Isomorfier

Ex: Gruppen av symmetrier hos en liksidig triangel har tabellen

$\circ$	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

$$r \cdot s = r r^2 = r^3$$

S_3

$\circ$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

$(123)(12)$ $\qquad$ $(123)*(123)$

$x^2 =$
$= x * x$

$\mathbb{Z}$

$2^2 = 2*2 = 2+2$

$\alpha(i) = id$, $\alpha(r) = (123)$, $\alpha(s) = (132)$

$\alpha(x) = (12)$ $\qquad rx = y \qquad \alpha(y) = \alpha(r)\alpha(x)$

$= (123)(12) = (13)$

$\boxed{\alpha(gh) = \alpha(g)\alpha(h)}$

$\alpha(z) = \alpha(ry) = (123)(13) = (23)(1)$

Kolla övriga produkter.

Omflyttning av raderna

$\circ$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)

Omflytta sedan kolumnerna.

Cykliska grupper

Ex: I U_7 säg vi att

$\{3, 3^2 = 9 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}$

$= U_7$ U_7 genereras av 3 generator

En cyklisk grupp är en grupp som genereras av ett element på det här sättet

Ex: En cyklisk grupp kan vara oändlig

$G = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, \ldots\}$ Tex $(\mathbb{Z}, +) = (\{\ldots, -2, -1, 0, 1, 2, \ldots\}, +)$

$1^{-2} = 1^{-1} * 1^{-1} = (-1) * (-1) = (-1) + (-1) = -2$

Alla ändliga cykliska grupper av en fix ordning är isomorfa.
(isomorfism : generator $\to$ generator)
Den cykliska gruppen med n element betecknas C_n. (tex $C_n \cong (\mathbb{Z}_n, +)$)

isomorfa

$C_n = (1, x, x^2, x^3, \ldots, x^{n-1})$

Direkta produkter

Om A och B är två grupper så kan vi bilda en ny grupp $A \times B$ genom att förse mängden $A \times B$ med operationen $(a,b) * (c,d) = (ac, bd)$.

Vi verifierar att det blir en grupp:

$G1$: $(a,b), (c,d) \in A \times B \Rightarrow (a,b) * (c,d) \in A \times B$.

$G2$: OK, $G3$: $\underbrace{(e_A, e_B)}_{e_{A \times B}} * (c,d) = (c,d)$

$G4$: $(a,b)^{-1} = (a^{-1}, b^{-1})$

Ex: $C_2 \times C_3 \approx C_6$ men $C_2 \times C_4 \not\approx C_8$

Lösn: Låt $C_2 = \{1, x\}$, $C_3 = \{1, y, y^2\}$ då får vi $C_2 \times C_3 = \{(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2)\}$. Om vi tar potenser av elementet (x,y) (paret av generatorerna) får vi

(x,y), $(x,y)^2 = (x^2,y^2) = (1,y^2)$, $(x,y)^3 = (x^3,y^3) = (x,1)$

$(x,y)^4 = (x^4,y^4) = (1,y)$, $(x,y)^5 = (x^5,y^5) = (x,y^2)$

$(x,y)^6 = (x^6,y^6) = (1,1)$ (x,y) har ordning 6 och är därmed en generator och gruppen är cyklisk $\approx C_6$.

Låt $C_4 = \{1, z, z^2, z^3\}$

$(x, z)^2 = (1, z^2)$, $(x, z)^3 = (x, z^3)$

$(x, z)^4 = (1, 1)$ (x, z) har ordning 4.

$(x, z^2)^2 = (1, z^4) = (1, 1)$ (x, z^2) ordning 2

$(x, z^3)^2 = (1, z^2)$ $(x, z^3)^3 = (x, z^5) = (x, z)$

$(x, z^3)^4 = (1, 1)$ (x, z^3) har ordning 4

Alla elementen har ordning ≤ 4

$\Rightarrow$ gruppen $C_2 \times C_4$ är inte cyklisk

och därmed $C_2 \times C_4 \not\cong C_8$.

Sats: Om m, n relativt prima så är $C_m \times C_n \approx C_{mn}$.

bevis: Vi tar och räknar potenser av (x, y) (där x generator för C_m och y generator för C_n)

$(x, y)^s = (x^s, y^s)$ så om $(x, y)^s = (1, 1)$ måste $x^s = 1$ och $y^s = 1$. Men x har ordning m så $m | s$ och y har ordning n så $n | s$. Då $SGD(m, n) = 1 \Rightarrow mn | s$.

Å andra sidan är $(x, y)^{mn} = ((x^m)^n, (y^n)^m) = (1, 1)$.

$\Rightarrow (x, y)$ har ordning $m \cdot n$.

$C_4 = \{1, z, z^2, z^3\}$ $\qquad$ $\{1, z^2\}$

	1	z^2
1	1	z^2
z^2	z^2	1

$\approx C_2$

Delgrupper

En delmängd H till en grupp $(G, *)$ som uppfyller gruppaxiomen med $*$ kallas en delgrupp.

Ex: $\{id, (123), (132)\}$ är en delgrupp till S_3. C_3 är en delgrupp till C_6 eftersom $C_6 \approx C_2 \times C_3$ och

$C_3 \approx \{(1,1), (1,y), (1,y^2)\}$ $\quad$ $C_6 = \{1, z, z^2, z^3, z^4, z^5\}$

Sats: Om H är en delmängd till en grupp G som uppfyller villkoren

i) $x, y \in H \Rightarrow xy \in H$

ii) $x \in H \Rightarrow x^{-1} \in H$

då är H en delgrupp till G.

Speciellt om $|H| < \infty$ så räcker villkor i).

Bevis: i) $\Leftrightarrow$ G1, ii) $\Leftrightarrow$ G4. G2 följer automatiskt. G3 fås av $x^{-1}x = e$.

Om $|H| < \infty$ och $x \in H$ ser i) att alla potenser av x ligger i H, och den följden måste upprepa s.i.s.

Så $x^m = e$ för ngt m och

därmed $x \cdot x^{m-1} = e \Rightarrow x^{-1} = x^{m-1} \in H$.

Ex: Låt $Z(G) = \{h \in G;\ hg = gh$ för alla $g \in G\}$. T ex $e \in Z(G)$.

$Z(G)$ är en delgrupp.

Vi måste kolla att om $h_1, h_2 \in Z(G)$

så gäller att $h_1 h_2 \in Z(G)$.

$$h_1 h_2 g = h_1 g h_2 = g h_1 h_2 \Rightarrow h_1 h_2 \in Z(G).$$

ii) $h^{-1} \in Z(G)$ Vi vet att $hg = gh$

$$\Rightarrow hgh^{-1} = g \Rightarrow gh^{-1} = h^{-1}g.$$