10

Groepentheorie
02-02-11

opg 1) $G = (\mathbb{Z}/3700\mathbb{Z})^*$

a) 3700 in priemgetallen factoriseren

$3700 = 2.1850 = 2.2.925 = 2.2.5.185 = 2.2.5.5.37$

$3700 = 2^2.5^2.37$

De Chinese Reststelling gebruiken geeft

$(\mathbb{Z}/3700\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^* \times (\mathbb{Z}/37\mathbb{Z})^*$

want $ggd(4,25) = ggd(4,37) = ggd(25,37) = 1$

$(\mathbb{Z}/4\mathbb{Z})^* = \{\bar{1}, \bar{3}\}$

$(\mathbb{Z}/25\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{11}, \bar{12}, \bar{13}, \bar{14}, \bar{16}, \bar{17}, \bar{18}, \bar{19}, \bar{21}, \bar{22}, \bar{23}, \bar{24}\}$

$\#(\mathbb{Z}/25\mathbb{Z})^* = 20$

37 is een priemgetal, dus $\#(\mathbb{Z}/37\mathbb{Z})^* = 36$

Al deze groepen zijn eindig, dus de orde van een element, moet een deler zijn van het totale aantal elementen in de groep.

Een element van orde 5 kan alleen in $(\mathbb{Z}/25\mathbb{Z})^*$ zitten.

$\bar{2} \in (\mathbb{Z}/25\mathbb{Z})^*$ heeft orde 4 : $2^4 = \bar{16} = 1 \bmod 25$

~~$\bar{3} \in (\mathbb{Z}/25\mathbb{Z})^*$ $3.\bar{3} = \bar{9}$, $\bar{9}.\bar{3} = \bar{27} = \bar{12}$, $\bar{12}.\bar{3} = \bar{36} = \bar{1}$~~

~~$\bar{6}.\bar{3} = \bar{18} = \bar{3}$~~

Het blijkt dat $\bar{16} \in (\mathbb{Z}/25\mathbb{Z})^*$ heeft ord$(\bar{16}) = 5$,

Dus $(1 \bmod 4, 16 \bmod 25, 1 \bmod 37)$ heeft orde 5 en

$(\mathbb{Z}/3700\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^* \times (\mathbb{Z}/37\mathbb{Z})^*$

Dus dan moet $(\mathbb{Z}/3700\mathbb{Z})^*$ ook een element van orde 5 hebben.

b) Voor $(a \bmod 4, b \bmod 25, c \bmod 37) \in (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^* \times (\mathbb{Z}/37\mathbb{Z})^*$
geldt $\text{ord}(a \bmod 4, b \bmod 25, c \bmod 37) = \text{kgv}(\text{ord}(a \bmod 4), \text{ord}(b \bmod 25), \text{ord}(c \bmod 37))$

37 is een priemgetal, dus om een element van orde 37 te hebben, moet één van de afzonderlijke groepen een element met orde 37 hebben.
$\#(\mathbb{Z}/4\mathbb{Z})^*, \#(\mathbb{Z}/25\mathbb{Z})^*, \#(\mathbb{Z}/37\mathbb{Z})^* < 37$,
dus ze hebben geen element van orde 37,
en dus $\text{ord}(\bar{a}, \bar{b}, \bar{c}) \neq 37$, $\forall \bar{a} \in (\mathbb{Z}/4\mathbb{Z})^*, \bar{b} \in (\mathbb{Z}/25\mathbb{Z})^*, \bar{c} \in (\mathbb{Z}/37\mathbb{Z})^*$
En dus heeft ook $G = (\mathbb{Z}/3700\mathbb{Z})^*$ geen element van orde 37

c) Als $\text{kgv}(a, b, c) = 8$, dan ~~in ieder geval~~ één van de drie $= 8$ en de anderen zijn 2, of 4 of 1
We zoeken dus een element met orde 8 in één van de 3 groepen.
$8 \nmid \#(\mathbb{Z}/4\mathbb{Z})^*$ en $8 \nmid \#(\mathbb{Z}/25\mathbb{Z})^*$, en ook ~~maar wel~~ $8 \nmid \#(\mathbb{Z}/37\mathbb{Z})^* = 36$.
~~Dus kijken of $(\mathbb{Z}/37\mathbb{Z})^*$ een element met orde 8 heeft,~~
~~zo ja, dan G ook en zo nee, dan G niet~~
Dus geen van de groepen heeft een element met orde 8,
dus in $(\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^* \times (\mathbb{Z}/37\mathbb{Z})^*$ zit ook geen element met orde 8 en dus omdat $G \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/25\mathbb{Z})^* \times (\mathbb{Z}/37\mathbb{Z})^*$
zit er ook geen element met orde 8 in G.

Opg 2) $\tau = (5\,6\,7\,9\,8)(3\,4\,5\,6)(2\,3\,4\,5)(1\,2\,7)$
a) τ schrijven als product van disjuncte cykels
$\tau = (1\,4\,7)(2\,9\,8\,5)(3\,6)$, $\tau = \sigma_1 \cdot \sigma_2 \cdot \sigma_3$ $\sigma_1 = (1\,4\,7)$ $\sigma_2 = (2\,9\,8\,5), \sigma_3 = (3\,6)$
Voor de orde geldt $\text{ord}(\tau) = \text{kgv}(\text{ord}(\sigma_1), \text{ord}(\sigma_2), \text{ord}(\sigma_3))$.
Een k-cykel heeft orde k,
dus $\text{ord}(\tau) = \text{kgv}(3, 4, 2) = 12$.

b) Het teken is een homomorfisme,
en $\varepsilon(\sigma_i) = (-1)^{l_i - 1}$
Dus $\varepsilon(\tau) = \varepsilon(\sigma_1).\varepsilon(\sigma_2).\varepsilon(\sigma_3) = (-1)^2.-1.(-1)^3 = 1$
Dus τ is een even permutatie.

c) We weten dat in S_n de conjugatieklassen alleen van de cykel typen afhangen.
We moeten dus bepalen hoeveel permutaties in S_9 er zijn van de vorm 4-cykel, 3-cykel, 2-cykel.
Voor de 4-cykel: als je de kleinste van de genomen getallen voor aan zet zijn er
$\binom{9}{4}.3!$ mogelijke manieren om een 4-cykel te maken
Voor de 3-cykel zijn dan nog 5 getallen over en zet weer de kleinste voor aan, dan zijn er
$\binom{5}{3}.2$ manieren om dan nog een 3 cykel te maken.
De 2-cykel ligt dan vast.
Dus de conjugatieklasse van τ in S_9
bevat $\binom{9}{4}3!.\binom{5}{3}.2 = \frac{9!}{4!.5!}\cdot\frac{5!.2!}{3!.2!} = \frac{9!}{4!} = 15120$ elementen.

opg 3) p priemgetal, G groep bestaande uit alle bijecties $\tau_{a,b}$ van $\mathbb{Z}/p^2\mathbb{Z}$ naar zichzelf.
$\tau_{a,b}(x \bmod p^2) = (ax + b) \bmod p^2$
$b \in \{0, 1, \dots, p^2-1\}$ en $a = 1 + kp$ voor $0 \le k \le p-1$

a) Bepaal de inverse van $\tau_{a,b}$
Dus we zoeken $\tau^{-1}_{a,b}$ zodat $\tau_{a,b} \circ \tau^{-1}_{a,b} = \tau^{-1}_{a,b} \circ \tau_{a,b} = id_G$
Dus $\tau^{-1}_{a,b}(\tau_{a,b}(x \bmod p^2)) = \tau^{-1}_{a,b}((ax+b) \bmod p^2) = x \bmod p^2$
Stel $\tau^{-1}_{a,b} = \tau_{c,d}$, dan $\tau^{-1}_{a,b}(\tau_{a,b}(x \bmod p^2)) = (c(ax+b)+d) \bmod p^2 \stackrel{?}{=} x \bmod p^2$
Dus $\overline{ca}x = \overline{1}$ en $\overline{-cb} = \overline{d}$ $l = p-k$
neem $c = 1 + lp$, dan $cax = (1+lp)(1+kp)x = (1 + (l+k)p + (l+k)lp^2)x$
$= (1 + p^2 + (l+k)p^2)x = x \bmod p^2$
neem $d = -(1+lp).b = (-b - lpb) \bmod p^2$
Dan $d \in \{0, 1, \dots, p^2-1\}$ en $0 \le l \le p-1$

Nu is ook $r_{a,b}(r^{-1}_{a,b}(x \bmod p^2)) = x \bmod p^2$?

$r_{a,b}(r^{-1}_{a,b}(x \bmod p^2)) = r_{a,b}((cx+d) \bmod p^2) = a(cx+d)+b \bmod p^2$

$acx = cax \bmod p^2 = x \bmod p^2$

$ad+b = -acb+b \bmod p^2 = -cab+b+\bmod p^2 = -b+b \bmod p^2 = 0 \bmod p^2$

Dus $r_{a,b}(r^{-1}_{a,b}(x \bmod p^2)) = x \bmod p^2$

Dus $r^{-1}_{a,b} = r_{c,d}$ met $c = i+kp$ voor ~~$0 \le k \le p-1$~~ $l = p-k$, dan $0 \le l \le p-1$

en $d = -cb \bmod p^2$ en $d \in \{0, 1, \dots, p^2-1\}$

Dus $r^{-1}_{a,b} \in G$

b) $r_{1,1}(x \bmod p^2) = x+1 \bmod p^2$

$r_{p+1,0}(r_{1,1}(x \bmod p^2) = (p+1)(x+1) \bmod p^2 = px+x+p+1 \bmod p^2$

$r_{p+1,0}(x \bmod p^2) = (p+1)x \bmod p^2$

$r_{p+1,0}(r_{1,1}(x \bmod p^2) = (p+1)x+1 \bmod p^2 = px+x+1 \bmod p^2$

We zien $r_{p+1,0}(r_{1,1}(x \bmod p^2)) \neq r_{1,1}(r_{p+1,0}(x \bmod p^2))$

want $p \neq 0 \bmod p^2$,

Dus G is niet commutatief.

opg 4 G, H groepen

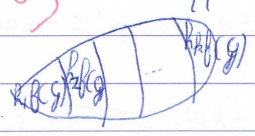
$f: G \to H$ en $g: H \to G$ homomorfismen.

Bewijs dat als zowel de index van $f(G)$ in H als ook de index van $g(H)$ in G eindig zijn, dan volgt dat de index van $g(f(G))$ in G ook eindig is.

Bewijs: We weten $f(G)$ in H heeft eindige index in H,

dus er zijn $h_1, \dots, h_k$ zodat $H = \bigcup_{i=1}^{k} h_i f(G)$ en ~~alle $h_i f(G)$~~

en alle $h_i f(G) \cap h_j f(G) = \emptyset \ \forall i,j, i \neq j$



$g(f(G))$ is een samenstelling van homomorfismes, dus is ook weer een homomorfisme, dus $g(f(G))$ is een ondergroep van G

Ook zijn er $g_1, \dots, g_l$ zodat $G = \bigcup_{j=1}^{l} g_j g(H)$

Neem $x \in G$, dan geldt dus $x = g_j \cdot g(h)$ voor bepaalde $j \in \{1, \dots, l\}$ en $h \in H$, $g_j \in G$
Maar ook $g(h) \in H$ en dus $h = h_i \cdot f(y)$ voor bepaalde $i \in \{1, \dots, k\}$ $y \in G$, $h_i \in H$

en dus $x = g_j \cdot g(h) = g_j \cdot g(h_i \cdot f(y)) = g_j \cdot g(h_i) \cdot g(f(y))$

Dus $x \in g_j \cdot g(h_i) \cdot g(f(G))$ voor willekeurige $x \in G$
zijn en dus $g_j \in G$ en $h_i \in H$
zodat $x \in g_j \cdot g(h_i) \cdot g(f(G))$

Dus $g(f(G))$ heeft eindige index in G $\square$

opg 5) $H \leq$ wordt voortgebracht door $(2,0,2), (6,6,6), (8,36,38)$

$A = \begin{pmatrix} 2 & 6 & 8 \\ 0 & 6 & 36 \\ 2 & 6 & 38 \end{pmatrix}$ Nu "vegen"

5

$A \overset{3^e Rij - 1^e Rij}{\sim} \begin{pmatrix} 2 & 6 & 8 \\ 0 & 6 & 36 \\ 0 & 0 & 30 \end{pmatrix} \overset{\substack{3^e kolom \\ -3\times 1^e kolom \\ 3^e kolom \\ -4\times 1^e kolom}}{\sim} \begin{pmatrix} 2 & 0 & 80 \\ 0 & 6 & 36 \\ 0 & 0 & 30 \end{pmatrix} \overset{\substack{3^e kolom \\ -6\times 2^e kolom}}{\sim} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 30 \end{pmatrix}$

Dus de elementaire delers van H zijn $2, 6, 30$
Dus $\mathbb{Z}^3/H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$

in $\mathbb{Z}/2\mathbb{Z}$ komen de ordes 1 en 2 voor
in $\mathbb{Z}/6\mathbb{Z}$ komen de ordes 1, 2, 3, 6 voor
In $\mathbb{Z}/30\mathbb{Z}$ kunnen voorkomen ordes 1, 2, 3, 5, 6, 10, 15, 30 (de delers van 30)

$ORD(0) = 1$ alle ordes komen voor
$ORD(1) = 30$
$ORD(2) = 15$
$ORD(3) = 10$
$ORD(5) = 6$
$ORD(6) = 5$
$ORD(10) = 3$
$ORD(15) = 2$

4

Voor $\bar{a} \in \mathbb{Z}/2\mathbb{Z}$, $\bar{b} \in \mathbb{Z}/6\mathbb{Z}$, $\bar{c} \in \mathbb{Z}/30\mathbb{Z}$
geldt $ORD(\bar{a}, \bar{b}, \bar{c}) = kgV(ORD(a), ORD(b), ORD(c))$
maar de ordes van de elementen van $\mathbb{Z}/2\mathbb{Z}$ en $\mathbb{Z}/6\mathbb{Z}$
komen ook voor in de ordes van elementen van $\mathbb{Z}/30\mathbb{Z}$.
Dus $kgV(ORD(a), ORD(b), ORD(c)) \leq 30$

Dus de ordes die voorkomen zijn de ordes van $\mathbb{Z}/30\mathbb{Z}$