LEKTION 04-28

Betrackta grupper $(\mathbb{Z}_6, +)$ och $(\mathbb{Z}_7^*, \cdot)$. de är två grupper med 6 element. Man kan rita upp grupptabellerna:(pg 24)

Då ser man att man kan bilda en bijektion: $\mathbb{Z}_6 \to \mathbb{Z}_7^*$ genom:

$$[0] \to [1], [1] \to [3], [2] \to [2], [3] \to [6], [4] \to [4], [5] \to [5]$$

Tabellen av värdelement ser ut precis som tabellen av $(\mathbb{Z}_6, +)$.

Vi sger att grupper r isomorfa.

Definition 0.1. Två grupper $(G_1, *), (G_2, \circ)$ är isomorfa om det finns en bijektion:

$$\phi : G_1 \to G_2$$

s att $\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$ för varje $g_1, g_2 \in G_1$

Exempel Låt $(G_1, *), (G_2, \circ)$ vara två isomorfa grupper, genom isomorfi ϕ.

- Låt $0 \in G_1$ vara det noll=elent i G_1 och $1 \in G_2$ vara det noll=elent i G_2. Visa att $\phi(0) = 1$

  Låt $g \in G_1$. Vi vet att:

  $$\phi(0 * g) = \phi(0) \circ \phi(g) \text{ och } \phi(0 * g) = \phi(g)$$

  Det följer att $\phi(0) \circ \phi(g) = \phi(g) = 1 \circ \phi(g)$ och

  $$(\phi(0) \circ \phi(g)) \circ \phi(g)^{-1} = (1 \circ \phi(g)) \circ \phi(g)^{-1}$$

  Enligd (G1)+(G2) har vi

  $$\phi(0) \circ (\phi(g) \circ \phi(g)^{-1}) = 1 \circ (\phi(g)) \circ \phi(g)^{-1})$$

  $$\phi(0) \circ 1 = \phi(0) = 1 \circ 1 = 1$$

- Låt $-g$ vara inverelement till $g \in G_1$ och h^{-1} vara inverelemnt av $h \in G_2$. Visa att $\phi(-g) = \phi(g)^{-1}$.

  Vi ska visa att $\phi(-g) \circ \phi(g) = 1$. Det är sant eftersom

  $$\phi(-g) \circ \phi(g) = \phi(g * (-g)) = \phi(0) = 1$$

Definition 0.2. En *ring* består av $(R, +, \cdot)$ där

- R är en mängd
- $+, \cdot$ är tvaa binära operationer så att:
  - $(R, +)$ äe en abelsk grupp.
  - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - $a \cdot (b + c) = a \cdot b + a \cdot c$ och $(b + c) \cdot a = b \cdot a + c \cdot a$.

Exempel

- $(\mathbb{Z}, +, \cdot)$ är en ring.
- $(\mathbb{Z}_n, +, \cdot)$ är en ring.

Definition 0.3. En *kropp* består av $(F, +, \cdot)$ där

- F är en mängd
- $+, \cdot$ är tvaa binära operationer så att:
  - $(F, +)$ äe en abelsk grupp. Låt 0 vara det nollelement.
  - $(F \setminus \{0\}, \cdot)$ är en abelsk grupp
  - $a \cdot (b + c) = a \cdot b + a \cdot c$ och $(b + c) \cdot a = b \cdot a + c \cdot a$.

Exempel För every primtal p är $(\mathbb{Z}_p, +, \cdot)$ en kropp.

Permutationer kan läsas i boken: pg 97-116.