en laat $H \subset \mathbb{Z}^{n+1}$ een ondergroep zijn. Definiëer

$$\pi \ : \ \mathbb{Z}^{n+1} \longrightarrow \mathbb{Z} \ \text{ door } \ \pi(m_1, \ldots, m_{n+1}) = m_{n+1}.$$

Dit is een homomorfisme, en de kern van π bestaat uit alle rijtjes $(m_1, \ldots, m_{n+1}) \in \mathbb{Z}^{n+1}$ met $m_{n+1} = 0$. We kunnen deze kern daarom identificeren met $\mathbb{Z}^n$. Omdat $H \subset \mathbb{Z}^{n+1}$ een ondergroep is, is $H \cap \mathrm{Ker}(\pi) \subset \mathbb{Z}^n$ er ook één. Uit de inductiehypothese volgt dat $H \cap \mathrm{Ker}(\pi) \cong \mathbb{Z}^k$ voor zekere k met $0 \leq k \leq n$.

Omdat $H \subset \mathbb{Z}^{n+1}$ een ondergroep is, is $\pi(H) \subset \mathbb{Z}$ dat ook. Dus $\pi(H) = m\mathbb{Z}$ met $m \geq 0$. Is hier $m = 0$, dan $\pi(H) = (0)$ dus $H \subset \mathrm{Ker}(\pi)$ oftewel $\mathbb{Z}^k \cong H \cap \mathrm{Ker}(\pi) = H$. Dus in dit geval zijn we klaar. Neem vanaf nu aan dat $m \neq 0$. Omdat $m \in m\mathbb{Z} = \pi(H)$, kunnen we $h_{k+1} \in H$ kiezen waarvoor geldt $\pi(h_{k+1}) = m$. Kies verder $h_1, \ldots, h_k \in H \cap \mathrm{Ker}(\pi)$ als beelden van $(1, 0, \ldots, 0), \ldots\ldots, (0, \ldots, 0, 1)$ onder een gekozen isomorfisme $\mathbb{Z}^k \cong H \cap \mathrm{Ker}(\pi)$. We gaan bewijzen dat

$$\psi \ : \ \mathbb{Z}^{k+1} \longrightarrow H \quad \text{met} \quad \psi(m_1, \ldots, m_{k+1}) = m_1h_1 + \ldots + m_{k+1}h_{k+1}$$

een isomorfisme is. Het is duidelijk dat ψ een homomorfisme is, en ook dat $\mathbb{Z}^{k+1}$ door ψ inderdaad binnen H wordt afgebeeld. We tonen eerst aan dat

ψ surjectief is. Laat $h \in H$ willekeurig. Dan geldt $\pi(h) \in \pi(H) = m\mathbb{Z}$, dus $\pi(h) = m\ell$ voor zekere $\ell \in \mathbb{Z}$. Er volgt dat $\pi(h - \ell h_{k+1}) = \pi(h) - \pi(\ell h_{k+1}) = m\ell - \ell m = 0$, dus $h - \ell h_{k+1} \in \mathrm{Ker}(\pi) \cap H$. Vanwege ons isomorfisme $\mathbb{Z}^k \cong \mathrm{Ker}(\pi) \cap H$ zijn er dan $\ell_1, \ldots, \ell_k \in \mathbb{Z}$ zodat $h - \ell h_{k+1} = \ell_1 h_1 + \ldots + \ell_k h_k$. Hieruit volgt dat $h = \psi(\ell_1, \ldots, \ell_k, \ell)$, dus ψ is surjectief.

Vervolgens laten we zien dat ψ injectief is. Wegens Stelling 3.3.6 volstaat het, aan te tonen dat $\mathrm{Ker}(\psi) = \{(0, \ldots, 0)\} \subset \mathbb{Z}^{k+1}$. Welnu, laat $(m_1, \ldots, m_{k+1}) \in \mathrm{Ker}(\psi)$. Dan geldt $m_1 h_1 + \ldots + m_{k+1} h_{k+1} = 0 \in H$, dus $m_1 h_1 + \ldots + m_k h_k = -m_{k+1} h_{k+1}$. Omdat $h_1, \ldots, h_k \in \mathrm{Ker}(\pi)$, volgt dan dat $-m_{k+1} h_{k+1} \in \mathrm{Ker}(\pi)$. Dus $0 = \pi(-m_{k+1} h_{k+1}) = -m_{k+1} m$. Onze aanname $m \neq 0$ levert dat $m_{k+1} = 0$, dus $m_1 h_1 + \ldots + m_k h_k = -m_{k+1} h_{k+1} = 0$. Hieruit volgt wegens $\mathbb{Z}^k \cong H \cap \mathrm{Ker}(\pi)$ dat $(m_1, \ldots, m_k) = (0, \ldots, 0) \in \mathbb{Z}^k$. Dus $m_1 = \ldots = m_k = m_{k+1} = 0$, hetgeen laat zien dat ψ injectief is.

De afbeelding ψ is dus een isomorfisme, en hiermee is met inductie de stelling bewezen. □

Opmerking 9.2.2 In bovenstaand bewijs is meermalen impliciet gebruikt dat voor een commutatieve groep H geldt $H \cong \mathbb{Z}^k$ precies dan, als er $h_1, \ldots, h_k \in H$ bestaan zodat elke $h \in H$ op *unieke* wijze te schrijven is als $h = m_1 h_1 + \ldots + m_k h_k$. Een groep H met deze eigenschap wordt een vrije abelse groep (met basis $h_1, \ldots, h_k$) genoemd.

Voorbeeld 9.2.3 Beschouw $H \subset \mathbb{Z}^3$ gegeven door

$$H = \left\{(a, b, c) \in \mathbb{Z}^3 \mid a + 2b + 3c \equiv 0 \bmod 6\right\}.$$

Het is niet moeilijk in te zien, dat H een ondergroep van $\mathbb{Z}^3$ is (bijvoorbeeld: H is de kern van het homomorfisme: $\mathbb{Z}^3 \to \mathbb{Z}/6\mathbb{Z}$ gegeven door $(a, b, c) \mapsto a + 2b + 3c \bmod 6$). Wegens Stelling 9.2.1 en Opmerking 9.2.2 bestaan er dus $r \in \{0, 1, 2, 3\}$ en $h_1, \ldots, h_r \in H$ zodat H de vrije abelse groep met basis $h_1, \ldots, h_r$ is. We gaan zulke $r, h_1, \ldots, h_r$ bepalen volgens de methode van het bewijs van Stelling 9.2.1.

Laat $\pi_i : \mathbb{Z}^3 \to \mathbb{Z}$ de projectie op de $i$de coördinaat zijn. Er geldt $\pi_3(H) = \mathbb{Z}$, want $(1, 1, 1) \in H$, dus $1 \in \pi_3(H)$ en een ondergroep van $\mathbb{Z}$ die 1 bevat, is gelijk aan $\mathbb{Z}$. Het bewijs van Stelling 9.2.1 laat zien, dat nu $(1, 1, 1)$ samen met een basis voor $\mathrm{Ker}(\pi_3) \cap H$ een basis voor H is. Nu is

$$\mathrm{Ker}(\pi_3) \cap H = \{(a, b, 0) \mid a + 2b \equiv 0 \bmod 6\}.$$

Er geldt $\pi_2(\mathrm{Ker}(\pi_3) \cap H) = \mathbb{Z}$, want $(4, 1, 0) \in \mathrm{Ker}(\pi_3) \cap H$ en $\pi_2(4, 1, 0) = 1$. Dus een basis voor $\mathrm{Ker}(\pi_3) \cap H$ bestaat uit bijvoorbeeld $(4, 1, 0)$ samen met een basis voor $\mathrm{Ker}(\pi_2) \cap \mathrm{Ker}(\pi_3) \cap H$. Omdat

$$\mathrm{Ker}(\pi_2) \cap \mathrm{Ker}(\pi_3) \cap H = \{(a, 0, 0) \mid a \equiv 0 \bmod 6\} = \mathbb{Z}(6, 0, 0),$$

vinden we tenslotte

$$H = \mathbb{Z} \cdot (6,0,0) + \mathbb{Z} \cdot (4,1,0) + \mathbb{Z} \cdot (1,1,1).$$

We gaan vervolgens laten zien, dat er voor een ondergroep $H \subset \mathbb{Z}^n$ precies één getal k met $0 \leq k \leq n$ bestaat zodat $H \cong \mathbb{Z}^k$. Dit volgt vrij eenvoudig uit het volgende.

Stelling 9.2.4 *Als $\mathbb{Z}^k \cong \mathbb{Z}^\ell$, dan $k = \ell$.*

Bewijs. Bekijk de samenstelling $\mathbb{Z}^k \cong \mathbb{Z}^\ell \to \mathbb{Z}^\ell/2\mathbb{Z}^\ell$. Hier is de tweede afbeelding het kanonieke homomorfisme naar een factorgroep, en $2\mathbb{Z}^\ell = 2\mathbb{Z} \times \ldots \times 2\mathbb{Z}$. Deze samenstelling is een surjectief homomorfisme, en de kern is precies $2\mathbb{Z}^k$. Wegens Stelling 8.2.1 is dus $\mathbb{Z}^k/2\mathbb{Z}^k \cong \mathbb{Z}^\ell/2\mathbb{Z}^\ell$.

Nu geldt voor elke $m \geq 0$ dat $\mathbb{Z}^m/2\mathbb{Z}^m \cong (\mathbb{Z}/2\mathbb{Z})^m$, immers het homomorfisme $\mathbb{Z}^m \to (\mathbb{Z}/2\mathbb{Z})^m$ gegeven door $(n_1, \ldots, n_m) \mapsto (n_1 \bmod 2, \ldots, n_m \bmod 2)$ is surjectief en heeft als kern precies $2\mathbb{Z}^m$; pas dus opnieuw Stelling 8.2.1 toe.

In ons geval volgt $(\mathbb{Z}/2\mathbb{Z})^k \cong (\mathbb{Z}/2\mathbb{Z})^\ell$. De eerste groep heeft 2^k elementen en de tweede 2^ℓ, dus volgt $k = \ell$ zoals we wilden bewijzen. □

Gevolg 9.2.5 *Als $H \subset \mathbb{Z}^n$ een ondergroep is, dan is er precies één k zodat $H \cong \mathbb{Z}^k$ (en die k voldoet aan $0 \leq k \leq n$).*

Bewijs. Blijkens Stelling 9.2.1 bestaat er zo'n k. Als zowel k_1 als k_2 voldoen, dan $\mathbb{Z}^{k_1} \cong H \cong \mathbb{Z}^{k_2}$, dus wegens Stelling 9.2.4 volgt $k_1 = k_2$. □

9.3 De structuur van eindig voortgebrachte abelse groepen

De hoofdstelling van de theorie van eindig voortgebrachte commutatieve groepen is de volgende.

Stelling 9.3.1 *Is A een eindig voortgebrachte commutatieve groep, dan bestaat er een uniek getal $r \geq 0$ en een uniek (eventueel leeg) rijtje $(d_1, \ldots, d_m)$ met alle $d_i \in \mathbb{Z}$ en $d_i > 1$ en $d_m | d_{m-1} | \ldots | d_1$, zodat*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}.$$

Definitie 9.3.2 Voor een eindig voortgebrachte commutatieve groep A heet het getal r in Stelling 9.3.1 de *rang* van A. De getallen $d_1, \ldots, d_m$ heten de *elementaire delers* van A.

Voorbeeld 9.3.3

1. Is $H \subset \mathbb{Z}^n$ een ondergroep, dan wegens Gevolg 9.2.5 $H \cong \mathbb{Z}^k$ voor een unieke k. In het bijzonder is H dan eindig voortgebracht, en Stelling 9.3.1 klopt in dit geval, met $\text{rang}(H) = k$ en een leeg rijtje elementaire delers.

2. Voor de eindige commutatieve groep $A = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ geldt $\text{rang}(A) = 0$ (allicht), en $(d_1, d_2) = (12, 2)$. Immers,

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Het belangrijkste hulpmiddel in het bewijs van Stelling 9.3.1 luidt als volgt.

Stelling 9.3.4 *Als $H \subset \mathbb{Z}^n$ met $H \neq (0)$ een ondergroep is, dan bestaat er een basis $f_1, \ldots, f_n$ van $\mathbb{Z}^n$ en voor zekere k met $1 \leq k \leq n$ een rijtje $(d_1, \ldots, d_k)$ van gehele getallen $d_i > 0$ met $d_k | d_{k-1} | \ldots | d_1$, zodat $d_1 f_1, \ldots, d_k f_k$ een basis voor H is.*

Bewijs. Kies een basis $e_1, \ldots, e_n$ voor $\mathbb{Z}^n$ (bijvoorbeeld de standaardbasis), en een basis $g_1, \ldots, g_k$ voor H (die bestaat vanwege Stelling 9.2.1). Dan geldt $g_i = a_{1i}e_1 + \ldots + a_{ni}e_n \;\; (i = 1, \ldots, k)$ voor zekere $a_{ij} \in \mathbb{Z}$. De getallen a_{ij} vormen een matrix

$$\begin{pmatrix} a_{1\,1} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nk} \end{pmatrix}.$$

Bij elk paar $(\beta = \{e_1, \ldots, e_n\}, \gamma = \{g_1, \ldots, g_k\})$ krijgen we op deze wijze een $n \times k$ matrix met gehele coëfficiënten, die uitdrukt hoe de basis γ wordt gegeven in termen van de basis β. Vervangen we de basis β door een andere, of vervangen we de basis γ door een andere, dan krijgen we in het algemeen een andere matrix. Uiteindelijk willen we, door deze bases te veranderen uitkomen op een β' voor $\mathbb{Z}^n$ en een γ' voor H, zodat de bijbehorende matrix

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_k \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

is.

Het volgende algoritme maakt in eindig veel stappen van onze beginmatrix een matrix van de gewenste vorm, met dus alleen op de hoofddiagonaal evt. getallen $\neq 0$.

Algoritme.

stap 1 Als A de nulmatrix is, dan zijn we klaar. Zoniet, zoek dan een a_{ij} zodat $|a_{ij}|$ positief en zo klein mogelijk is. Verwissel de eerste en de $i$de rij, en ook de eerste en de $j$de kolom. De nieuwe matrix heeft dan a_{11} ongelijk aan nul, en minimaal. We gaan nu de rest van de eerste kolom schoonvegen.

stap 2 Als een getal a_{i1} in de eerste kolom (met $i \neq 1$) ongelijk is aan nul, tel dan een geschikt veelvoud van de eerste rij bij de $i$de rij op zodat a_{i1} wordt vervangen door een getal r met $0 \leq r < |a_{11}|$. Is $r \neq 0$, verwissel dan vervolgens de $i$de en de eerste rij. Dit herhalen we tot de rest van de eerste kolom alleen uit nullen bestaat.

stap 3 Geheel analoog vegen we vervolgens de rest van de eerste rij schoon.

stap 4 We willen er vervolgens voor zorgen dat elk getal in de matrix door a_{11} deelbaar wordt. Is dit voor a_{ij} nog niet het geval, vervang dan de $i$de rij door de $i$de plus de eerste (dat verandert alleen iets in de eerste kolom), en tel een geschikt veelvoud van de eerste kolom bij de $j$de kolom op. Dat levert een a_{ij} die in absolute waarde kleiner is dan a_{11}. Deze is $\neq 0$, want anders zou a_{ij} al door a_{11} deelbaar zijn geweest. Begin nu opnieuw met stap 1. De nieuwe a_{11} die we zo krijgen is strict kleiner in absolute waarde dan de oude, dus na eindig veel stappen hebben we inderdaad bereikt dat alle a_{ij} door a_{11} deelbaar zijn.

stap 5 Ga vervolgens dezelfde stappen 1 t/m 4 uitvoeren op de matrix verkregen uit de oude door de eerste rij en kolom weg te laten. De eigenschap dat a_{11} alle getallen in de matrix deelt blijft hierbij behouden, dus we vinden een a_{22} die een veelvoud van a_{11} is, zodat alle overige getallen in de tweede rij en kolom van de matrix nul zijn, en zodat a_{22} alle a_{ij} met $i, j \geq 3$ deelt. Zo doorgaand vinden we een matrix met $a_{ij} = 0$ als $i \neq j$ en $a_{11}|a_{22}| \ldots |a_{kk}$.

stap 6 Door tenslotte rijen met ± 1 te vermenigvuldigen en de volgorde van de bijbehorende bases om te keren, wordt een matrix als verlangd verkregen.

We moeten nu aantonen, dat de veranderingen in de beginmatrix die in bovenstaand algoritme plaatsvinden, overeenkomen met het vervangen van een basis van $\mathbb{Z}^n$ of van H door een andere. Hiertoe beschrijven we een aantal manieren om van een basis op een andere over te gaan, en geven voor elk van die manieren aan, wat er met de matrix gebeurt.

1. Verwissel in de basis voor $\mathbb{Z}^n$ de $j$de en de $k$de basisvector.

   Dit levert uiteraard weer een basis voor $\mathbb{Z}^n$ op. Een element $a_1e_1 + \ldots + a_je_j + \ldots + a_ke_k + \ldots + a_ne_n$ wordt ten aanzien van de nieuwe basis geschreven als $a_1e_1 + \ldots + a_ke_k + \ldots + a_je_j + \ldots + a_ne_n$. Met andere woorden, in de matrix die we hebben worden de $j$de en de $k$de rij verwisseld.

2. Verwissel in de basis voor H de $j$de en de $k$de basisvector. Het effect hiervan op de matrix is, dat de $j$de en $k$de kolom omgewisseld worden.

3. Vervang de $j$de basisvector e_j van $\mathbb{Z}^k$ door z'n tegengestelde $-e_j$.

   Ook dit levert natuurlijk opnieuw een basis op. Ten aanzien van de nieuwe basis heeft een element van $\mathbb{Z}^n$ als $j$de coördinaat -1 maal de $j$de coördinaat op de oude basis. Dus het effect op onze matrix is, dat alle getallen in de $j$de rij met -1 worden vermenigvuldigd.

4. Vervang de $j$de basisvector van de gegeven basis voor H door z'n tegengestelde. Het effect hiervan op de matrix is, dat alle getallen in de $j$de kolom met -1 worden vermenigvuldigd.

5. Laat $a \in \mathbb{Z}$, laat $i \neq j$, en vervang in de basis voor $\mathbb{Z}^n$ de basisvector e_i door $e'_i = e_i - ae_j$.

   Ook dit levert inderdaad een nieuwe basis voor $\mathbb{Z}^n$. Immers, de afbeelding $\mathbb{Z}^n \to \mathbb{Z}^n$ gegeven door

   $$\begin{gathered} a_1e_1 + \ldots + a_ie_i + \ldots + a_je_j + \ldots + a_ne_n \\ \mapsto \\ a_1e_1 + \ldots + a_ie_i + \ldots + (a_ia - a_j)e_j + \ldots + a_ne_n \end{gathered}$$

   is een isomorfisme van groepen (ga na!), en $\{e_1, \ldots, e_i, \ldots, e_n\}$ gaat onder deze afbeelding over in $\{e_1, \ldots, e'_i, \ldots, e_n\}$.

   Verder geldt

   $$\begin{gathered} a_1e_1 + \ldots + a_ie_i + \ldots + a_je_j + \ldots + a_ne_n \\ = \\ a_1e_1 + \ldots + a_i(e_i - ae_j) + \ldots + (a_j + a_ia)e_j + \ldots + a_ne_n, \end{gathered}$$

en dat betekent dat het effect op onze matrix is, dat de $j$de rij vervangen wordt door de $j$de plus a maal de $i$de.

6. Tenslotte kunnen we in de basis voor H analoog de g_i vervangen door $g_i - ag_j$. Net als in het bovenstaande geval blijkt, dat dit als effect op de matrix heeft dat de $j$de kolom wordt vervangen door de $j$de plus a maal de $i$de.

De conclusie uit de hier gegeven mogelijke basisveranderingen is, dat als de $n \times k$ matrix A uitdrukt hoe een basis van H wordt weergegeven ten aanzien van een basis van $\mathbb{Z}^n$, en de matrix B is uit A verkregen door herhaald de volgende stappen uit te voeren:

1. in de gegeven matrix twee rijen of twee kolommen verwisselen;
2. in de gegeven matrix een rij of kolom met -1 vermenigvuldigen;
3. in de gegeven matrix een rij/kolom vervangen door die rij/kolom plus a maal een andere rij/kolom;

dan stelt ook B een matrix voor die een basis voor H uitdrukt in een basis voor $\mathbb{Z}^n$. Hiermee is de stelling bewezen. □

Opmerking 9.3.5 Merk op dat het hierboven gegeven procedé in feite algemener toepasbaar is. Namelijk, als we $H \subset \mathbb{Z}^n$ geven als $H = \mathbb{Z}g_1 + \ldots + \mathbb{Z}g_k$ voor zekere $g_i \in \mathbb{Z}^n$, zonder daarbij te veronderstellen dat de g_i een basis voor H vormen, dan kunnen we op dezelfde manier een matrix maken en op dezelfde manier gaan vegen. Uiteindelijk levert dit weer een matrix op met alleen op de diagonaal getallen ongelijk aan nul. De kolommen $\neq 0$ van de uiteindelijke matrix beschrijven dan een basis voor H, uitgedrukt in één of andere basis voor $\mathbb{Z}^n$. Dit levert dus een manier om voor een door eindig veel voortbrengers gegeven ondergroep van $\mathbb{Z}^n$ enerzijds Stelling 9.2.1 opnieuw te bewijzen, en anderzijds ook echt een basis voor zo'n ondergroep te vinden.

Met behulp van Stelling 9.3.4 kunnen we in elk geval het bestaan van $r, d_1, \ldots, d_m$ in Stelling 9.3.1 nu gaan bewijzen.

Bewijs. (van het bestaan van $r, d_1, \ldots, d_m$ in Stelling 9.3.1.) Laat A een eindig voortgebrachte commutatieve groep zijn. Volgens Stelling 9.1.3 geldt dan $A \cong \mathbb{Z}^n/H$ voor een ondergroep $H \subset \mathbb{Z}^n$. Kies bases $f_1, \ldots, f_n$ van $\mathbb{Z}^n$ en $d_1 f_1, \ldots, d_k f_k$ van H zoals in Stelling 9.3.4. Onder het isomorfisme

$\mathbb{Z}^n \cong \mathbb{Z}^n$ gegeven door $\sum a_i f_i \mapsto (a_1, \ldots, a_n)$ gaat H over in de ondergroep $d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots \times d_k\mathbb{Z} \times (0) \times \ldots \times (0)$. Maak vervolgens een afbeelding

$$\varphi \ : \ \mathbb{Z}^n \longrightarrow \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}$$

gegeven door $\varphi(a_1, \ldots, a_n) = (a_1 \bmod d_1, \ldots, a_k \bmod d_k, a_{k+1}, \ldots, a_n)$. Dit is een surjectief homomorfisme, met kern $d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots \times d_k\mathbb{Z} \times (0) \times \ldots \times (0)$. Derhalve geldt vanwege Stelling 8.2.1 dat

$$\begin{aligned} A \cong \mathbb{Z}^n/H &\cong \mathbb{Z}^n/\left(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots \times d_k\mathbb{Z} \times (0) \times \ldots \times (0)\right) \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}^{n-k}. \end{aligned}$$

Als we tenslotte nog de factoren $\mathbb{Z}/1\mathbb{Z} \cong (0)$ in dit product weglaten, en de volgorde van de factoren veranderen, levert dit precies de existentie in Stelling 9.3.1 □

Er rest ons nog, de uniciteit van de getallen $r, d_1, \ldots, d_m$ in Stelling 9.3.1 aan te tonen. Hierbij is het volgende nuttig.

Definitie 9.3.6 Laat A een abelse groep zijn. De verzameling $A_{\text{tor}} = \{a \in A \mid \text{ord}(a) < \infty\}$ is dan een ondergroep van A, die de *torsie ondergroep* van A wordt genoemd.

Ga zelf na dat A_{tor} inderdaad een ondergroep is. Er geldt dat A/A_{tor} behalve het eenheidselement geen elementen van eindige orde heeft (ga na!). Is A eindig voortgebracht, dan weten we dat $A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}$, en in de tweede groep hier zijn elementen van eindige orde precies de elementen $(0, \ldots, 0, \overline{a_1}, \ldots, \overline{a_m})$, met $\overline{a_i} \in \mathbb{Z}/d_i\mathbb{Z}$. Hieruit volgt $A_{\text{tor}} \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}$, en bovendien $A/A_{\text{tor}} \cong \mathbb{Z}^r$.

Uit bovenstaande discussie volgt in het bijzonder dat r uniek bepaald is. Immers, er geldt $\mathbb{Z}^r \cong A/A_{\text{tor}}$, en dat kan vanwege Stelling 9.2.4 slechts voor één r.

Ook zien we dat $d_1 \cdot \ldots \cdot d_r = \#\left(\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}\right) = \#A_{\text{tor}}$ dus het product van de getallen d_1 t/m d_m hangt niet van de gekozen schrijfwijze als in Stelling 9.3.1 af.

Met argumenten van dit soort zullen we de uniciteit van $r, d_1, \ldots, d_m$ gaan aantonen. Eerst geven we nog een paar eenvoudiger aan te tonen feitjes. Het getal d_1 (dat is de grootste van de elementaire delers) is uniek. Immers, het getal d_1 is het grootste getal dat voorkomt als orde van een element van $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}$ (ga na!). Dus is het de maximale orde van een element van A_{tor}, en daarmee ligt het vast.

Ook het *aantal* elementaire delers is direct te beschrijven in termen van A. Immers, neem een priemgetal p. Vermenigvuldigen met p is een homomorfisme van A naar A, en de kern daarvan noemen we $A[p]$. Dit is dus een ondergroep van A, en ook van A_{tor}. Het aantal elementen van deze ondergroep $A[p]$ is gelijk aan het aantal elementen $(\overline{a_1}, \ldots, \overline{a_m}) \in \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}$ dat voldoet aan $p(\overline{a_1}, \ldots, \overline{a_m}) = (\overline{0}, \ldots, \overline{0})$. Men rekent na, dat dit aantal gelijk is aan p^k, met k het aantal d_i's zodat $p|d_i$. Deze k is maximaal wanneer we p een priemdeler van d_m kiezen; in dat geval is $k = m$. Onze conclusie is dat m gelijk is aan de maximale exponent k, zodat er een priemgetal is met $\#A[p] = p^k$. Dit bepaalt m in termen van A.

Bewijs. (van de uniciteit van de elementaire delers in Stelling 9.3.1.) Het uiteindelijke bewijs van de uniciteit van $d_1, \ldots, d_m$ kan bijvoorbeeld met inductie naar $\#A_{\text{tor}} = d_1 \cdot \ldots \cdot d_m$ gegeven worden. Voor $\#A_{\text{tor}} = 1$ is het rijtje elementaire delers leeg, dus hiervoor geldt de uniciteit. Stel $\#A_{\text{tor}} = N > 1$, en neem de uniciteit aan voor alle A' met $\#A'_{\text{tor}} < N$. Laat $d_1, \ldots, d_m$ een rijtje elementaire delers zijn voor A. Omdat $N > 1$ is, geldt $d_m > 1$. Dus kunnen we een priemgetal $p|d_m$ kiezen. Beschouw nu de factorgroep $A' = A/A[p]$. Omdat A eindig voortgebracht is, is A' dat ook, en er geldt $A'_{\text{tor}} \cong \mathbb{Z}/\frac{d_1}{p}\mathbb{Z} \times \ldots \times \mathbb{Z}/\frac{d_m}{p}\mathbb{Z}$. Uit de inductieveronderstelling volgt, dat de getallen $d_1/p, \ldots, d_m/p$ uniek bepaald zijn, en daarmee zijn d_1 t/m d_m dat ook. □

We beschouwen tenslotte nogmaals bepaalde ondergroepen van $\mathbb{Z}^n$, en met name kijken we wanneer zo'n ondergroep eindige index in $\mathbb{Z}^n$ heeft.

Stelling 9.3.7 *Stel dat in $\mathbb{Z}^n$ een ondergroep H wordt voortgebracht door n elementen $g_1, \ldots, g_n$, met $g_i = a_{1i}e_1 + \ldots + a_{ni}e_n$ voor zekere basis $\{e_1, \ldots, e_n\}$ van $\mathbb{Z}^n$. Zij $A = (a_{ij})$ de $n \times n$ matrix hierbij; dan geldt dat H eindige index heeft in $\mathbb{Z}^n$ precies dan, als* $\det(A) \neq 0$.

Is $\det(A) \neq 0$, *dan geldt* $\#\mathbb{Z}^n/H = |\det(A)|$.

Bewijs. Met de veegmethode beschreven in het bewijs van Stelling 9.3.4 kunnen we A overvoeren in een diagonaalmatrix met getallen $d_1, \ldots, d_n$ op de diagonaal. Merk op dat bij dat vegen de determinant op teken na niet verandert, dus $\det(A) = |d_1 \cdot \ldots \cdot d_n|$. Net als in het bewijs van Stelling 9.3.4 volgt dat $\mathbb{Z}^n/H \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$. Laatstgenoemde groep is eindig precies dan, als alle d_i's ongelijk aan 0 zijn. Is dit het geval, dan geldt $\#\mathbb{Z}^n/H = |d_1 \cdot \ldots \cdot d_n| = |\det(A)|$. □

Voorbeeld 9.3.8 Neem $A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 2 & 2 \\ 3 & 4 & 2 \end{pmatrix}$ en $B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 2 \\ 3 & 4 & 2 \end{pmatrix}$.

Er geldt $\det(A) = 0$ en $\det(B) = 4$. Voor de ondergroepen $H_1 = A(\mathbb{Z}^3)$ en $H_2 = B(\mathbb{Z}^3)$ van $\mathbb{Z}^3$ geldt dus dat de factorgroep $\mathbb{Z}^3/H_1$ oneindig is, en dat $\mathbb{Z}^3/H_2$ uit precies 4 elementen bestaat. Met de in het bewijs van Stelling 9.3.4 gegeven veegmethode kunnen we A transformeren tot een diagonaalmatrix met de getallen $1, 2, 0$ op de diagonaal. Bijgevolg is $\mathbb{Z}^3/H_1 \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Evenzo kunnen we B tot de diagonaalgedaante met $1, 2, 2$ op de diagonaal omwerken. Dus geldt $\mathbb{Z}^3/H_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Het element van orde 2 in $\mathbb{Z}^3/H_1$ is de klasse $(0, 1, 1) + H_1$. Immers, dit is niet het nulelement van $\mathbb{Z}^3/H_1$, want dat zou betekenen dat $(0, 1, 1) \in H_1$ hetgeen niet het geval is (bijvoorbeeld omdat elk element van H_1 een tweede coördinaat heeft die even is). De orde van $(0, 1, 1) + H_1$ is inderdaad 2, want $2 \cdot ((0, 1, 1) + H_1) = (0, 2, 2) + H_1 = (0, 0, 0) + H_1$, omdat $(0, 2, 2) \in H_1$.

Probeer analoog zelf de drie elementen met orde 2 in $\mathbb{Z}^3/H_2$ te vinden!

9.4 Opgaven

1. Laat zien dat de vermenigvuldiggroep $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ niet eindig voortgebracht is.

2. Bewijs dat als N een normaaldeler in een eindig voortgebrachte groep G is, dan is de factorgroep G/N ook eindig voortgebracht.

3. Laat $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ en $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ gegeven zijn. Bepaal $U = ST$, en laat zien dat $\mathrm{ord}(S) = 4$ en $\mathrm{ord}(U) = 6$ en dat S en U de groep $\mathrm{SL}_2(\mathbb{Z})$ voortbrengen.

4. Schrijf de matrix $\left(\begin{smallmatrix} 55 & 21 \\ 34 & 13 \end{smallmatrix}\right)$ als product van machten van $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ en $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

5. Toon aan dat $\mathrm{GL}_2(\mathbb{Z})$ eindig voortgebracht is, en geef expliciete voortbrengers die allemaal eindige orde hebben (het kan bijvoorbeeld met drie voortbrengers, van orde $2, 4$ en 6).

6. Geef een alternatief bewijs voor het feit dat $\mathbb{Z}^{k_1} \ncong \mathbb{Z}^{k_2}$ als $k_1 \neq k_2$, door het aantal elementen van $\mathbb{Z}^k/2\mathbb{Z}^k$ te bekijken.

7. Geef een basis voor de ondergroep $H \subset \mathbb{Z}^4$, gegeven door $H = \{(a, b, c, d) \mid a + b + c + d = 0 \text{ en } a \equiv c \bmod 12\}$.

8. Bepaal de rang en de elementaire delers van elk van de volgende groepen.

   (a) $\mathbb{Z} \times 17\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

   (b) $(\mathbb{Z}/15\mathbb{Z})^*$

   (c) $(\mathbb{Z}/17\mathbb{Z})^*$

   (d) $\mathbb{Z}^3$ modulo de ondergroep voortgebracht door $(1, 2, 0)$ en $(3, 0, 0)$.

   (e) A/H, waarbij $A \subset \mathbb{Z}^5$ de groep van alle vijftallen met som 0 is, en $H = A \cap B(\mathbb{Z}^5)$ voor de matrix $B = \begin{pmatrix} -13 & 1 & 1 & 0 & 0 \\ 1 & -13 & 1 & 0 & 0 \\ 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 & -3 \end{pmatrix}$.

9. Hoeveel onderling niet isomorfe commutatieve groepen met precies 72 elementen bestaan er?

10. (a) Gebruik dat $5^{2^{n+1}} - 1 = (5^{2^n} - 1)(5^{2^n} + 1)$ om te bewijzen, dat er precies $n + 2$ factoren 2 in $5^{2^n} - 1$ zitten.

    (b) Leidt uit (a) af, dat de orde van $\overline{5}$ in $(\mathbb{Z}/2^n\mathbb{Z})^*$ gelijk is aan 2^{n-2} (voor $n \geq 2$).

    (c) Laat zien dat voor $n \geq 2$ de afbeelding $a \bmod 2^n \mapsto a \bmod 4$ een welgedefinieerd, surjectief homomorfisme van $(\mathbb{Z}/2^n\mathbb{Z})^*$ naar $(\mathbb{Z}/4\mathbb{Z})^*$ oplevert, met als kern de ondergroep voortgebracht door $\overline{5}$.

    (d) Bepaal het aantal elementen van orde ≤ 2 in $(\mathbb{Z}/2^n\mathbb{Z})^*$, en geef vervolgens de rang en de elementaire delers van $(\mathbb{Z}/2^n\mathbb{Z})^*$.

11. (a) Laat zien dat als A een eindige commutatieve groep is, en p een priemgetal dat het aantal elementen van A niet deelt, dan is $A/pA \cong (0)$.

    (b) Laat zien dat als $A = \mathbb{Z}/N\mathbb{Z}$, en p is een priemgetal met $p|N$, dan is $A/pA \cong \mathbb{Z}/p\mathbb{Z}$.

    (c) Toon aan, dat als A een eindig voortgebrachte abelse groep is en p een priemgetal, dan is $\#A/pA = p^k$, waarin k gelijk is aan de som van de rang van A en het aantal elementaire delers van A dat door p deelbaar is.

12. Laat $d \geq 3$ een geheel getal zijn. We gaan in deze opgave het polynoom $X^2 + X + d$ bestuderen. Zij $\alpha_d \in \mathbb{C}$ een nulpunt van dit polynoom. Definiëer $A_d = \{a + b\alpha_d \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

    (a) Laat zien dat A_d een ondergroep van de optelgroep $\mathbb{C}$ is, en $A_d \cong \mathbb{Z}^2$.

    (b) Neem $\beta = a + b\alpha_d \in A_d$. Toon aan dat $\beta A_d = \{\beta \cdot \gamma \mid \gamma \in A_d\}$ een ondergroep is van A_d, en dat voor $\beta \neq 0$ geldt $\#A_d/\beta A_d = a^2 - ab + db^2$.

    (c) We gaan nu veronderstellen dat er een getal a met $0 \leq a \leq d - 2$ bestaat zodat $a^2 + a + d$ geen priemgetal is. Kies bij deze a de kleinste priemdeler p van $a^2 + a + d$. Laat zien dat $p \leq d - 1$ geldt.

    (d) Met a en p als boven, neem $H = pA_d + (a - \alpha_d)A_d = \{p\gamma + (a - \alpha_d)\delta \mid \gamma, \delta \in A_d\}$. Laat zien dat $H \subset A_d$ een ondergroep is, met voortbrengers $p, p\alpha_d, a - \alpha_d, d + (a + 1)\alpha$. Concludeer hieruit dat $\#A_d/H = p$.

(e) Laat zien dat H geen ondergroep van de gedaante βA_d kan zijn. Wel heeft H de eigenschap, dat voor elke $h \in H$ en $\gamma \in A_d$ het product $h\gamma$ ook weer in H zit (H is gesloten onder vermenigvuldigen met A_d); ga dit na.

(f) Concludeer, dat indien a^2+a+d *niet* voor alle a met $0 \leq a \leq d-2$ een priemgetal is, dan bevat A_d een ondergroep die gesloten is onder vermenigvuldigen met A_d, maar die niet van de gedaante βA_d voor een $\beta \in A_d$ is.

(g) Van A_{41} en A_{17} is bekend, dat alle ondergroepen die gesloten onder vermenigvuldigen met A_d zijn, van de vorm βA_d zijn. Welke conclusies trek je daaruit voor de polynomen $X^2 + X + 17$ resp. $X^2 + X + 41$?