Tentamen Algebra 1, 20 juni 2019

Schets van uitwerkingen

Opgave 1

Definieer de permutatie $\sigma \in S_{11}$ 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) Wat is de inverse van σ?

d) We bekijken de werking van $\mathbb{Z}$ op $X = \{1, 2, 3, \ldots, 11\}$ gegeven door

$$\mathbb{Z} \to S(X), \quad k \mapsto \sigma^k.$$

Wat is het aantal banen van deze werking?

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) $(1\ 6\ 9\ 4\ 2)(3\ 7\ 8\ 5)$

d) Voor elk van de twee disjuncte cykels is de verzameling van elementen uit die cykel een baan. Bovendien zijn er nog twee dekpunten, namelijk 10 en 11. Er zijn dus precies 4 banen. Zie bovenaan pagina 22 van het dictaat.

Opgave 2

a) Laat zien dat 2 een primitieve wortel is modulo 19.

b) Hoeveel primitieve wortels zijn er modulo 19?

c) Laat zien dat de multiplicatieve groep $(\mathbb{Z}/38\mathbb{Z})^*$ cyclisch is en geef een voortbrenger.

Oplossing

a) De groep $(\mathbb{Z}/19\mathbb{Z})^*$ heeft orde $\phi(19) = 18$, dus er geldt $2^{18} \equiv 1 \pmod{19}$. De orde k van 2 modulo 19 is dus een deler van 18, en 2 is een primitieve wortel modulo 19 dan en slechts dan als de orde k gelijk is aan 18. De enige priemdelers van $18 = 2 \cdot 3^2$ zijn 2 en 3, dus als de orde k kleiner was dan 18, dan zou k dus een deler van $18/2 = 9$ of van $18/3 = 6$. Het is dus voldoende om te laten zien dat $2^6 \not\equiv 1 \pmod{19}$ en $2^9 \not\equiv 1 \pmod{19}$.

Modulo 19 geldt $2^4 = 16 \equiv -3$, dus $2^6 = 2^4 \cdot 2^2 \equiv -3 \cdot 4 \equiv 7 \not\equiv 1$ en $2^9 = (2^4)^2 \cdot 2 \equiv (-3)^2 \cdot 2 \equiv 18 \equiv -1 \not\equiv 1$, dus we concluderen dat 2 inderdaad een primitieve wortel is.

b) De groep $(\mathbb{Z}/19\mathbb{Z})^*$ is cyclisch van orde 18, dus het aantal elementen dat deze groep voortbrengt is $\phi(18) = 6$.

c) Met behulp van de Chinese reststelling krijgen we een isomorfisme

$$(\mathbb{Z}/38\mathbb{Z})^* \cong (\mathbb{Z}/19\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z})^*,$$

want $\gcd(2, 19) = 1$. Omdat $(\mathbb{Z}/2\mathbb{Z})^*$ de triviale groep is, volgt dat $(\mathbb{Z}/38\mathbb{Z})^*$ isomorf is met de groep $(\mathbb{Z}/19\mathbb{Z})^*$ waarvan we al hadden gezien dat die cyclisch is. Sterker nog, de natuurlijke afbeelding $(\mathbb{Z}/38\mathbb{Z})^* \to (\mathbb{Z}/19\mathbb{Z})^*$ is een isomorfisme. Een voortbrenger voor $(\mathbb{Z}/19\mathbb{Z})^*$ is 2, en het element $2 + 19 = 21$ beeldt daar op af. Dus een voorbrenger is bijvoorbeeld 21 modulo 38.

Opgave 3

a) Bestaat er een $x \in \mathbb{Z}$ met $18x \equiv 1 \pmod{2019}$? Zo ja, bepaal zo'n x.

b) Bestaat er een $x \in \mathbb{Z}$ met $19x \equiv 1 \pmod{2019}$? Zo ja, bepaal zo'n x.

Oplossing

a) Nee, want 18 een 2019 zijn beide deelbaar door 3, dus $18r + 2019s$ is deelbaar door 3 voor alle gehele r, s, dus er zijn geen gehele r, s met $18r + 2019s = 1$.

a) Ja, want $\gcd(19, 2019) = 1$. Met behulp van het Euclidische algoritme vinden we $4 \cdot 2019 - 425 \cdot 19 = 1$, dus $-425 \cdot 19 \equiv 1 \pmod{2019}$, dus we kunnen nemen $x = -425$.

Opgave 4

Zij K de symmetriegroep van een kubus en X de verzameling van de vier lichaamsdiagonalen van de kubus. Zij $\phi\colon K \to S(X)$ de natuurlijke werking.

a) Wat is de kern van ϕ?

We hebben in het dictaat en op het college gezien dat er een determinantafbeelding

$$\det\colon K \to \{\pm 1\}$$

is waarvan de kern de ondergroep $K^+ \subset K$ van draaiingen is. Zij verder

$$\varepsilon\colon S(X) \to \{\pm 1\}$$

de gebruikelijke tekenafbeelding. Zij tenslotte $G = \{\pm 1\} \times \{\pm 1\}$ de groep van de vier paren $(\pm 1, \pm 1)$ met coördinaatsgewijze vermenigvuldiging.
b) Laat zien dat het homomorfisme $K \to G$ dat een symmetrie f stuurt naar $\big(\det f, \varepsilon(\phi(f))\big)$ een kern van orde 12 heeft.
c) Laat zien dat de abels gemaakte K_{ab} isomorf is met G.
d) Hoeveel homomorfismen zijn er van K naar G?
Oplossing
a) De kern bestaat uit de identiteit en de puntspiegeling in het middelpunt van de kubus (zie bovenaan pagina 57).
b) We laten eerst zien dat dit homomorfisme, dat we ψ noemen, surjectief is. Het is voldoende om te laten zien dat de twee elementen $(-1, 1)$ en $(1, -1)$ die samen G voortbrengen in het beeld zitten. Het eerste is het beeld van de puntspiegeling in het middelpunt van de kubus. Het tweede is het beeld van bijvoorbeeld een draaiing over 90 graden rond een lijn door de middelpunten van twee tegenoverliggende zijvlakken, want zo'n draaiing werkt als een 4-cykel op de vier lichaamsdiagonalen. Omdat ψ surjectief is en G orde 4 heeft, volgt $|\operatorname{im}\psi| = 4$. Een van de isomorfiestellingen geeft $\operatorname{im}\psi \cong K/\ker\psi$, dus $|\ker\psi| = |G|/|\operatorname{im}\psi| = 48/4 = 12$.
Alternatief: Er geldt $\ker\psi = \ker\det \cap \ker(\varepsilon \circ \phi) = K^+ \cap \phi^{-1}(\ker\epsilon)$. Omdat ϕ beperkt tot een isomorfisme $K^+ \to S(X) \cong S_4$, gaat deze doorsnede onder ϕ isomorf over in $\ker\epsilon \cong A_4$, dus de gezochte orde is $|A_4| = 12$. Uit de laatste regel van het vorige argument volgt dan $|\operatorname{im}\psi| = 4$, dus we vinden ook (weer) dat ψ surjectief is.
c) Omdat G abels is, is de commutatorondergroep $[K, K]$ bevat in de kern van ψ, en dus heeft $[K, K]$ hooguit orde 12. Aan de andere kant bevat de groep $[K, K]$ de commutatorondergroep $[K^+, K^+]$ van K^+, en omdat K^+ isomorf is met S_4, is de commutatorondergroep $[K^+, K^+]$ isomorf met de groep A_4 van orde 12, dus de groep $[K, K]$ heeft ook minstens orde 12. We zagen ook al dat ψ surjectief was, dus we concluderen dat $[K, K]$ gelijk is aan de kern van ψ. De isomorfiestelling geeft ons dan een isomorfisme

$$K_{\mathrm{ab}} = K/[K, K] = K/\ker\varphi \cong \operatorname{im}\psi = G.$$

d) Omdat G abels is, komt elk homomorfisme $K \to G$ van een uniek homomorfisme $K_{\mathrm{ab}} \to G$, dus het gezochte aantal is gelijk aan het aantal homomorfismen van $K_{\mathrm{ab}} \cong G$ naar G. Voor elk van de twee voortbrengers $(-1, 1)$ en $(1, -1)$ kunnen we een beeld x respectievelijk y in G kiezen zolang $x^2 = y^2 = (1, 1)$, maar dat laatste geldt voor alle elementen $x, y \in G$. Het beeld van het element $(-1, -1)$ ligt dan vast en is xy. We hebben dus twee onafhankelijke keuzes van vier elementen, dus het gezochte aantal is $4 \cdot 4 = 16$.

Opgave 5
Zij n een even geheel getal en zij $g \in S_n$ een $(n-1)$-cykel.
a) Bewijs dat de normalisator N_g van g in S_n orde $n-1$ heeft.
b) Laat zien dat deze normalisator N_g bevat is in A_n.
c) Laat zien dat de conjugatieklasse van g in S_n de vereniging is van twee even grote conjugatieklassen in A_n.
Oplossing
a) De conjugatieklasse C in S_n is een baan onder de conjugatiewerking van S_n op zichzelf, en de normalisator is de stabilisator. Als m de grootte van de conjugatieklasse is, dan volgt dus $m \cdot |N_g| = |S_n| = n!$. Omdat er geldt $m = n!/(n-1)$ (want zoveel $(n-1)$-cykels zijn er), volgt $N_g = n - 1$.
b) De machten van g commuteren met g en zijn dus bevat in N_g. Dat zijn al $n-1$ elementen, en dus alle elementen van N_g. Er volgt dus $N_g = \langle g \rangle$. Omdat n even is, is g een even permutatie, dus $g \in A_n$ en dus $N_g \subset A_n$.
c) De normalisator van g in A_n is de doorsnede van A_n met de normalisator N_g in S_n, en dus

gelijk aan N_g, en deze normalisator van g in A_n heeft dus ook $n-1$ elementen. De baan onder de conjugatiewerking van A_n (dus de conjugatieklasse van g in A_n) heeft dus grootte $|A_n|/(n-1) = \frac{1}{2} \cdot n!/(n-1) = \frac{1}{2} \cdot |C|$. Dit geldt voor elke $(n-1)$-cykel, dus elke conjugatieklasse in A_n die bevat is in C heeft $\frac{1}{2} \cdot |C|$ elementen. Hieruit volgt het gevraagde direct.