# Extinderi de inele şi corpuri - o posibilă lecţie de recapitulare finală

***Dumitru GHERMAN*** [1]

Pentru ca recapitularea să aibă eficienţă, trebuie ca în organizarea ei să se ţină de unele principii:

- la recapitulare nu se parcurge din nou întreaga materie;
- trebuie să se urmărească, pe cât este posibil, realizarea unei legături între diversele ramuri ale matematicii şcolare;
- recapitularea trebuie să aducă elemente noi, probleme care pot fi rezolvate prin prelucrarea creatoare a cunoştinţelor anterioare;
- se are în vedere stimularea lucrului individual al elevului, folosind bibliografia indicată de profesor şi / sau căutând noi surse;
- recapitularea trebuie să ţină cont de structura şi cerinţele examenelor şcolare.

În cele ce urmează, vom prezenta un proiect didactic pentru o posibilă lecţie de recapitulare finală la clasa a XII-a. Nu ne propunem să rezolvăm toate problemele sau să demonstrăm toate teoremele ce vor apărea; majoritatea aparţin fondului clasic şi poate fi consultată bibliografia.

**I. Inelul întregilor pătratici.** Fie $d$ un număr întreg liber de pătrate; definim

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{x \in \mathbb{C} \mid x = m + n\sqrt{d},\ m, n \in \mathbb{Z}\right\}.$$

**1)** $\left(\mathbb{Z}\left[\sqrt{d}\right]; +, \cdot\right)$ este un subinel al corpului numerelor complexe, chiar domeniu de integritate.

**2)** $\mathbb{Z}\left[\sqrt{d}\right]$ este izomorf cu inelul matricelor de forma $\begin{pmatrix} m & n \\ dn & m \end{pmatrix}$, $m, n \in \mathbb{Z}$, în raport cu operaţiile uzuale cu matrice.

**3)** Inelele $\mathbb{Z}\left[\sqrt{d}\right]$ şi $\mathbb{Z}\left[\sqrt{d'}\right]$ sunt izomorfe dacă şi numai dacă $d = d'$ (se arată în primul rând că un izomorfism $f$ între cele două inele invariază elementele lui $\mathbb{Z}$ şi atunci el este bine determinat de valoarea $f\left(\sqrt{d}\right)$).

**4)** Subinelele unitare ale lui $\mathbb{Z}\left[\sqrt{d}\right]$ sunt de forma

$$A_n = \left\{a + bn\sqrt{d} \mid a, b \in \mathbb{Z}\right\}, \quad n \in \mathbb{N}.$$

**5)** Definim aplicaţia *normă* $N : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}$, $N\left(m + n\sqrt{d}\right) = m^2 - dn^2$. Dacă notăm cu $\bar{x} = m - n\sqrt{d}$ conjugatul întregului pătratic $x = m + n\sqrt{d}$, se arată că $N$ are proprietăţi asemănătoare modulului: $N(x) = x \cdot \bar{x}$, $N(xy) = N(x) \cdot N(y)$. De aici, $x \in U\left(\mathbb{Z}\left[\sqrt{d}\right]\right) \Leftrightarrow N(x) \in U(\mathbb{Z}) = \{\pm 1\}$.

**6)** Grupul multiplicativ al elementelor inversabile din $\mathbb{Z}[i]$ este $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

[1] Profesor, Liceul Teoretic "Mihail Sadoveanu", Paşcani

**7)** Fie $\alpha \in \mathbb{C} \backslash \mathbb{Q}$ astfel încât mulţimea $A = \{m + n\alpha \mid m, n \in \mathbb{Z}\}$ este inel faţă de operaţiile uzuale din $\mathbb{C}$. Dacă $A$ are exact patru elemente inversabile, atunci $A = \mathbb{Z}[i]$.

**8)** Dacă $d \in \{2, 3, 5\}$, atunci $U(\mathbb{Z}[d])$ conţine o infinitate de elemente şi putem găsi în $U(\mathbb{Z}[d])$ elemente pozitive oricât de mici (este suficient să găsim un singur element, considerând apoi puterile acestuia şi conjugatele lor).

Problemele **1-6** sunt rezolvate în [**3**]; problema **7** a fost propusă de *Marcel Ţena* la etapa finală a Olimpiadei de Matematică în 1997, iar **8** poate fi găsită în variantele examenului de bacalaureat din ultimii ani.

**II Corpul numerelor pătratice.** Fie $d$ un număr întreg liber de pătrate; definim

$$\mathbb{Q}\left(\sqrt{d}\right) = \left\{z \in \mathbb{C} \mid z = a + b\sqrt{d},\ a, b \in \mathbb{Q}\right\}.$$

**1)** $\left(\mathbb{Q}\left(\sqrt{d}\right); +, \cdot\right)$ este subcorp al lui $\mathbb{C}$ (inversul elementului nenul $a + b\sqrt{d}$ este $\frac{1}{a^2 - db^2}\left(a - b\sqrt{d}\right) \in \mathbb{Q}\left(\sqrt{d}\right)$, deoarece $a^2 - db^2 \neq 0$; altfel, se ajunge la $\sqrt{d} = \pm\frac{a}{b} \notin \mathbb{R}\backslash\mathbb{Q}$!).

**2)** $\mathbb{Q}\left(\sqrt{d}\right)$ este izomorf cu mulţimea matricelor de forma $\begin{pmatrix} a & b \\ db & a \end{pmatrix}$, $a, b \in \mathbb{Q}$, care formează corp în raport cu operaţiile uzuale.

**3)** Corpurile $\mathbb{Q}\left(\sqrt{d}\right)$ şi $\mathbb{Q}\left(\sqrt{d'}\right)$ sunt izomorfe dacă şi numai dacă $d = d'$; singurele automorfisme ale corpului $\mathbb{Q}\left(\sqrt{d}\right)$ sunt aplicaţia identică şi cea de conjugare, ambele invariind elementele lui $\mathbb{Q}$.

**4)** Dacă un subcorp $K \subset \mathbb{C}$ este astfel încât $End\ K = \{f, g\}$ şi $f(x) = g(x) \Rightarrow x \in \mathbb{Q}$, atunci există un întreg liber de pătrate $d \neq 1$ pentru care $K = \mathbb{Q}\left(\sqrt{d}\right)$.

**5)** Dacă $f \in \mathbb{Q}[x]$, atunci $f(\bar{z}) = \overline{f(z)}$, $\forall z \in \mathbb{Q}\left(\sqrt{d}\right)$; de aici urmează că orice polinom cu coeficienţi raţionali, are eventualele rădăcini din $\mathbb{Q}\left(\sqrt{d}\right)$ în perechi conjugate.

Problemele **1-3** pot fi găsite în [**3**], problema **4** a fost propusă la etapa finală a Olimpiadei de Matematică din 1988 de către *Marcel Ţena*, iar **5** poate fi rezolvată urmând pas cu pas demonstrarea unor rezultate analoage din manuale.

**III Extinderi pătratice. Corpuri pitagorice.** Fie $r \in \mathbb{Q}_+^*$ astfel încât $\sqrt{r} \notin \mathbb{Q}$; definim ca mai sus corpul $\mathbb{Q}(\sqrt{r})$, care este subcorp al lui $\mathbb{R}$ din pozitivitatea lui $r$.

**1)** $\mathbb{Q}(\sqrt{r})$ este cel mai mic subcorp al lui $\mathbb{R}$ care include $\mathbb{Q} \cup \{\sqrt{r}\}$.

**2)** Putem gândi pe $\mathbb{Q}(\sqrt{r})$ ca un $\mathbb{Q}$-spaţiu vectorial, definind înmulţirea "vectorilor" din $\mathbb{Q}(\sqrt{r})$ cu "scalari" din $\mathbb{Q}$ prin restricţionarea înmulţirii obişnuite din $\mathbb{Q}(\sqrt{r})$ (de fapt, din $\mathbb{R}$). Dimensiunea acestui spaţiu vectorial este 2, o bază fiind $\{1, \sqrt{r}\}$ (a se găsi şi alte baze!).

**3)** Polinomul $f = X^2 - r \in \mathbb{Q}[X]$ este ireductibil peste $\mathbb{Q}$, dar admite rădăcina $\sqrt{r}$ în $\mathbb{Q}(\sqrt{r})$; orice alt polinom $g \in \mathbb{Q}[X]$ care admite rădăcina $\sqrt{r}$ se divide prin $f$. Spunem că $f$ este *polinomul minimal* al lui $\sqrt{r}$.

**4)** Din puncte de vedere geometric, extinderea lui $\mathbb{Q}$ la $\mathbb{Q}\left(\sqrt{d}\right)$ se face utilizând compasul. De exemplu, $\sqrt{r}$ este abscisa unuia dintre punctele de intersecţie ale cercului de centru $O$ şi rază $\frac{1}{2}(r+1)$ cu dreapta $y=\frac{1}{2}(r-1)$.

**5)** Considerând $r_1, r_2, \dots \in \mathbb{Q}_+^*$, definim $\mathbb{Q}_{r_1}=\mathbb{Q}\left(\sqrt{r_1}\right)$, $\mathbb{Q}_{r_2}=\mathbb{Q}_{r_1}\left(\sqrt{r_2}\right)$, ... , $\mathbb{Q}_{r_n}=\mathbb{Q}_{r_{n-1}}\left(\sqrt{r_n}\right)$, ... ; spunem că am *adjuncţionat* la $\mathbb{Q}$, pe rând, elementele $\sqrt{r_1}, \sqrt{r_2}, \dots, \sqrt{r_n}, \dots$ . Am construit astfel şirul de extinderi

$$\mathbb{Q} \subset \mathbb{Q}_{r_1} \subset \mathbb{Q}_{r_2} \subset \dots \subset \mathbb{Q}_{r_n} \subset \dots \subset \mathbb{R}.$$

Cum $\mathbb{Q}$ este mulţime numărabilă, putem alege $r_1, r_2, \dots, r_n, \dots$ astfel încât orice număr obţinut, pornind de la $\mathbb{Q}$, prin efectuarea unui număr finit de adunări, scăderi, înmulţiri, împărţiri şi extrageri de rădăcini pătrate (un astfel de număr se numeşte *număr pitagoric*) să aparţină unui anumit $\mathbb{Q}_{r_n}$. Notăm $\mathbb{K}=\bigcup\limits_n \mathbb{Q}_{r_n}$ - mulţimea numerelor pitagorice; se arată că aceasta nu depinde de alegerea şirului $r_1, r_2, \dots, r_n, \dots$ şi că formează un subcorp al lui $\mathbb{R}$, închis la operaţiile aritmetice şi la extragerea rădăcinii pătrate şi care este "cel mai mic" (în sensul incluziunii) cu aceste proprietăţi.

**IV Construcţii cu rigla şi compasul.**

1) Dacă $L$ este un subcorp al lui $\mathbb{R}$ iar $(D)$ este o dreptă ce trece prin două puncte având coordonatele în $L \times L$, atunci ecuaţia dreptei are coeficienţi din $L$. Analog, un cerc care are centrul de coordonate din $L \times L$ şi trece printr-un astfel de punct, are coeficienţii ecuaţiei sale din $L$.

2) Fie $L$ subcorp în $\mathbb{R}$, iar $M(x,y)$ un punct în plan; spunem că $M$ *este constructibil cu rigla şi compasul* plecând de la $L$ dacă el poate fi obţinut prin intersecţii de drepte şi cercuri având coeficienţii în $L$. Dacă $M$ este un astfel de punct, atunci fie $x, y \in L$, fie există $u \in L, u>0$ astfel încât $x, y \in L(\sqrt{u})$.

3) Numim *număr constructibil cu rigla şi compasul* un număr real ce este coordonată a unui punct constructibil. Se arată că orice număr real constructibil este totodată şi număr pitagoric. Ca o consecinţă, polinomul minimal al unui număr constructibil are gradul putere a lui 2. De aici rezultă *imposibilitatea dublării cubului, trisecţiei unghiului şi cuadraturii cercului* (pentru amănunte, v.[**1**],[**2**],[**4**]).

4) Corpul ordonat $\mathbb{K} \subset \mathbb{R}$ se bucură de un anumit tip de completitudine, numită *completitudine euclidiană*: cercetat cu rigla şi compasul, nu se va putea spune niciodată că lipseşte vreun punct. Tocmai confuzia dintre această completitudine şi *completitudinea Cantor - Dedekind* a lui $\mathbb{R}$ a întârziat soluţionarea problemelor clasice ale antichităţii.

**Bibliografie**


1. **T. Bîrsan** - *Trisecţia unghiului*, Recreaţii Matematice, 2/2001, 38-41.
2. **E. Moise** - *Geometrie elementară dintr-un punct de vedere superior*, E.D.P., Bucureşti, 1980.
3. **C. Niţă, T. Spircu** - *Probleme de structuri algebrice*, Ed. Tehnică, Bucureşti, 1974.
4. **I. Tofan, C. Volf** - *Algebră - Inele, Module, Teorie Galois*, Ed. Matrix-Rom, Bucureşti, 2001.