## SEMINAR 13

De aici încolo ne vom situa în $k = \mathbb{C}$.

Începem prin a relua câteva lucruri despre grupul

$$\boldsymbol{\mu_n} = \{z \in \mathbb{C};\ z^n = 1\}$$

(probabil le-aţi mai întâlnit). Aceasta pentru că e unul dintre cele mai importante grupuri, iar scopul e să vedem ilustrări ale acestui fapt. Aţi văzut în liceu că elementele sale sunt

$$\alpha_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k = \overline{0, n-1};$$

în particular, ordinul grupului multiplicativ $\boldsymbol{\mu_n}$ este $n$. În general, a cunoaşte un grup înseamnă a-i cunoaşte un sistem de generatori şi relaţiile care există între aceştia. Avem:

1. Grupul $\boldsymbol{\mu_n}$ e ciclic. De fapt, un element $\alpha_k \in \boldsymbol{\mu_n}$ e generator al lui $\boldsymbol{\mu_n}$ dacă şi numai dacă $(k, n) = 1$.

Soluţie. E de aşteptat ca treaba să fie ciclică din moment ce $\boldsymbol{\mu_n}$ face parte din cercul unitate $S^1$. Într-adevăr, formula lui de Moivre ne spune că $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ e generator al lui $\boldsymbol{\mu_n}$: oricare ar fi $\alpha_k \in \boldsymbol{\mu_n}$, $\alpha_k = \zeta^k$.

Acum, fie $\alpha_k$ un generator al lui $\boldsymbol{\mu_n}$. Trebuie să arătăm că $(n, k) = 1$. Deoarece $\alpha_k$ generează $\boldsymbol{\mu_n}$, există $l$ aşa încât $\zeta = \alpha_k^l$. Atunci

$$\zeta = \alpha_k^l = (\zeta^k)^l \Leftrightarrow \zeta^{kl-1} = 1$$
$$\Leftrightarrow \cos\frac{2\pi(kl-1)}{n} + i\sin\frac{2\pi(kl-1)}{n} = 1$$

aşa că trebuie să avem $\frac{2\pi(kl-1)}{n} = 2s\pi$ pentru un $s \in \mathbb{Z}$. Astfel, există $s, l \in \mathbb{Z}$ aşa încât $kl + n \cdot (-s) = 1$, adică $(n, k) = 1$ (cf. seminar 11, ex. 3).

Invers, ca să vedem că un $\alpha_k$ cu $(n, k) = 1$ generează $\boldsymbol{\mu_n}$, e clar că putem parcurge drumul invers al implicaţiilor anterioare (cf. aceluiaşi exerciţiu) şi găsim că $\alpha_K^l = \zeta$; deoarece $\zeta$ e generator, rezultă că şi $\alpha_k$ e generator.

Ne amintim că funcţia lui Euler $\varphi : \mathbb{N} \longrightarrow \mathbb{C}$ asociază unui număr natural $n$ numărul $\varphi(n)$ = numărul acelor $m \in \mathbb{N}$, $m \leq n$, ce sunt prime cu $n$ (deci $Im(\varphi) \subseteq \mathbb{N}$). Ca orice funcţie aritmetică interesantă, $\varphi$ e multiplicativă: dacă $m, n \in \mathbb{N}$ sunt coprime, atunci $\varphi(mn) = \varphi(m)\varphi(n)$. Astfel, grupul multiplicativ $\mu_n$ are $\varphi(n)$ generatori (cf. ex. 1). Aceşti generaori se numesc rădăcinile primitive de ordin $n$ ale unităţii.

Relaţionările dintre grupurile $\boldsymbol{\mu_n}$ sunt dictate de divizibilitate astfel:

2. Fie $m, n \in \mathbb{N}$. Atunci
*(a)* $\boldsymbol{\mu_m \subseteq \mu_n \Leftrightarrow m \mid n}$
*(b)* $\boldsymbol{\mu_m \cap \mu_n = \mu_{(m,n)}}$

Soluţie. *(a)* Dacă $m \mid n$, scriem $n = um$. Atunci, pentru orice $\alpha \in \boldsymbol{\mu_m}$ avem $\alpha^n = (\alpha^m)^u = 1^u = 1$, *i.e.* $\alpha \in \boldsymbol{\mu_n}$, aşa că $\boldsymbol{\mu_m \subseteq \mu_n}$.
Reciproc, presupunem că $\boldsymbol{\mu_m \subseteq \mu_n}$. Fie $\zeta = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$, generator al lui $\boldsymbol{\mu_m}$. Conform ipotezei, avem $\zeta \in \boldsymbol{\mu_n}$, adică $\zeta^n = 1$, sau $\cos\frac{2\pi n}{m} + i\sin\frac{2\pi n}{m} = 1$, de unde $\frac{2\pi n}{m} = 2\pi k$ pentru un anume $k \in \mathbb{Z}$, sau $n = km$, şi deci $m \mid n$.
*(b)* Fie $d = (m, n)$. Ştim că există $k, l \in \mathbb{Z}$ aşa încât $d = km + ln$. Dacă $\alpha \in \boldsymbol{\mu_m} \cap \boldsymbol{\mu_n}$, atunci $\alpha^d = (\alpha^m)^k(\alpha^n)^l = 1 \cdot 1 = 1$, *i.e.* $\alpha \in \boldsymbol{\mu_d}$. Astfel, $\boldsymbol{\mu_m \cap \mu_n \subseteq \mu_d}$. Invers, dacă $\alpha \in \boldsymbol{\mu_d}$, fie $u, v \in \mathbb{N}$ aşa încât $m = ud$ şi $n = vd$. Atunci $\alpha^m = (\alpha^d)^u = 1$ şi $\alpha^n = (\alpha^d)^v = 1$, adică $\alpha \in \boldsymbol{\mu_m}$ şi $\alpha \in \boldsymbol{\mu_n}$.

Iată şi impactul teoremei fundamentale a aritmeticii asupra grupurilor $\boldsymbol{\mu_n}$:

3. $\boldsymbol{\mu_n} = \bigcup_{d|n} P_d$, reuniunea fiind disjunctă (la finalul seminarului trecut, pentru orice $N \in \mathbb{N}$, s-a notat mulţimea rădăcinilor primitive de ordin $N$ ale unităţii cu $P_N$).

Soluţie. Să notăm $\bigcup_{d|n} P_d = P$. Dacă $\zeta$ e un element din $P$, înseamnă că există $d$ cu $d \mid n$ aşa încât $\langle\zeta\rangle = \boldsymbol{\mu_d}$, iar $\boldsymbol{\mu_d \subseteq \mu_n}$ (cf. ex. 2, *(a)*), şi deci $\zeta \in \boldsymbol{\mu_n}$. Astfel, $P \subseteq \boldsymbol{\mu_n}$.
Reciproc, fie $\alpha \in \boldsymbol{\mu_n}$. Atunci fie $d = ord(\alpha)$. Teorema lui Lagrange ne spune că ordinul subgrupului generat de $\alpha$ divide ordinul grupului ambiant $\boldsymbol{\mu_n}$, *i.e.* $d \mid n$. Apoi, deoarece $d = ord(\alpha)$, $\alpha^d = 1$, *i.e.* $\alpha \in \boldsymbol{\mu_d}$, şi cum $|\boldsymbol{\mu_d}| = |\langle\alpha\rangle| = d$, $\langle\alpha\rangle = \boldsymbol{\mu_d}$, *i.e.* $\alpha \in P_d$. Aşadar, avem

şi $\boldsymbol{\mu_n} \subseteq P$.
Mai rămâne de arătat că reuniunea e disjunctă, *i.e.* că pentru orice $d \neq d'$ cu $d \mid n$ şi $d' \mid n$ avem $P_d \cap P_{d'} = \emptyset$. Fie $x \in P_d \cap P_{d'}$. Atunci scriem $x = \cos\frac{2k\pi}{d} + i\sin\frac{2k\pi}{d}$, $0 \leq k < d$ şi $x = \cos\frac{2l\pi}{d'} + i\sin\frac{2l\pi}{d'}$, $0 \leq l < d'$, cu $(d,k) = 1$ şi $(d',l) = 1$, şi deci, de exemplu,

$$\sin\frac{2k\pi}{d} - \sin\frac{2l\pi}{d'} = 0$$

sau

$$2\cos\frac{\frac{2k\pi}{d} + \frac{2l\pi}{d'}}{2}\sin\frac{\frac{2k\pi}{d} - \frac{2l\pi}{d'}}{2} = 0$$

de unde

$$\frac{k\pi d' \pm l\pi d}{dd'} = 2r\pi$$

pentru un $r \in \mathbb{Z}$, sau $kd' \pm ld = 2rdd'$. De aici vedem că $d \mid kd'$, şi cum $(k,d) = 1$, rezultă că $d \mid d'$ (cf. sem. 11, ex. 4), dar şi că $d' \mid ld$, aşa că $d' \mid d$. Aşadar, $d = d'$.

Să extrapolăm puţin din prima parte a soluţiei excerciţiului precedent. Aţi văzut că toate subgrupurile lui $(\mathbb{Z}, +)$ sunt $n\mathbb{Z}$, cu $n \in \mathbb{N}$. Grupurile $\boldsymbol{\mu_n}$ sunt subgrupuri ale lui $(\mathbb{C}^*, \cdot)$ (mai precis, ale lui $S^1$): mai sunt şi altele? (finite, desigur). Avem:

4. Singurele subgrupuri finite ale lui $(\mathbb{C} \setminus \{0\}, \cdot)$ sunt $\boldsymbol{\mu_n}$-urile.

Soluţie. Fie $U$ un subgrup finit al grupului $(\mathbb{C}^*, \cdot)$. Atunci fie $n < \infty$ ordinul lui $U$ şi scriem $U = \{x_1, x_2, \ldots, x_n\}$. Ideea e să mai exprimăm $U$ într-un alt mod. Fie $x \in U$ oarecare. Atunci elementele $xx_i$ şi $xx_j$ sunt mutual diferite: dacă $i \neq j$, atunci $x_i \neq x_j$, deci $xx_i \neq xx_j$. Astfel, produsele $xx_i$, $i = \overline{1,n}$, acoperă întregul $U$, *i.e.* $U = \{xx_1, xx_2, \ldots, xx_n\}$ (produsele $xx_i$ se află în $U$ căci $U$ e subgrup!). În particular, elementul $xx_1 \cdot xx_2 \cdot \ldots \cdot xx_n$ trebuie să fie tot una cu elementul $x_1x_2\ldots x_n$, adică $x^n(x_1x_2\ldots x_n) = x_1x_2\ldots x_n$, de unde $x^n = 1$. Astfel, $x$ fiind ales arbitrar, vedem că $U \subseteq \boldsymbol{\mu_n}$, şi cum $|U| = n = |\boldsymbol{\mu_n}|$, rezultă $U = \boldsymbol{\mu_n}$.

Cam atât despre grupurile $\boldsymbol{\mu_n}$. Până să vedem aplicaţii concrete ale acestora care le relevă importanţa, vreau să zic două vorbe care (sper) să justifice de ce ne-am aştepra, înainte de toate, ca grupurile $\boldsymbol{\mu_n}$ să aibă un cuvânt important de spus. Deoarece, geometric, elementele lui $\boldsymbol{\mu_n}$ sunt vârfurile unui poligon regulat cu $n$ laturi înscris în cercul $S^1$, cu cât $n$ e mai mare, cu atât $\boldsymbol{\mu_n}$ e o mai bună aproximare a cercului.

Astfel, $\boldsymbol{\mu_n}$-urile sunt trunchieri ale cercului aşa cum pentru o funcţie infinit derivabilă $f$, sumele parţiale ale seriei Taylor sunt trunchieri ale lui $f$. Dar de la cerc putem să pornim fie pe un drum geometric, fie pe drumul analizei (de exemplu, analiza Fourier se ocupă cu problema reprezentării funcţiilor periodice cu ajutorul funcţiilor cos şi sin; dar a da o funcţie periodică definită pe $\mathbb{R}$, înseamnă a da o funcţie definită pe $S^1$, aşa că atunci când avem de-a face cu funcţii discrete, o idee pentru a le înţelege este să mimăm pentru $\boldsymbol{\mu_n}$-uri teoria Analizei Fourier). Concluzie: când ne aflăm într-un cadru în care nu mai avem parte de cerc aşa cum îl ştim (clasic), cum ar fi cadrurile date de $\mathbb{F}_q$-uri, $\boldsymbol{\mu_n}$-urile salvează situaţia. Dar atunci va interveni ceva nou pe lângă geometrie şi analiză: prin $\boldsymbol{\mu_n}$-uri se scurge şi informaţie de natură aritmetică!!! Într-adevăr, pentru orice $n \in \mathbb{N}$, $\boldsymbol{\mu_n} \simeq \mathbb{Z}_n$ via $\alpha_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mapsto k$, $k = \overline{0, n-1}$.

Înainte de a continua, o întrebare: care este varianta funcţională ("dual㔠) a afirmaţiei "... cadru *în* care nu avem parte de cerc?" Răspuns: "... cadru *pe* care nu avem parte de funcţia exponenţială $e^x$". De fapt, ca să ne înţelegem mai bine, iată încă o bijuterie a lui Euler: $e^{i\theta} = \cos\theta + i\sin\theta$, $\theta \in \mathbb{R}$. Intuitiv, de unde e scoasă minunăţia asta? Cu formula lui de Moivre scriem, pentru orice $n \in \mathbb{N}$, $\cos\theta + i\sin\theta = (\cos\frac{\theta}{n} + i\sin\frac{\theta}{n})^n$. Dar e bine cunoscută limita următoare: $\lim_{x\to 0}\frac{\sin x}{x} = 1$, adică, pentru valori mici ale lui $x$, $\sin x$ e aproape tot una cu $x$. Astfel, pentru valori mari ale lui $n$, cantitatea $(\cos\frac{\theta}{n} + i\sin\frac{\theta}{n})^n$ se apropie de $(1 + \frac{i\theta}{n})^n$, şi ştim că aceasta din urmă se duce către $e^{i\theta}$ ($e = \lim_{n\to\infty}(1 + \frac{1}{n})^n$). În particular, luând $\theta = \pi$, găsim că $e^{i\pi} + 1 = 0$ (sublim...). Totuşi, dincolo de estetică, importanţa formulei stă în faptul că ne relevă cum se extinde funcţia exponenţială de la $\mathbb{R}$ la $\mathbb{C}$...

Să revenim. Date două funcţii $f, g : \mathbb{N} \longrightarrow \mathbb{C}$ aşa încât $g(n) = \sum_{d|n} f(d)$, oricare ar fi $n$ (deci sumarea se face după toţi divizorii lui $n$), ar trebui să putem recupera şi pe $f$ din $g$. Însă care să fie "factorul" de compensare?

Definiţie. Funcţia aritmetică $\mu : \mathbb{N} \longrightarrow \mathbb{C}$, dată prin:

$$\mu(n) = \begin{cases} 1, & \text{pentru } n = 1 \\ (-1)^s, & \text{dacă } n = p_1 p_2 \dots p_s, \text{ cu } p_i \text{ prime distincte} \\ 0, & \text{în rest (adică dacă în descompunerea lui } n \text{ apar pătrate)} \end{cases}$$

se numeşte funcţia Möbius.

5. $\mu$ e multiplicativă.

Soluţie. Fie $m, n \in \mathbb{N}$ cu $(m, n) = 1$. Dacă $m = 1$ sau $n = 1$, e evident că $\mu(mn) = \mu(m)\mu(n)$. Dacă $m$ e de forma $m = p_1 p_2 \dots p_r$ şi $n$ e de forma $n = q_1 q_2 \dots q_s$, atunci descompunerea lui $mn$ în factori primi este

$$mn = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$$

pentru că $(m, n) = 1$, şi deci

$$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$$

În fine, dacă unul dintre $m$ şi/ sau $n$ nu e liber de pătrate, atunci nici $mn$ nu va fi liber de pătrate, şi deci $\mu(mn) = 0 = \mu(m)\mu(n)$.

6.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{dacă } n = 1 \\ 0, & \text{dacă } n > 1 \end{cases}$$

Soluţie. Dacă $n = 1$ e clar. Fie $n > 1$. Atunci scriem $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, $s \geq 1$. Deoarece $\mu$ nu vede "multiplicităţile", avem

$$\sum_{d|n} \mu(d) = \sum_{1 \leq i \leq s} \mu(p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_s^{\epsilon_s}) = \sum (-1)^{\sum \epsilon_i} = (1-1)^s = 0$$

(unde $\epsilon_i \in \{0, 1\}$) conform formulei binomiale (singura diferenţă ar fi că termenii din $\sum (-1)^{\sum \epsilon_i}$ vor apărea, posibil, în altă oridine faţă de cum apar termenii din dezvoltarea binomială a lui $(1 + (-1))^s$).

Acum putem vedea:

7. (inversiunea Möbius) Date două funcţii $f, g : \mathbb{N} \longrightarrow \mathbb{C}$, aşa încât $g(n) = \sum_{d|n} f(d)$, pentru orice $n$, avem că

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}), \quad \forall n.$$

Soluţie. Calculăm:

$$\begin{aligned} \sum_{d|n} \mu(d) g(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d'|n} \sum_{d|\frac{n}{d'}} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \end{aligned}$$

(dacă ne uităm la modul de sumare din expresia $\sum_{d|n}\mu(d)\sum_{d'|\frac{n}{d}}f(d')$, un moment de reflecţie vă convinge că, la nivelul argumentelor, când urcăm în prima sumă coborâm în a doua, şi invers, şi deoarece suntem în cadru comutativ, nu pierdem nimic dacă inversăm sumările). Dar pentru $d' \neq n$, avem că $\frac{n}{d'} \neq 1$, şi deci $\sum_{d|\frac{n}{d'}}\mu(d) = 0$, iar în $d' = n$ avem $\sum_{d|\frac{n}{d'}}\mu(d) = 1$ (cf. ex. 6), aşa că obţinem formula.

De fapt, aşa cum s-a remarcat, tot ceea ce a contat a fost că ne-am situat în cadru comutativ, aşa că avem:

8. Fie $G$ un grup abelian şi fie $f, g : \mathbb{N} \longrightarrow G$ două funcţii:
*(a)* (varianta aditivă) De obicei, un grup abelian e prezentat în scriere aditivă. În acest caz, enunţul, ca la ex. 7, dacă $g(n) = \sum_{d|n} f(d), \forall n$, atunci $f(n) = \sum_{d|n}\mu(d)g(\frac{n}{d}), \forall n$.
*(b)* (varianta multiplicativă) În schimb, dacă $G$ e prezentat în variantă multiplicativă, enunţul e astfel: dacă $g(n) = \prod_{d|n} f(d)$, atunci $f(n) = \prod_{d|n} g(\frac{n}{d})^{\mu(d)}, \forall n$.

Dar ce treabă are funcţia lui Möbius cu ce discutăm noi aici?

9. Fie $n \in \mathbb{N}$ oarecare şi fie $\mu$ funcţia lui Möbius. Atunci

$$\mu(n) = \sum_{\zeta \in P_n} \zeta$$

Soluţie. Considerăm funcţiile $S_1, S_2 : \mathbb{N} \longrightarrow \mathbb{C}$, date prin $S_1(n) = \sum_{\alpha \in \boldsymbol{\mu_n}} \alpha$ şi $S_2(n) = \sum_{\zeta \in P_n} \zeta$. Am văzut că $\boldsymbol{\mu_n} = \bigcup_{d|n} P_d$ disjunct (ex. 3), aşa că $S_1(n) = \sum_{d|n} S_2(n)$, oricare ar fi $n$, de unde, aplicând inversiunea Möbius (ex. 7)

$$S_2(n) = \sum_{d|n}\mu(d)S_1(\frac{n}{d}).$$

Însă $S_1(N)$ e uşor de calculat:

$$S_1(N) = \begin{cases} 1, & \text{dacă } N = 1 \\ 0, & \text{altminteri} \end{cases}$$

(e prima relaţie Viète: $X^N - 1 = \prod_{\alpha \in \boldsymbol{\mu_N}} (X - \alpha)$). Astfel, dacă $d < n$, avem $S_1(\frac{n}{d}) = 0$, iar pentru $d = n$ avem $S_1(\frac{n}{d}) = 1$, şi deci $S_2(n) = \mu(n)$.

Aceasta e doar o apariţie a unor cantităţi profunde ce se formează în Teoria Numerelor: sumele Ramanujan...

Ca să înţelegem imaginea de ansamblu, ne amintim ce spuneam în seminarul 5: intuiţia începe în mediul continuu. Atunci să ne uităm la ce se întâmplă în Analiza Matematică (fără a intra, din păcate, în detalii). Spuneam că problema iniţială din cadrul Analizei Fourier a fost să se decidă condiţii care să asigure exprimarea unei funcţii $f$ în funcţie de sin şi cos (raţiunile de la care a pornit Fourier se găsesc în fizică, anume rezolvarea ecuaţiei coardei vibrante şi a ecuaţiei căldurii, însă problema se impunea şi din raţiuni pur matematice, aşa cum arată vorbele lui Riemann din a sa teză de disertaţie). Mai precis, dată o funcţie
$f : [0, 1] \subset \mathbb{R} \longrightarrow \mathbb{R}$, când se întâmplă ca $f(x) = \sum_{n=0}^{\infty} A_n \cos nx + B_n \sin nx$? Sau, folosind formula lui Euler, putem exprima speranţa mai condensat sub forma $f(x) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n x}$, iar aşteptările asupra coeficienţilor $a_n$ sunt următoarele:

$$a_n = \int_0^1 f(x) e^{2\pi i n x} dx$$

Sunt varii rezultate care asigură răspuns pozitiv, însă trebuie făcute precise lucrurile asupra convergenţei seriei... În orice caz, e clar ce condiţie trebuie impusă de la bun început: $f$ trebuie să fie periodică pe $\mathbb{R}$. Apoi, ca să se trateze analog şi funcţiile $\mathbb{R} \longrightarrow \mathbb{R}$ ce nu sunt neapărat periodice, înlocuim limbajul discret cu cel continuu: înlocuim întregii $n \in \mathbb{Z}$ ce indexează coeficienţii $a_n$ cu numere reale, şi înlocuim sumele $\sum_{n=-\infty}^{\infty}$ cu integrale $\int_{-\infty}^{\infty}$. Astfel, dată $f : \mathbb{R} \longrightarrow \mathbb{R}$, suntem conduşi la a considera funcţia

$$\hat{f} : \mathbb{R} \longrightarrow \mathbb{R}$$
$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$$

(varianta continuă a coeficienţilor $a_n$, $n \in \mathbb{Z}$) şi să vedem când se întâmplă ca

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi) e^{2\pi i x \xi} d\xi$$

(varianta continuă a exprimării $f(x) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n x}$). Din nou, visul acesta nu se îndeplineşte mereu: trebuie impuse nişte condiţii tehnice de regularitate asupra lui $f$. În fine, spaţiul Schwarz este răspunsul, notat $\mathcal{S}(\mathbb{R})$:

Teoremă. Dacă $f \in \mathcal{S}(\mathbb{R})$, atunci avem că

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi) e^{2\pi i x \xi} d\xi$$

Acum, mai uitaţiv-ă încă o dată la ex. 7 şi la ex. 9! Într-adevăr, formula de inversiune a lui Möbius e încă un semnal al *motivelor*; ăsta-i şi cazul legii de reciprocitate pătratică a lui Gauss...

Acum să revenim la subiectul nostru: aritmetica polinoamelor. Închegăm elementele grupului $\boldsymbol{\mu_n}$ în polinomul

$$\Phi_n(X) = \prod_{\zeta \in P_n} (X - \zeta)$$

(al $n$-lea polinom ciclotomic). Iată cum se prezintă teorema fundamentală a aritmeticii aici:

10. (Dedekind)

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Soluţie. Ţinând cont de cum este afectat $\boldsymbol{\mu_n}$ de teorema fundamentală (ex. 3), avem

$$\begin{aligned} X^n - 1 &= \prod_{\alpha \in \boldsymbol{\mu_n}} (X - \alpha) = \prod_{\alpha \in \cup_{d|n} P_d} (X - \alpha) \\ &= \prod_{d|n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d|n} \Phi_d. \end{aligned}$$

În treacăt observăm şi următoarea consecinţă:

11. (Gauss) Pentru orice $n \in \mathbb{N}$,

$$\sum_{d|n} \varphi(d) = n,$$

$\varphi$ fiind funcţia lui Euler.

Soluţie. Trecem la grade în relaţia lui Dedekind.

Nu e chiar corect ce-am spus: încă nu ştim că $\Phi_n$-urile sunt ireductibile peste $\mathbb{Q}$! Vom vedea data viitoare că, într-adevăr, descompunerea din ex. 10 e cea a lui $X^n - 1$ în factori primi în $\mathbb{Q}[X]$, apoi o aplicaţie surprinzătoare a polinoamelor ciclotomice, şi (probabil) nişte exerciţii recapitulative.