

## Numeri prime și polinoame ireductibile

Vom lucra tot cu înțelele  $\mathbb{Z}$  și  $K[x]$ ,  $K$  corp comutativ.

Definiție. Un număr întreg  $p \neq 0$  se numește prim dacă  $p \neq 0, p \neq \pm 1$  și dacă  $p = ab$  cu  $a, b \in \mathbb{Z}$ , atunci unul dintre  $a$  și  $b$  este  $\pm 1$ .

(Formulare echivalentă:  $p$  este prim dacă  $p \neq 0, \pm 1$  și singurii divizori ai lui  $p$  sunt  $\pm 1$  și  $\pm p$ ).

Definiție. Un polinom  $P \in K[x]$  se numește ireductibil dacă  $P$  nu este constant (adică  $P \notin K$ ) și dacă  $P = AB$  cu  $A, B \in K[x]$ , atunci unul dintre  $A$  și  $B$  este constant (obligatoriu  $\neq 0$ ).

Observație. Înainte de cont că  $U(\mathbb{Z}) = \{1, -1\}$  și  $U(K[x]) = K \setminus \{0\}$ , cele două definiții sunt complet similare. Pentru fiecare divizor  $R = \mathbb{Z}$  sau  $R = K[x]$ , definiția consideră elemente  $p$  din  $R$  cu proprietatea că  $p \neq 0, p \notin U(R)$  și  $p = ab \Rightarrow a \in U(R)$  sau  $b \in U(R)$ .

Pt.  $R = \mathbb{Z}$  astfel de elemente  $p$  se numesc numere prime, iar pt.  $R = K[x]$  astfel de elemente  $p$  se numesc polinoame ireductibile.

Un număr întreg  $n \neq 0, \pm 1$  care nu este prim se numește număr compus.

Un polinom  $f \in K[x]$ ,  $f$  neconstant, care nu este ireductibil se numește polinom reductibil.

Propozitie. Fie  $P \in K[x]$ , unde  $K$  este corp comutativ. Atunci:

- (1) Dacă  $\deg P = 1$ , atunci  $P$  este ireductibil.
- (2) Dacă  $\deg P \geq 2$  și  $P$  are o rădăcină în  $K$ , atunci  $P$  este redusabil.
- (3) Dacă  $\deg P \in \{2, 3\}$ , atunci  $P$  este redusabil ( $\Rightarrow P$  nu are nicio rădăcină în  $K$ ).

Dem. (1)  $P = AB$  cu  $A, B \in K[x] \Rightarrow 1 = \deg P = \deg A + \deg B \Rightarrow$   
 $\Rightarrow \deg A = 0$  sau  $\deg B = 0$ , deci unul dintre  $A$  și  $B$  este constant.

(2) Fie  $\deg P \geq 2$ . Dacă  $P$  are rădăcina  $a \in K$ , din teorema lui Bézout  $x-a \mid P$ , deci există  $F \in K[x]$  cu  $P = (x-a) \cdot F$ . Cum  $\deg P \geq 2$ , rezultă că  $\deg F \geq 1$ , deci  $F$  nu este constant. Aceasta rezultă că  $P$  este redusabil (este produs de două polinoame neconstante).

(3) " $\Rightarrow$ " rezultă din (2).

" $\Leftarrow$ " Presupunem că  $P$  nu are rădăcini în  $K$ . Arătăm că  $P$  este redusabil. Într-adevăr, atfel ar exista  $A, B \in K[x]$  neconstante cu  $P = AB$ . Din  $\deg P = \deg A + \deg B$ , în ambele cazuri  $\deg P = 2$  sau  $\deg P = 3$  rezultă că unul dintre  $\deg A$  și  $\deg B$  este 1, și atunci unul dintre  $A$  și  $B$  are o rădăcină în  $K$ ; acesta este rădăcină și pt.  $P$ , contradicție. Rezultă că  $P$  este redusabil.

---

Observație Dacă  $\deg P > 3$ , stim din (2) că  $P$  este redusabil ( $\Rightarrow P$  nu are nicio rădăcină în  $K$ ). Reciproc nu mai este adeverit; de exemplu  $P = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$  nu are nicio rădăcină în  $\mathbb{Q}$ , dar este redusabil.

Propozitie. Fie  $R = \mathbb{Z}$  sau  $R = K[x]$ , cu  $K$  corp comutativ, și fie  $p \in R$  un element nemul și neînversabil. Atunci p este prim (în cazul  $R = \mathbb{Z}$ ) sau ireductibil (în cazul  $R = K[x]$ ) dacă și numai dacă pt. orice  $a, b \in R$  cu  $p \mid ab$  avem  $p \mid a$  sau  $p \mid b$ .

Dem. Presupunem că  $p$  este prim (în cazul  $R = \mathbb{Z}$ ) sau ireductibil (în cazul  $R = K[x]$ ) și fie  $a, b \in R$  cu  $p \mid ab$ . Dacă  $p \nmid a$ , fie  $d = (p, a)$ . Atunci  $p = dp'$  pt. un  $p' \in R$  și din definițiele elementelor prime (în  $\mathbb{Z}$ ) și a polinoamelor ireductibile (în  $K[x]$ ), rezultă că  $d$  este înversabil sau  $p$  este înversabil. În fel acesta  $d$  este asociat cu  $p$ , de unde ar rezulta că  $p \mid a$ , contradicție. Așadar  $d$  este înversabil și atunci  $d = 1$  (cum  $d = (p, a)$ , el e posibil în cazul  $R = \mathbb{Z}$  să nu văd în cazul  $R = K[x]$ ). Obținem că  $(p, a) = 1$ . Atunci cum  $p \mid ab$ , din  $(\vee)d$  rezultă că de la  $p \mid ab$ , rezultă că  $p \mid b$ .

Reciproc, presupunem că pt. orice  $a, b \in R$  cu  $p \mid ab$  avem  $p \mid a$  sau  $p \mid b$ . Fie atunci  $p = ab$  cu  $a, b \in R$ . Atunci  $p \mid ab$ , deci  $p \mid a$  sau  $p \mid b$ . Dacă  $p \mid a$ , atunci  $a = p \times$  pt. un  $x \in R$ , de unde  $p = p \times b$ , deci  $x \in b = 1$  și obținem că  $b$  este înversabil. Similar, dacă  $p \mid b$ , rezultă că  $a$  este înversabil.

Teorema. (1) Fie  $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ . Atunci  $a$  se poate scrie ca produs de numere prime. În plus, această scriere este unică în sensul că  $\frac{a}{p_1 \cdots p_n} = p'_1 \cdots p'_m$  cu  $n, m \in \mathbb{N}^*$  și  $p_1, \dots, p_n, p'_1, \dots, p'_m$  prime, atunci  $n = m$  și există o permutare  $\sigma \in S_m$  astfel încât  $p_i \sim p'_{\sigma(i)}$  pt. orice i. (adică factorii primi din cele două descompuneri sunt asociati în divizibilitatea în perechi).

(2) Fie  $f \in K[X]$  cu  $\deg(f) \geq 1$ , unde  $K$  este corp comunitativ. Atunci  $f$  se poate scrie ca produs de polinoame irreductibile. În plus, această scriere este unică în sensul că dacă  $f = P_1 \cdots P_n = P'_1 \cdots P'_m$  cu  $n, m \in \mathbb{N}^*$  și  $P_1, \dots, P_n, P'_1, \dots, P'_m$  polinoame irreductibile, atunci  $n = m$  și există o permutare  $\sigma \in S_m$  astfel încât  $P_i \sim P'_{\sigma(i)}$  pt. orice  $1 \leq i \leq n$ .

Demonstratie. Demonstrem moi întâi partesele de existență a scrierii.

(1) (pt. Z) Presupunem prin absurd că nu toate numerele naturale  $\geq 2$  se pot scrie ca produs de prime.

Ebe atunci  $a$  cel mai mic nr. natural  $\geq 2$  care nu se poate scrie ca produs de prime. În particular  $a$  nu este prim (altfel ar fi un produs de prime cu un singur factor), deci  $a = bc$  pt. niste  $b, c \in \mathbb{N}$ ,  $b, c \geq 2$ .

Cum  $b < a$  și  $c < a$ , minimulitatea lui  $a$  garantă că  $b$  și  $c$  se pot scrie ca produse de prime, și atunci și  $bc = a$  e un produs de prime, contradicție.

Obținem astfel că orice  $a \in \mathbb{N}$ ,  $a \geq 2$  e produs de prime.

Atunci  $\exists$  clor  $c \in \mathbb{Z}$ ,  $a \in \mathbb{Z}$ ,  $a \leq -2$ ,  $\exists$  produs de prime, deoarece  $-a \in \mathbb{N}$  și  $-a \geq 2$ , deci  $-a$  este produs de prime, iar pt. un prim p natural, avem că  $\exists$   $-p$  este prim în  $\mathbb{Z}$ .

(2) (pt.  $K[x]$ ). Presupunem numărul de grade  $\deg f$  este produs de polinoame irreductibile. Fie atunci  $f$  un polinom de grad minim posibil, unde cele care nu se pot scrie ca produs de polinoame irreductibile. În particular,  $f$  nu este polinom irreductibil, deci există  $g, h \in K[x]$  de grade  $\geq 1$ , cu  $f = gh$ . Atunci  $\deg g < \deg f$ , și minimalitatea gradului lui  $f$  arată că  $g \mid h$  și  $h$  se pot scrie ca produs de polinoame irreductibile. Obținem că  $\exists$   $g, h \in K[x]$  de grade  $\geq 1$  cu  $gh = f$  este produs de polinoame irreductibile, contradicție.

Pentru porția de unicitate dăm demonstrație comună  
pt. (1) și (2). Arătăm că  $\exists$   $p_1 \cdots p_n = p'_1 \cdots p'_m$ ,

unde  $n, m \in \mathbb{N}^*$  și  $p_1, \dots, p_n, p'_1, \dots, p'_m$  sunt prime din  $\mathbb{Z}$  sau polinoame irreductibile din  $K[x]$ , atunci  $n = m$  și există  $\sigma \in S_m$  cu  $p_i = p'_{\sigma(i)}$  pt. orice  $1 \leq i \leq n$ .

Demonstrăm prin inducție după  $n$ .

Pt.  $n=1$ , avem  $p_1 = p'_1 \cdots p'_m$ . Dacă  $m \geq 2$ , em avem  $p_1 = p'_1 (p'_2 \cdots p'_m)$  și cum  $p_1$  e prim (resp. irreductibil),

em ~~obține~~ obține că  $p'_1$  e inversabil sau  $p'_2 \cdots p'_m$  inversabil (de unde  $\exists p'_2$  e inversabil), contradicție.  
Aseadar  $m=1$  și  $p_1 = p'_1$ .

(AR)

(19)

Presupunem că există  $p_{n+1}$  și demonstrăm că  $n$  (inducentă)

Din  $p_1 \cdots p_m = p'_1 \cdots p'_{m'}$  obținem că  $p_n \mid p'_1 \cdots p'_{m'}$ . Cum  $p_n$  e prim (resp. polinom ireductibil), rezultă că există  $1 \leq j \leq m'$  cu  $p_n \mid p'_j$ . Atunci  $p'_j = p_n \cdot x$  pt. un  $x \in K$ .

Cum  $p_n$  nu este inversibil, rezultă că  $x$  este inversibil, în particular  $p_n \sim p'_j$ . Apoi  $p_i \cancel{\sim} p'_i$ .

$$p'_1 \cdots p'_{m'} = p'_1 \cdots p'_{j-1} p_n \cancel{\sim} p'_{j+1} \cdots p'_{m'} \text{ și simplificând cu } p_n \text{ din}$$

$$p_1 \cdots p_m = p'_1 \cdots p'_{m'} \text{ obținem } p_1 \cdots p_{n-1} = (\cancel{x} p'_1) p'_2 \cdots p'_{j-1} p'_{j+1} \cdots p'_{m'}$$

[decid cumva  $j=1$ , membrul drept va fi  $(\cancel{x} p'_1) p'_2 \cdots p'_{m'}$ ].

Cum  $\cancel{x} p'_i \sim p'_i$ , avem că  $\cancel{x} p'_i$  e prim (resp. pol. ireductibil) și aplicând ipoteza de inducție ultimei epedalări, obținem că  $n-1 = m-1$  (deci  $n=m$ ) și există o bijectie  $\beta: \{1, \dots, n-1\} \rightarrow \{1, \dots, m\} \setminus \{j\}$  pentru care

$p_i \sim p'_{\beta(i)}$  pt. orice  $1 \leq i \leq n-1$ . Observăm că numerele sunt aici de forma  $\cancel{x} p'_i \sim p'_i$ , deci decid un

$p_i \sim \cancel{x} p'_i$ , atunci avem și  $p_i \sim p'_i$ . Atunci funcție

$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ ,  $\sigma(i) = \beta(i)$  pt.  $1 \leq i \leq n-1$  și

$\sigma(n)=j$ , este bijectivă, deci  $\sigma \in S_n$  și  $p_i \sim p'_{\sigma(i)}$  pt. orice  $1 \leq i \leq n$ , ceea ce aduce demonstrație.

Baza inducției

Observație (1) Orice număr din  $\mathbb{Z}$  este de forma  $p$  sau  $-p$ , cu  $p$  număr natural nenul.

(2) Orice polinom ireductibil din  $K[x]$  este de formă

$c \neq 0$ , unde  $c \in K \setminus \{0\}$  și  $f$  este polinom ireductibil monic.

(3) Dacă  $p$  și  $p'$  sunt numere naturale prime (respectiv polinoame ireductibile monice), atunci  $p \sim p'$  dacă și numai dacă  $p = p'$ .

O consecință imediată a Teoremei și Observației precedente este:

Teoremă. (i) Fie  $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ . Atunci  $a$  se poate scrie

sub forma  $a = \varepsilon \cdot p_1^{x_1} \cdots p_r^{x_r}$ , cu  $\varepsilon \in \{-1\}$ ,  $p_i \in \mathbb{N}^*$ ,   
  $p_1, \dots, p_r$  numere naturale prime și  $x_1, \dots, x_r \in \mathbb{N}^*$ .

Mai mult, această scriere este unică, în sensul că

$$a = \varepsilon p_1^{x_1} \cdots p_r^{x_r} = \eta q_1^{\beta_1} \cdots q_s^{\beta_s} \quad (\text{unde } \eta \in \{-1\}, \eta \in \mathbb{N}^*)$$

$q_1, \dots, q_s$  numere naturale prime și  $\beta_1, \dots, \beta_s \in \mathbb{N}^*$ ) implică

$\varepsilon = \eta$ ,  $r = s$  și există o permutare  $\sigma \in S_r$  cu  $p_i = q_{\sigma(i)}$  și  $x_i = \beta_{\sigma(i)}$  pentru  $1 \leq i \leq r$ .

(2) Fie  $f \in K[x]$  cu  $\deg(f) \geq 1$ . Atunci  $f$  se poate scrie

sub forma  $f = c p_1^{x_1} \cdots p_r^{x_r}$ , cu  $c \in K \setminus \{0\}$ ,  $r \in \mathbb{N}^*$ ,

$p_1, \dots, p_r$  polinoame ireductibile monice și  $x_1, \dots, x_r \in \mathbb{N}^*$ .

Mai mult, această scriere este unică, în sensul că

$$f = c p_1^{x_1} \cdots p_r^{x_r} = d q_1^{\beta_1} \cdots q_s^{\beta_s} \quad (\text{unde } c \in K \setminus \{0\}, s \in \mathbb{N}^*)$$

$q_1, \dots, q_s$  polinoame ireductibile monice și  $\beta_1, \dots, \beta_s \in \mathbb{N}^*$ )

implică  $c = d$ ,  $r = s$  și există  $\sigma \in S_r$  cu  $p_i = q_{\sigma(i)}$  și

$$x_i = \beta_{\sigma(i)} \text{ pt. orice } 1 \leq i \leq r.$$

(AR)

(21)

Lemă. (1) Fie  $a \in \mathbb{Z} \setminus \{0, 1, -1\}$  și  $a = \epsilon P_1^{\alpha_1} \cdots P_n^{\alpha_n}$  descompunerea lui  $a$  ca din Teorema precedentă,(1). Atunci divizorii întregi ai lui  $a$  sunt numerele de forma  $N P_1^{\beta_1} \cdots P_n^{\beta_n}$ , cu  $\nu \in \{-1, 0, 1\}$  și  $\beta_1, \beta_2 \in \mathbb{N}$  cu  $\beta_i \leq \alpha_1, \dots, \beta_n \leq \alpha_n$ .

(2) Fie  $f \in K[x]$  cu  $\deg(f) \geq 1$  și  $f = c P_1^{\alpha_1} \cdots P_n^{\alpha_n}$  descompunerea lui  $f$  ca din Teorema precedentă,(2). Atunci divizorii lui  $f$  din  $K[x]$  sunt polinoamele de forma  $d P_1^{\beta_1} \cdots P_n^{\beta_n}$ , cu  $d \in K \setminus \{0\}$  și  $\beta_1, \beta_2 \in \mathbb{N}$  cu  $\beta_i \leq \alpha_1, \dots, \beta_n \leq \alpha_n$ .

Dem. (1) Este clar că un număr de forme  $N P_1^{\beta_1} \cdots P_n^{\beta_n}$  ce împart este divizor al lui  $a$ , deoarece

$$a = (N P_1^{\beta_1} \cdots P_n^{\beta_n})(\epsilon N P_1^{\alpha_1} \cdots P_n^{\alpha_n}) \quad [\text{folosind } N^2 = 1].$$

Așadar că orice divizor este de acestă formă.

Fie  $x \in \mathbb{Z}$  cu  $x \mid a$ . Atunci există  $y \in \mathbb{Z}$  cu  $a = xy$ .

Dacă este un număr natural pentru care  $p \nmid xy$ , atunci  $p \mid a = \epsilon P_1^{\alpha_1} \cdots P_n^{\alpha_n}$ , deci  $p \mid p_i$  pt. un  $1 \leq i \leq n$ , și atunci  $p = p_i$ . Așadar fiecare divizor  $x \mid y$  este sau  $\pm 1$ , sau în descompunerea lor ca din Teorema (1) sau că primele dintre  $p_1, \dots, p_n$ . Așadar  $x = N P_1^{\beta_1} \cdots P_n^{\beta_n}$  și  $y = \frac{a}{x} = P_1^{\alpha_1} \cdots P_n^{\alpha_n}$  pt. multă  $N, \alpha_i \in \{-1, 0, 1\}$  și  $\beta_1, \beta_2, \alpha_1, \dots, \alpha_n \in \mathbb{N}$ . (cazul  $x = \pm 1$  rezine că  $\beta_1 = \dots = \beta_n = 0$ ). Obținem că

$\epsilon P_1^{\alpha_1} \cdots P_n^{\alpha_n} = a = xy = N P_1^{\beta_1} \cdots P_n^{\beta_n} \cdot P_1^{\alpha_1 + \gamma_1} \cdots P_n^{\alpha_n + \gamma_n}$  și, deoarece de unicitatea reprezentării din Teorema (1), obținem că

$\beta_1 + \gamma_1 = \alpha_1, \dots, \beta_n + \gamma_n = \alpha_n$ , de unde  $\beta_1 \leq \alpha_1, \dots, \beta_n \leq \alpha_n$ .

(2) se dovedește fel ca (1).

Dacă avem la dispoziție descompunerile ca produs de numere prime (polinoame ireductibile) ale două numere întregi (polinoame din  $K[x]$ ), putem calcula c.m.m.d.c și c.m.m.m.c al lor ca în următorul rezultat.

Propozitie. (1) Fie  $a = \epsilon p_1^{\alpha_1} \cdots p_n^{\alpha_n}$  și  $b = \eta p_1^{\beta_1} \cdots p_n^{\beta_n}$  două numere întregi nenule, unde  $\epsilon, \eta \in \{-1, 1\}$ ,  $\alpha_i, \beta_i \in \mathbb{N}$  și,   
 $p_1, \dots, p_n$  numere naturale prime și  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{N}$  distincte.  
(Observație: e posibil ca factorii primi să îlui a să nu coincida cu factorii primi să îlui b; în scrierile de mai sus  $p_1, \dots, p_n$  sunt toti factorii primi pozitive distincti care apar în cel puțin unul dintre a și b, și permisam ca  $\alpha_i, \beta_i$  să fie 0, cind factorul  $p_i$  nu apare în  $a$  sau  $b$ ).

Așunci

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_n^{\min(\alpha_n, \beta_n)} \neq 0$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdots p_n^{\max(\alpha_n, \beta_n)}.$$

(2). Fie  $f = c p_1^{\alpha_1} \cdots p_n^{\alpha_n}$  și  $g = d p_1^{\beta_1} \cdots p_n^{\beta_n}$  două polinoame nenule din  $K[x]$ , unde  $c, d \in K \setminus \{0\}$ ,  $\alpha_i, \beta_i \in \mathbb{N}$ ,  $p_1, \dots, p_n$  polinoame ireductibile monice distincte și  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{N}$ .

Așunci

$$(f, g) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_n^{\min(\alpha_n, \beta_n)} \neq 0$$

$$[f, g] = p_1^{\max(\alpha_1, \beta_1)} \cdots p_n^{\max(\alpha_n, \beta_n)}.$$

Demonstrare. Demonstrația (1); (2) se face similar.

Cum  $\min(x_i, \beta_i) \leq x_i \leq \max(x_i, \beta_i)$  pt. orice  $1 \leq i \leq r$ , rezultă din lemea precedentă că  $\frac{\min(x_1, \beta_1)}{P_1} \cdots \frac{\min(x_r, \beta_r)}{P_r} \mid a \text{ și}$

$$a \nmid P_1 \quad \cdots \quad P_r \quad ; \text{ similar } \frac{\min(x_1, \beta_1)}{P_1} \cdots \frac{\min(x_r, \beta_r)}{P_r} \mid b \text{ și}$$

$$b \nmid P_1 \quad \cdots \quad P_r$$

Așadar  $\frac{\min(x_1, \beta_1)}{P_1} \cdots \frac{\min(x_r, \beta_r)}{P_r}$  este divizor comun al lui  $a$  și  $b$ ; în plus, din lemea precedentă orice alt divizor comun al lui  $a$  și  $b$  este de formă  $\frac{s_1}{P_1} \cdots \frac{s_r}{P_r}$  cu  $s_i \in \{-1, 1\}$  și

$s_1, \dots, s_r \in \mathbb{N}$  cu  $s_i \leq x_i$  și  $s_i \leq \beta_i$  pt. orice  $i$ , ceea ce

$$s_i \leq \min(x_i, \beta_i). \text{ Obținem că } \frac{s_1}{P_1} \cdots \frac{s_r}{P_r} \mid \frac{\min(x_1, \beta_1)}{P_1} \cdots \frac{\min(x_r, \beta_r)}{P_r},$$

$$\text{de unde } \frac{\min(x_1, \beta_1)}{P_1} \cdots \frac{\min(x_r, \beta_r)}{P_r} = (a, b).$$

De exemplu,  $\frac{\max(x_1, \beta_1)}{P_1} \cdots \frac{\max(x_r, \beta_r)}{P_r}$  este multiplu comun al lui  $a$  și  $b$ ; în plus, orice alt multiplu comun al lui  $a$  și  $b$  trebuie să fie de formă  $\theta \frac{s_1}{P_1} \cdots \frac{s_r}{P_r} \cdot M$ , unde  $\theta \in \{-1\}$ ,  $s_1, \dots, s_r \in \mathbb{N}$  cu  $x_i \leq s_i \leq \beta_i \leq s_i$  pt. orice  $1 \leq i \leq r$ , iar  $M \geq 1$  sau  $M = \prod$  produs de puteri de prime differente de  $P_1, \dots, P_r$ . Atunci  $\max(x_i, \beta_i) \leq s_i$ ,

$$\text{de unde } \frac{\max(x_1, \beta_1)}{P_1} \cdots \frac{\max(x_r, \beta_r)}{P_r} \mid \theta \frac{s_1}{P_1} \cdots \frac{s_r}{P_r} M, \text{ ceea ce}$$

$$\frac{\max(x_1, \beta_1)}{P_1} \cdots \frac{\max(x_r, \beta_r)}{P_r} = [a, b].$$

Observație. Faptul că  $[a, b] = \frac{\max(x_1, \beta_1)}{P_1} \cdots \frac{\max(x_r, \beta_r)}{P_r}$  nu este o proprietate unică.

Se poate demonstra și folosind că  $(a, b) \cdot [a, b] = ab$  și

în plus că  $x_i + \beta_i - \min(x_i, \beta_i) = \max(x_i, \beta_i)$  pt.

orice  $1 \leq i \leq r$ .

Teorema. (1) Multimea numerelor naturale prime este infinită.

(2) Multimea polinoamelor irreductibile monice din  $K[x]$ , unde  $K$  este corp comutativ, este infinită.

### Demonstrare

(1) Presupunem prin absurd că ar exista doar un număr finit de numere naturale prime,

fie acestea  $p_1, \dots, p_n$ . Fie  $a = 1 + p_1 \cdots p_n$ , care este un număr natural  $> 1$ . Atunci  $a$  este produs de numere prime, deci există  $i$  cu  $p_i | a$ , și atunci  $p_i | a - p_1 \cdots p_n = 1$ , contradicție cu  $p_i$  prim.

(2) Presupunem prin absurd că există doar un număr finit de polinoame irreductibile monice, fie acestea  $P_1, \dots, P_m$ . Atunci  $f = 1 + P_1 \cdots P_m$  este un polinom de grad  $\geq 0$ , deci este produs de polinoame irreductibile monice și o constantă, de unde există  $i$  cu  $P_i | f$ . Atunci

$P_i | f - P_1 \cdots P_m = 1$ , contradicție cu  $\deg(P_i) \geq 1$ .

Observăm că în cazul în care  $K$  este corp infinit, o demonstrație imediată la (2) este următoarea:

$x-a$  este polinom irreductibil monic pt. orice  $a \in K$  și există o infinitate de astfel de polinoame.