

Aritmetică în elor \mathbb{Z} și $K[x]$, K corp comut.

(1)

Să începem prin a observa că mulțimea \mathbb{Z} și $K[x]$ sunt integre, $U(\mathbb{Z}) = \{\pm 1\}$, $U(K[x]) = K^*$.

Teorema împărțirii cu rest

Fie $R \subseteq \mathbb{Z}$ sau $K[x]$. Atunci pentru orice $a, b \in R$, $b \neq 0$, există și sunt unice $q, r \in R$ astfel încât

$$a = bq + r, \text{ cu } \begin{cases} 0 \leq r < |b|, \text{ dacă } R = \mathbb{Z} \\ \text{grad } r < \text{grad } b, \text{ dacă } R = K[x] \end{cases}$$

Dem. $R = \mathbb{Z}$: fie $R = \min \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\}$.

Dacă $R = a - bq \geq |b|$, atunci $0 \leq a - b(q + \frac{\text{sgn}(b)}{\pm 1}) < R$, contradicție. Deci $R < |b|$.

Fie $q', r' \in \mathbb{Z}$, $a = bq' + r'$, $0 \leq r' < |b|$; atunci $b(q - q') = r' - r \Rightarrow |b||q - q'| = |r' - r| < |b| \Rightarrow q = q'$ și $r = r'$. //

Def. q și r se numesc câțul și restul împărțirii, iar R restul împărțirii.

Ex. $-17 = 2(-9) + 1$

Def. Fie $R = \mathbb{Z}$ sau $K[x]$ și $a, b \in R$. Spunem

că a divide b dacă există $c \in R$ astfel încât $b = ac$. În scriem $a \mid b$. Se mai spune că a este divizor al lui b sau că b este multiplu al lui a .

Obs. Dacă $b \neq 0$, atunci $b \mid a \Leftrightarrow$ restul împărțirii lui a la b este 0.

Def. $a, b \in R$ sunt associate în divizibilitate dacă $a \mid b$ și $b \mid a$.

Not. $a \sim b$

- Prop. (i) $a|b \Leftrightarrow bR \subseteq aR$. (2)
- (ii) $a|b$, $b|c \Rightarrow a|c$.
- (iii) $a|b$, $a|c \Rightarrow a|\alpha b + \beta c$, (\forall) $\alpha, \beta \in R$.
- (iv) $a|b \Rightarrow \begin{cases} |a| \leq |b|, \text{ dc. } R = \mathbb{Z} \\ \text{grad } a \leq \text{grad } b, \text{ dc. } R = K[X]. \end{cases}$
- (v) $a, b \in R$ sunt asoc. în divizib. dc. și numai dc. $\{a = \pm b, \text{ dc. } R = \mathbb{Z}\}$
 $\{a = \alpha b, \alpha \in K^*, \text{ dc. } R = K[X]\}$.

Def. Fie $a, b \in R$. Un elem. $d \in R$ este un cel mai mare divisor comun al lui a și b dc. (i) $d|a$, $d|b$
(ii) $d'|a$, $d'|b \Rightarrow d' \mid d$.
Scriem $d = (a, b)$. Dc. $(a, b) = 1$, at. suntem că a și b sunt prime între ele.
Un element $m \in R$ este un cel mai mic multiplu comun al lui a și b dc.

- (i) $a|m$, $b|m$
(ii) $a|m'$, $b|m' \Rightarrow m \mid m'$.

Scriem $m = [a, b]$.

În R orice două elemente au un comun dc și acesta se obține prin Algoritmul lui Euclid

Fie $a, b \in R$, $b \neq 0$. Avem $a = bq_1 + r_1$, $0 \leq r_1 < |b|$; apoi, dc. $r_1 \neq 0$, $b = r_1 q_2 + r_2$, $0 \leq r_2 < |r_1|$; apoi, dc. $r_2 \neq 0$, $r_1 = r_2 q_3 + r_3$, $0 \leq r_3 < r_2$, etc.

Oltimul articol nu are strict descrezătorie
de nr. naturale $r_1 > r_2 > \dots$ care
ne poate fi infinit, deci nu existe un
 $n \in \mathbb{N}^*$ al $r_n \neq 0$ și $r_{n+1} = 0$.

Aveam că $(a, b) = r_n$, deci cum dă - săl lui a și b este ultimul rest ≠ 0 din algoritmul lui Euclid.

$$\begin{array}{l} \text{Ex: } a=18, b=24 \\ \left. \begin{array}{l} a \text{ ia valoare } 18, 24, 18, 6 \\ b \xrightarrow{n} 24, 18, 6 \\ r \xrightarrow{n} 18, 6, 0 \end{array} \right\} \Rightarrow (18, 24) = 6. \end{array}$$

Prop. Orice ideal al lui R este principal.

Dem. $I \leq R$, $I \neq 0$. Fie $\underline{a \in I}$, $a \neq 0$, cu
lat minimum dc. $R = \mathbb{Z}$, respectiv grad a minim
dc. $R = K[x]$. Arătăm că $\boxed{I = aR}$. Evident,
 $a \in I \Rightarrow aR \subseteq I$. Reciproc, fie $\underline{b \in I}$; at.
 $b = aq + r$, $0 \leq r < |a|$, dc. $R = \mathbb{Z}$
 $\left\{ \begin{array}{l} \text{grad } r < \text{grad } a, \text{ dc. } R = K[x]. \end{array} \right.$

Dar $\underline{r = b - aq} \in I$ și at. $\underline{r = 0}$. //

Prop. $a, b \in R$. Aveam:

- (i) $aR + bR = [a, b]R$
- (ii) $aR \cap bR = [a, b]R$

(iii) $(a, b)[a, b]$ este asociat în diviz. cu ab.

Prop. Fie $a, b, c \in R \setminus \{0\}$. Aveam:

- (i) Dacă $d = (a, b)$, at. $(\exists) \alpha, \beta \in R$ al $d = \alpha a + \beta b$.
- (ii) Dacă $d = (a, b)$, $a = da'$, $b = db'$, at. $(a', b') = 1$.

(iii) $(a,b) = 1, (a,c) = 1 \Rightarrow (a,bc) = 1$. (7)

(iv) $a \mid bc, (a,b) = 1 \Rightarrow a \mid c$.

(v) $a \mid c, b \mid c, (a,b) = 1 \Rightarrow ab \mid c$.

Def. Un element $p \in R$ s.m. prim d.c.

(i) $p \neq 0, p \notin U(R)$

(ii) $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$.

Def. Un element $q \in R$ s.m. ireductibil d.c.

(i) $q \neq 0, q \notin U(R)$

(ii) $q = ab \Rightarrow a \in U(R)$ sau $b \in U(R)$.

Prop. În R numările de primă și ireductibil coincid.

În consecință, un $p \in \mathbb{Z}$ este primă d.c. $p \neq 0, \pm 1$ și nu are ca divizori de către $\pm 1, \pm p$, iar un $f \in K[x]$ este ireductibil d.c. nu se poate scrie ca produs de două polinoame de grad ≥ 1 .

Def. Un număr număr care nu este primă s.m. complet, iar un polinom care nu este ireductibil s.m. reductibil.

Prop. Fie $p \in R$ elem. prim. At. inelul factor R/pR este corp.

Exemplu 1) $\pm 2, \pm 3, \pm 5, \dots$ sunt numere prime
2) x este ined. în $K[x]$, iar x^2 este reductibil.
 $K[x]/(x) \cong K$ (corp).

Prop. (i) Orice polinom de gradul 1 din $K[x]$ este ireductibil.

(ii) Un polinom de grad 2 sau 3 din $K[x]$ este ireductibil dacă și numai dacă nu

are rădăcini în K . În general, fără ireducibilitate. Reciproc este fals!

Ex. 1) $x^2 - 2$ este ireducibil în $\mathbb{Q}[x]$, dar este redusabil în $\mathbb{R}[x]$.

2) $x^2 + x + 1 \in \mathbb{Z}_2[x]$ ireducibil.

$x^3 + x + 1 \in \mathbb{Z}_2[x]$ ireducibil.

$x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$ nu are rădăcini în \mathbb{Z}_2 , dar este redusabil.

Teorema Orice elem. nenul și neinvazabil din R se scrie ca produs finit de elemente prime. Mai mult, scrierea este unică (prinț la o asociere cu divizibilitate și abstracție, făcând de ordinul factorilor).

Corolar Fie $a, b \in R \setminus \{0\}$ neinvazabile,

$$a = p_1^{k_1} \cdots p_r^{k_r}, \quad b = p_1^{l_1} \cdots p_r^{l_r}, \quad k_i, l_j \geq 0.$$

$$\text{Atunci } (a, b) = p_1^{min(k_1, l_1)} \cdots p_r^{min(k_r, l_r)}$$

$$[a, b] = p_1^{\max(k_1, l_1)} \cdots p_r^{\max(k_r, l_r)}$$

Teorema

(i) Multimea nr. naturale prime este în finită.

(ii) Multimea polinoamelor ireductibile și numice din $K[x]$ este în finită.