

Inlever opdracht 5

Luc Veldhuis

2 mei 2017

1. Gegeven is dat $V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ een normaaldeler is van S_4 . Als $\rho = (1\ 4)$, $\sigma = (1\ 2\ 3\ 4)$ en $\tau = (1\ 2\ 3)$ in S_4 , geldt dan dat $\bar{\rho}\bar{\sigma} = \bar{\tau}^2$ in S_4/V_4 ?

Omdat gegeven is dat V_4 een normaaldeler is van S_4 ($V_4 \trianglelefteq S_4$), weten we dat geldt voor alle elementen $\bar{a}, \bar{b} \in S_4/V_4$ dat $\bar{a}\bar{b} = \overline{ab} \in S_4/V_4$. Nu zien we dat $\bar{\rho}\bar{\sigma} = \overline{\rho\sigma} = \overline{(1\ 4)(1\ 2\ 3\ 4)} = \overline{(1\ 2\ 3)}$ en dat $\bar{\tau}^2 = \overline{\tau\tau} = \overline{\tau^2} = \overline{(1\ 2\ 3)(1\ 2\ 3)} = \overline{(1\ 3\ 2)}$

De vraag is dus of $\overline{(1\ 2\ 3)} = \overline{(1\ 3\ 2)}$?

Dit is niet het geval als deze elementen in andere nevenklassen zitten.

Uit Proposition 4 [1, p.80] halen we nu dat de elementen zelfde nevenklassen hebben. $\overline{(1\ 2\ 3)} = (1\ 2\ 3)V_4$ gelijk aan $(1\ 3\ 2)V_4 = \overline{(1\ 3\ 2)}$ als geldt dat $(1\ 3\ 2)^{-1}(1\ 2\ 3) \in V_4$

We weten $(1\ 3\ 2)^{-1} = (1\ 2\ 3)$, dus dit geeft $(1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \notin V_4$. Dus dit betekent dat $(1\ 3\ 2)V_4 \neq (1\ 2\ 3)V_4$, omdat ze niet in dezelfde nevenklasse zitten.

Dus $\overline{(1\ 2\ 3)} \neq \overline{(1\ 3\ 2)}$, dus $\bar{\rho}\bar{\sigma} \neq \bar{\tau}^2$ in S_4/V_4

2. Zij p een oneven priemgetal en $G = D_{2p}$ de diëdergroep met $2p$ elementen

(a) Bepaal alle ondergroepen van G .

G is eindig, want we weten hoeveel elementen erin zitten, namelijk $2p$. Dus weten we dat voor alle ondergroepen H de formule van Lagrange geldt:

$$|H| \mid |G|$$

Dus het aantal elementen in H moet $2p$ delen met p een oneven priem, dus groter dan 2. Dan geeft dit $|H| = 1, 2, p, 2p$, want dit zijn alle delers van $2p$

Nu hoeft het niet perse zo te zijn dat deze ondergroepen ook bestaan.

We gaan proberen ondergroepen te vinden van deze groottes:

Voor $|H| = 1$: We weten dat het evenwichts element altijd in een groep moet zitten, dus $e \in H$, dus $H = \{e\}$. Dus dit is ook de enige mogelijkheid. Dit is meteen een ondergroep, want $\forall x, y \in H$ geldt dat $x^{-1}y \in H$

Voor $|H| = 2p$: We weten dat de groep G precies $2p$ elementen heeft. Dus dit is de enige ondergroep die aan deze eis voldoet. Ook weten we dat G een ondergroep is van G . Dus $H = G$.

Voor $|H| = 2$: Nu zoeken we een element zodat $t^2 = e$. Voor elk element in de vorm sr^i met $0 \leq i < p$ geldt $(sr^i)^2 = sr^i sr^i = s sr^{-i} r^i = s sr^{i-i} = e$. Een ondergroep in de vorm $\langle sr^i \rangle$ heeft maar 2 elementen want $\langle sr^i \rangle = \{e, sr^i\}$

Voor elementen in de vorm r^i met $1 \leq i < p$ geldt niet dat $(r^i)^2 = r^{2i} = r^p = e$, want $0 \leq i < p$, dus $2 \leq 2i < 2p$. Dus de enige manier waarop dit mogelijk is, zou zijn als $2i = p$, maar p is oneven, en $2i$ is even. Dus $2i \neq p$ voor geen enkele i . Daarom blijven alleen groepen van de vorm $\langle sr^i \rangle$ met $0 \leq i < p$ over.

Voor $|H| = p$: We zoeken een groep met p elementen. Het makkelijkste is een element t zodat $|t| = p$, want dan zijn er p verschillende elementen. Dit volgt uit de definitie van de orde van een element. We hebben net laten zien dat alle elementen in de vorm sr^i orde 2 hebben, dus dan zouden we al meerdere elementen in deze vorm moeten hebben, maar als we een samenstelling van $sr^i sr^j$ hebben met $0 \leq i < j < p$, geeft dit $sr^i sr^j = s sr^{j-i} = r^{j-i}$. Omdat G geen een eindige groep is, geldt dat elk element in G en dus ook in H een eindige orde heeft. Voor het element r^{j-i} element geldt, omdat p priem is, en $i < j < p$, en $j - i \neq 0$ en $j - i \neq p$, dat $(r^{j-i})^n = r^{(j-i)n} = r^p = e$ als $p \mid n(j - i)$.

We gebruiken nu dat elk getal een unieke priemontbinding heeft. We weten $j - i < p$, dus $p \nmid (j - i)$, dus moet wel gelden $p \mid n$. Dus $n = pk$ met $k \in \mathbb{Z}$.

Er zijn maar p elementen die de vorm hebben van r^i , dus als $n > p$, geldt dat er meer dan p elementen de vorm r^i hebben. Dit leidt tot een tegenspraak, dus moet wel gelden $k = 1$, dus $n = p$. Dus het element r^i heeft orde p . Maar omdat r^i minimaal p unieke elementen nodig heeft, en we al 2 elementen hadden waar we mee begonnen, zitten er nu al minimaal $p + 2$ elementen in de groep

H . Maar de aanname was $|H| = p$, dus het kan niet zo zijn dat elementen in de vorm sr^i, sr^j met $0 \leq i < j < p$ in een groep van deze vorm zitten.

Het enige andere alternatief zijn elementen in de vorm r^i . We gaan kijken wat de orde is voor een element van deze vorm.

Neem r^i met $1 \leq i < p$, dan is $p \neq i \neq 0$

Omdat G een eindige groep is, geldt dat elk element in G en dus ook in H een eindige orde heeft.

Dus bestaat er een n zodat $(r^i)^n = r^p = e$ voor een zeker n . Dit is alleen het geval als $p|ni$. We gebruiken hier de eigenschap dat elk natuurlijk getal een unieke priemontbinding heeft. Omdat $i < p$ geldt $p \nmid i$, dus er moet wel gelden $p|n$. Dit kan alleen als $n = pk$ met $k \in \mathbb{Z}$. Ook geldt dat er maar p elementen zijn van de vorm $r^j \in D_{2p}$, dus moet het wel gelden dat $n = p$, omdat er anders meer elementen in die vorm in D_{2p} zouden zitten. Dus voor elke r^i met $1 \leq i < p$ geldt $|r^i| = p$.

Dus de ondergroep $H = \{r^i | 0 \leq i < p\} = \langle r \rangle$ heeft precies p elementen, en is een ondergroep omdat het geschreven kan worden als generator. Er zijn nu in totaal: 1 ondergroep van de vorm $|H| = 1$, p ondergroepen in de vorm $|H| = 2$, 1 ondergroep in de vorm $|H| = p$, en 1 ondergroep in de vorm $|H| = 2p$, dit geeft ons $1 + p + 1 + 1 = p + 3$ verschillende ondergroepen.

- (b) Welke van deze ondergroepen zijn normaaldeler van G en welke niet? Leg dit zorgvuldig uit.

We hebben in de vorige opdracht als ondergroepen van G de volgende groepen gevonden: $\{e\}, G, \langle r \rangle$ en $\langle sr^i \rangle$ met $0 \leq i < p$.

Een ondergroep N is een normaaldeler als $\forall g \in G$ het geldt dat $gNg^{-1} = N$, met $gNg^{-1} = \{gng^{-1} | n \in N\}$ waarbij gng^{-1} een geconjungeerde van n voor g wordt genoemd.

Uit het boek [1, p. 84] halen we dat $G \trianglelefteq G$ en $\{e\} \trianglelefteq G$ altijd normaaldelers zijn.

Dus nu moeten we nog controleren of de ondergroepen $\langle r \rangle$ en $\langle sr^i \rangle$ met $0 \leq i < p$ normaaldelers zijn.

Eerst controleren we de ondergroep $\langle r \rangle$

Omdat we dit kunnen schrijven als generator, kunnen we door aan te tonen dat alle geconjungeerden van r in $\langle r \rangle$ liggen, laten zien dat het een normaaldeler is. [1, p. 82]

Kies nu een element in de vorm r^j met $0 \leq j < p$, dan geldt $r^j r r^{-j} = r^{j-j+1} = r \in \langle r \rangle$

Kies nu een element in de vorm sr^j met $0 \leq j < p$, dan geldt $(sr^j)^{-1} = sr^j$, dan geldt $sr^j r sr^j = sr^j sr^{-1} r^j = s sr^{-j} r^{-1} r^j = r^{-1+j-j} = r^{-1}$, maar omdat $r \in \langle r \rangle$, zit ook $r^{-1} \in \langle r \rangle$.

Dus alle geconjungeerden van r zitten in $\langle r \rangle$.

Dus $\langle r \rangle$ is een normaaldeler.

Nu nog de groepen $\langle sr^i \rangle$ met $0 \leq i < p$.

Omdat we dit kunnen schrijven als generator, kunnen we door aan te tonen dat alle geconjungeerden van sr^i in $\langle sr^i \rangle$ liggen, laten zien dat het een normaaldeler is.

Kies nu een element in de vorm r^j met $0 \leq j < p$, dan geldt $r^j sr^i r^{-j} = sr^{-j} r^i r^{-j} = sr^{-2j+i}$

Omdat $\langle sr^i \rangle = \{e, sr^i\}$, is het enige element van deze vorm in $\langle sr^i \rangle$ het element sr^i .

De vraag is nu of voor een zekere i en voor alle j met $0 \leq j < p$ geldt dat $-2j + i \bmod p = i$. Neem $j = 1$, dit kan omdat het moet gelden voor alle $0 \leq j < p$ en $p > 2$. Dit geeft $i - 2 \bmod p = i$. Dus $p|(i - 2) - i$ dus $p|2$, maar $p > 2$, dus dit is nooit mogelijk.

Dus er bestaan elementen $g \in G$, zodat $gsr^i g^{-1} \notin \langle sr^i \rangle$.

Dus de ondergroepen in de vorm $\langle sr^i \rangle$ met $0 \leq j < p$ zijn nooit normaaldelers.

Samenvattend, de volgende ondergroepen zijn ook normaaldelers: $G, \{e\}, \langle r \rangle$.

Referenties

- [1] Abstract algebra, Dummit, David Steven and Foote, Richard M, 2004, Wiley Hoboken