(ii) (21)

Dem. Definim ~~$\varphi: A[X] \to B$ prin~~ $\overline{\varphi}: A[X] \to B$ prin
$$\overline{\varphi}(a_0 + a_1X + \dots + a_nX^n) = \varphi(a_0) + \varphi(a_1)b + \dots + \varphi(a_n)b^n.$$

Arătăm că $\overline{\varphi}$ are proprietățile cerute.

- $\overline{\varphi}(f+g) = \overline{\varphi}(f) + \overline{\varphi}(g)$ pt. orice $f, g \in A[X]$.

Scriem ~~$f = a_0 + \dots + a_nX$~~ f și g de aceeași lungime (completând eventual cu zerouri)

$f = a_0 + a_1X + \dots + a_nX^n$, $g = c_0 + c_1X + \dots + c_nX^n$. Atunci
$$\begin{aligned}
\overline{\varphi}(f+g) &= \overline{\varphi}\big((a_0+c_0) + (a_1+c_1)X + \dots + (a_n+c_n)X^n\big)\\
&= \varphi(a_0+c_0) + \varphi(a_1+c_1)b + \dots + \varphi(a_n+c_n)b^n\\
&= \varphi(a_0) + \varphi(c_0) + (\varphi(a_1)+\varphi(c_1))b + \dots + (\varphi(a_n)+\varphi(c_n))b^n\\
&= \big(\varphi(a_0) + \varphi(a_1)b + \dots + \varphi(a_n)b^n\big) + \big(\varphi(c_0) + \varphi(c_1)b + \dots + \varphi(c_n)b^n\big)\\
&= \overline{\varphi}(a_0 + a_1X + \dots + a_nX^n) + \overline{\varphi}(c_0 + c_1X + \dots + c_nX^n)\\
&= \overline{\varphi}(f) + \overline{\varphi}(g).
\end{aligned}$$

- $\overline{\varphi}(fg) = \overline{\varphi}(f)\overline{\varphi}(g)$ pt. orice $f, g \in A[X]$.

Fie acum $f = \sum_{i=\overline{0,n}} a_iX^i$, $g = \sum_{j=\overline{0,m}} c_jX^j$ (nu mai e nevoie să luăm neapărat scrieri de aceeași lungime).

Atunci $\overline{\varphi}(fg) = \overline{\varphi}\Big(\sum_{k=\overline{0,m+n}} \Big(\sum_{i+j=k} a_ic_j\Big)X^k\Big)$
$$= \sum_{k=\overline{0,m+n}} \varphi\Big(\sum_{i+j=k} a_ic_j\Big)b^k, \text{ iar}$$

(ip) (22)

$$\overline{\varphi}(f)\,\overline{\varphi}(g)=\Big(\sum_{i=\overline{0,n}}\varphi(a_i)b^i\Big)\Big(\sum_{j=\overline{0,m}}\varphi(c_j)b^j\Big)$$

$$=\sum_{\substack{i=\overline{0,n}\\ j=\overline{0,m}}}\varphi(a_i)\varphi(c_j)\,b^{i+j}$$

$$=\sum_{h=\overline{0,m+n}}\Big(\sum_{i+j=h}\varphi(a_i)\varphi(c_j)\Big)b^h$$

$$\xlongequal[\text{inele}]{\varphi\text{ morfism}}\sum_{h=\overline{0,m+n}}\varphi\Big(\sum_{i+j=h}a_ic_j\Big)b^h,$$

de unde $\overline{\varphi}(fg)=\overline{\varphi}(f)\overline{\varphi}(g)$.

- $\overline{\varphi}(1)=1$, clar.

Așadar $\overline{\varphi}$ este morfism de inele. În plus, este clar că $\overline{\varphi}(a)=\varphi(a)$ pt. orice $a\in A$ și $\overline{\varphi}(X)=\varphi(1)b=b$.

Arătăm că $\overline{\varphi}$ e unic cu aceste proprietăți. Într-adevăr, dacă $F:A[X]\to B$ ar fi un alt morfism de inele cu $F(a)=\varphi(a)$ pt. orice $a\in A$ și $F(X)=b$, atunci

$$F(a_0+a_1X+\dots+a_nX^n)=F(a_0)+F(a_1)F(X)+\dots+F(a_n)F(X)^n$$
$$=\varphi(a_0)+\varphi(a_1)b+\dots+\varphi(a_n)b^n=\overline{\varphi}(a_0+a_1X+\dots+a_nX^n),$$

deci $F=\overline{\varphi}$ și demonstrația este încheiată.

1p 23

Fie A inel comutativ, $f=a_0+a_1X+\dots+a_nX^n\in A[X]$ și B un inel comutativ astfel încât A e subinelul lui B.

Dacă $x\in B$, atunci elementul $a_0+a_1x+\dots+a_nx^n\in B$, notat cu $f(x)$, se numește valoarea lui f în x.

Observăm că dacă aplicăm Proprietatea de universalitate

$$\begin{tikzcd} A \arrow[r, hook] \arrow[dr, "\varphi"'] & A[X] \arrow[d, dashed, "\bar\varphi"] \\ & B \end{tikzcd}$$

pt. φ = morfismul incluziune al lui A în B (adică $\varphi(a)=a\ \forall a\in A$) și elementul $x\in B$, atunci

$$\bar\varphi(f)=f(x) \text{ pt. orice } f\in A[X].$$

Cum $\bar\varphi$ e morfism de inele, rezultă că

$$(f+g)(x)=f(x)+g(x) \text{ și } (fg)(x)=f(x)g(x)$$

pt. orice polinoame $f,g\in A[X]$.

$\bar\varphi$ s.n. morfismul evaluare în x.

Def. Fie $f\in A[X]$, $f\neq 0$. Atunci un element $a\in A$ se numește *rădăcină a lui f* dacă $f(a)=0$.

Mai general, dacă B este inel comutativ și A este subinel al lui B, un element $x\in B$ se numește *rădăcină în B a lui f* dacă $f(x)=0$.

Observație Dacă $A\subset B$ inele comutative și $f\in A[X]$, atunci putem privi pe f și ca pe un element din $B[X]$, deoarece $A[X]$ e subinel în $B[X]$.

Astfel, o rădăcină $x\in B$ a lui f în B este exact o rădăcină a lui f atunci când e privit ca polinom în $B[X]$.

ip 24

<u>Teorema împărțirii cu rest pt. polinoame</u>. Fie A un inel comutativ și fie $f, g \in A[X]$ astfel încât $g \neq 0$ și coeficientul dominant al lui g este element inversabil al lui A. Atunci există și sunt unice $q, r \in A[X]$ astfel încât

$$f = q g + r \quad \text{și} \quad \deg(r) < \deg(g).$$

<u>Dem</u>. <u>Existența</u>: Dacă $\deg(f) < \deg(g)$, luăm $q = 0$ și $r = f$.

Fie $\deg(f) \geq \deg(g)$. Demonstrăm prin inducție după $\deg(f)$. [presupunând g fixat de grad m].

Dacă $\deg(f) = \deg(g)$, fie $f = a_m X^m + \dots + a_0$ și $g = b_m X^m + \dots + b_0$, cu $a_m \neq 0$ și b_m inversabil; atunci $f - b_m^{-1} a_m g$ are grad $< m$ (deoarece coeficientul lui X^m este $a_m - b_m^{-1} a_m b_m = 0$) și $f = b_m^{-1} a_m g + (f - b_m^{-1} a_m g)$. Luăm $q = b_m^{-1} a_m$ și $r = f - b_m^{-1} a_m g$, gata!

Pt. pasul de inducție, fie $n > \deg(g)$ și presupunem afirmația adevărată pt. orice f cu $\deg(f) < n$. Demonstrăm că e adevărată și pt. $\deg(f) = n$. Fie $f = a_n X^n + \dots + a_0$, cu $a_n \neq 0$. Atunci $f - b_m^{-1} a_n X^{n-m} g$ are grad $< n$ (la fel ca mai sus, coeficientul lui X^n este 0) și din ipoteza de inducție (plus observația inițială pt. deg < deg(g) = m) rezultă că există $q_0, r_0 \in A[X]$

cu $\deg(r_0) < \deg(g)$ și $f - b_m^{-1} a_n X^{n-m} g = q_0 g + r$,

de unde $f = (b_m^{-1} a_n X^{n-m} + q_0) g + r_0$.

Luăm $q = b_m^{-1} a_n X^{n-m} + q_0$ și $r = r_0$, gata!

<u>Unicitatea</u>: Presupunem că $f = q_1 g + r_1 = q_2 g + r_2$

cu $\deg(r_1), \deg(r_2) < \deg(g)$. Atunci $(q_1 - q_2) g = r_2 - r_1$

și cum $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(g)$,

obținem $\deg((q_1 - q_2) g) < \deg(g)$. Dacă $q_1 - q_2 \neq 0$,

atunci cum coeficientul dominant al lui g e inversabil,

rezultă că $\deg((q_1 - q_2) g) = \deg(q_1 - q_2) + \deg(g)$

[într-adevăr, luând $q_1 - q_2 = \alpha_h X^h + \dots$, $g = b_m X^m + \dots$, cu $\alpha_h \neq 0$,

avem $(q_1 - q_2) g = \alpha_h b_m X^{h+m} + \dots$ și $\alpha_h b_m \neq 0$, deoarece

b_m e inversabil și $\alpha_h \neq 0$],

de unde $\deg((q_1 - q_2) g) \geq \deg(g)$, contradicție.

Așadar $q_1 - q_2 = 0$, adică $q_1 = q_2$ și atunci și

$r_1 = r_2 = f - q_1 g$.

<u>Terminologie</u>. Cu notațiile ca în Teoremă, q și r

se numesc câtul și restul împărțirii

lui f la g.

Exercițiu. Dacă $f = X^2$, $g = 2X \in \mathbb{Z}[X]$, atunci nu există $q, r \in \mathbb{Z}[X]$ cu $\deg(r) < \deg(g)$ și $f = qg + r$. Așadar condiția de inversabilitate a coeficientului dominant al lui g din teoremă nu poate fi eliminată.

Def. Fie $f, g \in A[X]$, unde A e inel comutativ. Spunem că g divide pe f (scriem $g \mid f$) dacă există $h \in A[X]$ cu $f = gh$.

Corolar (Teorema lui Bézout). Fie A inel comutativ, $f \in A[X]$ și $a \in A$. Atunci restul împărțirii lui f la polinomul $X-a$ este polinomul constant $f(a)$.

În particular, a este rădăcină a lui f dacă și numai dacă $(X-a) \mid f$.

Dem. Fie $f = q\cdot(X-a) + r$ împărțirea cu rest a lui f la $X-a$ (observăm că $X-a$ are coeficient dominant 1, care e inversabil). Atunci $\deg(r) < \deg(X-a) = 1$, deci r e polinom constant, adică $r \in A$. Evaluăm în a (adică aplicăm morfismul evaluare în a, $\bar{\varphi}: A[X] \to A$) și obținem $f(a) = r$ [deoarece clar $\bar{\varphi}(X-a) = a-a = 0$].

ip 27

<u>Observație</u>. Partea finală a Teoremei lui Bézout se poate reformula astfel: mulțimea polinoamelor din $A[X]$ care au rădăcina a este exact idealul principal generat de $X-a$ în $A[X]$.

<u>Exerciții</u>.

① Fie I și J ideale în inelul comutativ R astfel încât $I+J=R$. Să se arate că $I\cap J=IJ$. Folosind apoi Lema chineză a resturilor, deduceți că

$$\frac{R}{IJ}\simeq\frac{R}{I}\times\frac{R}{J}.$$

② Fie A un inel comutativ și $a\in A$. Să se arate că există un izomorfism de inele $\frac{A[X]}{(X-a)}\simeq A$.

③ Să se arate că $\frac{\mathbb{R}[X]}{(X^2-1)}\simeq\mathbb{R}\times\mathbb{R}$. (izo de inele).

(indicație: folosiți ① și ②).

④ Considerăm inelul factor $\frac{\mathbb{Z}[X]}{(X^2-1)}$, în care notăm cu $\widehat{f}$ clasa lui f, unde $f\in\mathbb{Z}[X]$.

(i) Dacă $I=(X-1)$ și $J=(X+1)$, arătați că $I+J\neq\mathbb{Z}[X]$.

(ii) Arătați că $\frac{\mathbb{Z}[X]}{(X^2-1)}=\{\widehat{a+bX}\mid a,b\in\mathbb{Z}\}$ și că pt. $a,b,c,d\in\mathbb{Z}$ avem $\widehat{a+bX}=\widehat{c+dX}\iff a=c$ și $b=d$.

(iii) Să se determine idempotenții din $\frac{\mathbb{Z}[X]}{(X^2-1)}$.

(iv) Arătați că $\frac{\mathbb{Z}[X]}{(X^2-1)}\not\simeq\mathbb{Z}\times\mathbb{Z}$.

⑤ Să se arate că $\frac{\mathbb{C}[X]}{(X^2+1)}\simeq\mathbb{C}\times\mathbb{C}$.

⑥ Să se arate că $\frac{\mathbb{R}[X]}{(X^2+1)}\simeq\mathbb{C}$.

IP 28

Rădăcini multiple

În continuare A va fi un domeniu de integritate.

<u>Definiție</u> Fie $f \in A[X]$ un polinom nenul, $a \in A$ și $i \in \mathbb{N}^*$. Spunem că a este rădăcină multiplă de ordin i a lui f dacă $(X-a)^i \mid f$ și $(X-a)^{i+1} \nmid f$.

<u>Observații</u> (1) a e rădăcină multiplă de ordin i pt. f $\Longleftrightarrow$

$\Longleftrightarrow$ există $g \in A[X]$ cu $f=(X-a)^i \cdot g$ și $g(a) \neq 0$.

<u>Dem</u> "$\Rightarrow$" Dacă a e rădăcină multiplă de ordin i, atunci $(X-a)^i \mid f$, deci există $g \in A[X]$ cu $f=(X-a)^i \cdot g$. În plus, $g(a) \neq 0$, pt. că altfel am avea $X-a \mid g$, deci $g=(X-a)\cdot g_1$ pt. un $g_1 \in A[X]$, și ar rezulta că $f=(X-a)^{i+1} \cdot g_1$, adică $(X-a)^{i+1} \mid f$, contradicție.

"$\Leftarrow$" ~~Dacă~~ $f=(X-a)^i \cdot g$, atunci clar $(X-a)^i \mid f$.

Arătăm că $(X-a)^{i+1} \nmid f$. Într-adevăr, dacă am avea $(X-a)^{i+1} \mid f$, ar rezulta că $f=(X-a)^{i+1} \cdot h$ pt. un $h \in A[X]$. Atunci $(X-a)^i \cdot g=(X-a)^{i+1} \cdot h$ și cum $A[X]$ e domeniu de integritate ar rezulta că $g=(X-a)\cdot h$, de unde $g(a)=0$, contradicție.

Așadar $(X-a)^{i+1} \nmid f$, deci a este rădăcină multiplă de ordin i a lui f.

(2) Dacă $f \in A[X]$ nenul și $a \in A$ e rădăcină multiplă de ordin $i \geq 1$ pt. f, atunci $i \leq \deg(f)$; într-adevăr e clar că $\deg((X-a)^i \cdot h) = i + \deg(h) \geq i$ [chiar și când A nu e domeniu de integritate]

Prop. Fie $f, g \in A[X]$ polinoame nenule, $a \in A$ și $i, j \in \mathbb{N}^*$. Dacă a este rădăcină multiplă de ordin i pt. f și rădăcină multiplă de ordin j pt. g, atunci a este rădăcină multiplă de ordin $i+j$ pt. fg.

Dem. Avem $f = (X-a)^i \cdot f_1$ și $g = (X-a)^j \cdot g_1$, cu $f_1, g_1 \in A[X]$ și $f_1(a) \neq 0$, $g_1(a) \neq 0$. Atunci

$$fg = (X-a)^{i+j} \cdot f_1 g_1, \text{ iar } (f_1 g_1)(a) = f_1(a) g_1(a) \neq 0.$$

Din observația precedentă $\Rightarrow$ a e rădăcină multiplă de ordin $i+j$ a lui fg.

Exercițiu. Fie $u, v \in A[X]$ polinoame nenule, $a \in A$ și $i \in \mathbb{N}^*$. Dacă a este rădăcină multiplă de ordin i pt. u și $v(a) \neq 0$, atunci a este rădăcină multiplă de ordin i pt. uv.

Prop. Fie $f \in A[X]$ polinom nenul, $a_1, \dots, a_r$ elemente distincte din A (unde $r \in \mathbb{N}^*$), astfel încât a_1 e rădăcină multiplă de ordin i_1 pt. f, ..., a_r e rădăcină multiplă de ordin i_r pt. f (unde $i_1, \dots, i_r \in \mathbb{N}^*$). Atunci există $g \in A[X]$ cu

$$f = (X-a_1)^{i_1} \cdots (X-a_r)^{i_r} \cdot g \text{ și } g(a_1) \neq 0, \dots, g(a_r) \neq 0.$$

Dem. Procedăm prin inducție după r.

Pt. $r=1$ rezultă din observația de mai înainte.

Presupunem adevărat pt. $r-1$ și demonstrăm pentru r (unde $r \geq 2$).

Din ipoteza de inducție există $h \in A[X]$ cu

$$f = (X-a_1)^{i_1} \dots (X-a_{r-1})^{i_{r-1}} \cdot h \quad \text{și} \quad h(a_1) \neq 0, \dots, h(a_{r-1}) \neq 0.$$

Notăm $u = (X-a_1)^{i_1} \dots (X-a_{r-1})^{i_{r-1}}$. Cum $f = uh$, $f(a_r) = 0$ și $u(a_r) \neq 0$, rezultă că $h(a_r) = 0$, deci a_r e rădăcină pt. h. Fie i ordinul de multiplicitate al rădăcinii a_r în h. Din Exercițiul precedent rezultă că a_r e rădăcină multiplă de ordin i în f, deci $i = i_r$. Atunci din cazul $r=1$ avem $h = (X-a_r)^{i_r} \cdot g$ pt. un polinom g cu $g(a_r) \neq 0$. În plus, din $h(a_1) \neq 0, \dots, h(a_{r-1}) \neq 0$ rezultă că și $g(a_1) \neq 0, \dots, g(a_{r-1}) \neq 0$. Acum

$$f = (X-a_1)^{i_1} \dots (X-a_{r-1})^{i_{r-1}} h = (X-a_1)^{i_1} \dots (X-a_{r-1})^{i_{r-1}} (X-a_r)^{i_r} g$$

ceea ce încheie demonstrația.

<u>Corolar</u>. Fie $f \in A[X]$ un polinom de grad $n \geq 1$. (unde A este un domeniu de integritate, așa cum am stabilit de la început). Atunci numărul rădăcinilor lui f, numărate cu ordinele lor de multiplicitate, este cel mult n.

<u>Dem.</u> Dacă $a_1, \dots, a_r$ sunt rădăcini distincte cu ordine de multiplicitate $i_1, \dots, i_r$, atunci $f = (X-a_1)^{i_1} \dots (X-a_r)^{i_r} g$ pt. un $g \in A[X]$. Egalând gradele, obținem că