Curs 1 + 2

Def $(G, \cdot, 1)$ grup $\Leftrightarrow$ $\begin{cases} (xy)z = x(yz) \\ \cancel{\exists y \forall z \quad zy = yz = z} \\ \cancel{\forall x \exists y \quad x} \\ \forall z \quad z1 = 1z = z \\ \forall x \exists y \quad xy = yx = 1 \end{cases}$

Obs A mulțime

$\{f : A \to A \mid f \text{ bijectivă}\} = S(A)$ grup!

$A = \{1, \dots n\} \Rightarrow$ grupul permutărilor de n elemente.

$S(A) = S_n$

$|S_n| = n!$

$$\boxed{\begin{array}{l} H \leq G \Rightarrow |H| \mid |G| \\ G = \bigcup_{b \in G} bH \text{, partiție!} \end{array}}$$

Th Cayley $\forall$ G grup, $G \leq S(G)$

Dem $\forall g \in G$, g se asociază cu

$f_g : G \to G$, $f_g(x) = gx$

> f bijectivă

> $f_1 = id$

> $f_g \circ f_h = f_{gh}$

> $f_{g_1} = f_{g_2} \Rightarrow g_1 = g_2$

Def $H \le G$ subgrup normal $\iff \forall x \in G$
$xHx^{-1} = G$

not $H \trianglelefteq G$

Def $h : G_1 \to G_2$ homomorfism $\iff$

$h(1) = 1$; $h(xy) = h(x)h(y)$

$\{x \mid h(x) = 1\} = \operatorname{Ker} h$

Prop $\operatorname{Ker} h \trianglelefteq G_1$ şi $G_1 / \operatorname{Ker} h \simeq \operatorname{Im} h \le G_2$

$\alpha \in \operatorname{Ker} h$

$h(x\alpha x^{-1}) = h(x) \underset{1}{\underset{\parallel}{h(\alpha)}} h(x)^{-1} = 1$

etc...

$A \subseteq G \Rightarrow \langle A \rangle = \bigcap\limits_{A \subseteq H < G} H$ subgrup generat de A

$a \in G$, $\langle a \rangle$ subgrupul generat de a. ; $\mathbb{Z} = \langle 1 \rangle$

a are ordin finit $\iff \langle a \rangle$ finit.

$\langle a \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ unde $n = \operatorname{ord} a$ = cel mai mic n a.î. $a^n = 1$

Obs G abelian $\iff xy = yx \ \forall x, y$

notaţie $(G, +, 0)$ alte exemple...

Obs $H \leq \mathbb{Z}/n\mathbb{Z} \Rightarrow H \simeq \mathbb{Z}/m\mathbb{Z}$
unde $m \mid n$.

$$\varepsilon : S_n \longrightarrow (\{+1, -1\}, \cdot)$$

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

homomorfism

$\operatorname{Ker} \varepsilon := A_n$, $|S_n / A_n| = 2$

> Orice permutare se scrie ca produs de transpoziții ($\leq n-1$)

> Orice permutare se scrie ca produs de cicluri disjuncte.

> $(k \ \ k+1) = (1\ 2 \ldots n)^{k-1} (1\ 2)(1\ 2 \ldots n)^{1-k}$

> $(i\ j) = (j-1\ \ j)(j-2\ \ j-1) \ldots (i+1\ \ i+2) \cdot (i\ \ i+1)(i+1\ \ i+2) \ldots (j-2\ \ j-1)(j-1\ \ j)$

unde $i < j$.

> $(a_1\, a_2 \ldots a_k) = (a_1 a_2)(a_2 a_3) \ldots (a_{k-1} a_k)$

Deci

> Transpozițiile $(K \quad K+1)$ generează S_n

> Cele două elemente $(1,2)$ și $(1,2,\dots n)$ generează S_n!

Inele

Def $(R, +, \cdot, 0, 1)$ inel $\Leftrightarrow$

$(R, +, 0)$ grup abelian

$(xy)z = x(yz)$

$x1 = 1x = x$

și $x(y+z) = xy + xz$ distributivitate.

$(y+z)x = yx + zx$

Exemplu $(\mathbb{Z}, +, \cdot, 0, 1)$

Def $I \subseteq R$ ideal $\Leftrightarrow$ $\forall a, b \in I \quad a+b \in I$

$\forall x \in R \quad a \in I \quad ax \in I$

Def $h: R_1 \to R_2$ homomorfism $\Leftrightarrow$ $h(a+b) = h(a) + h(b)$

$h(ab) = h(a) H(b)$

$h(1) = 1$

$Ker(h) = \{ x \in R_1 \mid h(x) = 0 \}$

<u>Prop</u> Ker h ideal în R_1, și

$$R_1 / \operatorname{Ker} h = \operatorname{Im} h \leq R_2 \text{ subinel.}$$

<u>Exemplu esențial</u>

$I \subseteq \mathbb{Z}$ ideal $\Rightarrow \exists\, n \in \mathbb{Z} \quad I = n\mathbb{Z}$

Luăm $n = \min \{ x \in I \mid x > 0 \} \ldots$

$n\mathbb{Z} + m\mathbb{Z} = \gcd(m,n)\,\mathbb{Z}$

$n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(m,n)\,\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ inel!

$R^{\times} = \{ x \in R \mid \exists\, y \in R \quad xy = 1 \}$

$x \in (\mathbb{Z}/n\mathbb{Z})^{\times} \iff \gcd(x,n) = 1$, relativ prime.

<u>Lema chineză</u> $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

izomorfism de inele!

Se arată ușor

$$\gcd(m,n) = 1 \Rightarrow \underset{\text{ca inele}}{\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n}$$

$$\mathbb{Z} \xrightarrow{p} \mathbb{Z}_n \times \mathbb{Z}_m$$

$$p(a) = (a \bmod n,\ a \bmod m)$$

$$\operatorname{Ker} p = mn\mathbb{Z} \Rightarrow \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \quad !$$

Def $\varphi : \mathbb{N} \to \mathbb{N}$ Indicatorul lui Euler.

$\varphi(0) = 0,\ \varphi(1) = 1$

$\varphi(n) = \# \{ k \mid k < n,\ \gcd(k, n) = 1 \} = |\mathbb{Z}_n^\times|$

Lema $\gcd(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

deoarece $\mathbb{Z}_{mn}^\times \simeq \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$

T $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Dem
$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

$$= p_1^{\alpha_1} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Teorema lui Euler

$a, n > 0$, $\gcd(a,n) = 1$ $\Big|$ $a^{\varphi(n)} \equiv 1 \mod n$

<u>Proof</u> $|\mathbb{Z}_n^\times| = \varphi(n)$, $a \in \mathbb{Z}_n^\times$, $\operatorname{ord}(a) \mid |\mathbb{Z}_n^\times|$

deoarece $\langle a \rangle \leq \mathbb{Z}_m$ și întotdeauna $H \leq G \Rightarrow |H| \mid |G|$

fiindca $G = \bigcup_{b \in G} bH$, reuniune de clase!

---

p prim, $p \nmid a \rightarrow a^{p-1} \equiv 1 \mod p$

<u>Obs</u> $\mathbb{Z}$ inel euclidian $\forall a, b\ \exists!\ r, q$ ~~$|r| < |b|$~~, $q > 0$, $0 \leq r < |b|$

$$a = bq + r$$

- De aceea idealele lui $\mathbb{Z}$ sunt generate de 1 element.

$$m\mathbb{Z} \subseteq \mathbb{Z}$$

- Algoritmul lui Euclid pt. calcularea lui $\gcd(a, b)$

<u>Obs</u> $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$

$a = 100$, $b = 17$

$$a = 100 = 5 \cdot \underline{17} + \underline{15}$$
$$\underline{17} = 1 \cdot \underline{15} + \underline{2}$$
$$\underline{15} = 7 \cdot \underline{2} + \underline{1}$$

$1 = \underline{15} - 7 \cdot \underline{2} = \underline{15} - 7(\underline{17} - \underline{15}) = 8 \cdot \underline{15} - 7 \cdot \underline{17} = 8 \cdot (-5) \cdot \underline{17} - 7 \cdot 1$

$1 = -47 \cdot 17 \mod 100$

$1 = 53 \cdot 17 \mod 100$

$\boxed{17^{-1} \mod 100 = 53}$

$$\begin{array}{r} 53 \cdot \\ 17 \\ \hline 371 \\ 53 \\ \hline 901 \end{array} = 1 \mod 100$$

$|\mathbb{Z}_{100}^{\times}| = \varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$= 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40,$

$\mathbb{Z}_{100}^{\times} = \mathbb{Z}_4^{\times} \times \mathbb{Z}_{25}^{\times} = \{1, 3\} \times \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12,$
$13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

$$\begin{array}{r} 18 \cdot \\ 7 \\ \hline 126 \end{array} \mod 25 = 1!$$

$17 = (17 \mod 4, 17 \mod 25) = (1, 17)$

$\cancel{7^{-1} = (3^{-1}, 7^{-1}) = (3, 18)}$

$\cancel{25 = 3 \cdot \underline{7} + \underline{4}}$ $\cancel{1 = \underline{4} - \underline{3} = \underline{4} - (\underline{7} - \underline{4}) = 2 \cdot \underline{4} - \underline{7} =}$

$\cancel{\underline{7} = 1 \cdot \underline{4} + \underline{3}}$ $\cancel{= 2 \cdot (-3) \cdot \underline{7} - \underline{7} = -7 \cdot 7 = 18 \cdot \underline{7}}$

$\cancel{\underline{4} = 1 \cdot \underline{3} + \underline{1}}$

$\cancel{x = 4k + 3 = 25l + 18}$ 43

$\cancel{10 \quad 38}$
$\cancel{17 \quad 45}$
$\cancel{24 \quad 52}$
$\cancel{31 \quad 59}$

$17^{-1} = \cancel{(1, 13)}\ (1, 3)$

$25 = 1 \cdot \underline{17} + \underline{8}$

$\underline{17} = 2 \cdot \underline{8} + \underline{1}$

$1 = \underline{17} - 2 \cdot \underline{8} = 17 - 2(-17) = 3 \cdot 17 = \cancel{[illegible]}$

$4k + 1 = 25l + 3 \Rightarrow 53$

Corpuri

$(K, +, \cdot, 0, 1)$ corp $\iff$ $(K, +, 0)$ grup abelian
~~$(K, \cdot, 1)$~~
$(K \setminus \{0\}, \cdot, 1)$ grup
+ distributiv în raport cu $\cdot$.

Exemple

$\mathbb{Q}$

$\mathbb{Z}/p\mathbb{Z}$; $\mathbb{Z}_p^\times = \{1, 2, \dots p-1\}$

> Wedderburn: orice corp finit este comutativ.

> Orice corp finit are caracteristică p, prim.

> Corpurile finite au p^k elemente, p prim (fiind sp. vectoriale $/\mathbb{Z}_p$)

> Două corpuri finite cu același nr de elemente sunt izomorfe.

> $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r} \iff s \mid r$

Exemplu $\mathbb{F}_4$

$X^2 + X + 1$ nu are soluții în $\mathbb{F}_2 = \mathbb{Z}_2$

Fie ω cu $\omega^2 + \omega + 1 = 0$. $\mathbb{F}_4 = \mathbb{F}_2[\omega] = \{0, 1, \omega, \omega+1\}$

$\omega^2 + 1 + \omega \cancel{+1} \cancel{+1} = 0$ O.K.

$\omega \cdot (\omega + 1) = \omega^2 + \omega = 1$

$1, \omega, \omega^2, \omega^3 = \omega(\omega+1) = 1$; $\mathbb{F}_4^\times \simeq \mathbb{Z}_3$ ciclic.

Teoremă K corp comutativ

G grup finit $\leq (K \setminus \{0\}, \cdot, 1)$

$\Rightarrow G$ ciclic

Dem. $|G| = n$. Vrem să arătăm că în G $\exists$ el. de ordin n

$n = p_1^{r_1} \cdots p_k^{r_k}$

$\forall i = 1 \ldots k \quad \exists x_i \in G \quad x_i^{\frac{n}{p_i}} \neq 1$

altfel polinomul $X^{\frac{n}{p_i}} - 1$ ar avea |soluții| > grad $\lightning$

$y_i = x_i^{\frac{n}{p_i^{r_i}}} \Rightarrow ord(y_i) = p^{r_i}$

$y_i^{p_i^{r_i}} = x_i^n = 1$. Dacă $ord\, y_i = p_i^s$ cu $s < r_i$ atunci

$y_i^{p_i^{r_i - 1}} = x^{\frac{n}{p_i}} = 1$ $\lightning$ $ord(y_i) = p_i^{r_i}$

$y = y_1 y_2 \cdots y_k$ ordinele sunt prime între ele $\Rightarrow ord(y) = n$!

$\langle y \rangle = G$ ciclic !

Exemplu $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$!

2, 4, 1, 2 ...

3, 2, 6, 4, 5, 1, 3

Caz particular de corp finit

$\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

xy sau $x \wedge y$ sau $\min(x, y)$

$\neg$	0	1
	1	0

$\vee$	0	1
0	0	1
1	1	1

$x \vee y$ sau $\max(x, y)$

<u>Teoremă</u> Orice funcția $f : \{0,1\}^k \longrightarrow \{0, 1\}$ se exprimă cu $\vee, \wedge, \neg$.

Dem

$$f = \bigvee_{\substack{(\varepsilon_1, \dots \varepsilon_n) \\ f(\varepsilon_1, \dots \varepsilon_n) = 1}} x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n}$$

unde $x_i^0 = \neg x_i$

$x_i^1 = x_i$

<u>Exemplu</u> $x + y = x^0 y^1 \vee x^1 y^0 = (x \wedge \neg y) \vee (\neg x \wedge y)$

<u>Obs</u> ~~xxy~~ $x \wedge y = \neg(\neg x \vee \neg y)$ deci $\neg$ și $\vee$ sunt suficiente.

Obs $x \mid y$ NAND, Sheffer Stroke

$\mid$	0	1
0	1	1
1	1	0

$$\neg x := (x \mid x)$$

$$x \vee y := (x \mid x) \mid (y \mid y)$$

Deci Sheffer Stroke generează termeni care reprezintă toate funcțiile.

Mai general

$\mathbb{F}$ corp finit, $|\mathbb{F}| = n \Rightarrow \forall f : \mathbb{F}^k \to \mathbb{F}$ e dată de un polinom.

Sol 1 Interpolarea. $\mathbb{F} = \{a_1, \dots a_n\}$

$$f(x_1, \dots x_k) = \sum_{\substack{\cancel{(a_1, \dots a_k)} \\ (\varepsilon_1, \dots \varepsilon_k)}} \frac{\prod_{a_i \neq \varepsilon_1} (x_1 - a_i)}{\prod_{a_i \neq \varepsilon_1} (\varepsilon_1 - a_i)} \frac{\prod (x_2 - a_i)}{\prod_{a_i \neq \varepsilon_2} (\varepsilon_2 - a_i)} \dots f(\varepsilon_1, \dots \varepsilon$$

Sol 2 $x^{n-1} = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$ când $|\mathbb{F}| = n$

$$f(x_1, \dots x_k) = \sum_{(\varepsilon_1, \dots \varepsilon_n)} \left(1 - (x_1 - \varepsilon_1)^{n-1}\right) \dots \left(1 - (x_n - \varepsilon_n)^{n-1}\right) f(\varepsilon_1, \dots \varepsilon$$