$n = i_1 + \dots + i_r + \deg(g)$. Rezultă că f nu poate avea decât un număr finit de rădăcini distincte (altfel am putea alege $r > n$ și obține astfel o contradicție), iar apoi luând $a_1, \dots, a_r$ ca să fie toate rădăcinile distincte, obținem că

$i_1 + \dots + i_r \leq n$, adică numărul rădăcinilor lui f, numărate cu multiplicități, este cel mult n.

Observație. Dacă A nu este domeniu de integritate, se poate întâmpla ca un polinom nenul să aibă chiar și o infinitate de rădăcini. Fie de exemplu $A = B \times C$, unde B și C sunt inele, iar C este infinit. Fie $f = aX \in A[X]$, unde $a = (1_B, 0_C)$, un polinom de grad 1. Atunci

$$f((0_B, c)) = (1_B, 0_C) \cdot (0_B, c) = (0_B, 0_C) = 0 \text{ pt. orice}$$

$c \in C$, deci orice element de forma $(0, c)$ este rădăcină a lui f. Prin urmare f are o infinitate de rădăcini.

Propoziție (Relațiile lui Viète)
Fie A un domeniu de integritate și $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ un polinom de grad $n \in \mathbb{N}^*$ din $A[X]$ (așadar $a_n \neq 0$). Dacă f are n rădăcini $x_1, \dots, x_n$ în A (scrise în listă cu multiplicități, fiecare de atâtea ori cât este ordinul ei de multiplicitate), atunci

$f = a_n(X-x_1)\dots(X-x_n)$ și

$$-a_{n-1} = a_n(x_1+\dots+x_n) \qquad \left(= a_n \sum_{1\le i\le n} x_i\right).$$

$$a_{n-2} = a_n(x_1x_2+\dots+x_1x_n+\dots+x_{n-1}x_n) \qquad \left(= a_n \sum_{1\le i<j\le n} x_i x_j\right)$$

$$(-1)^k a_{n-k} = a_n(x_1x_2\dots x_k+\dots+x_{n-k+1}x_{n-k+2}\dots x_n) \qquad \left(= a_n \sum_{1\le i_1<\dots<i_k\le n} x_{i_1}\dots x_{i_k}\right)$$

$$(-1)^n a_0 = a_n(x_1\cdot\ldots\cdot x_n).$$

<u>Demonstrație</u>. Din ultima Propoziție precedentă avem că $f=(X-x_1)\dots(X-x_n)g$ pt. un $g\in A[X]$ (scriem fiecare $(X-a_p)^{i_p}$ din acea propoziție sub forma $\underbrace{(X-a_p)\cdot\ldots\cdot(X-a_p)}_{i_p \text{ ori}}$).

Egalând gradele, avem $n=\deg(f)=n+\deg(g)$, deci $\deg(g)=0$, adică g e constant. Egalând acum coeficienții dominanți, obținem $g=a_n$, de unde $f=a_n(X-x_1)\dots(X-x_n)$.

Efectuând înmulțirile în membrul drept obținem

$$f = a_nX^n - a_n(x_1+\dots+x_n)X^{n-1} + a_n(x_1x_2+\dots+x_1x_n+\dots+x_{n-1}x_n)X^{n-2}$$
$$-\dots+(-1)^k a_n(x_1\dots x_k+\dots+x_{n-k+1}\dots x_n)X^{n-k}+$$
$$+\dots+(-1)^n a_n x_1\dots x_n.$$

Într-adevăr, un termen în care apare X^{n-k} în membrul drept se obține selectând în n-k dintre factorii în paranteze termenul X, iar în k dintre factori termenul al doilea, de forma $-x_i$, luând produsul termenilor selectați și înmulțind cu a_n.

Egalând acum coeficienții termenilor de același grad în egalitatea precedentă, obținem relațiile dorite.

<u>Exercițiu</u>. Fie p un număr natural prim. Să se arate că:

(i) Mulțimea $\mathbb{Z}_p\setminus\{\hat{0}\}$ este grup cu înmulțirea din $\mathbb{Z}_p$. Deduceți că $a^{p-1}=\hat{1}$ pt. orice $a\in\mathbb{Z}_p\setminus\{\hat{0}\}$.

(ii) Polinomul $f=X^{p-1}-\hat{1}\in\mathbb{Z}_p[X]$ are rădăcinile $\hat{1},\dots,\widehat{p-1}$, toate simple (adică cu ordin de multiplicitate 1).

(iii) Folosind relațiile lui Viète deduceți că

$$(p-1)!\equiv -1 \pmod{p} \quad \text{[Teorema lui Wilson]}.$$

<u>Derivata formală a unui polinom și rădăcini multiple</u>

Fie K un corp comutativ. Atunci $K[X]$ este un K-spațiu vectorial (atenție: nu este finit dimensional, o bază a sa este $1, X, X^2, \dots\dots$).

Din proprietatea de universalitate a spațiilor vectoriale rezultă că există o unică aplicație liniară $D: K[X] \to K[X]$ pentru care

$$\begin{cases} D(1) = 0 \\ D(X^i) = iX^{i-1} \text{ pt. orice } i \in \mathbb{N}^* \end{cases}.$$

Astfel, dacă $f = a_n X^n + \dots + a_1 X + a_0$, atunci $D(f) = n a_n X^{n-1} + \dots + a_1$ (Exercițiu: să se verifice direct că aplicația D dată de această formulă este aplicație liniară).

$D(f)$ se numește derivata formală a polinomului f (a se observa asemănarea cu formula care dă derivata uzuală a unei funcții polinomiale de la $\mathbb{R}$ la $\mathbb{R}$).

<u>Prop.</u> Pt. orice $f, g \in K[X]$ are loc

(*) $\quad D(fg) = D(f)g + fD(g)$.

<u>Dem.</u> Arătăm că dacă $u = u_1 + \dots + u_p$, $v = v_1 + \dots + v_q$, unde $u_1, \dots, u_p, v_1, \dots, v_q \in K[X]$, și formula (*) e adevărată pt. $f = u_i$ și $g = v_j$ pt. orice $1 \le i \le p, 1 \le j \le q$, atunci (*) e adevărată și pt. $f = u$ și $g = v$.

Într-adevăr,

$$D(uv) = D\Big(\sum_{\substack{1\le i\le p\\1\le j\le q}} u_i v_j\Big) = \sum_{\substack{1\le i\le p\\1\le j\le q}} D(u_i v_j)$$

$$= \sum_{\substack{1\le i\le p\\1\le j\le q}} \Big(D(u_i)v_j + u_i D(v_j)\Big)$$

$$= \left(\sum_{1\le i\le p} D(u_i)\right)\left(\sum_{1\le j\le q} v_j\right) + \left(\sum_{1\le i\le p} u_i\right)\left(\sum_{1\le j\le q} D(v_j)\right)$$

$$= D(u)\, v + u\, D(v).$$

Cum orice polinom este o sumă finită de monoame de forma aX^i, o consecință a celor de mai sus este că pt. a demonstra $(*)$ pt. orice f, g este suficient să verificăm că $(*)$ are loc pt. polinoame de forma

$$f = aX^i,\ g = bX^j \text{ cu } a,b\in K,\ i,j\in \mathbb{N}.$$

Dacă $i=0$, atunci $D(f)=0$ și

$(*) \Leftrightarrow D(ag) = a D(g)$, adevărat pt. că D liniară.

La fel dacă $j=0$. Presupunem acum $i,j>0$. Atunci

$$D(fg) = D(abX^{i+j}) = (i+j)abX^{i+j-1}$$

$$= iabX^{i+j-1} + jabX^{i+j-1}$$

$$= (iaX^{i-1})(bX^j) + (aX^i)(jbX^{j-1})$$

$$= D(f)\,g + f\,D(g),$$ adică $(*)$ are loc pt. f și g.

<u>Notație</u>: Dacă $f\in K[X]$.
$D(f)$ se notează cu f' sau $f^{(1)}$.
$D(f')$ se notează cu f'' sau $f^{(2)}$.
Pt. orice $i\ge 1$, $D(f^{(i)})$ se notează cu $f^{(i+1)}$.
În plus, notăm și $f^{(0)} = f$.

$f^{(n)}$ s.n. a-n-a derivată formală a lui f.

~~Exercițiu. Dacă $f = (X-a)^n$, unde $a \in K$, $n \in \mathbb{N}^*$, atunci $f^{(1)} = n(X$~~

<u>Exercițiu</u>. Fie $n \in \mathbb{N}$, $n \geq 2$ și $f_1, \dots, f_n \in K[X]$.

Atunci $\Delta(f_1 f_2 \cdots f_n) = \Delta(f_1) f_2 \cdots f_n + f_1 \Delta(f_2) f_3 \cdots f_n + \dots + f_1 \cdots f_{n-1} \Delta(f_n)$

<u>Exercițiu</u>. Fie $f = (X-a)^n$, unde $a \in K$, $n \in \mathbb{N}^*$. Atunci

$$f^{(1)} = n(X-a)^{n-1}$$

$$f^{(2)} = n(n-1)(X-a)^{n-2}$$

$$f^{(i)} = n(n-1)\cdots(n-i+1)(X-a)^{n-i} \quad \text{pt. } 1 \leq i \leq n.$$

$$f^{(n)} = n! \cdot 1_K \,($$

$$f^{(n+1)} = f^{(n+2)} = \dots = 0.$$

<u>Exercițiu</u>. Fie K un corp comutativ de caracteristică $p > 0$. Atunci pentru orice $f \in K[X]$ avem $f^{(p)} = 0$.

<u>Exercițiu</u>. Fie $f, g \in K[X]$. Atunci $(fg)^{(n)} = \sum_{k=0}^{n} C_n^k f^{(n-k)} g^{(k)}$ pt. orice $n \in \mathbb{N}^*$.

<u>Propoziție</u>. Fie K un corp comutativ de caracteristică zero. Fie $f \in K[X]$ cu $\deg(f) = n \in \mathbb{N}^*$ și $a \in K$. Atunci

$$f = f(a) + \frac{f^{(1)}(a)}{1!} \cdot (X-a) + \frac{f^{(2)}(a)}{2!} \cdot (X-a)^2 + \dots + \frac{f^{(n)}(a)}{n!} \cdot (X-a)^n.$$

[observație: prin $\frac{1}{i!}$ înțelegem de fapt inversul în K al elementului $i! \cdot 1_K$, care element este nenul deoarece K are caracteristică 0].

<u>Dem</u>. Mulţimea $\{1, X-a, (X-a)^2, \dots, (X-a)^n\}$ este bază a K-spaţiului vectorial format din toate polinoamele de grad $\leq n$ (deoarece polinoamele listate au gradele $0, 1, \dots, n$). Rezultă că există (şi sunt unice) $c_0, c_1, \dots, c_n \in K$ cu $f = c_0 + c_1 \cdot (X-a) + \dots + c_n \cdot (X-a)^n$. (*)

Evaluând în a $\Rightarrow f(a) = c_0$.

Aplicăm apoi Δ lui (*) şi obţinem

$$f^{(1)} = c_1 + c_2 \cdot 2(X-a) + \dots + c_n \cdot n(X-a)^{n-1}. \quad (**)$$

Evaluăm în a $\Rightarrow f^{(1)}(a) = c_1 = c_1 \cdot 1!$

Aplicăm Δ lui (**) şi obţinem

$$f^{(2)} = \sum_{2 \leq i \leq n} c_i \cdot i \cdot (i-1) \cdot (X-a)^{i-2}.$$

Evaluăm în a $\Rightarrow f^{(2)}(a) = c_2 \cdot 2!$

Continuăm recurent şi obţinem $f^{(i)}(a) = c_i \cdot i!$ pt. orice $1 \leq i \leq n$. Cum $char(K) = 0$, rezultă că $c_i = \frac{f^{(i)}(a)}{i!}$ şi înlocuind în (*) obţinem formula dorită.

<u>Prop</u>. Fie K un corp comutativ, $f \in K[X]$ nenul şi $a \in K$. Dacă a este rădăcină multiplă de ordin i pt. f, atunci $f(a) = f^{(1)}(a) = \dots = f^{(i-1)}(a) = 0$.

Dem. Avem $f=(X-a)^i h$ pt. un $h\in K[X]$.

Notăm $g=(X-a)^i$. Fie $1\le n\le i-1$. Un exercițiu precedent arată că

$f^{(n)}=(gh)^{(n)}=\sum_{k=0,n} C_n^k\, g^{(n-k)} h^{(k)}$ și evaluând în a

obținem $f^{(n)}(a)=\sum_{k=0,n} C_n^k\, g^{(n-k)}(a)\, h^{(k)}(a)$. $(*)$

Un alt exercițiu precedent arată că pt. $1\le j\le i-1$ avem

$g^{(j)}=i(i-1)\dots(i-j+1)(X-a)^{i-j}$, deci $g^{(j)}(a)=0$.

Cum în $(*)$ $n-k\le n\le i-1$, obținem că

$g^{(n-k)}(a)=0$ pt. orice $0\le k\le n$ [ținem cont și

că pt. $k=n$ avem $g^{(0)}(a)=g(a)=0$].

Rezultă că $f^{(n)}(a)=0$.

Prop. Fie K un corp comutativ de caracteristică 0, $f\in K[X]$ nenul și $a\in K$. Atunci a este rădăcină multiplă de ordin i pt. f dacă și numai dacă

$f(a)=f^{(1)}(a)=\dots=f^{(i-1)}(a)=0$ și $f^{(i)}(a)\ne 0$.

Dem. Presupunem că a este rădăcină multiplă de ordin i.

Am arătat deja în Prop. precedentă că $f(a)=f^{(1)}(a)=\dots=f^{(i-1)}(a)=0$.

Avem $f=gh$, unde $g=(X-a)^i$ și $h(a)\ne 0$. Atunci

$f^{(i)}=g^{(i)}h+C_i^1 g^{(i-1)}h^{(1)}+\dots+C_i^{i-1}g^{(1)}h^{(i-1)}+gh^{(i)}$.

Evaluând în a și ținând cont că

$g(a) = g^{(1)}(a) = \dots = g^{(i-1)}(a) = 0$ și $g^{(i)}(a) = i! \cdot 1_K \neq 0$,

avem $f^{(i)}(a) = \underbrace{g^{(i)}(a)}_{\neq 0} \cdot \underbrace{h(a)}_{\neq 0} \neq 0$.

Reciproc, presupunem că $f(a) = f^{(1)}(a) = \dots = f^{(i-1)}(a) = 0$ și $f^{(i)}(a) \neq 0$. Atunci cum $f^{(i)} \neq 0$, avem $n = \deg(f) \geq i$ și dintr-o propoziție precedentă rezultă că

$$f = f(a) + \frac{f^{(1)}(a)}{1!}(X-a) + \dots + \frac{f^{(n)}(a)}{n!}(X-a)^n$$

$$= \frac{f^{(i)}(a)}{i!}\cdot(X-a)^i + \frac{f^{(i+1)}(a)}{(i+1)!}(X-a)^{i+1} + \dots + \frac{f^{(n)}(a)}{n!}(X-a)^n.$$

E clar că $(X-a)^i \mid f$ (se poate da factor comun $(X-a)^i$).

Apoi $(X-a)^{i+1} \nmid f$, deoarece altfel ar rezulta că

$$0 \neq \frac{f^{(i)}(a)}{i!}(X-a)^i = f - (X-a)^{i+1} \cdot \left[\frac{f^{(i+1)}(a)}{(i+1)!} + \dots + \frac{f^{(n)}(a)}{n!}(X-a)^{n-i-1}\right]$$

se divide cu $(X-a)^{i+1}$, contradicție, deoarece un polinom de grad i nu se poate divide cu unul de grad $i+1$.
Așadar a e rădăcină multiplă de ordin i pt. f.

<u>Obs.</u> În caracteristică $\neq 0$ rezultatul precedent nu mai e adevărat.
Fie p prim și $f = X^p \in K[X]$, unde K are caracteristică p (de exemplu $K = \mathbb{Z}_p$). Atunci $a=0$ e rădăcină multiplă de ordin p pt. f, car $f' = pX^{p-1} = 0$, deci $f^{(n)} = 0 \ \forall n \geq 1$ și atunci $f(0) = f^{(1)}(0) = \dots = f^{(n)}(0) = \dots = 0$.

Inele de polinoame de mai multe nedeterminate

Fie A un inel comutativ. Pentru fiecare $n \in \mathbb{N}^*$ definim inelul de polinoame $A[X_1, \dots, X_n]$ în n nedeterminate $X_1, \dots, X_n$ (cu coeficienți în A) prin recurență, astfel:

- pt. $n=1$, $A[X_1]$ este inelul de polinoame într-o nedeterminată X_1 (a fost construit deja, singura diferență este că notăm nedeterminata cu X_1 în loc de X).

- pt. $n=2$, $A[X_1, X_2]$ este $(A[X_1])[X_2]$, adică inelul de polinoame într-o nedeterminată X_2 cu coeficienți în inelul comutativ $A[X_1]$.

- Pasul recurent (similar cu $1 \to 2$ de mai sus): presupunem că am construit $A[X_1, \dots, X_{n-1}]$, unde $n \geq 2$. Atunci definim
$$A[X_1, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n],$$
adică inelul de polinoame într-o nedeterminată X_n, cu coeficienți în inelul comutativ $A[X_1, \dots, X_{n-1}]$.

Un element de forma $a X_1^{i_1} \dots X_n^{i_n}$ din $A[X_1, \dots, X_n]$, unde $a \in A$ și $i_1, \dots, i_n \in \mathbb{N}$, se numește monom (cu convenția că $X_j^0 = 1$ pt. orice $1 \leq j \leq n$).

Demonstrăm prin inducție după $n \geq 1$ că orice element din $A[X_1, \dots, X_n]$ este sumă de monoame.