Polinoame şi ecuaţii algebrice

Andrei Mărcuş

Cuprins

Introducere

Până la începutul secolului XIX, scopul principal al algebrei era găsirea formulelor de rezolvare a ecuaţii algebrice, adică exprimarea soluţiilor în funcţie de coeficienţi, folosind expresii cu radicali. Dacă babilonienii şi egiptenii antici ştiau să rezolve unele ecuaţii de gradul 2, doar în perioada Renaţerii italiene au fost obţinute formulele de rezolvare pentru ecuaţiile de gradul 3 şi 4. A reieşit că problema, formulată astfel, nu are întotdeauna soluţie, Paolo Ruffini şi Niels Henrik Abel demonstrând la începutul secolului 19 că ecuaţia generală de grad mai mare sau egal cu 5 nu e rezolvabilă prin radicali. Teoria lui Galois (1830), care asociază un grup fiecărei ecuaţii şi trage concluzii asupra ecuaţiei din studiul structurii gupului, a facut lumină asupra acestui subiect. Ideea originală a lui Abel şi Galois a fost să investigheze permutările rădăcinilor ecuaţiei, ei devenind astfel creatorii teoriei grupurilor.

Prezentul volum îşi are originea în cursurile predate de autor la Facultatea de Matematică şi Informatică a Universităţii Babeş-Bolyai din Cluj. Prezentăm o serie de probleme clasice, dar abordarea se bazează pe studiul sistematic al algebrelor de polinoame şi al extinderilor de corpuri comutative, precum şi al diferitelor structuri de grup asociate acestora. Cartea este destinată în primul studenţilor masteranzi şi profesorilor de matematică, parcurgerea ei necesitând familiaritate cu noţiunile şi rezultatele fundamentale din teoria grupurilor, teoria inelelelor şi algebra liniară.

Ecuaţii algebrice | 1

Începem cu prezentarea a câtorva metode clasice de rezolvare a unor ecuaţii cu coeficienţi complecşi. Ecuaţia de gradul 2 a fost în esenţă rezolvată deja în antichitate de către babilonieni, în timp ce soluţiile ecuaţiilor de gradul 3 şi 4 au fost descoperite de matematicieni italieni din perioada Renaşterii.

1.1 Ecuaţii binome. Grupul rădăcinilor unităţii

Fie $n \in \mathbb{N}$, $n \geq 1$ şi considerăm întâi ecuaţia

$$x^n = 1 \tag{1.1}$$

în $\mathbb{C}$. Notăm cu U_n mulţimea rădăcinilor acestui polinom. Elementele mulţimii U_n se numeşte **rădăcini de ordinul** n **ale unităţii**. Este uşor de arătat că $(\mathrm{U}_n, \cdot)$ este grupul ciclic generat de $\varepsilon_1 := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ şi $(\mathrm{U}_n, \cdot) \simeq (\mathbb{Z}_n, +)$.

Exerciţiul 1.1. Să se arate că

$$\mathrm{U}_n := \{\varepsilon_k := \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1\}$$

Considerăm acum **ecuaţia binomă**

$$x^n = z, \tag{1.2}$$

unde $z = r(\cos t + i\sin t) \in \mathbb{C}$ este dat.

Exerciţiul 1.2. Să se arate că soluţiile ecuaţiei binome sunt

$$x_k := \sqrt[n]{r}(\cos(t + 2k\pi)/n + i\sin(t + 2k\pi)/n) = x_0\varepsilon_k,$$

unde $k \in \{0, \ldots, n-1\}$. Aceste soluţii sunt vârfurile unui poligon regulat cu n laturi înscris în cercul de centru O şi rază $\sqrt[n]{r}$.

1.2 Ecuaţia de gradul 2

Considerăm ecuaţia cu coeficienţi complecşi

$$y^2 + ay + b = 0. \tag{1.3}$$

Substituim pe y cu $x - a/2$ şi obţinem ecuaţia binomă

$$x^2 = a^2/4 - b, \tag{1.4}$$

cu soluţiile $x_{1,2} = \pm\sqrt{a^2/4 - b}$; rezultă că $y_{1,2} = x_{1,2} - a/2$.

1.3 Ecuaţia de gradul 3

Considerăm ecuaţia cu coeficienţi complecşi cu soluţiile $y_1, y_2, y_3 \in \mathbb{C}$

$$y^3 + ay^2 + by + c = 0 \tag{1.5}$$

Substituim pe y cu $x - a/3$ şi obţinem ecuaţia

$$x^3 + x(b - a^2/3) + (2a^3/27 - ab/3 + c) = 0,$$

deci este suficient de studiat ecuaţia de forma

$$x^3 + px + q = 0. \tag{1.6}$$

Formulele lui Cardano

Această metodă este datorată lui Scipione del Ferro (1465-1526), Niccolò Tartaglia (1499-1557) şi Gerolamo Cardano (1501-1576).

Căutăm soluţia x sub forma $x = u + v$. Din egalitatea $(u+v)^3 = u^3 + v^3 + 3uv(u+v)$ rezultă că $(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$, adică $x^3 - 3uvx - (u^3+v^3) = 0$. Atunci avem

$$\begin{cases} -3uv & = p \\ -(u^3+v^3) & = q \end{cases} \Longleftrightarrow \begin{cases} uv & = -p/3 \\ u^3+v^3 & = -q \end{cases} \Longrightarrow \begin{cases} u^3v^3 & = -p^3/27 \\ u^3+v^3 & = -q; \end{cases}$$

rezultă că u^3 şi v^3 sunt rădăcinile ecuaţiei $z^2 + qz - p^3/27 = 0$, adică

$$z_{1,2} = -q/2 \pm \sqrt{p^3/27 + q^2/4}.$$

Fie $u, v \in \mathbb{C}$ astfel încât $u^3 = z_1$ şi $v^3 = z_2$ şi $uv = -p/3$; atunci soluţiile căutate sunt:

$$x_1 = u + v,\ x_2 = \varepsilon u + \varepsilon^2 v,\ x_3 = \varepsilon^2 u + \varepsilon v,$$

unde $\varepsilon \neq 1$ este o radăcină de ordinul 3 a unităţii. (Metoda rezolventei lui Lagrange conduce la aceleaşi calcule.)

Exerciţiul 1.3. a) Să se arate că x_1, x_2, x_3 sunt într-adevăr rădăcinile ecuaţiei $x^3 + px + q = 0$, adică au loc formulele lui Viete:

$$x_1 + x_2 + x_3 = 0, \qquad x_1x_2 + x_2x_3 + x_1x_3 = p, \qquad x_1x_2x_3 = -q.$$

b) Să se rezolve ecuaţiile:

1. $y^3 + 6y^2 + 21y + 52 = 0$.
2. $y^3 + 3y^2 - 3y - 14 = 0$.

c) (*Discuţia ecuaţiei cu coeficienţi reali*) Presupunem că $p, q \in \mathbb{R}$. Discriminantul polinomului $f = X^3 + pX + q$ este definit prin $\Delta(f) := -4p^3 - 27q^2 = -108(\frac{q^2}{4} + \frac{p^3}{27})$. Să se arate că:

1. Dacă $\Delta(f) < 0$, atunci $x_1 \in \mathbb{R}$ şi $x_2, x_3 \in \mathbb{C}$ sunt conjugate.
2. Dacă $\Delta(f) = 0$, atunci $x_1 = 2\alpha,\ x_2 = x_3 = -\alpha \in \mathbb{R}$.
3. Dacă $\Delta(f) > 0$, atunci x_1, x_2, x_3 sunt distincte două câte două (*casus irreducibilis*).

1.4 Ecuaţia de gradul 4

Considerăm ecuaţia cu coeficienţi complecşi cu soluţiile $y_1, y_2, y_3, y_4 \in \mathbb{C}$

$$y^4 + ay^3 + cy^2 + dy + e = 0. \tag{1.7}$$

Substituim pe y cu $x - a/4$; rezultă că este suficient de studiat ecuaţia de forma

$$x^4 + px^2 + qx + r = 0. \tag{1.8}$$

Metoda rezolventei lui Lagrange (1736-1813)

Căutăm soluţia x sub forma $x = u+v+w$. Observăm că $(u+v+w)^2 = u^2+v^2+w^2+2(uw+vw+uv)$, adică $(u+v+w)^2-(u^2+v^2+w^2) = 2(uw+vw+uv)$. Ridicând la puterea a doua obţinem $(u+v+w)^4-2(u+v+w)^2(u^2+v^2+w^2)+(u^2+v^2+w^2)^2 = 4(u^2w^2+v^2w^2+u^2v^2)+8uvw(u+v+w)$. Rezultă că

$$x^4-2(u^2+v^2+w^2)x^2-8uvwx-2(u^2v^2+u^2w^2+v^2w^2)+u^4+v^4+w^4 = 0,$$

deci

$$\begin{cases} u^2+v^2+w^2 & = -p/2 \\ u^2v^2+u^2w^2+v^2w^2 & = (p^2-4r)/16\,; \\ u^2v^2w^2 & = q^2/64 \end{cases}$$

rezultă că u^2, v^2, w^2 sunt soluţiile ecuaţiei de gradul 3

$$z^3+(p/2)z^2+((p^2-4r)/16)z-q^2/64 = 0.$$

Fie z_1, z_2, z_3 rădăcinile acesteia, şi fie

$$u = \pm\sqrt{z_1},\ v = \pm\sqrt{z_2},\ w = \pm\sqrt{z_3}$$

astfel încât $uvw = -q/8$. Atunci

$$x_1 = u+v+w,\ x_2 = u-v-w,\ x_3 = -u+v-w,\ x_4 = -u-v+w.$$

Exerciţiul 1.4. a) Să se arate că x_1, x_2, x_3, x_4 sunt într-adevăr rădăcinile ecuaţiei $x^3+px^2+qx+r = 0$, adică au loc formulele lui Viete:

- $x_1+x_2+x_3+x_4 = 0$,
- $x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4 = p$,
- $x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_3 = -q$,
- $x_1x_2x_3x_4 = r$.

b) Să se rezolve ecuaţia $y^4-4y^3-6y^2-92y-91 = 0$.

Metoda lui Lodovico Ferrari (1522-1565)

Ecuaţia $x^4 + px^2 + qx + r = 0$ (unde $q \neq 0$, deoarece dacă $q = 0$, atunci avem o **ecuaţie bipătrată** uşor de rezolvat) se scrie sub forma

$$(x^2 + (p/2) + \alpha)^2 - (2\alpha x^2 - qx + (\alpha^2 + p\alpha - r + (p^2/4)) = 0,$$

unde al doilea termen este pătrat perfect dacă α satisface ecuaţia de gradul 3

$$q^2 - 8\alpha(\alpha^2 + p\alpha - r + p^2/4) = 0.$$

Cu α astfel determinat, obţinem ecuaţia

$$(x^2 + p/2 + \alpha)^2 - 2\alpha(x - q/(4\alpha))^2 = 0,$$

deci notând $\theta^2 := 2\alpha$, este suficient de rezolvat ecuaţiile de gradul al doilea

$$x^2 - \theta x + (p/2 + \alpha + q/(2\theta)) = 0, \qquad x^2 + \theta x + (p/2 + \alpha - q/(2\theta)) = 0.$$

Exerciţiul 1.5. Să se rezolve ecuaţia $x^4 + px^2 + qx + r = 0$ descompunând

$$x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 + cx + d).$$

Polinoame 2

Prezentăm construcţia formală a algebrei de polinoame în una sau mai multe nedeterminate cu coeficienţi într-un inel asociativ, comutativ cu unitate.

2.1 Polinoame într-o nedeterminată

În acest paragraf, notăm cu A un inel asociativ, comutativ cu unitate.

2.1.1 Construcţia inelului de polinoame

Fie $A^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to A\}$ a mulţimea *şirurilor* cu termeni din A. Dacă $f \in A^{\mathbb{N}}$, atunci notăm $f = (a_0, a_1, \dots)$, unde $a_n = f(n)$ pentru orice $n \in \mathbb{N}$.

Pe mulţimea $A^{\mathbb{N}}$ definim următoarele operaţii: dacă $f = (a_0, a_1, \dots)$ şi $g = (b_0, b_1, \dots)$, atunci

$$(f+g)(n) = f(n) + g(n) = a_n + b_n,$$
$$(fg)(n) = \sum_{i+j=n} f(i)g(j) = \sum_{i+j=n} a_i b_j.$$

Mai departe, fie

$$\operatorname{supp}(f) = \{n \in \mathbb{N} \mid a_n \neq 0\}$$

suportul lui f, şi fie

$$A^{(\mathbb{N})} = \{f \in A^{\mathbb{N}} \mid \operatorname{supp}(f) \text{ mulţime finită}\}.$$

Teorema 2.1.1. a) *$A^{\mathbb{N}}$ inel comutativ cu unitate.*

b) *$A^{(\mathbb{N})}$ este subinel unital al lui $A^{\mathbb{N}}$, iar*

$$\iota_A : A \to A^{(\mathbb{N})}, \quad \iota_A(a) = (a, 0, 0, \dots)$$

este morfism unital injectiv de inele. (Identificăm pe a cu $\iota_A(a)$.)

c) *Fie* $X = (0,1,0,\dots)$. *Dacă* $f \in A^{(\mathbb{N})}$ *astfel încât* $a_i = 0$ *pentru orice* $i > n$, *atunci*

$$f = a_0 + a_1 X + \dots a_n X^n = \sum_{k=0}^{n} a_k X^k,$$

şi această scriere este unică.

Demonstraţie. a) Este uşor de văzut că $(A^{\mathbb{N}},+)$ este grup abelian. Studiem proprietăţile înmulţirii. Deoarece A este inel comutativ, rezultă că „$\cdot$” este operaţie comutativă. Dacă $f,g,h \in A^{\mathbb{N}}$, atunci pentru orice $n \in \mathbb{N}$ avem

$$\begin{aligned}
((f+g)h)(n) &= \sum_{i+j=n} (f+g)(i)h(j) \\
&= \sum_{i+j=n} (f(i)+g(i))h(j) \\
&= \sum_{i+j=n} (f(i)h(j)+g(i)h(j)) \\
&= \sum_{i+j=n} f(i)h(j) + \sum_{i+j=n} g(i)h(j) \\
&= (fh)(n) + (gh)(n) = (fh+gh)(n),
\end{aligned}$$

$$\begin{aligned}
((fg)h)(n) &= \sum_{i+j=n} (fg)(i)h(j) \\
&= \sum_{i+j=n} (\sum_{k+l=i} (f(k)g(l))h(j) \\
&= \sum_{k+l+j=n} f(k)g(l)h(j) \\
&= \sum_{k+m=n} f(k) \sum_{l+j=m} g(l)h(j) \\
&= \sum_{k+m=n} (f(k)(gh)(m) = (f(gh))(n).
\end{aligned}$$

În fine, elementul unitate al lui $A^{\mathbb{N}}$ este $1 = (1,0,0,\dots)$.

b) Observăm că $0 = (0,0,\dots)$, $1 = (1,0,\dots) \in A^{(\mathbb{N})}$, şi dacă $f,g \in A^{(\mathbb{N})}$ astfel încât $f(i) = 0$ dacă $i > m$, $g(j) = 0$ dacă $j > n$, atunci $(f+g)(i) = 0$ dacă $i > \max\{m,n\}$, $(-f)(i) = 0$ dacă $i > m$, şi $(fg)(i) = 0$ dacă $i > m+n$. Proprietăţile operaţilor se moştenesc şi vedem uşor că ι_A este morfism unital injectiv de inele.

c) Observăm că $X^k(i) = \delta_{ik}$, adică,

$$X^k = (\underset{0}{0}, \underset{1}{0}, \dots, 0, \underset{k}{1}, 0, \dots),$$

şi dacă $a = \iota_A(a) = (a, 0, \dots)$, atunci $(aX^k)(i) = a\delta_{ik}$; rezultă că

$$\begin{aligned} f &= (a_0, a_1, \dots, a_n, 0, \dots) \\ &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots) \\ &= \sum_{k=0}^{n} a_k X^k, \end{aligned}$$

şi unicitatea scrierii este evidentă. □

Definiţia 2.1.2. a) $A^{\mathbb{N}}$ se numeşte *inelul seriilor formale* cu coeficienţi în A, iar $A^{(\mathbb{N})}$ se numeşte *inelul de polinoame cu coeficienţi în A şi nedeterminata X*; elementele $a_i := f(i) \in A$ sunt *coeficienţii* lui f.

Notaţii: $A^{\mathbb{N}} = A[[X]]$, $A^{(\mathbb{N})} = A[X] = \{f = \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N},\ a_i \in A\}$.

Dacă $f = (a_0, a_1, \dots) \in A[[X]]$, atunci folosim notaţia formală $f = \sum_{i=0}^{\infty} a_i X^i$.

b) Dacă $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ este un polinom nenul, atunci

$$\deg(f) = \max\{i \in \mathbb{N} \mid a_i \neq 0\}$$

este *gradul* lui f. Prin definiţie, $\deg 0 = -\infty$.

c) Dacă $\deg(f) = n$, atunci a_n este *coeficientul dominant* al lui f. În acest caz, dacă $a_n = 1$, atunci spunem că f este polinom monic.

d) Dacă $f \in A[[X]]$ este o serie formală, atunci $o(f) = \min\{n \in \mathbb{N} \cup \{\infty\} \mid a_n \neq 0\}$ este *ordinul* lui f.

Exerciţiul 2.1. a) Dacă $f, g \in A[X]$, atunci

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}, \quad \deg(fg) \leq \deg(f)\deg(g).$$

b) Dacă A este domeniu de integritate, atunci şi $A[X]$ este domeniu de integritate, şi $\deg(fg) = \deg(f)\deg(g)$.

c) $a \in A$ este inversabil în $A[X] \Leftrightarrow a$ este inversabil în A.

d) Dacă A domeniu de integritate, atunci $\mathrm{U}(A[X]) = \mathrm{U}(A)$.

Exerciţiul 2.2. Fie A un comutativ cu unitate inel, şi $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$. Să se arate că:

a) f divizor al lui zero $A[X] \Leftrightarrow (\exists)a \in A,\ a \neq 0$ astfel încât $af = 0$.

b) f este inversabil în $A[X] \Leftrightarrow a_0$ este inversabil în A şi a_i sunt elemente nilpotente, dacă $i \geq 1$.

c) f este nilpotent în $A[X] \Leftrightarrow a_0, \ldots, a_n$ sunt elemente nilpotente.

Exerciţiul 2.3. Fie $f, g \in A[[X]]$. Să se arate că:

a) $o(f+g) \geq \min\{o(f), o(g)\}$; $o(fg) \geq o(f) + o(g)$.

b) Dacă A domeniu de integritate, atunci şi $A[[X]]$ este domeniu de integritate.

c) f este inversabil în $A[[X]] \Leftrightarrow a_0$ este inversabil în A.

d) Să se calculeze inversul lui $1 + X$.

2.1.2 Proprietatea de universalitate a inelului de polinoame

Următoarea proprietate caracterizează inelul de polinoame.

Teorema 2.1.3. *Fie A şi B inele cu unitate, unde A este comutativ, $\phi : A \to B$ morfism unital de inele, şi fie $x \in B$ astfel încât $x\phi(a) = \phi(a)x$ pentru orice $a \in A$.*

Atunci există un unic morfism unital $\bar{\Phi}_x : A[X] \to B$ astfel ca $\bar{\Phi}_x \circ \iota_A = \phi$ şi $\bar{\Phi}_x(X) = x$.

Demonstraţie. Presupunem că $\bar{\Phi}_x$ există, şi arătăm că este unic. Într-adevăr, dacă $f = \sum_{i=0}^{n} a_iX^i$, atunci

$$\bar{\Phi}_x(f) = \sum_{i=0}^{n} \bar{\Phi}_x(a_i)\bar{\Phi}_x(X)^i = \sum_{i=0}^{n} \phi(a_i)x^i.$$

Fie deci

$$\bar{\Phi}_x : A[X] \to B, \qquad \bar{\Phi}_x(f) = \sum_{i=0}^{n} \phi(a_i)x^i,$$

şi arătăm că $\bar{\Phi}_x$ satisface proprietăţile enunţate. Dacă $a \in A$, atunci

$$(\bar{\Phi}_x \circ \iota_A)(a) = \bar{\Phi}_x(\iota_A(a)) = \bar{\Phi}_x(a) = \phi(a).$$

Dacă $f = \sum_{i\geq 0} a_i X^i,\ g = \sum_{j\geq 0} b_j X^j \in A[X]$, atunci

$$\begin{aligned}\bar{\Phi}_x(f+g) &= \bar{\Phi}_x(\sum_{k\geq 0}(a_k+b_k)X^k) = \sum_{k\geq 0}(\phi(a_k)+\phi(b_k))x^k \\ &= \sum_{k\geq 0}\phi(a_k)x^k + \sum_{k\geq 0}\phi(b_k)x^k = \bar{\Phi}_x(f)+\bar{\Phi}_x(g). \\ \bar{\Phi}_x(fg) &= \bar{\Phi}_x(\sum_{k\geq 0}(\sum_{i+j=k} a_i b_j)X^k) = \sum_{k\geq 0}(\sum_{i+j=k}\phi(a_i)\phi(b_j))x^k \\ &= (\sum_{i\geq 0}\phi(a_i)x^i)(\sum_{k\geq 0}\phi(b_j)x^j) = \bar{\Phi}_x(f)\bar{\Phi}_x(g). \qquad \square\end{aligned}$$

Exerciţiul 2.4. Fie $\phi : A \to B$ şi $\psi : B \to C$ morfisme unitale de inele. Să se arate că:

a) Există un unic morfism $\phi[X] : A[X] \to B[X]$ astfel încât $i_B \circ \phi = \phi[X] \circ i_A$, unde $i_A : A \to A[X]$ este injecţia canonică.

b) $\mathbf{1}_A[X] = \mathbf{1}_{A[X]}$ şi $(\psi \circ \phi)[X] = \psi[X] \circ \phi[X]$.

Definiţia 2.1.4. În teoreme de mai sus fie $A = B$ şi $\phi = \mathbf{1}_A$. Atunci funcţia $\tilde{f} : A \to A,\ \ \tilde{f}(a) = \Phi_x(f)$ se numeşte *funcţia polinomială* asociată lui f, şi spunem că $f(x) = \tilde{f}(x) \in A$ este *valoarea* lui f în x .

2.1.3 Teorema împărţirii cu rest. Rădăcinile polinoamelor

Vom nota de obicei prin A un domeniu de integritate şi prin $K = \mathrm{frac}(A) = \{\frac{a}{b} \mid b \neq 0\}$ *corpul fracţiilor* lui A.

Teorema 2.1.5. *Fie A un domeniu de integritate, şi fie $f = a_0 + a_1 X + \cdots + a_m X^m$, $g = b_0 + b_1 X + \cdots + b_n X^n \in A[X]$, astfel încât b_n este inversabil în A. Atunci există polinoame $q, r \in A[X]$ unic determinate, astfel ca*

$$f = gq + r, \quad \deg(r) < \deg(g).$$

Demonstraţie. Folosim inducţie după m. Dacă $m < n$, atunci $q = 0$ şi $r = f$. Fie $m \geq n$ şi presupunem că afirmaţia este adevărată pentru polinoame de grad mai mic ca m. Fie

$$f' = f - g a_m b_n^{-1} X^{m-n}.$$

Deoarece $\deg(f') < m$, există $q', r \in A[X]$ astfel încât $f' = gq' + r',\ \deg(r) < \deg(g)$; rezultă că

$$f = f' + g a_m b_n^{-1} X^{m-n} = (a_m b_n^{-1} X^{m-n} + q')g + r.$$

Dacă $f = gq + r = gq_1 + r_1$, $\deg(r), \deg(r') < \deg(g)$, atunci $r - r_1 = (q_1 - q)g$, $\deg(r - r_1) < \deg(g)$, deci $q = q_1$, $r = r_1$. □

Definiţia 2.1.6. a) Dacă $f(a) = 0$, atunci spunem că $x \in A$ este *rădăcină* a lui f.

b) Spunem că a este *rădăcină de multiplicitate* k a lui f (unde $k \geq 0$), dacă există $q \in A[X]$ astfel încât

$$f = (X - a)^k q, \quad q(a) \neq 0.$$

Corolar 2.1.7. *Presupunem că A este domeniu de integritate.*

a) **(Teorema lui Bezout)** *$a \in A$ este rădăcină a polinomului f dacă şi numai dacă $f = (X - a)q$, unde $q \in A[X]$.*

b) *Dacă $\deg(f) = n$, atunci f are cel mult n rădăcini în corpul fracţiilor K al lui A.* (Numărăm şi multiplicităţile rădăcinilor.)

Demonstraţie. a) Observăm că pentru orice $a \in A$, $f = (X - a)q + f(a)$.

b) Inducţie după n. Dacă $n = 1$, $f = a_1 X + a_0 \in K[X]$, atunci $a = a_1^{-1} a_0 \in K$ este rădăcină a lui f.

Presupunem că $n > 1$ şi fie $a \in K$ o rădăcină a lui f; atunci $f = (X - a)g$ şi $\deg g = n - 1$. Din ipoteza inducţiei rezultă că g are cel mult $n - 1$ rădăcini în K, deci f are cel mult n rădăcini în K. □

Exerciţiul 2.5 (Formulele lui Viéte)**.** Dacă $x_1, \ldots, x_n$ sunt rădăcinile polinomului $f = a_n + a_{n-1}X + \cdots + a_1 X^{n-1} + a_0 X^n \in A[X]$, atunci

$$\begin{aligned}
-a_1 &= a_0(x_1 + x_2 + \cdots + x_n) \\
a_2 &= a_0(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n) \\
&\ldots \\
(-1)^k a_k &= a_0(x_1 \ldots x_k + \cdots + x_{n-k+1} \ldots x_n) \\
&\ldots \\
(-1)^n a_n &= a_0(x_1 \ldots x_n).
\end{aligned}$$

Exerciţiul 2.6. Să se determine restul împărţirii lui $f \in K[X]$ la g, dacă:

a) $g = (X - a)(X - b)$, $a \neq b$.

b) $g = (X - a)^2$.

Exerciţiul 2.7. Fie $\psi : A[X] \to A^A$, $\psi(f) = \tilde{f}$. Să se arate că:

a) ϕ este morfism unital de inele.

b) Dacă A este corp finit, atunci ψ este surjectiv şi nu este injectiv.

c) Dacă A este domeniu de integritate infinit, atunci ψ este injectiv şi nu este surjectiv.

Următoarea teoremă se mai numeşte **teorema fundamentală a algebrei clasice**. Demonstraţia o vom da mai târziu.

Teorema 2.1.8 (Gauss–d'Alembert)**.** *Orice polinom de grad ≥ 1 cu coeficienţi în corpul $\mathbb{C}$ al numerelor complexe are cel puţin o rădăcină în $\mathbb{C}$.*

Exerciţiul 2.8. Orice polinom de grad n cu coeficienţi în $\mathbb{C}$ are exact n rădăcini în $\mathbb{C}$.

Exerciţiul 2.9. Să se arate că $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ este rădăcină a polinomului $X^2 - \mathrm{Tr}(z)X + N(z)$, unde $\mathrm{Tr}(z) := z + \bar{z}$ este *urma* lui z şi $N(z) := z\bar{z}$ este *norma* lui z.

Exerciţiul 2.10. a) Fie $f \in \mathbb{R}[X]$ şi $k \in \mathbb{N}$. Dacă $z = a + bi \in \mathbb{C}$ este rădăcină de multiplicitate k a lui f, atunci şi $\bar{z} = a - bi$ este rădăcină de multiplicitate k a lui f.

b) Fie $f \in \mathbb{Q}[X]$ şi $k \in \mathbb{N}$. Dacă $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ este rădăcină de multiplicitate k a lui f, atunci şi $\bar{z} = a - b\sqrt{d}$ este rădăcină de multiplicitate k a lui f.

Exerciţiul 2.11. Fie $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ şi $a = \frac{r}{s}$ o fracţie ireductibilă. Dacă a este rădăcină a lui f, atunci $r|a_0$ şi $s|a_n$.

Exerciţiul 2.12. a) Polinomul $X^2 - \hat{1}$ are 4 rădăcini în $\mathbb{Z}_{15}$.

b) Polinomul $X^2 + 1$ are o infinitate de rădăcini în corpul $\mathbb{H}$ al cuaternionilor.

c) Mai general, dacă $q = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ este un cuaternion, fie $\bar{q} = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$ *conjugatul* lui x, $N(q) = q\bar{q}$ *norma* lui q, şi $\mathrm{Tr}(q) = q + \bar{q}$ *urma* lui q. Să se arate că q este rădăcină a polinomului $X^2 - \mathrm{Tr}(q)X + N(q)$; acest polinom are o infinitate de rădăcini în $\mathbb{H}$, dacă $\mathrm{Tr}(q)$, şi $N(x)$ sunt fixaţi şi $b^2 + c^2 + d^2 > 0$.

2.1.4 Derivata formală a unui polinom. Rădăcini multiple

Fie K un corp comutativ.

Familia de vectori $(1, X, X^2, \dots)$ formează o bază a K-spaţiului vectorial $K[X]$. Din proprietatea de universalitate a spaţiilor vectoriale rezultă că există o unică funcţie liniară $D : K[X] \to K[X]$ astfel ca $D(X^k) = kX^{k-1}$ pentru orice $k \in \mathbb{N}$. În general, dacă $f = \sum_{k=0}^{n} a_kX^k$, atunci

$$D(f) = f' = f^{(1)} = \sum_{k=1}^{n} ka_kX^{k-1}.$$

Polinomul $D(f) = f'$ se numeşte *derivata formală* a polinomului f.

Lema 2.1.9. 1) $D(f+g) = D(f) + D(g)$, $D(af) = aD(f)$;
2) $D(fg) = D(f)g + fD(g)$; $D(f_1 \dots f_n) = \sum_{i=1}^{n} f_1 \dots f_{i-1} D(f_i) f_{i+1} \dots f_n$;
3) $D(g \circ f) = (D(g) \circ f) D(f)$.

Demonstraţie. 1) Dacă $f = \sum_{k \geq 0} a_k X^k$, $g = \sum_{k \geq 0} b_k X^k$, atunci

$$D(f+g) = D(\sum_{k \geq 0} (a_k + b_k) X^k) = \sum_{k \geq 0} k(a_k + b_k) X^{k-1} =$$
$$= \sum_{k \geq 0} k a_k X^{k-1} + \sum_{k \geq 0} k b_k X^{k-1} = D(f) + D(g),$$

$$D(af) = D(a \sum_{k \geq 0} a_k X^k) = D(\sum_{k \geq 0} a a_k X^k) = \sum_{k \geq 0} k a a_k X^{k-1} = a \sum_{k \geq 0} k a_k X^{k-1} = aD(f).$$

2) Dacă $f = X^i$ şi $g = X^j$, atunci $fg = X^{i+j}$ şi

$$D(fg) = (i+j) X^{i+j-1} = X^i j X^{j-1} + i X^{i-1} X^j = (i+j) X^{i+j-1} = fD(g) + D(f)g.$$

Dacă $f = \sum_{i=0}^{n} a_i X^i$ şi $g = \sum_{j=0}^{m} b_j X^j$, atunci $fg = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^i X^j$.

$$D(fg) = \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j D(X^i X^j) = \sum_{k=1}^{n+m} \sum_{i+j=k} (a_i b_j X^i D(X^j) + a_i b_j D(X^i) X^j) =$$
$$= \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j X^i D(X^j) + \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j D(X^i) X^j = fD(g) + D(f)g.$$

Pentra a demonstra afirmaţia generală folosim inducţia după n. Dacă $n = 1$, atunci $D(f_1) = D(f_1)$. Presupunem că afirmaţia este adevărată pentru n, şi arătăm pentru $n+1$:

$$D(f_1 \dots f_n f_{n+1}) = D(f_1 \dots f_n) f_{n+1} + f_1 \dots f_n D(f_{n+1}) =$$
$$= (\sum_{i=1}^{n} f_1 \dots D(f_i) \dots f_n) f_{n+1} + f_1 \dots f_n D(f_{n+1}) =$$
$$= \sum_{i=1}^{n+1} f_1 \dots D(f_i) \dots f_n f_{n+1}.$$

3) Dacă $g = X^k$, atunci $g \circ f = f^k$ şi $D(g) = kX^{k-1}$, şi din b) rezultă că

$$D(g \circ f) = D(f^k) = kf^{k-1}D(f) = (D(g) \circ f)D(f).$$

În general, dacă $g = \sum_{k=0}^{n} b_k X^k$, atunci

$$D(g \circ f) = \sum_{k=1}^{n} b_k D(f^k) = \sum_{k=1}^{n} b_k k f^{k-1} D(f) = ((D(g)) \circ f)D(f). \qquad \square$$

Derivata de ordin superior se defineşte prin inducţie:

$$f^{(0)} = f, \;\; f^{(1)} = D(f), \quad f^{(k+1)} = D^{k+1}(f) = D(f^{(k)}).$$

Lema 2.1.10 (formula lui Taylor)**.** *Dacă $f \in K[X]$, $\deg(f) = n$ şi $a \in K$, atunci există elementele $b_0, \ldots, b_n \in K$ astfel încât*

$$f = \sum_{k=0}^{n} b_k (X-a)^k.$$

Dacă $\mathrm{char} K = 0$*, atunci coeficienţii b_k sunt unic determinaţi:*

$$b_k = \frac{f^{(k)}(a)}{k!}$$

pentru orice $k \in \mathbb{N}$.

Demonstraţie. Folosim inducţie după $\deg f$. Dacă $\deg f < 1$, atunci $f = a_0 \in K$. Dacă $\deg f = 1$, atunci $f = a_0 + a_1 X = a_1(X-a) + a_1 a + a_0$. Presupunem că $n > 1$, şi afirmaţia este adevărată pentru polinoame de grad mai mic ca n. Fie $f = (X-a)f_1 + f(a)$, unde $\deg f_1 = n-1$. Din ipoteza inducţiei rezultă că

$$f_1 = \sum_{k=0}^{n-1} b_k (X-a)^k,$$

deci

$$f = f(a) + \sum_{k=0}^{n-1} b_k (X-a)^{k+1}.$$

Dacă $\mathrm{char}\, K = 0$ şi $f = \sum_{k=0}^{n} b_k (X-a)^k$, atunci $f(a) = b_0 = (f^{(0)}(a))/(0!)$, şi prin derivare obţinem $f^{(k)}(a) = k! b_k, \quad k = 0, \ldots, n.$ $\square$

Observaţii 2.1.11. 1) Dacă $K = \mathbb{Z}_p$, unde p este un număr prim, atunci char $= p$. De aceea, pentru orice $k \geq p$ avem $k!b_k = 0$.

2) Dacă caracteristica corpului K este 0 şi $f \in K[X]$, atunci $f' = 0$ dacă şi numai dacă $f \in K$.

3) Fie $p \neq 0$ caracteristica corpului K şi fie $f \in K[X]$; $f' = 0$ dacă şi numai dacă f are forma:

$$f = a_0 + a_1X^p + a_2X^{2p} + \cdots + a_nX^{np}$$

adică $f \in K[X^p]$.

Teorema 2.1.12. *Fie* $f \in K[X], a \in K, k \in \mathbb{N}^*$ *şi* char $K = 0$.

1) *Dacă a este rădăcină de multiplicitate k a lui f, atunci a este rădăcină de multiplicitate $(k-1)$ a derivatei $D(f)$ şi avem că $f^{(0)}(a) = f^{(1)}(a) = \cdots = f^{(k-1)}(a) = 0$ şi $f^{(k)}(a) \neq 0$.*

2) *Reciproc, dacă $f^{(0)}(a) = f^{(1)}(a) = \cdots = f^{(k-1)}(a) = 0$ şi $f^{(k)}(a) \neq 0$, atunci a este rădăcină de multiplicitate k a lui f.*

Demonstraţie. 1) Presupunem că $f = (X-a)^k g$ şi $g(a) \neq 0$. Derivăm pe f:

$$D(f) = k(X-a)^{k-1}g + (X-a)^k D(g) = (X-a)^{k-1}[kg + (X-a)D(g)].$$

Rezultă că $(X-a)^{k-1}|D(f)$ şi $g_1(a) = kg(a) \neq 0$, unde $g_1 = kg + (X-a)D(g)$. Astfel am arătat că dacă a este rădăcină de multiplicitate k a lui f, atunci a este rădăcină de multiplicitate $(k-1)$ a derivatei $D(f)$. Prin inducţie se arată că a este rădăcină de multiplicitate $(k-i)$ a lui $f^{(i)}$, $i = 1, \ldots, k$, deci a este rădăcină de multiplicitate 1 a lui $f^{(k-1)}$, şi este rădăcină de multiplicitate (0) a lui $f^{(k)}$, adică $f^{(k)}(a) \neq 0$.

2) Aplicând formula lui Taylor rezultă că

$$\begin{aligned} f &= \sum_{j=0}^{n} (f^{(j)}(a))/(j!)(X-a)^j = \sum_{i=k}^{n} (f^{(i)}(a))/(i!)(X-a)^i = \\ &= (X-a)^k((f^{(k)}(a))/(k!) + (X-a)f^{(k+1)}(a))/((k+1)!) + \ldots). \end{aligned}$$

Notăm

$$g := (f^{(k)}(a))/(k!) + (X-a)f^{(k+1)}(a))/((k+1)!) + \ldots;$$

rezultă că $(X-a)^k|f$ şi $g(a) \neq 0$, deoarece $f^{(k)} \neq 0$. □

2.2 Polinoame în mai multe nedeterminate

2.2.1 Construcţia inelului de polinoame

Definiţia 2.2.1. 1) Fie A un inel comutativ netrivial ($1 \neq 0$) şi considerăm algebra de polinoame $A[X_1]$ de o nedeterminată. Algebra $A[X_1, X_2] = (A[X_1])[X_2]$ se numeşte *algebra de polinoame de două nedeterminate*.

2) În general, definim prin recurenţă *algebra de polinoame de n nedeterminate* $A[X_1, \ldots, X_n]$ astfel:

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n].$$

Dacă $f \in A[X_1, \ldots, X_n]$, atunci f se scrie unic sub forma

$$f = \sum_{k=0}^{n} f_k X_n^k = \sum_{(k_1,\ldots,k_n), k_i \geq 0} a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n},$$

unde numărul elementelor nenule $f_k \in A[X_1, \ldots, X_{n-1}]$ şi $a_{k_1,\ldots,k_n} \in A$ este finit.

3) Termenul $a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n}$ se numeşte *monom*. Acest monom are *gradul* $k_1 + \cdots + k_n$.

4) *Gradul polinomului* f este $\deg f = \max\{k_1 + \cdots + k_n \mid a_{k_1,\ldots,k_n} \neq 0\}$.

5) Dacă $k_1 + \cdots + k_n$ este constant pentru orice $a_{k_1,\ldots,k_n}$, atunci spunem că f este *polinom omogen*.

6) Polinomul f se scrie unic sub forma

$$f = h_0 + h_1 + \cdots + h_m,$$

unde $h_i \in A[X_1, \ldots, X_n]$ sunt polinoame omogene şi $\deg(h_i) = i$. Atunci spunem că $h_0, h_1, \ldots, h_m$ sunt *componentele omogene ale lui* f.

Afirmaţiile de mai jos generalizează teoremele cunoscute în cazul algebrei $A[X]$ a polinoamelor într-o nedeterminată.

Observaţii 2.2.2. 1) Dacă $f, g \in A[X_1, \ldots, X_n]$, atunci

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\};$$

$$\deg(fg) \leq \deg(f) + \deg(g).$$

2) Dacă A este domeniu de integritate, atunci $\deg(fg) = \deg(f) + \deg(g)$ şi $A[X_1, \ldots, X_n]$ este de asemenea domeniu de integritate.

Teorema 2.2.3 (proprietatea de universalitate a algebrei de polinoame)**.** *Fie B un inel comutativ cu unitate, $\varphi : A \to B$ un morfism unital de inele şi $b_1, \dots, b_n \in B$. Atunci există un unic morfism de A-algebre $\bar{\varphi}_{b_1 \dots b_n} : A[X_1, \dots, X_n] \to B$ astfel încât $\bar{\varphi}_{b_1 \dots b_n} \circ i = \varphi$ şi $\bar{\varphi}_{b_1 \dots b_n}(X_i) = b_i$, deci diagrama*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\iota_A"'] & B \\ A[X_1, \dots, X_n] \arrow[ur, dotted, "\bar{\varphi}_{b_1,\dots,b_n}"'] & \end{tikzcd}$$

este comutativă, şi în general avem

$$\bar{\varphi}_{k_1 \dots k_n}(f) = \sum_{(b_1,\dots,b_n)} \varphi(a_{k_1,\dots,k_n}) b_1^{k_1} \dots b_n^{k_n}.$$

Demonstraţie. Folosim inducţie după n. Dacă $n = 1$, atunci afirmaţia este adevărată pe baza Teoremei 2.1.3. Presupunem că este adevărată pentru $n-1$ şi aplicând ipoteza inducţiei, rezultă că este adevărată şi pentru n. Detaliile demonstraţiei sunt lăsate pe seama cititorului. □

Definiţia 2.2.4. În teorema de mai sus fie $A = B$ şi $\phi = \mathbf{1}_A$. Atunci funcţia

$$\tilde{f} : A^n \to A, \quad \tilde{f}(a_1, \dots, a_n) = \Phi_{a_1,\dots,a_n}(f)$$

se numeşte *funcţie polinomială* de n variabile.

Exerciţiul 2.13. a) Dacă A este domeniu de integritate şi $f, g \in A[X_1, \dots, X_n]$, atunci $\deg(fg) = \deg(f) + \deg(g)$.

b) numărul monoamelor de grad k în n-variabile este C_{n+k-1}^k.

Exerciţiul 2.14 (Formula polinomului)**.** Să se arate că

$$(X_1 + \dots + X_n)^k = \sum_{k_1 + \dots + k_n = k} \frac{k!}{k_1! \dots k_n!} X_1^{k_1} \dots X_n^{k_n}.$$

Exerciţiul 2.15. a) Dacă $a_1, \dots, a_n \in A$, atunci $A[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) \simeq A$.

b) Dacă $I \trianglelefteq A$ este un ideal, atunci $A[X_1, \dots, X_n]/I[X_1, \dots, X_n] \simeq (A/I)[X_1, \dots, X_n]$.

Exerciţiul 2.16. Fie $\phi : A \to B$ şi $\psi : B \to C$ morfisme unitale de inele. Să se arate că:

a) Există unic morfism $\phi[X_1, \dots, X_n] : A[X_1, \dots, X_n] \to B[X_1, \dots, X_n]$ astfel încât $i_B \circ \phi = \phi[X_1, \dots, X_n] \circ i_A$, unde $i_A : A \to A[X_1, \dots, X_n]$ este injecţia canonică.

b) $\mathbf{1}_A[X_1, \dots, X_n] = \mathbf{1}_{A[X_1,\dots,X_n]}$ şi $(\psi \circ \phi)[X_1, \dots, X_n] = \psi[X_1, \dots, X_n] \circ \phi[X_1, \dots, X_n]$.

2.2.2 Polinoame simetrice

Dacă $\sigma \in S_n$ este o permutare de grad n, atunci din proprietatea de universalitate a algebrei de polinoame rezultă că asocierea $X_i \mapsto X_{\sigma(i)}$, $1 = 1, \dots, n$ determină morfismul de A-algebre

$$\sigma^* : A[X_1, \dots, X_n] \to A[X_1, \dots, X_n].$$

Exemplul 2.2.5. a) Dacă $f = aX_1X_2X_3 + X^2X_3 + X_1X_2X_3^2 \in A[X_1, X_2, X_3]$, $a \neq 0$ şi $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, atunci $\sigma^*(f) = aX_3X_1X_2 + X_3^2X_2 + X_3X_1X_2^2$.

b) În general, dacă $f = \sum a_{i_1 \cdots_n} X_1^{i_1} \cdots X_n^{i_n} \in A[X_1, \dots, X_n]$, atunci

$$\sigma^*(f) = \sum a_{i_1 \dots i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n}.$$

Definiţia 2.2.6. Spunem că $f \in A[X_1, \dots, X_n]$ este *polinom simetric*, dacă $\sigma^*(f) = f$ pentru orice $\sigma \in S_n$.

Exemplul 2.2.7. 1) Dacă $n = 2$ şi $f = X_1^2 + X_2^2 + X_1X_2$, atunci f este polinom simetric, deoarece $\sigma^*(f) = f$ pentru orice $\sigma \in S_2$.

2) Fie $g = X_1^2X_2$, $\sigma = (12)$. Deoarece $\sigma^*(g) = X_1X_2^2 \neq g$, rezultă că g nu este polinom simetric.

3) Dacă $P_n = X_1^n + X_2^n + \cdots + X_n^n \in A[X_1, \dots, X_n]$, atunci P_n este polinom simetric.

4) Fie

$$\begin{aligned}
s_1 &= X_1 + X_2 + \cdots + X_n = \sum_{i=1}^{n} X_i \\
s_2 &= X_1X_2 + X_1X_3 + \cdots + X_1X_n + \cdots + X_{n-1}X_n = \sum_{1 \le i < j \le n} X_iX_j \\
s_3 &= X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n = \sum_{1 \le i_1 < i_2 < i_3 \le n} X_{i_1}X_{i_2}X_{i_3} \\
&\dots \\
s_k &= X_1X_2 \dots X_k + \cdots + X_{n-k+1} \dots X_n = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \dots X_{i_k} \\
&\dots \\
s_n &= X_1X_2 \dots X_n.
\end{aligned}$$

Polinoame $s_1, s_2, \dots, s_n$ se numeşte *polinoame simetrice elementare*.

Fie $M = aX_1^{k_1} \dots X_n^{k_n}$, $M' = a'X_1^{k'_1} \dots X_n^{k'_n} \in A[X_1, \dots, X_n]$ două monoame.

Prin definiţie, $M > M'$, dacă există $j \in \{1, \dots, n\}$ pentru care $k_1 = k'_1$, $k_2 = k'_2, \dots, k_{j-1} = k'_{j-1}$ şi $k_j > k'_j$. Relaţia „$<$" este tranzitivă si se numeşte *ordonarea lexicografică* a monoamelor.

Se observă uşor că *în mulţimea monoamelor orice şir strict descrescător este finit.*

Spunem că monomul M este *termenul principal* al polinomului $f \in A[X_1, \dots, X_n]$, dacă M este cel mai mare termen al lui f în ordonarea lexicografică.

Exemplul 2.2.8. 1) $X_1^2X_2^5 > X_1^2X_2^4X_3^7$.

2) Termenul principal al polinomului $f = X_1^2X_2 + X_1X_2^2 + X_3^2 + X_2^4 + X_1^2X_2^2$ este $X_1^2X_2^2$.

3) Termenul principal al polinomului simetric s_k este $X_1 \dots X_k$.

Lema 2.2.9. *Dacă $M_1, M_2, N_1, N_2 \in A[X_1, \dots, X_n]$ sunt monoame astfel încât $M_1 > M_2$, atunci:*

1) $M_1N_1 > M_2N_1$.

2) *Dacă $N_1 > N_2$, atunci $M_1N_1 > M_2N_2$.*

3) *Dacă $f, g \in A[X_1, \dots, X_n]$, M este termenul principal al lui f şi N este termenul principal al lui g, atunci fg este termenul principal al lui MN.*

Demonstraţie. Fie $M_1 = aX_1^{k_1} \dots X_n^{k_n}$, $M_2 = bX_1^{l_1} \dots X_n^{l_n}$, $N_1 = cX_1^{m_1} \dots X_n^{m_n}$. Deoarece $M_1 > M_2$, rezultă că $k_1 = l_1, \dots, k_{s-1} = l_{s-1}, k_s > l_s$, deci $k_1 + m_1 = l_1 + m_1, \dots, k_{s-1} + m_{s-1} = l_{s-1} = m_{s-1}, k_s + m_s > l_s + m_s$, adică $M_1N_1 > M_2N_1$.

2) aplicând de două ori punctul 1), rezultă că $M_1N_1 > M_2N_1 > M_2N_2$.

3) rezultă din 2). □

Lema 2.2.10. *Dacă $f \in A[X_1, \dots, X_n]$ este un polinom simetric, iar $M_1 = aX_1^{k_1} \dots X_n^{k_n}$ este termenul principal al lui f, atunci $k_1 \geq k_2 \geq \dots \geq k_n$.*

Demonstraţie. Presupunem că există un indice i pentru care $k_i < k_{i+1}$, şi fie

$$M' = aX_1^{k_1} \dots X_{i-1}^{k_{i-1}} X_i^{k_{i+1}} X_{i+1}^{k_i} X_{i+2}^{k_{i+2}} \dots X_n^{k_n};$$

rezultă că $M' = \sigma^*(M)$, unde $\sigma^* = (i, i+1) \in S_n$. Deoarece f este polinom simetric, rezultă că M' este termen al lui f şi $M' > M$, contradicţie. □

Teorema 2.2.11 (Teorema fundamentală a polinoamelor simetrice)**.** *Dacă f este un polinom simetric din $A[X_1, \dots, X_n]$, atunci există un unic polinom $g \in A[Y_1, \dots, Y_n]$ astfel încât $f = g(s_1, \dots, s_n)$, unde s_i, $i = 1, \dots, n$ sunt polinoamele simetrice elementare.*

Demonstraţie. Existenţa: presupunem că $f \neq 0$, şi fie $aX_1^{k_1} \dots X_n^{k_n}$ termenul principal al lui f; am văzut că $k_1 \geq \dots \geq k_n \geq 0$. Observăm că termenul principal al polinomului $s_1^{l_1} \dots s_n^{l_n}$ este

$$X_1^{l_1+l_2+\dots+l_n} X_2^{l_2+\dots+l_n} \dots X_i^{l_i+\dots+l_n} \dots X_n^{l_n},$$

adică $X_1^{k_1} \dots X_n^{k_n}$, unde $k_i = i_i + \dots + l_n$. Rezultă că termenul principal al polinomului $as_1^{k_1-k_2} s_2^{k_2-k_3} \dots s_n^{k_n}$ este $aX_1^{k_1} \dots X_n^{k_n}$.

Fie $f_1 = f - as_1^{k_1-k_2} s_2^{k_2-k_3} \dots s_n^{k_n}$ şi $g_1 = aY_1^{k_1-k_2} \dots Y_n^{k_n} \in A[Y_1, \dots, Y_n]$; rezultă că f_1 este polinom simetric, al cărui termen principal este mai mic ca termenul principal al lui f.

Continuând procedeul cu f_1, există $g_2 \in A[Y_1, \dots, Y_n]$ astfel încât polinomul $f_2 = f_1 - g_2(s_1, \dots, s_n)$ este simetric, şi termenul principal al lui f_2 este mai mic ca termenul principal al lui f_1.

După $n-1$ paşi obţinem $f_{n-1} = f_{n-2} - g_{n-1}(s_1, \dots, s_n)$, unde termenul principal al lui f_{n-1} este mai mic ca termenul principal al lui f, şi există $n \in \mathbb{N}$ pentru care $f_n = f_{n-1} - g_n(s_1, \dots, s_n) = 0$; rezultă că $f = g_1(s_1, \dots, s_n) + \dots + g_n(s_1, \dots, s_n)$.

Fie $g = g_1 + \dots + g_n \in A[Y_1, \dots, Y_n]$; atunci $f = g(s_1, \dots, s_n)$.

Unicitatea: fie $f = g_1(s_1, \dots, s_n) = g_2(s_1, \dots, s_n)$, adică $(g_1 - g_2)(s_1, \dots, s_n) = 0$, şi arătăm că $g_1 = g_2$. Este suficient de arătat că dacă $h \in A[Y_1, \dots, Y_n]$ şi $h(s_1, \dots, s_n) = 0$, atunci $h = 0$.

Presupunem că $h \neq 0$, $h = \sum a_{l_1 \dots l_n} Y_1^{l_1} \dots Y_n^{l_n}$, unde $a_{l_1 \dots l_n} \neq 0$; termenul principal al polinomului $a_{l_1 \dots l_n} s_1^{l_1} \dots s_n^{l_n}$ este $a_{l_1 \dots l_n} X_1^{k_1} \dots X_n^{k_n}$, unde $k_i = l_i + \dots + l_n$, iar termenul principal al lui $a_{l'_1 \dots l'_n} s_1^{k'_1} \dots s_n^{k'_n}$ este $a_{l'_1 \dots l'_n} X_1^{k'_1} \dots X_n^{k'_n}$, unde $k'_i = l'_i + \dots + l'_n, i \in \{1, \dots, n\}$.

Observăm că dacă $(l_1, \dots, l_n) \neq (l'_1, \dots, l'_n)$, atunci $(k_1, \dots, k_n) \neq (k'_1, \dots, k'_n)$; rezultă că dacă $M = aX_1^{k_1} \dots X_n^{k_n}$ este termen principal al lui h, atunci termenul M nu se reduce, adică $h(s_1, \dots, s_n) \neq 0$, ceea ce este o contradicţie. $\square$

Exerciţiul 2.17. Să se arate că:

a) $(\tau \circ \sigma)^* = \sigma^* \circ \tau^*$ şi $e^*(f) = f$ $(\forall) f \in A[X_1, \dots, X_n]$.

b) Mulţimea polinoamelor simetrice formează un subinel al lui $A[X_1, \dots, X_n]$.

c) $f \in A[X_1, \dots, X_n]$ este simetric dacă şi numai dacă componentele omogene ale lui f sunt simetrice.

Exerciţiul 2.18. Să se aplice teorema fundamentală a polinoamelor simetrice în următoarele cazuri:

a) $f = (X_1 - X_2)^2 (X_2 - X_3)^2 (X_3 - X_1)^2$.

b) $f = \sum_{i \neq j} X_i^3 X_j = S(X_1^3 X_2)$.
c) $f = \sum_{i,j,k} X_i^5 X_j^2 X_k = S(X_1^5 X_2^2 X_3)$.
d) $f = (-X_1 + X_2 + \cdots + X_n)(X_1 - X_2 + \cdots + X_n) \ldots (X_1 + X_2 + \cdots - X_n)$.

2.2.3 Formulele lui Newton–Waring

Considerăm polinomul simetric

$$P_k = X_1^k + \cdots + X_n^k.$$

Din teorema fundamentală a polinoamelor simetrice rezultăcă există un polinom $g_k \in \mathbb{Z}[Y_1, \ldots, Y_n]$ pentru care $P_k = g_k(s_1, \ldots, s_n)$. Ar fi dificil de calculat polinoamele g_k, de aceea căutăm o relaţie între polinoamele simetrice P_k şi $s_1, \ldots, s_n$.

Dacă $k_1 \geq \cdots \geq k_n$, fie $\mathrm{Orb}(X_1^{k_1} \ldots X_n^{k_n}) = \{X_{\sigma(1)}^{k_1} \ldots X_{\sigma(n)}^{k_n} \mid \sigma \in S_n\}$ şi fie

$$S(X_1^{k_1} \ldots X_n^{k_n}) = \sum_{M \in \mathrm{Orb}(X_1^{k_1} \ldots X_n^{k_n})} M$$

„cel mai mic” polinom simetric, al cărui termen principal este $X_1^{k_1} \ldots X_n^{k_n}$.

Cazul 1. Presupunem că $k \leq n$.

$$\begin{aligned}
P_1 &= s_1 \\
P_{k-1} s_1 &= (X_1^{k-1} + \cdots + X_n^{k-1})(X_1 + \cdots + X_n) = \\
&= P_k + S(X_1^{k-1} X_2) \\
P_{k-2} s_2 &= (X_1^{k-2} + \cdots + X_n^{k-2})(X_1 X_2 + \cdots + X_{n-1} X_n) = \\
&= S(X_1^{k-1} X_2) + S(X_1^{k-2} X_2 X_3) \\
P_{k-3} s_3 &= (X_1^{k-3} + \cdots + X_n^{k-3})(X_1 X_2 X_3 + \cdots + X_{n-2} X_{n-1} X_n) = \\
&= S(X_1^{k-2} X_2 X_3) + S(X_1^{k-3} X_2 X_3 X_4) \\
&\ldots \\
P_{k-i} s_i &= (X_1^{k-i} + \cdots + X_n^{k-i})(X_1 X_2 \ldots X_i + \cdots + X_{n-i+1} \ldots X_n) = \\
&= S(X_1^{k-i+1} X_2 \ldots X_i) + S(X_1^{k-i} X_2 \ldots X_{i+1}) \\
&\ldots \\
P_1 s_{k-1} &= (X_1 + \cdots + X_n)(X_1 \ldots X_{k-1} + \cdots + X_{n-k} \ldots X_n) = \\
&= S(X_1^2 X_2 \ldots X_{k-1}) + kS(X_1 \ldots X_k).
\end{aligned}$$

Înmulţim egalitatea I cu (-1) , egalitatea II cu $(-1)^2$,..., în general, egalitatea i cu $(-1)^i$ şi egalitatea $(n-1)$ cu $(-1)^{k-1}$. Adunând, obţinem:

$$P_k - P_{k-1}s_1 + P_{k-2}s_2 - \cdots + (-1)^i P_{k-i}s_i + \cdots + (-1)^{k-1}P_1 s_{k-1} + (-1)^k k s_k = 0.$$

Cazul 2. Presupunem că $k > n$.

$$\begin{aligned}
P_{k-1}s_1 &= (X_1^{k-1} + \cdots + X_n^{k-1})(X_1 + \cdots + X_n) = \\
&= P_k + S(X_1^{k-1}X_2) \\
P_{k-2}s_2 &= (X_1^{k-2} + \cdots + X_n^{k-2})(X_1X_2 + \cdots + X_{n-1}X_n) = \\
&= S(X_1^{k-1}X_2) + S(X_1^{k-2}X_2X_3) \\
P_{k-3}s_3 &= (X_1^{k-3} + \cdots + X_n^{k-3})(X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n) = \\
&= S(X_1^{k-2}X_2X_3) + S(X_1^{k-3}X_2X_3X_4) \\
&\ldots \\
P_{k-i}s_i &= (X_1^{k-i} + \cdots + X_n^{k-i})(X_1X_2\ldots X_i + \cdots + X_{n-i+1}\ldots X_n) = \\
&= S(X_1^{k-i+1}X_2\ldots X_i) + S(X_1^{k-i}X_2\ldots X_{i+1}) \\
&\ldots \\
P_{k-n}s_n &= S(X_1^{k-n+1}X_2\ldots X_n).
\end{aligned}$$

Analog obţinem

$$P_k - P_{k-1}s_1 + P_{k-2}s_2 - \cdots + (-1)^i P_{k-i}s_i + \cdots + (-1)^n P_{k-n}s_n = 0.$$

Exerciţiul 2.19. Fie $P_k = X_1^k + \cdots + X_n^k$.

a) Să se exprime P_2, P_3 şi P_4 în funcţie de s_1, s_2, s_3 şi s_4, dacă $n = 2, 3$ şi dacă $n \geq 4$.

b) Dacă $n = 4$, să se exprime s_1, s_2, s_3 şi s_4 în funcţie de P_1, P_2, P_3 şi P_4.

2.2.4 Discriminantul unui polinom

Considerăm următorul polinom în n nedeterminate:

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (X_j - X_i) \in \mathbb{Z}[X_1, \ldots, X_n].$$

Dacă $\sigma \in S_n$, atunci $\sigma^*(\Delta_n) = \operatorname{sgn}(\sigma)\Delta_n$, adică Δ_n nu este polinom simetric, dar Δ_n^2 este polinom simetric.

Definiţia 2.2.12. Δ_n^2 se numeşte *discriminant*ul familiei de nedeterminate $(X_1, \dots, X_n)$.

$$\Delta_n^2 = \begin{vmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \dots & X_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & X_1 & \dots & X_1^{n-1} \\ 1 & X_2 & \dots & X_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \dots & X_n^{n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} n & P_1 & P_2 & \dots & P_{n-1} \\ P_1 & P_2 & P_3 & \dots & P_n \\ P_2 & P_3 & P_4 & \dots & P_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{n-1} & P_n & P_{n+1} & \dots & P_{2n-2} \end{vmatrix}$$

Fie $f = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbb{C}[X]$, $a_0 \neq 0$. Presupunem că $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ sunt rădăcinile lui f.

Definiţia 2.2.13. Elementul

$$\Delta(f) = a_0^{2n-2}\Delta_n^2(\alpha_1, \dots, \alpha_n) \in \mathbb{C}$$

se numeşte *discriminant*ul polinomului f.

Observaţii 2.2.14. a) $\Delta(f) = 0 \Longleftrightarrow f$ are rădăcini multiple.

b) Din teorema fundamentală a polinoamelor simetrice şi din formulele lui Viete rezultă că discriminantul $\Delta(f)$ se exprimă în funcţie de coeficienţii $a_1, \dots, a_n$.

Exemplul 2.2.15. Fie $n = 2$, $f = X^2 + aX + b$ şi α_1, α_2 rădăcinile lui f. Determinăm $\Delta(f)$ în funcţie de coeficienţii polinomului f. Avem

$$P_1(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2 = -a, \quad P_2(\alpha_1, \alpha_2) = \alpha_1^2 + \alpha_2^2 = s_1^2 - 2s_2 = a^2 - 2b,$$

deci în acest caz

$$\Delta(f) = \begin{vmatrix} 2 & -a \\ -a & a^2 - 2b \end{vmatrix} = 2a^2 - 4b - a^2 = a^2 - 4b$$

coincide cu discriminantul cunoscut.

Exerciţiul 2.20. Să se calculeze discriminanţii următoarelor polinoame cu coeficienţi complecşi:

a) $f = aX^2 + bX + c$.
b) $f = X^3 + aX + b$.
c) $f = X^3 + aX^2 + bX + c$.
d) $f = X^n + a$.
e) $f = X^n + X^{n-1} + \cdots + X + 1$.

2.2.5 Rezultanta a două polinoame. Radăcini comune

Fie

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n,$$
$$g = b_0X^m + b_1X^{m-1} + \cdots + a_{m-1}X + b_m,$$

polinoame cu coeficienţi complecşi, unde $n, m > 0$, dar nu excludem cazul $a_0 = 0$ sau $b_0 = 0$.

Definiţia 2.2.16. *Rezultanta* polinoamelor f şi g este următorul determinant de ordin $n+m$:

$$\mathrm{Res}(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & . & & . & . & a_n & 0 & . & \dots & . \\ 0 & a_0 & a_1 & a_2 & & . & . & . & a_n & 0 & \dots & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & 0 \\ . & . & . & 0 & a_0 & a_1 & a_2 & . & . & . & \dots & a_n \\ b_0 & b_1 & b_2 & . & . & b_m & 0 & . & . & . & \dots & . \\ 0 & b_0 & b_1 & b_2 & . & . & b_m & 0 & . & . & \dots & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & 0 \\ . & . & . & 0 & b_0 & b_1 & b_2 & . & . & . & \dots & b_m \end{vmatrix}$$

unde primele m linii conţin coeficienţii lui f, iar ultimele n linii conţin coeficienţii lui g.

Teorema 2.2.17. *Fie $f, g \in \mathbb{C}[X]$. Următoarele afirmaţii sunt echivalente:*

(i) $\mathrm{Res}(f,g) = 0$.
(ii) *Există $f_1, g_1 \in \mathbb{C}[X]$ pentru care $fg_1 + f_1g = 0$, $\deg f_1 < n$, $\deg g_1 < m$.*
(iii) *$a_0 = b_0 = 0$ sau există $h \in \mathbb{C}[X]$ pentru care $h \mid f$, $h \mid g$ şi $\deg h \geq 1$.*

Demonstraţie. (iii)$\Longleftrightarrow$(ii). Presupunem că $h \in \mathbb{C}[X]$, $h \mid f,\ h \mid g$ şi $\deg h \geq 1$. Atunci există polinoamele $f_1, g_1 \in \mathbb{C}[X]$ astfel încât $f = hf_1$ şi $g = -hg_1$; rezultă că $fg_1 + f_1g = 0$, $\deg f_1 < n$, $\deg g_1 < m$. Dacă $a_0 = b_0 = 0$, atunci fie $f_1 = f$ şi $g_1 = -g$.

Invers, dacă f şi g nu au factor comun propriu, atunci din egalitatea $fg_1 = -f_1g$ rezultă că $f \mid f_1$ şi $g \mid g_1$, deci $\deg f < n$, $\deg g < m$ şi $a_0 = b_0 = 0$.

(ii)$\Longleftrightarrow$(i). există polinoamele

$$f_1 = c_0X^{n-1} + c_1X^{n-2} + \cdots + c_{n-1},$$
$$g_1 = d_0X^{m-1} + d_1X^{m-2} + \cdots + d_{m-1}$$

pentru care $fg_1 + f_1g = 0$ dacă şi numai dacă sistemul de ecuaţii omogene

$$\begin{array}{lll}
a_0d_0 + & b_0c_0 & = 0 \\
a_1d_0 + a_0d_1 + & b_1c_0 + b_0c_1 & = 0 \\
a_2d_0 + a_1d_1 + a_0d_2 + & b_2c_0 + b_1c_1 + b_0c_2 & = 0 \\
\ldots\ldots\ldots\ldots & & \\
\end{array}$$

are o soluţie netrivială $(d_0, \ldots, d_{m-1}, c_0, \ldots, c_{n-1})$. O astfel de soluţie există dacă şi numai dacă $\mathrm{Res}(f,g)^t = 0$, adică dacă $\mathrm{Res}(f,g) = 0$. □

Teorema 2.2.18. *Presupunem că*

$$f = a_0(X - \alpha_1)\ldots(X - \alpha_n),$$
$$g = b_0(X - \beta_1)\ldots(X - \beta_m).$$

Atunci

$$\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^m \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Demonstraţie. Deoarece $\mathrm{Res}(f,g) = (-1)^{mn}\mathrm{Res}(g,f)$, este suficient de demonstrat prima egalitate. Mai departe, este suficient de studiat „cazul general”: putem presupune că $g(\alpha_1), \ldots, g(\alpha_n)$ sunt numere distincte două câte două.

Considerăm polinoamele $f,\ g - Y \in \mathbb{C}[Y][X]$; atunci

$$\mathrm{Res}(f, g - Y) = (-1)^m a_0 Y^n + \cdots + \mathrm{Res}(f,g).$$

Observăm că α_i este rădăcină comună a polinoamelor f şi $g - g(\alpha_i)$, deci ambele se divid prin $(X - \alpha_i)$. Din teorema anterioară rezultă că $\mathrm{Res}(f, g - g(\alpha_i) = 0$, deci conform teoremei lui Bézout, polinomul $\mathrm{Res}(f, g - Y) \in \mathbb{C}[Y]$ este divizibil cu $(g(\alpha_i) - Y)$, $i = 1, \ldots, n$. Deoarece $g(\alpha_1), \ldots, g(\alpha_n)$ sunt numere distincte două câte două, rezultă că $\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n}(g(\alpha_i) - Y)$, şi în fine, înlocuim pe Y cu 0. □

Teorema 2.2.19. $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a_0} \operatorname{Res}(f, f')$.

Demonstraţie. Conform Teoremei 2.2.18. $\operatorname{Res}(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$. Deoarece

$$f' = a_0 \sum_{i=1}^{n} \prod_{j \neq i} (X - \alpha_i),$$

rezultă că $f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j)$, deci

$$\begin{aligned} \operatorname{Res}(f, f') &= a_0^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= a_0 (-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{j<i} (\alpha_i - \alpha_j)^2 \\ &= a_0 (-1)^{\frac{n(n-1)}{2}} \Delta(f). \qquad \square \end{aligned}$$

Exerciţiul 2.21. Să se calculeze rezultanta $\operatorname{Res}(f, g)$, unde
a) $f = a_0 X^2 + a_1 X + a_2$ şi $g = b_0 X^2 + b_1 X + b_2$.
b) $f \in \mathbb{C}[X]$ şi $g = X - a$.

Exerciţiul 2.22. Fie $f, g, h \in \mathbb{C}[X]$. Să se arate că:
a) $\operatorname{Res}(fg, h) = \operatorname{Res}(f, h) \operatorname{Res}(g, h)$.
b) $\Delta(fg) = \Delta(f)\Delta(g) \operatorname{Res}(f, g)$.

2.3 Aritmetica în inele de polinoame

2.3.1 Inele euclidiene, principale, factoriale

În acest paragraf examinăm în detaliu proprietăţile aritmetice ale inelului de polinoame. Deoarece în $K[X]$ are loc teorema împărţirii cu rest, primul rezultat este următorul:

Teorema 2.3.1. $(K[X], \deg)$ *este inel euclidian.*

Exemplul 2.3.2. 1) Dacă $f \in K[X]$ şi $\deg f = 1$, atunci f este polinom ireductibil.

2) Dacă $\deg f = 2$ sau $\deg f = 3$, atunci f este ireductibil dacă şi numai dacă f nu are rădăcini în K.

Într-adevăr, dacă $f(a) = 0$, atunci conform teoremei lui Bezout, $f = (X - a)g$, adică f nu este ireductibil. Invers, presupunem că f nu are rădăcini în K şi fie $f = gh$,

unde $\deg g,\ \deg h \geq 1$. Dacă $\deg g = 1$, atunci $g = aX + b$ şi $-b/a$ este rădăcină a lui g; rezultă că $f(-b/a) = 0$, adică f are rădăcină în K, contradicţie.

3) Polinomul $f = X^4 + 1 \in \mathbb{R}[X]$ nu are rădăcini în $\mathbb{R}$, dar este reductibil:

$$f = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

4) Corpul K se numeşte algebric închis, dacă orice $f \in K[X]$, cu $\deg f \geq 1$ are rădăcină în K (de exemplu $\mathbb{C}$ este algebric închis); rezultă că polinomul $f \in K[X]$ este ireductibil dacă şi numai dacă $\deg f = 1$.

5) Polinomul $f \in \mathbb{R}[X]$ este ireductibil dacă şi numai dacă $\deg f = 1$ sau dacă $\deg f = 2$ şi $\Delta(f) < 0$.

Observaţii 2.3.3. 1) În inelul $A[X]$ avem $f \sim 1 \Longleftrightarrow f \in \mathrm{U}(A)$, şi

$$f \sim g \Longleftrightarrow (\exists) a \in \mathrm{U}(A) : g = af.$$

2) În inelul $K[X]$ avem $f \sim 1 \Longleftrightarrow f \in K^*$, şi

$$f \sim g \Longleftrightarrow (\exists) a \in K^* : g = af.$$

Teorema 2.3.4. *Dacă A nu este corp, atunci $A[X]$ nu este inel cu ideale principale.*

Demonstraţie. Arătăm că există $I \trianglelefteq A[X]$ astfel încât I nu este ideal principal. Deoarece A nu este corp, există un element neinversabil $a \in A,\ a \neq 0$. Fie

$$I = (a, X) = \{ag + Xh \mid g, h \in A[X]\} \trianglelefteq A[X].$$

Presupunem că există $f \in A[X]$ astfel încât $(a, X) = f$. Atunci există $g \in A[X]$ astfel încât $a = fg$ şi $h \in A[X]$ astfel încât $X = fh$; rezultă că $\deg f = 0$, adică $f \in A$, şi f inversabil deoarece $fh = X$. Atunci $(f) = A[X] = (a, X)$, deci există $u, v \in A[X]$ astfel încât $1 = au + vX$; rezultă că $v = 0$, deci $au = 1$, adică $a \in \mathrm{U}(A)$, contradicţie. $\square$

Putem enunţa rezultatul principal al acestei secţiuni:

Teorema 2.3.5. *Dacă A este inel factorial, atunci $A[X]$ este inel factorial.*

Pentru demonstraţia teoremei avem nevoie de câteva noţiuni şi leme.

Teorema 2.3.6. *Dacă $p \in A$ este element prim al domeniului de integritate A, atunci p este prim şi în $A[X]$.*

Demonstraţie. Deoarece $p \in A$ element prim rezultă că p nu este inversabil. Presupunem că $f, g \in A[X]$ şi $p|fg$, şi arătăm că $p|f$ sau $p|g$. Fie $f = \sum_{i=0}^{n} a_i X^i$ şi $g = \sum_{j=0}^{m} b_j X^j$, unde $a_i, b_j \in A$, şi presupunem că $p \nmid f$ şi $p \nmid g$.

Atunci există $k = \min\{i \geq 0 \mid p \nmid a_i\}$, $0 \leq k \leq n$ şi $l = \min\{j \geq 0 \mid p \nmid b_j\}$, $0 \leq l \leq m$. Deoarece $fg = \sum_{r=0}^{m+n} c_r X^r$, pe baza celor de mai sus rezultă că

$$p|c_{k+l} = a_0 b_{k+l} + a_1 b_{k+l-1} + \cdots + a_k b_l + \cdots + a_{k+l-1} b_1 + a_{k+l} b_0.$$

Deoarece p divide elementele $a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}$, rezultă că $p|a_k b_l$; dar p este prim, deci $p|a_k$ sau $p|b_l$, contradicţie. □

Definiţia 2.3.7. Fie A un inel factorial, $f \in A[X]$, $f = \sum_{i=0}^{n} a_i X^i$, şi

$$c(f) = (a_0, \ldots, a_n)$$

conţinutul lui f . Polinomul f se numeşte *primitiv*, dacă $c(f) \sim 1$.

Observaţii 2.3.8. $f = c(f) \cdot f'$, unde $c(f) \in A$ şi $f' \in A[X]$ polinom primitiv. Această scriere este unică, adică dacă $f = af' = bf''$, unde $f', f'' \in A[X]$ sunt polinoame primitive, atunci $a \sim b$ şi $f' \sim f$".

Lema 2.3.9 (Gauss)**.** *Fie A un inel factorial. Dacă $f, g \in A[X]$ sunt polinoame primitive, atunci fg este polinom primitiv. În general, avem*

$$c(fg) = c(f)c(g).$$

Demonstraţie. Presupunem că fg nu este primitiv, adică $c(fg) \nsim 1$. Atunci există $p \in A$ element prim astfel încât $p|c(fg)$, deci $p|fg$. Deoarece p este prim în $A[X]$, rezultă că $p|f$ sau $p|g$ ceea ce contrazice primitivitatea lui f şi g.

În general: $fg = c(f)f'c(g)g'$, unde $f', g' \in A[X]$ sunt polinoame primitive, deci $f'g'$ este primitiv; în acelaşi timp, $fg = c(fg)h$, unde $h \in A[X]$ este polinom primitiv; rezultă că $f'g' \sim h$ şi $c(f)c(g) \sim c(fg)$. □

Lema 2.3.10. *Fie A un inel factorial, $K = frac(A) = \{a/b \mid a, b \in A,\ b \neq 0\}$ şi $f \in A[X]$. Polinomul f este ireductibil în $A[X]$ dacă şi numai dacă f este primitiv şi ireductibil în $K[X]$.*

Demonstraţie. Arătăm că dacă f este primitiv şi ireductibil în $K[X]$, atunci f este ireductibil $A[X]$. Într-adevăr, presupunem prin absurd că f nu este ireductibil în $A[X]$, adică $f = gh$, $g,h \in A[X]$ şi $g,h \not\sim 1$. Deoarece f este primitiv, rezultă că $\deg g, \deg h \geq 1$, adică f este reductibil în $K[X]$, contradicţie.

Invers, presupunem că f este ireductibil în $A[X]$ şi reductibil în $K[X]$, adică $f = gh$, unde $g,h \in K[X]$, $\deg g$, $\deg h \geq 1$. Fie $g = (a/b)g_1$ şi $h = (c/d)h_1$, unde $a/b, c/d \in K$ şi $g_1, h_1 \in A[X]$ sunt primitive; rezultă că $f = (a/b)(c/d)g_1h_1$, adică $bdf = acg_1h_1$.

Deoarece f este ireductibil în $A[X]$, rezultă că f este primitiv; dar g_1h_1 este primitiv (pentru că g_1, h_1 sunt primitive), deci $bd \sim ac$ şi $f \sim g_1h_1$ în $A[X]$, adică f este reductibil în $A[X]$, ceea ce este o contradicţie. □

Demonstraţia Teoremei 2.3.5. a) Arătăm că în $A[X]/\sim$ orice lanţ strict descrescător este finit.

Fie $f_i \in A[X]$, $i \in \mathbb{N}$, astfel încât $f_{i+1}|f_i$, şi arătăm că există $n \in \mathbb{N}$ astfel încât $f_{i+1} \sim f_i$ pentru orice $i \geq n$. Fie $f_i = a_ig_i$, unde $a_i \in A$ şi $g_i \in A[X]$ sunt polinoame primitive. Deoarece $f_{i+1}|f_i$, rezultă că $a_{i+1}g_{i+1}|a_ig_i$; dar $(a_{i+1}, g_i) = 1$, deci $a_{i+1}|a_i$ şi $g_{i+1}|g_i$.

Deoarece A este inel factorial, există $n_1 \in \mathbb{N}$ astfel încât $a_{i+1} \sim a_i$ pentru orice $i \geq n_1$. Deoarece $g_{i+1}|g_i$, rezultă că $\deg g_{i+1} \leq \deg g_i$, adică există $n_2 \in \mathbb{N}$ astfel încât $\deg g_{i+1} = \deg g_i$ pentru orice $i \geq n_2$; rezultă că există $h \in A$ astfel încât $g_i = g_{i+1}h$, dar g_i, g_{i+1} sunt primitive, de aceea $h \sim 1$ şi $g_i \sim g_{i+1}$ pentru orice $i \geq n_2$.

Fie $n = \max\{n_1, n_2\}$; atunci $f_i = a_ig_i \sim a_{i+1}g_{i+1} = f_{i+1}$ pentru orice $i \geq n$.

b) Arătăm că dacă f este ireductibil în $A[X]$, atunci f este prim. Dacă $\deg f = 0$, atunci $f \in A$ şi f este ireductibil în A. Deoarece A este factorial, rezultă că f este prim în A, deci f este prim în $A[X]$.

Presupunem că $\deg f \geq 1$. Din Lema 2.3.10. rezultă că f este primitiv şi ireductibil în $K[X]$. Deoarece $K[X]$ este inel euclidian, este şi inel factorial, de aceea f este prim în $K[X]$.

Presupunem că în $f|gh$ $A[X]$; rezultă că $f|gh$ în $K[X]$, deci $f|g$ sau $f|h$. Dacă $f|g$ în $K[X]$, atunci există $q \in K[X]$ astfel încât $g = fq$. Fie $g = ag_1$, $q = (b/c)q_1$, unde $a, b.c \in A$ şi $g_1, q_1 \in A[X]$ sunt primitive; atunci $ag_1 = (b/c)fq_1$, adică $acg_1 = bfq_1$. Aplicând Lema lui Gauss 2.3.9. rezultă că $ac \sim b$ şi $g_1 \sim fq_1$. Deoarece $f|g_1$ în $A[X]$ şi $(a, f) = 1$, rezultă că $f|g$ în $A[X]$. □

Dăm în continuare două criterii de ireductibilitate.

Teorema 2.3.11 (Eisenstein)**.** *Fie A un inel factorial, $K = K(A)$ corpul fracţiilor lui A, $p \in A$ un element ireductibil şi $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$.*

Dacă $p \nmid a_n$, $p|a_i$ pentru orice $i < n$, şi $p^2 \nmid a_0$, atunci f este ireductibil în $K[X]$ (deci şi în $A[X]$, dacă f este primitiv.)

Demonstraţie. Presupunem că f polinom primitiv şi reductibil, adică $f = gh$, unde $g, h \in A[X]$ şi $\deg g, \deg h \geq 1$.

Fie $g = \sum_{i=0}^{m} b_i X^i$, $h = \sum_{j=0}^{l} c_j X^j$, $m + l = n$ $(m, l \geq 1)$. Atunci $a_n = b_m c_l$, şi deoarece $p \nmid a_n$, rezultă că $p \nmid b_m$ şi $p \nmid c_l$.

Deoarece $a_0 = b_0 c_0$, şi conform ipotezei $p|a_0$, dar $p^2 \nmid a_0$, putem presupune că $p|b_0$ şi $p \nmid c_0$. Fie $k = \min\{j \geq 0 \mid p \nmid b_j\}$; rezultă că $0 < k \leq m < n$, deci $p|a_k$.

Ştim că $a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_{k-1} c_1 + b_k c_0$; din minimalitatea lui k rezultă că $p|b_0, b_1, \ldots, b_{k-1}$ de $p \nmid b_k$ şi $p \nmid c_0$, adică $p \nmid b_k c_0$, contradicţie. □

Teorema 2.3.12. *Fie A, B inele factoriale şi fie $\varphi : A \to B$ un morfism surjectiv de inele. Fie*

$$\bar{\varphi} : A[X] \to B[X], \quad \bar{\varphi}(f) = \sum_{i=0}^{n} \varphi(a_i) X^i$$

morfismul surjectiv indus de proecţia canonică. Fie $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ şi presupunem că $\deg(f) = \deg(\bar{\varphi}(f)) \geq 1$ şi că f este primitiv. Dacă $\bar{\varphi}(f)$ este ireductibil în $B[X]$, atunci f este ireductibil în $A[X]$.

Demonstraţie. Presupunem că f este reductibil în $A[X]$, adică $f = gh$, unde $g, h \in A[X]$, şi $\deg g$, $\deg h \geq 1$; rezultă că $\bar{\varphi}(f) = \bar{\varphi}(g)\bar{\varphi}(h)$. Deoarece $\deg(f) = \deg(\bar{\varphi}(f))$, rezultă că $\deg(g) = \deg(\bar{\varphi}(g)) \geq 1$ şi $\deg(h) = \deg(\bar{\varphi}(h)) \geq 1$, adică $\bar{\varphi}(f)$ este reductibil, contradicţie. □

Exerciţiul 2.23. a) $f \in \mathbb{C}[X]$ este ireductibil $\Leftrightarrow \deg f = 1$.

b) $f \in \mathbb{R}[X]$ este ireductibil $\Leftrightarrow \deg f = 1$ sau $\deg f = 1$ şi $\Delta(f) < 0$.

Exerciţiul 2.24. a) Să se determine polinoamele ireductibile $f \in \mathbb{Z}_2[X]$, dacă $\deg f \leq 6$.

b) Să se determine polinoamele ireductibile $f \in \mathbb{Z}_3[X]$, dacă $\deg f \leq 3$.

Exerciţiul 2.25. Fie A un inel factorial, $K = K(A)$ corpul fracţiilor lui A, $\frac{r}{s} \in K$ o fracţie ireductibilă, şi fie $f = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$.

Dacă $f(\frac{r}{s}) = 0$, atunci $r|a_0$ şi $s|a_n$.

Exerciţiul 2.26. Fie p un număr prim şi fie $n \neq 1$. Aplicând criteriul lui Eisenstein, să se arate că următoarele polinoame sunt ireductibile în $\mathbb{Z}[X]$:

a) $f = X^n \pm p$.

b) $f = X^{p^n} + p - 1$.

c) $f = X^{p-1} + \cdots + X + 1$. (Indicaţie: fie $Y = X + 1$.)

Exerciţiul 2.27. Fie $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, p un număr prim, şi fie

$$\hat{f} = \hat{a}_0 + \hat{a}_1X + \cdots + \hat{a}_nX^n \in \mathbb{Z}_p[X].$$

Presupunem că $p \not| a_n$. Să se arate că dacă $\hat{f}$ este ireductibil, atunci f este ireductibil.
Aplicaţie. a) $f = X^4 - 3X^3 + 10X^2 - 6X + 1$, $p = 2$.

b) $f = X^5 - 5X^4 - 6X + 1$, $p = 5$.

c) $f = X^p - X + a$, $(a, p) = 1$.

Extinderi de corpuri | 3

Matematicianul norvegian Niels Henrik Abel (1802–1829) a fost primul primul care a arătat în 1824 că nu orice ecuaţie de grad 5 poate fi rezolvată prin radicali, o demonstraţie incompletă fiind data de Paolo Ruffini în 1799. Pentru o discuţie generală a acestei probleme, matematicianul francez Évariste Galois (1811-1832) a utilizat grupuri de permutări şi creat ceea ce azi numim teoria lui Galois. Această teorie furnizează un criteriu general de rezolvabilitate prin radicali. Rezultatele sale au fost publicate doar în 1846 de către Liouville. Teoria lui Galois modernă foloseşte grupurile pentru a studia extensiile de corpuri şi are multiple aplicaţii şi generalizări.

3.1 Extinderi finite

În cele ce urmează, prin corp înţelegem corp comutativ. Dacă K este subcorp al corpului L, atunci L se numeşte *extindere* a lui K, şi notăm: $K \leq L$ sau L/K. Dacă $K \leq L$, atunci L este K-algebra, deci în particular, L este K-spaţiu vectorial.

Definiţia 3.1.1. Fie L/K o extindere de corpuri. Dimensiunea lui L peste K se notează $[L : K]$ şi se numeşte *gradul extinderii*:

$$[L : K] = \dim_K L$$

Spunem că L este *extindere finită* a lui K, dacă $[L : K]$ este finit.

Teorema 3.1.2. *Dacă $K \leq L \leq L'$ sunt extinderi de corpuri, atunci*

$$[L' : K] = [L : K][L' : L].$$

Demonstraţie. Fie $\{x_i \mid i \in I\}$ o bază a lui L peste K şi fie $\{y_j \mid j \in J\}$ o bază a lui L' peste L. Este suficient de arătat că $\{x_i y_j \mid (i, j) \in I \times J\}$ este o bază a lui L' peste

K. Dacă $a \in L'$, atunci există $b_j \in L$, astfel încât $a = \sum_{j \in J} b_j y_j$, unde suma este finită. Pentru orice b_j există $\alpha_{ij} \in K$ astfel ca $b_j = \sum_{i \in I} \alpha_{ij} x_i$. Rezultă că

$$a = \sum_{i \in I,\ j \in J} \alpha_{ij} x_i y_j,$$

adică a este combinaţie liniară elementelor mulţimii $\{x_i y_j \mid (i,j) \in I \times J\}$,cu coeficienti în K. Deci, L' este K-spaţiu vectorial generat de $\{x_i y_j \mid (i,j) \in I \times J\}$.

Presupunem că $\sum \alpha_{ij} x_i y_j = 0$, unde $\alpha_{ij} \in K$ şi $(i,j) \in I \times J$. Obţinem:

$$\sum_{j \in J} (\sum_{i \in I} \alpha_{ij} x_i) y_j = 0$$

de unde rezultă că $\sum_{i \in I} \alpha_{ij} x_i = 0$ pentru orice j, deci $\alpha_{ij} = 0$, pentru orice $i \in I$ şi pentru orice $j \in J$. Am arătat că elementele $x_i y_j$, unde $(i,j) \in I \times J$, liniar independente peste K. □

3.2 Extinderi algebrice

Fie L/K o extindere de corpuri.

Definiţia 3.2.1. a) Spunem că $a \in L$ este *element algebric peste K,* dacă există $f \in K[X]$, $f \neq 0$ astfel ca $f(a) = 0$.

Un element $a \in L$, care nu e algebric peste K se numeşte *element transcendent* peste K.

b) Dacă un element al corpul numerelor complexe $\mathbb{C}$ este algebric peste $\mathbb{Q}$, atunci elementul se numeşte *număr algebric*. Un element din $\mathbb{C}$ care este transcendent peste $\mathbb{Q}$, se numeşte *număr transcendent*.

c) Extinderea de corpuri $K \leq L$ se numeşte *extindere algebrică*, dacă orice $a \in L$ este element algebric peste K.

De exemplu, $\sqrt{2} \in \mathbb{R}$ este număr algebric, deoarece este rădăcină a polinomului $X^2 - 2 \in \mathbb{Q}[X]$; $i \in \mathbb{C}$ este număr algebric, deoarece este rădăcină a polinomului $X^2 + 1 \in \mathbb{Q}[X]$; $\pi = 3,1415\ldots$ este număr transcendent (F. Lindemann); $e = 2,71\ldots$ este număr transcendent (Ch. Hermite).

Teorema 3.2.2. *Orice extindere finită este algebrică.*

Demonstraţie. Dacă este extindere finită $K \leq L$ şi $[L:K] = \dim_K L = n$, atunci pentru orice $a \in L$ elemente $1, a, a^2, \ldots, a^n$ sunt liniar dependente în L. Rezultă că există elementele α_i, $i = 0, \ldots, n \in K$ nu toate nule, astfel ca

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0.$$

Fie $f = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_n X^n \in K[X]$, şi $f \neq 0$. De aici rezultă că $f(a) = 0$, deci a este element algebric peste K. $\square$

Definiţia 3.2.3. a) Fie $K \leq L$ şi $A \subseteq L$. Notăm prin $K[A]$ subinelul lui L generat de K şi A; prin $K(A)$ notăm subcorpul lui L generat de $K \cup A$ (cel mai mic subcorp al lui L conţinând pe $K \cup A$), şi spunem că am *adjuncţionat* la K elementele lui A.

b) În particular, dacă $A = \{a_1, \ldots, a_n\}$ atunci notăm $K(A) = K(a_1, \ldots, a_n)$. O extindere $K \leq L$ se numeşte *de tip finit*, dacă există $a_i \in L$, $(i = 1, \ldots, n)$ astfel ca $L = K(a_1, \ldots, a_n)$.

c) O extindere se numeşte simplă $K \leq L$ se numeşte *simplă*, dacă există $a \in L$ astfel ca $L = K(a)$. În acest caz, spunem că a este element *primitiv* al extinderii $K \leq L$.

Observaţii 3.2.4. 1) Orice extindere finită este de tip finit.

Într-adevăr dacă $K \leq L$ este o extindere finită, atunci L are o bază finită $\{a_1, \ldots, a_n\}$. Rezultă că $L = K(a_1, \ldots, a_n)$.

2) $K[A] \subseteq K(A)$.

3) Dacă $K \leq L$ şi $A \subseteq L$, atunci $K(A) = K$ dacă şi numai dacă $A \subseteq K$.

4) $K[a] = \{f(a) \mid f \in K[X]\} = \{\alpha_0 + \alpha_1 a + \cdots + \alpha_n a^n \mid \alpha_i \in K,\ n \in \mathbb{N}\}$.

5) $K(a) = \{\frac{f(a)}{g(a)} \mid f, g \in K[X],\ g(a) \neq 0\}$.

6) $K[A] = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n], n \in \mathbb{N},\ a_1, \ldots, a_n \in A\}$.

7) $K(A) = \{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in K[X_1, \ldots, X_n], a_1, \ldots, a_n \in A, g(a_1, \ldots, a_n) \neq 0,\ n \in \mathbb{N}\}$.

Teorema 3.2.5. *Dacă $a \in L$ este element algebric peste K, atunci există unic $f \in K[X]$ polinom nenul, astfel ca:*

(1) $f(a) = 0$;

(2) *f este polinom monic* (coeficientul principal a lui f (dominant) este 1);

(3) *dacă $g \in K[X]$, $g \neq 0$ şi $g(a) = 0$, atunci $f \mid g$.* (Deci f este polinomul nenul de cel mai mic grad pentru care a este rădăcină.)

Demonstraţie. Fie $\phi : K \to L$, $\phi(\alpha) = \alpha$, şi fie

$$\bar{\Phi}_a : K[X] \to L, \quad \bar{\Phi}_a(g) = \alpha_0 + \alpha_1 a + \cdots + \alpha_m a^m,$$

unde $g = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m \in K[X]$. Din proprietatea de universalitate a inelului de polinoame rezultă că $\bar{\Phi}_a$ este morfism unital de inele. Deci $\operatorname{Ker}\bar{\Phi}_a = \{g \in K[X] \mid g(a) = 0\}$ este ideal, deci ideal principal al lui $K[X]$. Deoarece a este algebric, rezultă că $\operatorname{Ker}\bar{\Phi}_a \neq 0$, adică există $0 \neq f \in K[X]$ astfel ca $\operatorname{Ker}\bar{\Phi}_a = (f)$. Deci, f satisface condiţiile (1) şi (3) din teoremă.

Deoarece, că $(f) = (f')$ dacă şi numai dacă f şi f' sunt asociate în $K[X]$, rezultă că există unic $f \in K[X]$ monic, astfel ca $\operatorname{Ker}\bar{\Phi}_a = (f)$. □

Definiţia 3.2.6. a) Fie $a \in L$ un element algebric peste K. Polinomul f de mai sus se numeşte *polinom minimal* peste K al elementului a, şi notăm $f =: m_{K,a}$. Gradul polinomului $m_{K,a}$ este *gradul a*.

b) Fie $a, b \in L$ elemente algebrice peste K. Dacă a şi b au acelaşi polinom minimal peste K, atunci a şi b se numesc *conjugate* peste K.

Teorema 3.2.7 (Caracterizarea extinderilor algebrice simple)**.** *Fie $K \leq L$ o extindere de corpuri şi fie $a \in L$ un element algebric peste K. Fie $0 \neq f \in K[X]$.*

1) *$f = m_{K,a}$ dacă şi numai dacă*

(1) *$f(a) = 0$;*

(2) *f este monic;*

(3) *f ireductibil în $K[X]$.*

2) *Presupunem că $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_{n-1} X^{n-1} + X^n$ polinom minimal al lui a. Atunci:*

(a) $K(a) = K[a] \simeq K[X]/(f)$;

(b) $[K(a) : K] = n = \deg f$ *şi* $\{1, a, a^2, \ldots, a^{n-1}\}$ *este bază în* $K(a)$*;*

(c) *Înmulţirea în K-algebra $K(a)$ se exprimă în baza $1, a, a^2, \ldots, a^{n-1}$ folosind:*

$$a^n = -\alpha_0 - \alpha_1 a - \cdots - \alpha_{n-1} a^{n-1}$$

(c) *Dacă $b \in L$ este rădăcină a lui f, atunci există un unic izomorfism de K-algebre $\phi : K(a) \to K(b)$ astfel încât $\phi(a) = b$.*

Demonstraţie. 1) „$\Longrightarrow$” Presupunem că $f = gh$, unde $g.h \in K[X]$. Atunci $0 = f(a) = g(a)h(a)$, şi deoarece L este corp, rezultă că $g(a) = 0$ sau $h(a) = 0$, deci $f \mid g$ sau $f \mid h$; rezultă că $f \sim g$ sau $f \sim h$, deci f este ireductibil.

„$\Longleftarrow$” Deoarece $f(a) = 0$, rezultă că $m_{K,a} \mid f$; dar f este ireductibil, deci $f \sim m_{K,a}$. Deoarece ambele sunt polinoame monice, rezultă că $f = m_{K,a}$.

2) (a) Dacă $\bar{\Phi}_a : K[X] \longrightarrow L$, $\bar{\Phi}_a(g) = g(a)$ este morfism de inele, atunci $\operatorname{Im}\bar{\Phi}_a = K[a]$ şi $\operatorname{Ker}\bar{\Phi}_a = (f)$. Deci, pe baza teoremei I de izomofism pentru inle, $K[X]/(f) \simeq K[a]$. Deoarece f este ireductibil în $K[X]$, rezultă că f este ideal maximal al lui $K[X]$. Deci $K[X]/(f)$ este corp, deci şi $K[a]$ este corp, şi deoarece $K[a] \subseteq K(a)$, rezultă că $K(a) = K[a]$.

(b) Deoarece a are gradul n peste K, rezultă că elementele $1, a, a^2, \ldots, a^{n-1}$ sunt liniar independente peste K.

Dacă $b \in K(a) = K[a]$, atunci din egalitatea $K[a] = \operatorname{Im}\bar{\Phi}_a$ rezultă că există $g \in K[X]$, astfel ca $b = g(a)$. Împărţind pe g la f primim un cât q şi un rest r astfel ca: $g = fq + r$, $\deg r < \deg f$, de unde:

$$b = g(a) = f(a)q(a) + r(a) = r(a)$$

şi aceasta arată că K-spaţiul liniar $K(a)$ este generat de elementele $1, a, a^2, \ldots, a^{n-1}$. Deci, $1, a, a^2, \ldots, a^{n-1}$ formează o bază a lui $K(a)$ peste K.

(c) Din egalitate $f(a) = 0$ rezultă că

$$\begin{aligned} a^{n+1} &= -\alpha_0 a - \alpha_1 a^2 - \cdots - \alpha_{n-1} a^n = \\ &= \alpha_{n-1}\alpha_0 - (\alpha_0 - \alpha_{n-1}\alpha_1)a - (\alpha_1 - \alpha_{n-1}\alpha_2)a^2 - \cdots - (\alpha_{n-2} - \alpha_{n-1}^2)a^{n-1} \end{aligned}$$

Din aproape în aproape primim elementele $a^{n+2}, \ldots, a^{2n-2}$ ca şi combinaţie liniară a lui $1, a, a^2, \ldots, a^{n-1}$.

(d) Din 1) rezultă că f este polinomul minimal al lui b, deci afirmaţiile (a), (b), (c) de mai sus sunt valabile şi pentru b. Considerăm izomorfismele de K-algebre $\bar{\Phi}_a : K[X] \to K(a)$ şi $\bar{\Phi}_b : K[X] \to K(b)$ de mai sus. Fie

$$\varphi : K(a) \to K(b), \quad \varphi = \bar{\Phi}_b \circ \bar{\Phi}_a^{-1}.$$

Atunci φ este izomorfism de K-algebre şi avem

$$\varphi(\beta_0 + \beta_1 a + \cdots + \beta_{n-1}a^{n-1}) = \beta_0 + \beta_1 b + \cdots + \beta_{n-1}b^{n-1}$$

pentru orice $\beta_0, \ldots, \beta_{n-1} \in K$.

Deoarece K şi a generează pe $K(a)$, există unic astfel de izomorfism. $\square$

Observaţii 3.2.8. 1) Din teorema de mai sus pe baza rezultă că pentru orice $b \in K(a)$ există o expresie polinomială:

$$b = g(a) = \beta_0 + \beta_1 a + \cdots + \beta_{n-1} a^{n-1} \in K(a),$$

unde $g \in K[X]$.

2) Dacă $b \in K(a)$, $b \neq 0$, atunci b se scrie în forma de mai sus şi atunci expresia polinomială a lui b^{-1} se obţine astfel:

Din faptul că f este prim în $K[X]$, respectiv $\deg g \leq \deg f$, rezultă că f şi g relativ prime în $K[X]$, deci există $u, v \in K[X]$ astfel ca $ug + vf = 1$, de unde rezultă că $u(a)g(a) = 1$, deoarece $f(a) = 0$. Deci, $b^{-1} = u(a)$.

3) Dacă $a \in L$ este element algebric peste K, atunci extinderea $K \leq K(a)$ este finită, deci şi algebrică.

4) Dacă a $K \leq L$ este extindere finită, atunci pentru orice $a \in L$ algebric peste K, gradul lui a divide pe $[L : K]$.

Într-adevăr, din Teorema 3.2.2. rezultă că a este algebric peste K. Din Teorema 3.1.2. rezultă că $[L : K] = [L : K(a)][K(a) : K]$. Deci, din Teoreme 3.2.7. 2), gradul lui a divide pe $[L : K]$.

5) Dacă $K \leq L$ şi $a_1, a_2 \in L$ sunt elemente algebrice peste K, cu acelaşi polinom minimal, adică sunt conjugate, atunci corpurile $K(a_1)$ şi $K(a_2)$ sunt izomorfe.

Într-adevăr, $K(a_1) \simeq K[X]/(f) \simeq K(a_2)$, unde f este polinomul minimal al lui a_1 şi a_2.

6) Fie $a_1, \ldots, a_n \in L$ algebrice peste K. Atunci $K(a_1, \ldots, a_n) = K[a_1, \ldots, a_n]$, adică pentru orice $b \in K(a_1, \ldots, a_n)$ există $g \in K[X_1, \ldots, X_n]$ astfel încât $b = g(a_1, \ldots, a_n)$.

7) Dacă $K \leq L$, $L = K(a_1, \ldots, a_n)$ şi fiecare a_i este algebric peste $K(a_1, \ldots, a_{i-1})$, unde $(i = 1, \ldots, n)$ atunci extinderea $K \leq L$ este finită, deci şi algebrică. În particular, dacă $a_1, \ldots a_n$ sunt element algebrice peste K, atunci extinderea $K \leq L$ este finită.

Într-adevăr, orice $m_i = [K(a_1, \ldots, a_{i-1}, a_i) : K(a_1, \ldots, a_{i-1})]$, $i = 1, \ldots, n$ este finit, şi rezultă că $[L : K] = m_1 m_2 \ldots m_n$.

8) Dacă $K \leq L$ şi A este mulţimea elementelor din L algebrice peste K, atunci $K \subseteq A$ şi A este subcorp al lui L.

Într-adevăr, dacă $a \in K$, atunci a este rădăcină a polinomului $X - a \in K[X]$, adică a este algebric peste K. Deci, $K \subseteq A$. Dacă $a_1, a_2 \in A$, atunci din 7) rezultă că a $K \leq K(a_1, a_2)$ este extindere algebrică, de unde rezultă că $K(a_1, a_2) \subseteq A$. Deoarece $a_1, a_2 \in K(a_1, a_2)$ şi $K(a_1, a_2)$ este corp, rezultă că $a_1 - a_2 \in K(a_1, a_2) \subseteq A$. Dacă $a_2 \neq 0$, atunci $a_1 a_2^{-1} \in K(a_1, a_2) \subseteq A$. Deci, A este subcorp al lui L.

9) Mulţimea $\mathbb{A} := \{z \in \mathbb{C} \mid z$ este număr algebric $\}$ a numerelor algebrice este subcorp al lui $\mathbb{C}$.

10) Nu orice extindere algebrică este finită; de exemplu $\mathbb{Q} \leq \mathbb{A}$ este algebrică dar nu este finită.

Teorema 3.2.9 (tranzitivitatea extinderilor algebrice)**.** *Dacă a $K \leq L$ şi $L \leq L'$ sunt extinderi algebrice, atunci $K \leq L'$ este extindere algebrică.*

Demonstraţie. Dacă $a \in L'$ atunci există $g \in L[X]$, $0 \neq g = \beta_0 + \beta_1 X + \cdots + \beta_n X^n$ astfel ca $g(a) = 0$. Fie $L'' := K(\beta_0, \beta_1, \ldots, \beta_n)$; atunci a este algebric peste L şi din Observaţia3.2.8. 7) rezultă că extinderile $K \leq L''$ şi $L'' \leq L(a)$ sunt finite. Deci extinderea $K \leq L(a)$ este finită, şi $K \leq L(a)$ este algebrică. Deci, a este element algebric peste K. □

Exemplul 3.2.10. 1) Dacă $\in \mathbb{R}_+$ este număr algebric, atunci $\sqrt[n]{a}$ este algebric. Într-adevăr, dacă $f(a) = 0$, unde $0 \neq f \in \mathbb{Q}[X]$, atunci $\sqrt[n]{a}$ este rădăcină polinomului $f(X^n)$.

2) Numărul $a = \sqrt{8+\sqrt{5}} - \sqrt[7]{\sqrt{2}-\sqrt{3}}$ este algebric peste $\mathbb{Q}$, căci numerele algebrice formează un subcorp.

3) Numărul $a = \pi^2 - 3\pi + 2$ nu este algebric, deoarece dacă pentru polinomul $g \in \mathbb{Q}[X]$, $g \neq 0$ am avea $g(a) = 0$, atunci π ar fi rădăcină a lui $g(X^2 - 3X + 2)$, dar π nu este algebric.

Exerciţiul 3.1. Sunt algebrice următoarele numere?

a) $a = \sqrt{1+\pi^2}$

b) $b = \pi - \sqrt{\pi}$

c) $c = \pi^2 + \pi + \sqrt{1+2\pi}$.

Exerciţiul 3.2. Fie $f = X^3 - X + 1 \in \mathbb{Q}[X]$ şi fie $a \in \mathbb{C}$ rădăcină a lui f. Să se arate că:

a) f ireductibil şi să se determine $\frac{1}{a}$ în funcţie de $\{1, a, a^2\}$.

b) Fie $b = 1 - 2a + 3a^2 \in \mathbb{Q}(a)$. Să se calculeze $\frac{1}{b}$ ca o combinaţie liniară a lui $\{1, a, a^2\}$.

Exerciţiul 3.3. a) Fie $f = X^4 - 6X - 2 \in \mathbb{Q}[X]$. Să se arate că f este ireductibil peste $\mathbb{Q}$; dacă $a \in \mathbb{C}$ este rădăcină a lui f, să se calculeze $a^3 - 2a^5$, $\frac{1}{a}$ ca şi combinaţie liniară a bazei $\{1; a; a^2; a^3\}$.

b) Fie $f = X^4 + 6X - 2 \in \mathbb{Q}[X]$. Să se arate că f este ireductibil peste $\mathbb{Q}$; dacă $a \in \mathbb{C}$ este rădăcină a lui f, să se scrie elementele $u^6 - 2u^3$ şi $\frac{1}{u}$ ca şi combinaţie liniară a bazei $\{1, u, u^2, u^3\}$.

c) Fie $u \in \mathbb{C}$ rădăcină a polinomului $X^3 - 2X + 2$ (care este ireductibil peste $\mathbb{Q}$). Să se scrie elementele u^7, u^{-1} şi $u^4 + u^{-2}$ ca şi combinaţie liniară a bazei $\{1, u, u^2\}$.

d) Fie $u \in \mathbb{C}$ rădăcină a polinomului $X^4 - 3X + 3$ (care este ireductibil peste $\mathbb{Q}$). Să se scrie elementele $(u^3 - 3)^{-1}(u^2 + 2)$ ca şi combinaţie liniară a bazei $\{1, u, u^2, u^3\}$.

e) Să se arate că dacă $u \in \mathbb{C}$ este rădăcină a polinomului $f(x) = X^3 - 12X + 8$, atunci şi $\frac{u^2}{2} - 4$ este rădăcină.

Exerciţiul 3.4. Fie $a = \sqrt[3]{2}$ şi $K = \mathbb{Q}(a) \leq \mathbb{C}$. Să se calculeze în K:
a) $a^4 - a$; b) $\frac{1}{a}$; c) $\frac{a-2}{a+2}$.

Exerciţiul 3.5. Fie $a = \sqrt[4]{2}$ şi $K = \mathbb{Q}(a) \leq \mathbb{C}$. Să se calculeze în K:
a) $\frac{1}{a}$; b) $(a^3 + 2a^2 - a + 3)(2a^3 - 4a^2 + 5a - 1)$.

Exerciţiul 3.6. Să se arate că pentru orice $a, b \in \mathbb{Q}$, cu $a \neq b$, avem $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Exerciţiul 3.7. Să se determine gradul extinderilor $K/\mathbb{Q}$ de corpuri:
a) $\mathbb{Q}(\sqrt{7})$; b) $\mathbb{Q}(i\sqrt{5})$; c) $\mathbb{Q}(1 + i\sqrt{3})$;
d) $\mathbb{Q}(a + bi)$; e) $\mathbb{Q}(\sqrt{5}, \sqrt{6})$; f) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;
g) $\mathbb{Q}(i + \sqrt{5})$; h) $\mathbb{Q}(\sqrt{6} - i\sqrt{5})$; i) $\mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Exerciţiul 3.8. Să se determine polinoamele minimale peste $\mathbb{Q}$ respectiv peste $\mathbb{R}$ ale numerelor complexe de mai jos:
a) $\sqrt[3]{3}$; b) $1 - i\sqrt{3}$; c) $2 + i$; d) $i\sqrt[3]{3}$.

Exerciţiul 3.9. Fie $a = \sqrt[3]{1 + \sqrt{3}}$, $K = \mathbb{Q}(\sqrt{3})$,$L = \mathbb{Q}(a)$. Să se arate că:
a) $\mathbb{Q} \leq K \leq L$ şi $L = K(a)$;
b) $[L : \mathbb{Q}] = 6$;
c) $[K : \mathbb{Q}] = 2$;
d) $[L : K] = 3$ şi să se determine polinomul minimal $m_{K,a}$.

Exerciţiul 3.10. Fie $a = \sqrt{1 + \sqrt{3}} \in K$ unde $K = \mathbb{Q}(\sqrt{1 + \sqrt{3}})$ şi fie $L = \mathbb{Q}(\sqrt{3})$.
a) Să se determine polinomul minimal $m_{\mathbb{Q},a}$;
b) Să se arate că $[K : \mathbb{Q}] = 4$;
c) Să se arate că $\mathbb{Q} \leq L \leq K$ şi $[L : \mathbb{Q}] = 2$;
d) Să se determine polinomul minimal $m_{L,a}$.

Exerciţiul 3.11. Fie $a = i\sqrt{\sqrt[3]{2}-1}$, $L = \mathbb{Q}(a)$ şi $K = \mathbb{Q}(\sqrt[3]{2})$. Să se arate că:

a) $\mathbb{Q} \leq K \leq L$ şi $L = K(a)$;

b) a este rădăcină a polinomului $f = X^6 - 3X^4 + 3X^2 + 1 \in \mathbb{Q}[X]$;

c) $a \notin K$;

d) $[L : \mathbb{Q}] = 6$ şi f este ireductibil peste $\mathbb{Q}$.

Exerciţiul 3.12. Să se arate că pentru orice $n \geq 1$ există în $\mathbb{Q}[X]$ un polinom ireductibil de grad n. Deducem că pentru orice $n \geq 1$ $\mathbb{Q}$ are o extindere de grad n.

Exerciţiul 3.13. Fie $k \subseteq K$ o extindere de corpuri.

a) $[K : k] = 1$ dacă şi numai dacă $k = K$.

b) Dacă $[K : k]$ este un număr prim, să se arăte că nu există L corp astfel ca $k \subset L \subset K$; mai mult, pentru orice element $a \in K \setminus k$, avem K=k(a).

Exerciţiul 3.14. a) Dacă $K \leq L$ este o extindere algebrică şi K este infinit, atunci K şi L au acelaşi cardinal.

b) Dacă $K \leq L$ este o extindere algebrică şi K este finit, atunci L este finit sau numărabil.

Exerciţiul 3.15. Dacă $K \leq L$ şi $A, B \subseteq L$, atunci $(K(A))(B) = K(A \cup B) = (K(B))(A)$.

3.3 Corpul de descompunere al unui polinom

3.3.1 Adjuncţionarea unei rădăcini

În paragraful anterior, pornind cu o extindere $K \leq L$ şi un element $a \in L$ algebric peste K, am construit subcorpul $K(a)$ al corpului L, folosind polinomul minimal al lui a, care este ireductibil peste K. În cele ce urmează, pornim cu un corp K şi un polinom ireductibil $f \in K[X]$ şi construim o extindere $K(a)/K$ pe care o obţinem adjuncţionând la K o rădăcină a a polinomului f. Repetând construcţia, găsim (abstracţie făcând de un izomorfism) cel mai mic corp ce conţine pe K şi toate rădăcinile lui f.

Teorema 3.3.1. *Dacă K este un corp şi $f \in K[X]$ un polinom ireductibil monic, atunci există un corp L cu următoarele proprietăţi:*

(1) *K este izomorf cu un subcorp al lui L, adică putem considera că $K \leq L$.*

(2) *L conţine o rădăcină a a lui f astfel încât $L = K(a)$ şi $f = m_{K,a}$.*

Demonstraţie. Deoarece f este ireductibil în $K[X]$ rezultă că $f \notin K$ şi $L = K[X]/(f)$ este corp. Deci dacă $\alpha \in K^*$, atunci $p(\alpha) \notin (f)$ arată că proiecţia canonică $p : K[X] \to L$ este morfism injectiv, adică subcorpul $p(K)$ al lui L este izomorf cu K. Vom identifica pe K cu $p(K)$, şi considerăm că L este extindere a lui K şi $f \in L[x]$.

Fie $a := X + (f) \in L$ şi $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$. Atunci

$$f(a) = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n + (f) = f + (f) = (f),$$

de unde rezultă că $f(a) = 0$ în L. Deci, a este rădăcină a lui f. Deoarece $K \cup \{X\}$ generează inell $K[X]$ şi $p : K[X] \to L$ este morfism surjectiv, rezultă că $p(K \cup \{X\}) = K \cup \{a\}$ generează pe L. Deci, $L = K[a] = K(a)$. Deoarece f este ireductibil, rezultă că f este polinomul minimal al lui α. $\square$

Exemplul 3.3.2. 1) Am văzut că polinomul $X^2 + 1 \in \mathbb{R}[X]$ este ireductibil şi corpul $R[X]/(X^2+1)$ este o extindere de grad 2 a lui $\mathbb{R}$. Notând $i := X + (X^2+1)$ rădăcina lui X^2+1, adică $i^2 = -1$, vedem imediat că

$$\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}.$$

Obţinem astfel corpul $\mathbb{C}$ al numerelor complexe prin adjuncţia lui i la $\mathbb{R}$, adică $\mathbb{C} = \mathbb{R}(i)$.

2) Corpurile finite pe care le cunoaştem până acum sunt de forma $\mathbb{Z}_p$, unde p este un număr prim. Alte corpuri finite se pot construi folosind teorema de mai sus. Polinomul $f = X^2 - X - \hat{1} \in \mathbb{Z}_3[X]$ este ireductibil peste $\mathbb{Z}_3$, deoarece niciun element al lui $\mathbb{Z}_3$ nu este rădăcină a lui f. Deci, $K := \mathbb{Z}_3[x]/(f)$ este corp, $a := X + (f) \in K$ este rădăcină f şi $K = \mathbb{Z}_3(a)$. Elementele lui K au următoarea formă: $u = \alpha + \beta a$, unde $\alpha, \beta \in \mathbb{Z}_3$. Deci $|K| = 9$.

Dacă $u' = \alpha' + \beta' a \in K$, atunci $u + u' = (\alpha + \alpha') + (\beta + \beta')a$. Produseul uu' se obţine dacă folosim că $a^2 = a + \hat{1}$: $uu' = \alpha\alpha' + \beta\beta' + (\alpha\beta' + \alpha'\beta + \beta\beta')a$.

De exemplu, din faptul că $a^2 = a + \hat{1}$, rezultă că $a(a - \hat{1}) = \hat{1}$, ceea ce arată că $a^{-1} = a - \hat{1} = a + \hat{2}$. Calculăm inversa lui $\hat{1} + \hat{2}a$, care are forma $\alpha + \beta a$. Din egalitatea $(\alpha + \beta a)(\hat{1} + \hat{2}a) = \hat{1}$ rezultă sistemul de ecuaţii $\alpha + \hat{2}\beta = \hat{1}$, $\hat{2}\alpha = \hat{0}$, deci $\alpha = \hat{0}$ şi $\beta = \hat{2}$. De aici, $(\hat{1} + \hat{2}a)^{-1} = \hat{2}a$.

Teorema 3.3.3. *Fie K_1 şi K_2 corpuri şi fie*

$$f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n \in K_1[X], \qquad g = \beta_0 + \beta_1 X + \cdots + \beta_n X^n \in K_2[X]$$

polinoame de grad n. Fie $K_1(a_1)$ respectiv $K_2(a_2)$ corpuri obţinule prin adjuncţionarea la K_1 respectiv la K_2 a câte unei rădăcini ale polinoamelor f respectiv g folosind Teorema 3.3.1. Presupunem că f este ireductibil în $K_1[X]$ şi $\phi : K_1 \to K_2$ este un izomorfism care transformă pe f în g, adică $\phi(\alpha_i) = \beta_i$, $i = 0, 1, \ldots, n$.

Atunci g este ireductibil în $K_2[X]$, şi izomorfismul ϕ se prelungeşte unic la izomorfismul

$$\bar{\phi} : K_1(a_1) \to K_2(a_2),$$

astfel ca $\bar{\phi}(a_1) = a_2$, unde $a_1 = X + (f)$ şi $a_2 = X + (g)$.

$$\begin{tikzcd} K_1[X] \arrow[r, "\phi'"] \arrow[d, "p_1"'] & K_2[X] \arrow[d, "p_2"] \\ K_1(a_1) \arrow[r, dotted, "\bar{\phi}"'] & K_2(a_2) \end{tikzcd}$$

Demonstraţie. Din proprietatea de universalitate a inelului de polinoame rezultă că a ϕ se prelungeşte unic la izomorfismul $\phi' := \bar{\Phi}_X : K_1[X] \to K_2[X]$, astfel ca

$$\phi'(\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n) = \phi(\alpha_0) + \phi(\alpha_1)X + \cdots + \phi(\alpha_n)X^n,$$

de unde rezultă că $\phi'(f) = g$. Deci, g este ireductibil în $K_2[X]$. Am văzut că $K_1(a_1) = K_1[X]/(f)$ şi $K_2(a_2) = K_2[X]/(g)$. Dacă $p_i : K_i[X] \to K_i(a_i)$, $i = 1, 2$ sunt morfismele canonice, atunci $p_2 \circ \phi'$ este morfism surjectiv.

Deoarece $\phi'(f) = g$, rezultă că izomorfismul φ' duce idealul (f) în idealul (g), şi de aici rezultă că $\operatorname{Ker}(p_2 \circ \phi') = (f) = \operatorname{Ker} p_1$. Deci, există un izomorfism $\bar{\phi} : K_1(a_1) \to K_2(a_2)$ astfel ca diagrama de mai sus este comutativă. Rezultă că $\bar{\phi}$ este dat astfel:

$$\bar{\phi}(\alpha_0 + \alpha_1 a_1 + \cdots + \alpha_{n-1} a_1^{n-1}) = \phi(\alpha_0) + \phi(\alpha_1)a_2 + \cdots + \phi(\alpha_{n-1})a_2^{n-1}$$

unde $\alpha_i \in K$, $i = 0, 1, \ldots, n-1$, ceea ce arată că $\bar{\phi}$ este unic. □

3.3.2 Corpul de descompunere

Teorema 3.3.4. *Dacă $f \in K[X]$ şi $\deg f = n \geq 1$, atunci există o extindere F/K astfel ca:*

1. *f se descompune în a $F[X]$ astfel: $f = a(X - x_1)\ldots(X - x_n)$, unde a este coeficientul lui X^n în f şi $x_1, \ldots, x_n \in F$ nu sunt neapărat distincte;*

2. $F = K(x_1, \ldots, x_n)$.

Demonstraţie. folosim inducţie după n. Dacă $n = 1$ atunci este evident că $F = K$. Presupunem că $n > 1$ şi că a teorema este adevărată pentru orice corp K, şi pentru orice polinom de grad $(n-1)$ din $K[X]$.

Deoarece $K[X]$ este inel factorial, rezultă că f are un factor ireductibil g în $K[X]$. Deci, $g \notin K$, şi din Teoreme 3.1. rezultă că există o extindere $K_1 = K(x_1)$ a lui K astfel încât x_1 este rădăcină a lui g.

Deci, în $K_1[X]$ $f = (X - x_1)h$, unde $\deg h = n - 1$. Se aplică ipoteza inducţiei pentru $h \in K_1[X]$, de unde primim pe F. □

Următoare teoremă spune că există un unic corp care satisface condiţiile anterioare.

Teorema 3.3.5. *Fie K şi K' corpuri izomorfe, care satisfac ipotezele teoremei 3.3.4. Fie $\varphi : K \to K'$ un izomorfism care transformă pe f în g (adică $\varphi'(f) = g$, unde $\varphi' : K[X] \to K'[X]$ este izomorfism, $\varphi'(a) = \varphi(a)$, pentru orice $a \in K$ şi $\varphi'(X) = X$), atunci φ se prelungeşte la izomorfismul $\bar{\varphi} : F \to F'$.*

Demonstraţie. Demonstraţia este prin inducţie după $r = [F : K]$. Dacă $r = 1$, atunci $F = K$ şi $F' = L$. Deci în acest caz $\bar{\varphi} = \varphi$.

Dacă $r > 1$ şi teorema este adevărată pentru orice extindere a lui K care satisface ipotezele Teoremei 3.3.4. şi care are grad peste K mai mic decât r. Deoarece $r > 1$, rezultă că f are un divizor ireductibil $u \in K[X]$, cu $\deg u = m > 1$. Atunci $v := \varphi(u)$ este divizor ireductibil al lui g în $K'[X]$. Polinomul u are în F o rădăcină x_1 şi v are în F' o rădăcină x_1'. Deoarece $m > 1$ şi u şi v sunt ireductibile, rezultă că $x_1 \notin K$ şi $x_1' \notin K'$; din Teorema 3.3.3. rezultă că φ se prelungeşte la izomorfismul $\varphi_1 : K(x_1) \to K'(x_1')$. Din Teoremele 3.1.2. şi 3.2.7. rezultă că

$$[F : K] = [F : K(x_1)] \cdot m,$$

ceea ce arată că $[F : K(x_1)] < r$. Din ipoteza inducţiei rezultă că φ_1 se prelungeşte la izomorfismul $\bar{\varphi} : F \to F'$. □

Definiţia 3.3.6. Fie K un corp şi fie $f \in K[X]$, $\deg f = n \geq 1$. Corpul F unic determinat până la un izomorfism de Teoremele 3.3.4. şi 3.3.5. se numeşte *corpul de descompunere* al polinomului f peste K. Notaţie: $F = F_{f,K}$.

Observaţii 3.3.7. 1) Corpul de descompunere al lui $f \in K[X]$ (peste K) depinde de f şi de K. De exemplu, corpul de descompunere al lui $X^2+1 \in \mathbb{R}[X]$ este $\mathbb{C}$, iar al lui $X^2+1 \in \mathbb{Q}[X]$ este $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\}$.

2) Fie $f = \alpha_0 X^n + \alpha_1 X^{n-1} + \cdots + \alpha_{n-1}X + \alpha_n \in K[X]$, $\deg f = n > 0$ şi fie $x_1,\ldots,x_n$ rădăcinile lui f. Dacă $u = g/h \in K(X_1,\ldots,X_n)$ este fracţie raţională simetrică şi $h(x_1,\ldots,x_n) \neq 0$, atunci $u(x_1,\ldots,x_n) \in K$.

Într-adevăr, din teorema fundamentală a polinoamelor simetrice rezultă că u se scrie sub forma

$$u = g'(s_1,\ldots,s_n)/h'(s_1,\ldots,s_n),$$

unde $g',h' \in K[Y_1,\ldots,Y_n]$ şi $s_1,\ldots,s_n$ sunt polinoamele simetrice elementare în n nedeterminate. Din formulele lui Viéte rezultă că

$$s_i(x_1,\ldots,x_n) = (-1)^i \alpha_i/\alpha_0 \in K,$$

pentru orice $i = 1,\ldots,n$.

3) Dacă F este corp de descompunere al polinomului $f \in K[X]$, atunci din 3.2.8. 7) rezultă că extinderea $K \leq F$ este algebrică.

Exerciţiul 3.16. Să se determine corpul de descompunere peste $\mathbb{Q}$ pentru următoarele polinoame, unde $f \in \mathbb{Q}[X]$, $F = F_{f,\mathbb{Q}}$. Să se determine gradul extinderii $F/\mathbb{Q}$ şi o bază.

a) $f = X^3 - 3$; b) $f = X^4 + 1$; c) $f = X^4 + X^2 + 1$;
d) $f = X^4 - X^2 - 2$; e) $f = (X^2-6)(X^2+2)$; f) $f = X^4 + 9$.

Exerciţiul 3.17. Să se determine corpul de descompunere al lui $f = X^4 + X^3 + X + \hat{1}$ peste $\mathbb{Z}_2$.

Exerciţiul 3.18. Fie $L = K(a,b)$, $f = m_{K,a}$, $g = m_{K,b}$, $\deg f = m$, şi $\deg g = n$. Presupunem că $(m,n) = 1$. Să se arate că:

a) $[L:K] = mn$;

b) g este ireductibil peste $K(a)$ (deci $m_{K(a),b} = g$).

Exerciţiul 3.19. Fie u şi v numere naturale. Să se arate că $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{v})$ dacă şi numai dacă uv este pătrat perfect.

3.3.3 Rădăcini ale unităţii şi polinoame ciclotomice

În această secţiune discutăm factorii ireductibili ai polinomului $X^n - 1 \in \mathbb{Z}[X]$, precum şi proprietıaţile corpului de descompunere al acestui polinom.

Dacă $n \in \mathbb{N}^*$, atunci rădăcinile polinomului $X^n - 1$ sunt

$$\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n) = \varepsilon_1^k,$$

unde $k \in \{0, \ldots, n-1\}$; numerele complexe ε_k se numesc *rădăcini de ordin n ale unităţii*. Ştim că

$$\mathrm{U}_n = \{\varepsilon_k \mid k \in \{0, \ldots, n-1\}\} = \langle \varepsilon_1 \rangle \simeq (\mathbb{Z}_n, +)$$

este *grup ciclic de ordin n*, şi $\varepsilon_k = \varepsilon_1^k$ generează pe U_n dacă şi numai dacă $(n,k) = 1$; în acest caz spunem că ε_k este *rădăcină primitivă de ordin n a unităţii*. Vom nota $\varepsilon = \varepsilon_1$.

Polinomul

$$\Phi_n = \prod_{0 \le k < n, (k,n)=1} (X - \varepsilon_k)$$

se numeşte al n-lea *polinom ciclotomic*. Vedem că $\deg(\Phi_n) = \varphi(n)$, unde $\varphi(n)$ este numărul lui Euler. Fie P_m mulţimea rădăcinilor primitive de ordin m ale unităţii; atunci $\mathrm{U}_n = \bigcup_{m|n} P_m$ este o partiţie a lui U_n; rezultă că $n = \sum_{d|n, d>0} \varphi(d)$ şi

$$X^n - 1 = \prod_{0 \le k < n} (X - \varepsilon_k) = \prod_{m|n} \Phi_m.$$

Lema 3.3.8. 1) $\Phi_n \in \mathbb{Z}[X]$ *şi* $\Phi_n | (X^n - 1)$ *în* $\mathbb{Z}[X]$.

2) *Dacă* $m|n$, *atunci* $(X^m - 1) | (X^n - 1)$ *în* $\mathbb{Z}[X]$.

3) *Dacă* $m|n$ *şi* $1 \le m < n$, *atunci* $\Phi_n | ((X^n - 1)/(X^m - 1))$.

4) *Pentru orice număr prim* p, $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$.

5) Φ_n *este ireductibil în* $\mathbb{Z}[X]$.

6) *Dacă* $q \in \mathbb{N}$ *şi* $q \ge 2$, *atunci* $\Phi_n(q) \nmid (q-1)$.

Demonstraţie. 1) Folosim inducţie după n. Pentru $n = 1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Presupunem că afirmaţia este adevărată pentru Φ_m, unde $m < n$. Atunci $X^n - 1 = f\Phi_n$, unde $f \in \mathbb{Z}[X]$ şi coeficientul principal al lui f este 1, deci $\Phi_n \in \mathbb{Z}[X]$.

2) Dacă $m \mid n$, atunci orice rădăcină a polinomului $X^m - 1$ este c si rădăcină a lui $X^n - 1 = 0$.

5) Fie aici ε o rădăcină primitivă de ordin n a unităţii aleasă arbitrar, şi fie $f = m_{\mathbb{Q},\varepsilon}$ polinomul său minimal. Deoarece $\Phi_n(\varepsilon) = 0$ rezultă că $\Phi_n = fg$ unde $f, g \in \mathbb{Q}[X]$. Din Lema lui Gauss rezultă că $f, g \in \mathbb{Z}[X]$.

Fie p un număr prim, astfel ca $(p,n) = 1$. Atunci ε^p este de asemenea rădăcină primitivă de ordin n a unităţii, adică ε^p are ordin n în grupul $(\mathrm{U}_n, \cdot)$. Atunci $\Phi_n(\varepsilon^p) = 0$, deci $f(\varepsilon^p) = 0$ sau $g(\varepsilon^p) = 0$. Presupunem prin absurd că $f(\varepsilon^p) \neq 0$. Atunci $g(\varepsilon^p) = 0$.

Fie $h = g(X^p) \in \mathbb{Z}[X]$. Atunci ε este rădăcină a lui h, deoarece $h(\varepsilon) = g(\varepsilon^p) = 0$. Atunci $f = m_{\mathbb{Q},\varepsilon} \mid h$, şi din Lema lui Gauss avem $h = fq$, unde $q \in \mathbb{Z}[X]$. Considerăm morfismul de inele

$$\mathbb{Z}[X] \to \mathbb{Z}_p[X], \qquad f = a_0 + a_1X + \cdots + a_nX^n \longmapsto \overline{f} = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_mX^m.$$

Atunci $\overline{h} = \overline{f} \cdot \overline{q}$, dar $\overline{h} = \overline{g}(X^p) = \overline{g}^p$, deoarece conform teoremei lui Fermat, $\bar{a}^p = \bar{a}$ în $\mathbb{Z}_p$, deci $\overline{g}^p = \overline{f} \cdot \overline{g}$.

Dacă $\psi \in \mathbb{Z}_p[X]$ este un factor ireductibil al lui f, atunci $\psi \mid \overline{g}^p$, şi deoarece ψ este element prim în $\mathbb{Z}_p[X]$, obţinem $\psi \mid \bar{g}$. Deoarece $\bar{\Phi}_n = \bar{f}\bar{g}$, rezultă că $\psi^2 \mid \Phi_n$, şi atunci ψ este rădăcină dublă alui Φ_n. Dar aceasta este contradicţie, deoarece Φ_n are doar rădăcini simple. Rezultă că $f(\varepsilon^p) = 0$ pentru orice p număr prim. Deci în cazul $(p,n) = 1$, ε^p este rădăcină a lui f.

Fie ξ o rădăcină a lui Φ_n, adică ξ este rădăcină primitivă de ordin n a unităţii, deci există $m \in \{1, \ldots, n\}$ astfel ca $(m,n) = 1$ şi $\xi = \varepsilon^m$. Fie $m = p_1p_2 \ldots p_s$, unde p_i sunt numere prime, $(p_i, n) = 1$ pentru orice $1 \leq i \leq s$, deci avem $f(\varepsilon^{p_i}) = 0$. Deci $\Phi_n(\varepsilon^{p_i}) = 0$. Luăm în locul ε pe ε^{p_1}; prin inducţie după i obţinem $f((\varepsilon^{p_1})^{p_2}) = f(\varepsilon^{p_1p_2}) = 0$, deci $\Phi(\varepsilon^{p_1p_2}) = 0$.

Rezultă că $f(\xi) = f(\varepsilon^{p_1 \cdots p_s}) = 0$. Deoarece pentru orice rădăcină primitivă de ordin n a unităţii ξ acest lucru are loc, rezultă că orice rădăcină a lui Φ_n este şi rădăcină a lui f, deci $\Phi_n = f = m_{\mathbb{Q},\varepsilon}$ este ireductibil peste $\mathbb{Q}$.

6) Reprezentând numerele 1 şi ε în planul complex, observăm imediat că $|q - \varepsilon| > (q-1)$ pentru orice $\varepsilon \in P_n$, $\varepsilon \neq 1$. $\square$

Definiţia 3.3.9. *Corpul de descompunere $\mathbb{Q}(\varepsilon)$ al polinomului $X^n - 1 \in \mathbb{Q}[X]$ se numeşte al n-lea corp ciclotomic. Ştim că pentru orice $n \in \mathbb{N}$, $n \geq 1$, avem $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \varphi(n) = \deg(\Phi_n)$.*

Teorema 3.3.10. *Grupul* $\mathrm{Aut}(\mathbb{Q}(\varepsilon))$ *este izomorf cu* $\mathrm{U}(\mathbb{Z}_n)$ (acesta este grupul lui Galois, deci cu notaţia ce va fi introdusă în capitolul următor, avem $G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \simeq \mathrm{U}(\mathbb{Z}_n)$).

Demonstraţie. Grupul Galois $G = \mathrm{Aut}(\mathbb{Q}(\varepsilon))$ constă din automorfismele σ_k care au proprietatea

$$\sigma_k(\varepsilon) = \varepsilon_1^k = \varepsilon_k, \qquad (k,n) = 1,$$

deoarece ε_k trebuie să fie de asemenea rădăcină primitivă de ordin n a unităţii, deci avem

$$G = G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = \{\sigma_k \mid (k,n) = 1\}$$

Numărul acestor automorfisme este $\varphi(n)$, adică este ordinul grupului $\mathrm{U}(\mathbb{Z}_n)$. Definim o funcţie între grupurile G şi $(\mathrm{U}(\mathbb{Z}_n), \cdot)$ astfel ca lui $\sigma_k \in G$ îi corespunde $\hat{k} \in \mathrm{U}(\mathbb{Z}_n)$. Se observă uşor că această funcţie este bine definită şi este izomorfism de grupuri. □

Exerciţiul 3.20. Să se calculeze Φ_n, dacă $n = 1,2,3,4,5,6$, respectiv dacă $n = p$ este număr prim.

Exerciţiul 3.21. a) Să se arate că

$$\Phi_{p^n} = \Phi_p(X^{p^{n-1}}), \;\; \Phi_{p^n q^m} = \Phi_{pq}(X^{p^{n-1}q^{m-1}}), \;\; \Phi_{p^n q^m r^l} = \Phi_{pqr}(X^{p^{n-1}q^{m-1}r^{l-1}}).$$

b) Să se calculeze Φ_n, dacă $n = 8,9,10,12,72,180$.

Exerciţiul 3.22. Să se arate că pentru orice $q \in \mathbb{Q}$ există o rădăcină ε a unităţii pentru care $\sqrt{q} \in \mathbb{Q}(\varepsilon)$.

3.4 Corpuri finite

În acest paragraf demonstră celebra teoremă a lui Wedderburn, care spune că orice corp finit este comutativ, şi determinăm structura corpurilor finite.

Teorema 3.4.1. *Dacă K este un corp finit, atunci există un număr prim p şi există $n \in \mathbb{N}^*$ astfel încât $|K| = p^n$.*

Demonstraţie. Deoarece K este finit, rezultă că $\mathrm{char}\, K = p$ este număr prim, şi fie $L = P(K) \simeq \mathbb{Z}_p$ subcorpul prim al lui K. Atunci K este L-spaţiu vectorial, deci are o bază finită. Dacă $\dim_L K = n$, atunci $K \simeq L^n$, deci $|K| = |L|^n = p^n$. □

Teorema 3.4.2 (Wedderburn)**.** *Dacă K este corp finit, atunci K este comutativ.*

Demonstraţie. Fie $Z = Z(K) = \{a \in K \mid ax = xa, \forall x \in K\}$ centrul corpului K; este suficient de demonstrat că $Z = K$. Ştim că Z este subcorp al lui K, şi dacă $x \in K$, atunci $C_K(x) = \{a \in K \mid ax = xa\}$ este subcorp al lui K; rezultă că K şi $C_K(x)$ sunt spaţii vectoriale finit dimensionale peste Z. Dacă $|Z| = q$, atunci $|K| = q^n$ şi $|C_K(x)| = q^{n_x}$, unde $n = \dim_Z K$ şi $n_x = \dim_Z C_K(x)$. Mai departe, $|K^*| = q^n - 1$, $Z(K^*) = Z^*$ şi $|C_K(x)^*| = g^{n_x} - 1$, unde $C_K(x)^* = C_{K^*}(x)$ pentru orice $x \in K^*$.

Scriem ecuaţia pentru clasele de conjugare ale grupului $(K^*, \cdot)$:

$$|K^*| = |Z^*| + \sum_{x \in A} [K^* : C_K(x)^*]$$

unde A este sisteme de reprezentanţi pentru clasele netriviale; rezultă că

$$q^n - 1 = q - 1 + \sum_{x \in A} (q^n - 1)/(q^{n_x} - 1),$$

unde $n_x \mid n$ şi $n_x \neq n$ dacă $x \in A$. Din Lema 3.3.8. rezultă că $\Phi_n(q) | (q^n - 1)$ şi $\Phi_n(q) | (q^n - 1)/(q^{n_x} - 1)$, contradicţie, deoarece $\Phi_n(q) \nmid (q - 1)$. $\square$

Teorema 3.4.3 (subgrupurile multiplicative ale unui corp comutativ)**.** *Fie K un corp comutativ şi fie $G \leq (K^*, \cdot)$ un subgrup finit. Atunci $(G, \cdot)$ este grup ciclic.*

În particular, dacă K este corp finit, atunci K^* este grup ciclic.

Exemplul 3.4.4. a) Să determinăm subgrupurile finite ale lui $(\mathbb{R}^*, \cdot)$. Dacă $G \leq \mathbb{R}^*$ este de ordin n, atunci pentru orice $x \in G$ avem $x^n = 1$, deci $x = 1$ sau $x = -1$, deci $G = \{1\}$ sau $G = \{-1, 1\}$.

b) Dacă G este subgrup de ordin n al lui $(\mathbb{C}^*, \cdot)$, atunci

$$G = \mathrm{U}_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k \in \mathbb{Z}, k = \{0, 1, 2, \ldots, n-1\} \right\}.$$

c) Fie

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

corpul (necomutativ) al cuaternionilor, unde

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,\ i^2 = j^2 = k^2 = ijk = -1$$

Atunci grupul cuaternionilor $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \leq (\mathbb{H}^*, \cdot)$ nu e ciclic şi nu e comutativ.

d) Considerăm câteva cazuri particulare:

$m = 2 \qquad U(\mathbb{Z}_2) = \{\hat{1}\} = \langle \hat{1} \rangle$
$m = 3 \qquad U(\mathbb{Z}_3) = \{\hat{1}, \hat{2}\} = \langle \hat{2} \rangle$
$m = 4 \qquad U(\mathbb{Z}_4) = \{\hat{1}, \hat{3}\} = \langle \hat{3} \rangle$
$m = 5 \qquad U(\mathbb{Z}_5) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\} = \langle \hat{2} \rangle$
$m = 6 \qquad U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$
$m = 7 \qquad U(\mathbb{Z}_7) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\} = \langle \hat{3} \rangle$

Pentru demonstraţia Teoremei 3.4.3. avem nevoie de următoarea:

Lema 3.4.5. *Fie $(G, \cdot)$ un grup.*

a) *Dacă $x,\ y \in G,\ xy = yx,$ $\operatorname{ord}(x) = m,$ $\operatorname{ord}(y) = n$ şi $(m, n) = 1,$ atunci $\operatorname{ord}(xy) = mn.$*

b) *Dacă $x_1,\ x_2,\ \ldots,\ x_r \in G$ astfel încât $x_i x_j = x_j x_i,\ 1 \leq i, j \leq r,$ $\operatorname{ord}(x_i) = m_i \in \mathbb{N}^*$ şi $(m_i, m_j) = 1,\ i \neq j,$ atunci $\operatorname{ord}(x_1 x_2 \ldots x_n) = m_1 m_2 \cdots m_r.$*

Demonstraţia Teoremei 3.4.3. Fie $|G| = p_1^{m_1} \ldots p_r^{m_r}$, unde $r \geq 2,\ p_1,\ p_2,\ \ldots,\ p_r$ numere prime, $n_i \geq 1$. Arătăm că există $x \in G$, astfel încât $\operatorname{ord}(x) = n$.

Polinomul $X^{\frac{n}{p_i}} - 1 \in K[X]$ are cel mult n/p_i rădăcini în K, pentru orice $i = 1, \ldots, r$. Deoarece $n > \frac{n}{p_i}$, există $g_i \in G$ astfel încât $g_i^{\frac{n}{p_i}} \neq 1$. Fie $x_i = g_i^{n/p_i^{m_i}} \in G$ şi arătăm că $\operatorname{ord}(x_i) = p_i^{m_i}$. Într-adevăr,

$$(x_i)^{p_i^{m_i}} = (g_i^{\frac{n}{p_i^{m_i}}})^{p_i^{m_i}} = g_i^n = 1,$$

deoarece $|G| = n$ şi $\operatorname{ord}(g_i) \mid |G|$ conform Teoremei lui Lagrange. Deci $\operatorname{ord}(x_i) \mid p_i^{m_i}$, de unde $\operatorname{ord}(x_i) = p_i^m$, unde $m \leq m_i$. Presupunem că $m < m_i$,

$$1 = (x_i)^{p_i^{m_i}} = (g_i^{n/p_i})^{p_i^m} = g_i^{n/p_i^{m_i - m}},$$

deci $g_i^{n/p_i} = 1$, ceea ce contrazice alegerea lui g_i.

Fie $x = x_1 \cdots x_r \in G$. Deoarece G este comutativ, putem aplica lema anterioară. Deoarece $\operatorname{ord}(x_i) = p_i^{m_i}$ şi $(p_i, p_j) = 1$ dacă $i \neq j$, din Lema 3.4.5. b) rezultă că $\operatorname{ord}(x) = p_1^{m_1} \ldots p_r^{m_r} = n$. Deci $G = \langle x \rangle$ este ciclic. $\square$

Teorema 3.4.6 (existenţa şi unicitatea corpurilor finite)**.** 1) *Două corpuri finite cu acelaşi număr de elemente sunt izomorfe.*

2) *Pentru orice număr prim p şi pentru orice $n \in \mathbb{N}^*$, există un corp cu p^n elemente, notat $\mathbb{F}_{p^n}$, care este corpul de descompunere al polinomului $X^{p^n} - X \in \mathbb{Z}_p[X]$ peste $\mathbb{Z}_p$.*

Demonstraţie. 1) Fie $q := p^n$, $K = \{a_1 = 0, a_2, \ldots, a_q\}$ şi $K^* = K \setminus \{0\}$.

Ordinul elementului $a_i \in K^*$ în grupul $(K^*, \cdot)$ divide pe $|K^*| = q - 1$, de unde rezultă că $a_i^{q-1} - a_i = 1$, pentru orice $a_i \in K^*$; rezultă că $a_i^q - a_i = 0$, pentru orice $a_i \in K$. Deci orice element al lui K este rădăcină a polinomului $f := X^q - X \in \mathbb{Z}_p[X]$, şi f nu are alte rădăcini în corp de descompunere peste $\mathbb{Z}_p$. Rezultă că K este corpul de descompunere al lui f peste $\mathbb{Z}_p$.

Dacă L aste un alt cu $q = p^n$ elemente, atunci $P(L) \simeq \mathbb{Z}_p$, L este corpul de descompunere peste $P(L)$ al lui $g = X^q - X \in P(L)[X]$. Deci din Teorema 3.3.5. rezultă că $K \simeq L$.

2) Derivata formală a polinomului $f = X^q - X \in \mathbb{Z}_p[X]$ este $f' = qX^{q-1} - 1 = -1$, ceea ce arată că f are q rădăcini distincte în corpul de descompunere $F = F_{f,\mathbb{Z}_p}$. Funcţia

$$\psi : F \to F, \qquad \psi(a) = a^q$$

este automorfism de corpuri, deoarece ψ este puterea a n-a a *automorfismului Frobenius*. Rădăcinile polinomului f sunt chiar punctele fixe ale lui ψ. Deci rădăcinile lui f formează un subcorp cu q elemente $F_0 \leq F$; rezultă că $F_0 = F_{f,\mathbb{Z}_p}$, deci $|F| = p^n$. $\square$

Observaţii 3.4.7. a) Din teorema de mai sus rezultă că pentru orice număr prim p există, abstracţie făcând de un izomorfism, un unic corp cu p^n elemente, notat $\mathbb{F}_{p^n}$. Teoremele 3.4.6. şi 3.4.1. spun că orice corp finit este izomorf cu un corp de forma $\mathbb{F}_{p^n}$.

b) Dacă $K \leq L$ este o extindere de corpuri finite, atunci există $a \in L$ astfel ca $L = K(a)$, adică în L există element primitiv. Într-adevăr, $(L^*, \cdot)$ este grup ciclic. Dacă a generează acest grup, atunci $L = K(a)$.

Teorema 3.4.8 (subcorpurile unui corp finit)**.** *Fie K un corp finit, unde $|K| = p^n$.*

1) *Cardinalul unui suncorp al lui K este de forma p^m, unde $m \mid n$.*

2) *Dacă $m \in \mathbb{N}^*$ şi $m \mid n$, atunci K are un unic subcorp cu p^m elemente.*

Demonstraţie. 1) Dacă $L \leq K$, atunci subcorpul prim al lui L este $\mathbb{Z}_p$. Deci din Teorema 3.4.1.avem $|L| = p^m$, unde $m = [L : \mathbb{Z}_p]$. Deoarece $\mathbb{Z}_p \leq L \leq K$, rezultă că $n = m[K : L]$.

2) Fie $q := p^m$. Am văzut mai sus că rădăcinile din K ale polinomului $f := X^q - X \in \mathbb{Z}_p[X]$ sunt punctele fixe ale puterii a m-a ale automorfismului Frobenius $\varphi : K \to K$, $\varphi(x) = x^p$. Deci aceste rădăcini formează un subcorp L al lui K şi avem $|L| \leq q$.

Fie $k := n/m$. Atunci $|K| = q^k$ şi $|K^*| = q^k - 1$, unde $K^* = K \setminus \{0\}$. Deoarece $(K^*, \cdot)$ este grup ciclic, rezultă că K^* are un generator a. Dacă $s := (q^k - 1)/(q - 1)$, atunci $\mathrm{ord}(a^s) = q - 1$ în grupul $(K^*, \cdot)$; rezultă că

$$0, a^s, a^{2s}, \ldots, a^{(q-1)s} \tag{3.1}$$

sunt q elemente distincte şi $(a^{is})^{(q-1)} = 1$, $i = 1, \ldots, q-1$, de unde rezultă că $(a^{is})^q = a^{is}$, $i = 0, 1, \ldots, q-1)$. Deci, elemente din lista (3.1) sunt rădăcinile lui f, adică aparţin lui L. Rezultă că $|L| \geq q$, deci $|L| = q$.

În fine, arătăm că L este unicul subcorp cu q elemente al lui K. Într-adevăr dacă L' este subcorp cu q elemente al lui K, atunci L^* este grup cu $q - 1$ element, deci $x^{q-1} = 1$, pentru orice $x \in L'^*$. De aici rezultă că elementele lui L' sunt rădăcinile polinomului f. Deci, L' constă din elemente din lista (3.1), adică $L' = L$. □

Exerciţiul 3.23. Să se determine elementele generatoare ale lui $\mathbb{Z}_{13}^*$.

Exerciţiul 3.24. Să se determine elementele generatoare ale lui $\mathbb{Z}_{17}^*$.

Exerciţiul 3.25. Să se construiască corpul cu 4 elemente $\mathbb{F}_4$.

Exerciţiul 3.26. Să se construiască corpul $\mathbb{F}_8$.

Exerciţiul 3.27. Să se determine elementele generatoare ale lui $\mathbb{F}_8^*$.

Exerciţiul 3.28. Să se construiască corpul cu 9 elemente.

Exerciţiul 3.29. Să se determine elementele generatoare ale lui $\mathbb{F}_9^*$.

Exerciţiul 3.30. Fie $f = X^4 + \hat{1} \in \mathbb{Z}_3[X]$. Să se determine rădăcinile lui f.

Exerciţiul 3.31. Să se determine elementele generatoare ale lui $\mathbb{F}_{16}^*$.

Exerciţiul 3.32. Să se determine subcorpurile lui $\mathbb{F}_{16}$.

3.5 Corpuri algebric închise. Închiderea algebrică a unui corp

Definiţia 3.5.1. a) Un corp comutativ K se numeşte *algebric închis*, dacă pentru orice $f \in K[X]$, $f \neq 0$, rădăcinile lui f sunt în K, adică corpul de descompunere al polinomului f peste K coincide cu K.

b) Fie L/K o extindere de corpuri. Spunem că K este *algebric închis în* L, dacă pentru orice $f \in K[X]$, $f \neq 0$, rădăcinile lui f din L sunt în K.

Observaţii 3.5.2. 1) Dacă $K \leq L$, atunci K este algebric închis în L, dacă şi numai dacă elementele din L algebrice peste K sunt în K.

2) Dacă K este un corp, atunci următoarele afirmaţii sunt echivalente:

1. K este algebric închis;
2. orice extindere algebrică a lui K coincide cu K;
3. K este algebric închis în orice extindere L;
4. Dacă $f \in K[X]$ şi $\deg f \geq 1$, atunci f are o rădăcină în K;
5. Polinoamele ireductibile din $K[X]$ sunt polinoamele de grad 1.

3) Corpurile finit nu sunt algebric închise.

Într-adevăr dacă $K = \{a_1, \ldots, a_n\}$ atunci polinomul $f = 1 + (X - a_1) \ldots (X - a_n) \in K[X]$ nu are rădăcini în K.

Teorema următoare se mai numeşte *teorema fundamentală a algebri clasice*.

Teorema 3.5.3 (Gauss–d'Alembert)**.** *Corpul $\mathbb{C}$ al numerelor complexe este algebric închis.*

Demonstraţie. Cazul 1. Presupunem că $f \in \mathbb{R}[X]$, şi fie $\deg(f) = n = 2^k m$, unde $2 \nmid m$. Atunci arătăm inducţie după k că f are cel puţin o în rădăcină $\mathbb{C}$.

Dacă $k = 0$, atunci $\deg(f)$ număr impar, şi $\lim_{x\to\infty} f(x) = -\lim_{x\to-\infty} f(x)$; dar f este funcţie continuă, deci există $x \in \mathbb{R}$ astfel încât $f(x) = 0$.

Fie $k > 0$, şi presupunem că afirmaţia este adevărat pentru $k - 1$. Există o extindere $\mathbb{C} \leq L$ de corpuri astfel încât $f = a_n(X - x_1) \ldots (X - x_n)$, unde $x_i \in L$ pentru orice $i \in \{1, \ldots, n\}$.

Dacă $\alpha \in \mathbb{R}$, fie $z_{ij}^{\alpha} = x_i x_j + \alpha(x_i + x_j)$, unde $1 \leq i < j \leq n$, şi fie

$$g = \prod_{1 \leq i < j \leq n} (X - z_{ij}^{\alpha}) \in L[X].$$

Dacă $\sigma \in S_n$, $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ este funcţie bijectivă, atunci σ induce o funcţie bijectivă $\sigma' : \{(i, j) \mid i < j\} \to \{(i, j) \mid i < j\}$, $\sigma'(i, j) = \sigma(i)\sigma(j)$; rezultă că coeficienţii lui g sunt simetrici în $x_1, \ldots, x_n$, deci $g \in \mathbb{R}[X]$. Deoarece

$$\deg(g) = C_n^2 = n(n-1)/2 = 2^k m(2^k m - 1)/2 = 2^{k-1} m(2^k m - 1),$$

din ipoteza inducţiei rezultă că g are rădăcină în $\mathbb{C}$.

Am arătat, că pentru orice $\alpha \in \mathbb{R}$ există (i_α, j_α) astfel încât $z_{i_\alpha j_\alpha}^{\alpha} \in \mathbb{C}$. Deoarece $\mathbb{R}$ este mulţime infinită, rezultă că există $\alpha \neq \beta$ şi (i, j) astfel încât z_{ij}^{α}, $z_{ij}^{\beta} \in \mathbb{C}$; atunci $x_i x_j + \alpha(x_i + x_j) \in \mathbb{C}$ şi $x_i x_j + \beta(x_i + x_j) \in \mathbb{C}$, şi deoarece $\alpha \neq \beta$, rezultă că $x_i + x_j \in \mathbb{C}$ şi $x_i x_j \in \mathbb{C}$. Deoarece x_i, x_j sunt rădăcinile polinomului $X^2 - (x_i + x_j)X + x_i x_j \in \mathbb{C}[X]$, rezultă că $x_i, x_j \in \mathbb{C}$.

Cazul 2. Fie $f \in \mathbb{C}[X]$; deoarece $f\bar{f} \in \mathbb{R}[X]$, din cazul 1. rezultă că există $x \in \mathbb{C}$ astfel încât $f(x)\overline{f(x)} = 0$. Dacă $f(x) = 0$, atunci f are rădăcină complexă. Dacă $\bar{f}(x) = 0$, atunci $\overline{f(x)} = 0$, adică $f(\bar{x}) = 0$, deci f are rădăcină complexă. □

Teorema 3.5.4. *Fie $K \leq L$ şi fie $A = \{a \in L \mid a$ algebric peste $K\}$. Atunci:*

1) *A este algebric închis în L;*

2) *Dacă L este algebric închis, atunci şi A este algebric închis.*

Demonstraţie. 1) Într-adevăr, $K \leq A$ este extindere algebrică, şi dacă $b \in L$ este element algebric peste A, atunci din 3.2.8. 3), avem că $A \leq A(b)$ este extindere algebrică. Din Teorema 3.2.9. rezultă că a $K \leq A(b)$ extindere algebrică, de unde rezultă că b element algebric peste K, adică $b \in A$.

2) Dacă $f \in A[X]$, $f \neq 0$, atunci $f \in L[X]$, şi deoarece L este algebric închis, rezultă că rădăcinile lui f sunt în L. Deci, din 1) rezultă că rădăcinile lui f sunt în A, deci A este algebric închis. □

Corolar 3.5.5. *Corpul $\mathbb{A}$ al numerelor algebrice este algebric închis.*

Observaţii 3.5.6. $\mathbb{A}$ este mulţime numărabilă, adică $|\mathbb{A}| = \aleph_0$.

Definiţia 3.5.7. Corpul $\overline{K}$ se numeşte *închiderea algebrică* a corpului K, dacă $\overline{K}$ este algebric închis, şi $\overline{K}$ este extindere algebrică a lui K.

În cele ce urmează vom demonstra că orice corp are o închidere algebrică care este unică până la un izomorfism. Următoarea teoremă este folosită în demonstraţia unicităţii.

Teorema 3.5.8. *Dacă $K_1 \leq K_2$ este extindere algebrică şi K este corp algebric închis, atunci orice morfism nenul $\varphi : K_1 \to K$ se prelungeşte la un morfism $\overline{\varphi} : K_2 \to K$.*

Dacă $\varphi(K_1) \leq K$ este extindere algebrică şi K_2 este algebric închis, atunci orice morfism $\overline{\varphi} : K_2 \to K$ care prelungeşte pe φ este izomorfism.

Demonstraţie. Fie

$$\mathscr{M} := \{(L_1, \varphi') \mid K_1 \leq K_1' \leq K_2,\ \varphi' : K_1' \to K \text{ morfism},\ \varphi'_{|K_1} = \varphi\}.$$

Pe mulţimea $\mathscr{M}$ definim relaţia „$\leq$” astfel: $(K_1', \varphi') \leq (K_1'', \varphi'')$ dacă şi numai dacă $K_1' \subseteq K_1''$ şi $\varphi' = \varphi''_{|K_1'}$. Atunci „$\leq$” este relaţie de ordine. Mulţimea ordonată $\mathscr{M}, \leq)$ satisface ipotezele lemei lui Zorn. Deci, există un element maximal $(\overline{K}_1, \varphi) \in \mathscr{M}$. Arătăm că $\overline{K}_1 = K_2$.

Într-adevăr, dacă $\overline{K}_1 \neq K_2$, atunci există un element $b \in K_2 \setminus \overline{K}_1$, de unde rezultă că $\overline{K}_1 \subseteq \overline{K}_1(b)$. Dacă $f = \sum_{i=0}^{n} a_i X^i \in \overline{K}_1[X]$ este polinomul minimal al lui b şi $f' = \sum_{i=0}^{n} \overline{\varphi}(a_i) X^i$, respectiv b' este o rădăcină a lui f' în K, atunci din Teorema 3.3.3. rezultă că $\overline{\varphi}$ se prelungeşte la un morfism $\overline{\varphi'} : \overline{K}_1(b) \to \overline{\varphi}(\overline{K}_1)(b') \subseteq K$. Deci, $(\overline{K}_1, \overline{\varphi}) < (\overline{K}_1(b), \overline{\varphi'})$, ceea ce contrazice maximalitatea perechii $(\overline{K}_1, \overline{\varphi})$. Am arătat deci că $\overline{K}_1 = K_2$, adică φ se prelungeşte la un morfism $\overline{\varphi} : K_2 \longrightarrow K$.

Dacă $\varphi(K_1) \leq K$ este extindere algebrică şi $\overline{\varphi} : K_2 \to K$ este un morfism ce prelungeşte pe φ, atunci $\overline{\varphi}(K_2) \leq K$ este extindere algebrică, şi deoarece K_2 este algebric închis, şi $\overline{\varphi}(K_2)$ este algebric închis. Deci, $\overline{\varphi}(K_2) = K$, adică $\overline{\varphi}$ este izomorfism. □

Teorema 3.5.9. *Orice corp are o închidere algebrică unică până la un izomorfism.*

Demonstraţie. Existenţa. Fie $(K, +, \cdot)$ un corp şi M o mulţime care conţine pe K, nenumărabilă (adică $|M| > |\mathbb{N}|$) dacă K este finit, iar dacă K este infinit atunci $|M| > |K|$. Notăm prin $\mathscr{M}$ mulţimea corpurilor $(L, +, \cdot)$ care sunt extinderi algebrie ale lui K şi pentru care $L \subseteq M$. Pe mulţimea $\mathscr{M}$ definim relaţia „$\leq$”: $(L_1, +, \cdot) \leq (L_2, +, \cdot)$ dacă şi numai dacă $(L_2, +, \cdot)$ este extindere algebrică a lui $(L_1, +, \cdot)$. Atunci „$\leq$” relaţie de ordine, şi mulţimea ordonată $(\mathscr{M}, \leq)$ satisface ipotezele lemei lui Zorn. Deci, există un element maximal $(\overline{K}, +, \cdot) \in \mathscr{M}$.

Arătăm că $(\overline{K},+,\cdot)$ este algebric închis. Presupunem contrarul, adică, există o extindere algebrică $(L,+,\cdot)$ a lui $(\overline{K},+,\cdot)$, astfel ca $\overline{K} < L$. Din Teorema 3.2.9. rezultă că $(L,+,\cdot)$ este extindere algebrică a lui K; din alegerea lui M şi din Exerciţiul 3.14. rezultă că $|L| < |M|$. Deci există o funcţie injectivă $\alpha : L \to M$ astfel ca $\alpha(x) = x$ pentru orice $x \in \overline{K}$. Mulţimea $\alpha(L)$ devine corp cu următoarele operaţii: $\alpha(x_1) + \alpha(x_2) = \alpha(x_1 + x_2)$ şi $\alpha(x_1)\alpha(x_2) = \alpha(x_1x_2)$ (deci $\alpha(L)$ este izomorf cu corpul $(L,+,\cdot)$. Rezultă că $(\alpha(L),+,\cdot) \in \mathscr{M}$ şi $(\overline{K},+,\cdot) < (\alpha(L),+,\cdot)$, ceea ce contrazice maximalitatea lui $(\overline{K},+,\cdot)$.

Am arătat că $(\overline{K},+,\cdot)$ este algebric închis, dar deoarece $(\overline{K},+,\cdot)$ este extindere algebrică a lui K, rezultă că $(\overline{K},+,\cdot)$ este închiderea algebrică a lui $(K,+,\cdot)$.

Unicitatea. Dacă $\overline{K}$ şi L sunt închideri algebrice ale lui K, atunci din teorema anterioară rezultă că 1_K se prelungeşte la un izomorfism $\overline{K} \simeq L$. $\square$

Exemplul 3.5.10. 1) Închiderea algebrică a corpului $\mathbb{R}$ este $\mathbb{C}$, iar închiderea algebrică a lui $\mathbb{Q}$ este corpul $\mathbb{A}$ al numerelor algebrice.

2) Dacă $0 < m < n$, atunci $m! \mid n!$, şi avem următorul lanţ crescător:

$$\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \cdots$$

Fie

$$\mathbb{F}_{p^\infty} := \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^{n!}}.$$

Atunci $\mathbb{F}_{p^\infty}$ este un corp care conţine pe $\mathbb{F}_{p^n}$ ca subcorp pentru orice $n \in \mathbb{N}^*$. În corpul $\mathbb{F}_{p^\infty}$ orice element are ordin multiplicativ finit, $\mathbb{F}_{p^\infty}$ este infinit şi are caracteristica p. Se poate arăta că $\mathbb{F}_{p^\infty}$ este algebric închis, şi este închiderea algebrică a lui $\mathbb{F}_p$.

Exerciţiul 3.33. Să se arate că mulţimea ordonată $(\mathscr{M},\leq)$ din demonstraţia Teoremei 3.5.8. satisface ipotezele lemei lui Zorn.

Exerciţiul 3.34. Să se arate că mulţimea ordonată $(\mathscr{M},\leq)$ din demonstraţia Teoremei 3.5.9. satisface ipotezele lemei lui Zorn.

Teoria lui Galois | 4

Teoria lui Galois asociază unei extinderi de corpuri un grup, numit grupul Galois al extinderii. Teorema fundamentală acestei teorii stabileşte o conexiune între corpurile intermediare ale extinderii şi subgrupurile grupului Galois. Aceste subgrupuri sunt mai uşor de studiat, deorece sunt finite, în timp ce corpurile au de multe ori o infinitate de elemente.

4.1 Extinderi algebrice separabile

Fie K un comutativ corp.

Definiţia 4.1.1. a) Un polinom $f \in K[X]$ de grad n se numeşte *polinom separabil* (peste corpul K), dacă f are rădăcini n distincte în corpul său de descompunere.

b) $K \leq L$ este *extindere separabilă*, dacă orice element din L este rădăcină a unui polinom separabil peste Ki nak a e (adică polinomul său minimal este separabil).

Teorema 4.1.2. *$f \in K[X]$ este separabil peste K dacă şi numai dacă cel mai mare divizor comun al lui f şi f' este* 1.

Demonstraţie. Fie F corpul de descompunere al lui f; în $F[X]$ avem:

$$f = a(X - x_1)^{m_1} \dots (X - x_k)^{m_k},$$

unde a este coeficientul lui X^n în f (aici f este de grad n) şi $x_1, \dots, x_k$ sunt elemente distincte din F, iar $m_1, \dots, m_k$ sunt numere naturale. Rezultă că

$$\begin{aligned} f' = am_1(X - x_1)^{m_1 - 1}(X - x_2)^{m_2} \dots (X - x_k)^{m_k} + \dots \\ + am_k(X - x_1)_1^m \dots (X - x_{k-1})^{m_{k-1}}(X - x_k)^{m_k - 1} \end{aligned}$$

Rezultă că acel mai mare divizor comun d al polinoamelor f şi f' este produs de puteri ale ui $X - x_1, \dots, X - x_k$. Deci $d = 1$ dacă şi numai dacă dintre polinoamele

$X - x_1, \ldots, X - x_k$ niciunul nu îl divide pe f', şi aceasta are loc numai, dacă $m_1 = \cdots = m_k = 1$, adică f este separabil.

(Observăm, că cel mai mare divizor comun al polinoamelor f şi f' nu se schimbă când tercem de la $K[X]$ la $F[X]$, deoarece cel mai mare divizor comun se poate calcula cu algoritmul lui Euclid.) □

Corolar 4.1.3. a) *Fie $f \in K[X]$ un polinom ireductibil. Atunci f este separabil dacă şi numai dacă $f' \neq 0$.*

b) *Dacă* $\operatorname{char} K = 0$ *şi $f \in K[X]$ este polinom ireductibil, atunci f este separabil.*

c) *Fie* $\operatorname{char} K = p$ *un număr prim. Polinomul ireductibil $f \in K[X]$ are rădăcini multiple dacă şi numai dacă $f \in K[X^p]$.*

Demonstraţie. a) Deoarece $\deg f' < \deg f$ şi deoarece f este ireductibil, rezultă că dacă $f' \neq 0$, atunci cel mai mare divizor comun d al lui f şi f' este 1, de unde rezultă că f este separabil.

Dacă $f' = 0$, atunci $d = f \notin k$, ceea ce spune că f nu este separabil.

b) Dacă f este ireductibil în $K[X]$, atunci $f \notin K$, ceea ce implică $f' \neq 0$. Deci din a) rezultă că f este separabil.

c) Se aplică a) şi faptul, că $f' = 0$ dacă şi numai dacă $f \in K[X^p]$. □

Definiţia 4.1.4. Un corp K se numeşte *perfect*, dacă endomorfismul Frobenius $\varphi : K \to K$ este automorfism.

Exemplul 4.1.5. 1) Se observă uşor, că corpurile de caracteristică 0, corpurile algebric închise şi corpurile finite sunt perfecte.

2) Fie $K = \mathbb{Z}_p(X) = \{\frac{f}{g} \mid f, g \in \mathbb{Z}_p[X]\}$ corpul de fracţii al lui $\mathbb{Z}_p[X]$. În acest caz φ nu este surjectiv, deci K nu este perfect.

Teorema 4.1.6. *Un corp K este perfect dacă şi numai dacă orice extindere algebrică a sa este separabilă.*

Demonstraţie. Este suficient să considerăm cazul $\operatorname{char} K = p \neq 0$. Dacă ar exista un element x într-o extindere a corpului K, neseparabil peste K, atunci $m_{x,K} \in K[X^p]$. Deci

$$f = \sum_{i=0}^{n} a_i X^{pi}$$

Dacă corpul k este perfect, atunci există $b_i \in K$ astfel ca $b_i^p = a_i$. Atunci

$$f = \sum_{i=0}^{n} b_i^p X^{pi} = (\sum_{i=0}^{n} b_i X^i)^p$$

deci f ar fi reductibil în $k[X]$, ceea ce e contradicţie.

Invers, arătăm că dacă corp ul K nu este perfect, atunci există un element algebric a peste K, care nu e separabil. Deoarece corpul K nu e perfect, rezultă că există un polinom de forma $X^p - a$ (unde $a \in K$), care nu are nicio rădăcină în K. Este suficient de demonstrat că $X^p - a \in K[X^p]$ este ireductibil în $K[X]$ (pentru că atunci corpul de descompunere $F_{f,K}$ nu e extindere separabilă a lui K).

Într-adevăr fie, x şi y rădăcini ale polinom ului $X^p - a$ într-un corp algebric închis k. De aici obţinem $x^p = y^p$, de unde rezultă că $x = y$. Deci $X^p - a$ are o rădăcină x în k, cu multiplicitate p. Dacă $g := m_{x,k}$, obţinem

$$X^p - a = g^s.$$

Fie b termenul liber al lui g. Obţinem că $a = b^s$, unde $p = s \deg g$. Deoarece polinomul $X^p - a$ nu are rădăcină în k, rezultă că $s = 1$ şi deci $X^p - a$ este polinom ireductibil în $K[X]$. □

Teorema 4.1.7. *Fie K corp finit şi $K \leq L$ extindere separabilă finită. Atunci extinderea $K \leq L$ este simplă (are element primitiv).*

Demonstraţie. Deoarece $K \leq L$ este extindere finită, rezultă că există $u_1, \ldots, u_k \in L$ astfel încât $L = K(u_1, \ldots, u_k)$. Demonstrăm teorema în cazul $k = 2$, de unde prin inducţie rezultă cazul general.

Presupunem că $L = K(a,b)$. Fie $f = m_{a,K}$, $g = m_{b,K}$, $n = \deg f$, $m = \deg g$, iar $F = F_{fg,K}$ este corpul de descompunere al lui $fg \in K[x]$.

Deoarece extinderea $K \leq L$ este separabilă, obţinem că f are n rădăcini distincte $a_1 = a, a_2, \ldots, a_n$, iar g are m rădăcini distincte $b_1 = b, b_2, \ldots, b_m$.

Din faptul că K este infinit, rezultă că există $c \in K$ astfel ca

$$a_i + cb_j \neq a + bc$$

dacă $(i,j) \neq (1,1)$ şi $1 \leq i \leq n$, $1 \leq j \leq m$. Fie $d := a + bc$ şi arătăm că $L = K(d)$. Evident că avem $K(d) \subseteq K(a,b) = L$.

Coeficienţii polinomului $f_1 = f(d - cx)$ sunt în $K(d)$. Observăm că

$$f_1(b) = f(d - bc) = f(a) = 0$$

adică $b_1 = b$ este rădăcină comună a lui f_1 şi g. Din alegerea elementului c rezultă că f_1 şi g nu au alte rădăcini comune. Deci $X - b$ este cel mai mare divizor comun al lui f_1 şi g şi are coeficienţi în $K(d)$, de unde rezultă că coeficienţii lui $X - b$ sunt în $K(d)$. Deci $b \in K(d)$, şi deoarece $d = a + bc$ şi $c \in K$, rezultă că $a \in K(d)$. Obţinem că $k(a,b) \subseteq K(d)$. Am arătat astfel că $L = K(a,b) = K(d)$. □

Teorema 4.1.8. *Fie $k \leq K$ o extindere algebrică de corpuri de caracteristică $p > 0$.*

1) *Dacă K extindere separabilă a lui k, atunci $K = k(K^p)$.*

2) *Dacă $[K : k] < \infty$ şi $K = k(K^p)$, atunci K este extindere separabilă a lui k.*

3) *Elementul $x \in K$ este separabil peste k dacă şi numai dacă $k(x) = k(x^p)$. Dacă x este separabil peste k atunci $k(x)/k$ este extindere separabilă.*

Demonstraţie. 1) Deoarece K este extindere separabilă a lui k, rezultă că K este extindere separabilă a lui $k(K^p)$. Dacă $k(K^p) = K' \neq K$, atunci ar exista un element $x \in K$, pentru care este adevărat că $x \notin K'$. Atunci am văzut că $X^p - x^p$ este polinom ireductibil în $K'[X]$. Deoarece $X^p - x^p \in K'[X^p]$ ar rezulta că x nu e peste separabil K', ceea ce e contradicţie.

2) Presupunem că există un element $x \in K$ care nu este separabil peste k. Atunci polinomul minimal al lui x peste k are următoarea formă:

$$f = \sum_{i=0}^{n} a_i (X^p)^i, \qquad a_i \in k, \qquad n > 0.$$

Deci avem

$$\sum_{i=0}^{n} a_i (x^p)^i = 0 \tag{4.1}$$

Elementele $1, x, \ldots, x^n$ sunt liniar independente peste k, deci pot fi compoletate la o bază a lui K peste k. Fie deci $1, x, \ldots, x^n, y_1, \ldots, y_k$ o k-bază a lui K. Din faptul că $k(K^p) = K$, rezultă că elementele

$$1, x^p, \ldots, (x^p)^n, y_1^p, \ldots, y_k^p \tag{4.2}$$

generează pe K. Într-adevăr, din ipoteză rezultă că elementele lui K sunt combinaţii liniare de elemente din K^p cu coeficienţi în k, care sunt combinaţii liniare a elementelor

din (4.2) cu coeficienţi din k^p. Deci (4.2) este o bază a lui K peste k. Dar din (4.1) rezultă că în familia (4.2) primele $n+1$ elemente sunt liniar dependente.

3) Dacă x separabil peste k, atunci x este separabil şi peste $k(x^p)$. Dacă $x \notin k(x^p)$, atunci ar rezulta că x nu este separabil peste $k(x^p)$. Deci $x \in k(x^p)$ şi $k(x) = k(x^p)$.

Reciproc, dacă $k(x) = k(x^p)$, atunci rezultă că $k(x) = k((k(x))^p)$ şi din afirmaţia anterioară obţinem că orice element din $k(x)$ este separabil peste k. □

Corolar 4.1.9 (tranzitivitatea separabilităţii)**.** *Dacă $k \leq K$ şi $K \leq L$ sunt extinderi algebrice separabile, atunci şi $k \leq L$ este extindere separabilă.*

Demonstraţie. Putem presupune, că corpurile au caracteristica $p \neq 0$. Fie $x \in L$. Atunci x este separabil peste corpul K', care este corpul generat peste K de coeficienţii polinomului minimal al lui x peste k. Din 4.1.8. c) avem $K'(x^p) = K'(x)$, iar din 4.1.8. b) avem $k(K'^p) = K'$, deoarece $k \leq K'$ separabil. Deci

$$k((K'(x))^p) = K'(x^p) = K'(x)$$

şi aplicând din nou 4.1.8. b) obţinem că x este separabil peste k. □

Exerciţiul 4.1. Dacă K este perfect corp şi $f \in K[X]$ este polinom ireductibil, atunci f este separabil.

Exerciţiul 4.2. Fie $k \leq K \leq L$ extinderi algebrice.

a) Dacă $x \in L$ este separabil peste k, atunci x separabil şi peste K. În particular, dacă L este extindere separabilă a lui k, atunci L este extindere separabilă a lui K.

b) Orice extindere algebrică a unui corp perfect este corp perfect.

Exerciţiul 4.3. Să se determine un element primitiv al extinderii $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

4.2 Extinderi algebrice normale

Definiţia 4.2.1. Dacă $k \leq K$ este o extindere algebrică satisface a următoarele condiţii echivalente, atunci spunem că $k \leq K$ este *extindere normală.*

Teorema 4.2.2. *Fie $k \leq K$ o extindere algebrică, şi fie $\overline{k}$ o închidere algebrică a lui k ce conţine pe K. Următoarele afirmaţii sunt echivalente:*

(i) *orice k-automorfism al lui $\overline{k}$ induce un k-automorfism al lui Kt.*

(i') *Dacă $u \in \mathrm{Aut}_k(\bar{k})$, atunci $u(K) \subseteq K$.*

(ii) *Dacă un polinom ireductibil din $k[X]$ are o rădăcină în K, atunci orice rădăcină a sa este în K.*

(iii) *Pentru orice extindere algebrică L/K, orice k-automorfism al lui L induce un automorfism al lui K.*

Demonstraţie. (i)$\Rightarrow$ (i') este evident.

(i')$\Rightarrow$(i) Este suficient de demonstrat că u este surjectiv. Fie $y \in K$ şi $f \in k[X]$ polinomul minimal al lui y. Atunci u duce orice rădăcină a lui f din K într-o altă rădăcină a lui f din K. Deoarece u este injectiv şi şi mulţimea rădăcinilor lui f din K este finită, rezultă că u este surjectiv pe mulţimea rădăcinilor lui f în K. De aici rezultă că u surjectiv.

(i)$\Rightarrow$(ii) Fie $f \in k[X]$ un polinom ireductibil şi fie $x \in K$ o rădăcină a lui f. Dacă $y \in \overline{k}$ este o altă rădăcină a lui f, atunci există un k-izomorfism $u : k(x) \to k(y) \subseteq \overline{k}$ astfel încât $u(x) = y$, care se extinde la un k-automorfism $\overline{u} : \overline{k} \to \overline{k}$ conform Teoremei 3.5.8. Atunci din (i) rezultă că $\overline{u}(K) = K$, deci $u(x) = y \in K$.

(ii)$\Rightarrow$(iii) Fie $u : L \to L$ un k-automorfism, $x \in K$ şi $f \in k[X]$ polinomul minimal al lui x peste k. Atunci $u(x)$ este rădăcină a lui f, adică $u(x) \in K$, deci $u(K) \subseteq K$. De aici rezultă că $u(K) = K$ (analog cu (i')$\Rightarrow$(i)).

(iii)$\Rightarrow$(i) este evident. □

Teorema 4.2.3. 1) *O extindere finită $k \leq K$ este normală dacă şi numai dacă există un polinom $f \in k[X]$, al cărui corp de descompunere este K.*

2) *Dacă $k \leq K$ este o extindere, finită, normală şi separabilă, atunci există un polinom separabil $f \in k[X]$, al cărui corp de descompunere este K.*

Demonstraţie. Arătăm că corpul de descompunere al lui $f \in k[X]$ este extindere normală a lui k. Presupunem că K este corp de descompunere al lui $f \in k[X]$ şi că extinderea $k \subseteq K$ nu este normală. Rezultă că există $g \in k[X]$ care are o rădăcină $x_1 \in K$ e şi o rădăcină $x_2 \notin K$. Izomorfismul $\mathbf{1}_K$ se prelungeşte la un izomorfism

$$\varphi : k(x_1) \to k(x_2)$$

pentru care $\varphi(x_1) = x_2$.

Corpul K este corpul de descompunere al lui f pestei $k(x_1)$, iar $K(x_2)$ este corpul de descompunere al lui f peste $k(x_2)$. Deci izomorfismul φ se prelungeşte la izomorfismsul

$$\overline{\varphi} : K \to K(x_2).$$

Deoarece $\overline{\varphi}$ este prelungirea lui 1_K, rezultă că $\overline{\varphi}$ este izomorfism k-liniar. Pe de altă parte, deoarece $x_2 \notin K$ obţinem $\dim_k K < \dim_k K(x_2)$, ceea ce contrazice faptul că $\overline{\varphi}$ este izomorfism k-liniar.

Demonstrăm acum cealaltă implicaţie din 1) şi afirmaţia 2).

Presupunem că $k \subseteq K$ este extindere finită normală. Dacă $K = k$, atunci K este evident corp de descompunere. Dacă $K \neq k$, atunci există $x_1 \in K/k$, iar dacă $f_1 \in k[X]$ este polinomul minimal al lui x_1, atunci deoarece f_1 este ireductibil peste k şi $k \subseteq K$ este normală, rezultă că orice rădăcină lui f_1 este în K. Deci K_1 este corp de descompunere al lui f_1, este subcorp al lui K şi $k \neq K_1$. Dacă a $k \leq K$ este şi separabilă, atunci f_1 este polinom separabil, adică K_1 este corpul de descompunere al unui polinom separabil.

Dacă $K_1 \neq K$, atunci există $x_2 \in K \setminus K_1$, iar dacă $f_2 \in k[X]$ este polinomul minimal al lui x_2, atunci corp de descompunere K_2 al lui $f_1 f_2$ polinom este subcorp al lui K şi avem $K_1 < K_2$. Dacă extinderea $k \subset K$ este separabil, atunci şi f_2 este separabil; avem $f_1 \neq f_2$ şi deoarece f_1 şi f_2 sunt relativ prime, rezultă că f_1 şi f_2 sunt relativ prime. Deci f_1 şi f_2 nu au rădăcini comune. Rezultă că $f_1 f_2$ este separabil.

Dacă $K_2 \neq K$ atunci pe modelul anterior construim K_3 şi obţinem un şir strict crescător

$$k \subset K_1 \subset K_2 \subset K_3 \subset \dots$$

care conţine subcorpuri ale lui K şi care sunt corpuri de descompunere ale unor polinoame din $k[X]$, iar dacă $k \subset K$ este extindere separabilă , atunci aceste polinoame sunt separabile.

Dacă $k \leq K$ este extindere finită, obţinem că există $n > 0$, astfel ca $K = K_n$. $\square$

Exemplul 4.2.4. 1) Orice extindere de grad 2 este normală.

Într-adevăr fie $k \leq K$ o extindere de grad 2. Dacă $x \in K$ şi $x \neq k$, atunci $1, x$ este bază a lui K peste k, deci $K = k(x)$. Dacă $f = X^2 + aX + b$ este polinomul minimal al lui x, atunci f are gradul 2. Deoarece f are o rădăcină în K, rezultă că şi a doua rădăcină este în K (pentru că suma rădăcinilor este $-a \in K$). Deci K este corpul de descompunere al lui f, deci K/k este extindere normală.

2) Orice corp finit K este extindere normală a oricărui subcorp al său.

Într-adevăr dacă K are p^r elemente, unde p este caracteristica lui K, atunci K este corpul de descompunere al polinomului $X^{p^r} - X$, peste orice subcorp.

3) Fie $K = \mathbb{Q}(\sqrt[3]{4})$, privi ca extindere a lui $\mathbb{Q}$. Această extindere nu e normală.

Într-adevăr, polinomul minimal al lui $\sqrt[3]{4}$ este $X^4 - 3$, polinom care evident nu are toate rădăcinile în K.

4) Extinderile algebrice normale nu au proprietatea de tranzitivitate.

Într-adevăr, de exemplu $\mathbb{Q}(\sqrt[3]{4})$ nu este extindere normală a lui $\mathbb{Q}$, dar $\mathbb{Q}(\sqrt{3})$ este extindere normală a lui $\mathbb{Q}$, iar $\mathbb{Q}(\sqrt[3]{4})$ este extindere normală a lui $\mathbb{Q}(\sqrt{3})$.

Teorema 4.2.5. *Fie $L \supseteq K \supseteq k$ extinderi algebrice. Dacă L/k este extindere normală, atunci L/K este extindere normală.*

Demonstraţie. Fie $\overline{k}$ o închidere algebrică a lui k ce conţine pe L. Rezultă că orice $u \in \mathrm{Aut}_k(\overline{k})$ induce un k-automorfism al lui L, şi din faptul că $\mathrm{Aut}_K(\overline{k})$ este subgrup al lui $\mathrm{Aut}_k(\overline{k})$, rezultă că L este extindere normală a lui K. □

Teorema 4.2.6. *Fie K/k o extindere finită. Atunci există o extindere normală finită a lui k ce conţine pe K.*

Demonstraţie. Fie $K = k(x_1, x_2, \ldots, x_n)$ şi $f_i \in k[X]$ polinomul minimal al lui x_i, $i = 1, \ldots, n$. Atunci L este corp de descompunere al polinomului $f = \prod_{i=1}^{n} f_i$, care este inclusă într-un corp algebric închis $\overline{k}$ care conţine pe K. Aceasta este o extindere normală finită a lui k ce conţine pe K. □

Exerciţiul 4.4. Fie $k \leq L$ o extindere şi $K_1 \leq L$ respectiv $K_2 \leq L$ extinderi algebrice ale k. Notăm $K_1K_2 = k(K_1, K_2)$ subcorpul lui L generat de K_1 şi K_2.

a) Dacă K_1/K este extindere normală, atunci K_1K_2 este extindere normală a lui K_2.

b) Dacă K_1/k şi K_2/k sunt extinderi normale, atunci K_1K_2 şi $K_1 \cap K_2$ sunt extinderi normale ale lui k.

4.3 Grupul Galois al unei extinderi de corpuri

Fie K un corp şi $\mathrm{Aut}(K)$ grupul automorfismelor lui K. Fie a $k \leqslant K$ o extindere şi

$$\begin{aligned} G(K/k) = \mathrm{Aut}_k(K) &= \{\sigma \in \mathrm{Aut}(K) \mid \sigma(\alpha) = \alpha \ , \forall \alpha \in k\} \\ &= \{\sigma : K \to K \mid \sigma \text{ izomorfism de } k\text{-algebre}\}. \end{aligned}$$

Definiţia 4.3.1. Grupul $(G(K/k), \circ)$ se numeşte *grupul Galois* al extinderii K/k. Dacă $K = F_{f/k}$ este corpul de descompunere al polinomului $f \in k[x]$ peste k, atunci

$$G(f/k) := G(F_{f/k}/k)$$

este *grupul Galois al polinomului f* peste k, sau al ecuaţiei $f(x) = 0$ peste k.

Definiţia 4.3.2. Extinderea K/k se numeşte *extindere Galois*, dacă K/k este finită, normală şi separabilă.

Observaţii 4.3.3. 1) Fie $k \leqslant K \leqslant L$ extinderi de coruri. Dacă L/k este extindere Galoi, atunci şi L/K este Galois.

2) Dacă k este subcorpul prim al lui K, atunci $G(K/k) = \mathrm{Aut}(K)$.

Într-adevăr, pentru orice $a \in K$ avem $a = (m \cdot 1)(n \cdot 1)^{-1}$, unde $m, n \in Z$, $1 \in K$ şi $n \cdot 1 \neq 0$. Dacă $\sigma \in \mathrm{Aut}(K)$ atunci $\sigma(1) = 1$. Pentru orice $a \in K$ avem: $\sigma(a) = \sigma(m \cdot 1)\sigma(n \cdot 1)^{-1} = \sigma(m)\sigma(1)\sigma(n^{-1})\sigma(1) = (m1)(n1)^{-1} = a$, deci $\sigma \in G(K/k)$, adică $\mathrm{Aut}(K) \subseteq G(K/k)$. Deci $\mathrm{Aut}(K) = G(K/k)$.

3) Fie $k \leqslant K$ o extindere, $f \in k[X]$ un polinom şi $u \in K$ o rădăcină a lui f. Dacă $\sigma \in G(K/k)$, atunci şi $\sigma(u)$ este rădăcină a lui f.

Într-adevăr, fie $f = a_0 + a_1 x + \cdots + a_n x^n$. Atunci $a_0 + a_1 u + \cdots + a_n u^n = 0$; deoarece $\sigma(a_i) = a_i$, $i = 1, 2, \ldots, n$ şi σ este morfism, rezultă că $a_0 + a_1\sigma(u) + \cdots + a_n[\sigma(u)]^n = 0$, adică $\sigma(u)$ este rădăcină a lui f.

Teorema 4.3.4 (grupul Galois al unei extinderi Galois)**.** *Fie K/k o extindere Galois.*

1) *Există $x \in K$ astfel ca $K = k(x)$, şi $K = F_{f/k}$, unde $f := m_{k,x}$.*

2) $|G(K/k)| = [K : k] = \deg m_{k,x}$.

3) *Presupunem că* $\deg m_{k,x} = n$. *Atunci există morfismul injectiv de grupuri $\varphi : G(K/k) \hookrightarrow S_n$.*

Demonstraţie. 1) Deoarece K/k este finită şi separabilă, există element primitiv, adică există $x \in K$ element separabil astfel ca

$$K = k(x) = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1} \mid \alpha_i \in k\}.$$

Deoarece K/k este normală, rice rădăcină a lui $m_{k,x}$ este în K, deci $K = F_{f/k}$.

2) Fie $n := [K : k] = \deg f$. Fie $x = x_1, x_2, \ldots, x_n \in K$ rădăcinile lui f (distincte).

Dacă $\sigma \in G(K/k)$, atunci $\sigma(x)$ este rădăcină a lui f, deci $\sigma(x) \in \{x_1, x_2, \ldots, x_n\}$. Deoarece $K = k(x)$, elementul $\sigma(x)$ determină pe σ. Deci $|G(K/k)| \leqslant n$.

Arătm că $|G(K/k)| \geq n$. Deoarece x, x_i sunt conjugate, există k-automorfismul $\sigma_i : k(x) \to k(x_i)$ astfel încât $\sigma_i(x) = x_i$. Deoarece $k \leqslant k(x_i) \leqslant K$ şi $[K : k] = [k(x_i) : k] = \deg f$, rezultă că $k(x_i) = K$, deci $\sigma_1, \ldots, \sigma_n \in G(K/k)$ sunt automorfisme distincte.

3) Dacă $\sigma \in G(K/k)$ atunci pentru orice $i = 1, 2, \ldots, n$, $\sigma(x_i)$ este rădăcină a lui f, adică $\sigma(x_i) \in \{x_1, x_2, \ldots, x_n\}$. Am văzut că imaginile rădăcinilor determină pe σ.

Fie $\varphi : G(K/k) \to S_n$ astfel ca

$$\varphi(\sigma) = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{pmatrix}$$

Atunci $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$, deoarece $(\sigma \circ \tau)(x_i) = \sigma(\tau(x_i))$, deci φ este morfism de grupuri. Deoarece imaginile rădăcinilor determină pe σ, rezultă că φ este injectiv. $\square$

Din Teorema 4.3.4. avem că grupul Galois este subgrup al lui S_n. Când are loc egalitatea?

Teorema 4.3.5. 1) *Pentru orice $n > 0$ număr şi pentru orice corp K_0 există o extindere K/K_0 şi un polinom $f \in K[X]$ de grad n, al cărui grup Galois peste K este izomorf cu S_n.*

2) *Pentru orice $n > 0$ există un subcorp K al lui $\mathbb{R}$ şi un polinom $f \in K[X]$ de grad n, al cărui a grupul Galois peste K este izomorf cu S_n.*

Demonstraţie. 1) Fie $K' = K_0(X_1, \dots, X_n)$ corpul de fracţii al lui $K_0[X_1, \dots, X_n]$. Fie $K = K_0(s_1, \dots, s_n)$ subcorpul lui K' generat de K_0 şi de polinoamele simetrice $s_1, \dots, s_n$. Corpul de descompunere al polinomului

$$f = (X - X_1) \dots (X - X_n) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n \in K[X]$$

este K'. Arătăm că în acest caz morfismul injectiv

$$G(K/K') \to S_k, \qquad \sigma \to \varphi$$

este şi surjectiv. Dacă φ este o permutare a mulţimii $\{1, \dots, n\}$, atunci rezultă că există un morfism $\sigma : K_0[X_1, \dots X_n] \to K_0[X_1, \dots, X_n]$, pentru care $\sigma(a) = a$ şi $\sigma(x_i) = \sigma_{\varphi(i)}$, pentru orice $a \in K_0$ şi $i = 1, \dots, n$.

Putem prelungi pe σ la un automorfism $\sigma' : K' \to K'$, deci $\sigma' \in G(K/K')$ şi rezultă că morfismul $G(K/K') \to S_k$ duce pe σ' în φ.

2) Ca în 1) arătăm că $\mathbb{R}$ are un subcorp izomorf cu $\mathbb{Q}(s_1, \dots, s_n)$, ceea ce este echivalent cu afirmaţia că $\mathbb{R}$ are un subinel izomorf cu $\mathbb{Q}[X_1, \dots, X_n]$.

Folosim inducţie după n. Dacă $n = 0$, afirmaţia are loc pentru că $\mathbb{Q}$ este subcorp al lui $\mathbb{R}$. Presupunem că există un morfism injectiv $\sigma : \mathbb{Q}[X_1, \dots, X_n] \to \mathbb{R}$, şi fie

$a_i = \sigma(X_i)$, $i = 1, \ldots, n$. Din proprietatea de universalitate a inelului de polinoame rezultă că pentru orice $a \in \mathbb{R}$ există un omorfism

$$\sigma_a : \mathbb{Q}[X_1, \ldots, X_{n+1}] \to \mathbb{R}$$

care prelungeşte pe σ şi $\sigma_a(n+1) = a$. Rezultă că dacă scriem un element $f \in \mathbb{Q}[X_1, \ldots, X_{n+1}]$ sub forma

$$f = f_0 + f_1 X_{n+1} + \ldots + f_m X_{m+1},$$

unde $f_j \in \mathbb{Q}[X_1, \ldots, X_n]$, $j = 0, \ldots, m$, atunci

$$\sigma_a(f) = \sigma(f_0) + \sigma(f_1)a + \ldots + \sigma(f_m)a^m$$

şi $\sigma(f_j) \in \mathbb{Q}[a_1, \ldots, a_n] \subseteq \mathbb{Q}(a_1, \ldots, a_n)$.

În consecinţă, dacă σ_a nu e injectiv, atunci a este algebric peste $\mathbb{Q}(a_1, \ldots, a_n)$. Dacă niciun σ_a, unde a este număr real, nu ar fi injectiv, atunci ar rezulta că $\mathbb{R}$ este extindere algebrică a lui $\mathbb{Q}(a_1, \ldots, a_n)$, ceea ce ar implica că $\mathbb{R}$ este numărabil. Deci există a număr real, astfel ca σ_a este injectiv. $\square$

Teorema 4.3.6. 1) *Fie $f \in \mathbb{Q}[X]$ un polinom ireductibil de grad p număr prim. Presupunem că f are exact $p-2$ rădăcini reale . Atunci grupul Galois al lui f este izomorf cu S_p.*

2) *Pentru orice număr prim $p \geqslant 5$ există un polinom $f \in \mathbb{Q}[X]$ de grad p, al cărui grupul Galois este izomorf cu S_p.*

Demonstraţie. 1) Fie $K = F_{f,\mathbb{Q}}$ şi fie x_1, x_2 rădăcinile lui f care nu sunt reale. Deoarece $[\mathbb{Q}(x_1) : \mathbb{Q}] = p$ şi $K \supseteq \mathbb{Q}(x_1)$, rezultă că $p \mid [K : \mathbb{Q}]$; deoarece f este ireductibil şi $\mathbb{Q}$ este de caracteristică 0, rezultă că f este separabil şi deci

$$[K : \mathbb{Q}] = |G(K/\mathbb{Q})|.$$

Deci există un k-automorfism u de ordin p al lui K. Identificând $G = G(K/\mathbb{Q})$ cu un grup de permutari a rădăcinilor lui f, lui u îi corespunde un ciclu de lungime p. Aceasta induce un $\mathbb{Q}$-automorfism v al lui K, care permută x_1 cu x_2 şi fixează celelalte rădăcini ale lui f, adică v corespunde unei transpoziţii din S_p. Ştim că ordinul uniui ciclu de lungime l este l şi căordinul produsului a două cicluri disjuncte este cel mai mare divizor comun al ordinelor.

Deci G conţine un ciclu de ordin p, $\sigma = (i_1 \ \dots \ i_p)$, unde $i_k \in \{1, \dots, p\}$, $1 \leq k \leq p$. Putem presupune că G conţine transpoziţia $(1,2)$, şi deoarece o putere a lui σ este $(1\ 2\ \dots\ p)$, presupunem, că $(1\ 2 \dots\ p) \in G$. Astfel $\sigma(1\ 2)\sigma^{-1} = (2\ 3)$, ..., $\sigma(p-2\ p-1)\sigma^{-1} = (p-1\ p)$. Aceste transpoziţii generează pe G, deci $G = S_p$.

2) Fie m număr par, $m > 0$. Fie $n_1 < n_2 < \dots < n_{k-2}$, $k-2$ număr par, unde k este impar, $k > 3$. Considerăm polinomul

$$f = (X^2 + m)(X - n_1)(X - n_2)\dots(X - n_{k-2}).$$

Funcţia polinomială $\tilde{f}$ are $k-2$ rădăcini reale $n_1, n_2, \dots, n_{k-2}$. Din Teorema lui Rolle l rezultă că $\tilde{f}$ are cel puţin $k-3$ valori extreme, din care $\frac{k-3}{2}$ maxime şi $\frac{k-3}{2}$ minime. Deoarece $m \geqslant 2$ şi $n_1, n_2, \dots, n_{k-2}$ sunt numere pare, avem $|f(h)| > 2$ pentru orice h impar. Rezultă că valorile lui f în punctele de maxim sunt mai mari decât 2.

Fie $g = f - 2 \in \mathbb{Q}[X]$; atunci $\tilde{g}$ are cel puţin $\frac{k-3}{2}$ maxime şi $\frac{k-3}{2}$ minime. Valorile funcţiei $\tilde{g} : \mathbb{R} \to \mathbb{R}$ în punctele de maxim sunt mai mari ca 0. Deoarece avem $\frac{k-3}{2}$ maxime şi $\frac{k-3}{2}$ minime, rezultă că g are cel puţin $k-3$ rădăcini reale. Deoarece $g(n_{k-2}) = -f(n_{k-2}) - 2 = -2$ şi $g(+\infty) = +\infty$, rezultă că g mai are o rădăcină reală, care e mai mare ca n_{k-2}. Deci g are cel puţin $k-2$ rădăcini reale. Vom arăta, că pentru m suficient de mare g are două rădăcini complexe.

Fie $g = \prod_{i=1}^{k}(X - x_i)$ descompunerea lui g în $\mathbb{C}[X]$. Deoarece

$$g = (X^2 + m)(X - n_1)\dots(X - n_{k-2}) - 2,$$

obţinem

$$\sum_{i=1}^{k} x_i = \sum_{j=1}^{k-2} n_j \quad ; \quad \sum_{i<j} x_i x_j = \sum_{\alpha<\beta} n_\alpha n_\beta + m,$$

şi

$$\sum_{i=1}^{k} x_i^2 = \left(\sum_{i=1}^{k} x_i\right)^2 - 2\sum_{i<j} x_i x_j = \sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m.$$

Pentru m suficient de mare avem $\sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m < 0$, adică $\sum_{i=1}^{k} x_i^2 < 0$. Rezultă că cel puţin o rădăcină a lui g este complexă. Deoarece g are coeficienţi reali, are cel puţin două rădăcini complexe. Deoarece $\deg g = k$ şi g are cel puţin rădăcini $k-2$ reale, pentru m suficient de mare, g are $k-2$ rădăcini reale şi două rădăcini complexe.

Polinomul g este ireductibil. Într-adevăr,

$$f = X^k + a_1 X^{k-2} + \cdots + a_k,$$

unde $a_1, a_2, \ldots, a_k$ sunt numere pare. Deoarece $a_k = -mn_1n_2\ldots n_{k-2}$ şi $k > 3$, rezultă că $4|a_k$. Atunci coeficienţii $a_1, a_2, \ldots, a_{k-1}, a_{k-2}$ ai lui

$$g = f - 2 = X^k + a_1 X^{k-2} + \cdots + (a_k - 2)$$

sunt numere pare. Deoarece 4 nu divide pe $a_k - 2$ din criteriul lui Eisenstein rezultă că g este polinom ireductibil de grad k.

Dacă $k = p$ este număr prim, $p \geqslant 5$, atunci din 1) rezultă că grupul Galois al polinomului g este izomorf cu σ_p. □

Teorema 4.3.7 (automorfismele corpurilor finite)**.** *Fie $K = \mathbb{F}_{p^n}$ un corp finit şi $k = \mathbb{F}_{p^m}$ un subcorp. Atunci $G(K/k) = \langle \varphi^m \rangle$ este grup ciclic de ordin $d = n/m$, unde $\varphi : K \to K$, $\varphi(x) = x^p$ este endomorfismul Frobenius.*

Demonstraţie. Avem că d un număr natural, şi $k = \{x \in K \mid x^{p^m} = x\}$. Deoarece $\varphi^m(x) = x^{p^m}$, rezultă că $\varphi^{mi} \in G(K/k)$, $i = 1, 2, \ldots, d$. Mai departe, aceste automorfisme sunt distincte, deoarece dacă $\varphi^{si}(x) = \varphi^{mj}(x)$ pentru orice $x \in K$, unde $1 \leq i < j \leq d$, atunci

$$\begin{aligned} x^{n-m(j-i)} &= \varphi^{n-m(j-i)}(x) = \varphi^{n-mj}(\varphi^{mi}(x)) = \\ &= (\varphi^{n-mj}(\varphi^{mj}(x)) = \varphi^n(x) = x \end{aligned}$$

pentru orice $x \in K$. De aici rezultă că orice element al lui K este rădăcină a unui polinomn de grad mai mic ca p^n, contradicţie.

Pe de altă parte, K/k este extindere Galois simplă, $K = k(x)$, unde x generează grupul K^*. Obţinem că $|G(K/k)| = [K : k] = d$, deci

$$G(K/k) = \{\varphi^{mi} \mid i = 1, 2, \ldots, d\}$$

este generat de φ^m. □

Exerciţiul 4.5. Fie extinderea $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$. Să se determine grupul $G(\mathbb{Q}(i\sqrt{2})/\mathbb{Q})$.

Exerciţiul 4.6. Să se determine grupul Galois al polinomului $f = X^4 - 3 \in \mathbb{Q}[X]$.

Exerciţiul 4.7. Fie $2 \leq n \in \mathbb{N}$, şi $f = X^n - a \in \mathbb{Q}[X]$. Atunci $|G(f/\mathbb{Q})| = [F_{f,\mathbb{Q}} : \mathbb{Q}] \leq n(n-1)$.

Exerciţiul 4.8. Fie $f = X^n - a \in K[x]$, unde K este corp de caracteristică 0. Presupunem că K conţine rădăcinile de ordin n ale unităţii. Să se arate că $G(f/\mathbb{Q})$ este grup ciclic şi $|G(f/\mathbb{Q})| \mid n$.

Exerciţiul 4.9. Fie $f = X^n - 1 \in K[X]$. Să se arate că $G(F/K)$ este grup abelian.

4.4 Teorema fundamentală a teoriei lui Galois

Fie K/k o extindere, $G = G(K/k)$, $H \leq G$ şi fie

$$K^H = \{x \in K \mid \sigma(x) = x,\ \forall \sigma \in H\}$$

mulţimea elementelor H-invariante.

Lema 4.4.1. 1) $k \leqslant K^H \leqslant K$.

2) *Dacă* $H_1 \subseteq H_2$ *atunci* $K^{H_1} \supseteq K^{H_2}$.

Demonstraţie. 1) Fie $x \in k$ şi $\sigma \in G$. Atunci $\sigma(x) = x$. Deoarece $H \leqslant G$ şi $x \in k \leqslant K$, pentru orice $\sigma \in H$ avem $\sigma(x) = x$, adică $x \in K^H$, deci $k \subseteq K^H$. Evident, $K^H \subseteq K$.

Deoarece $k \leqslant K^H$, rezultă că $\left|K^H\right| \geqslant 2$ şi fie $x, y \in K^H$. Atunci $\sigma(x-y) = \sigma(x) - \sigma(y) = x - y$, adică $x - y \in K^H$; $\sigma(xy^{-1}) = \sigma(x)\sigma(y^{-1}) = xy^{-1}$, adică $xy^{-1} \in K^H$, deci K^H subcorp al lui K.

2) Fie $x \in K^{H_2}$ şi $\sigma \in H_1$; deoarece $H_1 \subseteq H_2$, $\sigma(x) = x$, deci $x \in K^{H_1}$. □

Teorema 4.4.2. *Fie* $k \leqslant L \leqslant K$.

1) $G(K/L) \leqslant (G, \circ)$, *unde* $G = G(K,k)$.

2) *Dacă* $k \leqslant L_1 \leqslant L_2 \leqslant K$, *atunci* $G(K/L_1) \supseteq G(K/L_2)$.

Demonstraţie. 1) Fie σ şi ψ automorfisme din $G(K/L)$ şi fie $x \in L$. Atunci $(\sigma \circ \psi)(x) = \sigma(\psi(x)) = \sigma(x) = x$, deci $\sigma \circ \psi \in G(K/L)$. Fie $\sigma \in G(K/L)$ şi fie $x \in L$, deci $\sigma(x) = x$; atunci $x = \mathbf{1}_K(x) = (\sigma^{-1} \circ \sigma)(x) = \sigma^{-1}(\sigma(x)) = \sigma^{-1}(x)$, deci $\sigma^{-1} \in G(K/L)$.

2) Fie $\sigma \in G(K/L_2)$. Atunci $\forall x \in L_2$ $\sigma(x) = x$. Deoarece $L_1 \subseteq L_2$, atunci $\forall x \in L_1$ avem că $\sigma(x) = x$, ceea ce este echivalent cu $\sigma \in G(K/L_1)$. □

Corpurile L pentru care $k \subseteq L \subseteq K$ se numesc corpuri intermediare. Avem o corespondenţă între corpurile intermediare şi subgrupurile lui $G(K/k)$.

Teorema 4.4.3 (Teorema fundamentală a teoriei lui Galois)**.** *Fie K/k o extindere Galois, $G = G(K/k)$ şi $\mathscr{K} = \{L \mid k \leqslant L \leqslant K\}$ laticea corpurilor intermediare. Fie*

$$\Phi : \mathscr{S}(G) \to \mathscr{K}, \qquad \Phi(H) = K^H,$$

$$\Psi : \mathscr{K} \to \mathscr{S}(G), \qquad \Psi(L) = G(K/L).$$

1) Φ, Ψ *sunt antiizomorfisme de latice, şi* $\Psi = \Phi^{-1}$.

2) *Dacă $k \leqslant L \leqslant K$, atunci L/k este extindere normală $\Leftrightarrow H = G(K/L) \trianglelefteq G$; în acest caz $G(L/k) \simeq \frac{G(K/k)}{G(K/L)} = G/H$.*

Demonstraţie. 1) Ştim din lema anterioară că Φ, Ψ sunt funcţii bine definite şi descrescătoare.

Arătam că pentru orice $H \leqslant G$ avem $G(K/K^H) = H$. Observăm că $H \subseteq G(K/K^H)$, deoarece dacă $\sigma \in H$, atunci pentru orice $x \in K^H$ avem $\sigma(x) = x$, adică $\sigma \in G(K/K^H)$. Fie $m = |H|$. Atunci este suficient de demonstrat că $|G(K/K^H)| \leq m$. Deoarece K/K^H este extindere Galois, $\left|G(K/K^H)\right| = [K : K^H]$ şi există $x \in K$ astfel ca $K = K^H(x)$. Fie

$$g := \prod_{\sigma \in H} (X - \sigma(x)) = (X - \sigma_1(x))(X - \sigma_2(x)) \dots (X - \sigma_m(x)),$$

unde $H = \{\sigma_1, \dots, \sigma_m\}$; rezultă că $g = X^m + \beta_{m-1}X^{m-1} + \dots + \beta_1 X + \beta_0$, unde $\beta_i \in K$. Din formulele lui A Viète rezultă că pentru orice $\sigma \in H$ avem $\sigma(\beta_i) = \beta_i$, deci $g \in K^H[X]$. (De exemplu, $-\beta_{n-1} = \sigma_1(x) + \dots + \sigma_n(x) \Longrightarrow -\sigma(\beta_{n-1}) = \sigma_1(x) + \dots + \sigma_n(x)$.) Deci $[K : K^H] = \deg m_{K^H,x} \leqslant m$, adică $\left|G(K/K^H)\right| \leqslant m$.

Arătam că pentru orice $k \leqslant L \leqslant K$ avem $K^{G(K/L)} = L$. Observăm, că $L \subseteq K^{G(K/L)}$, deoarece pentru orice $x \in L$ şi pentru orice $\sigma \in G(K/L)$ avem $\sigma(x) = x$, şi atunci $k \leqslant L \leqslant K^{G(K/L)} \leqslant K$. Deoarece K/L şi $K/K^{G(K/L)}$ sunt extinderi Galois, rezultă că $[K : L] = |G(K/L)|$ şi atunci,

$$[K : K^{G(K/L)}] = |G(K/K^{G(K/L)})| = |G(K/L)|.$$

Deoarece $[K : L] = [G(K/L)][K^{G(K/L)} : L]$, obţinem că $L = K^{G(K/L)}$.

2) este echivalent cu afirmaţia: *$H \trianglelefteq G$ dacă şi numai dacă K^H/k este extindere normală; în acest caz $G(K^H/k) \simeq G/H$.*

Presupunem că $H = G(K/K^H) \trianglelefteq G$ şi arătăm că K^H/k este extindere normală. Fie $x \in K^H = L$ şi fie x' o conjugată a lui x. Deoarece K/k este extindere Galois obţinem $x' \in K$. Arătăm că $x' \in L$, adică pentru orice $\tau \in H$ avem $\tau(x') = x'$. Ştim că există $\sigma' : k(x) \to k(x')$ k-automorfism astfel ca $\sigma'(x) = x'$. Atunci există $\bar{\sigma} : \bar{k} \to \bar{k}$ k-automorfism astfel ca $\bar{\sigma}_{|k(x)} = \sigma$. Deoarece K/k este normală, $\sigma = \bar{\sigma}_{|K} \in \mathrm{Aut}(K)$. Deci există $\sigma \in G(K/k)$ astfel ca $\sigma(x) = x'$. Deoarece $\sigma H \sigma^{-1} = H$, rezultă că $H = \{\sigma\tau\sigma^{-1} \mid \tau \in H\}$, şi pentru orice $\tau \in H$ avem $(\sigma\tau\sigma^{-1})(x') = \sigma(\tau(\sigma^{-1}(x'))) = \sigma(\tau(x)) = \sigma(x) = x'$, adică $x' \in L$.

Reciproc, presupunem că $k \leq L = K^H$ este normală, şi arătăm că $G(K/L) = H \trianglelefteq G$. Fie $\sigma \in G = G(K/k)$; deoarece L/k este normală, $\sigma_{|L} \in \mathrm{Aut}(L)$. Atunci $\varphi : G(K/k) \to G(L/k)$, $\varphi(\sigma) = \sigma_{|L}$ este morfism de grupuri, şi

$$\mathrm{Ker}\,\varphi = \{\sigma \in G \mid \sigma_{|L} = \mathbf{1}_L\} = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in L\} = G(K/L).$$

Deci $G(K/L) \trianglelefteq G$. Arătam că φ este surjectiv. Fie $\tau \in G(L/k)$; atunci există $\bar{\tau} : \bar{L} \to \bar{L}$ automorfism astfel ca $\bar{\tau}_{|L} = \tau$. Deoarece extinderea K/k este normală, pentru $\sigma := \bar{\tau}_{|K} : K \to K$ avem $\sigma \in G(K/k)$. Atunci $\varphi(\sigma) = \sigma_{|L} = \bar{\tau}_{|L} = \tau$, deci φ este surjectiv. Din Teorema I de izomorfism rezultă că $\frac{G(K/k)}{G(K/L)} \simeq G(L/k)$. □

Teorema 4.4.4. *Considerăm extinderile $k \leq K_1 \leq L$ şi $k \leq K_2 \leq L$ şi presupunem că $k \leq K_1$ este extindere Galois. Fie $G_1 := G(K_1/k)$, $G_2 := G(K_2/k)$ şi $G := G(K_1K_2/k)$.*

1) *Atunci extinderea $K_2 \subseteq K_1K_2$ este Galois, iar grupul $G(K_1K_2/K_2)$ este izomorf cu un subgrup al lui $G_1 = G(K_1/k)$.*

2) *Dacă $K_1 \cap K_2 = k$, atunci $G(K_1K_2/K_2) \simeq G_1 = G(K_1/k)$.*

3) *Dacă K_2/k este extindere normală, atunci K_1K_2 este extindere normală a lui k, şi dacă $K_1 \cap K_2 = k$, atunci*

$$G(K_1K_2/k) \simeq G_1 \times G_2.$$

Demonstraţie. 1) Corpul K_1 este corpul de descompunere al unui polinom separabil $f \in k[X]$. Deci dacă $x_1, \ldots, x_r$ sunt rădăcinile distincte ale lui f, atunci $K_1 = K(x_1, \ldots, x_r)$, ceea ce implică $K_1K_2 = K_2(x_1, \ldots, x_r)$.

Deci K_1K_2 este corpul de descompunere al lui f peste K_2 şi rezultă că extinderea $K_2 \subseteq K_1K_2$ este finită, normală şi separabilă.

Dacă $\sigma \in G(K_1K_2/K_2)$, atunci din $K \subseteq K_2$ rezultă că $\sigma(a) = a$ pentru orice $a \in K$. Mai departe, $\sigma(\{x_1, \ldots, x_r\}) = \{x_1, \ldots, x_r\}$. Rezultă că $\sigma(K_1) = K_1$ şi putem defini

k-automorfismul $\sigma_{|K_1} : K_1 \to K_1$. Aplicaţia

$$\rho : G(K_1K_2/K_2) \to G(K_1/k), \qquad \sigma \to \sigma_{|K_1}$$

este morfism.

Deoarece σ este determinat de restricţia la $x_1, \ldots, x_n$, rezultă că ρ este injectiv. Într-adevăr, dacă $\sigma \in \operatorname{Ker}\rho$, atunci $u_{|K_1} = \mathbf{1}_{K_1}$, adică $\sigma(x) = x$ pentru orice $x \in K_1$. Fie $z \in K_1K_2$. Atunci

$$z = \frac{\sum_{i=1}^m z_i y_i}{\sum_{j=1}^n z'_j y'_j},$$

unde $z_i,\ z'_j \in K_1$ şi $y_i,\ y'_j \in K_2$. Deoarece $\sigma \in G(K_1K_2/K_2)$, rezultă că σ este K_2-morfism. Deci $\sigma(z) = z$, pentru orice $z \in K_1K_2$, şi $\sigma = \mathbf{1}_{K_1K_2}$. În consecinţă, $\operatorname{Ker}\rho = \{\mathbf{1}_{K_1K_2}\}$, deci ρ este injectiv.

2) Arătăm că ρ surjectiv. Fie $G'_1 = \operatorname{Im}\rho$. Din teorema fundamentală a teoriei Galois avem că $G'_1 = G_1$ dacă şi numai dacă $K_1^{G'_1} = K_1^{G_1} = k$. Verificăm egalitatea $K_1^{G'_1} = k$. Dacă $a \in K_1^{G'}$, atunci $\tau(a) = a$, pentru orice $\tau \in G'_1$. Fie $\sigma \in G(K_1K_2/K_2)$, şi fie $\tau = \rho(\sigma) = \sigma_{|K_1}$. Deci $\sigma(a) = \tau(a) = a$, pentru orice $\sigma \in G(K_1K_2/K_2)$, adică $a \in (K_1K_2)^{G(K_1K_2/K_2)} = K_2$. Deoarece $a \in K_1$, rezultă că $a \in K_1 \cap K_2 = k$, deci $K_1^{G'} = k$. În consecinţă, $G'_1 = G_1$, deci ρ este surjectiv.

3) Se observă uşor că K_1K_2 este extindere normală a lui k. Definim funcţia

$$\rho : G \to G_1 \times G_2, \ \ \rho(\sigma) = (\sigma_{|K_1},\ \sigma_{|K_2}).$$

Atunci ρ este morfism de grupuri, şi arătăm că ρ este izomorfism.

Arătăm întâi că φ este injectiv. Fie $\sigma \in \operatorname{Ker}\rho$. Atunci $(\sigma_{|K_1},\ \sigma_{|K_2}) = (\mathbf{1}_{K_1},\ \mathbf{1}_{K_2})$ adică $\sigma(x) = x$ pentru orice $x \in K_1$ şi $\sigma(y) = y$ pentru orice $y \in K_2$. Fie $z \in K_1K_2$; atunci

$$z = \frac{\sum_{i=1}^m z_i y_i}{\sum_{j=1}^n z'_j y'_j},$$

unde $z_i,\ z'_j \in K_1$ şi $y_i,\ y'_j \in K_2$. Deci $\sigma(z) = z$; rezultă că $\sigma = \mathbf{1}_{K_1K_2}$, şi ρ este injectiv.

Arătăm că φ este surjectiv. Fie $(\tau_1, \tau_2) = G_1 \times G_2$. Din punctul anterior avem că pentru τ_1 există $\sigma_1 : K_1K_2 \to K_1K_2$, care este K_2-morfism astfel încât $\sigma_{1|K_1} = \tau_1$. Atunci $\varphi(\sigma_1) = (\tau_1,\ \mathbf{1}_{K_1})$. Analog pentru τ_2 există $\sigma_2 : K_1K_2 \to K_1K_2$, care este K_1-morfism astfel încât $\sigma_{2|K_2} = \tau_2$; atunci $\rho(\sigma_2) = (\mathbf{1}_{K_2}, \tau_2)$. Dacă $\sigma = \sigma_1\sigma_2$, atunci $\rho(\sigma) = \rho(\sigma_1\sigma_2) = \rho(\sigma_1)\rho(\sigma_2) = (\tau_1, \mathbf{1}_{K_1})(\mathbf{1}_{K_2}, \tau_2) = (\tau_1, \tau_2)$, deci ρ este surjectiv. $\square$

Corolar 4.4.5. *Fie k un corp şi $K_1, K_2, \ldots, K_n$ extinderi normale ale lui k astfel încât*

$$K_i \cap (K_{i-1}K_{i+1}\ldots K_n) = k$$

pentru orice $i = 1, 2, \ldots, n$. Dacă G_i este grupul Galois al extinderii K_i/k, (unde $1 \leqslant i \leqslant n$) şi G este grupul Galois al extinderii $K_1, K_2, \ldots, K_n/k$, atunci $G \simeq G_1 \times G_2 \times \cdots \times G_n$.

Demonstraţie. Folosim inducţie după n. Dacă $n = 2$, demonstraţia rezultă din teorema anterioară. Deoarece $K_n \cap (K_1 \ldots K_{n-1}) = k$ obţinem $G \simeq G(K_1 \ldots K_{n-1}/k) \times G_n$. Din ipoteza inducţiei rezultă că $G(K_1 \ldots K_{n-1}/k) \simeq G_1 \times G_2 \times \cdots \times G_{n-1}$, de unde obţinem $G \simeq G_1 \times G_2 \times \cdots \times G_n$. □

Exemplul 4.4.6. Fie $p_1, p_2, \ldots, p_n$ numere prime distincte. Considerăm corpul

$$K := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}).$$

Dacă $K_i = \mathbb{Q}(\sqrt{p_i})$, atunci $K = K_1K_2 \ldots K_n$. Vedem că

$$K_i \cap (K_1 \ldots K_{i-1}K_{i+1} \ldots K_n) = \mathbb{Q},$$

pentru orice $i = 1, 2, \ldots, n$. Notăm $G_i = G(K_i/\mathbb{Q})$, deci $G_i \simeq (\mathbb{Z}_2, +)$. Aplicând teorema anterioară, rezultă că $G(K/\mathbb{Q}) \simeq G_1 \times G_2 \times \cdots \times G_n \simeq \mathbb{Z}_2^n$.

Teorema 4.4.7. *Fie K un corp, $G \leqslant \mathrm{Aut}(K)$ un subgrup finit, şi fie*

$$F = K^G = \{a \in K \mid \sigma(a) = a, \forall \sigma \in G\}.$$

Atunci K/F este extindere Galois şi $G(K/F) = G$.

Demonstraţie. Fie $G = \{u_1, \ldots, u_n\}$, $x \in K$, şi fie $x_1 = x, x_2, \ldots x_n$ elementele distincte ale mulţimii $\{u_i(x) \mid i = 1, \ldots, n\}$. Din formulele lui Viéte rezultă că $f := \prod_{i=1}^{r}(X - x_r) \in F[X]$. Deoarece $f(x) = 0$, rezultă că x este element algebric peste F. Fie $g := m_{x,F}$. Deoarece $x_1, \ldots, x_r$ sunt conjugate, rezultă că $g(x_i) = 0$, $i = 1, \ldots, n$, deci $\deg g \geq r$; dar $g \mid f$, deci $g = f$. Deci x este separabil peste F şi K conţine toate conjugatele lui x. Deoarece x a fost ales arbitrar, rezultă că K/F este extindere algebrică normală şi separabilă.

Arătăm că K/F $[K : F] \leq n$. Presupunem că $[K : F] \geq n$ (eventual infinit). Fie $F \leq K' \leq K$ astfel încât $n < [K' : F] < \infty$. Atunci K'/F este extindere Galois, deci

există $x \in K'$ astfel încât $K' = F(x)$. Atunci $n \geq \deg m_{x,F} = [K' : F] > n$, contradicţie. Obţinem că K/F este extindere Galois, şi din teorema fundamentală a teoriei Galois rezultă că $G(K/F) = G$. $\square$

Exerciţiul 4.10. Fie $f \in \mathbb{Q}[X]$, $K = F_{f,\mathbb{Q}}$, $G = G(K/\mathbb{Q}) = G(f/\mathbb{Q})$. Să se determine K, G, $\mathscr{S}(G)$ şi, aplicând teorema fundamentală a teoriei Galois, subcorpurile lui K în următoarele cazuri:

a) $f = X^2 - d$ polinom, $d \in \mathbb{Z}$ un număr liber de pătrate;
b) $f = X^4 - 3$;
c) $f = (X^2 + 3)(X^2 - 5)$;
d) $f = X^3 + 2$.

Exerciţiul 4.11. Fie $f \in K[X]$ un polinom separabil şi fie $L := F_{f,K}$. Să se arate că f este ireductibil dacă şi numai dacă $G(f/K)$ este grup tranzitiv.

Exerciţiul 4.12. Fie K un corp de caracteristică 0 şi $f = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ un polinom separabil. Să se arate că discriminantul lui f este pătratul unui element K dacă şi numai dacă $G(f/K) \leq A_n$.

Aplicaţii ale teoriei lui Galois | 5

Galois a dat condiţii necesare şi suficiente pentru ca o ecuaţie algebrică să fie rezolvabilă prin radicali. Vom prezenta aici pe scurt aceste rezultate, precum şi imposibilitatea rezolvării câtorva probleme clasice de constructibilitate cu rigla şi compasul. Acestea sunt: problema din Delos (construcţia unui cub având dublul volumului unui cub dat), trisecţiunea unghiului (împărţirea unui unghi în trei părti egale), cuadratura cercului (construcţia unui pătrat de arie egală cu ara unui cerc dat) şi construcţia poligonului regulat cu n laturi.

5.1 Ecuaţii rezolvabile prin radicali. Teorema Abel–Ruffini

Fie k un corp de caracteristică 0. În acest paragraf, $\overline{k}$ este o închidere algebrică a lui k ce conţine orice extindere algebrică ce apare în continuare.

Definiţia 5.1.1. a) Elementul $x \in k$ se numeşte *radical* peste k, dacă x este rădăcină a unui polinom de forma $X^n - a \in k[X]$.

b) Se numeşte *extindere radicală simplă* a lui k corp de descompunere al unui polinom de forma $X^n - a \in k[X]$.

c) Extinderea algebrică $k \leq L$ se numeşte *extindere radicală*, dacă există şirul de subcorpuri

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_s = L$$

astfel ca K_{i+1} este extindere radicală simplă a lui K_i pentru orice $i = 0, 1, \ldots, s-1$.

d) Fie $f \in k[X]$, $\deg f > 0$. Spunem că ecuaţia $f(x) = 0$ este *rezolvabilă prin radicali*, dacă există o extindere radicală K/k care conţine toate rădăcinile lui f (adică $F_{f,k} \leq K$).

Observaţii 5.1.2. 1) Ştim că dacă b este rădăcină a lui $X^n - a$ şi ε este o rădăcină primitiv ă de ordin n a unităţii, atunci rădăcinile lui $X^n - a$ sunt distinctede forma

$\varepsilon^i b$, $0 \leq i \leq n-1$. Deci dacă K/k este extindere radicală simplă normală, atunci $K = k(\varepsilon, b)$.

2) Dacă K este extindere radicală a lui k şi L este extindere radicală a lui K, atunci L este extindere radicală a lui k, deci extinderile radicale sunt tranzitive şi finite. Deoarece extinderile normale nu sunt tranzitive, rezultă că extinderile radicale nu sunt neapărat normale. Astfel, de exemplu, $\mathbb{Q}(\sqrt[4]{3})$ este extindere radicală a lui $\mathbb{Q}$, dar ne este normală.

Teorema 5.1.3. *Fie k un corp de caracteristică 0 şi fie $f \in k[X]$, $\deg f > 0$. Ecuaţia $f(x) = 0$ este rezolvabilă prin radicali dacă şi numai dacă grupul Galois al lui f peste k este rezolubil.*

Corolar 5.1.4 (Abel–Ruffini)**.** *Ecuaţia generală de grad $n \geq 5$ nu este rezolvabilă prin radicali.*

Exerciţiul 5.1. Să se arate că ecuaţia $x(x^2-4)(x^2+2) = 2$ nu e rezolvabilă prin radicali peste $\mathbb{Q}$.

5.2 Constructibilitate cu rigla şi compasul

5.2.1 Numere complexe construibile cu rigla şi compasul

Fie $\mathscr{P}$ un plan şi fie mulţime finită de puncte $S = \{P_1, P_2, \ldots, P_n\}$ din $\mathscr{P}$, unde $n \geq 2$. Considerăm în $\mathscr{P}$ sistemul de coordonate xOy, unde originea este $O = P_1$, şi P_2 are coordonatele $(1,0)$.

Definim recursiv mulţimile de puncte $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_r \subseteq \ldots$ astfel. Fie $S_1 = S$ şi presupunem că mulţimea S_r este definită. Atunci S_{r+1} se obţine adăugând la S_r puncte construite astfel:

1° intersecţia a două drepte determinate de puncte existente;

2° intersecţia dintre o dreaptă şi un cerc sau intersecţia a două cercuri, unde cercurile au raze egale cu distanţele dintre perechi de puncte existente şi centrele în puncte existente;

Notăm

$$C(P_1, P_2, \ldots, P_n) = \bigcup_{r \geqslant 1} S_r.$$

Un punct P care este element al mulţimii $C(P_1, P_2, \ldots, P_n)$ se numeşte *constructibil cu rigla şi compasul* din punctele $P_1, P_2, \ldots, P_n$.

Considerăm funcţia bijectivă

$$\Theta : \mathscr{S} \to \mathbb{C}, \qquad \Theta(P) = x + iy,$$

unde P are coordonatele (x, y). Numărul complex $x + iy$ este *afixul* lui $P(x, y)$. Notăm $\Theta(P_i) = \alpha_i$ $(1 \leqslant i \leqslant n)$. Deci $\alpha_1 = 0$ şi $\alpha_2 = 1$. Notăm

$$\Theta(C(P_1, P_2, \ldots, P_n)) = C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Un număr complex $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ se numeşte *constructibil cu rigla şi compasul* din numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$. Vedem că α este constructibil dacă şi numai dacă $\Re\alpha$ şi $\Im\alpha$ sunt constructibile.

Teorema 5.2.1. *$C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este subcorp al lui $\mathbb{C}$, şi are următoarele proprietăţi:*

1) *Dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci $\bar{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$;*

2) *Dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$;*

3) *$C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este cel mai mic subcorp al lui $\mathbb{C}$ care conţine numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi satisface* 1), 2).

Demonstraţie. Fie $\alpha, \alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Notăm $\Theta(P) = \alpha$ şi $\Theta(P') = \alpha'$, unde $P, P' \in \mathscr{P}$. Deci $P, P' \in C(P_1, P_2, \ldots, P_n)$.

Punctul Q obţinut prin regula paralelogramului corespunde lui $\alpha + \alpha'$ şi este uşor de văzut că $\alpha + \alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Scriem α şi α' sub forma trigonometrică: $\alpha = r(\cos\varphi + i\sin\varphi)$, $\alpha' = r'(\cos\varphi' + i\sin\varphi')$; atunci

$$\alpha\alpha' = rr'[\cos(\varphi + \varphi') + i\sin(\varphi + \varphi')].$$

Deoarece $\varphi + \varphi'$ este evident constructibil cu rigla şi compasul, construim pe rr'. Din asemănarea triunghiurilor dreptunghice avem $\frac{x}{r} = \frac{r'}{1}$, de unde $x = rr'$. Vedem că x este constructibil cu rigla şi compasul. Deci $\alpha\alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Arătăm că acă $\alpha = r(\cos\varphi + i\sin\varphi) \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha \neq 0$, atunci $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Într-adevăr $\alpha^{-1} = \frac{1}{r}[\cos(-\varphi) + i\sin(-\varphi)]$. Atunci $\frac{x}{1} = \frac{1}{r}$, deci $x = \frac{1}{r}$. Deoarece x este constructibil, rezultă că $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deci $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ subcorp $\mathbb{C}$.

1) Fie $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Imediat rezultă că $\bar{\alpha} \in C(\alpha_1, \ldots, \alpha_n)$.

2) Fie $\alpha = r(\cos\varphi + i\sin\varphi) \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Atunci

$$\sqrt{\alpha} = \sqrt{r}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}).$$

Deoarece numărul $\sqrt{r}$ şi unghiul $\dfrac{\varphi}{2}$ sunt constructibile cu rigla şi compasul, rezultă că $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

3) Fie K un subcorp $\mathbb{C}$ care conţine pe $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi satisface proprietăţile 1), 2). Deoarece $-1 \in K$, din proprietatea 1) rezultă că $i = \sqrt{-1} \in K$. Dacă $\alpha = x + iy$, atunci din 1) obţinem $\bar{\alpha} = x - iy \in K$; rezultă că $x, y \in K$. Deci

$$\alpha = x + iy \in K \Longleftrightarrow x, y \in K.$$

Notăm $\mathscr{S}' = \Theta^{-1}(K)$. Arătăm că mulţimea de puncte $\mathscr{S}'$ este închisă faţă de construcţiile 1° şi 2°. Într-adevăr sistemul de ecuaţii

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}, \quad a, b, a', b', c, c' \in K$$

are soluţiile în K. Analog, sistemul de ecuaţii

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + mx + ny + p = 0 \end{cases}, \quad a, b, c, m, n, p \in K,$$

are soluţiile în K. Să mai observăm că intersecţia a două cercuri este intersecţia dintre un cerc şi axa radicală a celor două cercuri. Deoarece $P_1, P_2, \ldots, P_n \in \mathscr{S}'$, din 1° şi 2° rezultă că $C(P_1, P_2, \ldots P_n) \subseteq \mathscr{S}'$, deci

$$C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K,$$

deci $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este cel mai mic subcorp al lui $\mathbb{C}$ care conţine $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi satisface 1) şi 2). $\square$

5.2.2 Primul criteriu de constructibilitate

Deoarece $\mathbb{Q} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, obţinem

$$F := \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Dacă $n = 2$, atunci $F = \mathbb{Q}(\alpha_1, \alpha_2, \bar{\alpha}_1, \bar{\alpha}_2) = \mathbb{Q}$ şi $C(\alpha_1, \alpha_2) = C(0, 1)$ se numeşte mulţimea numere complexe constructibile cu rigla şi compasul.

Teorema 5.2.2 (Primul criteriu de constructibilitate)**.** *Numărul complex α este constructibil cu rigla şi compasul din $\alpha_1, \alpha_2, \ldots, \alpha_n$ dacă şi numai dacă există extinderile finite de corpuri*

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_r$$

astfel încât $\alpha \in F_r$ şi $[F_i : F_{i-1}] \leqslant 2$ pentru orice $1 \leqslant i \leqslant r$.

Demonstraţie. Notăm

$$K := \{\alpha \in \mathbb{C} \mid \exists\, F = F_0 < F_1 < F_2 < \ldots < F_r \text{ extinderi: } \alpha \in F_r,\ [F_i : F_{i-1}] \leqslant 2,\ \forall i\}.$$

Fie $\alpha, \beta \in K$; există $F = F_0 < F_1 < F_2 < \ldots < F_r$ extinderi finite, unde $\alpha \in F_r$ şi $[F_i : F_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$, respectiv $F' = F'_0 < F'_1 < F'_2 < \ldots < F'_r$, unde $\beta \in F'_r$ şi $[F'_j : F'_{j-1}] \leqslant 2$, $(1 \leqslant j \leqslant r')$. Obţinem extinderile

$$F = F_0 < F_1 < F_2 < \ldots < F_r = F_rF'_0 < F_rF'_1 < \ldots < F_rF'_{r'},$$

unde $[F_rF'_j : F_rF'_{j-1}] \leqslant 2$, pentru orice $1 \leqslant j \leqslant r'$. Deoarece $\alpha + \beta,\ \alpha\beta \in F_rF'_r$ şi $\alpha^{-1} \in F_r$, dacă $\alpha \neq 0$ rezultă că K subcorp $\mathbb{C}$. Deoarece F este închis la conjugare rezultă că şi K este închis la conjugare. Dacă

$$F = F_0 < F_1 < F_2 < \ldots < F_r$$

sunt extinderi finite astfel încât $[F_i : F_{i-1}] \leqslant 2$, $(1 \leqslant i \leqslant r)$, atunci F_i închis la extragerea rădăcinii pătrate. Deci K este închis la extragerea rădăcinii pătrate. Deoarece $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, rezultă că $C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$. Fie $\alpha \in K$ şi fie

$$F = F_0 < F_1 < F_2 < \ldots < F_r,$$

extinderi astfel încât $\alpha \in F_r$ şi $[F_i : F_{i-1}] \leqslant 2$, pentru orice $1 \leqslant i \leqslant r$. Arătăm prin inducţie că pentru orice i, $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Dacă $i = 0$, atunci

$$F_0 = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Presupunem că $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ şi arătăm că $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deoarece $[F_{i+1} : F_i] \geqslant 2$, obţinem $F_{i+1} = F_i(\beta)$, unde β este element algebric peste F_i, şi β are ca polinom minimal pe f, $\deg f \leq 2$. Deci β este rădăcină a unei ecuaţii de grad 2 cu coeficienti în $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deoarece $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ satisface proprietatea 2), rezultă că $\beta \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, deci $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Am arătat că $K \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, de unde $K = C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. $\square$

Corolar 5.2.3. *Dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci polinomul minimal al lui α peste F are gradul de forma 2^k.*

Demonstraţie. Există extinderile $F = F_0 < F_1 < F_2 < \ldots < F_r$, unde $\alpha \in F_r$, $[F_i : F_{i-1}] \leq 2$, $1 \leq i \leq r$. Rezultă că $[F_r : F] = 2^l$, unde $l > 0$. Deoarece

$$[F_r : F] = [F(\alpha) : F][F_r : F(\alpha)],$$

obţinem $[F(\alpha) : F] = 2^k$, unde $k \geqslant 0$. Dar $[F(\alpha) : F] = \deg m_{\alpha,F}$. Deci $\deg m_{\alpha,F} = 2^k$. □

5.2.3 Trisecţiunea unghiului

Problema este de a împărţi un unghi in trei părţi egale cu rigla şi compasul. Vom arăta că aceste lucru nu este întotdeauna posibil.

Un unghi dat φ este determinat de deci $u = \cos\varphi$. Trebuie deci să construim numărul $x = \cos\frac{\varphi}{3}$. Deoarece

$$\cos\varphi = 4\cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3},$$

de aceea x este rădăcină a ecuaţiei $4x^3 - 3x - u = 0$. Fie

$$f = 4X^3 - 3X - u.$$

Este suficient de demonstrat că există φ astfel încât $u = \cos\varphi \in \mathbb{Q}$ şi f ireductibil peste $\mathbb{Q}$. Atunci gradul $[F_{f,\mathbb{Q}} : \mathbb{Q}]$ este divizibil cu 3, deci nu este putere a lui 2.

De exemplu, fie $\varphi = 60^\circ$, care determină punctele P_1, P_2, P_3, unde

$$\alpha_3 = \cos 60^\circ + i\sin 60^\circ = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

În acest caz

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = \mathbb{Q}(i\sqrt{3}).$$

Fie $\alpha = \cos 20^\circ + i\sin 20^\circ$. Din egalitatea $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, pentru $\varphi = 20^\circ$ obţinem $\frac{1}{2} = 4\cos^3 20^\circ - 3\cos 20^\circ$. Deci $\cos 20^\circ$ rădăcină a polinomului ireductibil

$$f = 4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X].$$

Deci şi polinomul minimal al lui $\cos 20^\circ$ peste $\mathbb{Q}(i\sqrt{3})$ are grad 3. Din Corolarul 5.2.3. rezultă că $\cos 20^\circ \notin C(0, 1, i\sqrt{3})$.

5.2.4 Dublarea cubului (problema din Delos)

Problema este construcţia cu rigla şi compasul a unui cub având dublul volumului unui cub dat. Considerăm că cubul dat are latura 1, deci pornim de la corpul $F = \mathbb{Q}$ şi trebuie să construim numărul $\sqrt[3]{2}$, care este rădăcină a polinomului $X^3 - 2$. Acesta este ireductibil peste $\mathbb{Q}$, deci din Corolarul 5.2.3. rezultă că $\sqrt[3]{2} \notin C(0,1)$. Deci construcţia nu e posibilă.

5.2.5 Cuadratura cercului

Problema este construcţia cu rigla şi compasul a unui pătrat de arie egală cu ara unui cerc dat. Fie $P_1(0,0)$ centrul cercului şi $P_2(1,0)$ un punct pe cerc. Atunci latura pătratului este $\sqrt{\pi}$. Ferdinand Lindemann a arătat în 1882 că π nu este număr algebric. Rezultă că şi $\sqrt{\pi}$ este număr transcendent, deci $\sqrt{\pi} \notin C(0,1)$. Deci construcţia nu e posibilă.

5.2.6 Al doilea criteriu de constructibilitate

Definiţia 5.2.4. Extinderea $K \leq E$ se numeşte *pitagoreică*, dacă există extinderile

$$K = K_0 < K_1 < K_2 < \ldots < K_r = L$$

astfel încât $[K_i : K_{i-1}] \leqslant 2$, pentru orice $1 \leqslant i \leqslant r$.

Vedem că atunci K_i/K_{i-1} este extindere radicală simplă şi L/K este extindere extindere radicală. Ca în cazul extinderilor radicale, avem:

Teorema 5.2.5. *Dacă L/K este extindere pitagoreică, atunci există o extindere pitagoreică şi normală F/K astfel încât $L \subseteq F$.*

Teorema 5.2.6. *Fie L/K o extindere normală. Atunci L/K este extindere pitagoreică dacă şi numai dacă gradul $[L : K]$ este putere a lui 2.*

Demonstraţie. Presupunem că extinderea L/K este pitagoreică. Există extinderile

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L,$$

$[K_i : K_{i-1}] \leqslant 2$, pentru orice $1 \leqslant i \leqslant r$. Rezultă că $[L : K] = 2^s$, unde $s \geq 0$.

Invers, presupunem că $[E:K]=2^n$. Fie G grupul Galois $G(E/K)$ având ordin $|G|=2^n$. Notăm $Z_1=Z(G)$ centrul lui G. Deoarece G este 2-grup, $Z_1\neq\{e\}$. Deoarece şi G/Z_1 este 2-grup, a centrul lui este de forma Z_2/Z_1, unde $Z_2\leq G$, şi conţine cel puţin două elemente. Astfel avem lanţul de subgrupuri ale lui G:

$$Z_1\subset Z_2\subset\ldots\subset Z_{i-1}\subset Z_i\subset\ldots,$$

unde Z_i/Z_{i-1} este centrul lui G/Z_{i-1}. Deoarece pentru orice $i\geqslant 1$ Z_i/Z_{i-1} conţine cel puţin două elemente, există $r\geqslant 1$ astfel încât $G=Z_r$. Deoarece Z_i/Z_{i-1} este comutativ de ordin putere a lui 2, avem lanţul

$$\{e\}=H_0\subset H_1\subset H_2\subset\ldots\subset H_s=G,$$

astfel încât $H_i\trianglelefteq G$, $[H_i:H_{i-1}]=2$, $1\leqslant i\leqslant s$. Dacă notăm $K_i=E^H_{s-i}$, unde $0\leqslant i\leqslant s$, avem extinderile

$$K=K_0<K_1<\ldots<K_s=L.$$

Din teorema fundamentală a teoriei lui Galois avem $[K_i:K_{i-1}]=2$ pentru orice $1\leqslant i\leqslant s$. Deci L/K este extindere pitagoreică. □

Corolar 5.2.7 (Al doilea criteriu de constructibilitate)**.** *Numărul complex α este constructibil cu rigla şi compasul din $\alpha_1,\alpha_2,\ldots,\alpha_n$ dacă şi numai dacă există o extindere normală $F\leq L$ de grad putere a lui 2, astfel încât $\alpha\in L$.*

5.2.7 Constructibilitatea poligonului regulat cu n laturi

Problema revine la a împărţi cercul în n părti egale. Pe vremea lui Euclid era deja cunoscută construcţia în cazurile $n=2^k$, $3\cdot 2^k$, $5\cdot 2^k$ şi $15\cdot 2^k$. Gauss a fost primul care a construit poligonul regulat cu 17 laturi, în lucrarea *„Disquisitiones arithmeticae”*. Rezultatul general de mai jos este atribuit lui Gauss şi Pierre Wantzel (1837).

Fie punctele $P_1(0,0)$ şi $P_2(1,0)$, care determină cercul de rază 1. Trebuie studiată constructibilitatea numărului complex

$$\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

care este rădăcină primitivă de ordin n a unităţii. Ştim că $\mathbb{Q}(\varepsilon)$ este corpul de descompunere al polinomului $X^n-1\in\mathbb{Q}[X]$ şi că $[\mathbb{Q}(\varepsilon):\mathbb{Q}]=\phi(n)$.

Teorema 5.2.8. *Poligonului regulat cu n laturi este constructibil dacă şi numai dacă n este de forma*

$$n = 2^s p_1 p_2 \dots p_r,$$

unde $s \geqslant 0$, $r \geqslant 0$, *şi fiecare* p_i *este număr prim impar astfel încât* $p_i - 1$ *este putere a lui* 2.

Demonstraţie. Din al doilea criteriu, ε este constructibil dacă şi numai dacă $\phi(n) = [\mathbb{Q}(\varepsilon) : \mathbb{Q}]$ este putere a lui 2. Dacă $n = 2^s p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, unde $s \geqslant 0$, $p_1, p_2, \dots, p_k$ sunt numere prime impare distincte, atunci

$$\varphi(n) = 2^{a-1} p_1^{n_1-1}(p_1 - 1) \dots p_k^{n_k-1}(p_k - 1)$$

este putere a lui 2 dacă şi numai dacă $n_1 = n_2 = \dots = n_k = 1$ şi $p_1 - 1, \dots, p_k - 1$ sunt puteri ale lui 2. Fie $p_i - 1 = 2^{m_i}$, $1 \leqslant i \leqslant k$. Pentru ca p_i să fie număr prim, m_i trebuie să fie putere a lui 2. Într-adevăr, avem $m_i = 2^{t_i} u$, unde u este impar. Atunci

$$p_i = 2^{m_i} + 1 = \left(2^{2^{t_i}}\right)^u + 1.$$

Deoarece u este impar, $2^{2^{t_i}} + 1$ divide pe p_i. Deoarece p_i prim, $u = 1$, $m_i = 2^{t_i}$ şi $p_i = 2^{2^{t_i}} + 1$. □

Un număr prim de forma $p = 2^{2^n} + 1$ se numeşte *număr prim al lui Fermat*. Observăm, că pentru $n = 1, 2, 3, 4$ avem $p = 3, 5, 17, 257, 65537$. Pentru $n = 5$ Euler a arătat că $2^{32} + 1 = 641 \cdot 6700417$ nu este număr prim.

Exerciţiul 5.2. Să se construiască poligonul regulat cu 5 respectiv 10 laturi.

Exerciţiul 5.3. Să se arate că:

a) Trisecţiunea unghiurilor 90°, 180°, $\arccos \frac{11}{16}$ este posibilă.

b) Dacă $(k, n) = 1$, atunci $[\mathbb{Q}(\cos \frac{2k\pi}{n} : \mathbb{Q}] = \frac{\phi(n)}{2}$.

c) Trisecţiunea unghiului $\frac{2\pi}{n}$ este posibilă $\Longleftrightarrow \phi(3n) = 2^k$, unde $k \geq 1$.

d) Unghiul de n° este constructibil $\Longleftrightarrow 3 \mid n$.

Exerciţiul 5.4. Este constructibilă latura unui tetraedru regulat de volum 1?

Bibliografie

[1] T. Albu, Ion D. Ion, *Capitole de teoria algebrică a numerelor*. Editura Academiei, Bucureşti 1984.

[2] M. Artin, *Algebra*. Birkhäuser, Basel 1998.

[3] E.J. Barbeau, *Polynomials*. Springer-Verlag, New York 1989.

[4] P.A. Blaga, *Construcţii geometrice*. Note de curs, UBB, Facultatea de Matematică şi Informatică.

[5] G. Călugăreanu, P. Hamburg, *Exercises in basic ring theory*. Kluwer Academic Publishers, Dordrecht 1998.

[6] S. Crivei, *Basic Abstract Algebra*. Casa Cărţii de Ştiinţă, Cluj-Napoca 2002.

[7] D. Fadeev, I. Sominski, *Recueil d'exercises d'algébre supérieure*. Edition Mir, Moscou 1977.

[8] M.H. Fenrick, *Introduction to the Galois Correspondence*. 2nd Ed., Birkhauser, Basel 1996.

[9] J.B. Fraleigh, *A first course in abstract algebra*. Addison-Wesley, Reading 1968.

[10] J.A. Gallian, *Contemporary Abstract Algebra, Seventh Edition*. Brooks/Cole 2010.

[11] R. Godement, *Cours d'Algébre*. Hermann, Paris 1963.

[12] Ion D. Ion, N. Radu, *Algebra*. Ed. Didactică şi Pedagogică, Bucureşti 1981.

[13] Ion D. Ion, C. Niţă, D. Popescu, N. Radu, *Probleme de algebră*. Ed. Didactică şi Pedagogică, Bucureşti 1981.

[14] N. Jacobson, *Basic algebra I,II*. Freeman, San-Francisco 1984.

[15] A.I. Kostrikin, *Introduction à l'algébre*. Edition Mir, Moscou 1981.

[16] L. Koulikov, *Algébre et théorie des nombres*. Edition Mir, Moscou 1973.

[17] S. Lang, *Algebra*. Addison-Wesley, Reading 1965.

[18] A. Mărcuş, *Algebra*. Presa Univ. Clujeană, 2008.

[19] C. Năstăsescu, C. Niţă, C. Vraciu, *Teoria calitativă a ecuaţiilor algebrice*. Editura tehnică, Bucureşti 1979.

[20] C. Năstăsescu, C. Niţă, C. Vraciu, *Bazele algebrei I*. Ed. Academiei, Bucureşti 1986.

[21] L. Panaitopol, *Polinoame şi ecuaţii algebrice*. Ed. Albatros, Bucureşti 1980.

[22] I. Purdea, C. Pelea, *Probleme de algebră (ediţia a II-a)*. EIKON, Cluj-Napoca, 2008.

[23] I.V. Proskuriakov, *Problems in linear algebra*. Mir Publishers, Moscow 1978.

[24] I. Purdea, Gh. Pic, *Tratat de algebră modernă I*. Ed. Academiei, Bucureşti 1977.

[25] I. Purdea, *Tratat de algebră modernă II*. Ed. Academiei, Bucureşti 1982.

[26] J.J. Rotman, *Advanced modern algebra*. Prentice Hall, NJ 2002.

[27] I. Stewart, *Galois Theory. Fourth Edition*. Chapman and Hall/CRC 2015.

[28] J. Szendrei, *Algebra és számelmélet*. Tankönyvkiadó, Budapest 1974.

[29] I.R. Şafarevici, *Noţiunile fundamentale ale algebrei*. Ed. Academiei, Bucureşti 1989.

[30] J.-P. Tignol, *Galois' Theory of Algebraic Equations*. World Scientific, Singapore 2002.

[31] A. Tóth, *Noţiuni de teoria construcţilor geometrice*. Ed. Didactică şi Pedagogică, Bucureşti, 1963.

[32] S. Warner, *Modern Algebra*. Dover, New York 1990.

Glosar