Th Teorema fundamentală de izomorfism pentru grupuri. $f: G_1 \to G_2$

Atunci $\frac{G_1}{\operatorname{Ker} f} \simeq \operatorname{Im} f$

$\operatorname{Im} f \leq G_2$ (demonstrat în cursul precedent)

$\operatorname{Ker} f = \{ x \in G_1 \mid f(x) = e_2 \}$ e_2 - el. neutru G_2

e_1 - el. neutru G_1

$\operatorname{Ker} f \trianglelefteq G_1$

Demonstrație TFIG

Fie $\varphi : \frac{G_1}{\operatorname{Ker} f} \to \operatorname{Im} f$ prin formula $\varphi(\hat{g}) = f(g)$

Trebuie să demonstrăm că φ bine definită, morfism de grupuri, funcție bijectivă

• ~~$f: G_1 \to G_2$ morfism de grupuri~~

$\hat{g}_1 = \hat{g}_2 \overset{?}{\Rightarrow} \varphi(\hat{g}_1) = \varphi(\hat{g}_2)$

$\hat{g}_1 = h \cdot g_2$

$h \in \operatorname{Ker} f \Rightarrow f(h) = e$

$\varphi(g_1) = f(g_1) = f(h \cdot g_2) = f(h) * f(g_2) \Leftrightarrow$

$\Leftrightarrow \varphi(g_1) = f(g_2) = f(g_1) = \varphi(g_2)$ //

Scanned by CamScanner

$\left(\frac{G_1}{\ker f}, \perp\right)$

$\varphi(\hat{g}_1 \perp \hat{g}_2) =$

$\varphi\left(\hat{g}_1 \perp \hat{g}_2\right) = \varphi\left(\widehat{g_1 \perp g_2}\right) \overset{def}{=} f(g_1 \cdot g_2) = f(g_1) * f(g_2)$

$= \varphi(\hat{g}_1) * \varphi(\hat{g}_2)$ - deci este morfism

1. Funcția φ este surjectivă

Fie $x \in \operatorname{Im} f \Rightarrow x = f(g)$

Injectivitate

$\varphi(\hat{g}_1) = \varphi(\hat{g}_2) \Rightarrow \hat{g}_1 = \hat{g}_2$

$\varphi(\hat{g}_1 \perp \hat{g}_2^{-1}) = \varphi(\hat{g}_1) * \varphi(\hat{g}_2^{-1}) = \varphi(\hat{g}_1) * \cancel{\varphi(\hat{g}_1)}\ \varphi(g_2)^{-1}$

$= \varphi(\hat{g}_1) * \varphi(g_1)^{-1} = e_2$

$\varphi(g_1 \perp g_2^{-1}) = f(g_1 g_2^{-1})$ | $\Rightarrow f(g_1 g_2^{-1}) = e_2$

$\Rightarrow g_1 \cdot g_2^{-1} \in \ker f \Leftrightarrow g_1 = h g_2 \Leftrightarrow \hat{g}_1 = \hat{g}_2$

Atunci $\frac{G_1}{\ker f} \simeq \operatorname{Im} f$

Obs $(G_1, \cdot), (G_2, *)$ grupuri $f: G_1 \to G_2$ morfism de grupuri, sunt adevărate următoarele afirmații

a) f este injectivă

b) $\ker f = \{e\}$

$\Rightarrow$

$\left.\begin{array}{l} x \in \ker f \Rightarrow f(x) = e_2 \\ f \text{ este injectivă} \end{array}\right| \Rightarrow x = e_1$

$\Leftarrow$

$\ker f = \{e_1\}$

$g_1, g_2 \in G_1 \quad f(g_1) = f(g_2)$

$\cancel{f(g_1) = f(g_2^{-1})}$

$f(g_1 \cdot g_2^{-1}) = f(g_1) * f(g_2^{-1}) = f(g_1) * f(g_2)^{-1} =$

$= f(g_1) \cdot f(g_1)^{-1} = e_2 \Leftrightarrow g_1 \cdot g_2^{-1} = e_1 \Leftrightarrow g_1 = g_2 =$

$\Rightarrow f$ injectivă

Tema de vacanță: nume + primul prenume (n = nume, p = prenume)

1) Câte morfisme de grupuri $(\mathbb{Z}_n, +) \to (\mathbb{Z}_p, +)$

2) Este adevărat că $\mathbb{Z}_{np} \simeq \mathbb{Z}_n \times \mathbb{Z}_p$ justificați. $(+)$ $(+)$ $(+)$

3)

~~Aplicație~~ Teoremă

$(G,\cdot)$ grup ciclic $\Rightarrow$ $(G,\cdot) \simeq (\mathbb{Z},+)$ sau

$(G,\cdot) \simeq (\mathbb{Z}_n,+)$ pt $n \in \mathbb{N}^*$

Demonstrație

$G = \{h^n \mid n \in \mathbb{Z}\}$

$f: \mathbb{Z} \to G$, $f(n) = h^n$, $h \in G$

a) f este surjectivă, deoarece G este ciclic

b) f e ~~injectivă~~ morfism de grupuri

$f(m+n) = f(m) \cdot f(n) \Leftrightarrow$

$\Leftrightarrow h^{m+n} = h^m \cdot h^n \Rightarrow f$ este morfism de grupuri

TFIG $\quad \dfrac{\mathbb{Z}}{\operatorname{Ker} f} \simeq \operatorname{Im} f \simeq G$

Dacă $H \leq (\mathbb{Z},+)$ atunci $H = n\mathbb{Z}$ (demonstrată la seminar) $\Rightarrow$

$\Rightarrow \operatorname{Ker} f = n\mathbb{Z}$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \operatorname{Im} f$$

Dacă $n = 0 \Rightarrow \operatorname{Ker} f = \{0\} \Rightarrow f$ injectivă, f surjectivă $\Rightarrow G \simeq (\mathbb{Z},+)$

Dacă $n > 0 \Rightarrow \dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n$

Problema bonus

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Caesar shift

CER = UWJ

$C + 18 = 3 + 18 = 21$

$E + 18 =$

$R + 18 =$

REGE

$+17 + 4 + 6 + 4$

REPU | BLICA

+ + + + + + + + +

IVVY | SPOOR

$\hat{9} + \hat{17} = \hat{34} = \hat{8}$

$\hat{4} + \hat{4} = \hat{8}$

OUDYDQ | YIJOCA | XFCYKM | OOIHFM |

VTIY

lungime cuvânt = 6 (A beautiful mind)

$(G, \cdot)$ grup $|G| = p$ - prim

$G \simeq (\mathbb{Z}_p, +)$

Fie $x \in G - \{e\}$ ord$(x) = p$

ord$(x) \mid p \Rightarrow$

$x, x^2, x^3, \dots, x^{p-1}$

elemente distincte, dacă $ord(x) = p$

$x^i = x^j$

$1 \leq i < j \leq n$ $\Big| \Rightarrow x^{j-i} = e$

$ord(x) = p$ $\Big| \Rightarrow p \mid j-i \Rightarrow p = j-i$

$i \neq j$ (⇒)

$\Rightarrow$ contradicție $\Rightarrow x \neq x^2 \neq \dots \neq x^{p-1}$ (⇒) $G = \{x, x^2, \dots, x^{p-1}\}$

$g \in G \Rightarrow \exists\, i \in \{0, 1, \dots, p-1\}$ a.î. $g = x^i$

$f(g) = \hat{i}$, $f: (G, \cdot) \to (\mathbb{Z}_p, +)$

Exercițiu: funcția este izomorfism de grupuri.

<u>Seminar</u>

grup cu 4 elemente. $|G| = 4 \Rightarrow G \simeq \mathbb{Z}_4$

sau

$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

Într-un grup $(G, \cdot)$ $x, y \in G$ $(xy)^{-1} = y^{-1}x^{-1}$