6.04.2016.

ALGEBRĂ
SEMINAR 4

G grup.

$\frac{G}{H}$, H subgrup normal în G.

R. inel comutativ

Def: $I \trianglelefteq$ (I ideal al lui R)

1) $(I,+) \leq (R,+)$

2) $\left.\begin{array}{l}\forall\, i \in I \\ \forall\, r \in R\end{array}\right\} \Rightarrow r \cdot i \in I$

Exemplu R inel com.

$a \in R \Rightarrow aR \trianglelefteq R$.

$aR = \{ar \mid r \in R\}$

$(aR,+) \leq (R,+)$

$ar_1 + ar_2 = a(r_1+r_2)$

$ar + a\cdot(-r) = 0$.

$s\cdot(ar) = a(s\cdot r) \in aR$

$n \in \mathbb{N}$, $n \geq 2$.

$n\mathbb{Z} \trianglelefteq \mathbb{Z}$

$\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$

Construcția inelului factor

$I \trianglelefteq R$

$\frac{R}{I}$

$\boxed{\bar{r} = \bar{s} \text{ în } \frac{R}{I} \Leftrightarrow r - s \in I}$

Definim

$\bar{r} + \bar{s} \stackrel{def}{=} \overline{r+s}$

$\bar{r} \cdot \bar{s} \stackrel{def}{=} \overline{r \cdot s}$

$\left(\frac{R}{I}, +, \cdot\right)$ - inel comutativ

$r_1 + i_1 \quad \bar{r} = \overline{r_1}$

$s_1 + i_2 \quad \bar{s} = \overline{s_1}$

$i_{1,2} \in I$

$\Rightarrow \bar{r} + \bar{s} \stackrel{?}{=} \overline{r_1} + \overline{s_1}$

$\bar{r} \cdot \bar{s} \stackrel{?}{=} \overline{r_1} \cdot \overline{s_1}$

$(I, +) \leq (R, +)$

$$\begin{array}{ccc} \bar{r} + \bar{s} & = & \overline{r+s} \\ \| & & \| \\ \overline{r_1} + \overline{s_1} & = & \overline{r_1 + s_1} \end{array} \Rightarrow \cancel{r+s-(r_1+s_1) = (r-r_1)+(s-s_1)}$$

$\Rightarrow r + s - (r_1 + s_1) = i_2 \cdot i_2 \in I$

$(r - r_1) + (s - s_1) = i_1 + i_2 \in I$

$rs - r_1 s_1 = (r_1 + i_1)(s_1 + i_2) - r_1 s_1 = r_1 \cdot i_2 + i_1 s_1 + i_1 \cdot i_2 \in I.$

Corpuri finite (o să ne ajutăm de pag 0 și 1)

$R = \mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$

$I = 5\mathbb{Z}[i\sqrt{2}]$

$\frac{R}{I}$ - corp cu 25 elem.

inversul cât e.

$\overline{(1+i\sqrt{2})} \cdot \overline{(a+bi\sqrt{2})} = \overline{1} \mid \cdot \overline{(1-i\sqrt{2})}$

$\cancel{a + bi\sqrt{2} + ai\sqrt{2}}$

$\overline{3}\,\overline{(a+bi\sqrt{2})} = \overline{(1-i\sqrt{2})} \mid \cdot 2$ (pt că suntem în $\mathbb{Z}_5$)

$\overline{2}\cdot\overline{3} = \overline{1}$ $\qquad \overline{a+bi\sqrt{2}} = \overline{2-2i\sqrt{2}}$ — asta e inversul

---

$\overline{a+bi\sqrt{2}} = \overline{c+di\sqrt{2}} \Rightarrow \begin{cases} a = c \\ d = b \end{cases}$ $\quad x, y \in \mathbb{Z} \quad x = 5g + a \quad y = 5r + b$

$a, b \in \{0, 1, 2, 3, 4\}$ — a, b nu sunt simultan 0.

$\overline{x + yi\sqrt{2}} = \overline{a + bi\sqrt{2}}$

$x - a + (y-b)i\sqrt{2} = 5(g + ri\sqrt{2}) \in I$

$\Rightarrow \exists\, c, d \in \mathbb{Z}$ a.î. $\overline{(a+bi\sqrt{2})}\,\overline{(c+di\sqrt{2})} = \overline{1}$

$\overline{(a+bi\sqrt{2})}\cdot\overline{(c+di\sqrt{2})} = \overline{1} \mid \overline{(a-bi\sqrt{2})}$

$\overline{(a^2+2b^2)}\,\overline{(c+di\sqrt{2})} = \overline{(a-bi\sqrt{2})}$

nu se poate.

Dacă $a^2 + 2b^2 \equiv 0 \,(5)$

$a^2 \equiv -2b^2 \,(5) \mid ^2$ $\qquad$ p prim

$a^4 \equiv 4b^4 \,(5)$ $\qquad$ $a^{p-1} \overset{?}{\equiv} 0, 1$

$b \overset{5}{\equiv} 0 \Leftarrow 0 \overset{5}{\equiv} a^4 \overset{5}{\equiv} 0, 1$ (poate lua 2 val)

Dacă $a^4 \overset{5}{\equiv} 1$.

~~$4b^4 \overset{5}{\equiv} 1$~~

~~$b^4 \overset{5}{\equiv} 4$~~ nu se poate.

Deci putem împărți pt că $a^2+2b^2 \neq 0$ ✓

$$c \overset{5}{\equiv} \frac{a}{a^2+2b^2} \qquad d \overset{5}{\equiv} \frac{-b}{a^2+2b^2}.$$

ex anterior. $a = b = 1$

$$c \overset{5}{\equiv} \frac{1}{3} \equiv 2$$

$$d \overset{5}{\equiv} -\frac{1}{3} = -2.$$

$\overline{a+bi\sqrt{2}} = \overline{c+di\sqrt{2}}$ $\qquad I = 5\,\mathbb{Z}[i\sqrt{2}]$

$$a-c+(b-d)i\sqrt{2} = 5(x+yi\sqrt{2}) \qquad x,y \in \mathbb{Z}$$

$$a,c \in \{0,1,2,3,4\} \begin{cases} a-c = 5x & \Rightarrow a = c \\ b-d = 5y & \Rightarrow b = d \end{cases} \Rightarrow (a,b) = (c,d)$$

<u>Există corp</u> cu 15 elem ? NU.

<u>Presup</u> că $\exists$ K - corp $|K| = 15$.

$$n = \overbrace{1+1+\ldots+1}^{n \text{ ori}} \in K$$

1 elem neutru pt $(K^*, \cdot)$ $\qquad 0 \neq 1$.

0 —— " —— pt $(K, +)$

$15 = 0 \quad = 3 \cdot 5 \Rightarrow$ $3 = 0$ sau $5 = 0$ (dar nu simultan!)

$(G, \cdot)$

$g^{|G|} = e$ (el. neutru)

Caz I. $3=0$.

$\{0,1,2\}$ distincte în K

$(G,+) \leq (K,+)$

$x \in K \setminus G$ perechi diferite

$G_1 = \{a+bx \mid a,b \in \{0,1,2\}\}$

Pretindem $(G_1,+)$ grup cu $|G_1|=9$ elem.

$(3-a)+(3-b)x+a+bx=0$.

$a+bx=c+dx$.

Dacă $b \neq d$. $x = \frac{c-a}{b-d} \in \{0,1,2\}$ $\Big| \Rightarrow$ $b=d$, $a=c$

contradicție pt că $|G_1| \mid |K|$ $9/15$ Fals.

subgrupul lui K

Caz II.

$G_1 = \{a+bx \mid a,b \in \{0,1,2,3,4\}\}$.

$|G_1| = 25$.

și

$25 \mid 15$ ceea ce nu merge.

Dacă avem n - are cel puțin 2 diviz. primi distincți

$\Rightarrow \nexists$ corp cu n elem.

K corp finit. $\Rightarrow |K| = p^{\alpha}$
p prim.

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ $\quad p_1 < p_2 < \ldots < p_r$

$r \geq 2$.

$\alpha_j \in \mathbb{N}^* \ \forall j$ $\quad$ Pp. $\exists$ K corp $|K| = n$.

$n = \underbrace{1 + \ldots + 1}_{de\ n\ ori}$ $\quad p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} = 0 \Rightarrow \exists j$ a.î. $p_j = 0$

$p_i \neq p_j$ pt $i \neq j$.

Presup. că $p_1 = 0$.

$0, 1, 2 \ldots, p_1 - 1$ - diferite

$a, b \in \mathbb{Z}$ nu ambele 0
$\Rightarrow \exists\ c, d \in \mathbb{Z}$ a.î.
$ac + bd = (a, b)$

$i = j$ (în K) $0 \leq i < j \leq p - 2$

$\downarrow$ în $\mathbb{N}$

$1 \leq j - i \leq p - 1$

$(j - i, p) = 1$.

cel mai mare div com

$\Rightarrow \exists\ c, d \in \mathbb{Z}$ a.î. $0 = c\underbrace{(j-i)}_{0} + \underbrace{p}_{0} \cdot d = 1$ (în $\mathbb{Z}$)

$0 = 1$ Abs.

$F = \{0, 1, 2 \ldots p - 1\}$ în K.

F subcorp al lui K.

$(F, +, \cdot)$

K, L corpuri comut.

$K \subseteq L$. $\Rightarrow \exists$ structură de K spațiu vect pe L.

$k \cdot l$ (înmulț. cu scalari din K)

$k \in K$, $l \in L$.

$(k_1 + k_2) \cdot l = k_1 \cdot l + k_2 \cdot l$ (

$(k_1 \cdot k_2) l = k_1 \cdot (k_2 \cdot l) \cdot l$.

$1 \cdot l = l$.

$v_1, v_2 - v_n \in L$

bază pt K ca F sp. vectorial

$v \in K \Rightarrow v = x_1 \cdot v_1 + x_2 \cdot v_2 + \ldots + x_n v_n$

$x_i \in F$

$\boxed{|K| = p^n \text{ - card. grup trb să fie puterea unui nr prim}}$

---

p prim, $n \in \mathbb{N}^* \Rightarrow \exists K$ corp cu p^n elem? DA ✓

! K corp finit $\Rightarrow K$ comutativ

$\mathbb{Z}[i\sqrt{2}]$

$(\mathbb{Z}_3[i\sqrt{2}]$ - nu e corp.

are 9 elem

$\overline{a + ib\sqrt{2}}$

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

$(\overline{1 + i\sqrt{2}})(\overline{1 - i\sqrt{2}}) = \overline{3} = \overline{0}$ nu e corp.

$11\mathbb{Z}[i\sqrt{2}]$

$(\overline{3+i\sqrt{2}})(\overline{3-i\sqrt{2}}) = \overline{11} = \overline{0}$ nu e corp

---

$7\mathbb{Z}[i\sqrt{2}]$. - e corp cu 49 elem.

$(\overline{a+bi\sqrt{2}})(\overline{c+di\sqrt{2}}) = 1. \mid (\overline{a-bi\sqrt{2}})$

$a, b \in \{0, 1 \ldots 6\}$

a, b nu ambele 0.

$(a^2+2b^2)(c+di\sqrt{2}) = a - bi\sqrt{2}.$

$c \overset{7}{\equiv} \dfrac{a}{a^2+2b^2}$ $\quad d \overset{7}{\equiv} \dfrac{-b}{a^2+2b^2}$

$a^2+2b^2 \equiv 0 (7)$

$a^2 \overset{7}{\equiv} -2b^2 \mid^3$

$a^6 \equiv -b^6 (7)$

Dacă $a \neq 0 \Rightarrow a^6 \overset{7}{\equiv} 1$

$b^6 \overset{7}{\equiv} -1$ $\Big\}$ fals.

$b^6 = 0, 1$

$a = 0 \Rightarrow b = 0$ fals.

$\dfrac{\mathbb{Z}_3[x]}{(x^2+\overline{1})\mathbb{Z}_3[x]}$ corp cu 9 elemente.

$\mathbb{Z}_3[x]$ - polinoame cu coef. în $\mathbb{Z}_3$

$f \in \mathbb{Z}_3[x]$

$f = (x^2+1) \cdot g(x) + r(x)$ grad $r \leq 1$.

$f = (x+1)g(x) + a + bx \qquad a, b \in \mathbb{Z}_3[x]$

$\bar{f} = \overline{a+bx}$

$|K| = 9$

$\bar{0}$	$\bar{x}$	$\bar{x}$ ——	$\overline{2x}$	$\bar{x} \cdot \overline{2x} = 1.$
$\bar{1}$	$\overline{1+x}$	$1+x$	$\overline{1+2x}$	
$\bar{2}$	$\overline{2+x}$	$2x+1$	$\overline{2+2x}$	

$(1+x)(1+2x) = \overline{1+2x^2} = \overline{1-2} = -1.$

$(1+2x)(2+2x)$

$$K = \frac{\mathbb{Z}_3[x]}{(x^2+\bar{1})\mathbb{Z}_3[x]}$$