Groepen theorie

Luc Veldhuis

23 Mei 2017

Conjungatieklasse

G een groep. G werkt op $A = G$ door middel van conjungatie: $g \cdot a = gag^{-1}$ $(g \in G,\ a \in A)$
De baan van $a = \{gag^{-1} | g \in G\}$ heet de **conjungatieklasse** van a in G.
De stabilisator van a is $C_G(a) = \{gag^{-1} | g \in G\} \Leftrightarrow$ $\{ga = ag | g \in G\}$
Dus als G eindig is geldt: $|G| = |C_G(a)| \cdot |\text{conjungatieklasse van } a|$
en daarom $|\text{conjungatieklasse van } a| = \frac{|G|}{|C_G(a)|} = |G : C_G(a)|$

Voorbeeld

- $|\text{conjungatieklasse van } a| = 1 \Leftrightarrow gag^{-1} = a$ voor alle $g \in G$ $\Leftrightarrow ga = ag\ \forall g \in G \Leftrightarrow a \in Z(G)$
- In D_8 heeft s als conjungatieklasse $\{s, sr^2\}$ en $C_{D_8}(s) = \{e, r^2, s, sr^2\}$ (ga na).

§4.3 Groepswerkingen

Stelling (klassenformule)

Als G een eindige groep is, $g_1, \ldots, g_r$ representanten van de conjungatieklassen in G met meer dan 1 element, dan

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G \ C_G(g_i)|$$

met $GC_G(g_i)$ de conjungatieklassen van g_i met meer dan 1 element.

Voorbeeld

$G = S_3$, 3 conjungatieklassen: $\{e\}, \{\text{2-cykels}\}, \{\text{3-cykels}\}$.
Dan zegt de formule: $3! = 1 + (2 + 3)$, want $|Z(S_3)| = 1$, en er zijn 3 2-cykels en 2 3-cykels.

§4.3 Groepswerkingen

Stelling

Als p een priemgetal is en G een groep met $|G| = p^a$ met $a \geq 1$ ('G is een p-groep') dan geldt dat $Z(G) \neq \{e\}$ (niet triviaal.)

Bewijs

In de klassenformule is elke $|G : C_G(g_i)|$ een positieve deler van $|G| = p^a$, groter dan 1. $\Rightarrow$ elke $|G : C_G(g_i)|$ is $p, p^2, \ldots,$ want p is priem.
p deelt $|G| = p^a$ met $a \geq 1$. Uit de klassenformule volgt $p||Z(G)|$ $\square$

Gevolg

Als $|G| = p^2$ met p priem, dan is G isomorf met $\mathbb{Z}/p^2\mathbb{Z}$ of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

§4.3 Groepswerkingen

Bewijs

Als $|G|$ een element van orde p^2 heeft dan is G cyklisch en dus isomorf met $\mathbb{Z}/p^2\mathbb{Z}$
Als G niet zo'n element bevat, dan heeft elk element $\neq e$ in G orde p (Lagrange).
Kies $e \neq x \in Z(G)$, dat kan, want G is een p-groep, dus x heeft orde p.
Kies $y \in G$, $y \notin \langle x \rangle$ en $|\langle x \rangle| = p$.
Dan is $G = \langle x, y \rangle$ (Lagrange) en $G = \{x^i y^j | i, j \in \mathbb{Z}\}$ want $x \in Z(G)$ dus commuteert met alles.
Dan is $\phi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ met $\phi(\bar{a}, \bar{b}) \mapsto x^a y^b$ en welgedefinieerd, surjectief, homomorfisme (want $xy = yx$) (ga na)
Bijde zijden p^2 elementen, dus ϕ is ook injectief $\Rightarrow \phi$ is bijectief, dus er is een isomorfisme tussen $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong G$

§4.3 Groepswerkingen

Gevolg van klassenformule: Stelling van Cauchy

Als G een eindige groep is, p priemdeler van de orde van G, dan bevat G een element van orde p.

Voorbeeld

Groepen van orde 6. Zo'n groep bevat x van orde 2 en y van orde 3 (Cauchy), dan $\langle x, y\rangle = G$, volgens Lagrange, want $\langle x\rangle \leqslant \langle x, y\rangle$ en $\langle y\rangle \leqslant \langle x, y\rangle$. Ook $|G : \langle y\rangle| = \frac{|G|}{|\langle y\rangle|} = \frac{6}{3} = 2$, dus $\langle y\rangle$ is een normaaldeler van G.
$\langle y\rangle = \{e, y, y^2\}$. Daarom is $e \neq xyx^{-1} \in \langle y\rangle$. Dus $xyx^{-1} = y$ of $xyx^{-1} = y^2 = y^{-1}$
Uit de eerste oplossing volgt $xy = yx$ met $|xy| = 6$ (Ga na) en $G \cong \mathbb{Z}/6\mathbb{Z}$
Dan is G isomorf met D_6 volgens: $x \mapsto s$, $y \mapsto r$ (Ga na)

Mogelijke isomorfismes

Dus: groepen van orde ≤ 10:

Orde	Isomorf met
1	$\{e\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$ of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$ of $D_6 \cong S_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$ of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ of $(\mathbb{Z}/2\mathbb{Z})^3$ of D_8 of Q
9	$\mathbb{Z}/9\mathbb{Z}$ of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	$\mathbb{Z}/10\mathbb{Z}$ of D_{10}

Bewijs

- G is abels. Doe inductie naar $|G|$. $|G| = p$: al gezien: elk element $x \neq e$ heeft orde p.
  Als $|G| > p$, neem $y \in G$, $y \neq e$. Als $m = |y|$ en $p|m$ dan heeft $y^{\frac{m}{p}}$ orde p.
  Als $p \nmid m$ dan deelt p de orde van $G/\langle y \rangle$ (Dat is $\frac{|G|}{m}$)
  Volgens inductie aanname heeft $G/\langle y \rangle$ een element z van orde p.
  Dan deelt p de orde van z want $|\langle z \rangle| = |\bar{z}| \cdot |\langle y \rangle \cap \langle z \rangle|$. Dan heeft $z^{\frac{|z|}{p}}$ orde p.

Bewijs

- G is niet abels. Doe weer inductie naar de orde van G. Dan geeft de klassenformule:
  $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$ met $|G|$ deelbaar door p.
  Als $p||Z(G)|$ dan heeft $Z(G)$ een element van orde p volgens 1, want $Z(G)$ is abels.
  Als $p \nmid |Z(G)|$ dan is er een g_i met $p \nmid |G : C_G(g_i)| = \frac{|G|}{|C_G(g_i)|}$.
  Omdat $p||G|$ geldt $p||C_G(g_i)|$. Die groep is kleiner dan $|G|$, dus volgens inductie bevat de een element van orde p.

$\square$

Herhaling

y orde m, $n \in \mathbb{Z}$, orde(y^n)= $\frac{m}{ggd(n,m)}$

Stelling

De enige normaaldelers van A_5 zijn $\{e\}$ en A_5.
Gevolg: de enige normaaldelers van A_n zijn $\{e\}$ en A_n.

Bewijs

Een normaaldeler is een ondergroep de bestaat uit conjungatieklassen.
Conjungatieklassen in A_5:
$e = 1$, 3-cykels $= \binom{5}{3}\frac{3!}{3} = 20$, 5-cykels $= \binom{5}{5}\frac{5!}{5}$, 2-2-cykels $= \binom{5}{3}\binom{3}{2}\frac{1}{2!} = 15$, dus $|A_5| = 60$
Neem σ een 3-cykel: $|C_{S_5}(\sigma)| = \frac{|S_5|}{|\text{3-cykels}|} = \frac{120}{20} = 6$ elementen en $C_{S_5}(\sigma) = \langle(1\ 2\ 3),(4\ 5)\rangle$
$C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$. |Conjungatieklasse in $A_5| = \frac{|A_5|}{|C_{A_5}(\sigma)|} = \frac{60}{3} = 20$, dus $C_{A_5}(\sigma) = \langle(1\ 2\ 3)\rangle$
A_5 heeft 5 conjungatieklassen met groottes $1, 20, 12, 12, 15$.
De orde van de normaaldeler van A_5 moet $|A_5| = \frac{5!}{2} = 60$ delen. (Lagrange), maar heeft ook orde $k1 + k20 + k12 + k12 + k15$ met $k \in \{0, 1\}$. Na wat proberen: dit kan alleen als dat 1 of 60 is. Dus als de normaaldeler $\{e\}$ of A_5 is. Dus $[A_5, A_5] = A_5$

Voorbeeld

$[S_2, S_2] = A_2 = \{e\}$, $[S_3, S_3] = A_3$ en $[A_3, A_3] = \{e\}$,
$[S_4, S_4] = A_4$,
$[A_4, A_4] = V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
$[S_n, S_n] = A_n$ voor $n \leq 5$ en $[A_n, A_n] \leqslant A_n$ voor $n \geq 5$.