24.02.2016.

ALGEBRĂ

CURS 1

Inel

Definiție $(R,+,\cdot)$ s.n. inel (unitar) dacă:

i) $(R,+)$ grup comutativ.

ii) $(R,\cdot)$ monoid (cu unitate) ~~$0\neq 1$~~.

iii) $a\cdot(b+c)=a\cdot b+a\cdot c$.

$(a+b)\cdot c=a\cdot c+b\cdot c \quad \forall a,b,c\in R$.

$$\mathbb{Z}[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c\in\mathbb{Z}\}$$

$(\mathbb{Z}[\sqrt[3]{2}],+,\cdot)$ inel $\quad (\sqrt[3]{2})^2=\sqrt[3]{4}$

Notații

0 - elementul neutru pt +

1 - —————//— $\cdot$ $\quad 0\neq 1$.

$0\cdot a=0$.

$0\cdot a=(0+0)\cdot a=\underline{0\cdot a}+\underline{0\cdot a}$

$b=b+b \qquad b=0\cdot a$

$b=b+b \mid +c \qquad \exists c$ a.î. $b+c=c+b=0$

$0\cdot a=\underline{0}=b+c=(b+b)+c=b+(b+c)=b+0=\underline{b}$

Inelul claselor de resturi mod n $(\mathbb{Z}_n,+,\cdot)$

Gauss - de la el vine

$x =$ anul.

a restul împ. lui x la 19.

b — " — x la 4

c — " — x la 7.

d — " — $19a+15$ la 30.

e — " — $2b+4c+6d+6$ la 7.

Paște $= d+e+4$ Aprilie sau Mai.

Dacă $d+e+4 \leq 30$ intră în Aprilie

Dacă $d+e+4 \geq 31$ în Mai.

$x = 2016$.

$$\begin{array}{r|l} 2016 & 19 \\ \hline 19 & 106 \\ \overline{116} & \\ 114 & \\ \overline{2} & \end{array}$$

$$\begin{array}{r|l} 2016 & 7 \\ \hline 14 & 288 \\ \overline{61} & \\ 56 & \\ \overline{56} & \\ 56 & \\ \overline{=} & \end{array}$$

$$\boxed{\begin{array}{l} a = 2 \\ b = 0 \\ c = 0 \end{array}}$$

$d = (19 \cdot 2 + 15) \overset{30}{\equiv} \boxed{23}$.

$e = 6 \cdot 23 + 6 = 6 \cdot 24 \overset{7}{\equiv} 6 \cdot 3 = 18 \overset{7}{\equiv} 4$

$\boxed{e = 4}$

Paște: $23 + 4 + 4 = 31$. și vine $\underline{1 \text{ Mai}}$

Temă 1. Care este primul an după 3000 a.î. paștele cade pe 1 Mai?

alexgica@yahoo.com

2.

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
0 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

Vigenere (sec 16)

~~STEAUA~~.

CURSUL | E PLICTISITOR
UNVSOL | W

STEAUA

18 19 4 0 20 10

$2+18=20=U$
$20+19=39 \overset{26}{\equiv} 13 = N$

---

decri MSNFYJWGTVJTVDMFRFMMSOMB TRSF

lung cod ≤ 6 - e vb de alfab dicrocalite.

Scop: Teorema (Euler): $a \in \mathbb{Z}$, $m \in \mathbb{N}^*$ $(a,m)=1$

Atunci $a^{\varphi(m)} \equiv 1 (m)$

$$\varphi(m) = |U(\mathbb{Z}_m)| = m \prod_{\substack{p \text{ prim} \\ p|m}} \left(1-\frac{1}{p}\right)$$

Notație: $\hat{1}$ el. neutru al grupului.

$U(R) = \{ r \in S \mid \exists s \in R \text{ a.î. } r \cdot s = s \cdot r = 1 \}$.

Def R este corp dacă R inel și $U(R) = R \setminus \{0\}$.

$$\boxed{U(\mathbb{Z}/m) = \{\bar{a},\ a \in \mathbb{Z}, (a,m)=1\}}$$

$\bar{a} \in U(\mathbb{Z}_m) \overset{?}{\Longrightarrow} (a,m)=1.$

$\Rightarrow \exists\ \bar{b}$ a.î. $\bar{a}\cdot\bar{b} = \bar{1}$ $\quad m \mid ab-1 \overset{?}{\Rightarrow} (m,a)=1.$

Dacă p prim $\quad p \mid m$, $p \mid a$

$$\left.\begin{array}{l} p \mid m \mid ab-1 \\ p \mid a \Rightarrow p \mid ab \end{array}\right\} \Rightarrow p \mid ab-(ab-1)=1 \Rightarrow p \mid 1$$

„$\Leftarrow$" $(a,b)=1 \Rightarrow \exists\ b, c \in \mathbb{Z}$ a.î. $ab+mc=(a,m)=1.$

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

$\overline{ab+mc} = \bar{1} = \bar{a}\cdot\bar{b} + \bar{m}\cdot\bar{c}$

$\bar{m}=\bar{0} \quad \Rightarrow \bar{a} \in U(\mathbb{Z}_m)$

$a^{|U(\mathbb{Z}_m)|} \equiv 1(m)$ ex: $(U(R),\cdot)$ - grup - întotdeauna

Dem:

$(a,m)=1 \Rightarrow \bar{a} \in U(\mathbb{Z}_m)$

$\xrightarrow{\text{T. Lagr.}} \boxed{\bar{a}^{|U(\mathbb{Z}_m)|} = \bar{1}}$

Th. Lagrange

$(G,\cdot)$ grup finit, e - el. neutru al grupului

$g \in G$ - arbitrar.

Atunci $g^{|G|}=e$

G - mulțime finită

$|G|$ - card mult. G

Avem nev de o construcție.

$(R, +, \cdot)$ inel

$(S, \oplus, \odot)$ - inel

Am o str. de inel pe $R \times S$

$R \times S = \{(r, s) \mid r \in R, s \in S\}$

ex: $(R \times S, \perp, T)$ inel.

$(r_1, s_1) \perp (r_2, s_2) = (r_1 + r_2, s_1 \oplus s_2)$

$(r_1, s_1) \, T \, (r_2, s_2) = (r_1 \cdot r_2, r_1 \odot r_2)$

$(0_R, 0_S)$ - el neutru $+$

$(1_R, 1_S)$ - el n $\cdot$

$$\boxed{U(R \times S) = U(R) \times U(S)}$$

Lema chineză a resturilor $m, n \in \mathbb{N}^*$, $(m, n) = 1$.

$$\Rightarrow \boxed{\mathbb{Z}_{m,n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n}$$

Def: $(R, +, \cdot)$ și $(S, \oplus, \odot)$ sunt izomorfe (notez $R \simeq S$) dacă $\exists f: R \to S$, f biject a.î. $f(r+s) = f(r) \oplus f(s)$ $\forall r, s \in R$

și $f(r \cdot s) = f(r) \odot f(s)$ $\forall r, s \in R$

$f(1_R) = 1_S$

Dem:

$f(\bar{a}) = (\hat{a}, \tilde{a})$ — f este bine definită

$\tilde{a}$ — cls. mod n.

$\hat{a}$ — cls. mod m

$\bar{a}$ — clasa mod $m \cdot n$.

$f(\bar{a}+\bar{b}) = f(\bar{a}) + f(\bar{b})$

$f(\bar{a}\cdot\bar{b}) = f(\bar{a})\cdot f(\bar{b})$ $\qquad f(\bar{a}\cdot b) = f(\overline{ab}) = (\widehat{ab}, \widetilde{ab}) =$

$= (\hat{a}, \tilde{a})\cdot(\hat{b}, \tilde{b})$

$f(\bar{1}) = (\hat{1}, \tilde{1})$

f inj $\quad f(\bar{a}) = f(\bar{b})$

$(\hat{a}, \tilde{a}) = (\hat{b}, \tilde{b})$

$$\left.\begin{cases} \hat{a} = \hat{b} \Rightarrow m \mid a-b \\ \tilde{a} = \tilde{b} \Rightarrow n \mid a-b \\ (m,n)=1 \end{cases}\right\} m\cdot n \mid a-b \Rightarrow \bar{a} = \bar{b}$$

$f : M \to N$ $\quad M, N$ - finite.

f inj. $\quad$ dacă $|M| = |N|$ $\Big| \Rightarrow f$ biject.

$f : \mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

$|\mathbb{Z}_{mn}| = m\cdot n = |\mathbb{Z}_m \times \mathbb{Z}_n| \Rightarrow f$ biject

Asta e dem lemei. aproape...

R, S - inele.

$f : R \to S$ $\quad f$ izomorfism.

$$f(U(R)) = U(S)$$

$$U(R) \simeq U(S)$$

Remarcă: $U(\mathbb{Z}_{mn}) \simeq U(\mathbb{Z}_m \times \mathbb{Z}_n)$

$(m,n)=1$

$$U(R \times S) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$$

$$\Rightarrow |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)| \Rightarrow |U(\mathbb{Z}_m)| \cdot |U(\mathbb{Z}_n)|$$

$$|R \times S| = |R| \cdot |S|$$

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$ funcția e $\varphi(n)$. în spate.

Dem formulei:

$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$

$p_1 < p_2 < \ldots < p_r$

p_j prime, $\forall j = \overline{1,r}$

Folosim remarca. $\Rightarrow$ $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})$

$(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$. $i \neq j$.

$\varphi(p^{\alpha})$ $\quad p$ prim $\alpha \in \mathbb{N}^*$

$$|U(\mathbb{Z}_{p^{\alpha}})| = \varphi(p^{\alpha})$$

$$U(\mathbb{Z}_{p^{\alpha}}) = \{\bar{a} \mid a \in \mathbb{N},\ 0 \le a \le p^{\alpha}-1,\ (a, p^{\alpha}) = 1\}$$

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$$

$0 \cdot p$

$1 \cdot p$

$2 \cdot p$

$\vdots$

$(p^{\alpha-1}-1)p$

$p^{\alpha-1}$ nr.

$\varphi(u)$ din prop. $= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \ldots = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots$

$\ldots p_r^{\alpha_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_r}\right)$