Dacă $g \in F^* \Rightarrow g$ inversabil $\Rightarrow V = F[X] \Rightarrow U = K$
$g \in V$

Dacă $h \in F^* \Rightarrow V = (f) \Rightarrow U = \{0_K\}$ contradicție

$\Rightarrow K$ este corp comutativ.

Propoziție
Fie $f \in F[X]$ un polinom ireductibil. Atunci $\varphi : F \longrightarrow F[X]/(f)$, $\varphi(a) = a + (f)$ este un morfism injectiv de corpuri.
Deci, φ induce o structură de F - spațiu vectorial pe $F[X]/(f)$
În plus, $\dim_F F[X]/(f) = \text{grad}(f)$

Obs În general, se identifică F cu un subcorp al lui $F[X]/(f)$

Def: Fie $f = a_n X^n + \dots + a_1 X + a_0 \in F[X]$
Spunem că $h \in F$ este rădăcină pt. f dacă $f(h) = a_n h^n + a_{n-1} h^{n-1} + \dots + a_1 h + a_0 = 0$

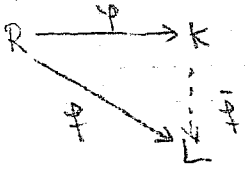
Teoremă
h este rădăcină pt. dacă $\exists\, f \in F[X]$ a.î. $f = (X-h) \cdot h$

CURS 12

29.05.2018

Elemente de teoria corpurilor XEROX → CURS

Teoremă (corpul fracțiilor unui domeniu de integritate)
Fie $(R, +, \cdot)$ un domeniu de integritate. Atunci, $\exists$ un corp K și un morfism unitar de inele $\varphi : R \to K$ a.î.:
a) φ este injectiv (adică putem identifica pe R cu un subinel a lui K)
b) Dacă L este corp și $f : R \to L$ este un morfism de inele unitar, atunci
$\exists!\, \bar{f} : K \to L$ morfism de corpuri a.î. $f = \bar{f} \circ \varphi$



Dem (schiță)
Fie $A = R \times R^* = \{(a,b) \mid a \in R, b \in R^*\}$
Pe A definim relația $\sim$ dată de
$(a,b) \sim (c,d) \iff a \cdot d = b \cdot c$
Se demonstrează că $\sim$ e o relație de echivalență pe A
(R) $(a,b) \sim (a,b) \iff a \cdot b = b \cdot a$ adevărat (pt. că înmulțirea e comutativă)
(T) $(a,b) \sim (c,d) \Rightarrow ad = bc \mid \cdot f \Rightarrow afd = bcf$
$(c,d) \sim (e,f) \Rightarrow cf = de \mid \cdot b \Rightarrow bcf = bed$
$\Rightarrow afd = bed$ ($d \neq 0$, R dom. de integritate) $\Rightarrow af = be \Rightarrow (a,b) \sim (e,f)$
(S) - temă
$K := A/\sim$ și notăm cu $\overline{(a,b)}$ clasa lui (a,b) în K
Definim operațiile $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,\ bd)}$
$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)}$
Se demonstrează că tripletul $(K,+,\cdot)$ este corp comutativ ($+$ și $\cdot$ sunt independente de alegerea reprezentanților)
$\varphi : R \to K$, $\varphi(a) = \overline{(a,1)}$

Def: K s.n. corpul fracțiilor asociat lui R

Def: Fie F un corp comutativ și $f \in F[X]$, $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$
Atunci funcția
$$\tilde{f}: F \to F, \quad \tilde{f}(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0$$ s.n. funcția polinomială asociată lui f.

Obs: Există situații când polinoamele diferite induc aceeași funcție polinomială
Exemplu:
$f, g \in \mathbb{Z}_2[X]$. $f(X) = X + \hat{1}$
$g(X) = X^3 + X^2 + X + \hat{1}$

α	$\hat{0}$	$\hat{1}$
$\tilde{f}(\alpha)$	$\hat{1}$	$\hat{0}$
$\tilde{g}(\alpha)$	$\hat{1}$	$\hat{0}$

$\Rightarrow \tilde{f} = \tilde{g}$, dar $f \neq g$

Def: Fie $f \in F[X]$. Spunem că $\alpha \in F$ e rădăcină pentru f dacă $\tilde{f}(\alpha) = 0$.
Exemplu
În exemplul anterior, $\alpha = \hat{1}$ e rădăcină pt. f și pt. g

Propoziție
Fie $f \in F[X]$ și $\alpha \in F$. Atunci α este rădăcină pt. $f \iff \exists\, g \in F[X]$ a.î. $f = (X-\alpha) \cdot g$.
($X - \alpha$ divide pe f)

Dem:
Teorema împărțirii cu rest: $\exists\, q, r \in F[X]$ a.î. $f = (X-\alpha) \cdot q + r$ și $\operatorname{grad}(r) < \operatorname{grad}(X-\alpha) = 1$

$\operatorname{grad}(r) < 1 \Rightarrow r \in F$
α rad. pt. $f \iff \tilde{f}(\alpha) = 0 \iff \underbrace{(\alpha-\alpha)}_{=0} \cdot q(\alpha) + r = 0 \iff r = 0$ ∎

Teorema
Fie $f \in F[X]$ un polinom de grad n. Atunci f are cel mult n rădăcini în F

Obs: Dacă $\operatorname{grad}(f) = n$ și f are n rădăcini (nu neapărat distincte) $\Rightarrow$
$\Rightarrow f = a_n (X - r_1) \cdot \dots \cdot (X - r_n)$, unde a_n - coeficientul lui X^n
$r_1, \dots, r_n$ - rădăcinile
- Există situații când polinoamele au mai puține rădăcini în F.

Exemplu:
a) $f = X^2 + 1 \in \mathbb{R}[X]$ nu are rădăcini în $\mathbb{R}$
b) $f = X^2 + X + \hat{1} \in \mathbb{Z}_2[X]$ nu are rădăcini în $\mathbb{Z}_2$

Ne interesează să extindem corpul la un corp în care polinomul dat să aibă n rădăcini

Def: Fie F un corp comutativ și $f \in F[X]$ un polinom de grad n. Spunem că un corp E e corpul de descompunere a lui f dacă:
a) $\exists\, \varphi: F \to E$ morfism de corpuri (injectiv)
și identificăm pe F cu $\varphi(F)$ (F devine subcorp în E)
b) polinomul f are n rădăcini în E
c) dacă L este un subcorp al lui E a.î. $F \subseteq L \subseteq E$ și f are n rădăcini în L, atunci $L = E$ (= cel mai mic corp în care găsim cele n rădăcini)

Teoremă
Orice polinom $f \in F[X]$ cu $\operatorname{grad}(f) \geq 1$ are un corp de descompunere.
Oricare două corpuri de descompunere asociate lui f sunt izomorfe.

Exemple

a) $f = X^2+1 \in \mathbb{R}[X]$

$\mathbb{C} = \mathbb{R}[X]/(f)$, $\widehat{X^2+1} = \hat{0}$ în $\mathbb{R}[X]/(f)$

$(f) = f \cdot \mathbb{R}[X]$ $\hat{X}^2 = -\hat{1}$ în $\mathbb{R}[X]/(f)$

$\widehat{X^3+2X^2+3X+4} = -\hat{X} - \hat{2} + 3\hat{X} + \hat{4} = 2\hat{X} + \hat{2}$ în $\mathbb{R}[X]/(f)$

($\hat{A}$ = clasa lui A în inelul factor)

$\Rightarrow \mathbb{C} = \{a\hat{i} + b\cdot\hat{i} \mid a,b \in \mathbb{R}\}$

Teoremă (teorema fundamentală a algebrei)

Orice polinom de grad $n \geq 1$ cu coeficienți complecși are n rădăcini complexe.

($\mathbb{C}$ este algebric închis)

Obs Un polinom $f \in F[X]$ cu $\text{grad}(f) \leq 3$ este ireductibil ($\Leftrightarrow$) el nu are rădăcini în F

$f = gh$ cu $\text{grad}(g) \geq 1$, $\text{grad}(h) \geq 1$, $\text{grad}(f) \leq 3$ $\Rightarrow \text{grad}(g) = 1$ sau $\text{grad}(h) = 1$

b) $f = X^3 + X + 1 \in \mathbb{Z}_2[X]$

f ireductibil $\Rightarrow E = \mathbb{Z}_2[X]/(f)$ este un corp (cu $2^3 = 8$ elemente)

Considerăm $\hat{f} = Y^3 + Y + 1 \in E[Y]$

Fie $e = X + (f) = \hat{X} \in E$, $E = \{aX^2 + bX + c + (f) \mid a,b,c \in \mathbb{Z}_2\}$

$\hat{f}(e) = [X+(f)]^3 + [X+(f)] + 1 = X^3 + X + 1 + (f) = f + (f) = 0$ în E

$\Rightarrow \hat{f}$ are rădăcini în E

$g = X^2 + X + (f)$

$g^2 = (X^2+X)^2 + (f) = X^4 + 2X^3 + X^2 + (f)$

$X^3 = -X - 1 \Rightarrow X^4 = -X^2 - X = X^2 + X$ (pt. că $2 = 0$ în $\mathbb{Z}_2$)

$\Rightarrow g^2 = X^2 + X + 2X + 2 + X^2 = X$

$g^3 = X^3 + X^2 + (f) = X^2 + X + 1 + (f)$

$\hat{f}(g) = X^2 + X + 1 + X^2 + X + 1 + (f) = (f)$

$\Rightarrow g$ este rădăcină ($2 = 0$)

Corpuri finite

Teoremă (Wedderburn)

Orice corp finit e comutativ

Dem: - folosește ecuația claselor de la grupuri și câteva proprietăți aritmetice ale rădăcinilor complexe de ordin n ale unității

Teoremă

Dacă F e un corp finit, atunci $\exists$ p-prim și $n \in \mathbb{N}^*$ a.î. $|F| = p^n$

Dem:

F domeniu de integritate $\Rightarrow$ caracteristica lui F este număr prim

$\Rightarrow \exists$ p-prim a.î. $\text{ord}_{(F,+)} \bar{1} = p$ (notăm cu $\bar{1}$ elementul neutru din F)

$K = \{\bar{0}, \bar{1}, \bar{2}, \ldots, (p-1)\cdot\bar{1}\}$ (înmulțirea cu scalari este

F - finit $\Rightarrow \dim_k F \in \mathbb{N}^* \Rightarrow \exists n \in \mathbb{N}^*$ a.î. $\dim_k F = n \Rightarrow$

$\Rightarrow |F| = |k|^n = p^n$

Teoremă

a) Dacă F este un corp finit, atunci $\exists\, p$ prim și $\exists\, \pi \in \mathbb{Z}_p[X]$ polinom ireductibil a.î. $F \simeq \mathbb{Z}_p[X]/(\pi)$, $|F| = p^{\text{grad}(\pi)}$

b) F este corpul de descompunere al polinomului $X^{p^n} - X$ peste $\mathbb{Z}_p[X]$, unde $p^n = |F|$

c) Orice două corpuri finite de același cardinal sunt izomorfe.

Exemple

1) Corpul de ordin $8 = 2^3$ ← grad π

$\pi = X^3 + X + 1 \in \mathbb{Z}_2[X]$ ireductibil

$F = \mathbb{Z}_2[X]/(\pi)$. Dacă $g \in \mathbb{Z}_2[X]$, notăm cu $\hat{g}$ clasa lui de echivalență în $\mathbb{Z}_2[X]/(\pi)$

$F = \{\hat{0}, \hat{1}, \hat{X}, \widehat{X+1}, \hat{X^2}, \widehat{X^2+1}, \widehat{X^2+X}, \widehat{X^2+X+1}\}$

$\left(\hat{X}^3 + \hat{X} + \hat{1} = 0 \Rightarrow \hat{X}^3 = \hat{X} + \hat{1}\right)$

$\widehat{X^2+1} \cdot \widehat{X^2+X+1} = \widehat{X^4+X^3+X^2+X^2+X+1} = \widehat{X^2+X+X+1+X+1} = \widehat{X^2+X}$

($X^4 + X^3 + X^2 + X^2 + X + 1 = 2X^2 = 0$; $X + 1 + X + 1 = 0$)

$\hat{X}^4 = \widehat{X^2+X}$

2) Corpul de ordin $27 = 3^3$

$\pi = X^3 + 2X^2 + 1 \in \mathbb{Z}_3[X]$

$F = \mathbb{Z}_3[X]/(\pi) = \{\widehat{aX^2+bX+c} \mid a, b, c \in \mathbb{Z}_3\}$

$\widehat{X^2+2X} \cdot \widehat{2X^2+X+1} = \widehat{2X^4+2X^3+2X^2+2X}$

$\hat{X}^3 = \widehat{-2X^2-1} = \widehat{X^2+2}$ (peste $\mathbb{Z}_3$, avem $-1 = 2$ și $-2 = 1$)

$2\hat{X}^3 = \widehat{2X^2+1}$

$2\hat{X}^4 = \widehat{2X^3+X} = \widehat{2X^2+X+1}$

$\Rightarrow \widehat{X^2+2X} \cdot \widehat{2X^2+X+1} = -\hat{1} = \hat{2}$

$\left(\widehat{X^2+2X}\right)^{-1} = \widehat{-2X^2-X-1} = \widehat{X^2+2X+2}$