

(Arithmetica) \rightarrow AR ①

Arithmetica lui \mathbb{Z} și $K[x]$ (K corp comutativ)

În acest capitol vom prezenta cîteva proprietăți aritmetice ale lui \mathbb{Z} și vom arăta că în celele \mathbb{Z} și $K[x]$ (K corp comutativ) au proprietăți aritmetice similare.

\mathbb{Z} și $K[x]$ sunt domenii de integritate.

Elementele inversibile (unitatile) lor sunt

$$U(\mathbb{Z}) = \{1, -1\}, \quad U(K[x]) = K \setminus \{0\}.$$

Reamintim că funcția grad, notată $\deg: K[x] \rightarrow \mathbb{N} \cup \{-\infty\}$, are proprietatea $\deg(fg) = \deg(f) + \deg(g)$ pt. orice $f, g \in K[x]$.

Teorema împărțirii cu rest în \mathbb{Z} . Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci există și sunt unice determinate $q, r \in \mathbb{Z}$ pentru care

$$a = qb + r \text{ și } 0 \leq r < |b|.$$

(q și r se numesc cîtul și restul împărțirii lui a la b).

Dem. Existența: Multimea $X = \{a - hb \mid h \in \mathbb{Z}\} \cap \mathbb{N}$ este nevoidă; înțeles că

$$a - hb \geq 0 \Leftrightarrow hb \leq a \Leftrightarrow \begin{cases} h \leq \frac{a}{b}, \text{ dacă } b > 0 \\ h \geq \frac{a}{b}, \text{ dacă } b < 0 \end{cases} \text{ și în}$$

ambele cazuri putem alege un $h \in \mathbb{Z}$ care să satisfacă inegalitatea.

Cum (\mathbb{N}, \leq) este sine ordonată (adică orice submultime nevoidă a lui \mathbb{N} are un cel mai mic element), X are un cel mai mic element, fie acesta $q = a - qb$, cu $q \in \mathbb{Z}$.

Atunci $a = qb + r$ și $r \geq 0$. Arătăm că $r < |b|$.

Într-adevăr, dacă suntem cu $a \geq |b|$, atunci
 $|a - b| \geq 0$ și $|a - b| = a - q_1 b - |b| = a - q_1 b - \varepsilon b$ (unde $\varepsilon = \begin{cases} 1, & \text{d}\overset{\circ}{\text{ar}} b > 0 \\ -1, & \text{d}\overset{\circ}{\text{ar}} b < 0 \end{cases}$)
 $= a - (q_1 + \varepsilon) b$, deci $|a - b| \in X$.

Cum $|a - b| < a$, suntem cu o contradicție.
Așadar q_1 și r_1 satisfac proprietățile dorite.

Unicitatea: Fie $a = q_1 b + r_1 = q_2 b + r_2$ cu $q_1, q_2, r_1, r_2 \in \mathbb{Z}$
și $0 \leq r_1, r_2 < |b|$. Atunci
 $|r_1 - r_2| \leq |b|$ și $|r_1 - r_2| = |(q_2 - q_1)b|$, de unde
 $|q_2 - q_1| \cdot |b| \leq |b|$. Cum $|b| \neq 0 \Rightarrow |q_2 - q_1| \leq 1$,
deci $q_2 - q_1 = 0$. Obținem $\varepsilon_1 = \varepsilon_2$ și atunci clar
 $\varepsilon_1 r_1 = r_2 (= a - q_1 b)$.

Am demonstrat la capitolul "Inele de polinoame"
că pt. un anel comutativ A are loc o teoremă de împărțire
cu rest a unui polinom $f \in A[x]$ la un polinom nenul
 $g \in A[x]$, cu condiția ca g să sătăcă coeficientul dominant
înversabil. În cazul în care $A = K$ este corp comutativ,
această condiție este automat satisfăcută (oicădă K nu este
înversabil), deci are loc următorul rezultat.

Teorema împărțirii cu rest în $K[x]$. Fie K un corp comutativ.
Atunci pentru orice $f, g \in K[x]$, $g \neq 0$, există și
sunt unice $q, r \in K[x]$ astfel încât
 $f = q \cdot g + r$ și $\deg(r) < \deg(g)$.

(q și r se numesc cotații și restul împărțirii lui f la g).

Este clară exemplificarea celor două teoreme de împărțirea cu rest, în \mathbb{Z} și $K[x]$, funcția modul din \mathbb{Z} și funcția grad din $K[x]$ înălțând evoluția similară. Această exemplificare face ca \mathbb{Z} și $K[x]$ să aibă multe proprietăți (aritmetice) comune. Un prim exemplu este:

Teorema. Fie $R = \mathbb{Z}$ sau $R = K[x]$, cu K corp comutativ. Atunci orice ideal al lui R este principal.

Dem. Fie I ideal în R . Dacă $I = 0$, atunci $I = (0)$, căre este ideal principal. Presupunem că $I \neq 0$.

Cazul $R = \mathbb{Z}$. Cum $I \neq 0$, el conține elemente strict positive (într-o ordene, fie $a \in I \setminus \{0\}$, dacă $a > 0$, atunci I îl conține și $-a$. Dacă $a < 0$, atunci I îl conține și $-a > 0$).

Fie b cel mai mic element strict pozitiv al lui I (există deoarece \mathbb{N} este bine ordonată și $I \cap \mathbb{N}^* \neq \emptyset$).

Astudăm că $I = (b)$ (dacă $I = b\mathbb{Z}$).

" \supseteq " Cum $b \in I$, ~~atunci~~ și I ideal $\Rightarrow (b) \subset I$.

" \subseteq " Fie $a \in I$. Împărțim pe a la b cu rest r obținem $a = qb + r$ cu $0 \leq r < b$. Atunci $r = a - qb \in I$ și din minimălitatea lui b rezultă că $r = 0$, deci $a = qb \in (b)$.

Cazul $R = K[x]$. Fie b un element nenul din I de grad minim posibil. Studiem că $I = (b)$ (dacă $I = bK[x]$)

" \supseteq " Cum $b \in I$ și I ideal $\Rightarrow (b) \subset I$.

" \subseteq " Fie $a \in I$. Împărțim pe a la b cu rest în $K[x]$ și obținem $a = qb + r$ cu $\deg(r) < \deg(b)$.

Atunci $r = a - qb \in I$ și minimul teore (predului) lui b este că $r=0$. Atunci $a = qb \in (b)$.

Concordanță asupra reprezentării elementelor din mulțimea factor:

(1) Fie $R = \mathbb{Z}$. Dacă $n \in \mathbb{N}^*$, atunci orice element din

$$\frac{\mathbb{Z}}{(n)} = \frac{\mathbb{Z}}{n\mathbb{Z}} (= \mathbb{Z}_n) \text{ se scrie unic sub forma}$$

\hat{r} cu $0 \leq r < n$. [într-edere pl. $a \in \mathbb{Z}$ fie $a = q \cdot n + r$ cu $0 \leq r < n$, atunci $\hat{a} = \hat{q} \cdot \hat{n} + \hat{r} = \hat{r}$].

(2) Fie $R = K[X]$. Dacă $f \in K[X]$ are grad $n \geq 1$, atunci orice element din $\frac{K[X]}{(f)}$ se reprezintă în mod

unic ca \hat{r} , cu $r \in K[X]$ și $\deg(r) \leq n-1$, deci sub forma $\underbrace{a_{n-1}X^{n-1} + \dots + a_0}_{r} \in K$ [ce locu] (ce locu)

Impart un polinom arbitrar $h \in K[X]$ la f și obținem $h = q f + r$, cu $\deg(r) \leq n-1$, și atunci $\hat{h} = \hat{r}$.

În particular, dacă corpul K este finit ~~cum este~~ cu m elemente, atunci $\frac{K[X]}{(f)}$ are m^n elemente.

Divizibilitate

În această secțiune presupunem peste tot că $R = \mathbb{Z}$ sau $R = K[X]$ cu K corp comutativ.

Definiție. Fie $a, b \in R$. Spunem că a divide b și notăm $a | b$ dacă există $c \in R$ cu $b = ca$.

(în loc de a divide b mai putem spune și b se divide cu a , sau a este un divizor al lui b , sau b este multiplu de a).

Este clar că $a \mid b$ și $b \in (a)$ și $a \in U(R)$.

Propozitie. Fie $a, b, c \in R$. Atunci:

$$(i) \quad a \mid b \Leftrightarrow (b) \subset (a);$$

$$(ii) \quad a \mid a$$

$$(iii) \quad a \mid b \text{ și } b \mid c \Rightarrow a \mid c$$

$$(iv) \quad a \mid b \text{ și } b \mid a \Leftrightarrow \exists u \in U(R) \text{ cu } b = ua \quad (\text{în acest caz presupunem că } a \text{ și } b \text{ sunt asociate în divizibilitate}),$$

$$(v) \quad a \mid b, a \mid c \Rightarrow \text{pt. orice } b', c' \in R \text{ avem } a \mid bb' + cc'.$$

$$(vi) \quad \left. \begin{array}{l} a \mid b \\ b \neq 0 \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} |a| \leq |b|, \text{ în cazul } R = \mathbb{Z} \\ \deg(a) \leq \deg(b), \text{ în cazul } R = K[X] \end{array} \right.$$

Dem. (i) " \Rightarrow " Dacă $a \mid b$, atunci $b = ca$ pt. un $c \in R$, de unde $b \in (a)$. Cum (a) este ideal, rezultă $(b) \subset (a)$.

" \Leftarrow " Fie $(b) \subset (a)$. Atunci $b \in (b)$, deci $\exists b \in (a)$, de unde există $c \in R$ cu $b = ca$, adică $a \mid b$.

$$(ii) \quad a = 1 \cdot a \Rightarrow a \mid a.$$

$$(iii) \quad a \mid b \Rightarrow \exists x \in R \text{ cu } b = xa$$

$$b \mid c \Rightarrow \exists y \in R \text{ cu } c = yb. \text{ Atunci}$$

$$c = yb = ya, \text{ deci } a \mid c.$$

$$(iv) \quad " \Rightarrow " \text{ Dacă } a = 0, \text{ atunci } a \mid b \Rightarrow b = 0 \text{ și } b = 1 \cdot a.$$

La fel, dacă $b = 0$, trebuie ca $a = 0$ și din nou $b = 1 \cdot a$.

Presupunem $a, b \neq 0$. Cum $a \mid b$ și $b \mid a \Rightarrow \exists u, v \in R$ cu $b = ua$ și $a = vb$.

$$\text{Atunci } b = ua = uvb, \text{ deci } (uv - 1)b = 0.$$

$$\text{Cum } b \neq 0 \text{ (în domeniul de integritate)} \Rightarrow uv = 1,$$

~~b=ua~~, deci $u \in U(R)$.

" \Leftarrow " Fie $b=ua$ cu $u \in U(R)$. Atunci clar $a \mid b$.

În plus, $a = u^{-1}b$, deci $\exists \frac{1}{u}b/a$.

(v) Fie $a \nmid b$ și $a \mid c$. Atunci există $x, y \in R$ cu
 $b = xa$ și $c = ya$, de unde

$$bb' + cc' = xab' + yac' = (xb' + yc')a.$$

Obținem $a \mid bb' + cc'$.

(vi) Fie $a \mid b$, deci $b = ac$ pt. un $c \in R$. Atunci:

- dacă $R = \mathbb{Z}$: $|b| = |a| \cdot |c| \geq |a| \cdot 1 = |a|$ (am folosit
 $cd \mid b \neq 0 \Rightarrow c \neq 0$, deci $|c| \geq 1$).

- dacă $R = K[x]$, atunci $\deg(b) = \deg(a) + \deg(c) \geq \deg(a)$
(am folosit $cd \mid b \neq 0 \Rightarrow c \neq 0$, deci $\deg(c) \geq 0$).

Observație. Dacă $a, b \in R$, $a \neq 0$, atunci

$a \mid b \Leftrightarrow$ restul împărțirii lui b la a este 0.

Dem " \Leftarrow " Dacă $b = q \cdot a + 0$, atunci clar $a \mid b$.

" \Rightarrow " Fie $b = qa + r$ împărțirea cu rest în R . Atunci

$r = b - qa \neq 0$, deci $a \nmid r$ (folosim (v) din Prop.).

Dacă $r \neq 0$, din Prop.(vi) ar rezulta că

$|a| \leq |r| = r$ în cazul $R = \mathbb{Z}$, și $\deg(a) \leq \deg(r)$

în cazul $R = K[x]$, ceea ce este o contradicție
cu faptul că r e restul împărțirii lui b la a .

Exercițiu. Definim pe R relația \sim prin $a \sim b (\Leftrightarrow a \nmid b$
sunt asociate în divizibilitate (adică $\exists u \in U(R)$ cu $b = ua$,
sau echivalent, $a \mid b$ și $b \mid a$)). Să se arate că \sim
este o relație de echivalență.

Definitie. Fie $a, b \in \mathbb{R}$. Atunci:

(1) Un element $d \in \mathbb{R}$ se numeste un cel mai mare divizor comun (respectiv c.m.m.d.c) al lui a si b daca $\begin{cases} d | a, d | b, \text{ si} \\ \text{pt. orice } d' \text{ cu } d' | a \text{ si } d' | b, \text{ avem } d' | d. \end{cases}$

(2) Un element $m \in \mathbb{R}$ se numeste un cel mai mic multiplu comun (respectiv c.m.m.m.c) al lui a si b daca $\begin{cases} a | m, b | m \text{ si} \\ \text{pt. orice } m' \text{ cu } a | m' \text{ si } b | m', \text{ avem } m | m'. \end{cases}$

Observatie. Daca $a | b$, atunci clar ca este un c.m.m.d.c al lui a si b , iar b este un c.m.m.m.c al lui a si b .

Problema. Exista un c.m.m.d.c si un c.m.m.m.c al lui a si b pt. orice $a, b \in \mathbb{R}$?

Raspunsul afirmativ este dat de urmatoarea

Teorema. Fie $a, b \in \mathbb{R}$ si $d, m \in \mathbb{R}$ doua elemente putin care $(a) + (b) = (d)$ si $(a) \cap (b) = (m)$ [observatie: existenta unor astfel de elemente d si m este garantata de faptul ca orice ideal este principal]. Atunci:

- (1) d este un c.m.m.d.c al lui a si b ,
- (2) m este un c.m.m.m.c al lui a si b ,
- (3) $d | m$ este asociat indivisibilite cu a si b .

Dem. (1) Cum $(a) + (b) = (d)$, avem $(a) \subset (d)$ si $(b) \subset (d)$, de unde $d | a$ si $d | b$.

(AR) 8

Este $d' \in \mathbb{R}$ cu $d' \mid a$ și $d' \mid b$. Arătăm că $d' \mid d$.

Într-adevăr, $d \in (d) = (a) + (b) \Rightarrow$ există $x, y \in \mathbb{R}$ cu $d = xa + yb$. Atunci $d' \mid xa + yb = d$, gata!

(2) $(m) = (a) \cap (b) \Rightarrow (m) \subset (a)$ și $(m) \subset (b)$, deci $a \mid m$ și $b \mid m$.

Arătăm că dacă $m' \in \mathbb{R}$, atunci $b \mid m'$, atunci $m \mid m'$.

Dacă $a \mid m' \Rightarrow (m') \subset (a)$, iar $b \mid m' \Rightarrow (m') \subset (b)$, de unde $(m') \subset (a) \cap (b) = (m)$, ceea ce arată că $m \mid m'$.

(3) Dacă $a=0$ sau $b=0$, atunci $m=0$ și $ab=d \cdot m=0$.

Presupunem $a, b \neq 0$.

Așezăm $d \mid a$ și $d \mid b$, deci $a = da'$ și $b = db'$, pt. niste $a', b' \in \mathbb{R}$.

Atunci $ab = da' \cdot db' = d \underbrace{(da' \cdot b')}_{\text{imodm}} = d \cdot m'$.

Dacă $m' = da'b' = ab'$, deci $a \mid m'$ și $m' = da'b' = a'b$,

deci $b \mid m'$. Cum m' e un c.m.m.m.c al lui a și b ,

rezultă că $m \mid m'$. Atunci $d \mid m \mid d \cdot m' = ab$, deci $d \mid ab$.

Acum $a \mid ab$ și $b \mid ab$, de unde $m \mid ab$, deci există d' cu $ab = md'$. Scriem acum $m = au = bv$ pt. niste $u, v \in \mathbb{R}$. Atunci $ab = aud'$, de unde $b = vd'$, și $ab = bvd'$, de unde $a = vd'$. Așează $d' \mid a$ și $d' \mid b$, deci avem $d' \mid d$. Atunci $ab = md' \mid md$, deci $ab \mid md$.

Am obținut că $d \mid ab$ și $ab \mid md$, deci $ab \sim md$.

AR

9

Observatie. Fie $a, b \in R$. Teorema precedenta arata ca daca $d \in R$ satisface $(a) + (b) = (d)$, atunci d este un c.m.m.d.c al lui a, b ; in particular, un c.m.m.d.c exista intotdeauna.

~~Resteaza~~ Atunci ~~d~~ fixam un astfel de element d , astfel pt. orice $d' \in R$ asociat cu divizibilitatea cu d , avem ~~si~~ $cd \neq d'$ este un c.m.m.d.c al lui a, b , deci $d \sim d' \Rightarrow (d) = (d')$, deci $(a) + (b) = (d')$ si aplicam (1) din teorema pt. d' .

Pe de altă parte, daca d'' este un alt c.m.m.d.c al lui a, b , atunci d'' trebuie sa fie asociat cu divizibilitatea cu d [intrebatorul, $d''|a, d''|b \Rightarrow d''|cd$, iar $d|a, d|b \Rightarrow d|d''$].

In consecinta multimesa tuturor c.m.m.d.c-ii lui a, b coincide cu multimesa elementelor asociate cu divizibilitatea cu d , adica $\{ud | u \in U(R)\}$.

In cazul $R = \mathbb{Z}$, acesta este $\{d, -d\}$, iar in cazul $R = K[x]$ este $\{cd | c \in K \setminus \{0\}\}$.

Acesta arata si ca pt. orice $a, b, d \in R$ avem $(a) + (b) = (d) \Leftrightarrow d$ este un c.m.m.d.c al lui a, b , si in plus, ca orice c.m.m.d.c d al lui a, b se scrie sub forma $d = xa + yb$ pt. niste $x, y \in R$.

Putem fixa un c.m.m.d.c pt. orice două elemente $a, b \in R$ nu ambele nule (decia un c.m.m.d.c este $\neq 0$)

(AR) 10

orice:

notăm $(a, b) = \begin{cases} \text{unicul c.m.m.d.c pozitiv, pt. } R = \mathbb{Z} \\ \text{unicul c.m.m.d.c monic, pt. } R = K[x]. \end{cases}$

Dacă $a = b = 0$, vom nota $(a, b) = 0$ (echivoc unicul c.m.m.d.c).

O discuție similară se poate face pt. c.m.m.m.c:

pt. orice $a, b \in R$ avem

$(a) \cap (b) = (m) \Leftrightarrow m$ este un c.m.m.m.c al lui $a \cap b$.

Dacă m este un c.m.m.m.c al lui $a \cap b$, atunci multimea tuturor c.m.m.m.c ei lui $a \cap b$ coincide cu multimea elementelor asociate în divizibilitate cu m . Dacă $a, b \neq 0$, atunci putem fixa un c.m.m.m.c al lui $a \cap b$, notat cu $[a, b]$, ce este unicul c.m.m.m.c pozitiv, din cazul $R = \mathbb{Z}$, sau unicul c.m.m.m.c monic, din cazul $R = K[x]$.

Dacă cel puțin unul dintre $a \cap b$ este nul, vom nota $[a, b] = 0$ (echivoc unicul c.m.m.m.c).

Definiție. Două elemente $a, b \in R$ se numesc relativ prime dacă $(a, b) = 1$.

Propozitie. Fie $a, b, c \in R \setminus \{0\}$. Atunci:

(i) $(a, b) = 1 \Leftrightarrow$ există $x, y \in R$ cu $x \cdot a + y \cdot b = 1$.

(ii) Dacă $(a, b) = d$, $a = da'$, $b = db'$, atunci $(a', b') = 1$.

(iii) $(ac, bc) \cap (a, b)c$ sunt asociate în divizibilitate.

(iv) $(a, c) = 1 \wedge (b, c) = 1 \Rightarrow (ab, c) = 1$.

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

Dem. (i) " \Rightarrow " Stim de la că orice c.m.m.d.c oricărui două elemente $a, b \in R$ este de forma $xa + yb$, cu $x, y \in R$.

Dacă $(a, b) = 1$, rezultă că există x, y cu $xa + yb = 1$.

" \Leftarrow " Fie $d = (a, b)$. Atunci $d \mid xa + yb = 1$, deci $d \mid 1$.

Cum $d > 0$ ($\forall t \cdot R = \mathbb{Z}$) sau d monic ($\forall t \cdot R = k[x]$), rezultă că $d = 1$.

(ii) Stim că $d = xa + yb$ pt. niste $x, y \in R$, și atunci $d = x'a'd + y'b'd$. Cum $d \neq 0$ (deoarece $a, b \neq 0$), obținem $x'a' + y'b' = 1$ și din (i) $\Rightarrow (a', b') = 1$.

(iii) Notăm $d = (a, b)$. Stim că $d = xa + yb$ pt. niste $x, y \in R$.

Atunci $dc = xac + ybc$, de unde $(ac, bc) \mid xac + ybc = dc$.

Pe de altă parte, $d \mid a$ și $d \mid b \Rightarrow d \mid ac$ și $d \mid bc$, de unde $d \mid (ac, bc)$.

Obținem că (ac, bc) și dc sunt asociate în divizibilitate.

$$\begin{aligned} (iv) \quad (a, c) = 1 &\Rightarrow \exists x_1, y_1 \in R \text{ cu } x_1 a + y_1 c = 1 \\ (b, c) = 1 &\Rightarrow \exists z, t \in R \text{ cu } z b + t c = 1 \end{aligned} \Rightarrow$$

$$\Rightarrow (x_1 a + y_1 c)(z b + t c) = 1 \Rightarrow x_1 z \underbrace{ab}_{\text{c}} + (x_1 t + y_1 z b + y_1 t c) \underbrace{c}_{=1} = 1$$

$$\Rightarrow (ab, c) = 1.$$

(v) Din (iii) stim că (ac, bc) este asociat în divizibilitate cu $(a, b)c = 1 \cdot c = c$, deci c e un c.m.m.d.c al elementelor ac și bc . Dar $a \mid ac$ și $a \mid bc$, de unde $a \mid c$.

Problema. Stim că orice două elemente $a, b \in R$ au un c.m.m.d.c. Cum se poate determina efectiv un astfel de c.m.m.d.c?

Teorema (Algoritmul lui Euclid) Fie $R = \mathbb{Z}$ sau $K[x]$ și fie $a, b \in R$, $b \neq 0$. Dacă $b \mid a$, atunci un c.m.m.d.c al elementelor a și b este b . Dacă $b \nmid a$, atunci:

- Împert a la b : $a = q_1 b + r_1$ (stîrnică $r_1 \neq 0$, pt că $b \nmid a$).
- Împert b la r_1 : $b = q_2 r_1 + r_2$ Dacă $r_2 = 0$, md opresc.
- Dacă $r_2 \neq 0$, împert r_1 la r_2 : $r_1 = q_3 r_2 + r_3$ Dacă $r_3 = 0$, md opresc.
- Dacă $r_3 \neq 0$, împert r_2 la r_3 : $r_2 = q_4 r_3 + r_4$ Dacă $r_4 = 0$, md opresc.
- și oare mai departe - - - - -

Atunci există n cu $r_n = 0$ (adică la un moment nos ne opresc)
și r_{n-1} este un c.m.m.d.c al elementelor a și b .

[Altă formulare: ultimul rest nenul din cînd sîr de împărțiri este un c.m.m.d.c al lui a și b].

Lemă. Dacă $u, v \in R$, $v \neq 0$ și $u = qv + r$ este împărțirea
lui u la v în R , atunci $(u, v) = (v, r)$.

Dem. Avem $(u, v) \mid v$ și $(u, v) \mid u - qv = r$, deci $(u, v) \mid (v, r)$.

Apoi $(v, r) \mid qv + r = u$ și $(v, r) \mid v$, deci $(v, r) \mid (u, v)$.

Rezultă că (u, v) și (v, r) sunt asociate în divizibilitate,
iar condiția impusă (> 0 în \mathbb{Z} , sau monic în $K[x]$) arată
 că sunt chiar egale.

Demonstrarea Teoremei. Presupunem prin absurd că $r_n \neq 0$ pt. oricăr. Atunci

- dacă $R = \mathbb{Z}$, avem $|b| > r_1 > r_2 > \dots$, un sîr infinit strict descrescător de numere naturale, contradicție.
- dacă $R = K[x]$, avem $\deg(b) > \deg(r_1) > \deg(r_2) > \dots$, tot un sîr infinit strict descrescător de numere naturale, contradicție.

Fie n primul nr natural pt. care $r_n = 0$ (unde algoritmul se opreste).

Din Lemă $\Rightarrow (a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-2}, r_{n-1})$. Dar

$$r_{n-2} = q_m r_{m-1} + r_m, \text{ deci } r_{m-1} \mid r_{n-2}, \text{ adică } (r_{n-2}, r_{m-1}) \text{ e asociat cu } r_{m-1}.$$

Observatie. Cu ajutorul algoritmului lui Euclid se poate obține și o reprezentare a lui (a, b) ca o combinație liniară de a și b . Într-adevăr,

$$a = q_1 b + r_1 \Rightarrow r_1 = a - q_1 b, \text{ o combinație liniară de } a \text{ și } b.$$

$$b = q_2 r_1 + r_2 \Rightarrow r_2 = b - q_2 r_1 \text{ și scriindu-l pe } r_1 \text{ ca o combinație liniară de } a \text{ și } b \text{ obținem o scriere similară pt. } r_2.$$

Continuând similar și la fiecare pas obținem o reprezentare a noului rest ca o combinație liniară de a și b , până ajungem la r_{m+1} .

Definiția c.m.m.d.c și c.m.m.m.c se poate extinde și la un număr finit de elemente. Astfel, dacă $n \in \mathbb{N}, n \geq 2$, și $a_1, \dots, a_n \in R$, atunci

- $d \in R$ se numește un c.m.m.d.c al elementelor a_1, \dots, a_n dacă $d | a_1, \dots, d | a_n$ și pt. orice d' cu $d' | a_1, \dots, d' | a_n$ avem $d' | d$.
- $m \in R$ se numește un c.m.m.m.c al elementelor a_1, \dots, a_n dacă $a_i | m, \dots, a_n | m$ și pt. orice m' cu $a_1 | m', \dots, a_n | m'$ avem $m | m'$.

Ca în cazul $n=2$, existența unui c.m.m.d.c și a unui c.m.m.m.c rezultă din Exercițiul următor, în felul că orice ideal este principal.

Exercițiu. Fie $a_1, \dots, a_n \in R$ și $d, m \in R$. Atunci

- (i) d este un c.m.m.d.c al lui a_1, \dots, a_n ($\Rightarrow (a_1) + \dots + (a_n) = (d)$).
- (ii) m este un c.m.m.m.c al lui a_1, \dots, a_n ($\Rightarrow (a_1) \cap \dots \cap (a_n) = (m)$).

Că o consecință, dacă d este un c.m.m.d.c al lui a_1, \dots, a_n , atunci orice element asociat în divizibilitate cu d este un c.m.m.d.c pt. a_1, \dots, a_n și orice c.m.m.d.c al lui a_1, \dots, a_n este asociat cu divizibilitatea cu d .

Vom nota cu (a_1, \dots, a_n) unicul c.m.m.d.c posibil (dacă $R=\mathbb{Z}$) sau monic (dacă $R=K[x]$), în cazul că nu toate a_i sunt nule, apoi $(0, 0, \dots, 0) = 0$.

Observații și convenții similare facem și pt. c.m.m.m.c.