ISOMORFIER

Exempel. Låt $G_1 = \mathbb{Z}_2 = \{[0],[1]\}$ med $\oplus$ och $G_2 = S_2 = \{(1),(1,2)\}$ med sammansätningen $\circ$. Grupptabellerna för G_1 och G_2 är följande

$\oplus$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$\circ$	(1)	(1,2)
(1)	(1)	(1,2)
(1,2)	(1,2)	(1)

Observera att om vi skriver (1) istället för [0] och (1,2) istället för [1] i första tabellen får vi den andra. Grupperna G_1 och G_2 är "lika" och det är bara deras element som betecknas på olika sätt. Betrakta avbildningen $\theta : \mathbb{Z}_2 \mapsto S_2$: $\theta([0]) = (1)$, $\theta([1]) = (1,2)$. Vi får att θ är en bijektion och

$$\theta([x] \oplus [y]) = \theta([x]) \circ \theta([y])$$

för godtyckliga $[x]$, $[y] \in \mathbb{Z}_2$.

Två grupper, G och H, är **isomorfa** om det finns en bijektion $\theta : G \mapsto H$, sådan att

$$\theta(a * b) = \theta(a) \# \theta(b), \text{ för alla } a, b \in G,$$

där $*$ är operationen i G och $\#$ är operationen i H.

Avbildningen θ kallas då en **isomorfi**, och vi skriver $G \approx H$.

Grupperna G_1 och G_2 från exemplet ovan är alltså isomorfa.

Exempel. Betrakta följande grupper: $(\mathbb{Z},+)$ och $(2\mathbb{Z},+)$. Definiera $\theta : \mathbb{Z} \mapsto 2\mathbb{Z}$ enligt $\theta(n) = 2n$ för varje $n \in \mathbb{Z}$. Klart att θ är bijektiv och $\theta(n+m) = 2(n+m) = 2n + 2m = \theta(n) + \theta(m)$ gäller för alla heltal m och n, dvs θ bevarar addition. Detta visar att θ är en isomorfi och $\mathbb{Z} \approx 2\mathbb{Z}$, fast $2\mathbb{Z} \subset \mathbb{Z}$.

Sats 18.1. Låt G vara en grupp med operation $*$, låt H vara en grupp med operation $\#$, och låt $\theta : G \mapsto H$ vara en avbildning sådan att $\theta(a * b) = \theta(a) \# \theta(b)$ för alla a, $b \in G$. Då

- **1.** $\theta(e_G) = e_H$
- **2.** $\theta(a^{-1}) = \theta(a)^{-1}$ för varje $a \in G$
- **3.** $\theta(a^k) = \theta(a)^k$ för varje $a \in G$
- **4.** $\theta(G)$, bilden av θ, är en delgrupp till H.
- **5.** Om θ är en-entydig så är $G \approx \theta(G)$

Satsen skall visas senare.

Sats 19.1. Antag att G och H är grupper och $G \approx H$. Då gäller

- $|G| = |H|$.
- G är abelsk $\Rightarrow$ H är abelsk.

- G är cyklisk $\Rightarrow H$ är cyklisk.
- G har en delgrupp av ordning $n \Rightarrow H$ har en delgrupp av ordning n.
- G har ett element av ordning $n \Rightarrow H$ har ett element av ordning n.

Exempel. **1.** $\mathbb{Z}_5$ och $\mathbb{Z}_6$ är inte isomorfa, ty $|\mathbb{Z}_5| = 5$ men $|\mathbb{Z}_6| = 6$.

2. $\mathbb{Z}_2 \times \mathbb{Z}_2$ och $\mathbb{Z}_4$ är inte isomorfa (**obs!** $|\mathbb{Z}_2 \times \mathbb{Z}_2| = |\mathbb{Z}_4| = 4$), ty varje element$\neq ([0],[0])$ i $\mathbb{Z}_2 \times \mathbb{Z}_2$ har ordning 2 (varför?), men $\mathbb{Z}_4$ har ett element av ordning 4, t ex $[1]$.

Sats 19.2. Varje cyklisk grupp av ordning n är isomorf med $\mathbb{Z}_n$. Dessutom, om G är en grupp av ordning p, där p är ett primtal, så är $G \approx \mathbb{Z}_p$.

Bevis. Om G är en cyklisk grupp av ordning n så finns det $a \in G$ sådant att $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$. Vi definierar $\theta : G \mapsto \mathbb{Z}_n$ genom $\theta(a^k) = [k]$, $k \in \mathbb{Z}$. Definitionen av denna funktion beror inte på heltalet k som definierar potensen: om $a^{k_1} = a^{k_2}$ så är $[k_1] = [k_2]$ ty $a^{k_1 - k_2} = e$ implicerar att $n|(k_1 - k_2)$ och därmed $[k_1] = [k_2]$. Man kontrollerar lätt att olika element a^k, a^m har olika bilder: $[k] = [m]$ betyder att $n|(k-m)$ vilket ger $a^{k-m} = e$ och $a^k = a^m$. Funktionen θ är en-entydig. Klart att den är surjektiv. Detta visar att θ är en bijektion. Vi har också att

$$\theta(a^k * a^l) = \theta(a^{k+l}) = [k+l] = [k] \oplus [l] = \theta(a^k) \oplus \theta(a^l).$$

Alltså är θ en isomorfi.

Om G är en grupp av ordning p, där p är ett primtal så är G cyklisk enligt en av följdsatserna till Lagranges sats vilket ger nu att $G \approx \mathbb{Z}_p$.

Fundamentala satsen om ändliga abelska grupper. Varje ändlig grupp G är isomorf med en direkt produkt av cykliska grupper av typen $\mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}}$, där p_i är primtal som kan vara lika. Direkta produkten är definierad entydigt av G om man bortser från faktorernas ordningsföljd.

Obs! Om G och H är grupper så är $G \times H \approx H \times G$

Exempel. Beskriv abelska grupper av ordning 100.

Vi har

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 5^2 = 2^2 \cdot 5^5.$$

Enligt satsen är varje abelsk grupp av ordning 100 isomorf med precis en av följande grupper:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5,\ \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^5},\ \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^5}.$$

Cayles sats. Varje ändlig grupp är isomorf med en permutations grupp.

Bevis. Multiplikationen till höger med ett element $a \in G$ ger en permutation, σ_a, av $G = \{a_1, a_2, \ldots, a_n\}$:

$$\sigma_a = \begin{pmatrix} a_1 & a_2 & \ldots a_n \\ a * a_1 & a * a_2 & \ldots a * a_n \end{pmatrix}$$

(Obs! alla $a * a_i$ är olika, ty $a * a_i = a * a_j$ ger $a_i = a_j$. Multiplikation med en produkt $a * b$ ger permutationen $\sigma_{a*b} = \sigma_a \circ \sigma_b$. Vi får alltså en avbildning $\theta : G \mapsto Sym(G)$: $\theta(a) = \sigma_a$ vilken uppfyller $\theta(a * b) = \theta(a) \circ \theta(b)$ för alla a, $b \in G$. Om $\theta(a) = \theta(b)$ så är $c * a = c * b$ för alla c, varav $a = b$. Låt H vara bilden av G. H är en delgrupp av $Sym(G)$ och $H \approx G$.

Följdsats. Varje grupp av ordning n är isomorf med en delgrupp av S_n.

Bevis. Man kan identifiera elementet a_i i G med talet i och ersätta $a * a_i = a_{p_i}$ med p_i för ett lämpligt index p_i. Då representerar vi σ_a med en permutation av talen $1, 2, \ldots, n$:

$$\sigma_a = \begin{pmatrix} 1 & 2 & \ldots n \\ p_1 & p_2 & \ldots p_n \end{pmatrix}$$
