Tentamen Algebra 1, 28 juni 2018

Korte schets van de oplossingen

Opgave 1 (7 punten)
Definieer de permutatie $\sigma \in S_9$ door $\sigma = (1\ 5\ 8\ 7\ 3)(2\ 4\ 7\ 3\ 6)(1\ 6\ 7\ 4\ 9\ 3)$.
a) Schrijf σ als product van disjuncte cykels.
b) Wat is de orde van σ?
c) Zij H de ondergroep van S_9 voortgebracht door σ. Wat is het aantal banen van de werking van H op de verzameling $\{1, 2, 3, \ldots, 9\}$?

Oplossing
a) $(1\ 2\ 4\ 9\ 6)(3\ 5\ 8\ 7)$
b) De orde is het kleinste gemene veelvoud van de cykellengtes 5 en 4, dus 20.
c) Voor elk van de twee disjuncte cykels is de verzameling van elementen uit die cykel een baan. Er zijn dus precies 2 banen. (Er zijn geen dekpunten, dat wil zeggen cykels van lengte 1 die uit de notatie zijn weggelaten.) Zie bovenaan pagina 22 van het dictaat. Het is ook mogelijk om deze opgave met de banenformule te doen, maar dat is veel meer werk.

Opgave 2 (9 punten)
Beschouw het getal $n = 561 = 3 \times 11 \times 17$.
a) Wat is de orde van de groep $(\mathbb{Z}/n\mathbb{Z})^*$?
b) Laat zien dat voor elk geheel getal a met $\text{ggd}(a, n) = 1$ geldt $a^{n-1} \equiv 1 \pmod{n}$.
c) Bepaal de orde van het element $\overline{2}$ in $(\mathbb{Z}/n\mathbb{Z})^*$.
d) Laat zien dat de groep $(\mathbb{Z}/n\mathbb{Z})^*$ niet cyclisch is.

Oplossing
a) $\varphi(n) = (3-1)\cdot(11-1)\cdot(17-1) = 2\cdot 10\cdot 16 = 320$.
b) Wegens de Chinese Reststelling is $(\mathbb{Z}/n\mathbb{Z})^*$ isomorf met $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* \times (\mathbb{Z}/17\mathbb{Z})^*$. Voor elke priem $p \in \{3, 11, 17\}$ geldt $\varphi(p) = p - 1$, dus voor elk element $x \in (\mathbb{Z}/p\mathbb{Z})^*$ geldt $x^{p-1} = x^{\varphi(p)} \equiv 1 \pmod{p}$. In $(\mathbb{Z}/3\mathbb{Z})^*$ en $(\mathbb{Z}/11\mathbb{Z})^*$ en $(\mathbb{Z}/17\mathbb{Z})^*$ geldt dus voor elk element x respectievelijk $x^2 \equiv 1$ en $x^{10} \equiv 1$ en $x^{16} \equiv 1$. Het kleinste gemene veelvoud van de exponenten 2 en 10 en 16 is 80, dus voor elk geheel getal a met $\text{ggd}(a, n) = 1$ geldt $a^{80} \equiv 1$ modulo 3 en 11 en 17 en wegens de Chinese Reststelling dus ook modulo n. Omdat 80 een deler is van $560 = n - 1$ volgt ook $a^{n-1} \equiv 1$ modulo n.
c) De orde van $\overline{2}$ in $(\mathbb{Z}/3\mathbb{Z})^*$ en $(\mathbb{Z}/11\mathbb{Z})^*$ en $(\mathbb{Z}/17\mathbb{Z})^*$ is respectievelijk 2 en 10 en 8 (check dat!). Het kleinste gemene veelvoud daarvan is 40, dus dat is de gezochte orde.
d) De groep heeft orde 320, maar elk element heeft een orde die een deler is van 80, dus er is geen element met orde 320. De groep is dus niet cyclisch.

Opgave 3 (10 punten)
Zij $G = A_4$ de alternerende groep. Zij $N \subset G$ de ondergroep voortgebracht door de elementen $\sigma = (12)(34)$ en $\tau = (13)(24)$.
a) Laat zien dat N bestaat uit de elementen $(1), \sigma$, τ en $\sigma\tau = \tau\sigma = (14)(23)$.
b) Laat zien dat N normaal is in G.
c) Laat zien dat het quotiënt G/N een abelse groep van orde 3 is.
d) Laat zien dat de commutatorondergroep $[G, G]$ gelijk is aan N. [Hint: gebruik c).]
e) Bepaal hoeveel homomorfismen er bestaan van G naar de groep $(\mathbb{Z}/13\mathbb{Z})^*$.

Oplossing
a) Uiteraard is $\sigma\tau = \tau\sigma = (14)(23)$ bevat in N. Het is ook makkelijk te checken dat de verzameling $\{(1), \sigma, \tau, \sigma\tau\}$ gesloten is onder vermenigvuldiging en het nemen van inversen. Dus is N gelijk aan deze verzameling van vier elementen.
b) Wegens 5.27 is N normaal dan en slechts dan als die de vereniging is van conjugatieklassen.

In S_4 vormen de permutaties van cykeltype $(2,2)$ een conjugatieklasse en dit zijn precies de niet-triviale elementen van N. De identiteit (1) vormt op zichzelf een conjugatieklasse en is dus is N de vereniging van conjugatieklassen in S_4 en dus normaal in S_4. Dan is N ook normaal in A_4.
c) Het quotënt G/N heeft orde $[G : H] = |G|/|N| = 12/4 = 3$ en elke groep van orde 3 is abels. (Elk niet-triviaal element van een groep van priem orde p heeft een orde die een deler is van p en dus gelijk aan p, dus elke groep van priem orde is cyclisch en dus abels.)
d) Uit c) en opgave 8.4 volgt de inclusie $[G, G] \subset N$. Voor de omgekeerde inclusie gebruiken we de identiteit $(abc)(adb)(abc)^{-1}(adb)^{-1} = (ad)(bc)$.
e) Omdat $(Z/13\mathbb{Z})^*$ abels is, is dit wegens Stelling 8.5 gelijk aan het aantal homomorfismen van $G/[G, G]$ naar $(Z/13\mathbb{Z})^*$. Omdat $G/[G, G] = G/N$ een cyclische groep van orde 3 is, is dit aantal gelijk aan het aantal elementen in $(Z/13\mathbb{Z})^*$ waarvan de orde een deler is van 3. (Immers, voor elke cyclische groep C voortgebracht door een element g van eindige orde n en elk homomorfisme $f : C \to H$ van C naar een groep H geldt $f(g)^n = f(g^n) = f(e_C) = e_H$, dus de orde van $f(g)$ deelt n; andersom geldt voor elke element $h \in H$ van orde een deler van n dat de afbeelding $C \to H$ gegeven door $g^k \mapsto x^k$ goed gedefinieerd is.) De groep $(\mathbb{Z}/13\mathbb{Z})^*$ is cyclisch van orde 12 en is dus isomorf met $\mathbb{Z}/12\mathbb{Z}$. Deze laatste groep heeft precies drie elementen waarvan de orde een deler van 3 is, namelijk $\overline{0}, \overline{4}$ en $\overline{8}$. Het gezochte aantal is dus drie.
De groep A_4 is isomorf met de groep van rotaties van de tetraëder, dus onderdelen a), b) en c) van deze opgave lijken veel op het verhaal op pagina 56/57 van het dictaat. Zie video van het college van 5 april, vanaf 0:20:20. Zie ook opgave 4.51 die zegt dat N normaal is in S_4.

Opgave 4 (8 punten)
Geef voor elk van de volgende beschrijvingen een voorbeeld met korte uitleg, of leg kort uit waarom zo'n voorbeeld niet bestaat.
a) Een groep G met een ondergroep H van index $[G : H] = 3$ die niet normaal is in G.
b) Een groep G met een werking op een verzameling X die niet transitief is.
c) Een groep G met een dekpuntsvrije werking op een verzameling X die niet trouw is.
d) Een groep G met precies 17 conjugatieklassen.

Oplossing
a) $\langle(12)\rangle \subset S_3$. Zie pagina 49 voor dit voorbeeld. Let op dat de genoemde groep H wel een ondergroep moet zijn van G; De ondergroep H van S_6 voortgebracht door $(1\,2)$ is bijvoorbeeld geen ondergroep van de groep G voortgebracht door de 6-cykel $(1\,2\,3\,4\,5\,6)$.
b) $G = \{1\}$ werkend op een verzameling X van minstens twee elementen.
c) Neem $n > 2$ en $A = \{\pm 1\}$ en werking van S_n op A gegeven door de samenstelling van het tekenafbeelding $\varepsilon : S_n \to A$ en het homomorfisme $A \to S(A), a \mapsto \lambda_a$ van de reguliere werking. (Elke dekpuntsvrije werking $H \to S(X)$ van een groep H op X, samengesteld met een niet-injectief surjectief homomorfisme $G \to H$ geeft een werking $G \to S(X)$ die aan de voorwaarden voldoet.)
d) $\mathbb{Z}/17\mathbb{Z}$. Een cyclische groep van orde n is abels; elk element vormt zijn eigen conjugatieklasse, dus er zijn n conjugatieklassen. De groepen S_7, S_8 en A_9 hebben respectievelijk 15, 22 en 18 conjugatieklassen. Let op dat in A_n de conjugatieklassen niet puur bepaald worden door het cykeltype.

Opgave 5 (6 punten)
Zij G een groep die werkt op een eindige verzameling X. Laat zien dat elke twee geconjugeerde elementen g en h van G evenveel dekpunten hebben.

Oplossing
Zij $a \in G$ een element waarvoor geldt $aga^{-1} = h$. Dan is er een bijectie $X^{\langle g\rangle} \to X^{\langle h\rangle}$ van de verzameling van dekpunten van g naar de verzameling van dekpunten van h gegeven door $x \mapsto a(x)$. Inderdaad, deze afbeelding is goed gedefinieerd, want voor een dekpunt x van g geldt $g(x) = x$ en dus $h(a(x)) = (aga^{-1})(a(x)) = a(g(x)) = a(x)$, dus $a(x)$ is een dekpunt van h. De afbeelding is bovendien een bijectie: de inverse wordt gegeven door de afbeelding $X^{\langle h\rangle} \to X^{\langle g\rangle}$ gegeven door

$x \mapsto a^{-1}(x)$ die om dezelfde reden goed gedefinieerd is.
Op pagina 58 van het dictaat staat $\tilde{g}gx = gx \Leftrightarrow g^{-1}\tilde{g}gx = x$, met andere woorden: gx is een dekpunt van $\tilde{g}$ dan en slechts dan als x een dekpunt is van de geconjugeerde $g^{-1}\tilde{g}g$ van $\tilde{g}$; zie de video van het college van 5 april, vanaf 1:30:00.
Let op (1): Het is niet per se zo dat x een dekpunt is van g dan en slechts dan als het een dekpunt is van h.
Let op (2): Je mag niet zomaar naar cykeltypes van g en h kijken. De groep G is immers niet per se bevat in $S(X)$. Sterker nog, de groep G zou oneindig kunnen zijn.
Let op (3): Je mag in het herschrijven van uitdrukkingen niet de inverse van x gebruiken; omdat X alleen maar een verzameling is zonder structuur betekent de inverse van X helemaal niets.

Opgave 6 (5 punten)
Zij G een eindige groep met precies 2 conjugatieklassen. Bewijs dat G orde 2 heeft.

Oplossing
Stel n is de orde van G. Dan is $n > 1$, want anders is er slechts één conjugatieklasse. Het eenheidselement van G vormt op zichzelf een conjugatieklasse, dus als er precies twee conjugatieklassen zijn, dan vormen de overige $n - 1$ elementen ook een klasse. De cardinaliteit van die klasse deelt de orde van de groep, dus we vinden dat $n - 1$ een deler is van n. Dan is $n - 1$ ook een deler van het verschil $n - (n - 1) = 1$, dus $n - 1 = 1$ en $n = 2$. Dit is opgave 5.43 uit het dictaat.