TENTAMEN GROEPENTHEORIE

21 JUNI 2012, 9.00–12.00 UUR

De onderstaande 7 opgaven zijn elk 5 punten waard. Daarbij krijg je 5 punten kado, zodat er in totaal 40 punten te behalen zijn.

(1) Deze opgave gaat over de vermenigvuldiggroepen $(\mathbb{Z}/51\mathbb{Z})^*$ en $(\mathbb{Z}/80\mathbb{Z})^*$.
   (a) [2 punten]. Laat zien dat deze groepen evenveel elementen hebben.
   (b) [3 punten]. Laat zien dat deze groepen niet isomorf zijn.

(2) In $\mathrm{SL}_2(\mathbb{Z})$ (dat is de groep van 2×2 matrices met gehele coëfficiënten en determinant 1) definiëren we

$$H := \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \; : \; n \in \mathbb{Z} \right\}.$$

   (a) [2 punten]. Toon aan dat H een ondergroep is van $\mathrm{SL}_2(\mathbb{Z})$.
   (b) [3 punten]. Bepaal de index $[\mathrm{SL}_2(\mathbb{Z}) : H]$ (Hint: Onder welke voorwaarde op $a, b \in \mathbb{Z}$ geldt $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) H = \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right) H$?).

(3) [5 punten]. Gegeven $\tau = (1\,2\,3)(2\,3\,4)(5\,6\,7)(7\,8\,9) \in S_9$ en $n = 2106^{2013} \in \mathbb{Z}$. Bereken τ^n.

(4) Laat $n \geq 3$, en nummer de hoekpunten van een regelmatige n-hoek als $1, 2, 3, \cdots, n$. Omdat elk element van de groep D_n een permutatie van deze hoekpunten levert, krijgen we zo een afbeelding $D_n \longrightarrow S_n$.

Bewijs dat het beeld van deze afbeelding in A_n ligt, dan en slechts dan als $n \equiv 1 \bmod 4$.

(Hint: kijk eerst ([2 punten]) welke permutatie er hoort bij een rotatie over $2\pi/n$; onder welke voorwaarde zit die permutatie in A_n? Kijk vervolgens hoe het zit met een spiegeling ([3 punten]).)

(5) [5 punten] Neem een priemgetal p en een groep G bestaande uit precies p^n elementen (voor zeker geheel getal $n \geq 1$). Laat zien dat het centrum van G uit tenminste p elementen bestaat.

(6) Gegeven een geheel getal $n \geq 2$. We duiden met G de groep aan, bestaande uit alle bijecties: $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gegeven door een formule $f(x) = ax+b$, waarbij a de groep $(\mathbb{Z}/n\mathbb{Z})^*$ doorloopt en b de groep $\mathbb{Z}/n\mathbb{Z}$.

Verder bestaat $N \subset G$ uit de bijecties f die voldoen aan

$$f(1 \bmod n) - f(0 \bmod n) = 1 \bmod n.$$

   (a) [2 punten].Toon aan dat N een normaaldeler in G is.
   (b) [3 punten]. Toon aan dat $G/N \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(7) Gegeven is de ondergroep

$$H := \mathbb{Z} \cdot (2, 5, 5) + \mathbb{Z}(6, 6, 6) \subset \mathbb{Z}^3.$$

   (a) [3 punten]. Wat is de orde van $(1, 0, 0) + H \in \mathbb{Z}^3/H$?
   (b) [2 punten]. Wat is de orde van $(0, 0, 1) + H \in \mathbb{Z}^3/H$?

1 a) priemfactorisatie:

$51 = 3 \cdot 17$

$80 = 2^4 \cdot 5$

$$\#(\mathbb{Z}/51\mathbb{Z})^* = \varphi(51) = \prod_{p|n} (p-1)p^{v_p(n)-1}$$

$$= 2 \cdot 16 = 32$$

$$\#(\mathbb{Z}/80\mathbb{Z})^* = \varphi(80) = \prod_{p|n} (p-1)p^{v_p(n)-1}$$

2

$$= 1 \cdot 2^3 \cdot 4 = 32$$

dus ze hebben evenveel elementen

b) chinese reststelling

$(\mathbb{Z}/80\mathbb{Z})^* = (\mathbb{Z}/16 \cdot 5\mathbb{Z})^*$

en $ggd(16,5) = 1$ dus

3

$(\mathbb{Z}/80\mathbb{Z})^* \cong (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$

en $(\mathbb{Z}/51\mathbb{Z})^* \cong (\mathbb{Z}/17\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$

ordes die voorkomen in $(\mathbb{Z}/80\mathbb{Z})^*$ zijn kgv van ordes van $(\mathbb{Z}/16\mathbb{Z})^*$ en $(\mathbb{Z}/5\mathbb{Z})^*$, en die zijn delers van $\#(\mathbb{Z}/16\mathbb{Z})^* = 8$ en $(\mathbb{Z}/5\mathbb{Z})^* = 4$, dus ordes 1, 2, 4 en 8

in $(\mathbb{Z}/17\mathbb{Z})^*$ geldt orde deelt $\#(\mathbb{Z}/17\mathbb{Z})^* = 16$

dus orde is 1, 2, 4, 8 of 16.

$3^2 = 9 \qquad 3^4 = 81 = 13 \bmod 17$

$3^8 = (13)^2 = 169 = (-1) \bmod 17$

$3^{16} = 1 \bmod 17$

dus 3 heeft orde 16 in $(\mathbb{Z}/17\mathbb{Z})^*$, dus $(\mathbb{Z}/51\mathbb{Z})^*$ bevat een element van orde 16 en $(\mathbb{Z}/80\mathbb{Z})^*$ niet, dus ze zijn niet isomorf

6

2 a) H_1) zit $e \in H$? $\quad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

zit in H $\quad (n = 0)$

H_2) stel $A \in H$, $B \in H$ dan ook $AB \in H$?

$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$

$$AB = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+a \\ 0 & 1 \end{pmatrix}$$

en $b, a \in \mathbb{Z}$ dus $b + a \in \mathbb{Z}$
dus $AB \in H$

H_3) stel $A \in H$, dan ook $A^{-1} \in H$?

$$\left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & 0 & 1 & -a \\ 0 & 1 & 0 & 1 \end{array}\right)$$

$A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$ en $-a \in \mathbb{Z}$ (want $a \in \mathbb{Z}$)

dus $A^{-1} \in H$

H voldoet aan H_1, H_2, H_3 en is een subset van $SL_2(\mathbb{Z})$ omdat het matrices zijn met gehele coefficienten en determinant 1, dus H is een ondergroep van $SL_2(\mathbb{Z})$

8

b) $[SL_2(\mathbb{Z}):H] = \# \{AH : A \in SL_2(\mathbb{Z})\}$

$IH = H$ is zo'n set
en voor alle $A \in H$ geldt $AH = H$

nu gaan we kijken naar $A \notin H$

kies $A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ en

$B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$

er geldt of $AH = BH$ of $(AH \cap BH) = \emptyset$

als $AH = BH$ dan ~~is~~ zijn er een H_1 en $H_2 \in H$
zodat $AH_1 = BH_2$
$H_1 = A^{-1}BH_2$ ($\det(A) = 1$, dus A inverteerbaar)
$A^{-1}B = H_1 H_2^{-1}$
dus $A^{-1}B \in H$

maar $A^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$ en $A^{-1}B = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b-a & 1 \end{pmatrix}$

dit zit in H als $b-a=0$, maar er zijn oneindig a's en b's te verzinnen waarvoor $b-a \neq 0$, hiervoor geldt dus $AH \neq BH$ (want $A^{-1}B \notin H$)

dus er zijn oneindig disjuncte sets in de vorm AH, dus de index is oneindig

8

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

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

$\text{orde}(\tau) = \text{kgv}(2,2,5) = 10$

~~$\tau^{2106^{2013}} = \left(\tau^{2106}\right)^{2106^{2012}} = \left(\tau^{2100}\tau^{6}\right)^{2106^{2012}}$~~ $2106 = 2\cdot 3^4 \cdot 13$

~~$= \left(\left(\tau^{10}\right)^{210}\tau^{6}\right)^{2106^{2012}} = \left(\tau^{6}\right)^{2106^{2012}}$~~

~~$= \tau^{(2106^{2012})\cdot 6} =$~~

want $\tau^{a+k\cdot 10} = \tau^{a}\cdot id = \tau^{a}$

$\tau^{2106^{2013}} = \tau^{a}$ waar $a = 2106^{2013} \bmod 10$

$2106^{2013} \bmod 10 = 6^{2013} \bmod 10$

$= 6^{2000}\cdot 6^{13} \bmod 10$

$= (6^2)^{1000}\cdot 6^{13}$

met rekenmachine, maar blijkt: $6^k \bmod 10 = 6$ voor alle k

$= 6^{1000}\cdot 6^{10}\cdot 6^{3} \bmod 10$

$= (6^2)^{500}\cdot (6^2)^{5}\cdot 6 \bmod 10$

$= (6^2)^{250}\cdot 6^{5}\cdot 6 \bmod 10$

$= (6)^{125}\cdot 6^{5}\cdot 6 \bmod 10$

$= (6^5)^{6}\cdot 6 \bmod 10$

$= 6^{7} \bmod 10$

$= (6^2)^{3}\cdot 6 \bmod 10$

$= 6^{3}\cdot 6 \bmod 10$

$= (6^2)^{2} \bmod 10$

$= 6^{2} \bmod 10$

$= 6 \bmod 10$ R

dus $\tau^{2106^{2013}} = \tau^{6} = (1\,2)^6(3\,4)^6(5\,6\,7\,8\,9)^6$

$= (5\,6\,7\,8\,9)$ R

4 de permutatie die hoort bij een rotatie over $2\pi/n$ is elk puntje een puntje op laten schuiven dus bij tegen de klok in draaien en nummeren krijg je

$$\rho \to (1\ 2\ 3\ \ldots\ n) = \tau$$

deze permutatie zit in A_n als

$$\varepsilon(\tau) = (-1)^{\Sigma(l_i - 1)} = (-1)^{l_i - 1} = (-1)^{n-1} = 1$$

dus dan en slechts dan als n oneven is zit deze permutatie in A_n

de spiegeling σ draait twee punten om

we kijken nu alleen naar n oneven, anders zit ρ al niet in A_n

als n oneven is, dan ligt 1 punt op de x-as, dus die hoeft niet verwisseld, de overige $n-1$ punten worden dan omgewisseld, dat levert $\frac{n-1}{2}$ 2 cykels als permutatie. deze permutatie is even dan en slechts dan als $\frac{n-1}{2}$ is even.

5

dus σ en ρ beelden af op A_n desda $\frac{n-1}{2} = 2k$

$n = 4k+1$ dus $n = 1 \bmod 4$

omdat σ en ρ de generatoren van de groep zijn en de afbeelding een isomorfisme moet gelden dat het beeld in A_n ligt d.e.s.d.a. het beeld van σ en ρ in A_n liggen $\Longleftrightarrow n = 1 \bmod 4$

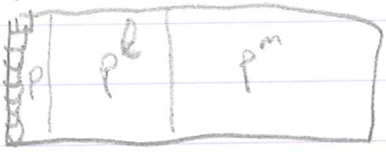
5 $\# G = p^n$

4 centrum $Z(G) = \{x \in G \mid \forall y \in G \;\; xy = yx\}$

voor de eindige groep G geldt
$\mathrm{ord}(x) \mid p^n \;\; \forall x$

dus $\mathrm{ord}(x) = 1$ of $\mathrm{ord}(x) = p^k$ voor een $k \leq n$

het centrum bestaat uit alle elementen die als conjugatieklasse alleen zichzelf hebben. G is disjuncte vereniging van conjugatieklassen:



elk aantal elementen van een conjugatie klasse deelt p^n dus is p^l voor een l

$G = \cup \, C_x$

$\# G = p^{l_1} + p^{l_2} + \dots + p^{l_m} + m \cdot 1$

want l kan ook nul zijn

$$p^n = \underbrace{p^{l_1} + p^{l_2} + \dots p^{l_m}}_{\text{deelt } p^n \text{ en is niet } p^n \text{, dus } \leq p^{n-1}} + m \cdot 1$$

nee

~~dit kan alleen~~ dus $m \geq \cancel{p^n - p^{n-1}} \geq p$

dus minstens p elementen die als conjugatieklasse alleen zichzelf hebben, dus $\# Z(G) \geq p$

6 $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$x \mapsto ax+b$ met $a \in (\mathbb{Z}/n\mathbb{Z})^*$

$b \in \mathbb{Z}/n\mathbb{Z}$

$N \subset G$ bijecties die voldoen aan

$f(1 \bmod n) - f(0 \bmod n) = 1 \bmod n$

a) ik definieer $\varphi: G \to (\mathbb{Z}/n\mathbb{Z})^*$

1

$ax+b \to a$ φ homomorfisme?

$\ker(\varphi) = \{ax+b \mid a = \bar{1}\} = \{x+b\}$

dus als $f \in \ker(\varphi)$

dan $f(\bar{1}) - f(\bar{0}) = \bar{1}+b-(\bar{0}+b) = \bar{1}$

dus $f \in N$ en als $f \in N$, dan

$a\bar{1}+b-(a \cdot \bar{0}+b) = a(\bar{1}-0) = a(\bar{1}) = \bar{1}$

dus $a = \bar{1}^{-1} = \bar{1}$

~~dan~~ $f \in \ker(\varphi)$

dus $\ker(\varphi) = N$ dus N is een normaaldeler in G

b) φ is surjectief, want voor elke $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$

3 ~~wordt~~ is er een bijectie $\bar{a}x+b$ b=?

dus $\varphi(G) = (\mathbb{Z}/n\mathbb{Z})^*$ en er geldt

$G/N \cong \varphi(G) = (\mathbb{Z}/n\mathbb{Z})^*$

7 a)

$$H = \begin{pmatrix} 2 \\ 5 \\ 5 \end{pmatrix} \mathbb{Z} + \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix} \mathbb{Z}$$

in $\mathbb{Z}^3/H$ is de groepsbewerking optellen, dus $\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + H \right)^k$

$$= k \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + H$$

de vraag is, wat is de kleinste k waarvoor dit gelijk is aan H?

$$k \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + H = H$$

dan en slechts dan als

$$k \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in H$$

de elementen van H zijn

$$m \cdot \begin{pmatrix} 2 \\ 5 \\ 5 \end{pmatrix} + n \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix}, \quad m, n \in \mathbb{Z}$$

dus $k \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = m \begin{pmatrix} 2 \\ 5 \\ 5 \end{pmatrix} + n \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix}$ $\quad k, m, n \in \mathbb{Z}$

om de onderste twee nul te krijgen moet gelden $5m = -6n$ en omdat $\gcd(5,6) = 1$ moet gelden $m = (6l)$ en $n = (-5l)$

er geldt dan $k = 2m + 6n = 2(6l) - 6(5l)$

$$= 12l - 30l = -18l \quad (l \in \mathbb{Z})$$

de kleinste positieve k waarvoor dat geldt is $k = 18$, dus de orde is 18

7 b)

$$k\begin{pmatrix}0\\0\\1\end{pmatrix} + H = H$$

desda

$$k\begin{pmatrix}0\\0\\1\end{pmatrix} \in H$$

maar $\begin{pmatrix}0\\0\\k\end{pmatrix}$ zit niet in de span van $\begin{pmatrix}2\\5\\5\end{pmatrix}$ en $\begin{pmatrix}6\\6\\6\end{pmatrix}$ $\forall k$

dus de orde van $\begin{pmatrix}0\\0\\1\end{pmatrix} + H$ is ∞ in $\mathbb{Z}^3/H$