Alg. C11
pag 1

Algebră Curs 11.

Corpuri finite

1) K corp finit $\Rightarrow |K| = p^n$, p prim
2) $\forall$ p prim $\forall n \in \mathbb{N}^* \Rightarrow \exists$ un corp cu p^n elemente

Fără demonstrații: 3) K corp finit $\Rightarrow$ K comutativ
4) K, L corpuri finite, $|K| = |L|$. Atunci $K \simeq L$ (sunt izomorfe)

$K \subseteq L$ K, L corpuri K subcorp.
Există o structură de spațiu vectorial pentru L peste K.
$(L, +) \rightarrow$ grup comutativ.
$k \in K$, $v \in L$ $k \odot v = k \cdot v$ înmulțirea din corpul L.

$$\begin{cases} (k_1 + k_2) \cdot v = k_1 v + k_2 v \\ (k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v) \\ k_1 (v_1 + v_2) = k \cdot v_1 + k \cdot v_2 \\ 1_K \cdot v = v. \end{cases}$$

Demonstrație 1) $|K| = m$

$\underbrace{1+1+\ldots+1}_{de\ m\ ori} = 0$ (T. Lagrange)

Notație: ⊛ $k = \underbrace{1+1+\ldots+1}_{de\ k\ ori}$, 1 - el. neutru față de „·” în corpul K.

$m = p_1 \ldots p_r$ p_j prime nu neapărat distincte

$0 = 1+1+\ldots+1 = \underbrace{(1+1\ldots+1)}_{p_1\ ori} \underbrace{(1+1+\ldots+1)}_{p_2\ ori} \ldots \underbrace{(1+1+\ldots+1)}_{p_r\ ori} \Rightarrow \exists p_j$ a.î. $\overset{⊛}{p_j} = 0$

$\left.\begin{matrix} K \text{ corp}, x \cdot y = 0 \\ x, y \in K \end{matrix}\right\} \Rightarrow x = 0$ sau $y = 0$

Este posibil să existe primele p, q $p \neq q$ a.î. $\begin{matrix} p = 0 \\ q = 0 \end{matrix}$? $\rightarrow$ NU.

Presupunem că $\exists$ p, q prime, $p \neq q$ a.î. $p = q = 0$ în K. $\Rightarrow$
$\Rightarrow \exists x, y \in \mathbb{Z}$ a.î. $px + qy = 1 = (p, q)$ relație în $\mathbb{Z}$.
În K: $0 \cdot x + 0 \cdot y = 1_K \Rightarrow 0_K = 1_K$ ✗

Am demonstrat că există un unic nr. prim p a.î. $p = 0$ (în K)

Există un subcorp K_0 al lui K, $K_0 \simeq \mathbb{Z}_p$. $|K_0| = p$.

$K_0 = \{0, 1, 2, 3, \ldots, p-1\}$ folosind notația ⊛. $|K_0| = p$. $\begin{cases} 0 \leq i < j \leq p-1 \text{ (nr. nat.)} \\ i = j \text{ (în K)} \end{cases} \Rightarrow$

$\Rightarrow j - i = 0 \Rightarrow \exists q$ prim, $q \mid j-i$ a.î. $q = 0$ (în K) $\rightsquigarrow$ nu este posibil

$K_0 \xrightarrow{f} \mathbb{Z}_p$ $f(j) = \hat{j}$

Exercițiu: f izomorfism de ~~grupuri~~ corpuri $\Rightarrow$ $\begin{cases} f(j+k) = f(j) + f(k) \\ f(j \cdot k) = f(j) \cdot f(k) \\ f(1_K) = \hat{1} \end{cases}$ f bij $\Leftrightarrow$ f surj $\Leftrightarrow$ f inj.
$|K_0| = |\mathbb{Z}_p|$

Folosesc construcția de la începutul cursului: $\Rightarrow$ K este spațiu vectorial peste K_0.

Alg Can
pag2.

Consider $e_1, e_2, \ldots, e_m$ o bază pentru K peste K_0. $K_0 \simeq \mathbb{Z}_p$

$g: \underbrace{K_0 \times K_0 \times \ldots \times K_0}_{m \text{ ori}} \to K$ cu $g(x_1, x_2 \ldots x_m) = x_1 e_1 + x_2 e_2 + \ldots + x_m e_m$

g este bijectivă $\Rightarrow$ g surjectivă $e_1, \ldots, e_m$ este sistem de generatori
g injectivă $e_1, \ldots, e_m$ liniar independent peste K_0 $\Big\} \Rightarrow$

$\xRightarrow{g \text{ bij}} |K| = |\overbrace{K_0 \times K_0 \times \ldots \times K_0}^{\text{de } m \text{ ori}}| = |K_0|^m = p^m$

În $\mathbb{Z}_3$: $f(X) = X^2 + \bar{1} \in \mathbb{Z}_3[X]$ $\quad f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{2}$, $f(\bar{2}) = \bar{5} = \bar{2}$ $\quad f$ ireductibil în $\mathbb{Z}_3[X]$.

$\exists K$ corp comutativ, $\mathbb{Z}_3 \subseteq K$ a.î. f are 2 rădăcini în K notate $(\alpha, -\alpha)$ $\quad \alpha \notin \mathbb{Z}_3$

$L = \{\bar{a} + \bar{b}\alpha \mid \bar{a}, \bar{b} \in \mathbb{Z}_3\}$ corp cu 9 elemente.

$\bar{a} + \bar{b}\alpha = \bar{a_1} + \bar{b_1}\alpha$

Dacă $\bar{b} \neq \bar{b_1} \Rightarrow \alpha = \frac{\bar{a_1} - \bar{a}}{\bar{b} - \bar{b_1}} \in \mathbb{Z}_3$, dar $\alpha \notin \mathbb{Z}_3$.

Deci $\bar{b} = \bar{b_1} \Rightarrow \bar{a} = \bar{a_1}$

$(\bar{a} + \bar{b}\alpha) + (-\bar{a} - \bar{b}\alpha) = 0$

$a, b \in \{0, 1, 2\}$ nu ambele 0

$(\bar{a} + \bar{b}\alpha)(\bar{c} + \bar{d}\alpha) = \bar{1}$

$\begin{cases} \bar{a}\bar{c} - \bar{b}\bar{d} = \bar{1} \\ \bar{a}\bar{d} + \bar{b}\bar{c} = 0 \end{cases} \Leftrightarrow \begin{cases} \bar{a}\bar{c} - \bar{b}\bar{d} = \bar{1} \\ \bar{b}\bar{c} + \bar{a}\bar{d} = 1 \end{cases}$ Sistem cu necunoscutele c, d. Are sol. unică $\Leftrightarrow$ det sist. $\neq \bar{0}$

$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = \bar{a}^2 + \bar{b}^2 \neq \bar{0} \Rightarrow$ sist. are sol. $\Rightarrow$ fiecare element are invers.

$f(X) = X^{p^m} - X \in \mathbb{Z}_p \Rightarrow \exists L$ corp com. $\mathbb{Z}_p \subseteq L$ a.î. f are toate rădăcinile în L.

nr. rădăcini f este p^m (nu există rădăcină multiplă).

Presupun că $\exists \alpha \in L$ rădăcină multiplă pt. f. $f(\alpha) = 0 \Rightarrow f'(\alpha) = 0 = p^m \alpha^{p^m - 1} - \bar{1} = -\bar{1}$

$K = \{\alpha \in L \mid f(\alpha) = 0\}$ $\quad |K| = p^m$

$(K, +, \cdot)$ corp, $\quad \alpha, \beta \in K \Rightarrow \alpha \cdot \beta \in K$.

$\begin{cases} \alpha^{p^m} = \alpha \\ \beta^{p^m} = \beta \end{cases} (\cdot) \Rightarrow (\alpha \cdot \beta)^{p^m} = \alpha^{p^m} \cdot \beta^{p^m} = \alpha \cdot \beta \Rightarrow \alpha \cdot \beta \in K$.

$\alpha \in K$, $\alpha \neq 0 \Rightarrow \frac{1}{\alpha} \in K$. $\quad \left(\frac{1}{\alpha}\right)^{p^m} = \frac{1}{\alpha^{p^m}} = \frac{1}{\alpha} \Rightarrow \frac{1}{\alpha} \in K. \Rightarrow (K^*, \cdot)$ grup com.

$(K, +)$ grup comutativ. $\quad \boxed{(x+y)^p = x^p + y^p}$ $\quad (x+y)^{p^2} = (x^p + y^p)^p = x^{p^2} + y^{p^2}$

$\alpha, \beta \in K \Rightarrow \alpha + \beta \in K$

$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} = \alpha + \beta$

$(-\alpha)^{p^m} = (-1)^{p^m} \alpha^{p^m} = (-1)^{p^m} \cdot \alpha = -\alpha \in K$. p prim şi în $\mathbb{Z}_2$ $-\bar{1} = \bar{1}$

Alg CM
pag 3.

3) K corp finit $\Rightarrow$ K comutativ

4) $\left.\begin{matrix} K, L \text{ corpuri finite} \\ |K| = |L| \end{matrix}\right\} \Rightarrow K \simeq L$

$2^{2017} = 2017 q + r \qquad 0 \le r \le 2016$

K corp com finit $\Rightarrow (K^*, \cdot)$ grup ciclic $(\exists\, g \in K^*$ a.î. $\langle g \rangle = K^* = \{g^n \mid n \in \mathbb{N}\}$

K, g cunoscute $|K|$ „mare"

secret $\qquad g^b$

$A(a) \xleftarrow{\quad g^b \quad} B(b)$ secret

$A(a) \xrightarrow{\quad g^a \text{ (calculat în K)} \quad} B(b)$

$(g^b)^a$

$(g^a)^b$ cheia comună va fi g^{ab}.

$g^a = h$. Problema logaritmului. E greu să-l găsești rapid pe a. $a = \log_g h$.

Fie $\alpha \in K$, $f(\alpha) = 0 \qquad \alpha^4 = -\bar{1} \quad \alpha \neq 0 \quad \alpha^8 = \bar{1}$

$\alpha^4 + 1 = \bar{0}$

$\alpha^2 + \frac{\bar{1}}{\alpha^2} = \frac{\alpha^4 + 1}{\alpha^2} = \frac{\bar{0}}{\alpha^2} = \bar{0}$

$K \ni u = \alpha + \frac{1}{\alpha} \qquad u^2 = \alpha^2 + \frac{1}{\alpha^2} + \bar{2} = \bar{2}$

$u^p = \left(\alpha + \frac{1}{\alpha}\right)^p = \alpha^p + \frac{1}{\alpha^p}$

$p \overset{8}{\equiv} 1 \qquad u^p = \alpha^p + \frac{1}{\alpha^p} \qquad p = 8t + 1 \qquad u^{p-1} = 1 \qquad u \neq 0$

$\alpha^p = (\alpha^8)^t \cdot \alpha = \alpha$.

Dacă $u = 0 \Rightarrow \alpha = -\frac{1}{\alpha} \Rightarrow$
$\Rightarrow \alpha^2 = -1 \quad \alpha^4 = 1 = -1$ doar $\mathbb{Z}_2$
$\Rightarrow$
$\Rightarrow u \neq 0$