Recap: 1) pt $\hat{x} \in \mathbb{Z}_m$

$\text{ord}(\hat{x}) = \frac{m}{\gcd(x,m)}$ → de câte ori adunăm $\hat{x} + \hat{x} + \dots \Rightarrow$ el neutru

2) pt $(g_1, g_2) \in G_1 \times G_2$

$\text{ord}(g_1, g_2) = \text{lcm}(\text{ord}(g_1), \text{ord}(g_2))$

Ex 1: Calc ord lui $(\hat{5}, \bar{3})$ în:

a) $(\mathbb{Z}_6, \mathbb{Z}_8, +)$

$\text{ord}(\hat{5}) = \frac{6}{\gcd(5,6)} = \frac{6}{1} = 6$ (în $\mathbb{Z}_6$)

$\text{ord}(\bar{3}) = \frac{8}{\gcd(8,3)} = \frac{8}{1} = 8$

$\Rightarrow \text{ord}(\hat{5}, \bar{3}) = \text{lcm}(\text{ord}(\hat{5}), \text{ord}(\bar{3})) = \text{lcm}(6,8) = 24$

b) $(\mathbb{Z}_{11}, \mathbb{Z}_9, +)$

$\text{ord}(\hat{5}) = \frac{11}{\gcd(11,5)} = 11$

$\text{ord}(\bar{9}) = \frac{9}{\gcd(9,9)} = \frac{9}{3} = 3$

$\Rightarrow \text{ord}(\hat{5}, \bar{3}) = \text{lcm}(11,3) = 33$

2) Det elem de ord 4 din $(\mathbb{Z}_{12}, \mathbb{Z}_{14}, +)$

(x, y)

$\text{ord}(x,y) = 4$

$\text{ord}(x) = \frac{12}{\gcd(x,12)}$

$\text{ord}(y) = \frac{14}{\gcd(y,14)}$

$\text{ord}(x) \in D_{12} = \{1, 2, 3, 4, 6, 12\}$

$\text{ord}(y) \in D_{14} = \{1, 2, 7, 14\}$

$\text{ord}(x) = 4, \text{ord}(y) = \{1, 2\}$

$\text{ord}(x) = 4 \Rightarrow \frac{12}{\gcd(12,x)} = 4 \Rightarrow \gcd(12,x) = 3 \Rightarrow x \in \{\hat{3}, \hat{9}\}$

1) $\text{ord}(y) = 1 \Rightarrow \frac{14}{\gcd(14,y)} = 1 \Rightarrow \gcd(14,y) = 14 \Rightarrow y = \{\bar{0}\}$ $\Rightarrow$

2) $\text{ord}(y) = 2 \Rightarrow \frac{14}{\gcd(14,y)} = 2 \Rightarrow \gcd(14,y) = 7 \Rightarrow y = \bar{7}$

$\Rightarrow (\hat{3}, \bar{0}), (\hat{9}, \bar{0}), (\hat{3}, \bar{7}), (\hat{9}, \bar{7})$

Recap: $R: G_1 \to G_2$ morf dacă:

1) $R(G_1) = G_2$

2) $R(g_1 + g_2) = R(g_1) + R(g_2)$

- $\ker R = \{x \in G_1 \mid R(x) = 0\}$

$\{y \in G_2 \mid R(x) = y\}$ pt $x \in G_1$

· $\mathrm{Im} f = 2\mathbb{Y}$ ...

3. Construiți morf de grup:

a) de la $\mathbb{Z}$ la $\mathbb{Z}_3$

1) $f(0) = \hat{0}$

dc $f(1) = \hat{0} \Rightarrow f(k) = f(\underbrace{1+1+\dots+1}_{k \text{ ori}}) = \underbrace{f(1)+f(1)+\dots+f(1)}_{de\ k\ ori} = \hat{0}, \forall k \in \mathbb{Z}$

dc $f(1) = \hat{1} \Rightarrow f(k) = \hat{k}$ / 3 morfisme

dc $f(1) = \hat{2} \Rightarrow f(k) = \hat{2k}$

$\mathbb{Z} \to \mathbb{Z}_3$

1) $f(x) = \hat{0}$

2) $f(k) = \hat{k}$

3) $f(k) = \hat{2k}$

b) de la $\mathbb{Z}_3$ la $\mathbb{Z}$

$f(\hat{0}) = 0$

dc $f(\hat{1}) = a \in \mathbb{Z}$

$f(\hat{1}+\hat{1}+\hat{1}) = f(\hat{0}) = 0$
$3 \cdot f(\hat{1}) = 3a$ $\Big\} \Rightarrow a = 0 \Rightarrow$ 1 morfism

$\mathbb{Z}_3 \to \mathbb{Z}$

1) $f(\hat{x}) = 0$

c) de la $\mathbb{Z}_3$ la $\mathbb{Z}_6$

$f(\hat{0}) = \bar{0}$

dc $f(\hat{1}) = a \in \mathbb{Z}_6$

$f(\hat{1}+\hat{1}+\hat{1}) = f(\hat{0}) = \hat{0}$
$= \overline{3 f(\hat{1})} = \overline{3a}$ / $\Rightarrow \overline{3a} = \bar{0}$ in $\mathbb{Z}_6$
$\hookrightarrow a = \bar{2}, \bar{0}, \bar{4}$

$f(\hat{2})$ poate fi $\bar{0}, \bar{4}, \bar{2}$

$\mathbb{Z}_3 \to \mathbb{Z}_6$:

1) $f(\hat{x}) = \bar{0}$

2) $\hat{0} \to \bar{0}$
$\hat{1} \to \bar{2}$
$\hat{2} \to \bar{4}$

3) $\hat{0} \to \bar{0}$
$\hat{1} \to \bar{4}$
$\hat{2} \to \bar{2}$

4) Det imag + ker pt morf de la la ex 3

a) $\mathbb{Z} \to \mathbb{Z}_3$

(1) $R(x) = \hat{0} \to \operatorname{Im} R = \{\hat{0}\}$

$\operatorname{Ker} R = \mathbb{Z}$

elem din $\mathbb{Z}$ care prin fct dau $\hat{0}$

2) $R(x) = \hat{x} \to \operatorname{Im} R = \mathbb{Z}_3$, $\operatorname{Ker} R = \{3a \mid a \in \mathbb{Z}\}$

3) $R(x) = \hat{2x} \to \operatorname{Im} R = \mathbb{Z}_3$, $\operatorname{Ker} R = \{3a \mid a \in \mathbb{Z}\}$

b) $\mathbb{Z}_3 \to \mathbb{Z}$

1) $R(\hat{x}) = 0 \to \operatorname{Im} R = \{0\}$, $\operatorname{Ker} R = ??$

c) $\mathbb{Z}_3 \to \mathbb{Z}_6$

(1) $R(\hat{x}) = \bar{0} \to \operatorname{Im} R = \{0\}$, $\operatorname{Ker} R = \mathbb{Z}_3$

(2) $\operatorname{Im} R = \{\bar{0}, \bar{2}, \bar{4}\}$, $\operatorname{Ker} R = \{\hat{0}\}$

(3) $\hat{1}$

Recap curs:

1) $\forall p$ prim, $\exists!$ (până la izo) un corp cu p^e elem, $e \in \mathbb{N}^*$

2) $K[X]/(R)$ - corp, dacă R - ireductibil în $K[X]$

$\mathbb{Z}_p$ = corp dc p = prim

5. Construim un corp cu: a) 4 elem

$K[X]$ - inele de pol e un corp

K = corp

$4 = 2^2$ → Caut poli în $\mathbb{Z}_2[X]$ de grad 2 ireductibil

$\to x^2 + x + \hat{1}$

$\mathbb{Z}_2[X]/(x^2+x+\hat{1})$ - „resturile" pot fi $\hat{0}, \hat{1}, x, x+\hat{1}$ cu grad < 2

b) 9 elem

$9 = 3^2$ → Caut poli în $\mathbb{Z}_3[X]$ de grad 2 ireductibili

$x^2 + \hat{1}$

$\mathbb{Z}_3[X]/(x^2+\hat{1})$

$\hat{0}, \hat{1}, \hat{2}$

$x, x+\hat{1}, x+\hat{2}$

$2x, 2x+\hat{1}, 2x+\hat{2}$