SEMINAR 8

Situaţia $\mathbb{Z} \subset \mathbb{Q}$ conduce imediat la definirea abstractă a corpului de fracţii asociat unui domeniu de integritate (comutativ). Să extrapolăm puţin mai mult din corpul numerelor raţionale. Când facem saltul de la $\mathbb{Q}$ la $\mathbb{R}$ (completăm dreapta), pierdem din vedere aspectul concret asupra multor numere (iraţionalele), pentru că saltul e brusc - şi este astfel deoarece specificul esenţial al metodei e acela de a transcede (indiferent de metoda aleasă). Astfel, deşi teoretic avem obţinut riguros continuumul numeric, ne îndepărtăm de la partea concretă referitoare la $\mathbb{R} \setminus \mathbb{Q}$: este dificil, în general, să decidem dacă un număr e iraţional sau nu (pentru că metoda transcendentă face loc unei întregi panoplii de raţionamente care ne conduc la numere: la π putem ajunge considerând raportul dintre lungimea unui cerc şi diametrul său, la $\sqrt{2}$ putem ajunge încercând să calculăm diagonala unui pătrat, iar la e putem ajunge încercând să rezolvăm ecuaţia diferenţială $u' = u$ (acele funcţii de o variabilă ale căror derivate sunt ele însele).

Pentru a trata sistematic situaţia din afara lui $\mathbb{Q}$, trebuie să facem un pas mai mic, adică să trecem de la $\mathbb{Q}$ la nişte numere care sunt mai apropiate ca natură de cele raţionale. Un număr raţional e o soluţie a unei ecuaţii de forma $ax + b = 0$, cu $a, b \in \mathbb{Z}$, $a \neq 0$. Atunci, un prim pas e să ne uităm la toate numerele $z \in \mathbb{C}$ (nu ne mai limităm doar la $\mathbb{R}$) care satisfac o ecuaţie algebrică $a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0 = 0$, cu $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Z}$ şi $a_n \neq 0$. Dintre acestea, care ar fi analoagele numerelor din $\mathbb{Z}$? Păi sunt acelea care sunt rădăcini ale unor ecuaţii de forma $z^n + a_{n-1} z^{n-1} + \ldots + a_0 = 0$ cu $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$ (deci coeficientul termenului de grad maxim e 1 - spunem că ecuaţia e monică). Mulţimea acestor numere se notează cu $\mathbb{A}$ şi este un inel (numit inelul întregilor algebrici). Deşi am redus din căutări, e încă prea mult să cerem a găsi pe $\mathbb{A}$ - acest inel e extrem de complicat. Atunci putem să luăm diverse corpuri $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ şi să încercăm să studiem inelele $A_K = K \cap \mathbb{A}$; mai precis, ar trebui să începem nu chiar cu toate aceste corpuri, ci cu acelea care, privite ca $\mathbb{Q}$ - spaţii vectoriale, au dimensiunea finită. La acestea ne-am tot referit când spuneam "corpuri aritmetice"; de fapt, un astfel de corp K se numeşte corp de numere, iar inelul său corespunzător, A_K se numeşte inelul de întregi algebrici din K.

Având în vedere discuţia, dat un corp de numere K, situaţia $A_K \subset K$ e similară situaţiei $\mathbb{Z} \subset \mathbb{Q}$. Dar atunci, ar trebui ca corpul de fracţii al lui A_K să fie K. Într-adevăr:

1. Fie K un corp de numere. Atunci K e corpul de fracţii al lui A_K.

Soluţie. Fie $n = dim_{\mathbb{Q}} K$ (în acest caz, acest număr se numeşte gradul extinderii $\mathbb{Q} \subset K$ şi se notează $[K : \mathbb{Q}]$); prin definiţie $n < \infty$. Fie şi $Q(A_K)$ corpul de fracţii al lui A_K. Arătăm că $K \subset Q(A_K)$. Fie $x \in K$ oarecare. Atunci trebuie să avem $dep_{\mathbb{Q}}\{1, x, \ldots, x^n\}$, adică există $a_0, \ldots, a_n \in \mathbb{Q}$, nu toţi nuli, astfel încât $a_0 + a_1 x + \ldots + a_n x^n = 0$. Observăm că putem presupune $a_i \in \mathbb{Z}$, $(\forall) 0 \leq i \leq n$ (înmulţim ecuaţia cu numitorul comun al fracţiilor a_i). Fie şi $m \in \mathbb{N}$ cel mai mare indice i cu proprietatea că $a_i \neq 0$. Observaţi că trebuie să avem $m \neq 0$ (de ce?). Înmulţind ecuaţia cu a_m^{m-1} obţinem

$$(a_m x)^m + a_{m-1}(a_m x)^{m-1} + \ldots + a_0 a_m^{m-1} = 0$$

adică $a_m x =: a \in A_K$, de unde $x = \frac{a}{a_m} \in Q(A_K)$.
Astfel, $Q(A_K) \supseteq K$. Însă sigur avem $K \supseteq Q(A_K)$ (de ce?), aşa că $Q(A_K) = K$.

În acest exerciţiu e prinsă o clasă largă de exemple: dacă ω e rădăcină de ordin n a unităţii, atunci $A_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$; $A_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$ şi, desigur, $A_{\mathbb{Q}} = \mathbb{Z}$. Nu cumva să credeţi că lucrurile stau mereu la fel, *i.e.* că $A_{\mathbb{Q}(*)} = \mathbb{Z}[*]$. De exemplu, dacă $d \in \mathbb{Z}$ e liber de pătrate, atunci

$$A_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{dacă } d \equiv 1 \,(mod\, 4) \\ \mathbb{Z}[\sqrt{d}], & \text{dacă } d \equiv 2, 3 \,(mod\, 4) \end{cases}$$

iar $A_{\mathbb{Q}(\sqrt{7},\sqrt{10})} \neq \mathbb{Z}[\alpha]$, $(\forall)\, \alpha \in A_{\mathbb{Q}(\sqrt{7},\sqrt{10})}$. Vă mai precizez şi faptul că nu e deloc lejeră stabilirea acestor exemple. De asemenea, de aici reiese că nu e indicat ca, dat un inel A de forma $\mathbb{Z}[\alpha]$, atunci când vi se cere să arătaţi că $Q(A) = \mathbb{Q}(\alpha)$ să vă apucaţi să argumentaţi spunând că $Q(A) = \mathbb{Q}(\alpha)$ pentru că A e inelul de întregi algebrici al lui $\mathbb{Q}(\alpha)$ şi folosim ex. 1 - dacă alegeţi să faceţi aşa, atunci trebuie să arătaţi că într-adevăr $A = A_K$, iar lucrul acesta e, în general, dificil.

2. Corpul de fracţii al inelului $\mathbb{Z}[i]$ este $\mathbb{Q}(i) = \{a + bi; a, b \in \mathbb{Q}\}$.

Soluţie. În primul rând, e clar că $\mathbb{Q}(i)$ e corp ($z\overline{z} = |z|^2$). Fie $K = Q(\mathbb{Z}[i])$; trebuie arătat că are loc un izomorfism de corpuri $K \simeq \mathbb{Q}(i)$. Atunci fie $\varphi : \mathbb{Z}[i] \longrightarrow K$ morfismul structural, $x \mapsto \frac{x}{1}$. Avem şi

incluziunea canonică $\mathbb{Z}[i] \overset{\iota}{\hookrightarrow} \mathbb{Q}(i)$. Atunci proprietatea de universalitate a corpului de fraţii ne spune că există un unic morfism de corpuri $\bar{\iota} : K \longrightarrow \mathbb{Q}(i)$ care face diagrama

$$\begin{array}{ccc} \mathbb{Z}[i] & \xhookrightarrow{\varphi} & K \\ \downarrow{\scriptstyle \iota} & \swarrow{\scriptstyle \bar{\iota}} & \\ \mathbb{Q}(i) & & \end{array}$$

comutativă. Ca orice morfism de corpuri, $\bar{\iota}$ e injectiv. Arătăm că e şi surjecţie. Fie $z = a + bi \in \mathbb{Q}(i)$. Scriem $a = \frac{m_1}{n_1}, b = \frac{m_2}{n_2}$, cu $m_i, n_i \in \mathbb{Z}$, $n_i \neq 0$, $i = 1, 2$. Notând $m_1 n_2 + m_2 n_1 = w \in \mathbb{Z}[i]$, avem că

$$\begin{aligned} z = \frac{1}{n_1 n_2} w = \iota(n_1 n_2)^{-1} \iota(w) = ((\bar{\iota} \circ \varphi)(n_1 n_2))^{-1} (\bar{\iota} \circ \varphi)(w) = \\ = \bar{\iota}(\varphi(n_1 n_2)^{-1}) \bar{\iota}(\varphi(w)) = \bar{\iota}(\varphi(n_1 n_2)^{-1} \varphi(w)) \end{aligned}$$

i.e. $z \in Im(\bar{\iota})$. Astfel, K e izomorf cu $\mathbb{Q}(i)$ prin $\bar{\iota}$.

În schimb, faptul că $A_{\mathbb{Q}(\omega)} = \mathbb{Z}[\omega]$ (în particular, $A_{\mathbb{Q}(i)} = \mathbb{Z}[i]$) e teoremă în toată regula! Precizare: numerele care nu sunt algebrice se numesc transcendente (tocmai pentru că nu sunt prinse în nicio ecuaţie algebrică, înseamnă că ele *transcend* toate polinoamele). Cum spuneam la început, e foarte dificil a depista numere transcendente; totuşi, căutaţi teorema lui Liouville.

Această construcţie asupra unui domeniu de integritate oferă o nouă clasă de corpuri, numite corpuri de funcţii. De exemplu, dacă k e un corp (comutativ), corpul de fracţii $K = k(X)$ al inelului de polinoame $k[X]$ e corpul de funcţii raţionale în "dimensiune" 1 peste k. În dimensiune n, vorbim despre $k(X_1, \ldots, X_n)$. Ideea legată de aceste corpuri e că, dat un obiect geometric peste k, acesta are o dimensiune, n să zicem, şi putem apela la funcţiile din $k(X_1, \ldots, X_n)$ (sau ceva asemănător) pentru a-l descrie. De obicei, cu funcţiile raţionale reuşim să descriem doar o parte din geometria obiectului, însă e o bucată consistentă.

Să ne uităm la S^1. Algebric, cercul e dat de ecuaţia $x^2 + y^2 = 1$. Proiectăm din punctul $(-1, 0)$ pe dreapta Oy, şi fie $(0, t)$ punctul de intersecţie. Ecuaţia dreptei d ce trece prin $(-1, 0)$ şi $(0, t)$ este $y = t(1 + x)$. Dreapta d va tăia S^1 în două puncte P, Q de coordonate $(x, y), (x', y')$. Ca să le scoatem, avem relaţia $1 - x^2 = y^2 = t^2(1 + x)^2$

($P \in S^1 \cap d$); pentru t fixat, soluţiile acestei ecuaţii în x sunt abscisele punctelor P şi Q. O rădăcină este $x = -1$. Apoi, eliminând $1 + x$, găsim $1 - x = t^2(1 + x)$. Astfel, dând drumul lui t, obţinem o parametrizare a lui S^1 dată prin $S^1 \ni P = (x, y) = (\varphi(t), \psi(t))$, unde $\varphi(t) = \frac{1-t^2}{1+t^2}$, iar $\psi(t) = \frac{2t}{1+t^2}$. Aşadar, cu ajutorul funcţiilor φ şi ψ cunoaştem aproape tot cercul (mai puţin un punct). Dar unde stau φ şi ψ? Sunt luate din corpul $\mathbb{R}(t)$. Amintiţi-vă când calculaţi anumite integrale în liceu folosind schimbarea de variabilă $t = \tan x$. Ei bine, iată motivul pentru care puteaţi să calculaţi acele integrale: de fapt, eraţi pe o curbă, iar acea curbă putea fi parametrizată cu funcţii din $\mathbb{R}(t)$! Cu această remarcă (a lui Euler) ne situăm într-un punct de concentraţie matematică enormă, ce a explodat în aşa numita teorie a integralelor abeliene, teorie care i-a avut în prim plan pe Euler, Abel, Jacobi şi Riemann.

Cam asta legat de corpurile de fracţii. De fapt, e cazul să vorim puţin şi despre o tehnică de definire de care deja aţi dat în câteva rânduri: proprietăţi de universalitate (ale corpurilor de fracţii, ale grupurilor factor, ale inelelor de polinoame, etc). Această metodă de definire bazată nu pe elemente, ci pe morfisme, e una dintre succesurile teoriei categoriilor, aşa că probabil cel mai bine e să vă sară în ajutor experienţa (deci să vă lămuriţi în timp). Ideea e că o proprietate de universalitate, dacă are loc, ne spune că avem un candidat natural pentru cutare construcţie. Astfel, pentru construcţia corpului de fracţii al unui domeniu A, avem candidatul natural (firesc) $Q(A) = \{\frac{a}{b}; a, b \in A, a \neq 0\}$, însă nu ne spune nimeni că n-ar mai fi şi alte corpuri K care să fie pe post de corp de fracţii al lui A; faptul că orice alt candidat K "factorizează" prin $Q(A)$ ne spune riguros că $Q(A)$ e alegerea naturală.

Acum trecem la exerciţii despre rădăcinile polinoamelor. De precizat că partea legată de soluţiile ecuaţiilor pe care o facem aici e plăpândă; grosul îl veţi vedea în anul III şi se numeşte teorie Galois.

3. Fie p un număr prim.
(i) Polinomul $X^{p-1} - 1 \in \mathbb{F}_p[X]$ are rădăcinile simple $\hat{1}, \ldots, \widehat{p-1}$.
(ii) (teorema lui Wilson) Avem că

$$(p-1)! \equiv -1 \, (mod \, p)$$

Soluţie. Afirmaţia (i) e mica teoremă a lui Fermat. De fapt, $\hat{1}, \ldots, \widehat{p-1} \in \mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ sunt rădăcinile lui $X^{p-1} - 1$ conform teoremei lui Lagrange în grupul multiplicativ $\mathbb{F}_p^*$ (şi sunt simple din motive de grad).
Pentru (ii) folosim "ultima" relaţie Viète, $a_n x_1 x_2 \ldots x_n = (-1)^n a_0$. La

noi, $a_0 = -1$, $a_n = 1$, $x_1 = \hat{1}$, $\ldots$, $x_n = \widehat{p-1}$, $n = p-1$ şi deci $\widehat{(p-1)!} = \widehat{(-1)^p}$, adică

$$(p-1)! \equiv (-1)^p \,(mod\, p) \equiv -1 \,(mod\, p)$$

(pentru $p = 2$ avem $1 \equiv -1(mod\, 2)$).

O problemă extrem de dificilă e cea a primalităţii. De exemplu, e 3628801 un număr prim? Citiţi şi despre numerele Carmichael.

Aţi văzut cum se calculează ordinul de multiplicitate al unei rădăcini cu ajutorul derivatei (formale); dar asta e valabil numai în caracteristică nulă! De exemplu, fie k un corp de caracteristică $char(k) = p > 0$. Atunci polinomul $f = X^p + X^{p^2} \in k[X]$ are rădăcina 0 cu ordinul de multiplicitate p, însă $f^{(i)}(0) = 0$, oricare ar fi $i > 0$ (încă un semn că lucrurile se complică în caracteristică pozitivă; în particular, peste corpurile finite).

Aşa cum ştiţi din liceu, pentru elemente $\alpha_1, \ldots \alpha_n$ dintr-un inel A (comutativ), sumele $\sigma_1 = \sum_{1 \le i \le n} \alpha_i$, $\sigma_2 = \sum_{1 \le i < j \le n} \alpha_i \alpha_j$, $\ldots$, $\sigma_n = \alpha_1 \alpha_2 \ldots \alpha_n$ se numesc sumele Viète.

4. Fie $f = X^3 + 2X^2 - 3X + 1 \in \mathbb{C}[X]$ şi fie x_1, x_2, x_3 rădăcinile lui f (teorema fundamentală a algebrei). Calculaţi: $x_1^2 + x_2^2 + x_3^2$, $x_1^3 + x_2^3 + x_3^3$, $x_1^4 + x_2^4 + x_3^4$, $\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$, $\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2}$, $\frac{1}{x_1+1} + \frac{1}{x_2+1} + \frac{1}{x_3+1}$.

Soluţie. Sumele Viète pentru x_1, x_2, x_3 sunt $\sigma_1 = -2$, $\sigma_2 = -3$ şi $\sigma_3 = -1$. Avem

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3) = \sigma_1^2 - 2\sigma_2 = 10$$

Pentru cuburi folosim efectiv şi faptul că x_1, x_2, x_3 sunt rădăcinile lui f. Avem
$x_1^3 + 2x_1^2 - 3x_1 + 1 = 0$
$x_2^3 + 2x_2^2 - 3x_2 + 1 = 0$
$x_3^3 + 2x_3^2 - 3x_3 + 1 = 0$
şi adunându-le, obţinem că $\sum x_i^3 + 2\sum x_i^2 - 3\sigma_1 + 3 = 0$, de unde $\sum x_i^3 = -3 - 6 - 20 = -29$.
Pentru ultima, facem schimbarea de variabilă $Y = \frac{1}{X+1}$ (cu alte cuvinte, considerăm automorfismul de $\mathbb{C}$- algebră al lui $\mathbb{C}(X)$ dat prin $X \mapsto \frac{1}{X+1}$ - exact asta înseamnă să schimbăm "coordonatele" (vezi teorema de inversiune locală din analiza matematică)). Atunci f se transformă în

$$g = (\tfrac{1-Y}{Y})^3 + 2(\tfrac{1-Y}{Y})^2 - 3\tfrac{1-Y}{Y} + 1$$

şi egalând cu 0 (trecând la numere), obţinem ecuaţia $5y^3-4y^2-y+1=0$. Fie y_1, y_2, y_3 rădăcinile acestei ecuaţii. Astfel, ni se cere, de fapt, să calculăm $y_1+y_2+y_3$, căci $y_i=\frac{1}{x_i+1}$, $i=1,2,3$, adică prima sumă Viète a celei de-a doua ecuaţii:$\frac{4}{5}$.

În general, date nişte numere $\alpha_1, \ldots, \alpha_n$ şi un număr $k \in \mathbb{N}^*$, sumele $s_k = \sum\limits_{1\leq i\leq n} \alpha_i^k$ se numesc sume Newton şi are loc următorul rezultat de legătură:

5. (*Formulele lui Newton*)
(i) Pentru orice $1 \leq k \leq n$

$$s_k - s_{k-1}\sigma_1 + \ldots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0$$

(ii) Pentru orice $k \geq n+1$

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 + \ldots + (-1)^n s_{k-n}\sigma_k = 0$$

Soluţie. (i) Calculăm termenii:

$$s_{k-1}\sigma_1 = (\sum_i \alpha_i^{k-1})(\sum_i \alpha_i) = \sum_i \alpha_i^k + \sum_{i\neq j} \alpha_i^{k-1}\alpha_j = s_k + \sum_{i\neq j} \alpha_i^{k-1}\alpha_j$$

$$s_{k-2}\sigma_2 = (\sum_i \alpha_i^{k-2})(\sum_{i<j} \alpha_i\alpha_j) = \sum_{i\neq j} \alpha_i^{k-1}\alpha_j + \sum_{i\neq j<p\neq i} \alpha_i^{k-2}\alpha_p\alpha_j$$

$$s_{k-3}\sigma_3 = (\sum \alpha_i^{k-3})(\sum_{i<j<p} \alpha_i\alpha_j\alpha_p) = \sum_{i\neq j<p\neq i} \alpha_i^{k-2}\alpha_j\alpha_p + \sum_{i\neq j<p<l\neq i,p\neq i} \alpha_i^{k-3}\alpha_j\alpha_p\alpha_l$$

$$\vdots$$

$$s_1\sigma_{k-1} = (\sum_i \alpha_i)(\sum_{i_1<\ldots<i_{k-1}} \alpha_{i_1}\ldots\alpha_{i_{k-1}}) = \sum_{i_1\neq i_2<\ldots<i_{k-1}} \alpha_{i_1}^2\alpha_{i_2}\ldots\alpha_{i_{k-1}} +$$
$$+ k\sum_{i_1<\ldots<i_{k-1}<i_k} \alpha_{i_1}\ldots\alpha_{i_{k-1}} = \sum \alpha_{i_1}^2\alpha_{i_2}\ldots\alpha_{i_{k-1}} + k\sigma_k$$

Acum, înmulţim a doua relaţie cu -1, pe a patra cu -1, etc, le adunăm şi obţinem relaţia dorită (faceţi calculele desfăcut pentru $k=4$, $n=5$).
(ii) Exact la fel (e doar un calcul).

Deşi se obţin uşor, aceste relaţii sunt importante: pe ele se testează simetria ecuaţiei. Gândiţi-vă că soluţiile unei ecuaţii sunt numere complexe, aşa că le putem reprezenta ca puncte în plan şi unindu-le cu segmente, obţinem o figură geometrică (un poligon) despre a cărei simetrie putem discuta. Dar cum facem precisă noţiunea de simetrie? Gândiţi-vă la cerc; e clar, intuitiv, că acesta e un obiect geometric cât se poate

de simetric. Observaţi că oricum l-am roti sau l-am translata în plan, simetria nu îi este afectată. Astfel, dat un obiect geometric, putem spune că e cu atât mai "simetric" cu cât e invariat de cât mai multe transformări geometrice ale planului. Dar cum algebrizăm acest criteriu de simetrie? Observaţi că pe mulţimea rădăcinilor $\{x_1, \ldots, x_n\}$ acţionează grupul permutărilor de grad n, S_n: pentru fiecare permutare σ_i şi pentru fiecare rădăcină x_j avem acţiunea $(\sigma_i, x_j) \mapsto x_{\sigma_i(j)}$ (asta e înlocuitoarea acţiunii transformărilor geometrice pe figura asociată), iar ecuaţia e cu atât mai "rezolvabilă" cu cât relaţiile de dependenţă ale lui Newton sunt invariate de cât mai multe elemente ale lui S_n! (incursiunea lui Galois).

Cum ne prindem dacă nişte numere date sunt, de fapt, rădăcini de ordin n ale unităţii? Iată o caracterizare a acestora:

6. Numerele complexe $\alpha_0, \ldots, \alpha_{n-1}$ sunt rădăcini de ordin n ale unităţii dacă şi numai dacă:

$$\begin{cases} \alpha_0 + \alpha_1 + \ldots + \alpha_{n-1} = 0 \\ \alpha_0^2 + \alpha_1^2 + \ldots + \alpha_{n-1}^2 = 0 \\ \vdots \\ \alpha_0^{n-1} + \alpha_1^{n-1} + \ldots + \alpha_{n-1}^{n-1} = 0 \\ \alpha_0^n + \alpha_1^n + \ldots + \alpha_{n-1}^n = n \end{cases}$$

Soluţie. Mai întâi presupunem că $\alpha_0, \ldots, \alpha_{n-1}$ sunt rădăcini de ordin n ale unităţii (elementele grupului μ_n). Atunci scriem $\alpha_k = \zeta^k$, $k = 0, 1, \ldots, n-1$, unde ζ e generator al lui μ_n, şi deci pentru orice $j \in \{1, 2, \ldots, n-1\}$ avem că $\sum\limits_{k=0}^{n-1} \alpha_k^j = \sum\limits_{k=0}^{n-1} (\zeta^j)^k = \frac{1-\zeta^{nj}}{1-\zeta^j} = 0$ (ζ generând μ_n). Pentru $j = n$, $\sum\limits_{k=0}^{n-1} \alpha_k^n = \sum\limits_{k=0}^{n-1} 1 = n$.
Reciproc, presupunem că $\alpha_0, \ldots, \alpha_{n-1}$ verifică sistemul din enunţ. Formăm polinomul monic din $\mathbb{C}[X]$ care are rădăcinile $\alpha_0, \ldots, \alpha_{n-1}$; fie acesta $f = X^n + a_1 X^{n-1} + \ldots + a_n$. Atunci ipoteza ne spune că $s_1 = s_2 = \ldots = s_{n-1} = 0$ şi $s_n = n$. Pe de altă parte, avem că

$$\begin{cases} s_1 - \sigma_1 = 0 \\ s_2 - s_1\sigma_1 + 2\sigma_2 = 0 \\ s_3 - s_2\sigma_1 + s_1\sigma_2 - 3\sigma_3 = 0 \\ \vdots \\ s_n - s_{n-1}\sigma_1 + s_{n-2}\sigma_2 - \ldots + (-1)^{n-1} s_1\sigma_{n-1} + (-1)^n n\sigma_n = 0 \end{cases}$$

(cf. ex. 5). Aşadar, reiese succesiv că $\sigma_1 = 0, \sigma_2 = 0, \ldots, \sigma_{n-1} = 0$, $\sigma_n = (-1)^{n+1}$ şi deci formulele lui Viète sunt $a_1 = -\sigma_1 = 0$, $a_2 = \sigma_2 = 0, \ldots$, $a_n = (-1)^n \sigma_n = -1$, *i.e.* $f = X^n - 1$; dar rădăcinile polinomului $X^n - 1$ sunt exact elementele lui μ_n.