Hertentamen Algebra 1, 13 juli 2018

Korte schets van de oplossingen

Opgave 1 (2+1+1+3=7 punten)
Definieer de permutatie $\sigma \in S_8$ door $\sigma = (1\ 8\ 2\ 3\ 4\ 6)(1\ 3\ 7\ 5)$.
a) Schrijf σ als product van disjuncte cykels.
b) Wat is de orde van σ?
c) Wat is het teken van σ?
d) Geef de disjuncte cykelnotatie van $\sigma^{(17^{2018})}$.

Oplossing.
a) $(1\ 4\ 6)(2\ 3\ 7\ 5\ 8)$.
b) $\text{kgv}(3,5) = 15$.
c) cykels van oneven lengte hebben teken 1, dus $1 \cdot 1 = 1$.
d) We zoeken 17^{2018} modulo 15. Omdat $\text{ggd}(17,15) = 1$, en $\varphi(15) = 8$, mogen we de exponent 2018 vervangen door n met $2018 \equiv n \pmod 8$. Omdat 2016 deelbaar is door 8 nemen we $n = 2$. We vinden $17^{2018} \equiv 17^2 \equiv 2^2 \equiv 4 \pmod{15}$. Dus, omdat disjuncte cykels commuteren,

$$\sigma^{(17^{2018})} = \sigma^4 = (1\ 4\ 6)^4(2\ 3\ 7\ 5\ 8)^4 = (1\ 4\ 6)(2\ 8\ 5\ 7\ 3).$$

Opgave 2 (3+2+2+3=10 punten) Merk op dat $399 = 3 \times 7 \times 19$.
a) Bestaat er een $a \in \mathbb{Z}$ met $37a \equiv 1 \pmod{399}$? Zo ja, bepaal zo'n a.
b) Wat is de orde van $(\mathbb{Z}/399\mathbb{Z})^*$?
c) Laat zien dat voor elke $x \in (\mathbb{Z}/399\mathbb{Z})^*$ geldt $x^{18} = \overline{1}$.
d) Bepaal de orde van $\overline{5}$ in $(\mathbb{Z}/399\mathbb{Z})^*$.

Oplossing.
a) Omdat 37 niet deelbaar is door de priemdelers 3, 7 en 19 van 399 geldt $\text{ggd}(37,399) = 1$, dus zo'n a bestaat. Met het algoritme van Euclides vinden we (in zes stappen) dat $151 \cdot 37 - 14 \cdot 399 = 1$, dus we kunnen $a = 151$ nemen. Je kunt ook de inverse modulo 3, 7 en 19 eerst bepalen en daarna met een expliciete versie van de Chinese reststelling een element a modulo 399 construeren dat aan de juiste congruenties voldot, maar dat is niet minder werk.
b) $\varphi(399) = (3-1) \cdot (7-1) \cdot (19-1) = 2 \cdot 6 \cdot 18 = 216$.
c) Wegens de Chinese reststelling is $(\mathbb{Z}/399\mathbb{Z})^*$ isomorf met $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^*$. De ordes van de factorgroepen zijn $2, 6$, respectievelijk 18. Die zijn alle delers van 18, dus in elk van de factorgroepen geldt $x^{18} = 1$ voor alle elementen x. Dat geldt dus ook in het product, dus in $(\mathbb{Z}/399\mathbb{Z})^*$.
d) De orde is wegens c) een deler van 18. In $(\mathbb{Z}/3\mathbb{Z})^*$ is de orde van $\overline{5}$ gelijk aan 2. In $(\mathbb{Z}/7\mathbb{Z})^*$ is de orde van $\overline{5}$ een deler van 6. Er geldt $\overline{5}^2 \equiv 4 \not\equiv 1 \pmod 7$, dus $\overline{5}^3 \equiv \overline{5}^2 \cdot \overline{5} \equiv \overline{4} \cdot \overline{5} \equiv \overline{20} \equiv -\overline{1} \not\equiv 1 \pmod 7$. De orde van $\overline{5}$ in $(\mathbb{Z}/7\mathbb{Z})^*$ is dus geen deler van 2 of 3, maar wel van 6, dus de orde is 6. Dat betekent dat de orde van $\overline{5}$ in $(\mathbb{Z}/399\mathbb{Z})^*$ een veelvoud is van 6 en een deler van 18, dus het is 6 of 18. In $(\mathbb{Z}/19\mathbb{Z})^*$ geldt $\overline{5}^2 \equiv 6 \pmod{19}$, dus $\overline{5}^4 \equiv (\overline{5}^2)^2 \equiv 6^2 \equiv -2 \pmod{19}$ en dus $\overline{5}^6 \equiv \overline{5}^4 \cdot \overline{5}^2 \equiv -2 \cdot 6 \equiv 7 \not\equiv 1 \pmod{19}$. Modulo 19 is de orde dus niet 6, dus modulo 399 ook niet. De orde modulo 399 is dus 18. Alternatief: Je checkt dat modulo 19 geldt $\overline{5}^9 \equiv 1 \pmod{19}$ en $\overline{5}^3 \not\equiv 1 \pmod{19}$, dus de orde van $\overline{5}$ in $(\mathbb{Z}/19\mathbb{Z})^*$ is 9. De orde modulo 399 is het kleinste gemene veelvoud van de ordes modulo 3, 7 en 19, dus gelijk aan $\text{kgv}(2,6,9) = 18$.

Opgave 3 (3+2+3+2=10 punten)
Zij p een oneven priemgetal en definieer $d = (p-1)/2$.
Zij G het beeld van het homomorfisme $\varphi\colon (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ gegeven door $\varphi(x) = x^2$.
Zij H het beeld van het homomorfisme $\chi\colon (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ gegeven door $\chi(x) = x^d$.
a) Laat zien dat G precies d elementen heeft.
b) Laat zien dat de elementen van G precies de nulpunten van het polynoom $X^d - \overline{1}$ zijn.
c) Laat zien dat er geldt $H = \{\overline{1}, -\overline{1}\}$.
d) Laat zien dat er een isomorfisme $(\mathbb{Z}/p\mathbb{Z})^*/G \xrightarrow{\sim} H$ bestaat.

Oplossing.
a) De kern van φ bestaat uit de nulpunten van $X^2 - \overline{1}$. Dat zijn er dus minstens 2, namelijk ± 1, en hooguit 2 wegens Lemma 7.8. Er geldt dus $|\ker\varphi| = 2$ en dus

$$|G| = |(\mathbb{Z}/p\mathbb{Z})^*/\ker\varphi| = (p-1)/|\ker\varphi| = (p-1)/2 = d.$$

b) Voor elke $y \in G$ is er een $x \in (\mathbb{Z}/p\mathbb{Z})^*$ met $x^2 = y$, dus $y^d = (x^2)^d = x^{2d} = x^{p-1} = \overline{1}$. Dus elk element van G is een nulpunt van het polynoom, dus we hebben al d nulpunten. Wegens Lemma 7.8 zijn er niet meer nulpunten, dus dit zijn ze allemaal.
c) Voor elk element $h \in H$ is er een $x \in (\mathbb{Z}/p\mathbb{Z})^*$ met $x^d = h$. Dus geldt $h^2 = (x^d)^2 = x^{2d} = x^{p-1} = \overline{1}$. Dus h is een nulpunt van $X^2 - \overline{1}$. Net als in a) zijn $\overline{1}$ en $-\overline{1}$ de enige nulpunten van dit polynoom, dus geldt $h \in \{\overline{1}, -\overline{1}\}$ en dus $H \subset \{\overline{1}, -\overline{1}\}$. Als $-\overline{1}$ niet in het beeld zou zitten, dan zouden alle $p-1$ elementen van $(\mathbb{Z}/p\mathbb{Z})^*$ een nulpunt zijn van $X^d - \overline{1}$ en dat is in tegenspraak met Lemma 7.8. Dus de inclusie $H \subset \{\overline{1}, -\overline{1}\}$ is een gelijkheid. Voor het laatste stuk van het argument zou je ook d) kunnen gebruiken: er geldt $|H| = |(\mathbb{Z}/p\mathbb{Z})^*|/|G| = (p-1)/d = 2$.
d) De kern van χ bestaat precies uit de nulpunten van $X^d - \overline{1}$, dus wegens b) geldt $\ker\chi = G$. Het homomorfisme χ induceert dus een isomorfisme

$$(\mathbb{Z}/p\mathbb{Z})^*/G = (\mathbb{Z}/p\mathbb{Z})^*/(\ker\chi) \xrightarrow{\sim} H.$$

Opgave 4 (5+4=9 punten)
a) Bepaal het aantal homomorfismen van D_{34} naar de (multiplicatieve) groep $\mathbb{C}^*$.
b) Bepaal het aantal homomorfismen van de (additieve) groep $\mathbb{Q}$ naar de (additieve) groep $\mathbb{Z}$.

Oplossing.
a) Wegens opgave 8.13 is $(D_{34})_{ab}$ isomorf met $V_4 = C_2 \times C_2$. Voor elk van de twee factoren C_2 kunnen we een beeld voor zijn voortbrenger kiezen. Dat beeld moet een orde hebben die een deler is van 2. In $\mathbb{C}^*$ zijn precies twee elementen z die voldoen aan $z^2 = 1$, namelijk ± 1. We vinden dus

$$\#\operatorname{Hom}(D_{34}, \mathbb{C}^*) = \#\operatorname{Hom}((D_{34})_{ab}, \mathbb{C}^*) = \#\operatorname{Hom}(C_2 \times C_2, \mathbb{C}^*) = \#\operatorname{Hom}(C_2, \mathbb{C}^*) \cdot \#\operatorname{Hom}(C_2, \mathbb{C}^*) = 2 \cdot 2 = 4.$$

b) Er is alleen het triviale homomorfisme dat alle elementen naar $0 \in \mathbb{Z}$ stuurt. Stel namelijk dat er een homomorfisme $f\colon \mathbb{Q} \to \mathbb{Z}$ is met een element $x \in \mathbb{Q}$ met $n = f(x) \neq 0$. Dan geldt voor $y = x/(2n)$ en $a = f(y)$ dat

$$2na = 2nf(y) = f(2ny) = f(x) = n,$$

maar $\mathbb{Z}$ bevat geen element a met $2na = n$. Tegenspraak, dus er is geen niet-triviaal homomorfisme.

Opgave 5 (2+3+4=9 punten)
Zij G een groep en $T \subset G$ een deelverzameling (dus niet per se een ondergroep).
Voor elke $a \in G$ definiëren we

$$aTa^{-1} = \{\, ata^{-1} \;:\; t \in T \,\}.$$

Definieer nu

$$F(T) = \left\{\, a \in G \;:\; aTa^{-1} = T \,\right\}.$$

a) Laat zien dat $F(T)$ een ondergroep is van G.
b) Laat zien dat er geldt $\#\{\, aTa^{-1} \;:\; a \in G \,\} = [G : F(T)]$.
c) Geef een voorbeeld van een groep G en een deelverzameling $T \subset G$ waarvoor de bijbehorende ondergroep $F(T)$ niet normaal is in G.

Oplossing.
Zij X de verzameling van alle deelverzamelingen van G. Dan geeft de constructie een werking van G op X en $F(T)$ is niets anders dan de stabilisator van T.
a) Stabilisatoren zijn in het algemeen ondergroepen.
b) De verzameling in het linkerlid is precies de baan van T, dus dit volgt uit Stelling 5.3.
c) Neem $G = S_3$ en $T = \{(12)\}$. De baan van T bestaat uit de drie verzamelingen die precies één transpositie bevatten. De index van $F(T)$ in S_3 is dus 3 wegens b) en heeft dus orde 2. Dus $F(T) = \{(1), (12)\}$ en deze ondergroep is niet normaal.