Cuprins

Prefață

În cartea de față sunt studiate două teme importante: proprietăți aritmetice ale inelelor şi extinderi de corpuri (cu aplicații).

Primul capitol prezintă noțiuni şi rezultate generale de teoria inelelor, ca: ideale, inele factor, teoreme de izomorfism, inele şi corpuri de fracții. Pentru importanța pe care o au în capitolele următoare, o atenție deosebită se acordă idealelor prime şi maximale.

Capitolul al doilea tratează proprietățile aritmetice ale inelelor care privesc: relația de divizibilitate în inele comutative, cel mai mare divizor comun şi cel mai mic multiplu comun, descompunerea în factori primi (ireductibili). Generalizând proprietăți ale inelului $\mathbb{Z}$ al întregilor raționali, sunt definite trei clase importante de inele: inelele euclidiene, inelele principale şi inelele factoriale. Deşi pornesc de la un lucru simplu (exprimarea celui mai mare divizor comun ca o combinație liniară de elementele date), relațiile lui Bézout (stabilite inițial în inelele euclidiene) deschid calea unor algoritmi numerici cu diverse aplicații. Aceleaşi relații Bézout există şi în inelele principale, fără a mai dispune însă de o metodă de calcul a lor. Inelele factoriale sunt caracterizate de proprietatea că elementele nenule şi neinversabile se descompun în produse de elemente prime. Merită subliniat faptul că proprietatea de inel factorial se transmite de la inelul coeficienților la inelul de polinoame.

În capitolul al III-lea, sunt studiate extinderile de corpuri, urmărind două direcții principale. Pe de o parte se urmăreşte extinderea unui corp de bază la un corp în care un polinom are toate rădăcinile. Se ajunge în acest mod la noțiunea de corp de descompunere al unui polinom şi închidere algebrică. Pe de altă parte, se urmăreşte proprietatea elementelor unei extinderi de a fi rădăcini ale unor polinoame cu coeficienți în corpul de bază, degajându-se în acest mod noțiunile de element algebric şi element transcendent. Este pus în evidență

corpul numerelor algebrice (al elementelor algebrice ale extinderii $\mathbb{C} \supseteq \mathbb{Q}$) care face obiectul teoriei algebrice a numerelor.

Capitolul IV conține o scurtă sinteză privind grupurile rezolubile. Sunt analizate special grupurile de permutări pentru legătura pe care o au în capitolele următoare cu rezolvarea ecuațiilor prin radicali.

În capitolul V apar elementele de teorie Galois. Sunt stabilite condiții în care corespondența între laticea $\mathscr{L}(L;K)$ a corpurilor intermediare în extinderea $L \supseteq K$ şi laticea $\mathscr{L}(G)$ a subgrupurilor grupului Galois asociat este o bijecție. În acest context, sunt studiate: rădăcinile primitive ale unității, corpurile finite, extinderile algebrice normale şi extinderile algebrice separabile.

Următorul capitol cuprinde două aplicații importante ale teoriei Galois. Prima dintre acestea se referă la rezolvarea ecuațiilor algebrice prin radicali. Folosind teorema fundamentală a teoriei Galois, se stabilesc condiții necesare şi suficiente ca o ecuație algebrică să fie rezolvabilă prin radicali. În particular, se obține teorema lui Abel şi Ruffini privind nerezolubilitatea prin radicali a ecuației generale de grad $n \geq 5$. A doua aplicație se referă la stabilirea unor condiții necesare şi suficiente de constructibilitate cu rigla şi compasul. Se obține în acest mod un răspuns elegant la problemele clasice de constructibilitate.

Fiecare capitol este urmat de un număr însemnat de probleme care permit aprofundarea noțiunilor şi rezultatelor studiate. În ultima parte a cărții sunt date soluțiile acestor probleme.

Conținutul cărții acoperă programa disciplinei Algebră III din anul II al domeniului matematică. Cele două teme studiate – proprietățile aritmetice ale inelelor şi extinderile de corpuri – sunt strâns legate de programa de matematică din învățământul preuniversitar şi de aceea sunt esențiale în pregătirea viitorului profesor de matematică. Cartea poate constitui de asemenea un suport util pentru pregătirea examenelor de definitivat, de obținere a gradelor didactice sau de ocupare a unui post în învățământ.

Autorii

Capitolul I

INELE. NOŢIUNI GENERALE

1. Inele şi morfisme de inele

1.1. **Definiţie.** *Spunem că mulţimea nevidă A, înzestrată cu două legi de compoziţie internă, "*" şi "#" are o structură de* ***inel****, dacă:*

- $(A,*)$ *are o structură de grup abelian;*
- $(A,\#)$ *are o structură de semigrup;*
- *# este distributivă* (*la stânga şi la dreapta*) *faţă de *.*

În condiţiile definiţiei 1.1., spunem simplu $(A,*,\#)$ este un inel. Dacă nu se pot crea confuzii, operaţiile unui inel sunt notate + şi $\cdot$. Elementul neutru al grupului $(A,+)$ se notează cu 0. Simetricul unui element a în raport cu + se notează cu $-a$ şi se numeşte *opusul lui a.*

Dacă operaţia *"$\cdot$"* are element neutru, atunci acesta se numeşte *element unitate* şi se notează de obicei cu 1. În acest caz se spune că $(A,+,\cdot)$ este un *inel unitar.* Elementele simetrizabile în raport cu $\cdot$ într-un inel unitar se mai numesc *elemente inversabile* sau *unităţi.* Mulţimea unităţilor inelului unitar A se notează cu $U(A)$. Operaţia $\cdot$ induce pe $U(A)$ o structură de grup, numit ***grup multiplicativ al unităţilor inelului*** *A*.

Se spune că inelul A este *nenul* dacă are cel puţin două elemente. Se spune că inelul A este *comutativ* dacă $\cdot$ este comutativă.

În orice inel A, $a\cdot 0 = 0\cdot a = 0$, pentru orice a din A. Se spune că elementul a din A este *un divizor la stânga* (*dreapta*) *al lui zero* dacă există $b \in A \setminus \{0\}$, astfel încât $a\cdot b = 0$ (respectiv $b\cdot a = 0$). Elementul 0 este un divizor la stânga şi la dreapta al lui zero.

1.2. **Definiţie.** *Un inel comutativ, unitar, nenul şi fără divizori ai lui zero diferiţi de zero se numeşte* ***domeniu de integritate*** *sau* ***inel integru.***

Mulţimea $\mathbb{Z}$ a numerelor întregi este un domeniu de integritate în raport cu operaţiile obişnuite de adunare şi de înmulţire şi avem $U(\mathbb{Z})=\{-1,1\}$.

Mulţimea $\mathcal{M}_n(\mathbb{R})$ a matricelor cu *n* linii, *n* coloane şi elemente reale este un inel unitar, necomutativ şi cu divizori ai lui zero pentru $n>1$. Grupul multiplicativ al unităţilor acestui inel se notează cu $GL_n(\mathbb{R})$ şi se numeşte ***grup liniar general de grad n peste*** $\mathbb{R}$.

Se notează $\mathbb{Z}[i]=\{z\in\mathbb{C}\,|\,\exists\, m,n\in\mathbb{Z},\ z=m+ni\}$. Adunarea şi înmulţirea numerelor complexe induc pe $\mathbb{Z}[i]$ o structură de inel, cunoscut sub numele de ***inelul întregilor lui Gauss.*** Aplicaţia:

$$N:\mathbb{Z}[i]\to\mathbb{N},\ \ N(m+ni)=m^2+n^2$$

este numită ***normă***. Folosind relaţia $N(z_1z_2)=N(z_1)N(z_2)$ deducem că $U(\mathbb{Z}[i])=\{-1,1,-i,i\}$.

1.3. **Definiţie.** *Un inel K, unitar, nenul cu* $U(K)=K\setminus\{0\}$ *se numeşte* ***corp.***

Mulţimile $\mathbb{Q},\mathbb{R},\mathbb{C}$ au o structură de corp în raport cu operaţiile obişnuite de adunare şi de înmulţire.

1.4. **Definiţie.** *Fie A, B două inele în care operaţiile sunt notate* + *şi* $\cdot$. *O aplicaţie* $f:A\to B$ *se numeşte* ***morfism de inele*** *dacă pentru orice* $a,b\in A,$ *au loc relaţiile:*

$$f(a+b)=f(a)+f(b)$$
$$f(ab)=f(a)f(b).$$

Un morfism de inele este în particular un morfism al grupurilor aditive subiacente. Rezultă $f(0)=0$ şi $f(-a)=-f(a),\ \ \forall a\in A.$

Dacă $(A,+,\cdot)$ este un inel, atunci aplicaţia identică 1_A este un morfism de inele, numit ***morfismul identic.***

Dacă $f:A\to B$ şi $g:B\to C$ sunt morfisme de inele, atunci $g\circ f$ este un morfism de inele.

Se spune că morfismul de inele $f: A \to B$ este un ***izomorfism***, dacă există un morfism de inele $g: B \to A$, asfel încât, $g \circ f = 1_A$ şi $f \circ g = 1_B$.

Un morfism de inele este izomorfism dacă şi numai dacă este bijectiv.

Dacă *A, B* sunt inele unitare atunci se spune că morfismul de inele $f: A \to B$ este ***morfism unitar*** dacă $f(1) = 1$.

1.5. **Definiţie.** *Fie A un inel comutativ şi unitar. Fie* $\rho: A \to B$ *un morfism unitar de inele. Se spune că B este o* ***A-algebră de morfism structural*** ρ *dacă* $\rho(a)b = b\rho(a)$, *pentru orice* $a \in A$ *şi* $b \in B$.

Dacă *A* este un inel comutativ şi unitar, atunci $\mathcal{M}_n(A)$ este o *A* - algebră de morfism structural $\rho: A \to \mathcal{M}_n(A)$, $\rho(a) = aI_n$.

Fie *B, C* două *A* - algebre, de morfisme structurale $\rho: A \to B$ şi $\tau: A \to C$. Un ***morfism de A-algebre*** este un morfism unitar de inele $f: B \to C$ astfel încât, $\tau = f \circ \rho$.

2. Subinele şi ideale

2.1. **Definiţie.** *Fie* $(A, +, \cdot)$ *un inel şi* A' *o submulţime nevidă a lui A. Se spune că* A' *este un* ***subinel*** *al inelului A, dacă operaţiile lui A induc pe* A' *o structură de inel.*

Se verifică uşor că A' este subinel al lui *A* dacă şi numai dacă pentru orice $a, b \in A'$, $a - b \in A'$ şi $ab \in A'$.

În particular, dacă A' este un subinel al lui *A,* atunci A' este un subgrup al grupului $(A, +)$.

Subinelele inelului $(\mathbb{Z}, +, \cdot)$ al numerelor întregi sunt de forma $n\mathbb{Z}$ unde $n \in \mathbb{N}$.

Pentru orice inel *A,* $\{0\}$ şi A sunt subinele ale lui *A*.

Fie $f: A \to B$ un morfism de inele. Mulţimea:

$$\operatorname{Im} f = \left\{ b \in B \middle| \exists a \in A, f(a) = b \right\}$$

este un subinel al lui *B*, numit ***imaginea morfismului f.***

Mulțimea:

$$Kerf = \{a \in A \mid f(a) = 0\}$$

este un subinel al lui A numit ***nucleul morfismului f*.**

Dacă $A_i,\ i \in I,$ sunt subinele ale inelului A, atunci $\bigcap_{i \in I} A_i$ este un subinel al lui A.

Dacă M este o submulțime a inelului A, atunci intersecția tuturor subinelelor lui A care includ M se numeşte ***subinel generat de mulțimea*** M.

2.2. **Propoziție.** *Mulțimea* $\mathscr{S}(A)$ *a subinelelor inelului A formează o latice completă în raport cu relația de incluziune.*

Demonstrație. Fie $A_i,\ i \in I,$ o familie de subinele ale lui A.

$inf(A_i)_{i \in I} = \bigcap_{i \in I} A_i$ iar $sup(A_i)$ este subinelul generat de $\bigcup_{i \in I} A_i$. □

Se demonstrează uşor şi următorul rezultat:

2.3. **Propoziție.** *Fie* $f : A \to B$ *un morfism surjectiv de inele. Fie*

$$\mathscr{S}(A, Kerf) = \{A' \mid A' \text{este subinel al lui } A,\ A' \supseteq Kerf\}.$$

Atunci aplicația:

$$F : \mathscr{S}(A, Kerf) \to \mathscr{S}(B)$$

definită prin $F(A') = f(A'),$ *pentru orice* $A' \in \mathscr{S}(A, Kerf),$ *este un izomorfism de mulțimi ordonate.*

2.4. **Definiție.** *Fie* $(A, +, \cdot)$ *un inel şi I o submulțime nevidă a lui A. Se spune că I este un* ***ideal stâng*** *al lui A, dacă*:

1) $a - b \in I,$ *pentru orice* $a, b \in I,$

2) $xa \in I,$ *pentru orice* $x \in A,$ *şi orice* $a \in I.$

Dacă I satisface condiția 1) *şi condiția:*

3) $ax \in I,$ *pentru orice* $a \in I$ şi $x \in A,$

atunci se spune că I este un ***ideal drept*** *al lui A.*

Un ideal stâng care este şi ideal drept se numeşte ***ideal bilateral.***

Într-un inel comutativ, noțiunile de ideal stâng, ideal drept şi ideal bilateral coincid. În acest caz se spune simplu, ideal.

Idealele inelului $(\mathbb{Z}, +, \cdot)$ sunt de forma $n\mathbb{Z}$ unde $n \in \mathbb{N}$.

Se observă că orice ideal (stâng sau drept) este şi un subinel.

Reciproca nu este adevărată. Mulțimea matricelor din $\mathcal{M}_n(\mathbb{R})$ care au 0 pe prima linie este un subinel al lui $(\mathcal{M}_n(\mathbb{R}),+,\cdot)$ dar nu este un ideal stâng.

Pentru orice inel *A,* mulțimile $\{0\}$ şi *A* sunt ideale bilaterale ale lui *A*, numite ***ideale improprii.*** Celelalte ideale se numesc ***ideale proprii.***

Dacă $f: A \to B$ este un morfism de inele, atunci *Kerf* este un ideal bilateral al lui *A*. Morfismul f este injectiv, dacă şi numai dacă $Kerf = \{0\}$.

Dacă $(K,+,\cdot)$ este un corp, atunci *K* nu are ideale proprii.

Reciproc, *dacă* $(A,+,\cdot)$ *este un inel unitar nenul, în care singurele ideale stângi şi drepte sunt* $\{0\}$ *şi A, atunci A este corp.*

Prin ***morfism de corpuri*** se înțelege un morfism unitar al inelelor subiacente.

Orice morfism de corpuri $f: K \to L$ *este injectiv.* Într-adevăr, *Kerf* este un ideal al lui *K*. Din $f(1) = 1 \neq 0$ rezultă $Kerf \neq K$, deci $Kerf = \{0\}$ şi f este injectiv.

Se deduce uşor că intersecția unei familii de ideale stângi (drepte sau bilaterale) este un ideal stâng (drept sau bilateral).

Dacă *M* este o submulțime a inelului *A,* atunci intersecția idealelor stângi (drepte sau bilaterale) ale lui *A* care includ *M* se numeşte ***ideal stâng*** (***drept*** sau ***bilateral***) ***generat de mulțimea*** *M.*

Un ideal stâng (drept sau bilateral) generat de un singur element se numeşte ***ideal principal.***

Toate idealele inelului ***Z*** sunt ideale principale.

Notăm cu $\mathcal{L}_s(A)$, ($\mathcal{L}_d(A)$, $\mathcal{L}(A)$) mulțimea idealelor stângi (drepte sau bilaterale) ale inelului *A*.

2.5. **Propoziție.** *Pentru orice inel A, mulțimile* $\mathcal{L}_s(A)$, ($\mathcal{L}_d(A)$, $\mathcal{L}(A)$) *sunt latice complete în raport cu relația de incluziune.*

Demonstrația este analoagă celei de la propoziția 2.2.

Dacă $\{I_t\}_{t\in T}$ este o mulțime de ideale stângi ale inelului *A,* atunci idealul stâng generat de $\bigcup_{t\in T} I_t$ se numeşte ***suma idealelor*** stângi $\{I_t\}_{t\in T}$ şi se notează $\sum_{t\in T} I_t$. Asemănător se defineşte suma unei mulțimi de ideale drepte sau bilaterale.

Dacă $T=\{1,2\}$, atunci $I_1+I_2=\{a+b|a\in I_1, b\in I_2\}$.

Fie *I* şi *J* două ideale stângi (drepte sau bilaterale) ale inelului *A*. În general, mulțimea $M=\{ab|a\in I, b\in J\}$ nu este un ideal stâng (drept sau bilateral) al lui *A*. Prin ***produs*** al ***idealelor*** stângi (drepte sau bilaterale) *I* şi *J* se înțelege idealul stâng (drept sau bilateral) generat de mulțimea *M.*

2.6. **Propoziție.** *Fie* $f: A\to B$ *un morfism surjectiv de inele şi*

$$\mathcal{L}(A, Kerf)=\{I|I \text{ ideal bilateral al lui A, } I\supseteq Kerf\}.$$

Atunci aplicația

$$F: \mathcal{L}(A, Kerf)\to \mathcal{L}(B)$$

definită prin $F(I)=f(I)$, *pentru orice I din* $\mathcal{L}(A, Kerf)$, *este un izomorfism de mulțimi ordonate.*

Demonstrația este analoagă celei de la propoziția 2.3.

3. Inel factor. Teoremele de izomorfism

Fie $(A,+,\cdot)$ un inel şi *I* un ideal bilateral al său. În particular, *I* este un subgrup normal al lui $(A,+,\cdot)$. Putem vorbi despre grupul factor $A/I=\{\hat{x}|x\in A\}$, $\hat{x}=x+I=\{x+h|h\in I\}$.

Dacă $x'\in\hat{x}$ şi $y'\in\hat{y}$, atunci există $h,k\in I$ aşa încât $x'=x+h$, $y'=y+k$. Rezultă:

$$x'y'=xy+hy+xk+hk=xy+l\in xy+I$$

deoarece $l\in I$. Rezultă că aplicația:

$$A/I\times A/I\to A/I,\ (\hat{x},\hat{y})\to \hat{x}\hat{y}=\widehat{xy}$$

este bine definită**.** Se verifică uşor că $(A/I,+,\cdot)$ este un inel. Acest inel poartă numele de ***inel factor*** al inelului A prin idealul său bilateral I. Elementul neutru al lui A/I este $\hat{0}=I$. Aplicaţia canonică

$$\pi : A \to A/I$$

definită prin $\pi(x)=\hat{x},$ pentru orice $x\in A$ este un morfism surjectiv de inele al cărui nucleu este $Ker\pi = I$.

Dacă A este inel unitar, atunci A/I este inel unitar şi $\hat{1}$ este elementul unitate. Dacă A este inel comutativ, atunci A/I este inel comutativ.

Pentru $A=\mathbb{Z}$ şi $I=n\mathbb{Z},$ inelul factor $\mathbb{Z}/n\mathbb{Z}$ se notează $\mathbb{Z}_n$ şi se numeşte ***inelul claselor de resturi modulo n.***

3.1. **Teorema fundamentală de izomorfism.** *Dacă* $f : A \to B$ *este un morfism de inele, atunci există un izomorfism*

$$\theta : A/Kerf \to Im f\ .$$

Demonstraţie. Kerf este ideal bilateral în A. Dacă $y\in x+Kerf$, atunci există $h\in Kerf$, astfel încât $y=x+h.$

$$f(y)=f(x)+f(h)=f(x).$$

Prin urmare, $\theta : A/Kerf \to Im f,\ \ \theta(\hat{x})=f(x),\ \ \forall x\in A,$ este bine definită. Se verifică uşor că θ este un morfism surjectiv de inele. Dacă $\hat{x}\in Ker\theta,$ atunci $\theta(\hat{x})=f(x)=0,$ deci $x\in Kerf$ şi $\hat{x}=\hat{0}.$ Prin urmare, θ este şi morfism injectiv, deci este izomorfism. □

3.2. **Teorema a doua de izomorfism.** *Fie* $(A,+,\cdot)$ *un inel,* A' *un subinel şi I un ideal bilateral al lui A. Atunci:*

a) $A'+I=\{a+h \mid a\in A', h\in I\}$ *este un subinel al lui A*;

b) $A'\cap I$ *este un ideal bilateral al lui* A';

c) *Există un izomorfism*

$$\theta : A'/(A'\cap I) \to (A'+I)/I\ .$$

Demonstraţie. Afirmaţia a) se verifică prin calcul direct. b) Este evident că I este şi ideal bilateral al lui $A'+I$.

Fie $f: A' \to (A'+I)/I$, $f(x) = x + I$, pentru orice $x \in A'$. Se verifică uşor că f este un morfism de inele. $\forall \hat{y} \in (A'+I)/I$, $\exists x \in A'$ şi $h \in I$ astfel încât $y = x + h$. Rezultă $\hat{y} = \hat{x} + \hat{h} = \hat{x} = f(x)$. Deci f este un morfism surjectiv şi $Im f = (A'+I)/I$. Dacă $x \in Kerf$, atunci $x \in A'$ şi $\hat{x} = \hat{0} = I$, deci $x \in A' \cap I$. Rezultă $Kerf = A' \cap I$ şi prin urmare $A' \cap I$ este un ideal bilateral al lui A'. Pentru c) se aplică teorema fundamentală de izomorfism lui f. □

3.3. **Teorema corespondenței.** *Fie $f: A \to B$ un morfism surjectiv de inele. Aplicația*:

$$F: \mathscr{L}(A, Kerf) \to \mathscr{L}(B),\ F(I) = f(I),\ \forall I \in \mathscr{L}(A, Kerf),$$

este un izomorfism de mulțimi ordonate.

În plus, dacă $I \in \mathscr{L}(A, Kerf)$ şi $J = f(I)$, atunci $A/I \simeq B/J$.

Demonstrație. Notațiile sunt cele din propoziția 2.6. Prima parte a teoremei rezultă chiar din 2.6. Pentru partea a doua, fie I un ideal din $\mathscr{L}(A, Kerf)$ şi $J = F(I)$. Fie

$$g: A \to B/J,\ g(x) = f(x) + J,\ \forall x \in A.$$

g este un morfism surjectiv de inele şi $Kerg = I$. În continuare se aplică morfismului g teorema fundamentală de izomorfism. □

3.4. **Teorema a treia de izomorfism.** *Fie $(A, +, \cdot)$ un inel oarecare şi I, J două ideale bilaterale ale lui A, $I \subseteq J$. Atunci J/I este un ideal bilateral al lui A/I şi există un izomorfism:*

$$(A/I)/(J/I) \simeq A/J.$$

Demonstrație. Fie $\pi: A \to A/I$ surjecția canonică. $Ker\pi = I$ de unde, $J \in \mathscr{L}(A, Ker\pi)$. Aplicând teorema 3.3., $F(J) = \pi(J) = J/I$ este un ideal bilateral al lui A/I şi $A/J \simeq (A/I)/(J/I)$. □

3.5. **Aplicație.** *Fie $n \in \mathbb{N}^*$. Să se determine idealele şi inelele factor ale lui $\mathbb{Z}_n$.*

Fie $\pi:\mathbb{Z}\to\mathbb{Z}_n$ surjecția canonică. Dacă J este un ideal în $\mathbb{Z}_n$, din 3.3., $J=\pi(I)$ unde I este un ideal al lui $\mathbb{Z}$ şi $I\supseteq Ker\pi=n\mathbb{Z}$. Deci $I=m\mathbb{Z}$ şi $m\mid n$. $J=\pi(I)=(m\mathbb{Z})/(n\mathbb{Z})$.

Conform 3.4., $\mathbb{Z}_n/J=(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z})\simeq\mathbb{Z}/m\mathbb{Z}=\mathbb{Z}_m$.

3.6. **Propoziție.** *În inelul* $\mathbb{Z}_n$, $n>1$:

$$U(\mathbb{Z}_n)=\left\{\hat{x}\,\middle|\,(x,n)=1\right\}.$$

Demonstrație. Dacă $\hat{x}\in U(\mathbb{Z}_n)$, atunci există $\hat{y}\in\mathbb{Z}_n$ astfel încât $\hat{x}\cdot\hat{y}=\hat{1}$. Rezultă $xy-1\in n\mathbb{Z}$, sau $\exists h\in\mathbb{Z}$, astfel încât $xy-1=nh$.

$$\text{Din } xy-nh=1, \text{ rezultă } (x,n)=1.$$

Reciproc, fie $x\in\mathbb{Z}$, astfel încât $(x,n)=1$. Există $u,v\in\mathbb{Z}$, astfel încât $ux+vn=1$. Rezultă $\hat{x}\cdot\hat{u}=\hat{1}$ şi $\hat{x}\in U(\mathbb{Z}_n)$. □

3.7**. Consecință.** *Fie* $n>1$. *Atunci* $\left|U(\mathbb{Z}_n)\right|=\varphi(n)$.

Demonstrație. Funcția φ este indicatorul lui Euler şi notează numărul numerelor naturale mai mici decât n şi prime cu n. Se aplică propoziția 3.6. □

3.8. **Teorema lui Euler.** Fie $n\in\mathbb{N}^*$ şi $a\in\mathbb{Z}$, $(n,a)=1$. Atunci:

(1) $$a^{\varphi(n)}\equiv 1(\bmod n).$$

Demonstrație. Din 3.6. rezultă $\hat{a}\in U(\mathbb{Z}_n)$. $(U(\mathbb{Z}_n),\cdot)$ este grup cu $\varphi(n)$ elemente. Rezultă $\hat{a}^{\varphi(n)}=\hat{1}$, ceea ce este tot una cu (1). □

3.9. **Mica teoremă a lui Fermat.** *Dacă p este un număr prim şi a este un număr întreg nedivizibil cu p, atunci:*

$$a^{p-1}\equiv 1(\bmod p).$$

Demonstrație. Se aplică 3.8. ținând seama că $\varphi(p)=p-1$. □

4. Caracteristica unui inel

Fie $(A,+,\cdot)$ un inel unitar al cărui element unitate îl notăm cu e. Aplicația

$$\rho:\mathbb{Z}\to A,\ \ \rho(m)=me,\ \ \forall m\in\mathbb{Z},$$

este un morfism unitar de inele. $Ker\rho$ este un ideal în $\mathbb{Z}$. Există $n\in\mathbb{N}$, astfel încât $Ker\rho=n\mathbb{Z}$. Numărul n poartă numele de ***caracteristică*** a inelului A şi se notează $carA$.

Apar două situații.

I. Morfismul ρ este injectiv. În acest caz, $Ker\rho=\{0\}$. Deci

(1) $$carA=0\Leftrightarrow\left(\forall m\in\mathbb{Z},\ me=0\Rightarrow m=0\right)$$

Inelul A conține în acest caz un subinel $Im\rho$ izomorf cu $\mathbb{Z}$ care poate fi identificat cu $\mathbb{Z}$. Însuşi inelul $\mathbb{Z}$ al numerelor întregi are caracteristica egală cu zero.

II. Morfismul ρ nu este injectiv. $Ker\rho=n\mathbb{Z}$ şi $n\in\mathbb{N}^*$. Inelul A are o caracteristică nenulă.

(2) $$carA=n\neq 0\Leftrightarrow n=\min\left\{m\in\mathbb{N}^*\,\middle|\,me=0\right\}.$$

Aplicând teorema fundamentală de izomorfism pentru inele,

$$\mathbb{Z}_n=\mathbb{Z}/Ker\rho\simeq Im\rho\subseteq A.$$

Inelul A conține un subinel izomorf cu inelul $\mathbb{Z}_n$ al claselor de resturi modulo n.

Însuşi inelul $\mathbb{Z}_n$ ($n\neq 0$) are caracteristica egală cu n.

4.1. **Propoziție.** *Dacă A este un domeniu de integritate cu caracteristică nenulă, atunci $carA$ este un număr prim.*

Demonstrație. Fie $carA=n\neq 0$. Să presupunem că există p şi q numere naturale, astfel încât $n=pq,\ 1<p<n$.

$$ne=0\Leftrightarrow(pe)(qe)=0\Leftrightarrow pe=0 \text{ sau } qe=0,$$

contradicție cu (2). Prin urmare, n este număr prim. □

Să considerăm acum K un corp comutativ. În particular, K este un domeniu de integritate.

În cazul $carK=0$, K conține un subinel izomorf cu $\mathbb{Z}$:

$$\{me \mid m \in \mathbb{Z}\}.$$

K fiind corp, va conține şi mulțimea elementelor de forma

$$\{(me)(ne)^{-1} \mid m,n \in \mathbb{Z},\ n \neq 0\}.$$

care formează un subcorp izomorf cu $\mathbb{Q}$. Deci:

Orice corp de caracteristică 0 *include un subcorp izomorf cu* $\mathbb{Q}$.

În cazul $carK = p \neq 0$, p este număr prim şi $Im\rho \simeq \mathbb{Z}_p$ este corp. Deci:

Orice corp de caracteristică nenulă p include un subcorp izomorf cu $\mathbb{Z}_p$.

Corpurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(X)$ au caracteristica 0.

Corpul $\mathbb{Z}_p$ cu *p* număr prim are caracteristica *p.*

5. Ideale prime şi ideale maximale

Acest paragraf este consacrat studiului a două tipuri de ideale importante în teoria inelelor.

5.1. **Definiție.** *Fie A un inel comutativ şi unitar iar P un ideal al său, diferit de A. Spunem că P este un* ***ideal prim*****,** *dacă:*

$$\forall a,b \in A,\ \ ab \in P \Rightarrow a \in P \ \ sau \ \ b \in P.$$

În inelul întregilor raționali, $(2) = 2\mathbb{Z}$ este un ideal prim deoarece, dacă produsul a două numere întregi este un număr par, atunci cel puțin unul dintre cele două numere este par.

Într-un inel integru *A*, idealul (0) este prim deoarece *A* nu are divizori ai lui zero diferiți de 0. Este adevărată şi reciproca: dacă în inelul comutativ, unitar, nenul *A,* idealul (0) este ideal prim, atunci *A* este inel integru.

5.2. **Propoziție.** *Fie A un inel comutativ unitar şi P un ideal al său, diferit de A. P este ideal prim al lui A, dacă şi numai dacă, pentru orice două ideale I şi J ale lui A :*

$$IJ \subseteq P \Rightarrow I \subseteq P \ \ sau \ \ J \subseteq P.$$

Demonstrație. "$\Rightarrow$" Fie *P* un ideal prim al lui *A* şi *I, J* ideale ale lui *A,* astfel încât $IJ \subseteq P$. Prin reducere la absurd, să presupunem că niciunul dintre idealele *I* şi *J* nu este inclus în *P* . Există $a \in I \setminus P$ şi

$b \in J \setminus P$. Din $ab \in IJ \subseteq P$ şi P ideal prim, rezultă $a \in P$ sau $b \in P$, contradicţie.

"$\Leftarrow$" Fie $a,b \in A$ astfel încât $ab \in P$. Notăm $I = (a)$ şi $J = (b)$. $IJ = (ab) \subseteq P$. Rezultă $I \subseteq P$ sau $J \subseteq P$, deci $a \in P$ sau $b \in P$. P este ideal prim. □

Propoziţia următoare arată cum se comportă idealele prime în raport cu imaginile directe şi reciproce prin morfisme.

5.3. **Propoziţie.** *Fie A, B două inele comutative unitare şi $f : A \to B$ un morfism unitar. Atunci:*

a) *Dacă P' este ideal prim în B, atunci $P = f^{-1}(P')$ este ideal prim în A;*

b) *Dacă f este morfism surjectiv, P este ideal prim în A şi $P \supseteq Kerf$, atunci $P' = f(P)$ este ideal prim în B.*

Demonstraţie. a) $P = f^{-1}(P') = \{a \in A \mid f(a) \in P'\}$. Deoarece f este morfism de inele şi P' este ideal în B, rezultă că P este ideal în A. Să presupunem $P = A$. Atunci $1 \in P$, $f(1) = 1 \in P'$, adică $P' = B$, contradicţie. Fie $a,b \in A$ cu $ab \in P$. Rezultă $f(ab) = f(a)f(b) \in P'$. Deoarece P' este ideal prim, $f(a) \in P'$ sau $f(b) \in P'$. Deci $a \in P$ sau $b \in P$. P este ideal prim în A.

b) $P' = f(P) = \{f(a) \mid a \in P\}$. Deoarece f este morfism surjectiv şi P este ideal în A, P' este ideal în B. Vom presupune că $P' = B$. Rezultă $1 \in P'$. Atunci există $a \in P$ astfel încât $f(a) = 1 = f(1)$. Se obţine: $f(a-1) = 0$, $a - 1 = c \in Kerf \subseteq P$, $1 = a - c \in P$ şi $P = A$, contradicţie. Deci $P' \neq B$.

Fie $x, y \in B$, astfel încât $xy \in P'$. Deoarece f este morfism surjectiv, există $a,b \in A$, astfel încât $x = f(a)$, $y = f(b)$. Atunci,

$$xy = f(a)f(b) = f(ab).$$

Există de asemenea $c \in P$, astfel încât $xy = f(c)$.

$$f(ab) = f(c) \Rightarrow ab - c = h \in Kerf \subseteq P \Rightarrow ab = h + c \in P.$$

Deoarece P este ideal prim în A, rezultă $a \in P$, deci $x = f(a) \in P'$, sau $b \in P$, deci $y = f(b) \in P'$. P' este ideal prim în B. □

5.4. **Consecință.** *Fie A un inel comutativ unitar şi P un ideal al lui A. Sunt echivalente condițiile:*

a) *P este ideal prim în A*;

b) A/P *este inel integru.*

Demonstrație. Fie $\pi : A \to A/P$ surjecția canonică. π este morfism surjectiv şi $Ker\pi = P$. Conform 5.3., *P* este ideal prim în *A* dacă şi numai dacă $(\hat{0})$ este ideal prim în A/P. Ultima condiție este echivalentă cu A/P este inel integru. □

5.5. **Definiție.** *Fie A un inel comutativ unitar şi M un ideal al lui A, diferit de A. Se spune că M este* ***ideal maximal*** *al lui A dacă pentru orice ideal I al lui A*:

$$M \subseteq I \Rightarrow M = I \text{ sau } I = A.$$

Cu alte cuvinte, un ideal maximal este un element maximal în mulțimea idealelor lui *A*, diferite de *A* (în raport cu relația $\subseteq$).

Un corp comutativ *K* nu are decât idealele (0) şi *K*. Deci (0) este ideal maximal. Reciproc, dacă într-un inel comutativ unitar *K*, (0) este ideal maximal, atunci *K* este corp.

5.6. **Propoziție.** *Fie A, B inele comutative unitare şi* $f : A \to B$ *un morfism unitar surjectiv. Atunci:*

a) *Dacă M este un ideal maximal al lui A şi* $M \supseteq Kerf$, *atunci* $f(M)$ *este ideal maximal în B;*

b) *Dacă* M' *este ideal maximal în B, atunci* $f^{-1}(M')$ *este ideal maximal în A.*

Demonstrație. Cu notațiile din teorema 3.3., aplicația

$$F : \mathcal{L}(A, Kerf) \to \mathcal{L}(B),\ F(I) = f(I),$$

este un izomorfism de mulțimi ordonate. Prin acest izomorfism, elementele maximale ale mulțimilor $\mathcal{L}(A, Kerf) \setminus \{A\}$ şi $\mathcal{L}(B) \setminus \{B\}$ se corespund. □

5.7. **Consecință.** *Fie A un inel comutativ unitar şi M un ideal al lui A . Sunt echivalente condițiile:*

a) *M este ideal maximal în A*;

b) A/M *este corp.*

Demonstrație. Fie $\pi : A \to A/M$ surjecția canonică. π este morfism surjectiv şi $Ker\pi = M$. Conform 5.6., *M* este maximal în *A*, da-

că şi numai dacă $(\hat{0})$ este ideal maximal în A/M. Ultima afirmaţie este echivalentă cu A/M este corp. □

5.8. **Consecinţă.** *Fie A un inel comutativ unitar şi M un ideal maximal al lui A. Atunci, M este ideal prim în A.*

Demonstraţie. Din M ideal maximal în A, rezultă A/M corp, deci A/M este inel integru şi ca urmare M este ideal prim. □

Să observăm că reciproca pentru 5.8. nu este adevărată. Astfel, (0) este ideal prim în inelul $\mathbb{Z}$ dar nu este ideal maximal.

6. Existenţa idealelor maximale

Scopul acestui paragraf este acela de a demonstra că în orice inel comutativ, unitar, nenul există ideale maximale. Reamintim că mulţimea ordonată $(M,\leq)$ este ***inductivă*** dacă orice parte a sa nevidă, total ordonată este majorată. În demonstraţie este necesară următoarea axiomă, numită în teoria mulţimilor, ***Lema lui Zorn:***

Orice mulţime ordonată, inductivă are elemente maximale.

6.1. **Teoremă (Lema lui Krull).** *Fie A un inel comutativ unitar şi I un ideal al lui A, diferit de A. Atunci există un ideal maximal M al lui A, astfel încât* $M \supseteq I$.

Demonstraţie. Notăm $\mathscr{P} = \{J \mid J \text{ ideal al lui } A,\ J \supseteq I,\ J \neq A\}$.

$\mathscr{P}$ este nevidă deoarece $I \in \mathscr{P}$. Afirmăm că $\mathscr{P}$ este inductivă în raport cu relaţia $\subseteq$.

Fie $\{I_t\}_{t\in T}$ o parte nevidă a lui $\mathscr{P}$, total ordonată.

Notăm $I' = \bigcup_{t\in T} I_t$. Se arată uşor că I' este ideal al lui A. Evident $I' \supseteq I$. Dacă $I' = A$, atunci există $t \in T$ astfel încât $1 \in I_t$. Rezultă că $I_t = A$, contradicţie. Prin urmare, $I' \neq A$, şi $I' \in \mathscr{P}$.

Evident, I' este un majorant pentru $\{I_t\}_{t\in T}$ şi ca urmare $\mathscr{P}$ este inductivă. Conform lemei lui Zorn, în $\mathscr{P}$ există elemente maximale. Fie $M \in \mathscr{P}$ un element maximal. M este un ideal în A, diferit de A şi $M \supseteq I$.

Fie H un ideal al lui A, astfel încât $H \supseteq M$. Dacă $H \neq A$, atunci $H \in \mathscr{P}$ şi cum M este maximal în $\mathscr{P}$ rezultă $H = M$. Deci M este ideal maximal în A. □

6.2. **Consecinţă.** *Fie A un inel comutativ, unitar, nenul. Atunci în A există ideale maximale.*

Demonstraţie. În teorema 6.1. se ia $I = \{0\}$. □

7. Inele şi corpuri de fracţii

În acest paragraf se urmăreşte ca, pentru un inel dat A, să se construiască o "extindere" în care anumite elemente din A să devină elemente inversabile. Extinderea se realizează cu ajutorul noţiunii de *A - algebră.* Dacă B este o A - algebră de morfism structural injectiv $\rho : A \to B$, atunci $A \simeq Im\,\rho$ şi A poate fi privit ca un subinel al lui B.

Să considerăm mai întâi K un corp comutativ şi $a, b \in K$, $b \neq 0$. Ecuaţia $bx = a$ are în K o singură soluţie şi anume $x = ab^{-1}$. Prin analogie cu notaţia folosită pentru numere raţionale, o expresie de forma ab^{-1} o vom nota cu a/b şi o vom numi *fracţie*. Pe a îl vom numi *numărător*, iar pe b îl vom numi *numitor*. Două fracţii a/b şi c/d sunt egale dacă şi numai dacă $ab^{-1} = cd^{-1}$, adică $ad = bc$. Ţinând seama de proprietăţile operaţiilor din K, să deducem regulile de calcul cu fracţii:

$$a/b + c/d = ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1} = (ad + bc)/(bd)$$

$$a/b \cdot c/d = (ab^{-1})(cd^{-1}) = (ac)(bd)^{-1} = (ac)/(bd)$$

Remarcăm că se pot considera fracţii $a/b = ab^{-1}$ cu păstrarea regulilor de calcul şi în cazul în care a, b sunt elemente ale unui inel comutativ şi unitar R şi $b \in U(R)$. În particular, b nu poate fi un divizor al lui zero.

Pornind de la aceste observaţii, fiind dat un inel comutativ şi unitar R vom căuta să construim o extindere a lui R în care elementele anumitei submulţimi S să fie inversabile.

7.1. **Definiţie.** *Fie R un inel comutativ şi unitar şi S o submulţime a sa. Se spune că S este un* ***sistem multiplicativ*** *dacă operaţia multiplicativă a lui R induce pe S o structură de monoid.*

Cu alte cuvinte, *S* este un sistem multiplicativ al lui *R* dacă:

- $1 \in S$;
- $s,t \in S \Rightarrow st \in S$.

Mulţimea numerelor întregi impare este un sistem multiplicativ al lui $\mathbb{Z}$. În acelaşi inel, mulţimea puterilor pozitive ale lui 2 este un sistem multiplicativ.

Mulţimea tuturor nondivizorilor lui zero din inelul comutativ şi unitar *R* este un sistem multiplicativ.

7.2. **Teoremă (*de existenţă a inelelor de fracţii*)**. *Fie R un inel comutativ şi unitar şi S un sistem multiplicativ al său format din nondivizori ai lui zero. Există o R-algebră R_S, de morfism structural injectiv $\rho : R \to R_S$, astfel încât:*

a) $\forall s \in S, \rho(s) \in U(R_S)$;

b) $\forall \alpha \in R_S, \exists a \in R, \exists s \in S,$ astfel încât $\alpha = \rho(a) \cdot \rho(s)^{-1}$.

Demonstraţie. Pe produsul cartezian $R \times S$ definim următoarea relaţie :

$$(a,s) \sim (b,t) \text{ dacă şi numai dacă } at = bs.$$

Relaţia $\sim$ este o relaţie de echivalenţă. Deoarece proprietatea de reflexivitate şi cea de simetrie sunt imediate, vom verifica numai proprietatea de tranzitivitate. Fie $(a,s),(b,t),(c,u) \in R \times S$ astfel încât $(a,s) \sim (b,t)$ şi $(b,t) \sim (c,u)$. Din relaţiile $at = bs$ şi $bu = ct$ rezultă $atu = bsu = cst$. Deoarece t nu este divizor al lui zero, se obţine $au = cs$, sau, $(a,s) \sim (c,u)$.

Clasa de echivalenţă a perechii (a,s) o vom nota a/s şi o vom numi ***fracţie***. Prin urmare

$$\frac{a}{s} = \widehat{(a,s)} = \{(b,t) \mid (a,s) \sim (b,t)\}.$$

Se observă că pentru orice $a \in R$ şi $s,t \in S$, $\frac{a}{s} = \frac{at}{st}$.

Mulţimea factor (a claselor de echivalenţă) o vom nota R_S :

$$R_S = \left\{ \frac{a}{s} \middle| a \in R,\ s \in S \right\}.$$

După modelul operațiilor cu fracții într-un corp comutativ, definim, pentru $\frac{a}{s}$ și $\frac{b}{t} \in R_S$:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},\ \ \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Deoarece S este sistem multiplicativ, din $s, t \in S$ rezultă $st \in S$.

Să demonstrăm mai întâi că operațiile sunt bine definite.

Fie $(a_1, s_1) \sim (a, s)$ și $(b_1, t_1) \sim (b, t)$. Deducem :

$$as_1 = a_1 s, \qquad bt_1 = b_1 t$$
$$as_1 tt_1 = a_1 stt_1, \qquad bt_1 ss_1 = b_1 tss_1$$
$$(at + bs)s_1 t_1 = (a_1 t_1 + b_1 s_1)st$$
$$(at + bs, st) \sim (a_1 t_1 + b_1 s_1, s_1 t_1)$$

adică operația aditivă este bine definită. În mod analog se arată că operația multiplicativă este bine definită.

Să verificăm asociativitatea operației aditive pe R_S.

Fie $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in R_S$.

$$\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} = \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right) \Leftrightarrow \frac{at + bs}{st} + \frac{c}{u} = \frac{a}{s} + \frac{bu + ct}{tu} \Leftrightarrow$$
$$\Leftrightarrow \frac{(at + bs)u + cst}{stu} = \frac{atu + (bu + ct)s}{stu} \Leftrightarrow$$
$$\Leftrightarrow \left[(at + bs)u + cts\right] stu = \left[atu + (bu + ct)s\right] stu.$$

Ultima egalitate rezultă din proprietățile operațiilor pe R.

Prin calcul se deduce că $(R_S, +)$ este un grup abelian în care elementul neutru este $\frac{0}{1}$ iar opusa fracției $\frac{a}{s}$ este $(-a)/s$.

Tot prin calcul se deduce că $(R_S,\cdot)$ este un monoid comutativ în care $\frac{1}{1}$ este elementul unitate. Să verificăm distributivitatea operației multiplicative față de cea aditivă. Pentru $\frac{a}{s},\frac{b}{t},\frac{c}{u}\in R_S$:

$$\left(\frac{a}{s}+\frac{b}{t}\right)\frac{c}{u}=\frac{a}{s}\cdot\frac{c}{u}+\frac{b}{t}\cdot\frac{c}{u}\Leftrightarrow\frac{at+bs}{st}\cdot\frac{c}{u}=\frac{actu+bcsu}{stu^2}\Leftrightarrow$$

$$\frac{(at+bs)c}{stu}=\frac{actu+bcsu}{stu^2}\Leftrightarrow(at+bs)c\cdot stu^2=(actu+bcsu)stu\,.$$

Ultima egalitate rezultă din proprietățile operațiilor pe R .

Prin urmare R_S are o structură de inel comutativ şi unitar în raport cu operațiile + şi $\cdot$.

Fie $\rho:R\to R_S$, $\rho(a)=\frac{a}{1}$. Se arată uşor că ρ este un morfism unitar şi injectiv de inele. Deoarece R_S este comutativ, rezultă imediat că R_S este o R-algebră în raport cu morfismul ρ.

Fie $s\in S$. $\rho(s)=\frac{s}{1}$, $\frac{1}{s}\in R_S$ şi $\frac{s}{1}\cdot\frac{1}{s}=\frac{s}{s}=\frac{1}{1}$. Deci $\rho(s)\in U(R_S)$ şi $\rho(s)^{-1}=\frac{1}{s}$, adică se verifică a). Fie $\frac{a}{s}\in R_S$. b) rezultă din relația:

$$\frac{a}{s}=\frac{a}{1}\cdot\frac{1}{s}=\rho(a)\cdot\rho(s)^{-1}.\qquad\square$$

Deoarece morfismul ρ din teorema 7.2. este injectiv, rezultă că $R\simeq Im\,\rho$. Prin acest izomorfism identificăm fiecare element $a\in R$ cu imaginea sa $\rho(a)=\frac{a}{1}$. Prin această identificare, pentru $a\in R$ şi $s\in S$:

$$s^{-1}=\left(\frac{s}{1}\right)^{-1}=\frac{1}{s},\ \frac{a}{s}=\frac{a}{1}\cdot\frac{1}{s}=a\cdot s^{-1}$$

Inelul R_S din teorema 7.2. poartă numele de ***inel de fracții al inelului*** *R*, ***cu numitori în*** *S* şi se mai notează şi $S^{-1}R$.

Dacă S este mulțimea tuturor nondivizorilor lui zero din R, atunci R_S se numește ***inel total de fracții*** al lui R.

Fie acum R un domeniu de integritate și $S = R \setminus \{0\}$. Considerăm $\frac{a}{s} \in R_S \setminus \{0\}$; atunci $a \neq 0$ și $\frac{s}{a} \in R_S$. Din $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{1}{1} = 1$ rezultă că $\frac{a}{s} \in U(R_S)$. Prin urmare R_S este un corp, numit ***corp de fracții al domeniului de integritate*** R.

În particular, corpul de fracții al lui $\mathbb{Z}$ este corpul $\mathbb{Q}$ al numerelor raționale.

Dacă se consideră un corp comutativ K, atunci corpul de fracții al domeniului de integritate $K[X]$ se notează $K(X)$ și se numește ***corp al fracțiilor raționale cu coeficienții în*** K, ***în nedeterminata*** X.

$$K(X) = \left\{ \frac{f}{g} \mid f, g \in K[X],\ g \neq 0 \right\}$$

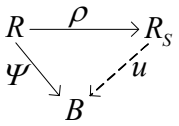
Operațiile + și $\cdot$ în $K(X)$ sunt definite ca în orice inel de fracții.

7.3. **Observație.** Fie K un corp comutativ, $S = K^*$, $\rho : K \to K_S$, $\rho(a) = \frac{a}{1}$. Pentru orice $\frac{a}{s} \in K_S$, $\frac{a}{s} = \frac{as^{-1}}{1} = \rho(as^{-1})$. Deci ρ este un izomorfism. Prin urmare, corpul de fracții al unui corp comutativ este izomorf cu corpul inițial.

7.4. **Teoremă (*Proprietatea de universalitate a inelelor de fracții*).** *Fie R un inel comutativ și unitar, S un sistem multiplicativ al său format din nondivizori ai lui zero. Atunci*:

(*) *Dacă B este o R-algebră de morfism structural $\psi : R \to B$, astfel încât, pentru orice $s \in S$, $\psi(s) \in U(B)$, atunci există un unic morfism de R- algebre $u : R_S \to B$.*

Demonstrație. Faptul că u este morfism de R-algebre presupune că următoarea diagramă este comutativă:



Dacă există un astfel de morfism, atunci, pentru orice $\frac{a}{s} \in R_S$

$$u\left(\frac{a}{s}\right) = u\left(\frac{a}{1}\right)u\left(\frac{1}{s}\right) = u\left(\rho(a)\right)\cdot u\left(\rho(s)\right)^{-1} = \psi(a)\cdot\psi(s)^{-1}.$$

Deci existența lui *u* implică unicitatea lui *u*. Să luăm ca definiție a unei aplicații $u : R_S \to B$ relația

$$u\left(\frac{a}{s}\right) = \psi(a)\cdot\psi(s)^{-1}.$$

Să arătăm că *u* este bine definită. Dacă $(a_1, s_1) \sim (a, s),$ atunci:

$as_1 = a_1 s,\ \psi(a)\psi(s_1) = \psi(a_1)\psi(s)\,,\ \psi(a)\psi(s)^{-1} = \psi(a_1)\psi(s_1)^{-1}$

(elementele de forma $\psi(r),\ r \in R$ comută cu orice elemente din *B*).

Să arătăm că *u* este morfism unitar de inele. Fie $\frac{a}{s}, \frac{b}{t} \in R_S$.

$$u\left(\frac{a}{s}+\frac{b}{t}\right) = u\left(\frac{at+bs}{st}\right) = \psi(at+bs)\cdot\psi(st)^{-1} =$$

$$= \left(\psi(a)\psi(t)+\psi(b)\psi(s)\right)\psi(s)^{-1}\psi(t)^{-1} =$$

$$= \psi(a)\psi(s)^{-1}+\psi(b)\psi(t)^{-1} = u\left(\frac{a}{s}\right)+u\left(\frac{b}{t}\right)$$

$$u\left(\frac{a}{s}\cdot\frac{b}{t}\right) = u\left(\frac{ab}{st}\right) = \psi(ab)\cdot\psi(st)^{-1} =$$

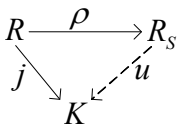
$$= \psi(a)\psi(s)^{-1}\cdot\psi(b)\psi(t)^{-1} = u\left(\frac{a}{s}\right)u\left(\frac{b}{t}\right)$$

$$u\left(\frac{1}{1}\right) = \psi(1)\cdot\psi(1)^{-1} = 1.$$

Relația $u \circ \rho = \psi$ rezultă din definiția lui *u*. □

7.5. **Consecință.** *Fie K un corp comutativ, R un subinel unitar al său. Atunci K include un subcorp izomorf cu corpul de fracții al lui R.*

Demonstrație. Deoarece K este corp comutativ, R nu are divizori ai lui zero, deci R este un domeniu de integritate şi putem vorbi despre corpul său de fracții. Considerăm diagrama:



unde ρ este morfismul din construcția corpului de fracții R_S iar j este morfismul incluziune.

Pentru orice $s \in S = R \setminus \{0\}$, $j(s) = s \in U(K)$. Din teorema 7.4. rezultă că există un morfism u de R-algebre care face diagrama comutativă. Cum R_S este un corp, u este injectiv. Deci $R_S \simeq Imu$ şi Imu este subcorp în K. □

Să aplicăm consecința 7.5. pentru $\mathbb{Z}[i]$, subinel al lui $\mathbb{C}$.

Subcorpul lui $\mathbb{C}$ izomorf cu corpul de fracții al lui $\mathbb{Z}[i]$ este format din elemente de forma:

$$(m+ni)(p+qi)^{-1} = \frac{mp+nq}{p^2+q^2} + i\frac{np-mq}{p^2+q^2},$$
$$m,n,p,q \in \mathbb{Z},\ p^2+q^2 \neq 0,$$

şi coincide cu $\mathbb{Q}[i] = \{a+bi \mid a,b \in \mathbb{Q}\}$.

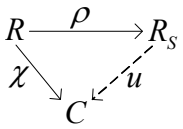
În final vom demonstra că proprietatea a) din teorema 7.2. şi ***proprietatea de universalitate*** (*) din teorema 7.4. determină inelul de fracții R_S până la un izomorfism.

7.6. **Teoremă (*unicitatea inelelor de fracții*).** *Fie R un inel comutativ şi unitar, S un sistem multiplicativ al său, format din nondivizori ai lui zero. Dacă C este o R-algebră de morfism structural* $\chi : R \to C$ *astfel încât :*

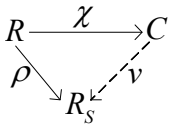
a) *pentru orice* $s \in S$, $\chi(s) \in U(C)$;

(*) *Dacă B este o R-algebră de morfism structural* $\psi : R \to B$, *astfel încât, pentru orice* $s \in S$, $\psi(s) \in U(B)$, *atunci există un unic morfism de R-algebre* $u : C \to B$;
atunci $C \simeq R_S$ (*izomorfism de R-algebre*).

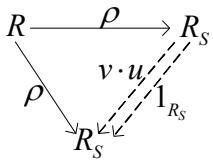
Demonstrație. Din a) şi din teorema 7.4. rezultă următorul morfism *u* de *R*-algebre:



Aplicând (*) pentru $B = R_S$, rezultă următorul morfism *v* de *R*-algebre:



Din $u \cdot \rho = \chi$ şi $v \cdot \chi = \rho$ rezultă $v \cdot u \cdot \rho = \rho$. Din unicitatea morfismului de *R*-algebre din teorema 7.4. şi din diagrama comutativă:



rezultă $v \cdot u = 1_{R_S}$. Analog $u \cdot v = 1_C$. Prin urmare, *u* este un izomorfism de *R* - algebre. □

Probleme propuse

1. Fie A un inel şi $n>1$ un număr natural. Pentru fiecare ideal bilateral I al lui A definim:

$$M_n(I)=\left\{(a_{ij})\in M_n(A)\,|\,a_{ij}\in I, 1\le i,j\le n\right\}.$$

Demonstraţi că:

a) $M_n(I)$ este un ideal bilateral în $M_n(A)$ şi funcţia $I\to M_n(I)$ este o bijecţie ce păstrează relaţia de incluziune între mulţimea idealelor bilaterale ale lui A şi mulţimea idealelor bilaterale ale lui $M_n(A)$.

b) $M_n(A)/M_n(I)\simeq M_n\left(A/I\right)$.

2. Fie A un inel comutativ şi unitar.

a) Notăm cu $rad(A)$ mulţimea elementelor nilpotente din A. Să se arate că $rad(A)$ este ideal în A şi să se determine numărul elementelor nilpotente din inelul $\mathbb{Z}_n$ unde $n\ge 2$. Deduceţi că $\mathbb{Z}_n$ este inel redus ($rad(A)=\{0\}$) dacă şi numai dacă n este liber de pătrate (adică $n\ne 1$ şi n nu se divide prin pătratul niciunui număr prim).

b) Arătaţi că suma a două elemente din A, unul nilpotent iar celălalt inversabil, este element inversabil în inelul A.

c) $f=\sum_{i=0}^{n}a_iX^i\in rad(A[X])\Leftrightarrow a_i\in rad(A)$, pentru $0\le i\le n$.

d) $f=\sum_{i=0}^{n}a_iX^i\in U(A[X])\Leftrightarrow a_0\in U\left(A\right)$, $a_i\in rad(A)$, $1\le i\le n$.

e) $f\in A[X]$ este divizor al lui zero în $A[X]$ dacă şi numai dacă există $a\in A\setminus\{0\}$ astfel încât $af=0$.

3. Să se determine idealele prime ale inelului $\mathbb{Z}_n$ unde $n\ge 2$. Caz particular, $\mathbb{Z}_{16}$, $\mathbb{Z}_{360}$.

4. Fie A un inel comutativ unitar. Arătaţi că M este ideal maximal în A dacă şi numai dacă pentru orice $a\in A\setminus M$ există $b\in A$ astfel încât $1-ab\in M$.

5. Arătați că orice ideal prim al unui inel comutativ, unitar, finit este ideal maximal.

6. Fie A un inel comutativ, unitar, astfel încât pentru orice $a \in A$ există $n \geq 1$ astfel încât $a^n = a$. Arătați că orice ideal prim în A este şi maximal.

7. Fie A un inel comutativ, unitar şi $a \in A$. Demonstrați că:

a) $A[X]/(X,a) \simeq A/(a)$;

b) (X,a) este ideal prim (respectiv ideal maximal) în $A[X]$ dacă şi numai dacă (a) este ideal prim (respectiv ideal maximal) în A;

c) (X) este ideal prim dar nu este maximal în inelul $\mathbb{Z}[X]$.

8. Considerăm A un inel comutativ, unitar, care verifică condiția lanțurilor descendente. Atunci, orice ideal prim în A este şi maximal.

9. În inelul comutativ, unitar A considerăm idealul I şi idealele prime P_1, $P_2, \ldots, P_n$. Dacă $I \subseteq \bigcup_{i=1}^{n} P_i$, arătați că există $i \in \overline{1,n}$, astfel încât $I \subseteq P_i$.

10. Fie P un ideal în inelul comutativ, unitar A, cu $P \neq A$. Notăm $S = A \setminus P$. Arătați că S este sistem multiplicativ dacă şi numai dacă P este ideal prim în A.

11. Fie A un inel comutativ, unitar, $a \in A$ un nondivizor al lui zero şi $S = \{1, a, a^2, a^3, \ldots\}$. Arătați că: $A_S \simeq A[X]/(aX - 1)$.

12. În inelul comutativ, unitar A considerăm $S \subseteq A$, un sistem multiplicativ format din nondivizori ai lui zero. Notăm cu S' mulțimea tuturor divizorilor elementelor din S. Arătați că:

a) S' este sistem multiplicativ format din nondivizori ai lui zero şi $S' \supseteq S$ (spunem că S' este *saturatul sistemului* S).

b) $A_S \simeq A_{S'}$.

Capitolul II

PROPRIETĂȚI ARITMETICE ALE INELELOR

Studiul aritmeticii numerelor întregi pune în evidență trei proprietăți remarcabile:

0.1. **Teorema împărțirii cu rest.** *Oricare ar fi numerele întregi a şi b,* $b \neq 0$, *există şi sunt unice numerele întregi q şi r astfel încât* $a = bq + r$ *şi* $0 \leq r < |b|$.

0.2. **Teoremă.** *Oricare ar fi idealul I ín inelul* $\mathbb{Z}$ *al numerelor întregi, există* $n \in \mathbb{N}$, *astfel încât I este idealul generat de n, deci* $I = (n) = n\mathbb{Z}$.

0.3. **Teorema fundamentală a aritmeticii.** *Oricare ar fi numărul întreg n* ($n \neq 0$, $n \neq 1$, $n \neq -1$), *există o descompunere a lui n de forma*:

$$n = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

unde $\varepsilon = 1$ *sau* $\varepsilon = -1$, $k \in \mathbb{N}^*$, $\alpha_i \in \mathbb{N}^*$, $i \in \overline{1,k}$, $p_1, \ldots, p_k$ *sunt numere prime distincte. În plus, această descompunere este unică, în afară de ordinea factorilor.*

Fiecare dintre aceste proprietăți are numeroase implicații în stabilirea altor rezultate privind inelul numerelor întregi. Este motivul pentru care condițiile din teoremele 0.1., 0.2., 0.3., au servit ca model pentru definirea unor clase de inele. Aceste clase fac obiectul capitolului de față.

Inelele cu care se lucrează în acest capitol sunt presupuse a fi comutative şi unitare.

1. Relația de divizibilitate. Relația de asociere în divizibilitate

În acest paragraf $(A,+,\cdot)$ este un inel.

1.1. **Definiție.** *Fie* $a,b\in A$. *Se spune* ***că a divide b*** *şi se notează* $a\mid b$, *dacă există* $c\in A$, *astfel încât* $b=ac$.

În condițiile definiției anterioare, se spune că *b* este un *multiplu* al lui *a* iar dacă $b\neq 0$, se spune că *a* este un *divizor* al lui *b*.

Cum în orice inel, $a\cdot 0=0$, pentru orice $a\in A$, rezultă $a\mid 0$ şi 0 este multiplu al oricărui element. Expresia *a este divizor al lui zero* se foloseşte numai în condițiile definiției 1.4. din capitolul I.

1.2. **Propoziție.** *Relația de divizibilitate pe un inel A este o relație de preordine, fără a fi în general o relație de ordine sau o relație de echivalență.*

Demonstrație. Se verifică uşor că relația de divizibilitate este reflexivă şi tranzitivă, deci este o relație de preordine. În general, relația de divizibilitate nu este antisimetrică. De exemplu, în inelul $\mathbb{Z}$, $2\mid -2$ şi $-2\mid 2$ dar $2\neq -2$. Deci $\mid$ nu este o relație de ordine. De asemenea, $\mid$ nu este o relație simetrică. În acelaşi inel $\mathbb{Z}$, $2\mid 6$ dar 6 nu divide 2. Deci $\mid$ nu este o relație de echivalență. □

Se pot verifica uşor următoarele proprietăți ale relației de divizibilitate:

- $1\mid a$, *pentru orice* $a\in A$;
- $-a\mid a$, *pentru orice* $a\in A$;
- $a\mid b$ *şi* $c\mid d \Rightarrow ac\mid bd$, *pentru orice* $a,b,c,d\in A$;
- $a\mid b \Rightarrow ac\mid bc$, *pentru orice* $a,b,c\in A$;
- $a\mid b$ *şi* $a\mid c \Rightarrow a\mid (b+c)$, *pentru orice* $a,b,c\in A$;
- $a\mid b_i$, $i\in\overline{1,n} \Rightarrow a\left|\sum_{i=1}^{n} c_i b_i\right.$, *pentru orice* $a,b_1,...,b_n,c_1,...,c_n\in A$.

Cum idealul generat de un element este format din mulțimea multiplilor acelui element, este normal să existe o strânsă legătură între

relația de divizibilitate şi idealele generate de elementele corespunzătoare.

1.3. **Propoziție.** *Fie* $a,b \in A$. *Sunt echivalente condițiile:*

i) $a \mid b$;

ii) $(a) \supseteq (b)$.

Demonstrație. Să presupunem că $a \mid b$. Rezultă $b \in (a)$, de unde $(b) \subseteq (a)$ (idealul generat de *b* fiind cel mai mic dintre idealele care conțin *b*). Reciproc, să presupunem că $(a) \supseteq (b)$. Rezultă $b \in (a)$, deci $a \mid b$. □

Relației de divizibilitate, ca relație de preordine, i se poate asocia în mod natural o relație de echivalență.

1.4. **Definiție.** *Fie* $a,b \in A$. *Spunem că a şi b sunt* ***asociate în divizibilitate*** *şi notăm* $a \sim b$ *dacă* $a \mid b$ *şi* $b \mid a$.

În inelul $\mathbb{Z}[i]$ al întregilor lui Gauss $(1+i) \sim (1-i)$ deoarece:

$$1+i = i(1-i) \text{ şi } 1-i = -i(1+i),$$

deci $(1+i) \mid (1-i)$ şi $(1-i) \mid (1+i)$.

În inelul $K[X]$ unde *K* este corp comutativ, $f \sim cf$ pentru orice $f \in K[X]$ şi $c \in K^*$. Într-adevăr, $f \mid cf$ şi din $f = c^{-1}(cf)$ rezultă şi $cf \mid f$.

Din 1.3. şi 1.4. rezultă imediat:

1.5. **Consecință.** *Fie* $a,b \in A$. *Sunt echivalente condițiile*:

i) $a \sim b$;

ii) $(a) = (b)$.

1.6. **Propoziție.** *Relația de asociere în divizibilitate pe inelul A este o relație de echivalență.*

Demonstrație. Proprietatea de reflexivitate a relației ~ rezultă din proprietatea de reflexivitate a relației |. Proprietatea de simetrie a relației ~ rezultă din definiție. Proprietatea de tranzitivitate a relației ~ se deduce din proprietatea de tranzitivitate a relației |. □

Relația de asociere în divizibilitate fiind o relație de echivalență determină pe inelul *A* clase de echivalență. În anumite situații este

convenabilă utilizarea unui sistem de reprezentanți pentru aceste clase (vezi paragraful 9).

1.7. **Propoziție.** *Fie* $u \in A$. *Sunt echivalente condițiile:*

a) $u \in U(A)$;

b) $u \sim 1$;

c) $(u) = A$;

d) $u \mid a$, *pentru orice* $a \in A$.

Demonstrație. Dacă u este inversabil în A, atunci există $u^{-1} \in A$, astfel încât $uu^{-1} = 1$, sau $u \mid 1$. Deci, a) $\Rightarrow$ b). Implicația b) $\Rightarrow$ c) rezultă din 1.5., idealul generat de 1 fiind întregul inel A. Dacă $(u) = A$, atunci orice element $a \in A$ este un multiplu al lui u, deci $u \mid a$. Prin urmare, c) $\Rightarrow$ d). Dacă presupunem adevărată d), în particular $u \mid 1$, deci există $v \in A$ astfel încât $uv = 1$ sau $u \in U(A)$. □

Echivalența condițiilor a) și b) din proprietatea anterioară ne permite să folosim notația mai comodă $a \sim 1$ în locul expresiei a este element inversabil al inelului A.

1.8. **Propoziție.** *Fie A un inel integru și* $a, b \in A$. *Sunt echivalente condițiile:*

a) $a \sim b$;

b) *există* $u \in U(A)$, *astfel încât* $b = ua$.

Demonstrație. Dacă $a = 0$, atunci $b = 0$ și se poate lua $u = 1$. Dacă $a \neq 0$, atunci din $a \sim b$ rezultă că există u, v în A astfel încât $b = ua$ și $a = vb$. De aici, $a = vua$. Cum A este inel integru și $a \neq 0$, rezultă $1 = uv$, deci $u \in U(A)$.

Dacă există $u \in U(A)$, astfel încât $b = ua$, atunci $a \mid b$. Din relația $a = u^{-1}b$ rezultă $b \mid a$, deci $a \sim b$. □

Propoziția 1.8. ne permite să descriem clasele de asociere în divizibilitate în diferite inele.

În inelul $\mathbb{Z}$, clasa de asociere în divizibilitate a lui $a \in A$ cuprinde elementele a și $-a$.

Deoarece $U(\mathbb{Z}[i])=\{1,-1,i,-i\}$, în inelul $\mathbb{Z}[i]$, clasa de asociere în divizibilitate a lui z cuprinde elementele $z,-z,iz,-iz$.

În inelul $K[X]$, K corp comutativ, clasa de asociere în divizibilitate a polinomului f cuprinde toate polinoamele de forma cf, $c\in K^*$.

Considerații analoage se pot face şi pe alte inele. Astfel, pentru

$$\mathbb{Z}\left[i\sqrt{5}\right]=\left\{m+ni\sqrt{5}\,\middle|\,m,n\in\mathbb{Z}\right\}$$

înzestrat cu structură de inel integru în raport cu adunarea şi înmulțirea numerelor complexe, se defineşte funcția

$$N:\mathbb{Z}\left[i\sqrt{5}\right]\to\mathbb{N},\ \ N\left(m+n\sqrt{5}\right)=m^2+5n^2.$$

Funcția N numită şi în acest caz ***normă,*** verifică proprietăți asemănătoare normei din inelul întregilor lui Gauss.

Se deduce $U\left(\mathbb{Z}\left[i\sqrt{5}\right]\right)=\{1,-1\}$, deci elementele asociate în divizibilitate cu $z\in\mathbb{Z}\left[i\sqrt{5}\right]$ sunt z şi $-z$.

2. Cel mai mare divizor comun. Cel mai mic multiplu comun

În acest paragraf, inelele vor fi presupuse domenii de integritate.

2.1. **Definiție.** *Fie a, b, d, elemente ale inelului A. Se spune că d este un* ***cel mai mare divizor comun*** *al elementelor a şi b dacă sunt îndeplinite condițiile:*

1) $d\,|\,a$ *şi* $d\,|\,b$;

2) *pentru orice* $d'\in A$, *din* $d'\,|\,a$ *şi* $d'\,|\,b$, *rezultă* $d'\,|\,d$.

Prima condiție arată că d este un divizor comun pentru elementele a şi b. A doua condiție arată că orice alt divizor comun al elementelor a şi b este şi un divizor al lui d. Dacă privim relația de divizibilitate ca relație de preordine, atunci 1) arată că d este un minorant pentru $\{a,b\}$ iar 2) arată că d este un cel mai mare minorant pentru $\{a,b\}$. Deci d este un $inf\{a,b\}$.

Nu în orice inel, orice două elemente au un cel mai mare divizor comun. Totuşi, în caz de existenţă, putem vorbi despre o anumită unicitate a acestuia.

2.2. **Propoziţie.** *Fie a, b două elemente ale inelului A pentru care există un cel mai mare divizor comun* $d \in A$. *Fie* $d_1 \in A$. *Atunci* d_1 *este un cel mai mare divizor comun pentru a şi b dacă şi numai dacă* $d \sim d_1$.

Demonstraţie. Să presupunem mai întâi că d_1 este un cel mai mare divizor comun pentru *a* şi *b*. Deci:

1′) $d_1 \mid a$ *şi* $d_1 \mid b$;

2′) *pentru orice* $d' \in A$, *din* $d' \mid a$ *şi* $d' \mid b$, *rezultă* $d' \mid d_1$.

Condiţia 1′) arată că în 2) se poate lua $d' = d_1$ şi rezultă $d_1 \mid d$. Condiţia 1) arată că în 2′) se poate lua $d' = d$ şi rezultă $d \mid d_1$. Deci, $d \sim d_1$.

Să presupunem acum $d_1 \sim d$. Din $d_1 \mid d$ şi din 1) rezultă $d_1 \mid a$ şi $d_1 \mid b$. Fie $d' \in A$, astfel încât $d' \mid a$ şi $d' \mid b$. Din 2) rezultă $d' \mid d$. Cum $d \mid d_1$, rezultă $d' \mid d_1$. Prin urmare, d_1 este un cel mai mare divizor comun pentru *a* şi *b*. □

Pentru cel mai mare divizor comun al elementelor *a* şi *b*, atunci când există, se foloseşte notaţia (a,b). Datorită propoziţiei 2.2., faptul că *d* este un cel mai mare divizor comun pentru *a* şi *b* îl notăm prin $d \sim (a,b)$.

Definiţia 2.1. se poate extinde în mod natural la un număr finit de elemente.

2.3. **Definiţie.** *Fie* $a_1,...,a_n,d \in A$, $n \geq 2$. *Se spune că d este un* ***cel mai mare divizor comun*** *al elementelor* $a_1,...,a_n$, *dacă*:

- $d \mid a_i$, $i \in \overline{1,n}$;

- *pentru orice* $d' \in A$, *din* $d' \mid a_i$, $i \in \overline{1,n}$, *rezultă* $d' \mid d$.

Se notează $d \sim (a_1,...,a_n)$.

2.4. **Propoziție.** *Fie A un inel în care orice două elemente au un cel mai mare divizor comun. Atunci orice n elemente din A,* $n \geq 2$, *au un cel mai mare divizor comun.*

Demonstrație. Raționăm prin inducție după *n.* Presupunem că orice $n-1$ elemente din A ($n>2$) au un cel mai mare divizor comun.

Fie $a_1,...,a_n \in A.$ Conform ipotezei de inducție există

$$d_1 \sim (a_1,...,a_{n-1}) \text{ şi } d \sim (d_1, a_n).$$

Din $d \mid d_1$ şi $d_1 \mid a_1,...,d_1 \mid a_{n-1}$, rezultă $d \mid a_1,...,d \mid a_{n-1}$. De asemenea, $d \mid a_n$.

Fie $d' \in A,$ astfel încât $d' \mid a_i$, $i \in \overline{1,n}.$ Rezultă $d' \mid d_1$ şi apoi $d' \mid d$. Deci, $d \sim (a_1,...,a_{n-1},a_n).$ □

Din demonstrația propoziției 2.4. a rezultat şi relația:

$$\big((a_1,...,a_{n-1}),a_n\big) \sim (a_1,...,a_{n-1},a_n).$$

2.5. **Definiție.** *Fie a,b elemente ale inelului A. Se spune că a şi b sunt* ***relativ prime*** *dacă 1 este un cel mai mare divizor comun pentru a şi b,* $1 \sim (a,b)$.

Se observă că două elemente sunt relativ prime dacă şi numai dacă singurii divizori comuni ai elementelor *a* şi *b* sunt elementele inversabile.

2.6. **Propoziție.** *Fie a,b două elemente ale inelului integru A, nu ambele nule, pentru care există* $d \sim (a,b)$. *Fie* $a_1,b_1 \in A,$ *astfel încât* $a = da_1,\ b = db_1.$ *Atunci,* a_1 *şi* b_1 *sunt relativ prime.*

Demonstrație. Fie *u* un divizor comun pentru a_1 şi b_1. Din $u \mid a_1$ şi $u \mid b_1$ rezultă $du \mid da_1 = a$ şi $du \mid db_1 = b$. Cum $d \sim (a,b),$ rezultă că $du \mid d$. Există $v \in A,$ astfel încât $d = duv.$ Deoarece *a* şi *b* nu sunt ambele nule, rezultă $d \neq 0$ şi $1 = uv.$ Deci, $u \in U(A)$ şi $a_1,\ b_1$ sunt relativ prime. □

2.7. **Propoziție.** *Fie A un inel integru şi* $a,b,c \in A$ *astfel încât există* (a,b) *şi* (ca,cb). *Atunci:*

$$(ca,cb) \sim c(a,b).$$

Demonstrație. Dacă $a = b = 0$ atunci $(ca, cb) \sim c(a,b) \sim 0$. La fel, dacă $c = 0$, atunci $(ca, cb) \sim c(a,b) \sim 0$.

În continuare presupunem $c \neq 0$ iar a şi b nu sunt ambele nule. Fie $d \sim (a,b)$ şi $d_1 \sim (ca, cb)$. Conform ipotezelor, $d \neq 0$ şi $d_1 \neq 0$. De asemenea:

$$a = da', \ b = db', \ a', b' \in A, \ (a', b') \sim 1$$

$$ca = d_1 a_1, \ cb = d_1 b_1, \ a_1, b_1 \in A, \ (a_1, b_1) \sim 1$$

Din $d \mid a$ rezultă $cd \mid ca$. Analog, $cd \mid cb$. Cum $(ca, cb) \sim d_1$, rezultă $cd \mid d_1$. Există $u \in A$, astfel încât $d_1 = cdu$. Vom arăta că $u \in U(A)$. Au loc relațiile:

$$ca = cda', \ ca = d_1 a_1 = cdua_1, \ cda' = cdua_1, \ a' = ua_1, \ u \mid a'.$$

Analog, $u \mid b'$. Cum $(a', b') \sim 1$, rezultă $u \in U(A)$.

Din $d_1 = cdu$, rezultă $d_1 \sim cd$. □

În demonstrația propoziției 2.7., este esențială ipoteza de existență a celui mai mare divizor comun pentru ambele perechi de elemente. Altfel, rezultatul nu se păstrează, aşa cum se constată din următorul exemplu:

În inelul $\mathbb{Z}\left[i\sqrt{5}\right]$, $\left(3, 1 + i\sqrt{5}\right) \sim 1$, dar elementele $2\left(1 + i\sqrt{5}\right)$ şi 6 nu au un cel mai mare divizor comun (verificarea acestor afirmații constituie un exercițiu pentru cititor).

2.8. **Consecință.** *Fie A un inel integru în care orice două elemente au un cel mai mare divizor comun. Fie $a, b, c \in A$ astfel încât $a \mid bc$ şi $(a,b) \sim 1$. Atunci, $a \mid c$.*

Demonstrație. Din ipoteze şi din propoziția anterioară, rezultă $(ca, cb) \sim c(a,b) \sim c$. Cum $a \mid ca$, $a \mid cb$, rezultă $a \mid c$. □

2.9. **Consecință.** *Fie A un inel integru în care orice două elemente au un cel mai mare divizor comun şi $a, b, c \in A$ astfel încât $a \mid c$, $b \mid c$ şi $(a,b) \sim 1$. Atunci, $ab \mid c$.*

Demonstrație. Există $c_1 \in A$ astfel încât $c = ac_1$.

Din $b \mid ac_1$ şi $(a,b) \sim 1$, conform consecinţei precedente, rezultă $b \mid c_1$. De aici, $ab \mid ac_1 = c$. □

2.10. **Definiţie.** *Fie A un inel integru şi* $a,b,m \in A$. *Se spune că m este un* ***cel mai mic multiplu comun*** *pentru a şi b, dacă sunt îndeplinite condiţiile*:

- $a \mid m$ *şi* $b \mid m$;

- *pentru orice* $m' \in A$, *din* $a \mid m'$ *şi* $b \mid m'$, *rezultă* $m \mid m'$.

Considerând relaţia | ca o relaţie de preordine pe A rezultă că m este un $sup\{a,b\}$.

Nu în orice inel integru, orice două elemente au un cel mai mic multiplu comun. Dacă pentru elementele $a,b \in A$, există un cel mai mic multiplu comun m, atunci $m_1 \in A$ este de asemenea un cel mai mic multiplu comun pentru a şi b dacă şi numai dacă $m \sim m_1$.

Pentru cel mai mic multiplu comun al elementelor a şi $b \in A$, atunci când există, se foloseşte notaţia $[a,b]$.

Definiţia celui mai mic multiplu comun se poate extinde în mod natural la un număr finit de elemente.

2.11. **Definiţie.** *Fie A un inel integru şi* $a_1,...,a_n,m \in A$, $n \geq 2$. *Se spune că m este un* ***cel mai mic multiplu*** *comun pentru elementele* $a_1,...,a_n$, *dacă*:

- $a_i \mid m$, $i \in \overline{1,n}$;

- *pentru orice* $m' \in A$, *din* $a_i \mid m'$, $i \in \overline{1,n}$, *rezultă* $m \mid m'$.

Ca şi în cazul celui mai mare divizor comun, din existenţa celui mai mic multiplu comun pentru orice două elemente, rezultă existenţa celui mai mic multiplu comun pentru orice număr finit de elemente şi are loc relaţia:

$$\left[[a_1,...,a_{n-1}],a_n\right] \sim [a_1,...,a_{n-1},a_n].$$

Aşa cum va rezulta din propoziţia următoare, condiţiile de existenţă a celui mai mare divizor comun şi a celui mai mic multiplu comun sunt echivalente.

2.12. **Propoziție.** *Fie A un inel integru. Sunt echivalente condițiile:*

a) *pentru orice două elemente din A există un cel mai mare divizor comun*;

b) *pentru orice două elemente din A există un cel mai mic multiplu comun*;

c) *intersecția oricăror două ideale principale din A este un ideal principal în A.*

Demonstrație. "a) $\Rightarrow$ b)" Fie $a,b \in A$ şi $d \sim (a,b)$. Este suficient să tratăm cazul $d \neq 0$. Rezultă $a = da'$, $b = db'$, $(a',b') \sim 1$.

Notăm $m = da'b'$ şi demonstrăm $m \sim [a,b]$. Din $m = ab' = ba'$ rezultă $a \mid m$ şi $b \mid m$. Fie acum $m' \in A$ astfel încât $a \mid m'$ şi $b \mid m'$. Obținem $m = ab' \mid m'b'$ şi $m = ba' \mid m'a'$. Deci

$$m \mid (m'a', m'b') \sim m'(a',b') \sim m',$$

adică $m \mid m'$. Prin urmare, $m \sim [a,b]$.

"b) $\Rightarrow$ a)" Fie $a,b \in A$ şi $m \sim [a,b]$. Este suficient să tratăm cazul în care a şi b sunt nenule. Există $a',b' \in A$ astfel încât $m = aa' = bb'$. Din $a \mid ab$ şi $b \mid ab$ rezultă $m \mid ab$, deci există $d \in A$ astfel încât $ab = dm$. Vom demonstra că $d \sim (a,b)$.

Din $ab = md = aa'd$ şi $d \neq 0$ rezultă $b = a'd$, deci $d \mid b$. Analog se deduce $d \mid a$.

Fie acum $d' \in A$ astfel încât $d' \mid a$ şi $d' \mid b$. Există $a_1, b_1 \in A$ astfel încât $a = d'a_1$, $b = d'b_1$. Notăm $m_1 = a_1 b_1 d'$. Din $m_1 = ab_1 = ba_1$ rezultă $a \mid m_1$ şi $b \mid m_1$. Cum $m \sim [a,b]$, rezultă $m \mid m_1$. Există $c \in A$ astfel încât $m_1 = mc$. Au loc relațiile: $d'mc = d'm_1 = ab = md$. Cum $m \neq 0$, rezultă $d'c = d$ sau $d' \mid d$. Deci, $d \sim (a,b)$.

"b) $\Rightarrow$ c)" Fie (a), (b) două ideale principale ale inelului A. Fie $m \sim [a,b]$. Vom demonstra că $(a) \cap (b) = (m)$.

Dacă $x \in (a) \cap (b)$, atunci $x \in (a)$ şi $x \in (b)$, deci $a \mid x$ şi $b \mid x$. Cum $m \sim [a,b]$, rezultă $m \mid x$ şi $x \in (m)$. Dacă $x \in (m)$, atunci $m \mid x$ şi cum $a \mid m$, $b \mid m$, rezultă $a \mid x$ şi $b \mid x$. Deci, $x \in (a) \cap (b)$.

"c) $\Rightarrow$ b)" Fie $a,b \in A$ şi $(a) \cap (b) = (m)$. Din $m \in (a)$ rezultă $a \mid m$. Analog rezultă $b \mid m$. Dacă $a \mid m'$ şi $b \mid m'$ atunci $m' \in (a) \cap (b) = (m)$, deci $m \mid m'$. Prin urmare, $m \sim [a,b]$. □

Din demonstrația propoziției 2.12. rezultă şi:

2.13. **Consecință.** *Fie A un inel integru în care orice două elemente au un cel mai mare divizor comun. Fie $a,b \in A$, $d \sim (a,b)$ şi $m \sim [a,b]$. Atunci, $ab \sim md$.*

3. Elemente ireductibile şi elemente prime

Vom clasifica elementele unui inel integru după mulțimea divizorilor acestora.

Dacă $a = 0$, atunci $d \mid a$, pentru orice $d \in A$.

Dacă $u \in U(A)$ şi $d \mid u$, atunci $d \in U(A)$.

Cum elementele inversabile divid orice element, rezultă că 0 este cel mai bogat în divizori iar elementele inversabile sunt cele mai sărace.

Fie acum $a \in A$, $a \neq 0$ şi $a \notin U(A)$.

Pentru $a' \in A$, $a' \sim a$, a' este un divizor al lui a.

Se spune că elementele inversabile şi elementele asociate în divizibilitate cu a sunt ***divizori improprii*** ai lui a. Ceilalți divizori, dacă există, se numesc ***divizori proprii.***

3.1. **Definiție.** *Fie A un inel integru şi $q \in A$, un element nenul şi neinversabil. Se spune că elementul q este **ireductibil** dacă satisface condiția:*

- pentru orice $d \in A$, din $d \mid q$ rezultă $d \sim q$ sau $d \sim 1$.

*În caz contrar se spune că elementul q este **reductibil** în A.*

Cu alte cuvinte, un element nenul şi neinversabil din A este ireductibil în A dacă nu are decât divizori improprii.

Exemple. 1°. Elementul 2 este ireductibil în inelul $\mathbb{Z}$ al întregilor raționali. Într-adevăr, 2 este nenul şi neinversabil în $\mathbb{Z}$ şi singurii divizori ai lui 2 sunt $-1, 1, 2, -2$. Trebuie să remarcăm că acelaşi element 2 este reductibil în inelul $\mathbb{Z}[i]$ al întregilor lui Gauss. Într-adevăr, $1+i \mid 2 = (1+i)(1-i)$, $1+i \notin U(\mathbb{Z}[i])$ şi $1+i$ nu este asociat în divizibilitate cu 2.

2° Fie K un corp comutativ. Vom arăta că orice polinom $f \in K[X]$ de gradul 1 este ireductibil în $K[X]$. Într-adevăr, $f \neq 0$, $f \notin U(K[X]) = K^*$. Dacă $h \in K[X]$ şi $h \mid f$, atunci există $g \in K[X]$ astfel încât $f = gh$. Rezultă $d^\circ h = 0$ sau $d^\circ h = 1$. Dacă $d^\circ h = 0$, atunci $h \in K^* = U(K[X])$. Dacă $d^\circ h = 1$, atunci $d^\circ g = 0$ şi $g \in K^*$, deci $h \sim f$.

Se deduce uşor că dacă elementul $q \in A$ este ireductibil în A şi $q' \in A$, $q' \sim q$, atunci q' este ireductibil în A.

3.2. **Propoziție.** *Fie A un inel integru şi $q \in A$, q ireductibil în A. Atunci, pentru orice $a \in A$, există (q,a).*

Demonstrație. Fie $a \in A$. Dacă $q \mid a$, atunci $q \sim (q,a)$. Dacă q nu divide a, atunci vom arăta că $(q,a) \sim 1$, adică elementele q şi a sunt relativ prime. Fie d un divizor comun al lui q şi a .Din $d \mid q$ şi q ireductibil rezultă $d \sim q$ sau $d \sim 1$. Cazul $d \sim q$ nu este posibil deoarece conduce la $q \mid a$, contrar ipotezei făcute. Deci $d \sim 1$. Prin urmare, $(q,a) \sim 1$. □

3.3. **Propoziție.** *Fie A un inel integru şi $q \in A$, nenul şi neinversabil. Sunt echivalente condițiile:*

a) *q este ireductibil;*

b) *pentru orice $a,b \in A$, din $q = ab$ rezultă ($q \sim a$ şi $b \sim 1$) sau ($q \sim b$ şi $a \sim 1$).*

Demonstrație. "a) $\Rightarrow$ b)" Presupunem q ireductibil şi fie $a,b \in A$ astfel încât $q = ab$. Cum a şi b sunt divizori ai lui q, rezultă ($a \sim q$ sau $a \sim 1$) şi ($b \sim q$ sau $b \sim 1$). Dacă $a \sim 1$ şi $b \sim 1$, atunci $q \sim 1$,

ceeace contrazice ipoteza. Deci cel puțin unul dintre elementele a şi b este asociat în divizibilitate cu q.

Dacă $a \sim q$, atunci există $u \in U(A)$ astfel încât $q = au$. Din $q = ab$ şi $a \neq 0$, rezultă $b = u \sim 1$.

Asemănător, în cazul $b \sim q$ rezultă $a \sim 1$.

"b) $\Rightarrow$ a)" Să presupunem că elementul q satisface condiția b). Fie d un divizor al lui q. Există $c \in A$ astfel încât $q = dc$. Conform lui b), rezultă $d \sim q$ sau $d \sim 1$. Prin urmare, q este ireductibil. □

Condiția b) din propoziția anterioară arată că un element ireductibil se poate scrie doar ca produs de divizori improprii. Este motivul pentru care elementele ireductibile se mai numesc ***elemente nedecompozabile.***

3.4. **Propoziție.** *Fie A un inel integru care nu este corp şi $q \in A$. Sunt echivalente condițiile.:*

a) *q este ireductibil în A;*
b) *(q) este maximal în mulțimea idealelor principale proprii ale lui A.*

Demonstrație. "a) $\Rightarrow$ b)" Presupunem q ireductibil în A. Din $q \neq 0$ rezultă $(q) \neq (0)$. Din q neinversabil rezultă $(q) \neq A$. Deci (q) este un ideal propriu în A. Fie (d) un ideal principal propriu în A astfel încât $(q) \subseteq (d)$. Rezultă $d \mid q$. Cum q este ireductibil, rezultă $d \sim q$ sau $d \sim 1$. Dacă $d \sim q$, atunci $(d) = (q)$. Cazul $d \sim 1$ nu este posibil deoarece $(d) \neq A$. Prin urmare, (q) este maximal în mulțimea idealelor principale proprii ale lui A.

"b) $\Rightarrow$ a)" *P*resupunem că (q) satisface condiția b). Cum (q) este ideal propriu, rezultă $(q) \neq A$ şi $(q) \neq (0)$. Deci, $q \not\sim 1$ şi $q \neq 0$. Fie $d \in A$, astfel încât $d \mid q$. Prin urmare, $(q) \subseteq (d)$. Dacă (d) este ideal impropriu, atunci $(d) = A$, deci $d \sim 1$. Dacă (d) este ideal propriu, atunci, din proprietatea de maximalitate a lui (q) rezultă $(q) = (d)$, deci $d \sim q$. Prin urmare q este ireductibil în A. □

3.5. **Definiție.** *Fie A un inel integru şi $p \in A$, un element nenul şi neinversabil. Se spune că p este* ***element prim*** *în A dacă:*

- pentru orice elemente $a,b \in A$, *din* $p \mid ab$ *rezultă* $p \mid a$ *sau* $p \mid b$.

Exemple. 1°. În inelul $\mathbb{Z}$ al întregilor raționali, 2 este un element prim. Într-adevăr, 2 este nenul şi neinversabil şi dacă produsul a două numere întregi este un număr par, atunci cel puțin unul din factori este număr par.

2°. Dacă A este un inel integru, atunci X este element prim în inelul $A[X]$. Într-adevăr, $X \neq 0$ şi $X \notin U(A[X]) = U(A)$. Considerăm $f = \sum_{i=0}^{n} a_i X^i$ şi $g = \sum_{j=0}^{m} b_j X^j$ două polinoame din $A[X]$ astfel încât $X \mid fg$. Rezultă că termenul liber al polinomului *fg* este nul, deci $a_0 b_0 = 0$. Deoarece A este inel integru, obținem $a_0 = 0$ sau $b_0 = 0$. Astfel, $X \mid f$ sau $X \mid g$.

Se poate verifica uşor că dacă $p \in A$ este un element prim şi $p_1 \in A$, $p_1 \sim p$, atunci p_1 este element prim în A.

3.6. **Propoziție.** *Fie A un inel integru şi p un element prim în A. Atunci p este element ireductibil în A.*

Demonstrație. Conform ipotezei, *p* este nenul şi neinversabil în A. Fie $a,b \in A$ astfel încât $p = ab$. Rezultă $p \mid ab$ şi, cum *p* este prim, rezultă $p \mid a$ sau $p \mid b$. Să considerăm cazul $p \mid a$. Obținem $p \sim a$ şi $b \sim 1$. La fel se tratează cazul $p \mid b$. Deci *p* este ireductibil în A. □

Reciproca propoziției 3.6. nu este în general adevărată.

Astfel, în inelul $\mathbb{Z}\left[i\sqrt{5}\right]$, 3 este ireductibil şi nu este prim.

Într-adevăr, $N(3) = 9$. Dacă $d \in \mathbb{Z}\left[i\sqrt{5}\right]$ şi $d \mid 3$, atunci $N(d) \mid N(3)$. Deci $N(d) \in \{1,3,9\}$. Dacă $N(d) = 1$, atunci $d \sim 1$. Dacă $N(d) = 9$, atunci rezultă $d \sim 3$. Cazul $N(d) = 3$ nu este posibil deoarece ecuația $m^2 + 5n^2 = 3$ nu are soluții în $\mathbb{Z}$. Deci 3 este element ireductibil în $\mathbb{Z}\left[i\sqrt{5}\right]$. Totuşi, 3 nu este element prim în acest inel. Într-adevăr,

$3 \mid \left(1+2i\sqrt{5}\right)\left(1-2i\sqrt{5}\right) = 21$ dar 3 nu divide nici pe $1+2i\sqrt{5}$ nici pe $1-2i\sqrt{5}$.

3.7. **Propoziție.** *Fie A un inel integru în care orice două elemente au un cel mai mare divizor comun. Atunci orice element ireductibil în A este prim în A.*

Demonstrație. Fie q un elemente ireductibil în A. q este nenul şi neinversabil. Fie $a,b \in A$, astfel încât $q \mid ab$. Ştim că $(q,a) \sim 1$ sau $(q,a) \sim q$.

Dacă $(q,a) \sim q$, atunci $q \mid a$.

Dacă $(q,a) \sim 1$, atunci $(qb,ab) \sim b$. Cum $q \mid qb$ şi $q \mid ab$, rezultă $q \mid b$.

Deci q este element prim în A. □

Din propozițiile 3.6. şi 3.7. rezultă că în inelele integre în care orice două elemente au un cel mai mare divizor comun, elementele prime coincid cu elementele ireductibile.

Deoarece în inelul $\mathbb{Z}\left[i\sqrt{5}\right]$ există elemente ireductibile care nu sunt prime, nu orice două elemente ale acestui inel au un cel mai mare divizor comun.

3.8. **Propoziție.** *Fie A un inel integru şi* $p \in A \setminus \{0\}$. *Sunt echivalente condițiile:*

a) *p este element prim*;

b) (p) *este ideal prim în A.*

Demonstrație. "a) $\Rightarrow$ b)" Presupunem p element prim în A. Din p neinversabil, rezultă $(p) \neq A$. Fie $a,b \in A$, astfel încât $ab \in (p)$. Rezultă $p \mid ab$ şi, cum p este prim în A, rezultă $p \mid a$ sau $p \mid b$, deci $a \in (p)$ sau $b \in (p)$. Deci (p) este ideal prim în A.

"b) $\Rightarrow$ a)" Presupunem (p) ideal prim în A. Din $(p) \neq A$ rezultă p neinversabil. Fie $a,b \in A$, astfel încât $p \mid ab$. Rezultă $ab \in (p)$. Cum

(p) este ideal prim, rezultă $a \in (p)$ sau $b \in (p)$, de unde $p \mid a$ sau $p \mid b$. Deci p este element prim în A. □

În particular, rezultă că în inelul $\mathbb{Z}$ al întregilor raționali, idealele prime sunt (0) şi (p) cu p număr prim.

3.9. **Propoziție.** *Fie A un inel integru şi p un element prim în A. Atunci p este prim şi în $A[X]$.*

Demonstrație. Remarcăm mai întâi că dacă $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ şi $a \in A$, atunci $a \mid f$ dacă şi numai dacă $a \mid a_i$, $i \in \overline{0,n}$. Deoarece p este prim în A, $p \neq 0$ şi $p \notin U(A) = U(A[X])$.

Fie $f = \sum_{i=0}^{n} a_i X^i$ şi $g = \sum_{j=0}^{m} b_j X^j$ două polinoame din $A[X]$ care verifică $p \mid fg$. Deoarece $fg = \sum_{k=0}^{n+m} c_k X^k$, $c_k = \sum_{i+j=k} a_i b_j$,

$$p \mid fg \Leftrightarrow p \mid c_k, \ k \in \overline{0,n+m}.$$

Să presupunem că $p \nmid f$ şi $p \nmid g$. Există $i \in \overline{0,n}$ şi $j \in \overline{0,m}$ astfel încât $p \nmid a_i$ respectiv $p \nmid b_j$. Notăm cu i_0 şi j_0 cei mai mici indici cu această proprietate. Din relațiile:

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = \ldots + a_{i_0-1} b_{j_0+1} + a_{i_0} b_{j_0} + a_{i_0+1} b_{j_0-1} + \ldots$$

$$p \mid a_i, \ i \in \overline{0,i_0-1}, \ \ p \nmid b_j, \ \ j \in \overline{0,j_0-1}, \ \ p \nmid c_{i_0+j_0},$$

rezultă $p \nmid a_{i_0} b_{j_0}$. Cum p este prim în A, rezultă $p \nmid a_{i_0}$ sau $p \nmid b_{j_0}$, contrar alegerii indicilor i_0 şi j_0.

Prin urmare, $p \mid f$ sau $p \mid g$. Deci p este prim în $A[X]$. □

4. Inele euclidiene

4.1. **Definiție.** *Fie A un inel integru şi $\varphi : A \setminus \{0\} \to \mathbb{N}$. Se spune că A este* ***inel euclidian*** *în raport cu funcția φ dacă sunt îndeplinite condițiile:*

a) *Pentru orice $a, b \in A \setminus \{0\}$, din $a \mid b$ rezultă $\varphi(a) \le \varphi(b)$;*

b) *Pentru orice $a, b \in A$ cu $b \neq 0$, există q şi r în A, astfel încât:*

$$a = bq + r \text{ şi } (r = 0 \text{ sau } \varphi(r) < \varphi(b)).$$

Prin analogie cu inelele uzuale, q din condiția b) poartă numele de ***cât*** iar r poartă numele de ***rest.***

Exemple. 1°. Pe inelul $\mathbb{Z}$ al întregilor raționali considerăm funcția valoare absolută, $\varphi(x) = |x|$, $\varphi : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$. Funcția φ satisface evident condiția a). Din teorema împărțirii cu rest pentru numerele întregi a şi b, $b \neq 0$, rezultă existența şi chiar unicitatea numerelor întregi q şi r, astfel încât:

$$a = bq + r \text{ şi } 0 \le r < |b|.$$

Din ultima relație rezultă $|r| < |b|$, deci $\mathbb{Z}$ este un inel euclidian în raport cu funcția valoare absolută.

Se observă că dacă pentru q şi r se formulează condițiile $a = bq + r$ şi $|r| < |b|$, atunci, în general, q şi r nu mai sunt unice. Astfel, pentru $a = 43$ şi $b = 5$, au loc relațiile:

$$43 = 5 \cdot 8 + 3 \text{ şi } |3| < |5|$$

dar şi relațiile:

$$43 = 5 \cdot 9 + (-2) \text{ şi } |-2| < |5|.$$

Prin urmare, există două perechi (q, r) care satisfac b), anume $(8,3)$ şi $(9,-2)$.

2°. Fie K un corp comutativ şi $K[X]$ inelul polinoamelor în nedeterminata X, cu coeficienți în K. Fie funcția ***grad,***

$$\varphi : K[X] \setminus \{0\} \to \mathbb{N}, \quad \varphi(f) = d^\circ f, \quad \forall f \in K[X] \setminus \{0\}.$$

Dacă $f, g \in K[X] \setminus \{0\}$ şi $f \mid g$, atunci $d^\circ f \le d^\circ g$, deci condiția a) este îndeplinită. Din teorema împărțirii cu rest pentru polinoamele

cu coeficienţi într-un corp comutativ, rezultă: există şi sunt unice polinoamele q şi r, numite *cât*, respectiv *rest*, astfel încât:

$$f = gq + r \text{ şi } (r = 0 \text{ sau } d^\circ f < d^\circ g).$$

Este îndeplinită şi condiţia b), deci $\left(K[X], d^\circ\right)$ este inel euclidian.

3°. Vom arăta că inelul $\mathbb{Z}[i]$ al întregilor lui Gauss este un inel euclidian în raport cu funcţia normă:

$$N : \mathbb{Z}[i] \to \mathbb{N},$$

$$N(m+ni) = m^2 + n^2, \text{ pentru orice } m+ni \in \mathbb{Z}[i].$$

Fie $a = m+ni$ şi $b = s+ti$ două elemente nenule din $\mathbb{Z}[i]$ astfel încât $a \mid b$. Rezultă $N(a) \mid N(b)$, ambele elemente aparţinând lui $\mathbb{N}^*$, deci $N(a) \le N(b)$.

Dacă presupunem $b \neq 0$, atunci:

$$\frac{a}{b} = \frac{m+ni}{s+ti} = x + iy, \text{ unde } x, y \in \mathbb{Q}.$$

Există un număr întreg q_1 astfel încât $|x - q_1| \le \frac{1}{2}$, anume $q_1 = [x]$ sau $q_1 = [x]+1$. Fie $u = x - q_1$, $|u| \le \frac{1}{2}$. Analog, există q_2, un număr întreg, astfel încât $|y - q_2| \le \frac{1}{2}$. Fie $v = y - q_2$, $|v| \le \frac{1}{2}$.

$$\frac{a}{b} = q_1 + iq_2 + u + iv \Leftrightarrow a = b(q_1 + iq_2) + b(u + iv)$$

Notăm:

$$q = q_1 + iq_2 \in \mathbb{Z}[i], \quad r = b(u+iv) = a - bq \in \mathbb{Z}[i].$$

Deci $a = bq + r$. Dacă $r \neq 0$, atunci:

$$N(r) = N(b)N(u+iv) = N(b)(u^2+v^2) \le N(b)\frac{1}{2} < N(b).$$

Fiind îndeplinite ambele condiţii din definiţia 4.1., $\mathbb{Z}[i]$ este inel euclidian în raport cu funcţia normă N.

Condiţia b) din definiţia 4.1. implică o serie de proprietăţi importante ale inelelor euclidiene.

4.2. **Lemă.** *Fie A un inel integru şi $a,b,q,r \in A$ astfel încât $a = bq + r$. Atunci, există cel mai mare divizor comun al elementelor a şi b dacă şi numai dacă există cel mai mare divizor comun al elementelor b şi r. În acest caz:*

$$(a,b) \sim (b,r).$$

Demonstraţie. Presupunem că există $d \sim (a,b)$. Deci $d \mid a$ şi $d \mid b$. Din $r = a - bq$ rezultă $d \mid r$. Deci *d* este un divizor comun pentru *b* şi *r*. Fie acum $d' \in A$ astfel încât $d' \mid b$ şi $d' \mid r$. Din $a = bq + r$ rezultă $d' \mid a$. Cum $d \sim (a,b)$, rezultă $d' \mid d$. Deci $d \sim (b,r)$. Elementele *a* şi *r* au un rol analog în relaţia $a = bq + r$ deoarece se poate scrie $r = b(-q) + a$. Ca urmare, din $d \sim (b,r)$, rezultă $d \sim (a,b)$. □

4.3. **Teoremă.** *Dacă (A,φ) este un inel euclidian, atunci pentru orice două elemente din A există cel mai mare divizor comun.*

Demonstraţie. Fie *a,b* două elemente din A.

Dacă $b = 0$, atunci $(a,b) \sim a$.

Dacă $b \neq 0$, atunci există $q_2, r_2 \in A$ astfel încât:

(1) $a = bq_2 + r_2$ şi ($r_2 = 0$ *sau* $\varphi(r_2) < \varphi(b)$).

Cazul în care un rest este 0 va fi tratat unitar mai târziu.

Dacă $r_2 \neq 0$, atunci există $q_3, r_3 \in A$ astfel încât:

(2) $b = r_2 q_3 + r_3$ şi ($r_3 = 0$ *sau* $\varphi(r_3) < \varphi(r_2)$).

Dacă $r_3 \neq 0$, atunci există $q_4, r_4 \in A$ astfel încât:

(3) $r_2 = r_3 q_4 + r_4$ şi ($r_4 = 0$ *sau* $\varphi(r_4) < \varphi(r_3)$).

. . . . . .

Dacă $r_k \neq 0$, atunci există $q_{k+1}, r_{k+1} \in A$ astfel încât:

(*k*) $r_{k-1} = r_k q_{k+1} + r_{k+1}$ şi ($r_{k+1} = 0$ *sau* $\varphi(r_{k+1}) < \varphi(r_k)$).

Observăm că în mulţimea $\mathbb{N}$ a numerelor naturale au loc relaţiile:

$$\varphi(b) > \varphi(r_2) > \varphi(r_3) > \ldots > \varphi(r_k) > \varphi(r_{k+1}) \geq 0.$$

Relaţii de forma (*k*) se pot obţine atât timp cât $r_k \neq 0$. Deoarece orice mulţime nevidă de numere naturale are un prim element ($\mathbb{N}$

este bine ordonată), rezultă că există un rang n, astfel încât $r_{n+1} = 0$. Vom scrie atunci ultimele două relații de forma (k):

$(n-1)$ $\qquad r_{n-2} = r_{n-1}q_n + r_n$

(n) $\qquad r_{n-1} = r_n q_{n+1}$.

Inegalitățile din relațiile (k) sunt necesare pentru a demonstra că există doar un număr finit de relații de acest fel.

Din relația (n) rezultă că există cel mai mare divizor comun al elementelor r_{n-1} și r_n și $r_n \sim (r_{n-1}, r_n)$.

Din relațiile $(n-1)$, (n), … ,(2), (1), aplicând succesiv lema 4.2., rezultă:

$$r_n \sim (r_{n-1}, r_n) \sim (r_{n-2}, r_{n-1}) \sim ... \sim (r_2, r_3) \sim (b, r_2) \sim (a, b). \qquad \square$$

Pentru uniformizarea scrierii relațiilor (1), (2),…,(n), vom nota $a = r_0$, $b = r_1$.

4.4. **Definiție.** *Fie* (A, φ) *un inel euclidian și* $a, b \in A$. *Relațiile* (1), (2), …, (n), *din teorema 4.3.*, *poartă numele de* ***Algoritmul lui Euclid*** *pentru elementele a și b.*

Din demonstrația teoremei 4.3., rezultă că *cel mai mare divizor comun al elementelor a și b este ultimul rest nenul din algoritmul lui Euclid, pentru elementele a și b.*

4.5. **Consecință.** *Într-un inel euclidian, orice element ireductibil este și un element prim.*

Demonstrație. Rezultă din propoziția 3.7. și din teorema 4.3. $\square$

Fie A un inel integru. Problema dacă inelul A poate fi înzestrat cu o structură de inel euclidian revine la a stabili dacă există o funcție $\varphi : A \setminus \{0\} \to \mathbb{N}$ astfel încât (A, φ) să fie un inel euclidian. Pentru a arăta că un anumit inel nu este euclidian, de obicei, se arată că acesta nu îndeplinește o anumită condiție necesară. Astfel inelul $\mathbb{Z}\left[i\sqrt{5}\right]$ nu este euclidian deoarece elementul 3 este ireductibil dar nu este prim.

Teorema 4.3. arată că se poate afla cel mai mare divizor comun pentru două elemente a, b, ale unui inel euclidian aplicând algoritmul lui Euclid, prin "împărțiri succesive".

În cazuri concrete poate interesa numărul de împărțiri succesive care trebuie efectuate pentru a afla (a,b). Din demonstrația teoremei 4.3. rezultă că $\varphi(b)$ poate fi folosit pentru majorarea numărului de împărțiri din algoritmul lui Euclid. În cazul inelului $\mathbb{Z}$ al întregilor raționali are loc:

4.6. **Teoremă.** (***a lui Lamé***) *Fie* $a,b\in\mathbb{N}^*,\ a>b$. *Numărul de împărțiri în algoritmul lui Euclid pentru elementele a şi b nu depăşeşte de* 5 *ori numărul cifrelor din scrierea în baza* 10 *a lui b*.

Demonstrație. Pentru aceasta, avem nevoie de câteva considerații ajutătoare.

Fie $(f_n)_{n\geq 1}$ şirul lui Fibonacci, definit prin:

$$f_1=f_2=1 \text{ şi } f_{n+1}=f_n+f_{n-1},\ n\geq 2.$$

4.7. **Lemă.** $f_n>\alpha^{n-2}$, *pentru* $n\geq 3$, *unde* $\alpha=\dfrac{1+\sqrt{5}}{2}$.

Demonstrație. Raționăm prin inducție.

$$f_3=2>\frac{1+\sqrt{5}}{2}=\alpha,\ f_4=3>\left(\frac{1+\sqrt{5}}{2}\right)^2=\alpha^2.$$

Presupunem $f_i>\alpha^{i-2}$, pentru $i\in\overline{3,k},\ k\geq 4$.

$$f_{k+1}=f_k+f_{k-1}>\alpha^{k-2}+\alpha^{k-3}=\alpha^{k-3}(\alpha+1)=\alpha^{k-3}\alpha^2=\alpha^{k-1}.\ \square$$

Revenim la **demonstrația teoremei** 4.6.

Fie:

$(k)\qquad r_{k-1}=r_kq_{k+1}+r_{k+1},\ k\in\overline{1,n},\ r_0=a,\ r_1=b,\ r_{n+1}=0,$

algoritmul lui Euclid pentru numerele naturale a şi b, $b\neq 0$. Au loc relațiile:

$q_i\geq 1$, pentru $i\in\overline{2,n}$;

$q_{n+1}\geq 2$ (altfel, $r_{n-1}=r_n$);

$r_n\geq 1=f_2$;

$r_{n-1}=r_nq_{n+1}\geq 2f_2=f_3$.

Presupunem:

$(*)\qquad r_{n-i}\geq f_{i+2}$ pentru $i\in\overline{0,k}$.

Rezultă:

$$r_{n-(k+1)} = r_{n-k}q_{n-k+1} + r_{n-k+1} \geq f_{k+2} + f_{k+1} = f_{k+3}.$$

Prin urmare, $(*)$ are loc pentru toate valorile $i \in \overline{0,n}$. În particular,

$$b = r_1 \geq f_{n+1} > \alpha^{n-1}.$$

Dacă b are s cifre în scrierea sa în baza 10, atunci $b < 10^s$. Deci, $\alpha^{n-1} < 10^s \Leftrightarrow (n-1)\lg\alpha < s$. Deoarece $\frac{1}{5} < \lg\alpha$, rezultă $n - 1 < 5s$.

Cum n şi s sunt numere naturale, $n \leq 5s$, relaţie ce demonstrează teorema lui Lamé. □

Evident, aplicarea algoritmului lui Euclid pentru două numere întregi revine la aplicarea acestuia pentru două numere naturale. De asemenea, în rolul lui b din teoremă se poare alege cel mai mic dintre cele două numere.

Se poare aborda şi problema inversă: fiind dat $n \in \mathbb{N}^*$, există două numere naturale a şi b astfel încât aplicarea algoritmului lui Euclid pentru a şi b să necesite exact n împărţiri?
Răspunsul este dat de:

4.8. **Teoremă.** *Dacă* $(f_n)_{n\geq 1}$ *este şirul lui Fibonacci, atunci aplicarea algoritmului lui Euclid pentru termenii* f_{n+2} *şi* f_{n+1} $(n \geq 1)$ *necesită exact n împărţiri*.

Demonstraţie. Şirul lui Fibonacci este strict crescător, începând cu al doilea termen. Relaţiile:

$$\begin{aligned}
&f_{n+2} = f_{n+1}\cdot 1 + f_n,\ 0 < f_n < f_{n+1}\\
&\vdots\\
&f_{k+1} = f_k \cdot 1 + f_{k-1},\ 0 < f_{k-1} < f_k\\
&\vdots\\
&f_4 = f_3 \cdot 1 + f_2,\ 0 < f_2 < f_3\\
&f_3 = f_2 \cdot 2
\end{aligned}$$

reprezintă exact cele n împărţiri din algoritmul lui Euclid pentru numerele f_{n+2} şi f_{n+1}. □

Din demonstrația teoremei 4.8. rezultă totodată că f_2 este cel mai mare divizor comun al termenilor f_{n+2} şi f_{n+1}. Prin urmare, oricare doi termeni consecutivi ai şirului lui Fibonacci sunt relativ primi.

5. Relațiile lui Bézout

Fie (A,φ) un inel euclidian şi $a,b\in A,\ b\neq 0$. Fie

(*k*) $\quad r_{k-1}=r_kq_{k+1}+r_{k+1},\ k\in\overline{1,n},\ r_0=a,\ r_1=b,\ r_{n+1}=0,$

algoritmul lui Euclid pentru elementele *a* şi *b*.

Vom arăta că toate resturile r_k se reprezintă ca nişte combinații liniare de *a* şi *b*, cu coeficienți în *A*. În particular, cel mai mare divizor comun r_n al elementelor *a* şi *b* va admite o astfel de reprezentare. Aceste relații se vor dovedi deosebit de utile în diverşi algoritmi.

5.1. **Teoremă.** *Fie* (A,φ) *un inel euclidian şi* $a,b\in A,\ b\neq 0$. *Fie secvența de vectori* $(w_k)_{0\le k\le n+1},\ w_k=(t_k,u_k,v_k)\in A^3$, *definită recurent astfel*:

$$w_0=(a,1,0),\ w_1=(b,0,1),$$

(1) $$w_{k+1}=w_{k-1}-q_{k+1}w_k,\ k\in\overline{1,n}$$

unde q_k ($k\in\overline{2,n+1}$) *sunt câturile din algoritmul lui Euclid pentru elementele a şi b* (*relațiile* (*k*), $k\in\overline{1,n}$). *Atunci*:

(B_k) $\quad t_k=r_k=u_ka+v_kb,\ k\in\overline{0,n+1}.$

Demonstrație. Raționăm prin inducție după *k*.

Pentru $k=0$: $t_0=a=r_0=1\cdot a+0\cdot b=u_0a+v_0b.$

Pentru $k=1$: $t_1=b=r_1=0\cdot a+1\cdot b=u_1a+v_1b.$

Presupunem că relațiile (B_k) au loc pentru $k\in\overline{0,i}$.

$$w_{i+1}=w_{i-1}-q_{i+1}w_i=(t_{i-1},u_{i-1},v_{i-1})-q_{i+1}(t_i,u_i,v_i)=$$
$$=(t_{i-1}-q_{i+1}t_i,u_{i-1}-q_{i+1}u_i,v_{i-1}-q_{i+1}v_i).$$

Deci:

$$t_{i+1} = t_{i-1} - q_{i+1}t_i = r_{i-1} - q_{i+1}r_i = r_{i+1}$$
$$u_{i+1} = u_{i-1} - q_{i+1}u_i$$
$$v_{i+1} = v_{i-1} - q_{i+1}v_i$$
$$r_{i+1} = t_{i+1} = r_{i-1} - q_{i+1}r_i = u_{i-1}a + v_{i-1}b - q_{i+1}(u_i a + v_i b) =$$
$$= (u_{i-1} - q_{i+1}u_i)a + (v_{i-1} - q_{i+1}v_i)b = u_{i+1}a + v_{i+1}b.$$

Rezultă că relațiile (B_k) sunt adevărate pentru $k \in \overline{0, n+1}$.

În particular, cel mai mare divizor comun *d* al elementelor *a* şi *b* se exprimă prin $d = r_n = u_n a + v_n b.$

Ultima dintre relațiile (B_k) se scrie: $0 = r_{n+1} = u_{n+1}a + v_{n+1}b.$ □

Relațiile (B_k), $k \in \overline{0, n+1}$ poartă numele de ***relațiile lui Bézout***.

Coeficienții u_k şi v_k din relațiile lui Bézout, poartă numele de ***coeficienți Bézout***.

Într-un inel euclidian oarecare, determinarea relațiilor lui Bézout pentru elementele *a* şi *b* presupune cunoaşterea câturilor q_k din algoritmul lui Euclid.

În cazul inelului $\mathbb{Z}$ al întregilor raționali, algoritmul lui Euclid şi relațiile lui Bézout se pot construi simultan. Este suficient să observăm că, în $\mathbb{Z}$, din $r_{k-1} = r_k q_{k+1} + r_{k+1}$ şi $0 \le r_{k+1} < r_k$, rezultă:

$$\frac{r_{k-1}}{r_k} = q_{k+1} + \frac{r_{k+1}}{r_k},\ q_{k+1} \in \mathbb{Z} \text{ şi } 0 \le \frac{r_{k+1}}{r_k} < 1.$$

Prin urmare,

(2) $$q_{k+1} = \left[\frac{r_{k-1}}{r_k} \right].$$

Determinarea relațiilor lui Bézout decurge astfel:

- vectorii w_0 şi w_1 sunt definiți în enunțul teoremei 5.1.;
- se determină câtul q_2 conform relației (2);
- se calculează vectorul w_2 conform relației (1);
- se repetă relațiile (2) şi (1) atât timp cât $r_k \neq 0$.

Calculele se pot sistematiza într-un tabel de forma:

k	0	1	2	$\cdots$	k	$\cdots$	n	$n+1$
t_k	a	b	t_2	$\ldots$	t_k	$\cdots$	t_n	0
u_k	1	0	u_2	$\cdots$	u_k	$\cdots$	u_n	u_{n+1}
v_k	0	1	v_2	$\cdots$	v_k	$\cdots$	v_n	v_{n+1}
q_k			q_2	$\cdots$	q_k	$\cdots$	q_n	q_{n+1}

Exemple. 1°. Fie $a = 243,\ b = 75.$

k	0	1	2	3	4
t_k	243	75	18	3	0
u_k	1	0	1	-4	25
v_k	0	1	-3	13	-81
q_k	-	-	3	4	6

Completarea tabelului, începând cu coloana pentru $k = 2,$ s-a făcut astfel:

$$q_2 = \left[\frac{243}{75}\right] = 3$$

$$t_2 = t_0 - q_2 t_1 = 243 - 75 \cdot 3 = 18$$

$$u_2 = u_0 - q_2 u_1 = 1 - 0 \cdot 3 = 1$$

$$v_2 = v_0 - q_2 v_1 = 0 - 1 \cdot 3 = -3, \text{ etc.}$$

În particular,

$$d = (243, 75) = r_3 = t_3 = 3 = -4 \cdot 243 + 13 \cdot 75$$

$$0 = r_4 = t_4 = 25 \cdot 243 - 81 \cdot 75.$$

În cazul inelului $\mathbb{Z}[i]$ al întregilor lui Gauss, determinarea câturilor se face astfel:

$$\frac{r_{k-1}}{r_k} = x + iy, \text{ unde } x, y \in \mathbb{Q}.$$

Se aleg $m, n \in \mathbb{Z}$ astfel încât $|x - m| \le \frac{1}{2}$ şi $|y - n| \le \frac{1}{2}$ (după cum am arătat în II.4., numerele *m* şi *n* nu sunt în general unice). Se obţine

$$q_{k+1} = m + ni$$

iar celelalte calcule decurg ca şi în cazul inelului $\mathbb{Z}$.

2°. Fie $a = -3 + 23i,\ b = 1 + 15i$ în inelul $\mathbb{Z}[i]$.

k	0	1	2	3	4	5
t_k	$-3+23i$	$1+15i$	$-5-7i$	$3+3i$	$1-i$	0
u_k	1	0	1	$1+i$	$3+2i$	$7-8i$
v_k	0	1	-2	$-1-2i$	$-4-4i$	$-13+10i$
q_k	-	-	2	$-1-i$	-2	$3i$

Completarea tabelului s-a făcut astfel:

$$\frac{r_0}{r_1} = \frac{t_0}{t_1} = \frac{-3+23i}{1+15i} = \frac{171}{113} + \frac{34}{113}i$$

$$x = \frac{171}{113},\ m = 2,\ |x - m| \le \frac{1}{2}$$

$$y = \frac{34}{113},\ n = 0,\ |y - n| \le \frac{1}{2}$$

$$q_2 = m + ni = 2$$

$$\frac{r_1}{r_2} = \frac{1+15i}{-5-7i} = -\frac{55}{37} - \frac{34}{37}i$$

$$x = \frac{-55}{37},\ m = -1$$

$$y = -\frac{34}{37},\ n = -1$$

$$q_3 = -1 - i$$

$$\frac{r_2}{r_3} = \frac{-5-7i}{3+3i} = -2 - \frac{1}{3}i$$

$$x = -2,\ m = -2$$

$$y = -\frac{1}{3},\ n = 0$$

$$q_4 = -2 + 0 \cdot i$$

$$\frac{r_3}{r_4} = \frac{3+3i}{1-i} = 3i$$

$$x = 0,\ m = 0$$

$$y = 3,\ n = 3$$

$$q_5 = 3i$$

În particular,

$$(-3+23i, 1+15i) \sim 1 - i = (3+2i)(-3+23i) + (-4-4i)(1+15i).$$

6. Ecuații liniare în inele euclidiene

Fie (A,φ) un inel euclidian. Considerăm ecuația liniară:

(1) $$ax+by=c$$

unde $a,b,c\in A.$ Se pune problema dacă ecuația (1) are soluții în A şi, în caz afirmativ, să se determine aceste soluții.

6.1. **Propoziție.** *Ecuația* (1) *are soluții în A dacă şi numai dacă*:

$$(a,b)\mid c.$$

Demonstrație. Presupunem că (1) are soluții şi fie $(x_0,y_0)\in A^2$ o soluție. Atunci, $ax_0+by_0=c.$ Dacă $d\sim(a,b),$ atunci $d\mid c.$

Reciproc, să presupunem că $(a,b)\sim d\mid c.$ Fie u şi v coeficienții Bézout astfel încât: $d=au+bv$ şi $c_1\in A$ astfel încât $c=dc_1.$ Cum

$$c=c_1ua+c_1vb,$$

obținem că (c_1u,c_1v) este o soluție a ecuației (1). □

Dacă $a=b=0,$ ecuația (1) are soluții dacă şi numai dacă $c=0.$ În acest caz, orice pereche $(x,y)\in A^2$ este o soluție pentru (1).

În continuare, vom presupune că a şi b nu sunt ambii nuli.

6.2. **Propoziție.** *Dacă ecuația* (1) *are soluții în A*, *atunci*, *orice soluție a acestei ecuații este de forma*:

(2) $$\begin{cases} x=c_1u+b_1t \\ y=c_1v-a_1t, \quad t\in A \end{cases}$$

unde $d\sim(a,b),\ a=da_1,\ b=db_1,\ c=dc_1,\ d=ua+vb.$

Demonstrație. Se verifică uşor că (2) este soluție pentru (1), oricare ar fi $t\in A.$

Reciproc, fie $(x,y)\in A^2$ o soluție pentru (1). Atunci, $ax+by=c.$ Deoarece $ac_1u+bc_1v=c,$ rezultă:

$$a(x-c_1u)+b(y-c_1v)=0.$$

Din $a=da_1,\ b=db_1,\ d\neq 0,$ rezultă:

$$a_1(x-c_1u)+b_1(y-c_1v)=0.$$

Pentru că $(a_1, b_1) \sim 1$, rezultă $b_1 \mid (x - c_1 u)$. Fie $t \in A$ astfel încât $x - c_1 u = b_1 t$. Deci, $x = c_1 u + b_1 t$ şi $y = c_1 v - a_1 t$. □

Exemple. 1°. Să se rezolve în $\mathbb{Z}$ ecuaţia:

$$243x + 75y = 21.$$

$d = (243, 75) = 3 \mid 21$. Conform exemplului 1° de la II.5.,

$3 = -4 \cdot 243 + 13 \cdot 75$, $u = -4$, $v = 13$, $a_1 = 81$, $b_1 = 25$, $c_1 = 7$.

Soluţiile întregi ale ecuaţiei sunt de forma:

$$\begin{cases} x = -4 \cdot 7 + 25t \\ y = 13 \cdot 7 - 81t, \quad t \in \mathbb{Z}. \end{cases}$$

2°. Să se rezolve în $\mathbb{Z}[i]$ ecuaţia:

$$(-3 + 23i)x + (1 + 15i)y = 2 + 4i.$$

Folosind relaţiile obţinute în exemplul II.5. 2°, rezultă:

$(-3 + 23i, 1 + 15i) \sim 1 - i \mid 2 + 4i$.

$1 - i = (3 + 2i)(-3 + 23i) + (-4 - 4i)(1 + 15i)$, $u = 3 + 2i$, $v = -4 - 4i$,

$a = -3 + 23i = (1 - i)(-13 + 10i)$, $a_1 = -13 + 10i$,

$b = 1 + 15i = (1 - i)(-7 + 8i)$, $b_1 = -7 + 8i$,

$c = 2 + 4i = (1 - i)(-1 + 3i)$, $c_1 = -1 + 3i$.

Soluţiile ecuaţiei sunt de forma:

$$\begin{cases} x = (3 + 2i)(-1 + 3i) + (-7 + 8i)t \\ y = (-4 - 4i)(-1 + 3i) - (-13 + 10)t, \quad t \in \mathbb{Z}[i]. \end{cases}$$

7. Inele principale

Se ştie că dacă H este un subgrup al grupului aditiv $\mathbb{Z}$ al întregilor raţionali, atunci există $n \in \mathbb{N}$ astfel încât

(1) $$H = n\mathbb{Z}.$$

În particular, orice ideal al inelului întregilor raţionali $\mathbb{Z}$ este de forma (1), adică este generat de un singur element.

Un ideal I al unui inel A, generat de un singur element, a, poartă numele de **ideal principal**.

7.1. **Definiţie.** *Fie A un inel integru. Se spune că A este* ***inel principal****, dacă orice ideal I al lui A este ideal principal.*

Exemple. 1°. Inelul $\mathbb{Z}$ al întregilor raționali este inel principal.

2°. Fie K un corp comutativ. Singurele ideale ale lui K sunt $O=(0)$ şi $K=(1)$. Cum K este şi inel integru, K este inel principal.

Teorema următoare ne va permite să dăm şi alte exemple de inele principale.

7.2. **Teoremă.** *Dacă A este inel euclidian, atunci A este inel principal.*

Demonstrație. Fie A inel euclidian în raport cu $\varphi: A\setminus\{0\}\to\mathbb{N}$.

Demonstrația este analoagă aceleia prin care se arată că orice subgrup al lui $\mathbb{Z}$ este de forma (1).

Fie I un ideal al lui A.

Dacă $I=\{0\}$, atunci $I=(0)$ este un ideal principal.

Dacă $I\neq\{0\}$, mulțimea $M=\{\varphi(x)\,|\,x\in I\setminus\{0\}\}$ este nevidă. Deoarece $M\subseteq\mathbb{N}$ şi $(\mathbb{N},\leq)$ este bine ordonată, în M există un prim element. Fie acesta $\varphi(a)$. Deci, $a\in I$, $a\neq 0$, $\varphi(a)\leq\varphi(x)$, pentru orice $x\in I\setminus\{0\}$.

Din $a\in I$, rezultă $(a)\subseteq I$.

Fie $x\in I$. Cum (A,φ) este inel euclidian şi $a\neq 0$, există $q,r\in A$ astfel încât:

$$x=aq+r \text{ şi } (r=0 \text{ sau } \varphi(r)<\varphi(a)).$$

Dacă $r\neq 0$, atunci $r=x-aq\in I$ şi $\varphi(r)<\varphi(a)$, contrar alegerii lui a. Deci, $r=0$ şi $x=aq\in(a)$. Rezultă $I\subseteq(a)$ şi, în final, $I=(a)$.

Cum A este inel integru şi orice ideal al său este principal, rezultă că inelul A este principal. □

Conform teoremei 7.1., se poate completa lista exemplelor de inele principale cu:

Inelul $\mathbb{Z}[i]$ al întregilor lui Gauss este inel principal.

Inelul $K[X]$ al polinoamelor cu coeficienți într-un corp comutativ K este un inel principal.

Există şi inele integre care nu sunt principale.

7.3. **Teoremă.** *Fie A un inel integru care nu este corp. Atunci, $A[X]$ nu este inel principal.*

Demonstrație. Deoarece A este inel integru şi nu este corp, există $a \in A,\ a \neq 0,\ a \notin U(A)$.

Fie I idealul generat în $A[X]$ de mulțimea $\{a, X\}$:

$$I = aA[X] + XA[X] = \left\{ ah_1 + Xh_2 \,\middle|\, h_1, h_2 \in A[X] \right\}.$$

Vom demonstra că I nu este ideal principal.

Prin reducere la absurd, să presupunem că există $f \in A[X]$ astfel încât $I = (f)$.

Din $a \in I$, rezultă că există $g \in A[X]$ astfel încât $a = fg$. Cum A este integru şi $a \neq 0$, rezultă $d^\circ f = 0$, deci $f \in A \setminus \{0\}$.

Din $X \in I$, rezultă că există $h \in A[X]$ astfel încât $X = fh$.

Notând cu b_1 coeficientul lui X din polinomul h, din ultima egalitate, rezultă $1 = fb_1$ adică $f \in U(A) = U(A[X])$. Prin urmare,

$$I = (f) = A[X].$$

Rezultă $1 \in I$, deci există $h_1, h_2 \in A[X]$ astfel încât $1 = ah_1 + Xh_2$.

Dacă notăm cu c_0 termenul liber al lui h_1, din ultima relație obținem că $1 = ac_0$ deci, $a \in U(A)$, contrar alegerii lui a.

În consecință, I nu este inel principal şi, ca urmare, $A[X]$ nu este inel principal. □

7.4. **Consecință.** *Următoarele inele nu sunt principale:*

a) $\mathbb{Z}[X]$;

b) $A[X_1, ..., X_n],\ n \geq 1$, *unde A este un inel integru care nu este corp;*

c) $K[X_1, ..., X_n],\ n \geq 2$, *unde K este corp comutativ*.

Demonstrație. a) rezultă direct din teorema 7.3. b) rezultă din teorema 7.3. şi din faptul că dacă A este inel integru care nu este corp, atunci şi $A[X_1, ..., X_n]$, cu $n \geq 1$, este inel integru care nu este corp. c) rezultă din teorema 7.3. şi din faptul că pentru K corp comutativ, $K[X]$ este inel integru care nu este corp. □

7.5. **Teoremă.** *Fie A un inel principal. Pentru orice două elemente a şi b din A, există* (a,b) *şi* $[a,b]$. *Dacă* $d \sim (a,b)$, *atunci există* $u, v \in A$ *astfel încât* $d = ua + vb$.

Demonstrație. Într-un inel principal, intersecția oricăror două ideale principale este, evident, tot un ideal principal. Conform propoziției 2.12., orice două elemente din A au un cel mai mare divizor comun şi un cel mai mic multiplu comun.

Se poate totuşi da şi o demonstrație directă, care pune în evidență şi alte aspecte.

Fie $a,b \in A.$ Cum A este inel principal, există $d \in A$ astfel încât:

(2) $$(a)+(b)=(d).$$

Vom demonstra că $d \sim (a,b)$.

Din $(a) \subseteq (d)$ rezultă $d \mid a.$ Analog, $d \mid b.$

Din relația (2) rezultă că există $u,v \in A$ astfel încât

(3) $$d = ua + vb.$$

Dacă $d' \in A$ şi $d' \mid a,\ d' \mid b,$ atunci, evident $d' \mid d.$ □

Din teorema 7.5., rezultă că şi în inelele principale există coeficienți Bézout (elementele u şi v din relația (3)).

Totuşi, spre deosebire de inelele euclidiene în care coeficienții Bézout se pot calcula efectiv, pornind de la algoritmul lui Euclid, în inelele principale, în general, nu există un algoritm efectiv de calcul pentru aceşti coeficienți.

Remarcăm, de asemenea, că relația (2) mai poate fi scrisă şi:

$$(d) = \left(\{a,b\}\right),$$

relație care justifică notația celui mai mare divizor comun, $d \sim (a,b)$.

7.6. **Consecință.** *Într-un inel principal, orice element ireductibil este prim.*

8. Descompunere în factori în inelele principale

În acest paragraf, vom demonstra că, într-un inel principal, orice element nenul şi neinversabil se descompune în produs de elemente ireductibile (sau elemente prime).

8.1. **Lemă.** *Într-un inel principal, orice şir crescător de ideale este staționar.*

Demonstrație. Considerăm un şir crescător de ideale $(I_n)_{n\geq 1}$. Astfel, $I_n \subseteq I_{n+1},\ \forall n \geq 1$. Notăm $I = \bigcup_{n=1}^{\infty} I_n$.

Demonstrăm că I este ideal în A. Fie $a,b \in I$. Există $n,m \in \mathbb{N}^*$ astfel încât $a \in I_n$ şi $b \in I_m$. Pentru a fixa ideile, fie $m \leq n$. Rezultă $a,b \in I_n$. Deci $a-b \in I_n \subseteq I$. Dacă $x \in A$, atunci, $xa \in I_n \subseteq I$.

Deoarece A este inel principal şi I este ideal în A, există $c \in I$ astfel încât $I = (c)$. Din $c \in I$ rezultă că există $n_0 \in \mathbb{N}^*,\ c \in I_{n_0}$.

Deci,

$$I = (c) \subseteq I_{n_0} \subseteq I_{n_0+1} \subseteq ... \subseteq I_{n_0+p} \subseteq ... \subseteq I.$$

Prin urmare,

$$I_{n_0} = I_{n_0+1} = ... = I_{n_0+p} = ...,$$

adică şirul $(I_n)_{n\geq 1}$ este staționar. □

8.2. **Teoremă.** *Dacă A este inel principal, atunci orice element nenul şi neinversabil din A se descompune în produs de elemente prime*.

Demonstrație. Vom raționa prin reducere la absurd. Să presupunem că există $a \in A$, astfel încât:

(*) "$a \neq 0,\ a \notin U(A)$, *a nu se reprezintă ca produs de elemente prime* (*ireductibile*) "

În particular, a nu poate fi ireductibil. Există $b,c \in A$, astfel încât:

$$a = bc,\ a \neq b,\ a \neq c,\ b \neq 1,\ c \neq 1.$$

Se obține în acest fel şirul crescător de ideale:

$$(a) \subset (a_1) \subset ... \subset (a_i) \subset (a_{i+1}) \subset ...$$

care nu este staționar, contrar lemei 8.1. Prin urmare, ipoteza făcută este falsă. Deci, orice element nenul şi neinversabil al inelului principal A se poate scrie ca produs de elemente prime (ireductibile). □

Se observă că teorema 8.2. asigură existența descompunerilor în factori primi (pentru elementele nenule şi neinversabile ale inelelor principale). O teoremă de unicitate se poate stabili chiar pe un cadru mai general.

8.3. **Teoremă.** *Fie A un inel integru,* $p_1,...,p_r \in A$, *elemente prime şi* $q_1,...,q_s \in A$, *elemente ireductibile astfel încât:*

(1) $$p_1p_2...p_r = q_1q_2...q_s.$$

Atunci,

$r = s$ *şi există o permutare* $\sigma \in \mathscr{S}_r$ *astfel încât* $p_i \sim q_{\sigma(i)}$, $i \in \overline{1,r}$.

Demonstrație. Vom raționa prin inducție după numărul *r* al factorilor primi din descompunerea (1).

Pentru $r = 1$, $p_1 = q_1q_2...q_s$. Deoarece elementul prim p_1 este şi ireductibil iar factorii q_j nu sunt inversabili, rezultă $s = 1$ şi $p_1 = q_1$.

Presupunem adevărată afirmația din teorema 8.3. pentru descompuneri în care numărul de factori primi este $r-1$, $r > 1$. Demonstrăm că afirmația rămâne adevărată şi pentru descompuneri în care numărul de factori primi este *r*. Fie deci:

(1) $$p_1p_2...p_r = q_1q_2...q_s$$

unde $p_1,...,p_r$ sunt elemente prime şi $q_1,...,q_s$ elemente ireductibile.

În particular, $p_r \mid q_1q_2...q_s$. p_r fiind prim, există $j \in \overline{1,s}$ astfel încât $p_r \mid q_j$. Pentru a nu complica scrierea, presupunem (schimbând eventual ordinea factorilor din descompunere) $j = s$. Deci, $p_r \mid q_s$.

Din q_s ireductibil şi $p_r \neq 1$ rezultă $p_r \sim q_s$. Fie $u \in U(A)$ pentru care $p_r = uq_s$. Înlocuind în relația (1) şi ținând cont că *A* este inel integru şi $p_r \neq 0$, rezultă:

(2) $$p_1...p_{r-2}p_{r-1} = q_1...q_{s-2}(q_{s-1}u).$$

Deoarece $q_{s-1}u$ este element ireductibil ($q_{s-1}u \sim q_{s-1}$), descompunerii (2) i se poate aplica ipoteza de inducție. Rezultă că $r-1 = s-1$ (deci $r = s$) şi, efectuând o permutare a factorilor, factorii din cele două descompuneri sunt asociați în perechi. Pentru a simplifica scrierea, putem presupune (schimbând eventual ordinea factorilor într-una dintre descompuneri şi renumerotând) că

$$p_1 \sim q_1,\ ...,\ p_{r-2} \sim q_{r-2},\ p_{r-1} \sim q_{r-1}u \sim q_{r-1}.$$

Adăugând relația $p_r \sim q_r$ se obțin toate afirmațiile din enunț, teorema fiind complet demonstrată. □

Într-un inel principal, elementele ireductibile şi elementele prime coincid. În concluzie, elementele nenule şi neinversabile ale unui inel principal se descompun în produse de factori primi şi aceste descompuneri sunt unice în afară de ordinea factorilor şi de asocierea în divizibilitate.

În particular, aceeaşi proprietate o au şi elementele nenule şi neinversabile ale inelelor euclidiene.

Să observăm că rezultatul din teorema 8.3. nu se păstrează dacă presupunem că factorii celor două descompuneri sunt elemente ireductibile. Astfel, în inelul integru $\mathbb{Z}\left[i\sqrt{5}\right]$, are loc relația:

$$3 \cdot 7 = \left(1 + 2i\sqrt{5}\right)\left(1 - 2i\sqrt{5}\right)$$

în care toți factorii sunt ireductibili dar $3 \nmid 1 + 2i\sqrt{5}$ şi $3 \nmid 1 - 2i\sqrt{5}$. Aşa cum vom vedea în paragraful următor, există şi inele care nu sunt principale şi în care elementele nenule şi neinversabile se pot descompune în produse de elemente prime.

9. Inele factoriale

9.1. **Definiție.** *Fie A un inel integru. Se spune că A este* ***inel factorial*** *dacă orice element nenul şi neinversabil din A este produs de elemente prime.*

Exemple. 1°. Inelul $\mathbb{Z}$ al întregilor raționali este un inel factorial. Acest fapt rezultă direct din teorema fundamentală a aritmeticii.

2°. Dacă A este un inel principal, atunci A este inel factorial. În particular, inelele euclidiene sunt inele factoriale. Acest fapt rezultă din teorema 8.2.

3°. Inelele $\mathbb{Z}[i]$ şi $K[X]$ (unde K este corp comutativ) sunt inele factoriale deoarece sunt inele euclidiene.

Alte exemple importante de inele factoriale vor rezulta din consecința 10.9.

Din teorema 8.3. rezultă:

9.2. **Consecință.** *Descompunerea în factori primi a unui element nenul şi neinversabil într-un inel factorial este unică, mai puțin ordinea factorilor şi asocierea în divizibilitate a acestora*.

Datorită unicității descompunerilor în factori primi, este posibilă o "standardizare" a reprezentării elementelor unui inel factorial.

Fie $(p_i)_{i\in I}$ un sistem complet de reprezentanți pentru clasele de echivalență formate din elemente prime.

Aşadar, oricare ar fi $p\in A,$ prim, există şi este unic $i\in I,$ astfel încât $p\sim p_i.$ Deci există $u\in U(A)$ astfel încât:

(1) $$p=up_i.$$

Fie $a\in A,\ a\neq 0,\ a\neq 1.$ Dacă A este inel factorial, atunci a este produs de elemente prime. Dacă pentru fiecare factor prim al lui a facem înlocuiri de forma (1) se obține:

(2) $$a=up_{i_1}^{\alpha_{i_1}}...p_{i_k}^{\alpha_{i_k}}$$

unde $u\in U(A),\ i_j\in I,\ \alpha_{i_j}\in\mathbb{N}^*,\ j\in\overline{1,k}.$

Pentru uniformizarea descompunerilor (2), vom lua $\alpha_i=0$ pentru $i\in I\setminus\{i_1,...,i_k\}$ şi punem:

(3) $$a=u\prod_{i\in I}p_i^{\alpha_i}$$

unde, ca de obicei, $\prod_{i\in I}p_i^{\alpha_i}=\prod_{\substack{i\in I\\ \alpha_i\neq 0}}p_i^{\alpha_i}.$

Extindem această scriere, cu convenția obişnuită, la cazul unei mulțimi vide de indici: $\prod_{i\in I}p_i^0=1.$

În acest mod, orice element $a\in A\setminus\{0\}$ admite o reprezentare de forma (3).

Relațiile de forma (3) poartă numele de ***descompuneri canonice*** ale elementelor nenule ale unui inel factorial.

Dacă

$$u\prod_{i\in I}p_i^{\alpha_i}=v\prod_{i\in I}p_i^{\beta_i},$$

unde $u, v \in U(A)$, $\alpha_i, \beta_j \in \mathbb{N}$, din consecința 9.2., rezultă că $\alpha_i = \beta_i$, $i \in I$. De aici, rezultă $u = v$.

Prin urmare, în descompunerea canonică (3), exponenții $\alpha_i \in \mathbb{N}$ şi factorul $u \in U(A)$ sunt unic determinați.

9.3. **Teoremă.** *Fie A un inel factorial,* $a, b \in A \setminus \{0\}$. *Fie*

$$a = u\prod_{i\in I} p_i^{\alpha_i},\ b = v\prod_{i\in I} p_i^{\beta_i}$$

descompunerile canonice ale lui a şi b. Atunci:

1. $a \mid b \Leftrightarrow \alpha_i \le \beta_i$, *pentru orice* $i \in I$;

2.există $d \sim (a,b)$ *şi* $d \sim \prod_{i\in I} p_i^{\min\{\alpha_i,\beta_i\}}$;

3.există $m \sim [a,b]$ *şi* $m \sim \prod_{i\in I} p_i^{\max\{\alpha_i,\beta_i\}}$.

Demonstrație. 1) Dacă $a \mid b$, există $c \in A \setminus \{0\}$ astfel încât $b = ac$. Fie $c = w\prod_{i\in I} p_i^{\gamma_i}$ descompunerea canonică a lui c. Din relația $b = ac$ rezultă $\beta_i = \alpha_i + \gamma_i \ge \alpha_i$, $i \in I$.

Reciproc, dacă $\alpha_i \le \beta_i$, atunci $b = a \cdot vu^{-1}\prod_{i\in I} p_i^{\beta_i - \alpha_i}$, deci $a \mid b$.

2) Fie $d = \prod_{i\in I} p_i^{\min\{\alpha_i,\beta_i\}}$. Din 1), rezultă $d \mid a$ şi $d \mid b$. Fie $d' \in A$, astfel încât $d' \mid a$ şi $d' \mid b$. Fie $d' = w\prod_{i\in I} p_i^{\gamma_i}$ descompunerea canonică a lui d' (din $a \ne 0$ rezultă $d' \ne 0$). Din $d' \mid a$, rezultă conform 1), $\gamma_i \le \alpha_i$, $i \in I$. Analog, $\gamma_i \le \beta_i$, $i \in I$. Deci, $\gamma_i \le \min\{\alpha_i, \beta_i\}$, $i \in I$, adică $d' \mid d$.

3) Se raționează analog cu 2). □

Se observă că modurile de calcul de la 2) şi 3) pentru cel mai mare divizor comun şi cel mai mic multiplu comun, într-un inel factorial, coincid cu modul de calcul stabilit în clasele elementare pentru cel mai mare divizor comun şi cel mai mic multiplu comun în mulțimea numerelor naturale.

9.4. **Consecință.** *Într-un inel factorial, orice element ireductibil este prim.*

Demonstrație. Rezultă din teorema 9.3. şi din propoziția 3.7. □

Având în vedere definiția 9.1. şi consecința 9.4. se pune problema dacă inelele factoriale ar putea fi definite ca inele integre în care orice element nenul şi neinversabil este produs de elemente ireductibile. Răspunsul la această problemă este negativ. Vom folosi un contraexemplu.

9.5. **Lemă.** *În inelul* $\mathbb{Z}\left[i\sqrt{5}\right]$, *orice element nenul şi neinversabil este un produs de elemente ireductibile.*

Demonstrație. Fie $z = m + ni\sqrt{5} \in \mathbb{Z}\left[i\sqrt{5}\right],\ z \neq 0,\ z \neq 1.$

Vom raționa prin inducție după $N(z) = m^2 + 5n^2$. Valoarea minimă a lui $N(z)$, în acest caz, este 4.

Dacă $N(z) = 4$ şi $d \in \mathbb{Z}\left[i\sqrt{5}\right],\ d \mid z,$ atunci $N(d) \mid 4$ de unde $N(d) \in \{1,2,4\}$. Dacă $N(d) = 1,$ atunci $d \sim 1$. Egalitatea $N(d) = 2$ este imposibilă. Dacă $N(d) = 4 = N(z),$ atunci $d \sim z$. Prin urmare, z este element ireductibil.

Presupunem că elementele lui $\mathbb{Z}\left[i\sqrt{5}\right]$ de normă cuprinsă în $[4, n-1],\ n \geq 5,$ sunt produse de elemente ireductibile.

Fie $z \in \mathbb{Z}\left[i\sqrt{5}\right]$ cu $N(z) = n.$ Dacă z este ireductibil, nu mai este nimic de demonstrat. Altfel, există $z_1, z_2 \in \mathbb{Z}\left[i\sqrt{5}\right]$ astfel încât

$$z = z_1 z_2,\ \ z_1 \neq 1,\ \ z_2 \neq 1.$$

Rezultă $4 \leq N(z_1),\ N(z_2) < n.$ Conform ipotezei de inducție, z_1 şi z_2 sunt produse de elemente ireductibile, deci z este produs de elemente ireductibile. □

Totuşi, inelul $\mathbb{Z}\left[i\sqrt{5}\right]$ nu este un inel factorial în sensul definiției 9.1., deoarece conține elemente ireductibile care nu sunt prime.

Condiția:

(α) "*Orice element nenul şi neinversabil al lui A este un produs de elemente ireductibile*"

rămâne o condiție necesară ca un inel să fie factorial, fără a fi și o condiție suficientă. Se poate completa această condiție pentru a obține condiții necesare și suficiente.

9.6. **Teoremă.** *Fie A un inel integru. Sunt echivalente condițiile:*

1) *A este inel factorial;*

2) *(α) și orice element ireductibil este prim;*

3) *(α) și orice două elemente au un c.m.m.d.c;*

4) *(α) și descompunerea unui element nenul și neinversabil în factori ireductibili este unică în afară de ordinea factorilor și de asocierea în divizibilitate.*

Demonstrație. "$1) \Rightarrow 3)$" rezultă din teorema 9.3.. "$3) \Rightarrow 2)$" rezultă din propoziția 3.7.. "$2) \Rightarrow 1)$" este evidentă. "$1) \Rightarrow 4)$" rezultă din 9.1. și 9.2..

"$4) \Rightarrow 2)$" Fie $q \in A$, un element ireductibil. Va trebui să demonstrăm că dacă $a, b \in A$ și $q \mid ab$, atunci $q \mid a$ sau $q \mid b$.

Dacă unul dintre elementele a și b este zero sau inversabil, atunci implicația este evidentă.

Altfel, $a = q_1 ... q_r$, $b = q_{r+1} ... q_{r+s}$ unde q_j sunt elemente ireductibile, $j \in \overline{1, r+s}$.

Din $q \mid ab$, rezultă că există $c \in A$ pentru care $ab = cq$, iar $c \neq 0$ și $c \neq 1$ (altfel, unul dintre elementele a, b este zero sau inversabil).

Prin urmare, $c = q_1' ... q_t'$ unde q_i' sunt ireductibile, $i \in \overline{1, t}$. Deci,

$$q_1 ... q_{r+s} = q \cdot q_1' ... q_t'.$$

Datorită unicității descompunerii, rezultă că există $j \in \overline{1, r+s}$ astfel încât $q \sim q_j$. Dacă $j \leq r$, atunci $q \mid a$ iar dacă $j > r$, atunci $q \mid b$.

Prin urmare, q este element prim în A. □

10. Factorialitatea inelelor de polinoame

Principalul rezultat al acestui paragraf constă în faptul că proprietatea de inel factorial se transmite de la inelul A la inelul $A[X]$ al polinoamelor.

Reamintim mai întâi câteva proprietăți.

Dacă A este inel integru, atunci şi $A[X]$ este inel integru şi:

$$U(A[X]) = U(A).$$

Dacă p este element prim în inelul integru A, atunci p este element prim şi în inelul $A[X]$ (propoziția 3.9.).

De asemenea, se deduce uşor că dacă $a \in A$ şi $f \in A[X]$, atunci $a \mid f$ dacă şi numai dacă a divide toți coeficienții lui f.

10.1. **Definiție.** *Fie A un unel factorial şi* $f = \sum_{i=0}^{n} a_i X^i \in A[X]$.

Cel mai mare divizor comun al coeficienților polinomului f poartă numele de ***conținut al polinomului*** *f şi se notează* $c(f)$.

$$c(f) \sim (a_0, a_1, ..., a_n).$$

Se spune că f este ***polinom primitiv*** *dacă* $c(f) \sim 1$.

De exemplu, $f = 6X^4 + 3X^2 + 8X + 10$ este un polinom primitiv în $\mathbb{Z}[X]$.

Dacă $f \in A[X] \setminus \{0\}$ (A inel factorial), atunci:

(1) $$f = c(f) \cdot f_1$$

unde f_1 este un polinom primitiv, de acelaşi grad cu f.

Dacă $f \in A[X]$ şi $a \in A$, ținând cont de propoziția 2.7., obținem:

(2) $$c(af) \sim a \cdot c(f).$$

10.2. **Lemă.** (***Gauss***) *Produsul a două polinoame primitive este un polinom primitiv.*

Demonstrație. Fie $f, g \in A[X]$, două polinoame primitive. Să presupunem că fg nu este primitiv.

Din $c(fg) \neq 0$ şi $c(fg) \notin U(A)$, cum A este inel factorial, rezultă că există $p \in A$, prim astfel încât $p \mid c(fg)$. Rezultă $p \mid fg$. Conform

propoziției 3.9., amintite mai sus, p este prim şi în $A[X]$, deci $p \mid f$ sau $p \mid g$. Rezultă $c(f) \notin U(A)$ sau $c(g) \notin U(A)$, contradicție. □

10.3. **Consecință.** *Fie A un inel factorial şi $f, g \in A[X]$. Atunci,*

$$c(fg) \sim c(f) \cdot c(g). \tag{3}$$

Demonstrație. Dacă $f = 0$ sau $g = 0$, atunci:

$$c(fg) \sim 0 \sim c(f) \cdot c(g).$$

Dacă $f \neq 0$ şi $g \neq 0$, atunci $f = c(f) \cdot f_1$, $g = c(g) \cdot g_1$, unde f_1 şi g_1 sunt polinoame primitive. Conform lemei 10.2., $f_1 g_1$ este şi el polinom primitiv. Rezultă:

$$c(fg) = c\big(c(f)c(g)f_1 g_1\big) \sim c(f)c(g)c(f_1 g_1) \sim c(f)c(g). \quad \square$$

10.4. **Lemă.** *Fie A un inel factorial, $f, g \in A[X]$ şi $a \in A \setminus \{0\}$. Dacă f este polinom primitiv şi $f \mid ag$, atunci $f \mid g$.*

Demonstrație. Din $f \mid ag$, rezultă că există $h \in A[X]$ astfel încât:

$$ag = fh. \tag{4}$$

Conform consecinței 10.3.,

$$c(h) \sim c(f)c(h) \sim c(fh) \sim c(ag) \sim ac(g).$$

Introducând un factor inversabil u, ales convenabil, putem scrie:

$$h = c(h)h_1 = uac(g)h_1$$

unde $h_1 \in A[X]$.

Înlocuind în (4), obținem $ag = fuac(g)h_1$. Cum $A[X]$ este inel integru şi $a \neq 0$, rezultă $g = fuc(g)h_1$ deci, $f \mid g$. □

Fie A un inel factorial şi K corpul de fracții al lui A.

Cum $A[X] \subseteq K[X]$ şi $K[X]$ este inel euclidian, este convenabil să transferăm unele proprietăți aritmetice din inelul $A[X]$ în $K[X]$.

10.5. **Lemă.** *Fie A un inel factorial şi K corpul său de fracții. Fie $f \in A[X]$, un polinom de grad ≥ 1. Sunt echivalente afirmațiile:*

a) f este polinom ireductibil în $A[X]$;

b) f este polinom primitiv în $A[X]$ şi ireductibil în $K[X]$.

Demonstrație. "a) $\Rightarrow$ b)" Să presupunem că f este ireductibil în $A[X]$. Cum $f = c(f) \cdot f_1$ şi $d^\circ f \geq 1$, rezultă $c(f) \sim 1$, deci f este po-

linom primitiv în $A[X]$. Să presupunem, prin reducere la absurd, că f este reductibil în $K[X]$. Există atunci $g,h \in K[X]$ astfel încât

(5) $$f = gh,\ \ d^\circ g \geq 1,\ \ d^\circ h \geq 1.$$

Deoarece $g \in K[X]$ şi K este corpul de fracţii al lui A, există $a \in A \setminus \{0\}$ astfel încât $ag \in A[X]$ (a poate fi, de exemplu, cel mai mic multiplu comun al numitorilor coeficienţilor lui g). Analog, există $b \in A \setminus \{0\}$ astfel încât $bh \in A[X]$. Din relaţia (5) rezultă:

(6) $$abf = (ag)(bh) = c(ag)g_1 bh$$

unde $g_1 \in A[X],\ d^\circ g_1 = d^\circ g$ şi g_1 este polinom primitiv.

Deci, $g_1 \mid abf$ în $A[X]$. Conform lemei 10.4., rezultă:

$$g_1 \mid f \text{ şi } 0 < d^\circ g_1 < d^\circ f,$$

contrar ipotezei că f este ireductibil în $A[X]$. Rezultă că f este ireductibil în $K[X]$.

"b) $\Rightarrow$ a)" Să presupunem acum că f este ireductibil în $K[X]$ şi este primitiv în $A[X]$. Fie $f = gh$ unde $g,h \in A[X]$.

Dacă $d^\circ g = 0,$ atunci

$$1 \sim c(f) \sim gc(h),$$

deci $g \in U(A) = U(A[X])$.

Analog, dacă $d^\circ h = 0,$ atunci $h \in U(A) = U(A[X])$.

Dacă $d^\circ g \geq 1$ şi $d^\circ h \geq 1$ rezultă că f este reductibil în $K[X]$, contrar ipotezei făcute.

Deci, din $f = gh,$ cu $g,h \in A[X]$, rezultă $g \sim 1$ sau $h \sim 1$ (în $A[X]$). Prin urmare, f este ireductibil în $A[X]$. □

10.6. **Consecinţă.** *Fie $f \in \mathbb{Z}[X]$ un polinom primitiv cu $d^\circ f \geq 1$. Polinomul f este ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă este ireductibil în $\mathbb{Q}[X]$.*

10.7. **Lemă.** *Dacă A este un inel factorial, atunci orice element ireductibil în $A[X]$ este prim în $A[X]$.*

Demonstraţie. Fie $f \in A[X],$ un element ireductibil.

Dacă $d^\circ f = 0$, f este ireductibil în A. Cum A este inel factorial, f este prim în A, deci prim în $A[X]$.

Considerăm acum cazul $d^\circ f \geq 1$. Conform lemei 10.5., f este polinom primitiv în $A[X]$ şi ireductibil în $K[X]$ unde K este corpul de fracţii al lui A. Fie $g, h \in A[X]$, astfel încât $f \mid gh$. În particular, $f \mid gh$ în $K[X]$. Deoarece $K[X]$ este inel euclidian şi f este ireductibil în $K[X]$, f este prim în $K[X]$. Deci, $f \mid g$ sau $f \mid h$ în $K[X]$.

Să considerăm că $f \mid g$ în $K[X]$. Există $g_1 \in K[X]$ astfel încât $g = g_1 f$. Fie $a \in A \setminus \{0\}$, $ag_1 \in A[X]$. Atunci $ag = f(ag_1)$ sau $f \mid ag$ în $A[X]$.

Deoarece f este polinom primitiv în $A[X]$, conform lemei 10.4., rezultă că $f \mid g$ în $A[X]$.

Cazul $f \mid h$ în $K[X]$ se tratează în mod analog.

Prin urmare, f este polinom prim în $A[X]$. □

Putem, în sfârşit, să prezentăm principalul rezultat al acestui paragraf.

10.8. **Teoremă.** *Dacă A este un inel factorial, atunci $A[X]$ este inel factorial.*

Demonstraţie. Din A inel integru, rezultă $A[X]$ inel integru.

Având în vedere lema 10.7. şi teorema 9.6., este suficient să demonstrăm că orice element nenul şi neinversabil al inelului $A[X]$ este un produs de elemente ireductibile.

Fie $f \in A[X]$, $f \neq 0$ şi $f \notin U(A[X]) = U(A)$. Vom raţiona prin inducţie după $d^\circ f$.

Dacă $d^\circ f = 0$, f este element nenul şi neinversabil al inelului A. Cum A este inel factorial, f este produs de elemente prime în A, deci prime în $A[X]$.

Presupunem că afirmaţia este adevărată pentru polinoame de grad mai mic decât n şi fie $f \in A[X]$ cu $d^\circ f = n$.

Din $f = c(f) \cdot f_1$, cum $c(f) \in A \setminus \{0\}$, rezultă că $c(f)$ este inversabil sau i se aplică raționamentul din prima parte. Rămâne să studiem polinomul primitiv f_1 cu $d^\circ f_1 = n$.

Dacă f_1 este polinom ireductibil, demonstrația se încheie.

Altfel, există $g, h \in A[X]$, astfel încât $f_1 = gh$, $g, h \notin U(A[X])$. Deoarece f_1 este polinom primitiv, $d^\circ g$, $d^\circ h > 0$. Astfel, $d^\circ g < n$ şi $d^\circ h < n$. Conform ipotezei de inducție, *g* şi *h* sunt produse de elemente ireductibile în $A[X]$. Deci f_1 (şi *f*) este produs de elemente ireductibile în $A[X]$. □

10.9. **Consecință.** *Dacă A este inel factorial, atunci* $A[X_1,...,X_n]$ *este inel factorial, pentru orice* $n \geq 1$.

Demonstrație. Se raționează prin inducție după *n*, folosind teorema 10.8. şi ținând cont că:

$$A[X_1,...,X_n] = A[X_1,...,X_{n-1}][X_n] \qquad \square$$

10.10. **Consecință.** *Fie K corp comutativ. Atunci* $K[X_1,...,X_n]$ *este inel factorial, pentru orice* $n \geq 1$.

Demonstrație. Afirmația rezultă din consecința 10.9., ținând cont că inelul $K[X]$ este inel factorial. □

10.11. **Consecință.** *Dacă A este inel factorial, atunci în inelul* $A[X_1,...,X_n]$, $(n \geq 1)$ *orice două elemente au un cel mai mare divizor comun şi orice element ireductibil este prim.*

Demonstrație. Afirmația se obține ca rezultat al consecinței 10.9. şi teoremei 9.6. □

10.12. **Observație.** Fie *A* un inel principal care nu este corp. Conform teoremei 7.3., $A[X]$ nu este inel principal. Pe de altă parte, *A* este inel factorial, deci şi $A[X]$ este inel factorial.

Fie $f, g \in A[X]$. Există $d \sim (f, g)$.

Totuşi, în general, nu există $u, v \in A[X]$ astfel încât $d = uf + vg$. Într-adevăr, existența coeficienților Bézout *u* şi *v* ar atrage după sine egalitatea $(f) + (g) = (d)$.

Această ultimă egalitate este falsă. De exemplu, în condițiile demonstrației teoremei 7.3., pentru

$$g = a \in A \setminus \left(\{0\} \cup U(A)\right) \text{ şi } f = X,$$

obţinem $d \sim 1$, dar $(a) + (X) \neq A[X]$.

Prin urmare, într-un inel factorial, orice două elemente au un cel mai mare divizor comun dar, în general, nu există coeficienţi Bézout.

11. Criterii de ireductibilitate

Fie A un inel factorial. Inelul $A[X]$ este, de asemenea, inel factorial (teorema 10.8.). Deci, orice polinom f cu coeficienţi în A, nenul şi neinversabil, este un produs de polinoame ireductibile în $A[X]$.

Totuşi, descompunerea efectivă a lui f în factori ireductibili este în general o problemă foarte dificilă, chiar dacă în A există un algoritm de descompunere în factori primi.

În aceste condiţii, este util chiar a putea recunoaşte dacă anumite polinoame sunt ireductibile. În continuare, vor fi prezentate câteva condiţii suficiente de ireductibilitate.

11.1. **Propoziţie.** *Fie A un inel factorial. Fie $f = \sum_{i=0}^{n} a_i X^i \in A[X]$, $n \geq 1$, $p \in A$ un element prim şi $k \in \mathbb{N}^*$, $k \leq n$. Dacă:*

$$p \mid a_i, \qquad i \in \overline{0, k-1};$$
$$p \nmid a_k;$$
$$p^2 \nmid a_0,$$

atunci există un factor ireductibil al lui f, de grad $\geq k$.

Demonstraţie. Deoarece A este inel factorial, $A[X]$ este inel factorial, deci f se descompune în $A[X]$ în produs de factori ireductibili:

$$f = f_1 f_2 \ldots f_r, \tag{1}$$

unde $f_i = a_{i0} + a_{i1}X + \ldots + a_{in_i}X^{n_i} \in A[X]$, pentru $i \in \overline{1, r}$.

Deoarece $p \in A$ este element prim, idealul (p) este prim în A, deci $\overline{A} = A/(p)$ este inel integru.

Fie $u: A[X] \to \overline{A}[X]$ morfismul unitar de inele care prelungeşte surjecţia canonică $\pi: A \to \overline{A}$ şi $u(X) = X$. Notând $u(g) = \overline{g}$, pentru orice $g \in A[X]$, din relaţia (1) rezultă:

(2) $$\overline{f} = \overline{f_1} \cdot \overline{f_2} \cdot \ldots \cdot \overline{f_r}.$$

În inelul factor $\overline{A}$, $\hat{a} = \hat{0}$ dacă şi numai dacă $p \mid a$.

Conform ipotezelor:

$$\overline{f} = \widehat{a_k} X^k + \ldots + \widehat{a_n} X^n \in \overline{A}[X], \ \widehat{a_k} \neq \hat{0}.$$

Deoarece $\overline{A}$ este inel integru, X este prim în $\overline{A}[X]$. Din $X \mid \overline{f}$ şi din (2), rezultă că există $i \in \overline{1,r}$, astfel încât $X \mid \overline{f_i}$. Putem presupune, $X \mid \overline{f_1}$, ceea ce este echivalent cu $\widehat{a_{10}} = \hat{0}$, sau $p \mid a_{10}$.

Cazul $k = 1$ este nesemnificativ, evident există cel puţin un factor ireductibil al lui f, de grad ≥ 1.

Ne referim mai departe la cazul $k \geq 2$, deci $X^k \mid \overline{f}$ şi $k \geq 2$.

Dacă există $j > 1$, astfel încât $X \mid \overline{f_j}$, atunci $\widehat{a_{j0}} = \hat{0}$, sau $p \mid a_{j0}$. Rezultă $p^2 \mid a_{10} \cdot \ldots \cdot a_{j0} \cdot \ldots \cdot a_{r0} = a_0$, contrar ipotezei. Deci, $X^k \mid \overline{f_1}$. De aici rezultă $d^\circ \overline{f_1} \geq k$ sau $\overline{f_1} = 0$.

Dacă $\overline{f_1} = 0$, atunci $\overline{f} = 0$, deci $\widehat{a_k} = \hat{0}$, contradicţie.

Astfel, $\overline{f_1} \neq 0$ şi $d^\circ \overline{f_1} \geq k$. Prin urmare, $d^\circ f_1 \geq k$. □

Exemplu. Polinomul

$$f = 3X^4 + 5X^3 + 6X^2 + 2X - 2$$

este ireductibil în $\mathbb{Z}[X]$.

Într-adevăr, $\mathbb{Z}$ este inel factorial iar elementele $p = 2$ şi $k = 3$ satisfac condiţiile din propoziţia 11.1.. Prin urmare, f are un factor ireductibil $f_1 \in \mathbb{Z}[X]$ cu $d^\circ f_1 \geq 3$. Dacă $d^\circ f_1 = 3$, atunci f are şi un factor ireductibil de gradul 1, deci o rădăcină raţională. Dar, ± 1, ± 2, $\pm\frac{1}{3}$, $\pm\frac{2}{3}$ nu sunt rădăcini ale lui f, deci f nu are rădăcini raţionale.

Prin urmare, $d^\circ f_1 = 4$. Deoarece f este polinom primitiv în $\mathbb{Z}[X]$, rezultă $f = f_1$, deci f este ireductibil în $\mathbb{Z}[X]$.

11.2. **Consecință.** (***Criteriul lui Eisenstein***) *Fie A un inel factorial şi $f = \sum_{i=0}^{n} a_i X^i \in A[X]$, $n \geq 1$, un polinom primitiv.*

Presupunem că există $p \in A$ un element prim astfel încât:

$$p \mid a_i, \qquad i \in \overline{0, n-1};$$
$$p \nmid a_n;$$
$$p^2 \nmid a_0.$$

Atunci, f este polinom ireductibil în $A[X]$.

Demonstrație. În propoziția 11.1. luăm $k = n$ şi rezultă că f are un factor ireductibil $f_1 \in A[X]$ cu $d^\circ f_1 = n$. Deoarece f este polinom primitiv, rezultă $f \sim f_1$. □

Dacă în ipoteza criteriului lui Eisenstein omitem condiția ca f să fie polinom primitiv, atunci concluzia devine: f este polinom ireductibil în $K[X]$, K fiind corpul de fracții al lui A.

Într-adevăr, din propoziția 11.1., rezultă că f are în $A[X]$ un factor ireductibil f_1 de grad n. Deci, $f = af_1$, $a \in A \setminus \{0\}$. Conform lemei 10.5., factorul f_1 este ireductibil în $K[X]$. Deoarece $f \sim f_1$ în $K[X]$, f este ireductibil în $K[X]$.

Este cunoscut faptul că în $\mathbb{C}[X]$, singurele polinoame ireductibile sunt cele de gradul 1. De asemenea, în $\mathbb{R}[X]$, singurele polinoame ireductibile sunt cele de gradul 1 şi cele de gradul 2 cu discriminant negativ. În $\mathbb{Q}[X]$, nu are loc un rezultat asemănător.

11.3. **Consecință.** *Pentru orice $n \in \mathbb{N}^*$, există un polinom ireductibil în $\mathbb{Q}[X]$, de grad n.*

Demonstrație. Polinomul $f = X^n - 2 \in \mathbb{Z}[X]$ satisface condițiile din criteriul lui Eisenstein pentru $p = 2$, deci f este ireductibil în $\mathbb{Z}[X]$ şi în $\mathbb{Q}[X]$. □

11.4. **Propoziție.** (***Criteriul reducției***) *Fie A un inel factorial şi B un inel integru. Fie $u: A \to B$ un morfism unitar de inele şi $\bar{u}: A[X] \to B[X]$ unicul morfism de inele care prelungeşte u şi $\bar{u}(X) = X$. Fie $f \in A[X]$ un polinom primitiv de grad ≥ 1. Dacă:*

$$\bar{u}(f) \text{ este ireductibil în } B[X] \text{ şi } d^\circ \bar{u}(f) = d^\circ f,$$

atunci f este ireductibil în $A[X]$.

Demonstrație. Prin reducere la absurd, presupunem că f este reductibil în $A[X]$. Deoarece f este polinom primitiv, rezultă:

$$f = gh, \quad g, h \in A[X], \quad d^\circ g \geq 1, \quad d^\circ h \geq 1.$$

Au loc relațiile:

$$\bar{u}(f) = \bar{u}(g)\bar{u}(h)$$

$$d^\circ f = d^\circ \bar{u}(f) = d^\circ \bar{u}(g) + d^\circ \bar{u}(h) \leq d^\circ g + d^\circ h = d^\circ f.$$

Rezultă $d^\circ \bar{u}(g) = d^\circ g \geq 1$ şi $d^\circ \bar{u}(h) = d^\circ h \geq 1$, deci $\bar{u}(f)$ este reductibil în $B[X]$, contrar ipotezei.

Prin urmare, f este polinom ireductibil în $A[X]$. □

Criteriul lui Eisenstein şi criteriul reducției oferă condiții suficiente ca un polinom să fie ireductibil. Aceste condiții nu sunt în general şi condiții necesare. Astfel, polinomul $f = X^2 + X + 2 \in \mathbb{Z}[X]$ este ireductibil, dar nu satisface condițiile din criteriul lui Eisenstein, pentru niciun număr prim p.

11.5. **Propoziție.** *Fie A un inel factorial şi $f \in A[X]$ un polinom primitiv, $d^\circ f \in \{2,3\}$. Fie K corpul de fracții al lui A. Polinomul f este ireductibil în $A[X]$ dacă şi numai dacă nu are rădăcini în K.*

Demonstrație. Presupunem că f este reductibil în $A[X]$. Deoarece f este polinom primitiv şi $d^\circ f \in \{2,3\}$, f are un factor $g \in A[X]$ de gradul 1, $g = aX + b$, $a \neq 0$. Rezultă că f are în K rădăcina $-a^{-1}b$. Prin urmare, dacă f nu are rădăcini în K, atunci f este ireductibil în $A[X]$.

Să presupunem că f are o rădăcină $\alpha \in K$. Atunci, $X - \alpha \mid f$, deci f este reductibil în $K[X]$. Cum A este inel factorial, rezultă că f este

reductibil în $A[X]$. Prin urmare, dacă f este ireductibil în $A[X]$, atunci f nu are rădăcini în K. □

Exemplu. Polinomul $f = X^3 + X + 1$ este ireductibil în $\mathbb{Z}[X]$. Într-adevăr, f este polinom primitiv şi nu are rădăcini în $\mathbb{Q}$. Conform propoziției 11.4., f este ireductibil în $\mathbb{Z}[X]$ (deci şi în $\mathbb{Q}[X]$).

Probleme propuse

1. Fie inelul $\mathbb{Z}\left[\sqrt{d}\right] = \left\{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\right\}$ unde $d \in \mathbb{Z}$ este un întreg liber de pătrate. Pentru $\alpha = m + n\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$, definim norma sa ca fiind $N(\alpha) = m^2 - dn^2$.

Arătați că pentru orice $\alpha, \beta \in \mathbb{Z}\left[\sqrt{d}\right]$:

a) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$;

b) $\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$;

c) $\alpha \sim \beta \Rightarrow N(\alpha) = \pm N(\beta)$;

d) $\alpha \in U\left(\mathbb{Z}\left[\sqrt{d}\right]\right) \Leftrightarrow N(\alpha) = \pm 1$;

e) $\alpha \mid \beta$ şi $N(\alpha) = \pm N(\beta)$ implică $\alpha \sim \beta$.

2. Arătați că în inelul $\mathbb{Z}\left[i\sqrt{5}\right]$, $\left(3, 1 + i\sqrt{5}\right) \sim 1$, dar elementele 6 şi $2\left(1 + i\sqrt{5}\right)$ nu au un cel mai mare divizor comun.

3. Fie $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$, unde d este întreg liber de pătrate. Arătați că dacă $N(\alpha)$ este număr prim, atunci α este ireductibil în $\mathbb{Z}\left[\sqrt{d}\right]$.

4. Determinați elementele inversabile din inelele: $\mathbb{Z}[i]$, $\mathbb{Z}\left[i\sqrt{3}\right]$, $\mathbb{Z}\left[i\sqrt{5}\right]$.

5. Să se arate că X^2+Y^2 este ireductibil în $\mathbb{Q}[X,Y]$.

6. Să se arate că 2 este reductibil în $\mathbb{Z}[i]$, dar 3 şi $1+i$ sunt ireductibile.

7. Fie $n\geq 3,$ număr natural impar astfel încât $\sqrt{n}\notin\mathbb{Z}.$ Arătaţi că 2 este ireductibil, dar nu este prim în $\mathbb{Z}\left[i\sqrt{n}\right].$

8. Fie $z\in\mathbb{Z}[i]$ cu $N(z)$ număr prim. Atunci, z este prim în $\mathbb{Z}[i]$.

9. Să se arate că un număr prim se descompune în $\mathbb{Z}[i]$ în produsul a cel mult doi factori primi.

10. Arătaţi că:

a) Orice element prim din $\mathbb{Z}[i]$ este divizor al unui număr prim din $\mathbb{Z}$;

b) Orice număr prim p de forma $p=4k+3$ este prim în $\mathbb{Z}[i]$;

c) Orice număr prim p de forma $p=4k+1$ este produsul a două elemente prime din $\mathbb{Z}[i]$ care nu sunt asociate în divizibilitate, dar sunt conjugate unul celuilalt;

d) Arătaţi că orice element prim al inelului $\mathbb{Z}[i]$ este asociat în divizibilitate cu un element al mulţimii $P=\{1+i\}\cup A\cup B$ unde A este mulţimea numerelor naturale prime de forma $p=4k+3$ iar B reuneşte toţi divizorii primi în $\mathbb{Z}[i]$ ai numerelor naturale prime de forma $p=4k+1$.

11. Să se descompună în factori primi în $\mathbb{Z}[i]$ elementele: $21+3i$, $60+90i$, $8+11i$.

12. Fie A un inel euclidian. Dacă $a,b\in A$ sunt relativ prime şi $m,n\in\mathbb{N},$ arătaţi că $\left(a^m-b^m,a^n-b^n\right)\sim a^d-b^d$ unde $d=(m,n).$

13. Fie A un inel întegru şi $\varphi : A \setminus \{0\} \to \mathbb{N}$ o funcție ce verifică proprietatea că pentru orice $a,b \in A,\ b \neq 0,$ există $q,r \in A$ astfel încât $a = bq + r$ unde $r = 0$ sau $\varphi(r) < \varphi(b)$. Definim:

$$\varphi' : A \setminus \{0\} \to \mathbb{N} \text{ prin } \varphi'(x) = \inf_{y \sim x} \{\varphi(y)\}.$$

Arătați că $\left(A, \varphi'\right)$ este inel euclidian.

14. Să se rezolve următoarele ecuații:

a) $375x - 192y = 21$ în $\mathbb{Z}$;

b) $(35 - 35i)x + (-6 + 12i)y = 1 - 7i$ în $\mathbb{Z}[i]$.

15. Fie $a,b \in \mathbb{Z}$ şi θ o rădăcină a ecuației $x^2 + ax + b = 0$.
Arătați că:

a) $\mathbb{Z}[\theta]$ este subinel al lui $\mathbb{C}$ şi $\mathbb{Z}[\theta] \supseteq \mathbb{Z}$.

b) $\mathbb{Z}[\theta] = \mathbb{Z}[\theta']$, unde θ' este cealaltă rădăcină a ecuației. Precizați când $\mathbb{Z}[\theta] = \mathbb{Z}$.

c) Pentru $d = a^2 - 4b < 0$ sau $d > 0$ dar nu pătrat perfect, definim funcția:

$$\varphi : \mathbb{Z}[\theta] \to \mathbb{N},\ \varphi(z) = \left|z\bar{z}\right|, \text{ unde } z = a + b\theta \text{ şi } \bar{z} = a + b\theta'.$$

Arătați că φ este o funcție multiplicativă şi caracterizați cu ajutorul ei elementele inversabile ale inelului $\mathbb{Z}[\theta]$.

d) Determinați o condiție suficientă pentru *a* şi *b* astfel încât inelul $\left(\mathbb{Z}[\theta], \varphi\right)$ să fie euclidian.

16. Arătați că $\mathbb{Z}\left[\sqrt{3}\right]$ şi $\mathbb{Z}\left[i\sqrt{2}\right]$ sunt inele euclidiene.

17. Dacă *A* este inel euclidian iar *S* este un sistem multiplicativ din *A* format din nondivizori ai lui zero, atunci inelul corespunzător de fracții, A_S, este inel euclidian.

18. Fie K un corp comutativ. Arătați că inelul $K[X,Y]/(XY-1)$ este euclidian.

19. Fie A un inel principal şi S un sistem multiplicativ din A format din nondivizori ai lui zero. Arătați că inelul corespunzător de fracții, A_S, este inel principal.

20. Dacă I şi J sunt ideale în $\mathbb{Z}$ astfel încât $IJ = I \cap J$, demonstrați că $I + J = \mathbb{Z}$.

21. Determinați în $\mathbb{Z}[i]$ un generator al idealul $I = (4+i, 1+i)$.

22. Fie A un inel factorial care nu este corp şi care are un număr finit de elemente inversabile. Arătați că în inelul A există o infinitate de elemente ireductibile neasociate în divizibilitate. Caz particular, $A = \mathbb{Z}[i]$.

23. Dacă A este integru, atunci $A[X]$ are o infinitate de elemente ireductibile neasociate.

24. Arătați că într-un inel factorial, idealele prime nenule minimale sunt principale.

25. Dacă A este un inel factorial şi S este un sistem multiplicativ din A format din nondivizori ai lui zero, atunci, inelul de fracții A_S este inel factorial.

26. Precizați care dintre următoare inele sunt euclidiene, principale sau factoriale:

$$\mathbb{Z}[X,Y],\ \mathbb{Z}_5[X,Y],\ \mathbb{Z}_6[X],\ \mathbb{Z}\left[i\sqrt{5}\right],\ \mathbb{Z}\left[\sqrt{26}\right],\ \mathbb{Z}\left[i\sqrt{3}\right].$$

27. Fie A un inel factorial şi $a,b,c \in A \setminus \{0\}$. Arătați că:

a) $[a,b,c](a,b)(b,c)(a,c) \sim abc(a,b,c)$;

b) $([a,b],c) \sim \left[(a,c),(b,c)\right]$;

c) $[(a,b),(b,c),(a,c)] \sim ([a,b],[b,c],[a,c])$.

28. Determinați în $\mathbb{Z}[X]$ un cel mai mare divizor comun pentru polinoamele $X^m - 1$ și $X^n - 1$ unde $m,n \in \mathbb{N}^*$.

29. Descompuneți în factori ireductibili în $\mathbb{R}[X]$, respectiv în $\mathbb{C}[X]$, polinomul $X^{2n} - 1$, $n \geq 1$.

30. Fie K un corp de caracteristică diferită de 2. Arătați că polinomul $X^2 + Y^2 - 1$ este ireductibil în $K[X,Y]$.

31. Să se arate că polinomul $f = X^{n-1} + X^{n-2} + ... + X + 1$ este ireductibil în $\mathbb{Z}[X]$ dacă și numai dacă n este număr prim.

32. Pentru p număr prim și n un număr natural, arătați că polinomul $f = X^{p^n} + p - 1$ este ireductibil în $\mathbb{Z}[X]$.

33. Fie $f = X^p - X + a \in \mathbb{Z}[X]$, unde p este număr prim și $p \nmid a$. Atunci, f este ireductibil în $\mathbb{Z}[X]$.

34. Să se arate că polinomul $f = X^5 - 5X^2 + 1$ este ireductibil în $\mathbb{Z}[X]$.

Capitolul III

EXTINDERI DE CORPURI

Fie $(L,+,\cdot)$ un corp şi K un subcorp al său.

Se spune că L este o ***extindere*** a lui K.

De exemplu:

Corpul complex $\mathbb{C}$ este o extindere a corpului real $\mathbb{R}$.

Corpul real $\mathbb{R}$ este o extindere a corpului numerelor raționale $\mathbb{Q}$.

Corpul $K(X)$ al fracțiilor raționale cu coeficienți în corpul comutativ K, în nedeterminata X, este o extindere a corpului K.

În acest capitol, corpurile vor fi presupuse comutative.

1. Subinel generat de o mulțime peste un corp

Fie $L \supseteq K$ o extindere de copuri şi $\theta \in L$. Orice subinel al lui L care include $K \cup \{\theta\}$, conține produsele de forma $a\theta^i$, $a \in K$, $i \in \mathbb{N}$, deci conține expresii de forma:

$$\sum_{i=0}^{n} a_i \theta^i \tag{1}$$

unde $n \in \mathbb{N}$, $a_i \in K$, $i \in \overline{0,n}$.

Notăm

$$K[\theta] = \left\{ b \in L \,\middle|\, \exists f \in K[X],\ b = f(\theta) \right\} = \left\{ f(\theta) \,\middle|\, f \in K[X] \right\}. \tag{2}$$

Elementele mulțimii $K[\theta]$ sunt de forma (1).

1.1. **Propoziție.** *$K[\theta]$ este subinel al lui L care include $K \cup \{\theta\}$.*

Demonstrație. Pentru $f = a \in K$, $f(\theta) = a \in K[\theta]$. Dacă $f = X$, atunci $f(\theta) = \theta \in K[\theta]$. Deci, $K[\theta] \supseteq K \cup \{\theta\}$.

Fie $b_1, b_2 \in K[\theta]$. Există $f_i \in K[X]$, astfel încât $b_i = f_i(\theta)$, $i \in \overline{1,2}$. Deoarece

$$b_1 - b_2 = f_1(\theta) - f_2(\theta) = (f_1 - f_2)(\theta) \in K[\theta],$$
$$b_1 b_2 = f_1(\theta) f_2(\theta) = (f_1 f_2)(\theta) \in K[\theta],$$

$K[\theta]$ este subinel al lui L. □

Propoziția 1.1. ne permite să dăm următoarea definiție:

1.2. **Definiție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta \in L$. $K[\theta]$ *definit în relația* (2) *poartă numele de* ***subinel generat de*** θ ***peste K***.

Din comentariile făcute la începutul paragrafului, rezultă că inelul $K[\theta]$ este cel mai mic dintre subinelele lui L care includ $K \cup \{\theta\}$.

1.3. **Consecință.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta \in L$. *Atunci,* $K[\theta] = \bigcap_{\substack{H \text{ subinel al lui } L \\ H \supseteq K \cup \{\theta\}}} H$.

Exemple. 1°. În extinderea $\mathbb{R} \supseteq \mathbb{Q}$, fie $\theta = \sqrt{2}$. Dacă considerăm $f = \sum_{i=0}^{n} a_i X_i \in \mathbb{Q}[X]$, atunci, $f\left(\sqrt{2}\right) = \sum_{i=0}^{n} a_i \left(\sqrt{2}\right)^i = a + b\sqrt{2}$, unde a şi b sunt numere raționale. Se deduce:

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}\right\}.$$

Să extindem construcția de mai sus la un număr oarecare de elemente.

Fie $L \supseteq K$ o extindere de corpuri şi $\theta_1, ..., \theta_n \in L$. Notăm

$$(3) \qquad K[\theta_1, ..., \theta_n] = \left\{b \in L \,\middle|\, \exists f \in K[X_1, ..., X_n],\ b = f(\theta_1, ..., \theta_n)\right\}$$
$$= \left\{f(\theta_1, ..., \theta_n) \,\middle|\, f \in K[X_1, ..., X_n]\right\}.$$

Ca şi în cazul $n = 1$, $K[\theta_1, ..., \theta_n]$ este un subinel al lui L care include $K \cup \{\theta_1, ..., \theta_n\}$. $K[\theta_1, ..., \theta_n]$ va fi numit ***subinelul generat de*** $\theta_1, ..., \theta_n$ ***peste K***. În plus, $K[\theta_1, ..., \theta_n]$ este cel mai mic dintre subinelele lui L care includ $K \cup \{\theta_1, ..., \theta_n\}$ şi

$$K[\theta_1, ..., \theta_n] = \bigcap_{\substack{H \text{ subinel al lui } L \\ H \supseteq K \cup \{\theta_1, ..., \theta_n\}}} H.$$

2°. În extinderea $\mathbb{R} \supseteq \mathbb{Q}$, fie $\theta_1 = \sqrt{2}$ şi $\theta_2 = \sqrt{3}$.

$$\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right] = \left\{ f\left(\sqrt{2},\sqrt{3}\right) \middle| f \in \mathbb{Q}[X,Y] \right\} =$$

$$= \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \middle| a,b,c,d \in \mathbb{Q} \right\}.$$

Dacă notăm $M = \{\theta_1,...,\theta_n\} \subseteq L$, unde $L \supseteq K$ este o extindere de corpuri, atunci în loc de $K[\theta_1,...,\theta_n]$ vom scrie $K[M]$. Se observă că dacă M_1 şi M_2 sunt două submulţimi finite ale lui L iar $M_1 \subseteq M_2$, atunci $K[M_1] \subseteq K[M_2]$.

Construcţia de mai sus poate fi extinsă la cazul unei mulţimi infinite.

Fie $L \supseteq K$ o extindere de corpuri şi $M \subseteq L$. Definim:

(4) $$K[M] = \bigcup_{\substack{M' \subseteq M \\ M' \text{ finită}}} K[M'].$$

1.4. **Propoziţie.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $M \subseteq L$. $K[M]$ *definit de* (4) *este un subinel al lui L care include* $K \cup M$.

Demonstraţie. Din (4), rezultă imediat $K[M] \supseteq K \cup M$.

Dacă $b_1, b_2 \in K[M]$, atunci există submulţimile finite M_1 şi M_2 ale lui M, astfel încât $b_i \in K[M_i]$, $i \in \overline{1,2}$.

Cum $K[M_i] \subseteq K[M_1 \cup M_2]$, pentru $i \in \overline{1,2}$, rezultă:

$$b_1 - b_2, b_1 b_2 \in K[M_1 \cup M_2] \subseteq K[M].$$

Prin urmare, $K[M]$ este subinel al lui L. □

1.5. **Definiţie.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $M \subseteq L$. $K[M]$ *definit de* (4) *se numeşte* ***subinel generat de mulţimea M peste corpul K***.

Din relaţia de definiţie (4), rezultă şi faptul că subinelul $K[M]$ este cel mai mic dintre subinelele lui L care includ $K \cup M$. Prin urmare:

$$K[M] = \bigcap_{\substack{H \text{ subinel al lui } L \\ H \supseteq K \cup M}} H.$$

Tot din relația (4) rezultă şi relația:

(5) $K[M]=\left\{f(\theta_1,...,\theta_n)\middle|n\in\mathbb{N}^*,\theta_1,...,\theta_n\in M,f\in K[X_1,...,X_n]\right\}$.

2. Corp de adjuncționare

Construcția din acest paragraf este asemănătoare celei de la 1. Deosebirea este aceea că în loc de subinele vom considera subcorpuri.

Fie $L\supseteq K$ o extindere de copuri şi $\theta\in L$.

Orice subcorp al lui L care include $K\cup\{\theta\}$, va conține şi expresii de forma

(1) $$\frac{f(\theta)}{g(\theta)}$$

unde $f,g\in K[X]$ şi $g(\theta)\neq 0$.

Notăm

(2) $$K(\theta)=\left\{b\in L\middle|\exists f,g\in K[X],\ g(\theta)\neq 0,\ b=\frac{f(\theta)}{g(\theta)}\right\}=$$

$$=\left\{\frac{f(\theta)}{g(\theta)}\middle|f,g\in K[X],\ g(\theta)\neq 0\right\}.$$

2.1. **Propoziție.** *$K(\theta)$ este un subcorp al lui L care include $K\cup\{\theta\}$.*

Demonstrație. Din (2), rezultă că mulțimea $K(\theta)$ este corpul de fracții al inelului $K[\theta]$. În particular, $K(\theta)\supseteq K[\theta]$. □

2.2. **Definiție.** *Fie $L\supseteq K$ o extindere de corpuri şi $\theta\in L$. $K(\theta)$ definit în relația* (2) *poartă numele de* ***corp de adjuncțiune a lui θ la K***.

Din comentariile de la începutul paragrafului, rezultă:

$K(\theta)$ este cel mai mic dintre subcorpurile lui L care includ $K\cup\{\theta\}$. Prin urmare,

(3) $$K(\theta)=\bigcap_{\substack{H\text{ subcorp al lui }L\\ H\supseteq K\cup\{\theta\}}}H.$$

Exemplu. În extinderea $\mathbb{R} \supseteq \mathbb{Q}$, pentru $\theta = \sqrt{2}$:

$$\mathbb{Q}\left(\sqrt{2}\right) = \left\{ \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \middle| a,b,c,d \in \mathbb{Q},\ c+d\sqrt{2} \neq 0 \right\} =$$

$$= \left\{ u+v\sqrt{2} \middle| u,v \in \mathbb{Q} \right\} = \mathbb{Q}\left[\sqrt{2}\right].$$

2.3. **Definiție.** *Se spune că extinderea $L \supseteq K$ este **simplă** dacă există $\theta \in L$ astfel încât $L = K(\theta)$. Elementul θ din această egalitate se numeşte **element primitiv** al extinderii.*

Extinderea $\mathbb{C} \supseteq \mathbb{R}$ este simplă deoarece $\mathbb{C} = \mathbb{R}(i)$. Un element primitiv al extinderii este numărul complex i. Mai există şi alte elemente primitive ale extinderii ca: $-i$, $1+i$, etc.

Extinderea $K(X) \supseteq K$, K corp comutativ, este tot o extindere simplă, X, $1-X$, $\frac{1}{X}$ fiind elemente primitive ale sale.

Fie $L \supseteq K$ o extindere de corpuri şi $\theta_1,...,\theta_n \in L$. Notăm

$$(4)\quad K(\theta_1,...,\theta_n) = \left\{ \frac{f(\theta_1,...,\theta_n)}{g(\theta_1,...,\theta_n)} \middle| f,g \in K[X_1,...,X_n],\ g(\theta_1,...,\theta_n) \neq 0 \right\}.$$

Din (4), rezultă că mulțimea $K(\theta_1,...,\theta_n)$ este corpul de fracții al inelului $K[\theta_1,...,\theta_n]$. $K(\theta_1,...,\theta_n)$ poartă numele de ***corp de adjuncționare a elementelor $\theta_1,...,\theta_n$ la K***.

Tot din relația (4) rezultă: $K(\theta_1,...,\theta_n)$ este cel mai mic dintre subcorpurile lui L care includ $K \cup \{\theta_1,...,\theta_n\}$ şi

$$K(\theta_1,...,\theta_n) = \bigcap_{\substack{H \text{ subcorp al lui } L \\ H \supseteq K \cup \{\theta_1,...,\theta_n\}}} H.$$

Notând $M = \{\theta_1,...,\theta_n\}$, vom scrie şi $K(\theta_1,...,\theta_n) = K(M)$.
Dacă M_1 şi M_2 sunt două submulțimi finite ale lui L iar $M_1 \subseteq M_2$, atunci $K(M_1) \subseteq K(M_2)$.

2.4. **Definiție.** *Se spune că extinderea $L \supseteq K$ este **de tip finit**, dacă există o submulțime finită M a lui L, astfel încât $L = K(M)$.*

Fie $L \supseteq K$ o extindere de corpuri şi M o submulţime oarecare a lui L. Definim:

(5) $$K(M) = \bigcup_{\substack{M' \subseteq M \\ M' \text{ finită}}} K(M').$$

2.5. **Propoziţie.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $M \subseteq L$. $K(M)$ *definit de* (5) *este un subcorp al lui L care include* $K \cup M$.

Demonstraţie. Din (5), rezultă imediat $K(M) \supseteq K \cup M$.

Dacă $b_1, b_2 \in K(M)$, atunci există submulţimile finite M_1 şi M_2 ale lui M, astfel încât $b_i \in K(M_i)$, $i \in \overline{1,2}$.

Cum $K(M_i) \subseteq K(M_1 \cup M_2)$, pentru $i \in \overline{1,2}$, şi $K(M_1 \cup M_2)$ este corp, rezultă:

$$b_1 - b_2,\ b_1 b_2,\ b_1^{-1}(b_1 \neq 0) \in K(M_1 \cup M_2) \subseteq K(M).$$

Prin urmare, $K(M)$ este subcorp al lui L. □

2.6. **Definiţie.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $M \subseteq L$. *Corpul* $K(M)$ *definit de relaţia* (5) *se numeşte* ***corp de adjuncţionare a mulţimii M la K***.

Din (5) şi din propoziţia 2.5., rezultă:

- $K(M)$ este cel mai mic dintre subcorpurile lui L care includ $K \cup M$.
- $K(M) = \bigcap_{\substack{H \text{ subcorp al lui } L \\ H \supseteq K \cup M}} H$.
- $K(M)$ este corpul de fracţii al lui $K[M]$.

2.7. **Propoziţie.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* M_1, M_2 *submulţimi ale lui L. atunci:*

a) *Dacă* $M_1 \subseteq M_2$, *atunci* $K(M_1) \subseteq K(M_2)$;

b) $K(M_1 \cup M_2) = K(M_1)(M_2)$.

Demonstraţie. a) rezultă direct din definiţia 2.4.

b) Din $M_1 \subseteq M_1 \cup M_2$, conform a), $K(M_1) \subseteq K(M_1 \cup M_2)$. Cum şi $M_2 \subseteq M_1 \cup M_2$, iar $K(M_1)(M_2)$ este cel mai mic subcorp al lui L care include $K(M_1) \cup M_2$, rezultă $K(M_1)(M_2) \subseteq K(M_1 \cup M_2)$.

Reciproc, din $K \cup (M_1 \cup M_2) \subseteq K(M_1)(M_2)$, rezultă celalată incluziune: $K(M_1 \cup M_2) \subseteq K(M_1)(M_2)$.
Prin urmare, $K(M_1)(M_2) = K(M_1 \cup M_2)$. □

3. Gradul unei extinderi. Extinderi finite

Fie *L* o extindere a corpului *K*. *L* poate fi organizat în mod natural cu o structură de spațiu vectorial peste *K*, astfel:

- grupul abelian $(L,+)$ este grupul subiacent al corpului $(L,+,\cdot)$;
- legea de compoziție externă

$$K \times L \to L,\ (a,x) \to ax,\ a \in K,\ x \in L,$$

este restricția operației multiplicative

$$L \times L \to L,\ (a,b) \to ab,\ a,b \in L.$$

Din axiomele structurii de corp a lui *L*, rezultă:

$$a(x+y) = ax + ay,$$
$$(a+b)x = ax + bx,$$
$$a(bx) = (ab)x,$$
$$1x = x,$$

oricare ar fi $a,b \in K$ şi oricare ar fi $x,y \in L$.

Deci, *L* este spațiu vectorial peste *K*.

În spațiul vectorial ${}_K L$, se poate vorbi despre dimensiune.

3.1. **Definiție.** *Fie $L \supseteq K$ o extindere de corpuri. Dimensiunea spațiului vectorial ${}_K L$ se numeşte* ***grad al extinderii*** *$L \supseteq K$ şi se notează $[L:K]$. Se spune că* ***extinderea*** *$L \supseteq K$ este* ***finită*** *dacă gradul său este finit:*

$$[L:K] = \dim {}_K L = n < \infty.$$

În caz contrar, ***extinderea*** *$L \supseteq K$ este* ***infinită*** *şi se notează*

$$[L:K] = \infty.$$

Extinderea $K \supseteq K$, unde *K* este un corp comutativ oarecare, este finită şi are gradul $[K:K] = 1$. Într-adevăr, $\{1\}$ este evident o bază în ${}_K K$, deci $\dim {}_K K = 1$. Reciproc, din $\dim {}_K L = 1$ şi $ind_K \{1\}$ rezultă că $\{1\}$ este o bază în ${}_K L$, deci $L = \{a \cdot 1 \mid a \in K\} = K$.

Extinderea $\mathbb{C} \supseteq \mathbb{R}$ este finită şi are gradul 2. Este suficient să arătăm că $\{1, i\}$ este o bază a spaţiului vectorial ${}_{\mathbb{R}}\mathbb{C}$. Într-adevăr,

$$\forall z \in \mathbb{C},\ \exists!\ a, b \in \mathbb{R},\ \text{astfel încât}\ z = a \cdot 1 + b \cdot i.$$

Deci, $[\mathbb{C} : \mathbb{R}] = \dim_{\mathbb{R}} \mathbb{C} = 2$.

Extinderea $K(X) \supseteq K$ este infinită (K este un corp comutativ oarecare). Este suficient să observăm că mulţimea

$$\{1, X, X^2, ..., X^n, ...\}$$

este liniar independentă peste K.

3.2. **Propoziţie.** *Orice extindere finită este o extindere de tip finit.*

Demonstraţie. Fie $L \supseteq K$ o extindere finită de grad $n = \dim_K L$. Fie $(e_1, ..., e_n)$ o bază a lui ${}_K L$. Au loc relaţiile:

$$L = \left\{ \sum_{i=1}^{n} a_i e_i \,\middle|\, a_i \in K,\ i \in \overline{1,n} \right\} \subseteq K(e_1, ..., e_n) \subseteq L.$$

Rezultă $L = K(e_1, ..., e_n)$, deci $L \supseteq K$ este o extindere de tip finit. □

Se observă că reciproca propoziţiei 3.2. nu este adevărată. Extinderea $K(X) \supseteq K$ (K corp comutativ) este o extindere de tip finit, chiar simplă, dar nu este extindere finită.

3.3. **Propoziţie.** (***tranzitivitatea extinderilor finite***) *Fie extinderile de corpuri $E \supseteq L$ şi $L \supseteq K$. Extinderea $E \supseteq K$ este finită dacă şi numai dacă extinderile $E \supseteq L$ şi $L \supseteq K$ sunt finite. În acest caz:*

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

Demonstraţie. Să presupunem că extinderea $E \supseteq K$ este finită. Deci, $\dim_K E = n < \infty$. Deoarece L este subspaţiu al lui ${}_K E$, $\dim_K L$ este finită, deci $L \supseteq K$ este extindere finită. Orice bază (finită) a lui ${}_K E$ este un sistem de generatori al lui ${}_L E$, deci şi $E \supseteq L$ este extindere finită.

Reciproc, presupunem că $E \supseteq L$ şi $L \supseteq K$ sunt finite.

Fie $[E : L] = p = \dim_L E$ şi $(y_1, ..., y_p)$ o bază a lui ${}_L E$.

Fie $[L : K] = q = \dim_K L$ şi $(x_1, ..., x_q)$ o bază a lui ${}_K L$.

Fie $z \in E$. Deoarece $(y_1,...,y_p)$ o bază a lui ${}_L E$, există $b_1,...,b_p \in L$, astfel încât:

(1) $$z = \sum_{j=1}^{p} b_j y_j.$$

Din $b_j \in L$, $j \in \overline{1,p}$ şi $(x_1,...,x_q)$ bază în ${}_K L$, rezultă că există $a_{1j},...,a_{qj} \in K$, astfel încât

(2) $$b_j = \sum_{i=1}^{q} a_{ij} x_i.$$

Înlocuind (2) în (1), rezultă:

$$z = \sum_{j=1}^{p} \sum_{i=1}^{q} a_{ij} x_i y_j.$$

Prin urmare, $\left(x_i y_j\right)_{\substack{i \in \overline{1,q} \\ j \in \overline{1,p}}}$ formează un sistem de generatori în ${}_K E$.

Fie $c_{ij} \in K$, $i \in \overline{1,q}$, $j \in \overline{1,p}$ astfel încât:

(3) $$\sum_{i=1}^{q} \sum_{j=1}^{p} c_{ij} x_i y_j = 0.$$

Relația (3) se mai poate scrie:

(4) $$\sum_{j=1}^{p} \left(\sum_{i=1}^{q} c_{ij} x_i \right) y_j = 0.$$

Deoarece $\sum_{i=1}^{q} c_{ij} x_i \in L$, $j \in \overline{1,p}$ şi $(y_1,...,y_p)$ este o bază în ${}_L E$, rezultă:

(5) $$\sum_{i=1}^{q} c_{ij} x_i = 0, \quad j \in \overline{1,p}.$$

Din $ind_K(x_1,...,x_q)$ şi din (5), rezultă $c_{ij} = 0$, $i \in \overline{1,q}$, $j \in \overline{1,p}$.

Prin urmare, $ind_K \left(x_i y_j\right)_{\substack{i \in \overline{1,q} \\ j \in \overline{1,p}}}$ şi, în final, $\left(x_i y_j\right)_{\substack{i \in \overline{1,q} \\ j \in \overline{1,p}}}$ formează o bază în ${}_K E$. În particular, $E \supseteq K$ este extindere finită şi

$$[E:K] = \dim_K E = pq = [E:L][L:K]. \qquad \square$$

3.4. **Propoziție.** *Fie* $L \supseteq K$ *o extindere finită, de grad n. Atunci:*

$$cardL = (cardK)^n.$$

Demonstrație. Fie $(e_1,...,e_n)$ o bază a lui ${}_K L$. Pentru orice $y \in L$ există şi sunt unici $c_1,...,c_n \in K$ astfel încât $y = \sum_{i=1}^{n} c_i e_i$. Rezultă că aplicația

$$K^n \to L,\ (c_1,...,c_n) \to \sum_{i=1}^{n} c_i e_i$$

este o bijecție. Prin urmare, $cardL = (cardK)^n$. □

4. Elemente algebrice şi elemente transcendente

Fie $L \supseteq K$ o extindere de corpuri şi $\theta \in L$. Relația (2) din III.1., sugerează definirea unei aplicații:

(1) $$u_\theta : K[X] \to K[\theta],$$

(2) $$u_\theta(f) = f(\theta),\ \ \forall f \in K[X].$$

Dacă $f, g \in K[X]$, atunci:

$$u_\theta(f+g) = (f+g)(\theta) = f(\theta) + g(\theta) = u_\theta(f) + u_\theta(g),$$
$$u_\theta(fg) = (fg)(\theta) = f(\theta)g(\theta) = u_\theta(f)u_\theta(g).$$

Prin urmare, u_θ este un morfism de inele. Din aceeaşi relație (2), III.1., rezultă că morfismul u_θ este surjectiv.

Vom considera în continuare două cazuri, după cum u_θ este sau nu injectiv.

Cazul I. Morfismul u_θ este injectiv. Afirmația este echivalentă cu $Keru_\theta = (0)$ sau cu a spune că singurul polinom f din $K[X]$ pentru care $u_\theta(f) = 0$ este polinomul nul.

4.1. **Definiție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta \in L$. *Se spune că* ***elementul*** θ *este* ***transcendent peste K*** (*sau* ***algebric independent peste K***) *dacă*:

$$\forall f \in K[X],\ \ f(\theta) = 0 \Rightarrow f = 0.$$

În general, demonstrarea transcendenței unui element este dificilă şi vom reveni asupra acestei probleme în III.10.

Numărul real π (raportul dintre lungimea unui cerc şi lungimea diametrului său) este transcendent peste $\mathbb{Q}$. Acest fapt a fost demonstrat pentru prima dată de către Lindemann în anul 1882.

Numărul real $e = \lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ este transcendent peste $\mathbb{Q}$. Acest fapt a fost demonstrat pentru prima dată de către Hermite în 1873.

Cazul II. Morfismul u_θ nu este injectiv. Această condiție este echivalentă cu $Keru_\theta \neq (0)$, sau cu a spune că există polinoame nenule $f \in K[X]$, astfel încât $f(\theta) = 0$.

4.2. **Definiție.** *Fie $L \supseteq K$ o extindere de corpuri şi $\theta \in L$. Se spune că* ***elementul*** θ *este* ***algebric peste K*** (*sau* ***algebric dependent peste K***) *dacă*:

$$\exists f \in K[X]\setminus\{0\},\ \textit{astfel încât}\ f(\theta) = 0.$$

Fie $a \in K$. Pentru că $f = X - a \in K[X]\setminus\{0\}$, verifică $f(a) = 0$, rezultă că *a* este algebric peste *K*.

Numărul $\sqrt{2} \in \mathbb{R}$ este algebric peste $\mathbb{Q}$. Într-adevăr, există polinomul $f = X^2 - 2 \in \mathbb{Q}[X]\setminus\{0\}$ cu $f\left(\sqrt{2}\right) = 0$.

Orice număr complex este algebric peste corpul numerelor reale. Într-adevăr, dacă $x = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, atunci:

$$f = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]\setminus\{0\} \text{ şi } f(x) = 0.$$

Fie $\theta \in L$, arbitrar ales, algebric peste *K*. Deoarece $Keru_\theta \neq (0)$ este ideal în $K[X]$ iar $K[X]$ este inel principal, $Keru_\theta$ este un ideal principal, generat de un polinom nenul. Acest generator este unic determinat dacă punem în plus condiția ca el să fie polinom unitar.

4.3. **Definiție.** *Fie θ un element algebric al extinderii $L \supseteq K$. Numim* ***polinom minimal al lui*** θ *peste K un polinom $p_\theta \in K[X]$ care satisface condițiile*:

a) $p_\theta(\theta) = 0$;

b) $\forall f \in K[X],\ f(\theta) = 0 \Rightarrow p_\theta \mid f$;

c) p_θ *este polinom unitar*.

Condițiile a) şi b) arată că p_θ este un generator al lui $Keru_\theta$ iar condiția c) determină p_θ în mod unic.

Pentru $\theta = \sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$, polinomul minimal al lui $\sqrt{2}$ peste $\mathbb{Q}$ este $p_{\sqrt{2}} = X^2 - 2 \in \mathbb{Q}[X]$. Într-adevăr, $p_{\sqrt{2}}\left(\sqrt{2}\right) = 0$. Fie $f \in \mathbb{Q}[X]$ pentru care $f\left(\sqrt{2}\right) = 0$. Atunci $f\left(-\sqrt{2}\right) = 0$ şi

$$\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right) = X^2 - 2 \mid f.$$

Pentru un număr complex $z = a + bi$ cu $b \neq 0$, polinomul minimal al lui z peste $\mathbb{R}$ este $p_z = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$. Se verifică $p_z(z) = 0$. Fie $f \in \mathbb{R}[X]$, astfel încât $f(z) = 0$. Atunci $f(\bar{z}) = 0$. Prin urmare, $\left(X - z\right)\left(X - \bar{z}\right) = X^2 - 2aX + a^2 + b^2 \mid f$.

Condiția b) din definiția 4.3. arată că polinomul minimal al elementului θ, algebric peste K, este de grad minim printre polinoamele nenule cu coeficienți în K care admit pe θ ca rădăcină.

4.4. **Propoziție.** *Fie* θ *un element algebric al extinderii* $L \supseteq K$. *Polinomul minimal* p_θ *al lui* θ *peste* K *este ireductibil în* $K[X]$.

Demonstrație. Presupunem, prin reducere la absurd, că p_θ este reductibil peste K. Există $g, h \in K[X]$ astfel încât:

$$p_\theta = gh, \quad d^\circ g < d^\circ p_\theta \text{ şi } d^\circ h < d^\circ p_\theta.$$

Din $0 = p_\theta(\theta) = g(\theta)h(\theta)$ rezultă $g(\theta) = 0$ sau $h(\theta) = 0$, contradicție cu faptul că p_θ este de grad minim printre polinoamele nenule cu coeficienți în K care admit pe θ ca rădăcină.

Se poate da şi o altă demonstrație care pune în evidență şi alte aspecte. Să aplicăm teorema fundamentală de izomorfism morfismului surjectiv de inele u_θ din (1), ținând seama că $\mathrm{Im}\, u_\theta = K[\theta]$ şi $Keru_\theta = (p_\theta)$. Rezultă:

(3) $$K[X]/(p_\theta) \simeq K[\theta].$$

Cum $K[\theta]$, ca subinel al corpului comutativ K, este domeniu de integritate, din (3) rezultă că (p_θ) este ideal prim nenul al lui $K[X]$. Astfel, p_θ este polinom ireductibil în $K[X]$. □

4.5. **Propoziție.** *Fie* $L \supseteq K$ *o extindere de corpuri,* $\theta \in L$ *şi* f *un polinom ireductibil şi unitar din* $K[X]$ *astfel încât* $f(\theta) = 0$. *Atunci,* $f = p_\theta$.

Demonstrație. Din ipoteze şi din condiția b) a definiției 4.3. rezultă $p_\theta \mid f$. Deoarece f este ireductibil şi $p_\theta \neq 1$, rezultă $p_\theta \sim f$. Cum ambele polinoame sunt unitare, rezultă $f = p_\theta$. □

4.6. **Propoziție.** *Fie* $L \supseteq K$ *o extindere finită şi* $\theta \in L$. *Atunci,* θ *este algebric peste K.*

Demonstrație. Fie $[L:K] = \dim_K L = n < \infty$. Cele $n+1$ elemente $1, \theta, \theta^2, ..., \theta^n \in L$ sunt liniar dependente peste K. Prin urmare, există $c_i \in K$, $i \in \overline{0,n}$, nu toate nule astfel încât:

(4) $$c_0 \cdot 1 + c_1\theta + c_2\theta^2 + ... + c_n\theta^n = 0$$

Fie $f = \sum_{i=0}^{n} c_i X_i \in K[X] \setminus \{0\}$. Din relația (4) rezultă $f(\theta) = 0$ şi astfel θ este algebric peste K. □

4.7. **Propoziție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta \in L$ *un element algebric peste K. Atunci*:

a) $K[\theta] = K(\theta)$;

b) *Extinderea* $K(\theta) \supseteq K$ *este finită şi* $[K(\theta):K] = d^\circ p_\theta$, *unde* p_θ *este polinomul minimal al lui* θ *peste K.*

Demonstrație. a) Revenim la relația (3) din demonstrația propoziției 4.4.:

(3) $$K[X]/(p_\theta) \simeq K[\theta].$$

Deoarece polinomul p_θ este ireductibil în inelul principal $K[X]$, idealul (p_θ) este maximal şi, ca urmare, $K[X]/(p_\theta)$ este corp. $K[\theta]$ este astfel corp şi coincide cu corpul său de fracții $K(\theta)$.

Pentru a demonstra b), fie $n = d^\circ p_\theta$. Este suficient să arătăm că:

(5) $$\left\{1, \theta, \theta^2, ..., \theta^{n-1}\right\}$$

formează o bază în ${}_K K(\theta)$. Fie $b \in K(\theta) = K[\theta]$. Există atunci f din $K[X]$ astfel încât $b = f(\theta)$. Deoarece $p_\theta \neq 0$, există şi sunt unice $q, r \in K[X]$ astfel încât $f = p_\theta q + r$ şi $d^\circ r < d^\circ p_\theta = n$.

$$b = f(\theta) = q(\theta) p_\theta(\theta) + r(\theta) = r(\theta) = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$$

unde $a_0, a_1, ..., a_{n-1} \in K$. Rezultă că (5) este un sistem de generatori în ${}_K K(\theta)$. Fie $c_0, c_1, ..., c_{n-1} \in K$ astfel încât

(6) $$\sum_{i=0}^{n-1} c_i \theta^i = 0.$$

Notăm $g = \sum_{i=0}^{n-1} c_i X_i \in K[X]$. Din (6) rezultă că $g(\theta) = 0$. Deoarece $d^\circ g < d^\circ p_\theta$ şi p_θ este de grad minim printre polinoamele nenule care admit θ ca rădăcină, rezultă $g = 0$. Deci, $c_i = 0$, $i \in \overline{0, n-1}$ şi elementele (5) sunt liniar independente peste K. Prin urmare, (5) este o bază în ${}_K K(\theta)$. Atunci, extinderea $K(\theta) \supseteq K$ este finită, de grad $n = d^\circ p_\theta$. □

4.8. **Propoziție.** *Fie $L \supseteq K$ o extindere de corpuri şi $\theta \in L$ un element transcendent peste K. Atunci*:

$$K[\theta] \simeq K[X].$$

În particular, extinderea $K(\theta) \supseteq K$ este infinită.

Demonstrație. Deoarece θ este transcendent peste K, morfismul

(1) $$u_\theta : K[X] \to K[\theta],$$

(2) $$u_\theta(f) = f(\theta), \quad \forall f \in K[X]$$

este un izomorfism de inele. Pentru că

$$u_\theta(cf) = (cf)(\theta) = cf(\theta) = c \cdot u_\theta(f), \quad \forall c \in K, \quad \forall f \in K[X]$$

este şi un izomorfism de K-spații vectoriale. Atunci,

$$\dim {}_K K[\theta] = \dim {}_K K[X] = \infty.$$

Cum $K[\theta]$ este subspațiu al spațiului vectorial ${}_K K(\theta)$, rezultă $\dim {}_K K(\theta) = \infty$ şi deci $K(\theta) \supseteq K$ este extindere infinită. □

4.9. **Consecință.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta_1,...,\theta_n$ *elemente din L, algebrice peste K. Atunci:*

a) $K[\theta_1,...,\theta_n] = K(\theta_1,...,\theta_n)$;

b) $K(\theta_1,...,\theta_n) \supseteq K$ *este extindere finită.*

Demonstrație. Raționăm prin inducție după *n*. Pentru $n = 1$, afirmațiile rezultă din propoziția 4.7. Presupunem a) şi b) adevărate pentru orice *n* elemente algebrice peste *K*, $n \geq 1$.

Fie $\theta_1,...,\theta_n,\theta_{n+1} \in L$ algebrice peste *K*. Conform ipotezei de inducție, $K[\theta_1,...,\theta_n] = K(\theta_1,...,\theta_n)$ şi extinderea $K(\theta_1,...,\theta_n) \supseteq K$ este finită.

Din θ_{n+1} algebric peste *K* rezultă θ_{n+1} algebric peste $K(\theta_1,...,\theta_n)$ şi, conform 4.7.,

(7) $K[\theta_1,...,\theta_n][\theta_{n+1}] = K(\theta_1,...,\theta_n)(\theta_{n+1})$ şi

(8) $K(\theta_1,...,\theta_n)(\theta_{n+1}) \supseteq K(\theta_1,...,\theta_n)$ este extindere finită.

Rezultă:

$$K[\theta_1,...,\theta_n,\theta_{n+1}] = K[\theta_1,...,\theta_n][\theta_{n+1}] = K(\theta_1,...,\theta_n)[\theta_{n+1}] =$$
$$= K(\theta_1,...,\theta_n)(\theta_{n+1}) = K(\theta_1,...,\theta_n,\theta_{n+1}).$$

Din ipoteza de inducție b) şi din (8), rezultă că $K(\theta_1,...,\theta_n,\theta_{n+1}) \supseteq K$ este extindere finită. □

Noțiunea de dependență algebrică poate fi extinsă la un număr oarecare de elemente.

4.10. **Definiție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\theta_1,...,\theta_n$ *elemente din L.*

Se spune că elementele $\theta_1,...,\theta_n$ *sunt* ***algebric dependente peste K*** *dacă există* $f \in K[X_1,...,X_n] \setminus \{0\}$ *astfel încât* $f(\theta_1,...,\theta_n) = 0$. *În caz contrar, spunem că elementele* $\theta_1,...,\theta_n$ *sunt* ***algebric independente peste K****.*

Se spune că mulțimea $M \subseteq L$ *este* ***algebric dependentă peste K*** *dacă există o submulțime finită a lui M, algebric dependentă peste K. În caz contrar, se spune că M este* ***algebric independentă peste K****.*

Pentru orice număr real *a*, numerele reale $\sin a$ şi $\cos a$ sunt algebric dependente peste $\mathbb{Q}$. Într-adevăr, pentru

$$f(X_1, X_2) = X_1^2 + X_2^2 - 1 \in \mathbb{Q}[X_1, X_2] \setminus \{0\},$$
$f(\sin a, \cos a) = 0.$

Fie $L \supseteq K$ o extindere de corpuri şi $M \subseteq L$.

Dacă M este algebric dependentă peste K şi $M_1 \subseteq L$, $M_1 \supseteq M$, atunci M_1 este algebric dependentă peste K.

Dacă M este algebric independentă peste K şi $M_1 \subseteq M$, atunci M_1 este algebric independentă peste K.

5. Extinderi algebrice şi extinderi transcendente

5.1. **Definiţie.** *Fie $L \supseteq K$ o extindere de corpuri. Se spune că $L \supseteq K$ este* ***extindere algebrică*** *dacă orice element al lui L este algebric peste K. În caz contrar, se spune că $L \supseteq K$ este* ***extindere transcendentă***.

Extinderea $\mathbb{C} \supseteq \mathbb{R}$ este o extindere algebrică deoarece orice număr complex este algebric peste $\mathbb{R}$.

Extinderea $\mathbb{R} \supseteq \mathbb{Q}$ este transcendentă deoarece există numărul real π care este transcendent peste $\mathbb{Q}$.

5.2. **Propoziţie.** *Dacă $L \supseteq K$ este o extindere finită, atunci extinderea $L \supseteq K$ este algebrică.*

Demonstraţie. Rezultă direct din 4.6. □

5.3. **Propoziţie.** (**tranzitivitatea extinderilor algebrice**) *Fie extinderile de corpuri $E \supseteq L$ şi $L \supseteq K$. Atunci, extinderea $E \supseteq K$ este algebrică dacă şi numai dacă extinderile $E \supseteq L$ şi $L \supseteq K$ sunt algebrice.*

Demonstraţie. Să presupunem că extinderea $E \supseteq K$ este algebrică. Atunci, orice element al lui E este algebric peste K. În particular, orice element al lui L este algebric peste K, deci $L \supseteq K$ este extindere algebrică. Fie $\theta \in E$. Cum $E \supseteq K$ este extindere algebrică, există un polinom nenul $f \in K[X] \subseteq L[X]$ astfel încât $f(\theta) = 0$. Prin urmare, θ este algebric şi peste L, deci $E \supseteq L$ este extindere algebrică.

Reciproc, să presupunem că extinderile $E \supseteq L$ şi $L \supseteq K$ sunt algebrice. Fie $\theta \in E$. Din θ algebric peste *L* rezultă că există

$$f = a_0 + a_1 X + ... + a_n X^n \in L[X] \setminus \{0\}$$

astfel încât $f(\theta) = 0$. Deoarece $a_0, a_1, ..., a_n \in L$ sunt algebrice peste *K*, rezultă, conform 4.9., că extinderea:

(1) $$L' = K(a_0, a_1, ..., a_n) \supseteq K$$

este finită. Evident, θ este algebric peste L'. Conform 4.7., extinderea:

(2) $$L'(\theta) \supseteq L'$$

este finită. Din relațiile (1), (2) şi din propoziția 3.3., rezultă că extinderea $L'(\theta) \supseteq K$ este finită, deci algebrică, conform 5.2. Astfel, θ este algebric peste *K*. Cum θ este un element oarecare din *E*, rezultă că $E \supseteq K$ este extindere algebrică. □

5.4. **Propoziție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi*

(3) $$L' = \left\{\theta \in L \middle| \theta \text{ este algebric peste } K\right\}.$$

Atunci, L' *este subcorp al lui L, care include K.*

Demonstrație. Dacă $a \in K$, atunci *a* este rădăcina polinomului nenul $f = X - a \in K[X]$ şi *a* este algebric peste *K*. Rezultă $K \subseteq L'$. Fie acum $\alpha, \beta \in L'$. Conform 4.9., extinderea $K(\alpha, \beta) \supseteq K$ este finită. Conform 5.2., ea este şi algebrică. Prin urmare, orice element *x* din $K(\alpha, \beta)$ este algebric peste *K*. Din $\alpha, \beta \in K(\alpha, \beta)$ şi $K(\alpha, \beta)$ subcorp al lui *L*, rezultă că $\alpha - \beta$, $\alpha\beta$ şi α^{-1} (dacă $\alpha \neq 0$) aparțin lui $K(\alpha, \beta)$. În particular, $\alpha - \beta$, $\alpha\beta$ şi α^{-1} (dacă $\alpha \neq 0$) sunt algebrice peste *K*, deci aparțin lui L'. Rezultă că L' este subcorp al lui *L*. □

Fie $L \supseteq K$ o extindere de corpuri şi L' subcorpul definit în (3). Se pot căuta elemente ale lui *L*, algebrice peste L'. Vom arăta că nu se mai obțin elemente noi.

5.5. **Propoziție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* L' *subcorpul definit de relația* (3). *Dacă* $\theta \in L$ *şi* θ *este algebric peste* L', *atunci* $\theta \in L'$.

Demonstrație. Din θ algebric peste L' rezultă că $L'(\theta) \supseteq L'$ este extindere finită, deci algebrică. Extinderea $L' \supseteq K$ este algebrică, conform definiției lui L'. Din 5.3., rezultă că $L'(\theta) \supseteq K$ este algebrică. Prin urmare, θ este algebric peste K şi $\theta \in L'$. □

Ultima propoziție justifică următoarea definiție.

5.6. **Definiție.** *Fie $L \supseteq K$ o extindere de corpuri. Mulțimea L' a elementelor lui L, algebrice peste K se numeşte* ***închidere algebrică a lui K în L***.

Din definiție, rezultă că extinderea $L \supseteq K$ este algebrică dacă şi numai dacă L coincide cu închiderea algebrică a lui K în L.

6. Proprietăți ale rădăcinilor polinoamelor

Noțiunile de element algebric şi element transcendent s-au degajat în paragrafele anterioare în funcție de proprietatea acestora de a fi sau nu rădăcini ale unor polinoame nenule cu coeficienți într-un corp de bază K. În paragrafele următoare vom urmări problema inversă. Fiind dat un polinom $f \in K[X]$, K corp comutativ, are f rădăcini în K? Dacă da, atunci cât poate fi numărul acestora? Dacă nu, atunci există o extindere L a lui K în care f are rădăcini? O parte din rezultate rămân adevărate chiar pe un cadru mai general al polinoamelor cu coeficienți într-un inel comutativ.

Este cunoscut rezultatul:

6.1. **Propoziție.** *Fie A un inel comutativ şi unitar. Fie $f \in A[X]$ şi $a \in A$. Atunci:*

a) *Restul împărțirii lui f la $X - a$ este egal cu $f(a)$;*

b) *$X - a \mid f$ dacă şi numai dacă a este rădăcină a lui f.*

Dacă a este o rădăcină a lui $f \in A[X]$, conform b), există g în $A[X]$ astfel încât $f = (X - a)g$. La rândul său, g poate avea rădăcina a. În acest caz, $(X - a)^2 \mid f$. În general, este posibil să avem relația $(X - a)^k \mid f$, $k \geq 2$. Totuşi, $k \leq d^\circ f$.

6.2. **Definiție.** *Fie A un inel comutativ şi unitar, $f \in A[X]$, $a \in A$ şi $k \in \mathbb{N}^*$. Se spune că a este* ***rădăcină multiplă*** *de ordin k a lui f dacă $(X-a)^k \mid f$ şi $(X-a)^{k+1} \nmid f$.*

Dacă a este o rădăcină multiplă de ordin k a lui f, rezultă că există $g \in A[X]$, astfel încât $f = (X-a)^k g$. Se observă că $g(a) \neq 0$ deoarece $g(a) = 0 \Rightarrow (X-a)^{k+1} \mid f$, contradicție.

Reciproc, dacă $f = (X-a)^k g$ şi $g(a) \neq 0$, atunci a este o rădăcină multiplă de ordin k a lui f.

Deci, condiția:

$$f = (X-a)^k g \text{ şi } g(a) \neq 0$$

este o condiție necesară şi suficientă ca a să fie rădăcină multiplă de ordin k pentru f.

6.3. **Propoziție.** *Fie A un inel integru, $f, g \in A[X]$ şi $a \in A$. Dacă a este rădăcină de ordin k pentru f şi de ordin l pentru g, atunci a este rădăcină multiplă de ordin $k+l$ pentru fg.*

Demonstrație. Există $f_1, g_1 \in A[X]$ astfel încât $f = (X-a)^k f_1$, $g = (X-a)^l g_1$ şi $f_1(a) \neq 0$, $g_1(a) \neq 0$. Rezultă:

$$fg = (X-a)^{k+l} f_1 g_1 \text{ şi } (f_1 g_1)(a) = f_1(a) g_1(a) \neq 0.$$

Prin urmare, a este rădăcină multiplă de ordin $k+l$ pentru fg. □

Propoziția 6.3. rămâne adevărată şi pentru $k = 0$ sau $l = 0$. În acest caz, prin a este rădăcină de ordin 0 pentru f vom înțelege că a nu este rădăcină pentru f.

6.4. **Propoziție.** *Fie A un inel integru şi $f \in A[X]$. Dacă $a_i \in A$ este rădăcină de ordin k_i pentru f, $i \in \overline{1,r}$ ($a_1, ..., a_r$ distincte), atunci există $g \in A[X]$ astfel încât*:

$$f = (X-a_1)^{k_1} ... (X-a_r)^{k_r} g.$$

Demonstrație. Raționăm prin inducție după r. Pentru $r = 1$, afirmația rezultă din definiția 6.2.

Presupunem afirmația adevărată pentru o valoare $r-1$, $r > 1$. Fie $a_1, ..., a_{r-1}, a_r \in A$, rădăcini multiple de ordine $k_1, ..., k_{r-1}, k_r$ respectiv. Conform ipotezei de inducție, există $h \in A[X]$ astfel încât:

$$f = (X - a_1)^{k_1} ... (X - a_{r-1})^{k_{r-1}} h.$$

Din $f(a_r) = 0$ şi A inel integru, rezultă $h(a_r) = 0$. Fie k ordinul de multiplicitate al lui a_r pentru h. Deoarece a_r nu este rădăcină pentru $(X - a_1)^{k_1} ... (X - a_{r-1})^{k_{r-1}}$, conform 6.3., rezultă că a_r este rădăcină multiplă de ordinul k pentru h. Deci, $k = k_r$. Rezultă:

$h = (X - a_r)^{k_r} g$ şi $f = (X - a_1)^{k_1} ... (X - a_{r-1})^{k_{r-1}} (X - a_r)^{k_r} g$. □

Convenim ca, atunci când numărăm rădăcinile unui polinom, fiecare rădăcină multiplă să o socotim de atâtea ori cât este ordinul său de multiplicitate.

6.5. **Propoziție.** *Fie A un inel integru şi $f \in A[X] \setminus \{0\}$. Atunci f are în A cel mult atâtea rădăcini cât este gradul său.*

Demonstrație. Cu notațiile din propoziția 6.4., dacă $a_1, ..., a_r$ sunt toate rădăcinile din A ale lui f, de ordine de multiplicitate $k_1, ..., k_r$, atunci $k_1 + ... + k_r \le d^\circ f$. □

Se poate observa că propoziția 6.5. nu mai rămâne adevărată dacă A nu este inel integru. Astfel, pentru polinomul $f = X^2 - \hat{1} \in \mathbb{Z}_8[X]$ obținem: $f(\hat{1}) = \hat{0}$, $f(\hat{3}) = \hat{0}$, $f(\hat{5}) = \hat{0}$, $f(\hat{7}) = \hat{0}$.

Fie A un inel comutativ şi unitar şi $f = \sum_{i=0}^{n} a_i X^i \in A[X]$.

Polinomul

$$Df = \sum_{i=1}^{n} i a_i X^{i-1}$$

poartă numele de ***derivată formală*** a polinomului f.

Urmând notațiile de la analiză matematică, vom nota $Df = f'$. Prin calcul direct, rezultă:

$$D(f + g) = Df + Dg, \quad D(cf) = cDf,$$

pentru orice $f, g \in A[X]$ şi orice $c \in A$. Folosind relația:

$$DX^{i+j} = (i + j)X^{i+j-1} = (DX^i)X^j + X^i(DX^j),$$

se deduce şi

$$D(fg) = (Df)g + f(Dg), \quad Df^n = nf^{n-1}(Df),$$

pentru orice $f, g \in A[X]$ şi orice $n \in \mathbb{N}$.

Derivata formală are un rol important în studiul rădăcinilor multiple.

6.6. **Propoziție.** *Fie A un inel integru de caracteristică zero. Fie* $f \in A[X]$. *Dacă* $a \in A$ *este rădăcină multiplă de ordinul k pentru f,* $k \geq 1$, *atunci a este rădăcină multiplă de ordinul* $k-1$ *pentru* f'.

Demonstrație. Din ipoteză, rezultă $f = (X-a)^k g$ şi $g(a) \neq 0$.

$$f' = k(X-a)^{k-1} g + (X-a)^k g' = (X-a)^{k-1}\left[kg + (X-a)g'\right].$$

Dacă notăm $h = kg + (X-a)g'$, atunci $f' = (X-a)^{k-1} h$. Deoarece A este inel integru de caracteristică zero, $h(a) = (k \cdot 1)g(a) \neq 0$. Deci, a este rădăcină multiplă de ordinul $k-1$ a lui f'. □

6.7. **Consecință.** *Fie A un inel integru de caracteristică zero. Fie* $f \in A[X]$. *Dacă* $a \in A$ *este rădăcină multiplă a lui f, de ordin k, cu* $k \geq 1$, *atunci*: $f(a) = f'(a) = \ldots f^{(k-1)}(a) = 0$ *şi* $f^{(k)}(a) \neq 0$.

Facem observația că pentru inele de caracteristică diferită de zero, dacă a este rădăcină de ordinul k pentru f, atunci a este rădăcină şi pentru f', fără a mai putea preciza ordinul său de multiplicitate.

Astfel, în $\mathbb{Z}_3[X]$, polinomul $f = X^3 - \hat{1} = (X-\hat{1})^3$ are rădăcina triplă $\alpha = \hat{1}$, dar $f' = 0$.

Tot în $\mathbb{Z}_3[X]$, polinomul $g = X^4 - X = X(X-\hat{1})^3$ are rădăcina triplă $\alpha = \hat{1}$ şi $g' = f = (X-\hat{1})^3$ are din nou pe $\hat{1}$ rădăcină triplă.

Din calculele făcute în demonstrația propoziției 6.6., rezultă că pentru un inel integru A, de caracteristică nenulă, dacă a este rădăcină multiplă de ordinul k a lui $f \in A[X]$, atunci $f' = 0$ sau a este rădăcină a lui f', de ordin $\geq k-1$.

6.8. **Propoziție.** *Fie A un inel integru şi* $f \in A[X]$, $d^\circ f > 1$. *Dacă f are o rădăcină multiplă în A, de ordin mai mare decât 1, atunci* $(f, f') \neq 1$. *Reciproc, dacă* $(f, f') \sim d$, $d^\circ d \geq 1$ *şi d are rădăcini în A, atunci f are rădăcini multiple în A.*

Demonstrație. Dacă a este o rădăcină multiplă de ordinul $k>1$, a lui f, atunci

$$(X-a)^{k-1} \mid f' \text{ şi } (X-a)^{k-1} \mid f, \text{ deci } (X-a)^{k-1} \mid (f, f') \neq 1.$$

Reciproc, fie $a \in A$ o rădăcină a lui $d \sim (f, f')$. Din $f(a)=0$, rezultă $f=(X-a)g$, $g \in A[X]$.

Cum $f'=g+(X-a)g'$ şi $f'(a)=0$, se obține $g(a)=0$, deci există $h \in A[X]$, astfel încât $g=(X-a)h$. În final, $f=(X-a)^2 h$ şi a este rădăcină multiplă a lui f de ordin ≥ 2. □

6.9. **Propoziție.** *Fie B un inel integru şi A un subinel al său. Fie* $f=\sum_{i=0}^{n} c_i X^i$, $n \geq 1$ *un polinom care are toate rădăcinile* $\alpha_1, ..., \alpha_n$ *în B* (*simple sau multiple*). *Atunci*,

$$(1) \qquad \begin{aligned} & c_n(\alpha_1+\alpha_2+...+\alpha_n)=-c_{n-1} \\ & c_n(\alpha_1\alpha_2+\alpha_1\alpha_3+...+\alpha_{n-1}\alpha_n)=c_{n-2} \\ & ..... \\ & c_n\alpha_1\alpha_2...\alpha_n=(-1)^n c_0. \end{aligned}$$

Demonstrație. Din propoziția 6.4., rezultă:

$$\begin{aligned} f &= c_n(X-\alpha_1)(X-\alpha_2)...(X-\alpha_n)= \\ &= c_n X^n - c_n(\alpha_1+\alpha_2+...+\alpha_n)X^{n-1}+ \\ &+c_n(\alpha_1\alpha_2+\alpha_1\alpha_3+...+\alpha_{n-1}\alpha_n)X^{n-2}-...+(-1)^n c_n\alpha_1\alpha_2...\alpha_n. \end{aligned}$$

Comparând cu expresia lui f, rezultă relațiile (1) numite ***relațiile lui Viète***. □

6.10. **Consecință.** *Fie K un corp comutativ şi* $f \in K[X]$ *un polinom de grad* $n \geq 1$. *Fie L o extindere a lui K în care f are toate rădăcinile* $\alpha_1, ..., \alpha_n$. *Atunci*, $\sum_{i=1}^{n} \alpha_i$, $\sum_{1 \leq i < j \leq n} \alpha_i\alpha_j$, ..., $\alpha_1\alpha_2...\alpha_n \in K$.

Demonstrație. Dacă $f=\sum_{i=0}^{n} c_i X^i \in K[X]$, din (1), rezultă:

$$\sum_{i=1}^{n} \alpha_i = -c_{n-1}c_n^{-1} \in K, \quad \sum_{1 \leq i < j \leq n} \alpha_i\alpha_j = c_{n-2}c_n^{-1} \in K, \ldots,$$

$$\alpha_1\alpha_2...\alpha_n = (-1)^n c_0 c_n^{-1} \in K. \qquad \square$$

6.11. **Consecință.** *Fie K un corp comutativ şi* $f \in K[X]$ *un polinom de grad* $n \geq 1$. *Fie L o extindere a lui K în care f are toate rădăcinile* $\alpha_1,...,\alpha_n$. *Fie* $g \in K[X_1,...,X_n]$, *un polinom simetric. Atunci*,

$$g(\alpha_1,...,\alpha_n) \in K.$$

Demonstrație. Din teorema fundamentală a polinoamelor simetrice, rezultă că există $h \in K[X_1,...,X_n]$, astfel încât $g = h(s_1,...,s_n)$ unde $s_1,...,s_n$ sunt polinoamele simetrice fundamentale.

Conform 6.10.:

$$s_1(\alpha_1,...,\alpha_n) = \alpha_1 + ... + \alpha_n \in K;\ \ s_2(\alpha_1,...,\alpha_n) = \sum_{1\leq i<j\leq n} \alpha_i\alpha_j \in K;\ \ldots,$$

$$s_n(\alpha_1,...,\alpha_n) = \alpha_1...\alpha_n \in K.$$

Rezultă că:

$$g(\alpha_1,...,\alpha_n) = h(s_1(\alpha_1,...,\alpha_n), s_2(\alpha_1,...,\alpha_n),..., s_n(\alpha_1,...,\alpha_n)) \in K. \quad \square$$

7. Corp de descompunere al unui polinom

Fie K un corp comutativ şi $f \in K[X]$, un polinom de grad $n \geq 1$.

În paragraful precedent am văzut că dacă polinomul f are rădăcinile $\alpha_1,...,\alpha_n \in K$, atunci f admite reprezentarea

$$f = a(X-\alpha_1)(X-\alpha_2)...(X-\alpha_n)$$

unde $a \in K^*$. Reciproc, dacă f se descompune în $K[X]$ în produs de factori liniari:

$$f = \prod_{i=1}^{n} (a_i X + b_i)$$

unde $a_i, b_i \in K$, $a_i \neq 0$, $i \in \overline{1,n}$, atunci f are toate rădăcinile în K, şi anume $\alpha_i = -a_i^{-1} b_i$, $i \in \overline{1,n}$. Prin urmare, posibilitatea descompunerii în $K[X]$ a unui polinom f în factori liniari este echivalentă cu existența în K a tuturor rădăcinilor lui f (atâtea rădăcini, cât este gradul lui f). Nu totdeauna un polinom $f \in K[X]$, $d^\circ f = n \geq 1$, are toate ră-

dăcinile în K. Se pune atunci problema găsirii unei extinderi L a lui K, astfel încât f să aibă în L toate rădăcinile.

Considerăm mai întâi cazul în care polinomul f este ireductibil şi este cunoscută o extindere L a lui K în care f are o rădăcină θ.

Aplicaţia:

$$u_\theta : K[X] \to K[\theta],\ u_\theta(g) = g(\theta),\ \forall g \in K[X],$$

este morfism surjectiv de inele al cărui nucleu este $Keru_\theta = (p_\theta),$ cu p_θ polinomul minimal al lui θ. Deoarece f este ireductibil în $K[X]$ şi $f(\theta) = 0,$ rezultă $f \sim p_\theta$. Deci, $Keru_\theta = (f)$. Din teorema fundamentală de izomorfism pentru inele, rezultă că există un izomorfism:

$$v : K[X]/(f) \to K[\theta],\ v(\widehat{g}) = g(\theta),\ \forall g \in K[X].$$

În particular, $v(\widehat{X}) = \theta$. Dar $K[X]/(f)$ poate fi construit chiar fără a cunoaşte extinderea L în care f are o rădăcină.

7.1. **Lemă.** *Fie K un corp comutativ şi $f \in K[X]$, un polinom ireductibil. Atunci, $L = K[X]/(f)$ este un corp, extindere finită a lui K şi $\theta = \widehat{X}$ este o rădăcină a lui f.*

Demonstraţie. Deoarece f este polinom ireductibil şi $K[X]$ este inel principal, (f) este ideal maximal şi $K[X]/(f)$ este corp.

Aplicaţia:

$$K \to K[X]/(f) = L,\ a \to \hat{a},\ \forall a \in K,$$

este un morfism (unitar) de corpuri, deci este un morfism injectiv. Prin acest morfism, K este izomorf cu imaginea lui. Identificând

$$a \equiv \hat{a},\ \forall a \in K,$$

K devine subcorp al lui L.

Să notăm $\theta = \widehat{X} \in L$. Dacă $f = \sum_{i=0}^{n} a_i X^i,\ a_n \neq 0,$ atunci:

$$f(\theta) = \sum_{i=0}^{n} a_i \theta^i = \sum_{i=0}^{n} \widehat{a_i}\,\widehat{X}^i = \widehat{f} = (f) = \hat{0} = 0,$$

adică θ este o rădăcină a lui f. În particular, elementul $\theta \in L$ este algebric peste K, $K[\theta] = K(\theta)$ este extindere finită a lui K de grad egal

cu $d^\circ p_\theta = d^\circ f$. Elementele lui L sunt de forma $\hat{g}$, $g \in K[X]$. Dacă $g = \sum_{j=0}^{m} b_j X^j$, atunci:

$$\hat{g} = \sum_{j=0}^{m} \hat{b}_j \hat{X}^j = \sum_{j=0}^{m} b_j \theta^j = g(\theta).$$

Prin urmare, $L = \{g(\theta) | g \in K[X]\} = K[\theta]$ şi deci $L \supseteq K$ este extindere finită cu $[L:K] = d^\circ f$. □

Dacă polinomul din lema 7.1. are gradul 1, atunci $[L:K] = 1$, deci $L = K$, rezultat normal deoarece, în acest caz, rădăcina lui *f* aparţine lui *K*.

7.2. **Teoremă.** *Fie K un corp comutativ şi* $f \in K[X]$, *un polinom de grad* ≥ 1. *Atunci, există o extindere a lui K în care f are toate rădăcinile.*

Demonstraţie. Raţionăm prin inducţie după gradul lui *f*.

Dacă $n = d^\circ f = 1$, atunci *f* are toate rădăcinile (una) în *K*.

Presupunem afirmaţia adevărată pentru polinoame de grad $< n$, ($n > 1$) şi fie $f \in K[X]$, un polinom de grad *n*.

Inelul $K[X]$ este inel factorial. Fie f_1, un factor ireductibil al lui *f*. Conform lemei 7.1., $L_1 = K[X]/(f_1)$ este un corp, extindere finită a lui *K*, în care f_1 are o rădăcină θ. Elementul θ este şi o rădăcină a lui *f* şi, în $L_1[X]$,

$$f = (X - \theta)g, \quad d^\circ g = n - 1.$$

Conform ipotezei de inducţie, există o extindere $L \supseteq L_1$ în care *g* are $n-1$ rădăcini (distincte sau nu). Astfel, în corpul *L*, polinomul *f* are *n* rădăcini. □

7.3. **Definiţie.** *Fie K un corp comutativ şi* $f \in K[X]$, *un polinom de grad* $n \geq 1$. *Fie* $L \supseteq K$ *o extindere în care f are n rădăcini* (*distincte sau nu*): $\alpha_1, ..., \alpha_n$. *Corpul* $K(\alpha_1, ..., \alpha_n)$ *poartă numele de* ***corp de descompunere al polinomului f****.*

Corpul de descompunere al polinomului $f \in K[X]$ este o extindere minimală a corpului K peste care f se descompune în factori liniari.

Exemple. 1°. Polinomul $f = X^2 + 3 \in \mathbb{Q}[X]$ are în $\mathbb{C}$ rădăcinile $\pm i\sqrt{3}$. Prin urmare, un corp de descompunere al lui f este:

$$\mathbb{Q}\left(i\sqrt{3}, -i\sqrt{3}\right) = \mathbb{Q}\left(i\sqrt{3}\right).$$

2°. Să determinăm un corp de descompunere pentru polinomul:

$$f = X^4 + X^3 + X + \hat{2} \in \mathbb{Z}_3[X].$$

Mai întâi, descompunem f în factori ireductibili. Deoarece f nu are rădăcini în $\mathbb{Z}_3$, f nu are factori ireductibili de gradul 1.

Căutăm o descompunere în produs de factori de gradul 2:

$$f = (X^2 + aX + b)(X^2 + cX + d);\ \ a,b,c,d \in \mathbb{Z}_3.$$

Efectuând produsul şi ținând seama de expresia inițială a lui f, se obține sistemul:

$$\begin{cases} a + c = \hat{1} \\ b + d + ac = \hat{0} \\ ad + bc = \hat{1} \\ bd = \hat{2}. \end{cases}$$

O soluție a acestui sistem este $a = \hat{1},\ b = \hat{2},\ c = \hat{0},\ d = \hat{1}$. Deci,

$$f = \left(X^2 + X + \hat{2}\right)\left(X^2 + \hat{1}\right).$$

Factorul $f_1 = X^2 + X + \hat{2}$ este ireductibil în $\mathbb{Z}_3[X]$, astfel că

$$L = \mathbb{Z}_3[X]/(f_1)$$

este un corp, extindere de gradul 2 a lui $\mathbb{Z}_3$, în care $\theta = \widehat{X}$ este o rădăcină a lui f_1. Dacă $L' \supseteq L$ este o extindere în care f_1 are şi o a doua rădăcină β, atunci $\theta + \beta = -\hat{1} = \hat{2}$.

Prin urmare, $\beta = \hat{2} - \theta = \hat{2} + \hat{2}\theta \in L$ este a doua rădăcină a lui f_1.

Cercetăm dacă factorul $f_2 = X^2 + \hat{1}$ are rădăcini în L.

Se ştie că elementele $\hat{1}$ şi θ formează o bază în L ca spaţiu vectorial peste $\mathbb{Z}_3$. Dacă $u+v\theta,\ u,v\in\mathbb{Z}_3,$ este o rădăcină a lui f_2, atunci $(u+v\theta)^2+\hat{1}=\hat{0}.$ Efectuând calculele şi ţinând seama că

$$\theta^2+\theta+\hat{2}=\hat{0},$$

rezultă sistemul:

$$\begin{cases}\hat{2}v(u+v)=\hat{0}\\ u^2+v^2+\hat{1}=\hat{0}.\end{cases}$$

Soluţiile sistemului sunt $(\hat{1},\hat{2})$ şi $(\hat{2},\hat{1})$. Factorul f_2 are în L rădăcinile $\hat{1}+\hat{2}\theta$ şi $\hat{2}+\theta.$

Prin urmare, corpul L conţine toate rădăcinile lui f:

$$\theta,\ \hat{2}+\hat{2}\theta,\ \hat{1}+\hat{2}\theta,\ \hat{2}+\theta.$$

Astfel, L este corp de descompunere al polinomului f. Peste L, f se descompune în factori liniari:

$$f=(X-\theta)\left(X-\hat{2}-\hat{2}\theta\right)\left(X-\hat{1}-\hat{2}\theta\right)\left(X-\hat{2}-\theta\right)=$$

$$=\left(X+\hat{2}\theta\right)\left(X+\hat{1}+\theta\right)\left(X+\hat{2}+\theta\right)\left(X+\hat{1}+\hat{2}\theta\right).$$

Din consideraţiile de mai sus, rezultă şi

$$L=\left\{u+v\theta\,\middle|\,u,v\in\mathbb{Z}_3\right\}=\mathbb{Z}_3(\theta).$$

Prin urmare, L este un corp cu 9 elemente.

Teorema 7.2. arată existenţa corpurilor de descompunere pentru un polinom.

În continuare vom urmări să demonstrăm unicitatea acestora.

7.4. **Lemă.** *Fie* $u:K\to K_1$ *un izomorfism de corpuri. Fie*

$$\overline{u}:K[X]\to K_1[X],$$

unicul izomorfism de inele care prelungeşte u, astfel încât $\overline{u}(X)=X$. *Fie* $f\in K[X]$ *un polinom ireductibil şi* $f_1=\overline{u}(f)$. *Fie* $L\supseteq K$ *o extindere în care f are o rădăcină* θ. *Fie* $L_1\supseteq K_1$ *o extindere în care* f_1 *are o rădăcină* θ_1. *Atunci există un izomorfism*

$$v:K(\theta)\to K_1(\theta_1)$$

care prelungeşte u şi astfel încât $v(\theta)=\theta_1$.

Demonstraţie. Considerăm diagrama:

$$\begin{array}{ccc} K[X] & \xrightarrow{u_\theta} & K[\theta] \\ \Big\downarrow{\scriptstyle \overline{u}} & & \Big\downarrow{\scriptstyle v} \\ K_1[X] & \xrightarrow{u_{\theta_1}} & K_1[\theta_1] \end{array}$$

unde u_θ şi u_{θ_1} sunt morfismele canonice. Din

$$\left(u_{\theta_1}\circ\overline{u}\right)(f)=u_{\theta_1}(f_1)=f_1(\theta_1)=0,$$

rezultă $Ker(u_{\theta_1}\circ\overline{u})\supseteq(f)$. Deoarece *f* este ireductibil, (f) este ideal maximal în $K[X]$. Cum $u_{\theta_1}\circ\overline{u}$ nu este morfismul nul, rezultă:

(1) $$Ker(u_{\theta_1}\circ\overline{u})=(f)=Keru_\theta.$$

Din proprietatea de universalitate a inelului factor, rezultă că există un morfism $v:K[\theta]\to K_1[\theta_1]$ astfel încât $v\circ u_\theta=u_{\theta_1}\circ\overline{u}$. Din (1) şi din $u_{\theta_1}\circ\overline{u}$ surjectiv, rezultă *v* izomorfism.

Pentru $a\in K$:

$$v(a)=v\left(u_\theta(a)\right)=u_{\theta_1}\left(\overline{u}(a)\right)=\overline{u}(a)=u(a),$$

adică *v* prelungeşte pe *u*. În plus,

$$v(\theta)=v\left(u_\theta(X)\right)=u_{\theta_1}\left(\overline{u}(X)\right)=u_{\theta_1}(X)=\theta_1. \qquad \square$$

7.5. **Lemă.** *Fie* $u:K\to K_1$ *şi* $\overline{u}:K[X]\to K_1[X]$ *izomorfismele din lema* 7.4. *Fie* $f\in K[X]$ *un polinom de grad* $n\geq 1$ *şi* $f_1=\overline{u}(f)$. *Fie* $L\supseteq K$ *o extindere în care f are rădăcinile* $\theta_1,...,\theta_n$ *şi* $L_1\supseteq K_1$ *o extindere în care* f_1 *are rădăcinile* $\theta_1',...,\theta_n'$.

Atunci există un izomorfism

$$v:K\left(\theta_1,...,\theta_n\right)\to K_1(\theta_1',...,\theta_n')$$

care prelungeşte u şi astfel încât (*renumerotând eventual rădăcinile*)

$$v(\theta_i)=\theta_i',\ \ i\in\overline{1,n}.$$

Demonstrație. Raționăm prin inducție după *n*.

Pentru $n=1$, dacă $f=aX+b\in K[X],\ a\neq 0$, atunci $\theta=-a^{-1}b$.

$$f_1=u(a)X+u(b),\ \theta_1=-u(a)^{-1}u(b)=u(\theta).$$

$$K(\theta)=K,\ K_1(\theta_1)=K_1,\ v=u.$$

Presupunem afirmația adevărată pentru valori mai mici decât *n* și considerăm $d^\circ f=n$. Fie *g* un factor ireductibil al lui *f*, $g_1=\overline{u}(g)$ este un factor al lui f_1. Putem presupune (eventual, printr-o renumerotare) că $g(\theta_1)=0$ și $g_1(\theta_1')=0$.

Din lema 7.4., rezultă că există un izomorfism $v_1:K(\theta_1)\to K_1(\theta_1')$ care prelungește *u* și astfel încât $v_1(\theta_1)=\theta_1'$.

Fie $\overline{v_1}:K(\theta_1)[X]\to K_1(\theta_1')[X]$ izomorfismul care prelungește v_1 și astfel încât $\overline{v_1}(X)=X$. În particular, $\overline{v_1}$ extinde și izomorfismul $\overline{u}$.

În $K(\theta_1)[X]$, $f=(X-\theta_1)h,\ d^\circ h=n-1$. Aplicând $\overline{v_1}$:

$$f_1=\overline{u}(f)=\overline{v_1}(f)=(X-\theta_1')h_1,\ h_1=\overline{v_1}(h).$$

Conform ipotezei de inducție, există un izomorfism:

$$v:K(\theta_1)(\theta_2,...,\theta_n)\to K_1\left(\theta_1'\right)\left(\theta_2',...,\theta_n'\right)$$

care prelungește v_1 (deci prelungește *u*) și astfel încât

$$v(\theta_i)=\theta_i',\ i\in\overline{2,n}.\qquad\square$$

7.6. **Teoremă.** *Fie K un corp comutativ și* $f\in K[X]$ *un polinom de grad* $n\geq 1$. *Fie* $K(\alpha_1,...,\alpha_n)$ *și* $K(\beta_1,...,\beta_n)$ *două corpuri de descompunere ale lui f. Atunci există un izomorfism*

$$v:K(\alpha_1,...,\alpha_n)\to K(\beta_1,...,\beta_n)$$

astfel încât $v(a)=a,\ \forall a\in K$ *și* $v(\alpha_i)=\beta_i,\ i\in\overline{1,n}$ (*efectuând eventual o renumerotare a rădăcinilor*).

Demonstrație. În lema 7.5., luăm:

$$K_1=K \text{ și } u=1_K,\ L=K(\alpha_1,...,\alpha_n),\ L_1=K(\beta_1,...,\beta_n)$$

și rezultă toate concluziile teoremei. $\square$

8. Corpuri algebric închise

Fie K un corp comutativ.

În paragraful anterior, am arătat că pentru orice polinom f din $K[X]$, de grad $n \geq 1$, există o extindere L a lui K în care f are toate rădăcinile. Ne interesează dacă există corpuri K astfel încât, pentru orice polinom f, să putem lua $L = K$. Aceasta revine la condiția:

K conține toate elementele algebrice peste K, din orice extindere a lui K.

Conform definiției 5.6., închiderea algebrică a lui K în extinderea sa L este un subcorp al lui L format din elementele algebrice peste K.

8.1. **Definiție.** *Fie K un corp comutativ. Se spune: K este* ***corp algebric închis*** *dacă pentru orice extindere L a lui K, K coincide cu închiderea algebrică a sa în L.*

Pentru moment, este mai uşor să dăm exemple de corpuri care nu sunt algebric închise.

Astfel, corpul $\mathbb{Q}$ al numerelor raționale nu este corp algebric închis. Într-adevăr, elementul $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$ este algebric peste $\mathbb{Q}$ dar $\sqrt{2} \notin \mathbb{Q}$.

8.2. **Propoziție.** *Fie K un corp comutativ. Sunt echivalente condițiile*:

a) *K este corp algebric închis*;

b) $\forall f \in K[X],\ d^{\circ} f \geq 1 \Rightarrow$ *f are toate rădăcinile în K*;

c) $\forall f \in K[X],\ d^{\circ} f \geq 1 \Rightarrow$ *f se descompune în* $K[X]$ *în produs de factori liniari*;

d) $\forall f \in K[X],$ *f ireductibil* $\Rightarrow d^{\circ} f = 1$.

Demonstrație. "a) $\Rightarrow$ d)" Fie $f \in K[X]$, ireductibil. Fie $L \supseteq K$ astfel încât $\exists \alpha \in L,\ f(\alpha) = 0$. Elementul α este algebric peste K. Deoarece K este corp algebric închis, rezultă $\alpha \in K$.
În $K[X]$, $X - \alpha \mid f$. Din f polinom ireductibil, rezultă $f \sim X - \alpha$, deci $d^{\circ} f = 1$.

"d) $\Rightarrow$ c)" Fie $f \in K[X]$, $d^{\circ} f \geq 1$. Deoarece $K[X]$ este inel factorial, f este produs de polinoame ireductibile (prime), care, conform d), au gradul 1.

"c) $\Rightarrow$ b)" Un polinom $f \in K[X]$, de grad $n \geq 1$, este, conform c), un produs de n factori de gradul 1. Fiecare dintre aceşti factori are o rădăcină în K.

"b) $\Rightarrow$ a)" Fie L o extindere a lui K şi $\alpha \in L$ un element algebric peste K. Fie $f \in K[X] \setminus \{0\}$ astfel încât $f(\alpha) = 0$. Conform b), rezultă $\alpha \in K$. Deci, K este corp algebric închis. □

Putem extinde exemplele de corpuri care nu sunt algebric închise.

Corpul $\mathbb{R}$ al numerelor reale nu este corp algebric închis deoarece polinomul $f = X^2 + 1$ nu are rădăcini în $\mathbb{R}$.

8.3. **Propoziție.** *Fie K un corp finit. Atunci K nu este corp algebric închis.*

Demonstrație. Fie $K = \{0, 1, a_3, ..., a_n\}$. Polinomul

$$f = X(X-1)(X-a_3)...(X-a_n) + 1$$

aparține lui $K[X]$ şi $f(a) = 1 \neq 0$, $\forall a \in K$. Deci f nu are rădăcini în K şi K nu este corp algebric închis. □

Aşa cum vom arăta în continuare, corpul $\mathbb{C}$ al numerelor complexe este corp algebric închis. Toate demonstrațiile acestei afirmații folosesc şi rezultate de analiză matematică.

8.4. **Lemă.** *Fie* $f \in \mathbb{C}[X]$ *de grad* $n \geq 1$ *şi* $z_0 \in \mathbb{C}$. *Dacă* $f(z_0) \neq 0$, *atunci există* $h \in \mathbb{C}$ *astfel încât:*

$$|f(z_0 + h)| < |f(z_0)|.$$

Demonstrație. $f(z_0 + h)$ admite reprezentarea:

$$f(z_0 + h) = A_0 + A_1 h + ... + A_n h^n$$

unde $A_i \in \mathbb{C}$, $i \in \overline{0, n}$. În plus, $A_0 = f(z_0)$. Fie

$$k = \min\{i \mid 1 \leq i \leq n,\ A_i \neq 0\} \text{ şi } h = t\sqrt[k]{-f(z_0)/A_k}$$

unde $t \in [0,1]$ iar $\sqrt[k]{-f(z_0)/A_k}$ este una dintre cele k valori ale radicalului complex.

Notăm:

$$B_j = A_j\left(\sqrt[k]{-f(z_0)/A_k}\right)^j,\ k<j\le n.$$

$$|f(z_0+h)| = |f(z_0)-t^k f(z_0)+t^{k+1}B_{k+1}+\ldots+t^n B_n| \le$$

$$\le (1-t^k)|f(z_0)|+t^{k+1}|B_{k+1}|+\ldots+t^n|B_n| = |f(z_0)|+g(t)t^k$$

unde $g(t) = -|f(z_0)|+t|B_{k+1}|+\ldots+t^{n-k}|B_n| \in \mathbb{R}[t]$.

Funcția polinomială $\widetilde{g}$ asociată lui g, $\widetilde{g}:[0,1]\to\mathbb{R}$ este continuă și $\widetilde{g}(0) = -|f(z_0)| < 0$. Rezultă că există $t_0 \in (0,1]$ astfel încât

$$\widetilde{g}(t_0) = g(t_0) < 0.$$

Pentru $h_0 = t_0\sqrt[k]{-f(z_0)/A_k}$,

$$|f(z_0+h_0)| \le |f(z_0)| + g(t_0)t_0^{\,k} < |f(z_0)|. \quad \square$$

8.5. **Lemă.** *Fie* $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, $a_n \neq 0$. *Fie şirul* $(z_p)_{p\ge1}$ *de numere complexe astfel încât* $|z_p| \to \infty$. *Atunci*

$$|f(z_p)| \to \infty \ \ (\textit{când}\ \ p\to\infty).$$

Demonstrație.

$$|f(z_p)| = |a_n z_p{}^n + \ldots + a_1 z_p + a_0| =$$

$$= |a_n||z_p|^n \left|1+\frac{a_{n-1}}{a_n}\cdot\frac{1}{z_p}+\ldots+\frac{a_0}{a_p}\cdot\frac{1}{z_p{}^n}\right| \ge$$

$$\ge a_n|z_p|^n\left(1-\left|\frac{a_{n-1}}{a_n}\right|\cdot\frac{1}{|z_p|}-\ldots-\left|\frac{a_0}{a_p}\right|\cdot\frac{1}{|z_p|^n}\right)\to\infty. \ \square$$

8.6. **Teorema fundamentală a algebrei (d'Alembert - Gauss)** *Orice polinom cu coeficienți complecşi, de grad* ≥ 1 *are cel puțin o rădăcină complexă.*

Demonstrație. Fie $f \in \mathbb{C}[X]$, $d^\circ f = n \ge 1$. Mulțimea

$$A = \{|f(z)| \,|\, z\in\mathbb{C}\} \subseteq \mathbb{R}$$

este mărginită inferior. Fie $m = \inf A$.

Vom arăta că există $z_0 \in \mathbb{C}$, astfel încât $|f(z_0)| = m$. Există un şir $(z_p)_{p\geq 1}$ de numere complexe, astfel încât

(1) $$|f(z_p)| \to m.$$

Să presupunem că şirul $(z_p)_{p\geq 1}$ este nemărginit. Există atunci un subşir al său $(z_{p_n})_{n\geq 1}$ astfel încât $|z_{p_n}| \to \infty$. Din lema 8.5., rezultă că $|f(z_{p_n})| \to \infty$, contradicție cu (1).

Prin urmare, şirul $(z_p)_{p\geq 1}$ este mărginit. Fie $(z_{q_n})_{n\geq 1}$ un subşir convergent al său, $z_{q_n} \to z_0$. Deoarece funcția polinomială $\widetilde{f}$ asociată lui *f* este continuă, $f(z_{q_n}) \to f(z_0)$. Din (1) rezultă $m = |f(z_0)|$.

Vom arăta că $f(z_0) = 0$.

Dacă $f(z_0) \neq 0$, atunci conform lemei 8.4., există $h \in \mathbb{C}$ astfel încât $|f(z_0 + h)| < |f(z_0)| = m$, contradicție.

Prin urmare $f(z_0) = 0$ şi teorema este demonstrată. □

8.7. **Consecință.** *Fie* $f \in \mathbb{C}[X]$, *un polinom de grad* ≥ 1. *Atunci f are în* $\mathbb{C}$ *exact n rădăcini (distincte sau nu).*

Demonstrație. Raționăm prin inducție după *n*.

Dacă $n = 1$, $f = aX + b$, $a, b \in \mathbb{C}$, $a \neq 0$. $\alpha = -a^{-1}b \in \mathbb{C}$ este rădăcină a lui *f*.

Presupunem afirmația adevărată pentru polinoame de grad $< n$, $n > 1$. Fie $f \in \mathbb{C}[X]$ de grad *n*. Conform teoremei 8.6., există $\alpha \in \mathbb{C}$ astfel încât $f = (X - \alpha)g$, $g \in \mathbb{C}[X]$ şi $d^\circ g = n - 1$. Din ipoteza de inducție, rezultă că *g* are în $\mathbb{C}$ $n-1$ rădăcini: $\alpha_2, \alpha_3, \ldots \alpha_n$. Ca urmare, *f* are în $\mathbb{C}$ *n* rădăcini: $\alpha_1 = \alpha, \alpha_2, \alpha_3, \ldots \alpha_n$. □

Din 8.6. şi 8.7., rezultă că $\mathbb{C}$ **este corp algebric închis**.

Existența unui corp algebric închis pune în evidență şi alte corpuri algebric închise.

8.8. **Propoziție.** *Fie K un corp comutativ şi L un corp algebric închis,* $L \supseteq K$. *Fie*

$$L' = \left\{\theta \in L \middle| \theta \text{ algebric peste } K\right\}.$$

Atunci, L' este un corp algebric închis.

Demonstrație. Conform propoziției 5.4., L' este subcorp al lui L. Fie $f \in L'[X]$, un polinom de grad ≥ 1. În particular, $f \in L[X]$.

Deoarece L este corp algebric închis, f are toate rădăcinile în L. Conform propoziției 5.5., acestea aparțin lui L'. Deci, L' este corp algebric închis. □

9. Închiderea algebrică a unui corp

Vom arăta în continuare că orice corp comutativ are o extindere care este corp algebric închis.

9.1. **Lemă.** *Fie K un corp comutativ. Atunci există $K_1 \supseteq K$, o extindere a lui K astfel încât, orice polinom $f \in K[X]$ de grad ≥ 1 are cel puțin o rădăcină în K_1.*

Demonstrație. Fie $P = \left\{f \in K[X] \middle| d^\circ f \geq 1\right\}$. Fiecărui polinom f din P îi asociem o nedeterminată X_f. Fie A inelul polinoamelor cu coeficienți în K şi în nedeterminatele $\left(X_f\right)_{f \in P}$. Fie I idealul lui A generat de mulțimea $\left\{f(X_f) \middle| f \in P\right\}$.

Afirmăm că $I \neq A$. Altfel, $1 \in I$ şi $\exists f_1, ..., f_n \in P$, $\exists g_1, ..., g_n \in A$, astfel încât:

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1 \tag{1}$$

Fie L o extindere a lui K în care fiecare polinom f_i are o rădăcină α_i, $i \in \overline{1,n}$. Înlocuind în (1) nedeterminatele X_{f_i} cu α_i şi celelalte nedeterminate cu 0, rezultă $0 = 1$, contradicție. Deci, $I \neq A$.

Conform lemei lui Krull, există un ideal maximal M, $M \supseteq I$. Fie $K_1 = A/M$, K_1 este corp. Aplicația

$$K \to K_1, \ a \to \hat{a}, \ \forall a \in K,$$

este un morfism de corpuri, deci este un morfism injectiv. Prin acest morfism, corpul K se identifică cu imaginea sa şi devine subcorp al lui K_1.

Fie $f \in K[X]$ de grad ≥ 1. Prin urmare, $f \in P$ şi $f(X_f) \in M$.

Pentru $\alpha = \widehat{X_f} \in K_1$, obţinem $f(\alpha) = f\left(\widehat{X_f}\right) = f\left(\hat{0}\right) = 0$. □

9.2. **Teoremă.** *Fie K un corp comutativ. Atunci există o extindere* $L \supseteq K$, *astfel încât L este un corp algebric închis*.

Demonstraţie. Conform 9.1., există o extindere K_1 a lui K astfel încât orice polinom cu coeficienţi în K, de grad ≥ 1, are o rădăcină în K_1. Presupunem construit corpul K_i, pentru un anumit $i \geq 1$. Conform 9.1., există o extindere $K_{i+1} \supseteq K_i$, astfel încât:

(*) $\quad \forall f \in K_i[X],\ d^\circ f \geq 1 \ \Rightarrow\ \exists \alpha \in K_{i+1},\ f(\alpha) = 0.$

Obţinem în acest mod lanţul de extinderi:

(2) $\quad K \subseteq K_1 \subseteq \ldots \subseteq K_i \subseteq K_{i+1} \subseteq \ldots$

astfel încât, pentru orice $i \geq 1$, are loc proprietatea (*).

Fie $L = \bigcup_{i=1}^{\infty} K_i$. Pe L vom defini o structură astfel:

dacă $\alpha, \beta \in L$, atunci există $i, j \in \mathbb{N}^*$, astfel încât $\alpha \in K_i$, $\beta \in K_j$. Putem presupune $i \leq j$. Atunci, $\alpha, \beta \in K_j$.

Definim $\alpha + \beta$ şi $\alpha\beta$ ca în corpul K_j. Este uşor de verificat că cele două operaţii pe L sunt bine definite şi $(L, +, \cdot)$ este un corp comutativ. Vom arăta că L este corp algebric închis.

Fie $f = \sum_{j=0}^{n} a_j X^j \in L[X]$, $n \geq 1$, $a_n \neq 0$. Este suficient să arătăm că f are o rădăcină în L. Există $i_0, i_1, \ldots, i_n \in \mathbb{N}^*$ astfel încât $a_j \in K_{i_j}$, $j \in \overline{0,n}$. Fie $i = \max\{i_0, i_1, \ldots, i_n\}$. Atunci, $f \in K_i[X]$. Conform (*), f are o rădăcină în $K_{i+1} \subseteq L$. □

În continuare vom cere ca extinderea L a corpului K, din teorema 9.2., să fie şi extindere algebrică.

9.3. **Definiție.** *Fie K un corp comutativ. Numim* ***închidere algebrică*** *a lui K, o extindere* $\overline{K} \supseteq K$, *astfel încât:*

a) $\overline{K}$ *este corp algebric închis;*

b) $\overline{K} \supseteq K$ *este extindere algebrică.*

Corpul $\mathbb{C}$ al numerelor complexe este o închidere algebrică a corpului $\mathbb{R}$ al numerelor reale. Într-adevăr, $\mathbb{C}$ este corp algebric închis şi $\mathbb{C} \supseteq \mathbb{R}$ este o extindere algebrică.

Fie $\overline{K}$ o închidere algebrică a lui *K*. Fie *L* un subcorp al lui $\overline{K}$ care include *K*. Deoarece extinderea $\overline{K} \supseteq L$ este algebrică, $\overline{K}$ este şi o închidere algebrică a lui *L*.

9.4. **Teoremă.** *Orice corp comutativ are o închidere algebrică.*

Demonstrație. Fie *K* un corp comutativ. Conform 9.2., există o extindere $L \supseteq K$ astfel încât *L* este algebric închis. Fie

(3) $$L' = \{\theta \in L \mid \theta \text{ este algebric peste } K\}.$$

Conform 8.8., L' este corp algebric închis. Din (3), rezultă că extinderea $L' \supseteq K$ este algebrică. Prin urmare, L' este o închidere algebrică a lui *K*. □

În continuare urmărim să demonstrăm unicitatea închiderii algebrice.

9.5. **Lemă.** *Fie K un corp comutativ şi* L_1, L_2 *două extinderi ale sale astfel încât* $L_1 \supseteq K$ *este extindere algebrică şi* L_2 *este corp algebric închis. Fie E un subcorp al lui* L_1, $E \supseteq K$. *Fie* $u : E \to L_2$, *un morfism de corpuri astfel încât* $u(a) = a$, *pentru orice* $a \in K$. *Atunci, există un morfism* $w : L_1 \to L_2$ *care prelungeşte u.*

Demonstrație. Fie

(4) $$P = \{(F, v) \mid F \text{ subcorp al lui } L_1, F \supseteq E, \ v \text{ prelungeşte } u\}.$$

P este nevidă, deoarece $(E, u) \in P$. Dacă (F_1, v_1) şi $(F_2, v_2) \in P$, atunci definim:

(5) $$(F_1, v_1) \leq (F_2, v_2) \Leftrightarrow F_1 \subseteq F_2 \text{ şi } v_2 \text{ prelungeşte } v_1.$$

Este uşor de verificat că relația $\leq$ definită de (5) este o relație de ordine. Vom arăta că mulțimea $(P, \leq)$ este inductivă.

Fie $\{(F_i, v_i)\}_{i\in I}$ o parte total ordonată a lui P. Notăm $F = \bigcup_{i\in I} F_i$. Se arată uşor că F este un subcorp al lui L_1. Definim $v: F \to L_2$ astfel: dacă $\alpha \in F$, există $i \in I$, astfel încât $\alpha \in F_i$. Punem $v(\alpha) = v_i(\alpha)$.

Se arată uşor că aplicaţia v este bine definită şi este un morfism de corpuri. În plus, $(F, v) \in P$. Este clar că (F, v) este un majorant pentru familia $\{(F_i, v_i)\}_{i\in I}$. Prin urmare, $(P, \leq)$ este o mulţime inductivă. Conform lemei lui Zorn, în P există elemente maximale.

Fie (F_0, v_0) un element maximal al lui P. Vom arăta că $F_0 = L_1$. Să presupunem, prin reducere la absurd, că există $\alpha \in L_1 \setminus F_0$. Deoarece extinderea $L_1 \supseteq K$ este algebrică, şi extinderea $L_1 \supseteq F_0$ este algebrică. Fie $p_\alpha \in F_0[X]$ polinomul minimal al lui α.

Fie $\overline{v_0}: F_0[X] \to v_0(F_0)[X]$ izomorfismul de inele care prelungeşte v_0 şi $\overline{v_0}(X) = X$. Fie $q = \overline{v_0}(p_\alpha) \in v_0(F_0)[X] \subseteq L_2[X]$. Deoarece corpul L_2 este algebric închis, polinomul q are o rădăcină β în L_2. Conform 7.4., există un izomorfism $v: F_0(\alpha) \to v_0(F_0)(\beta) \subseteq L_2$ care prelungeşte v_0 şi $v(\alpha) = \beta$.

Rezultă astfel,

$$(F_0(\alpha), v) \in P \text{ şi } (F_0(\alpha), v) > (F_0, v_0),$$

contradicţie. Deci, $F_0 = L_1$ şi lema este demonstrată. □

9.6. **Teoremă.** *Fie L_1 şi L_2 două închideri algebrice ale corpului comutativ K. Atunci, există un izomorfism $w: L_1 \to L_2$, astfel încât $w(a) = a$, pentru orice $a \in K$.*

Demonstraţie. În lema 9.5., luăm:

$$E = K \text{ şi } u: K \to L_2,\ u(a) = a,\ \forall a \in K.$$

Rezultă că există un morfism de corpuri $w: L_1 \to L_2$, care prelungeşte u. $w(L_1)$ este subcorp al lui L_2, izomorf cu L_1. Prin urmare, $w(L_1)$ este corp algebric închis.

Fie $\beta \in L_2$. Deoarece $L_2 \supseteq K$ este extindere algebrică, β este algebric peste *K*. Fie $p_\beta \in K[X] \subseteq w(L_1)[X]$ polinomul minimal al lui β. Deoarece $w(L_1)$ este corp algebric închis, p_β are toate rădăcinile în $w(L_1)$. Deci, $\beta \in w(L_1)$. Rezultă $w(L_1) = L_2$ şi ca urmare, *w* este un izomorfism. Pentru orice $a \in K$, $w(a) = u(a) = a$. □

10. Corpul numerelor algebrice

În acest paragraf, ne ocupăm de extinderea $\mathbb{C} \supseteq \mathbb{Q}$.

10.1. **Definiţie.** *Un număr complex, algebric peste corpul numerelor raţionale se numeşte* ***număr algebric****. Un număr transcendent peste* $\mathbb{Q}$ *se numeşte simplu,* ***număr transcendent****.*

Mulţimea numerelor algebrice va fi notată conform relaţiei (3) din III.5. cu $\mathbb{C}'$.

Conform propoziţiei 5.4., închiderea algebrică $\mathbb{C}'$ a lui $\mathbb{Q}$ în $\mathbb{C}$ este subcorp al lui $\mathbb{C}$ care include $\mathbb{Q}$.

Se spune simplu: $\mathbb{C}'$ este ***corpul numerelor algebrice***.

Studiul corpului numerelor algebrice face obiectul teoriei algebrice a numerelor şi printre izvoarele sale se numără şi cercetările legate de marea teoremă a lui Fermat.

10.2. **Propoziţie.** *Mulţimea* $\mathbb{C}'$ *a numerelor algebrice este numărabilă.*

Demonstraţie. Are loc egalitatea:

$$\mathbb{C}' = \left\{ z \in \mathbb{C} \middle| \exists f \in \mathbb{Z}[X] \setminus \{0\}, f(z) = 0 \right\}.$$

Dacă $f \in \mathbb{Z}[X]$, atunci vom nota cu $s(f)$ suma valorilor absolute ale coeficienţilor lui *f*. Dacă $m, n \in \mathbb{N}^*$, atunci notăm:

$$\mathscr{P}_{m,n} = \left\{ f \in \mathbb{Z}[X] \middle| d^\circ f = m,\ s(f) = n \right\}.$$

Fiecare mulţime $\mathscr{P}_{m,n}$ este finită.

Pentru $f \in \mathbb{Z}[X] \setminus \{0\}$ vom nota:

$$A_f = \left\{ \alpha \in \mathbb{C} \middle| f(\alpha) = 0 \right\}.$$

Fiecare mulţime A_f este finită.

Din egalitatea:

$$\mathbb{C}' = \bigcup_{m=1}^{\infty} \bigcup_{n=1}^{\infty} \bigcup_{f \in \mathscr{P}_{m,n}} A_f$$

rezultă că $\mathbb{C}'$ este cel mult numărabilă (o reuniune numărabilă de mulţimi finite este cel mult numărabilă).

Cum, $\mathbb{C}' \supseteq \mathbb{Q}$, rezultă că $\mathbb{C}'$ este numărabilă. □

10.3. **Consecinţă.** *Mulţimea numerelor transcendente este nenumărabilă*.

Demonstraţie. Deoarece $\mathbb{C}$ este nenumărabilă şi $\mathbb{C}'$ este numărabilă, rezultă că mulţimea numerelor transcendente, $\mathbb{C} \setminus \mathbb{C}'$, este nenumărabilă. □

Demonstraţia faptului că un număr complex este transcendent este, în general, dificilă. Abia în 1844, Liouville a dat un criteriu care oferă o condiţie necesară ca un număr real să fie algebric. Numerele reale care nu satisfac această condiţie sunt numere transcendente.

10.4. **Criteriul lui Liouville.** *Fie* $\alpha \in \mathbb{R}$, *o rădăcină a unui polinom ireductibil* $f \in \mathbb{Z}[X]$, *cu* $d^\circ f = r \geq 2$. *Atunci există o constantă* $c > 0$, *astfel încât, pentru orice* $p, q \in \mathbb{Z}$, $q > 0$, *să rezulte*

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^r}.$$

Demonstraţie. Arătăm mai întâi că $\alpha \notin \mathbb{Q}$. Dacă, prin reducere la absurd, $\alpha \in \mathbb{Q}$, atunci $X - \alpha \mid f$ şi f este reductibil în $\mathbb{Q}[X]$, deci în $\mathbb{Z}[X]$. Contradicţie.

Fie $p, q \in \mathbb{Z}$, $q > 0$.

Dacă $\left| \alpha - \frac{p}{q} \right| > 1$, atunci $\left| \alpha - \frac{p}{q} \right| > \frac{1}{2} \cdot \frac{1}{q^r}$.

Să considerăm cazul $\left| \alpha - \frac{p}{q} \right| < 1$.

Din $d^\circ f = r$ şi $f\left(\frac{p}{q}\right) \neq 0$, rezultă:

(1) $$\left| f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^r}.$$

Fie $\alpha_1 = \alpha, \alpha_2, ..., \alpha_r$ toate rădăcinile lui f (în $\mathbb{C}$).

Cum $f = a\prod_{i=1}^{r}(X-\alpha_i),\ a \in \mathbb{Z}^*$, rezultă $f\left(\frac{p}{q}\right) = a\prod_{i=1}^{r}\left(\frac{p}{q}-\alpha_i\right)$.

Pentru $i \geq 2$,

$$\left|\frac{p}{q}-\alpha_i\right| \leq \left|\frac{p}{q}-\alpha\right| + |\alpha| + |\alpha_i| < 1 + |\alpha| + |\alpha_i|$$

şi astfel,

(2) $$\left| f\left(\frac{p}{q}\right)\right| < a\left|\frac{p}{q}-\alpha\right| \prod_{i=2}^{r}\left(1+|\alpha|+|\alpha_i|\right) = \left|\frac{p}{q}-\alpha\right| \cdot M.$$

Din (1) şi (2) rezultă:

$$\left|\frac{p}{q}-\alpha\right| \cdot M > \frac{1}{q^r}.$$

Dacă notăm $c = \min\left\{\frac{1}{2}, \frac{1}{M}\right\}$, atunci

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^r},$$

pentru orice $p, q \in \mathbb{Z},\ q > 0$. □

Probleme propuse

1. Fie $L \supseteq K$ o extindere de corpuri cu $[L:K] = p$, număr prim. Să se arate că:

a) Dacă E este un subcorp al lui L şi $E \supseteq K$, atunci $E = L$ sau $E = K$.

b) Orice element $\theta \in L \setminus K$ este element primitiv al extinderii, adică $L = K(\theta)$.

2. Fie $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Determinați:

a) $\left[K:\mathbb{Q}\right]$;

b) o bază a extinderii $K \supseteq \mathbb{Q}$ şi forma elementelor lui *K*.

3. Arătați că pentru orice $n \in \mathbb{N}^*$, există o extindere de grad *n* a corpului $\mathbb{Q}$.

4. Fie $\alpha = u + iv$ un număr complex. Arătați că:

a) α este algebric peste $\mathbb{Q} \Leftrightarrow$ *u* şi *v* sunt algebrice peste $\mathbb{Q}$;

b) Dacă α este algebric peste $\mathbb{Q}$ şi $|\alpha| \in \mathbb{Q}$, atunci are loc relația:

$$\mathbb{Q}(\alpha) \cap \mathbb{R} = \mathbb{Q}(u).$$

5. Fie $L \supseteq K$ o extindere de corpuri. Arătați că următoarele condiții sunt echivalente:

a) $L \supseteq K$ este extindere algebrică;

b) Orice subinel al lui *L* care include *K* este corp.

6. Fie α o rădăcină a polinomului $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Considerăm elementul $\beta = 1 + 2\alpha - 2\alpha^2$ din $\mathbb{Q}(\alpha)$.

a) Determinați α^{-1} şi β^{-1} în $\mathbb{Q}(\alpha)$.

b) Aflați polinomul minimal al lui β peste $\mathbb{Q}$.

7. Fie $L \supseteq K$ o extindere de corpuri şi $\alpha, \beta \in L$ algebrice peste *K*. Să se demonstreze, printr-un raționament direct, că $\alpha + \beta$, $\alpha\beta$, $-\alpha$ şi α^{-1} (dacă $\alpha \neq 0$) sunt algebrice peste *K*.
Aplicație: Determinați polinomul minimal peste $\mathbb{Q}$ al elementului $\sqrt{2} + \sqrt[3]{3}$.

8. Fie $L \supseteq K$ o extindere de corpuri şi $\theta \in L$ algebric peste *K*. Printr-un raționament direct, să se arate că inelul $K[\theta]$ este corp.

9. Fie *K* un corp comutativ şi $f \in K[X]$ cu $d^\circ f = n \geq 1$. Fie *L* o extindere a lui *K* în care *f* are toate rădăcinile $\alpha_1, \alpha_2, ..., \alpha_n$. Se consideră polinomul simetric $g \in K[X_1, X_2, ...X_n]$.

Arătați că $g(\alpha_1,\alpha_2,...,\alpha_n)\in K$. Analog, pentru fracția simetrică $h\in K(X_1,X_2,...X_n)$.

10. Fie $L\supseteq K$ o extindere de corpuri şi $\alpha,\beta,a\in L,$ unde α,β sunt transcendente peste *K* şi *a* este algebric peste *K*. Precizați, dacă este posibil, natura elementelor:

$$-\alpha,\ \alpha^{-1},\ \alpha+\alpha^2,\ \alpha^n\ (n\geq 2),\ \alpha+\beta,\ \alpha\beta,\ a+\beta,\ a\beta.$$

11. Fie *K* un corp comutativ şi $a=\frac{f(X)}{g(X)}$ o fracție ireductibilă din $K(X),$ cu $g\neq 0$ şi $a\notin K$. Atunci, $\left[K(X):K(a)\right]=\max\left(d^\circ f,d^\circ g\right)$. În particular, arătați că corpul *K* este algebric închis în $K(X)$.

12. Fie $L\supseteq K$ o extindere de corpuri şi $f,g\in K[X],$ polinoame relativ prime, cu $g\neq 0$. Arătați că:

a) Extinderea $K\left(\frac{f(x)}{g(x)}\right)\subseteq K(x)$ este finită, $(\forall)x\in L,\ g(x)\neq 0.$

b) $x\in L$ este transcendent peste $K\ \Leftrightarrow\ \frac{f(x)}{g(x)}$ este transcendent peste *K*.

13. Fie $f=X^n-\alpha\in L[X],\ n\geq 1,$ unde *L* este o extindere a corpului comutativ *K*. Arătați că rădăcinile polinomului *f* sunt transcendente peste *K* dacă şi numai dacă α este transcendent peste *K*.

14. Ştiind că *e* şi π sunt numere transcendente, precizați natura numerelor $a=\frac{\sqrt{2}+\pi\sqrt[3]{5}-2\pi^2}{\sqrt{7}-\pi\sqrt[5]{3}+(1+i)\pi^2}$ şi $b=\sqrt{e}+\sqrt[3]{e}+\sqrt[5]{e}$.

15. Fie *K* corp comutativ, $f\in K[X]$ cu $d^\circ f=n\geq 1$ şi *L* corpul de descompunere pentru polinomul *f*. Atunci, $[L:K]\leq n!$.

16. Fie $f = X^4 + \hat{1} \in \mathbb{Z}_3[X]$.

a) Construiți un corp de descompunere L pentru f.

b) Precizați forma elementelor lui L şi $card(L)$.

Aceleaşi cerințe pentru polinoamele:

$$g = X^4 + X^3 + X^2 + \hat{4}X + \hat{3} \in \mathbb{Z}_5[X];$$

$$h = X^4 + \hat{2}X^3 + \hat{2}X + \hat{2} \in \mathbb{Z}_3[X].$$

17. Pentru polinomul $f = X^3 + \hat{2}X^2 + \hat{2} \in \mathbb{Z}_3[X]$, determinați un corp de descompunere. Aflați apoi în corpul construit, rădăcinile polinomului $g = \hat{2}X^2 + X + \hat{1} \in \mathbb{Z}_3[X]$.

18. Fie $f = X^6 - 2X^3 - 2 \in \mathbb{Q}[X]$ şi K corpul de descompunere al lui f. Atunci:

a) f este ireductibil în $\mathbb{Q}[X]$ şi rădăcinile sale sunt rădăcinile cubice ale lui $1 \pm \sqrt{3}$.

b) $\left\{\sqrt{3}, i\sqrt{3}, i\right\} \subset K$.

c) Considerând produsul a două rădăcini reale ale lui f, arătați că $\sqrt[3]{2} \in K$.

d) Fie $L = \mathbb{Q}\left(\sqrt[3]{2}, i, \sqrt{3}\right)$. Arătați că $[L:\mathbb{Q}] = 12$ şi că, adjuncționând la L o rădăcină cubică a unui element din L, se obține corpul K.

19. Fie $f = X^p - X + a \in K[X]$ unde K este un corp comutativ, de caracteristică p, număr prim. Arătați că:

a) Dacă α este o rădăcină a lui f într-o extindere a corpului K, atunci $\alpha + \hat{k}$ este rădăcină a lui f, pentru orice $\hat{k} \in \mathbb{Z}_p$.

b) În $K[X]$, f este ireductibil sau se descompune în produs de factori distincți, de gradul 1.

20. Fie K un corp de caracteristică diferită de 2 şi $a, b \in K$. Fie L, corpul de descompunere al polinomului $f = X^4 - (a+b)X^2 + ab$.

Arătați că $\left[L:K\right]=4 \Leftrightarrow a,\ b$ şi ab nu sunt pătrate perfecte în K.

21. Arătați că extinderile pătratice ale unui corp comutativ K sunt corpuri de descompunere ale unor polinoame ireductibile din $K[X]$ de forma:

i) $f=X^2-a,$ dacă $car(K)\neq 2;$

ii) $f=X^2-a$ sau $f=X^2+X-a,$ dacă $car(K)=2.$

22. Fie $L=K\left(X_1,...,X_n\right)$ corpul fracțiilor raționale în nedeterminatele $X_1,...,X_n,$ cu coeficienți în corpul comutativ K. Arătați că L este o extindere finită a corpului $E=K\left(s_1,...,s_n\right)$ unde $s_1,...,s_n$ sunt polinoamele simetrice fundamentale în $X_1,...,X_n$ şi să se determine gradul său.

23. Arătați că pentru un corp comutativ K, corpul $K(X)$ nu este algebric închis.

24. Fie $L\supseteq K$ o extindere de corpuri. Dacă orice polinom $f\in K[X]$ ireductibil, rămâne ireductibil în $L[X]$, atunci K este corp algebric închis în L.

25. Pentru $L\supseteq K,$ o extindere de corpuri, considerăm mulțimea:

$$\mathscr{L}_a=\left\{E\in\mathscr{L}\left(L;K\right)\mid E \text{ algebric închis în } L\right\}.$$

Arătați că $\left(\mathscr{L}_a,\subseteq\right)$ este o latice completă.

Caz particular: mulțimea subcorpurilor lui $\mathbb{C},$ algebric închise în $\mathbb{C},$ este o latice completă (în raport cu $\subseteq$).

26. Arătați că închiderea algebrică a lui $\mathbb{Q}\left(\sqrt{2}\right)$ în $\mathbb{C}$ coincide cu corpul numerelor algebrice.

27. Să se arate că numărul $\alpha=\sum_{n=0}^{\infty}\frac{1}{5^{n!}}$ este transcendent.

Capitolul IV

GRUPURI REZOLUBILE

Grupurile rezolubile joacă un rol important în caracterizarea ecuațiilor algebrice rezolvabile prin radicali. În acest capitol sunt prezentate proprietățile de bază ale grupurilor rezolubile. În particular, se studiază cazul grupurilor finite, al grupurilor de permutări şi al *p*-grupurilor (rezultatele referitoare la *p*-grupuri se regăsesc în cadrul problemelor propuse).

1. Şiruri normale de subgrupuri

Fie $(G,\cdot)$ un grup şi H un subgrup al său.

Reamintim că se spune că H este ***subgrup normal*** al lui G şi se notează $H \trianglelefteq G$ dacă

(1) $$xH = Hx, \ \forall x \in G.$$

Cu alte cuvinte, un subgrup este normal atunci când clasele sale de resturi la stânga coincid cu clasele de resturi la dreapta.

În mod evident, $(e) \trianglelefteq G$ şi $G \trianglelefteq G$.

Condiția (1) este echivalentă cu condiția:

(2) $$xhx^{-1} \in H, \ \forall x \in G \text{ şi } \forall h \in H.$$

Dacă $f : G \to G'$ este un morfism de grupuri, atunci $Kerf \trianglelefteq G$.

Fie $\mathscr{S}_n$ grupul de permutări de grad n şi $\mathscr{A}_n$ subgrupul permutărilor pare sau grupul altern de grad n. Dacă $\sigma \in \mathscr{S}_n$ şi $\tau \in \mathscr{A}_n$ atunci $\sigma\tau\sigma^{-1} \in \mathscr{A}_n$. Deci, $\mathscr{A}_n \trianglelefteq \mathscr{S}_n$.

1.1. **Definiție.** *Fie* $(G,\cdot)$ *un grup. Numim* ***şir normal*** *al lui G o secvență de subgrupuri ale lui G de forma*

(3) $G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = (e)$

unde $H_i \trianglelefteq H_{i-1}$ *pentru orice* $i \in \overline{1,s}$. *Numărul s se numeşte* ***lungimea*** *şirului normal* (3) *iar grupurile factor* H_{i-1}/H_i, $i \in \overline{1,s}$ *se numesc* ***factorii*** *şirului normal.*

$G \supseteq (e)$ este totdeauna un şir normal de lungime 1 şi singurul său factor este $G/(e) \simeq G$.

Dacă $H \trianglelefteq G$, atunci $G \supseteq H \supseteq (e)$ este un şir normal de lungime 2 având factorii G/H şi $H/(e) \simeq H$.

În particular, $\mathscr{S}_n \supseteq \mathscr{A}_n \supseteq (e)$ este un şir normal de lungime 2 având factorii $\mathscr{S}_n/\mathscr{A}_n \simeq \mathbb{Z}_2$ şi $\mathscr{A}_n/(e) \simeq \mathscr{A}_n$.

Studiem în continuare imaginile directe şi reciproce ale şirurilor normale prin morfisme de grupuri.

1.2. **Propoziție.** *Fie* $(G,\cdot)$ *un grup şi*

(3) $G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = (e)$

un şir normal al său.

Fie $f : G \to \overline{G}$ *un morfism surjectiv de grupuri şi* $\overline{H_i} = f(H_i)$, $i \in \overline{0,s}$. *Atunci,*

(4) $\overline{G} = \overline{H_0} \supseteq \overline{H_1} \supseteq \ldots \supseteq \overline{H_s} = \overline{(e)}$

este un şir normal al lui $\overline{G}$. *În plus, pentru orice* $i \in \overline{1,s}$, *există un morfism surjectiv de grupuri*

$$f_i : H_{i-1}/H_i \to \overline{H_{i-1}}/\overline{H_i}.$$

Demonstrație. Deoarece f este surjectiv, $f(G) = \overline{G} = \overline{H_0}$. Imaginea unui subgrup printr-un morfism de grupuri este de asemenea un subgrup. Deci, $\overline{H_i}$ sunt subgrupuri ale lui $\overline{G}$, pentru $i \in \overline{1,s}$. Mai mult, imaginea unui subgrup normal printr-un morfism surjectiv este un subgrup normal. Deci, $\overline{H_1} \trianglelefteq \overline{H_0}$. În general, considerând restricția lui f la H_{i-1} cu valori în $\overline{H_{i-1}}$ rezultă că $\overline{H_i} \trianglelefteq \overline{H_{i-1}}$, $i \in \overline{1,s}$. Evident, $\overline{H_s} = f(H_s) = \overline{(e)}$. Rezultă că (4) este un şir normal al lui $\overline{G}$.

Fie acum $i \in \overline{1,s}$, o valoare fixată şi $f_i : H_{i-1} / H_i \to \overline{H_{i-1}} / \overline{H_i}$ aplicaţia definită prin $f_i(xH_i) = f(x)\overline{H_i}$, $\forall x \in H_{i-1}$.

Dacă $y \in xH_i$, atunci există $h \in H_i$ astfel încât $y = xh$.

$$f(y)\overline{H_i} = f(x)f(h)\overline{H_i} = f(x)\overline{H_i},$$

ceea ce arată că f_i este bine definită.

Dacă $x, y \in H_{i-1}$, atunci

$$f_i(xH_i \cdot yH_i) = f_i(xyH_i) = f(xy)\overline{H_i} = f(x)f(y)\overline{H_i} =$$
$$= f(x)\overline{H_i} \cdot f(y)\overline{H_i} = f_i(xH_i)f_i(yH_i),$$

adică f_i este morfism de grupuri.

Fie $z\overline{H_i} \in \overline{H_{i-1}} / \overline{H_i}$. Rezultă $z \in \overline{H_{i-1}} = f(H_{i-1})$, deci există $x \in H_{i-1}$ astfel încât $z = f(x)$ şi $z\overline{H_i} = f_i(xH_i)$ ceea ce demonstrează surjectivitatea lui f_i. □

Conform propoziţiei 1.2., imaginea unui şir normal printr-un morfism surjectiv de grupuri este un şir normal de aceeaşi lungime. În plus, între factorii celor două şiruri normale există anumite morfisme canonice.

1.3. **Propoziţie.** *Fie* $f : G \to \overline{G}$ *un morfism de grupuri. Fie*

(4) $$\overline{G} = \overline{H_0} \supseteq \overline{H_1} \supseteq \ldots \supseteq \overline{H_s} = \overline{(e)}$$

un şir normal al grupului $\overline{G}$.

Pentru $i \in \overline{0,s}$ *se notează* $H_i = f^{-1}\left(\overline{H_i}\right)$. *Atunci,*

(3′) $$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = Kerf \supseteq (e)$$

este un şir normal al grupului G. În plus, pentru orice $i \in \overline{1,s}$, *există un morfism injectiv de grupuri*

$$f_i : H_{i-1} / H_i \to \overline{H_{i-1}} / \overline{H_i}.$$

Demonstraţie. $H_0 = f^{-1}\left(\overline{H_0}\right) = f^{-1}\left(\overline{G}\right) = G.$

$H_s = f^{-1}\left(\overline{H_s}\right) = f^{-1}\left(\overline{(e)}\right) = Kerf$. Cum imaginea reciprocă a unui subgrup normal printr-un morfism de grupuri este tot un subgrup

normal, rezultă că $(3')$ este un şir normal al grupului G. Şirul $(3')$ are, în general, lungimea mai mare cu 1 decât lungimea şirului (4).

Fie $i \in \overline{1,s}$, o valoare fixată. Definim $f_i : H_{i-1}/H_i \to \overline{H_{i-1}}/\overline{H_i}$ prin

$$f_i(xH_i) = f(x)\overline{H_i}, \quad \forall x \in H_{i-1}.$$

Din $x \in H_{i-1} = f^{-1}\left(\overline{H_{i-1}}\right)$, rezultă $f(x) \in \overline{H_{i-1}}$, deci:

$$f(x)\overline{H_i} \in \overline{H_{i-1}}/\overline{H_i}.$$

Dacă $y \in xH_i$, atunci există $h \in H_i$ astfel încât $y = xh$. Ca şi în demonstraţia propoziţiei 1.2., rezultă $f(x)\overline{H_i} = f(y)\overline{H_i}$, cu alte cuvinte, aplicaţia f_i este bine definită. Se arată de asemenea uşor că f_i este morfism de grupuri.

Fie $xH_i \in Kerf_i$. Deci, $f_i(xH_i) = f(x)\overline{H_i} = \overline{H_i}$. De aici rezultă că $f(x) \in \overline{H_i}$ sau $x \in H_i = f^{-1}\left(\overline{H_i}\right)$ şi $xH_i = H_i$ (elementul neutru al lui H_{i-1}/H_i). Ca urmare, f_i este un morfism injectiv de grupuri. □

Din propoziţia 1.3., rezultă că imaginea reciprocă a unui şir normal printr-un morfism de grupuri, completată cu (e), este un şir normal de lungime mai mare cu 1 decât lungimea şirului iniţial. Cele două şiruri normale au aceeaşi lungime dacă morfismul iniţial este injectiv.

1.4. **Observaţie.** Presupunem că morfismul f din propoziţia 1.3. este surjectiv. În acest caz, vom arăta că morfismele f_i sunt chiar izomorfisme.

Fie $y \in \overline{H_{i-1}}$. Deoarece f este surjectiv, există $x \in G$, astfel încât $f(x) = y$. Atunci, $x \in H_{i-1}$ şi $f_i(xH_i) = f(x)\overline{H_i} = y\overline{H_i}$ ceea ce justifică surjectivitatea lui f_i. Cum f_i, $i \in \overline{1,s}$, sunt şi morfisme injective, rezultă că sunt izomorfisme.

2. Şiruri rezolubile. Grupuri rezolubile

2.1. **Definiție.** *Se spune că* ***şirul*** *normal*

(3) $$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_s = (e)$$

al grupului G este ***rezolubil*** *dacă toți factorii săi sunt abelieni.*
Se spune că G este ***grup rezolubil*** *dacă admite cel puțin un şir normal rezolubil.*

Este evident că orice grup abelian G este rezolubil, şirul normal $G \supseteq (e)$ fiind rezolubil.

De importanță deosebită se vor dovedi grupurile neabeliene dar rezolubile.

Astfel, $\mathscr{S}_3$, care nu este abelian, este rezolubil. Într-adevăr, să considerăm şirul normal:

(5) $$\mathscr{S}_3 \supseteq \mathscr{A}_3 \supseteq (e).$$

Atunci,

$\left|\mathscr{S}_3 / \mathscr{A}_3\right| = \left(\mathscr{S}_3 : \mathscr{A}_3\right) = 2,$ deci $\mathscr{S}_3 / \mathscr{A}_3 \simeq \mathbb{Z}_2$ care este abelian.

$\mathscr{A}_3 / (e) \simeq \mathscr{A}_3 \simeq \mathbb{Z}_3$ care este de asemenea abelian.

Să arătăm că şi $\mathscr{S}_4$ este grup rezolubil. Pentru aceasta considerăm secvența de subgrupuri:

(6) $$\mathscr{S}_4 \supseteq \mathscr{A}_4 \supseteq H \supseteq (e)$$

unde $H = \{e, (12)(34), (13)(24), (14)(23)\}$.

H este un subgrup al lui $\mathscr{A}_4$, izomorf cu grupul lui Klein, deci abelian.

Mai mult, dacă $\sigma \in \mathscr{A}_4$ şi $(ij)(hk) \in H,$ atunci se verifică egalitatea:

$$\sigma(ij)(hk)\sigma^{-1} = \left(\sigma(i), \sigma(j)\right)\left(\sigma(h), \sigma(k)\right) \in H.$$

Deci, $H \trianglelefteq \mathscr{A}_4$.

$$\left|\mathscr{S}_4 / \mathscr{A}_4\right| = \left(\mathscr{S}_4 : \mathscr{A}_4\right) = \frac{\left|\mathscr{S}_4\right|}{\left|\mathscr{A}_4\right|} = 2 \Rightarrow \mathscr{S}_4 / \mathscr{A}_4 \simeq \mathbb{Z}_2$$

$$\left|\mathscr{A}_4 / H\right| = \left(\mathscr{A}_4 : H\right) = \frac{\left|\mathscr{A}_4\right|}{\left|H\right|} = 3 \Rightarrow \mathscr{A}_4 / H \simeq \mathbb{Z}_3.$$

Prin urmare, (6) este un şir rezolubil şi $\mathscr{S}_4$ este grup rezolubil.

3. Nerezolubilitatea grupurilor $\mathscr{S}_n$ pentru $n \geq 5$

Pentru studiul grupurilor $\mathscr{S}_n$, $n \geq 5$, demonstrăm mai întâi următorul rezultat ajutător.

3.1. **Lemă.** *Fie G un subgrup al lui $\mathscr{S}_n$, $n \geq 5$ şi $H \trianglelefteq G$ astfel încât G/H este abelian. Dacă G conţine toate ciclurile de lungime 3, atunci H conţine toate ciclurile de lungime 3.*

Demonstraţie. Fie $i, j, k \in \overline{1,n}$, distincte. Cum $n \geq 5$, rezultă că există $s, t \in \overline{1,n}$, distincte şi diferite de i, j, k. În G are loc egalitatea:

$$(jis)^{-1}(kit)^{-1}(jis)(kit) = (ijk).$$

Trecând la clase în grupul G/H şi ţinând seama de proprietatea de comutativitate a acestuia rezultă $\widehat{(ijk)} = \hat{e} = H$, deci $(ijk) \in H$. Cum i, j, k sunt arbitrare, H conţine toate ciclurile de lungime 3. □

3.2. **Teoremă.** *Grupul $\mathscr{S}_n$ al permutărilor de grad $n \geq 5$ nu este rezolubil.*

Demonstraţie. Prin reducere la absurd, să presupunem că $\mathscr{S}_n$ este rezolubil şi fie

$$\mathscr{S}_n = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = (e)$$

un şir rezolubil al lui $\mathscr{S}_n$. $\mathscr{S}_n$ conţine toate ciclurile de lungime 3, $H_1 \trianglelefteq H_0 = \mathscr{S}_n$ şi $\mathscr{S}_n / H_1$ este abelian. Rezultă, conform lemei 3.1., că H_1 conţine toate ciclurile de lungime 3.

Presupunem că pentru un argument $k \geq 1$, H_{k-1} conţine toate ciclurile de lungime 3. Cum $H_k \trianglelefteq H_{k-1}$ şi H_{k-1}/H_k este grup abelian, rezultă că H_k conţine toate ciclurile de lungime 3.

În definitiv, H_s conţine toate ciclurile de lungime 3, ceea ce contravine relaţiei $H_s = (e)$. Prin urmare, $\mathscr{S}_n$ nu este rezolubil. □

4. Grupuri rezolubile. Proprietăți generale

Revenim la studiul grupurilor rezolubile oarecare.

4.1. **Teoremă.** *Fie G un grup oarecare şi $H \trianglelefteq G$. Grupul G este rezolubil dacă şi numai dacă grupurile H şi G/H sunt rezolubile.*

Demonstrație. Să presupunem mai întâi că grupul G este rezolubil şi fie

(3) $$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = (e)$$

un şir rezolubil. Fie $j : H \to G,\ \ j(x) = x,\ \ x \in H,$ morfismul incluziune. Notăm $H_i' = j^{-1}(H_i) = H_i \cap H,\ \ i \in \overline{0,s}.$ Conform propoziției 1.3., şirul

(7) $$H = H_0' \supseteq H_1' \supseteq \ldots \supseteq H_s' = Kerj = (e)$$

este un şir normal al grupului H. În plus, pentru orice $i \in \overline{1,s},$ există un morfism injectiv de grupuri $f_i : H_{i-1}'/H_i' \to H_{i-1}/H_i.$

Deoarece (3) este rezolubil, factorii H_{i-1}/H_i sunt abelieni, deci $H_{i-1}'/H_i' \simeq \operatorname{Im} f_i$ sunt grupuri abeliene. Astfel, (7) este şir rezolubil şi ca urmare, H este grup rezolubil. Se observă în plus că un şir rezolubil pentru H se obține întersectând H cu fiecare termen al unui şir rezolubil al lui G.

Să considerăm surjecția canonică $\varphi : G \to G/H$ şi să notăm, ca în propoziția 1.2., $\overline{H_i} = \varphi(H_i),\ \ i \in \overline{0,s}.$ Rezultă

(8) $$G/H = \overline{H_0} \supseteq \overline{H_1} \supseteq \ldots \supseteq \overline{H_s} = \overline{(e)}$$

este un şir normal pentru G/H şi, în plus, pentru fiecare $i \in \overline{1,s},$ există un morfism surjectiv de grupuri $f_i : H_{i-1}/H_i \to \overline{H_{i-1}}/\overline{H_i}.$

Cum factorii H_{i-1}/H_i sunt abelieni, $\overline{H_{i-1}}/\overline{H_i}$ sunt de asemenea abelieni, deci (8) este un şir rezolubil şi G/H este grup rezolubil.

Pentru reciprocă, să presupunem că H şi G/H sunt grupuri rezolubile. Fie

(9) $$H = H_0' \supseteq H_1' \supseteq \ldots \supseteq H_r' = (e)$$

un şir rezolubil al lui H şi

(10) $$G/H = \overline{H_0} \supseteq \overline{H_1} \supseteq ... \supseteq \overline{H_t} = \overline{(e)}$$

un şir rezolubil al lui G/H. Aplicând propoziția 1.3. pentru surjecția canonică $\varphi : G \to G/H$ şi notând $H_i = \varphi^{-1}\left(\overline{H_i}\right)$,

(11) $$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_t \supseteq (e)$$

este un şir normal al lui *G*. Conform observației 1.4., morfismele $f_i : H_{i-1}/H_i \to \overline{H_{i-1}}/\overline{H_i}$ sunt izomorfisme şi ca urmare H_{i-1}/H_i sunt grupuri abeliene pentru $i \in \overline{0,t}$. În concluzie,

$$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_t = H = H_0' \supseteq H_1' \supseteq ... \supseteq H_r' = (e)$$

este un şir rezolubil al lui *G*. □

4.2. **Consecință.** *Fie G un grup. G este rezolubil dacă şi numai dacă are un şir normal cu factorii grupuri rezolubile.*

Demonstrație. Dacă *G* este rezolubil, atunci *G* are un şir rezolubil. Factorii acestui şir sunt abelieni, deci sunt grupuri rezolubile.

Reciproc, să presupunem că *G* are un şir normal

(3) $$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_s = (e)$$

cu factorii grupuri rezolubile. Vom demonstra prin inducție după *s*, că *G* este rezolubil.

Pentru $s = 2$ se aplică teorema 4.1.

Presupunem afirmația adevărată pentru valoarea $s-1$ şi demonstrăm că este adevărată şi pentru valoarea *s*, $s > 2$. Conform ipotezei de inducție, rezultă că H_1 este rezolubil. Atunci,

$$G = H_0 \supseteq H_1 \supseteq (e)$$

este un şir normal cu factorii rezolubili. Conform teoremei 4.1., *G* este rezolubil. □

5. Cazul grupurilor finite

5.1. **Teoremă.** *Fie G un grup finit. G este rezolubil dacă şi numai dacă are un şir normal cu factorii grupuri ciclice.*

Demonstrație. Dacă *G* admite un şir normal cu factorii ciclici, acel şir normal este rezolubil (orice grup ciclic este abelian), deci *G* este rezolubil.

Implicația reciprocă o demonstrăm prin inducție după $|G|$.

Dacă $|G| = 2,$ atunci G este ciclic şi $G \supseteq (e)$ este un şir normal cu factorii ciclici.

Presupunem afirmația adevărată pentru grupuri cu mai puțin de n elemente şi fie G un grup rezolubil cu n elemente, $n > 2.$ Fie (3) un şir rezolubil pentru G. Putem presupune, $H_1 \neq G.$

Tratăm mai întâi cazul în care $H_1 \neq (e).$

Atunci H_1 şi G/H_1 sunt grupuri rezolubile (conform teoremei 4.1.) şi $|H_1| < n,$ $|G/H_1| < n.$ Conform ipotezei de inducție, H_1 şi G/H_1 admit şiruri normale cu factorii ciclici. Fie acestea

$$H_1 = K_0 \supseteq K_1 \supseteq ... \supseteq K_r = (e)$$

$$G/H_1 = L_0 \supseteq L_1 \supseteq ... \supseteq L_t = \left(\hat{e}\right).$$

Fie $\varphi : G \to G/H_1$ surjecția canonică. Notăm $L_i' = \varphi^{-1}(L_i),$ $i \in \overline{1,t}.$

Atunci,

$$G = L_0' \supseteq L_1' \supseteq ... \supseteq L_t' = H_1 \supseteq (e)$$

este un şir normal. Ca şi în demonstrația teoremei 4.1., rezultă

$$L_{i-1}/L_i \simeq L_{i-1}'/L_i',\ i \in \overline{1,t}.$$

Astfel,

$$G = L_0' \supseteq L_1' \supseteq ... \supseteq L_t' = K_0 \supseteq K_1 \supseteq ... \supseteq K_r = (e)$$

este un şir normal cu factorii grupuri ciclice.

Să considerăm cazul $H_1 = (e).$

Şirul (3) se reduce în acest caz la $G \supseteq (e)$ şi ca urmare, G este abelian. Fie $x \in G \setminus \{e\}$ şi $H = (x).$ Dacă $H = G,$ atunci G este ciclic şi $G \supseteq (e)$ satisface condiția cerută. Dacă $H \neq G,$ atunci se repetă raționamentul de mai sus pentru $H_1 = H.$ □

Probleme propuse

1. Fie $M(A)=U(A)\times A,$ unde A este un inel comutativ, unitar. Pe $M(A)$ definim operația:

$$(a,b)*(c,d)=(ac,bc+d),\quad a,c\in U(A),\quad b,d\in A.$$

Arătați că $(M(A),*)$ este un grup rezolubil.

2. Fie p un număr prim. Un grup finit de ordin $p^n,$ unde $n\in\mathbb{N}^*$ se numește ***p – grup***. Arătați că:

a) Dacă $(G,\cdot)$ este un p – grup, atunci $Z(G)\neq(e).$

b) Orice p – grup este rezolubil.

3. Fie G_1 şi G_2 două grupuri rezolubile. Arătați că produsul lor direct, $G_1\times G_2,$ este şi el un grup rezolubil.

4. Fie D_n grupul diedral de grad n (grupul de simetrie al lui P_n, un poligon regulat cu n laturi), $n>2.$ Arătați că D_n este grup rezolubil, pentru orice $n>2.$

5. Fie $(G,\cdot)$ un grup şi $x,y\in G.$ Definim ***comutatorul elementelor*** x şi y ca fiind expresia $[x,y]=xyx^{-1}y^{-1}.$ Arătați că pentru orice $x,y,z\in G$ se verifică relațiile:

a) $xy=yx\Leftrightarrow[x,y]=e;$

b) $[xy,z]=x[y,z]x^{-1}[x,z];$

c) $[x,yz]=[x,y]y[x,z]y^{-1}.$

6. Fie G un grup astfel încât $(G:Z(G))=n,\ n\geq 1.$ Arătați că

a) în G există cel mult n^2 comutatori diferiți;

b) $[x,y]^{n+1}=[x,y^2][y^{-1}xy,y]^{n-1}$, pentru orice $x,y\in G.$

7. Definim G' ***subgrupul derivat*** al grupului G (sau ***comutantul*** lui G) ca fiind subgrupul generat de mulțimea comutatorilor lui G: $G' = \left\langle \left\{ [x, y] \mid x, y \in G \right\} \right\rangle$.

Subgrupul derivat al lui G se mai notează cu $G^{(1)}$ sau $[G, G]$. Atunci:

a) Stabiliți o reprezentare a elementelor lui G';

b) Arătați că G este grup comutativ dacă şi numai dacă $G' = (e)$;

c) Dacă G este finit, atunci $|G / G'| \leq |C_G(x)|$ unde $x \in G$ şi $C_G(x)$ este centralizatorul lui x în G (subgrupul lui G format din toate elementele grupului G care comută cu x);

d) Determinați subgrupul derivat al grupului $\mathscr{S}_n$ pentru $n \geq 1$;

e) Arătați că pentru $n \geq 5$, subgrupul derivat al lui $\mathscr{A}_n$ este $\mathscr{A}_n$.

8. Fie $f : G \to \overline{G}$ un morfism de grupuri. Arătați că $f(G') \subseteq \overline{G}'$. Stabiliți ce condiție suplimentară trebuie impusă lui f pentru a obține egalitate în relația precizată.

9. Fie G un grup şi $H \trianglelefteq G$. Arătați că:

a) $H' \trianglelefteq G$;

b) $G' \trianglelefteq G$.

10. Fie H un subgrup al grupului G. Atunci:

a) Dacă $H \supseteq G'$, demonstrați că $H \trianglelefteq G$ şi grupul factor G / H este abelian. Ce fel de grup este G / G' ?

b) Dacă $H \trianglelefteq G$ şi G / H este grup abelian, arătați că $H \supseteq G'$.

11. Fie G un grup. Pentru fiecare număr natural n definim recursiv subgrupurile $G^{(n)}$ ale lui G astfel:

$$G^{(0)} = G \text{ şi } G^{(n+1)} = \left[G^{(n)}, G^{(n)} \right] = \left(G^{(n)} \right)', \text{ pentru } n \geq 0.$$

$G^{(n)}$ poartă numele de al ***n*-lea *comutant*** al grupului G. Arătați că:

a) G este rezolubil dacă şi numai dacă există n număr natural nenul pentru care $G^{(n)} = (e)$.

b) Fie G un grup rezolubil iar n_0 cel mai mic număr natural pentru care $G^{(n_0)} = (e)$ (n_0 se va numi ***grad de rezolubilitate*** al lui G).

Dacă considerăm şirul rezolubil $(e) = H_r \trianglelefteq ... \trianglelefteq H_1 \trianglelefteq G$, atunci $G^{(i)} \leq H_i$, $1 \leq i \leq r$. În particular, $r \geq n_0$.

c) Stabiliți care este gradul de rezolubilitate al unui grup abelian G care are mai mult de un element şi al grupului $\mathscr{S}_3$.

12. Folosind caracterizarea grupurilor rezolubile de la exercițiul anterior, să se demonstreze că $\mathscr{S}_n$ nu este rezolubil pentru $n \geq 5$.

13. Un ***şir normal*** $G = H_n \supseteq H_{n-1} \supseteq ... \supseteq H_1 \supseteq H_0 = (e)$ al grupului G se numeşte ***central*** dacă $H_i / H_{i-1} \leq Z\left(G / H_{i-1}\right)$, pentru $i \in \overline{1,n}$. Grupul G se va numi ***grup nilpotent***.

a) Pentru grupul G construim recursiv şirul $\left(Z_n(G)\right)_{n\geq 0}$ astfel:

$$Z_0(G) = (e) \text{ şi } Z_{n+1}(G) / Z_n(G) = Z\left(G / Z_n(G)\right), \ n \geq 1.$$

Arătați că G este grup nilpotent dacă şi numai dacă există $n \in \mathbb{N}$ astfel încât $Z_n(G) = G$.

b) Demonstrați că orice grup rezolubil este nilpotent. Afirmația reciprocă este adevărată?

Capitolul V

ELEMENTE DE TEORIE GALOIS

În acest capitol apare ideea de bază a teoriei lui Galois şi anume, studiul proprietăţilor unor extinderi de corpuri cu ajutorul unui grup de automorfisme asociat extinderii. Dacă $L \supseteq K$ este o extindere de corpuri comutative, atunci cu $\mathscr{L}(L;K)$ se notează laticea subcorpurilor intermediare între L şi K. Dacă G este grupul Galois de automorfisme asociat extinderii $L \supseteq K$, atunci $\mathscr{L}(G)$ notează laticea subgrupurilor lui G.

În V.9., teorema fundamentată prezintă condiţii în care, între cele două latice se stabileşte o bijecţie. Pentru a ajunge aici a fost necesară studierea în paragrafele precedente a extinderilor normale şi separabile, precum şi stabilirea unor rezultate ajutătoare privind rădăcinile primitive ale unităţii şi corpurile finite. Teorema fundamentală a teoriei lui Galois va constitui instrumentul de bază folosit în capitolul următor pentru studiul rezolvării ecuaţiilor prin radicali.

1. Grup Galois al unei extinderi. Corespondenţe Galois

Fie M o mulţime oarecare. Prin ***permutare*** a mulţimii M se înţelege orice funcţie bijectivă $\sigma : M \to M$. Mulţimea tuturor permutărilor mulţimii M, notată $\mathscr{S}(M)$, formează un grup în raport cu compunerea funcţiilor, numit ***grupul permutărilor mulţimii*** M.

În continuare considerăm L un corp comutativ şi notăm mulţimea automorfismelor corpului L cu $Aut(L)$. Evident, $Aut(L) \subseteq \mathscr{S}(L)$.

Dacă $\sigma, \tau \in Aut(L)$, atunci $\sigma \circ \tau \in Aut(L)$ şi $\sigma^{-1} \in Aut(L)$.

Deci, $Aut(L)$ este un subgrup al lui $\mathscr{S}(L)$. $Aut(L)$ poartă numele de ***grup al automorfismelor corpului*** L.

Să presupunem, în plus, că L este o extindere a corpului K şi să notăm

(1) $$G(L\,|\,K)=\left\{\sigma\in Aut(L)\,\middle|\,\forall a\in K,\ \sigma(a)=a\right\}.$$

Dacă $\sigma,\tau\in G(L\,|\,K)$, atunci, $\sigma(a)=a$, $\tau(a)=a$, $\forall a\in K$.

$$(\sigma\circ\tau)(a)=\sigma(\tau(a))=\sigma(a)=a \text{ şi } \sigma^{-1}(a)=a,\ \forall a\in K.$$

Prin urmare, $\sigma\circ\tau\in G(L\,|\,K)$ şi $\sigma^{-1}\in G(L\,|\,K)$. Deci, $G(L\,|\,K)$ este un subgrup al lui $Aut(L)$.

Grupul $G(L\,|\,K)$ definit de relaţia (1) poartă numele de ***grup Galois al extinderii*** $L\supseteq K$.

Exemple. 1°. Fie L un corp oarecare şi P subcorpul său prim ($P\simeq\mathbb{Q}$ sau $P\simeq\mathbb{Z}_p$ pentru un anumit p prim).

Dacă $\sigma\in Aut(L)$, atunci $\sigma(1)=1$. De aici, se deduce că $\sigma(a)=a$, $\forall a\in P$. Prin urmare, $G(L\,|\,P)=Aut(L)$.

2°. Să considerăm extinderea $\mathbb{C}\supseteq\mathbb{R}$ şi $\sigma\in G(\mathbb{C}\,|\,\mathbb{R})$. Pentru orice $a\in\mathbb{R}$, $\sigma(a)=a$. Dacă $z=a+bi\in\mathbb{C}$, atunci:

$$\sigma(z)=\sigma(a)+\sigma(i)\sigma(b)=a+\sigma(i)b$$

$$-1=\sigma(-1)=\sigma(i^2)=\sigma(i)^2.$$

Rezultă $\sigma(i)=\pm i$. Dacă $\sigma(i)=i$, atunci $\sigma=1_{\mathbb{C}}$.

Dacă $\sigma(i)=-i$, atunci, pentru orice $z=a+bi\in\mathbb{C}$,

$$\sigma(z)=\sigma(a+bi)=a-bi=\overline{z}$$

cu alte cuvinte, σ este aplicaţia de conjugare.

$G(\mathbb{C}\,|\,\mathbb{R})$ conţine două elemente şi este izomorf cu $(\mathbb{Z}_2,+)$.

Pentru extinderea de corpuri $L\supseteq K$, fixată, să notăm

$$G=G(L\,|\,K)$$

şi cu $\mathscr{L}(G)$ mulţimea subgrupurilor lui G. Relaţia "$\subseteq$" este o relaţie de ordine pe $\mathscr{L}(G)$. Mai mult, $\mathscr{L}(G)$ este o latice completă în raport cu relaţia "$\subseteq$". Pentru o familie oarecare $(H_i)_{i\in I}$ de subgrupuri ale lui G:

$$\inf(H_i)_{i\in I}=\bigcap_{i\in I}H_i,\ \sup(H_i)_{i\in I}=\left\langle\bigcup_{i\in I}H_i\right\rangle.$$

Pentru aceeaşi extindere $L\supseteq K$ notăm:

$$\mathscr{L}(L;K)=\{E\mid E \text{ subcorp al lui } L,\ E\supseteq K\}$$

mulţimea subcorpurilor intermediare între *L* şi *K*. Relaţia de incluziune este o relaţie de ordine pe $\mathscr{L}(L;K)$. Mai mult, $\mathscr{L}(L;K)$ este o latice completă în raport cu relaţia "$\subseteq$". Dacă $(E_i)_{i\in I}$ este o familie de corpuri intermediare, atunci:

$$\inf(E_i)_{i\in I}=\bigcap_{i\in I}E_i,\quad \sup(E_i)_{i\in I}=K\left(\bigcup_{i\in I}E_i\right).$$

În cazul $I=\{1,2\}$, $K(E_1\cup E_2)$ se mai notează simplu E_1E_2 şi se numeşte ***compozit al corpurilor*** E_1 şi E_2.

Între cele două latice definite mai sus se stabilesc, în mod natural, două aplicaţii.

Fie

(2) $$F:\mathscr{L}(G)\to\mathscr{L}(L;K)$$

definită prin:

(3) $$F(H)=\{\alpha\in L\mid\sigma(\alpha)=\alpha,\ \forall\sigma\in H\}.$$

Este clar că $F(H)\supseteq K$. Se foloseşte şi notaţia $F(H)=L^H$.

Dacă $\alpha,\beta\in L^H$ şi $\alpha\neq 0$, atunci, pentru orice $\sigma\in H$:

$$\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)=\alpha-\beta\Rightarrow\alpha-\beta\in F(H)$$
$$\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)=\alpha\beta\Rightarrow\alpha\beta\in F(H)$$
$$\sigma(\alpha^{-1})=\sigma(\alpha)^{-1}=\alpha^{-1}\Rightarrow\alpha^{-1}\in F(H).$$

Deci, $F(H)$ este un subcorp al lui *L* care include *K* şi aplicaţia *F* este bine definită. Ca aplicaţie între două mulţimi ordonate, *F* este antimonotonă, adică:

$$\forall H_1,H_2\in\mathscr{L}(G),\ H_1\subseteq H_2\Rightarrow F(H_1)\supseteq F(H_2).$$

A două aplicaţie este definită astfel:

(4) $$\Phi:\mathscr{L}(L;K)\to\mathscr{L}(G)$$

(5) $$\Phi(E)=G(L\mid E),\ \forall E\in\mathscr{L}(L;K).$$

Aplicația Φ este bine definită deoarece din $L \supseteq E \supseteq K$ rezultă:

$$G(L \mid E) \subseteq G(L \mid K).$$

În general, dacă $E_1, E_2 \in \mathscr{L}(L;K)$, atunci,

$$E_1 \subseteq E_2 \Rightarrow \Phi(E_1) \supseteq \Phi(E_2),$$

cu alte cuvinte, şi aplicația Φ este antimonotonă.

Ținând seama de definiții, rezultă:

$$G(L \mid L^H) \supseteq H, \quad \forall H \in \mathscr{L}(G)$$

$$L^{G(L|E)} \supseteq E, \quad \forall E \in \mathscr{L}(L;K).$$

sau

$$(\Phi \circ F)(H) \supseteq H, \quad \forall H \in \mathscr{L}(G) \tag{6}$$

$$(F \circ \Phi)(E) \supseteq E, \quad \forall E \in \mathscr{L}(L;K). \tag{7}$$

Aplicațiile F şi Φ definite de relațiile (2) – (5) poartă numele de ***corespondențe Galois***. În V.9. vom prezenta condiții în care cele două aplicații sunt una inversa celeilalte.

2. Endomorfismul lui Frobenius. Corpuri perfecte

Fie K un corp comutativ de caracteristică p. Definim aplicația:

$$u : K \to K, \ u(a) = a^p, \ \forall a \in K. \tag{1}$$

Dacă $a, b \in K$, atunci:

$$u(ab) = (ab)^p = a^p b^p = u(a)u(b),$$

$$u(a+b) = (a+b)^p = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p = a^p + b^p = u(a) + u(b).$$

Am ținut seama că p este număr prim şi $p \mid C_p^k$ pentru $k \in \overline{1, p-1}$.

Prin urmare, u este morfism (unitar) de corpuri.

Morfismul definit în relația (1) poartă numele de ***endomorfismul lui Frobenius***.

Deoarece u este endomorfism şi $u^k = \underbrace{u \circ u \circ ... \circ u}_{k \text{ factori}}$ este endomorfism.

Cum $u^k(a) = a^{p^k}$, $\forall a \in K$, din proprietatea de morfism rezultă că într-un corp de caracteristică p:

$$(a+b)^{p^k} = a^{p^k} + b^{p^k},\ \forall a,b \in K,\ \forall k \in \mathbb{N}.$$

Se ştie că orice corp K de caracteristică p conţine un subcorp izomorf cu $\mathbb{Z}_p$. Se poate presupune chiar că $\mathbb{Z}_p$ este subcorp al lui K. Conform micii teoreme a lui Fermat:

$$a^p = a,\ \forall a \in \mathbb{Z}_p \text{ sau } u(a) = a,\ \forall a \in \mathbb{Z}_p.$$

Reciproc, dacă $a \in K$ şi $u(a) = a$, atunci $a^p = a$, sau a este o rădăcină a polinomului $f = X^p - X \in K[X]$. Deoarece f nu poate avea mai mult de p rădăcini în K şi toate elementele lui $\mathbb{Z}_p$ sunt rădăcini ale lui f, rezultă $a \in \mathbb{Z}_p$.

Prin urmare, *subcorpul $\mathbb{Z}_p$ al lui K coincide cu mulţimea elementelor lui K invariate de endomorfismul lui Frobenius*.

Ca orice morfism de corpuri, u este injectiv. Prin urmare,

$$\forall a,b \in K,\ a^p = b^p \Rightarrow a = b.$$

2.1. **Definiţie.** *Fie K un corp comutativ. Se spune despre K că este* ***corp perfect*** *dacă, $carK = 0$ sau $carK = p \neq 0$ şi endomorfismul lui Frobenius este izomorfism*.

Toate corpurile de caracteristică zero sunt corpuri perfecte.

În cazul corpurilor finite, din injectivitatea lui u rezultă şi surjectivitatea lui u. Deci, *corpurile finite sunt perfecte*.

Fie K un corp algebric închis de caracteristică $p \neq 0$. Pentru orice $b \in K$, polinomul $f = X^p - b \in K[X]$ are rădăcinile în K. Există $a \in K$, astfel încât $f(a) = 0$ sau $u(a) = b$. Prin urmare, u este surjectiv. Deci, *corpurile algebric închise sunt corpuri perfecte*.

În plus, revenind la polinomul f, din $f(a) = 0$, rezultă $b = a^p$ deci $f = (X-a)^p$ şi astfel, f are o rădăcină multiplă de ordinul p.

2.2. **Propoziţie.** *Fie K un corp de caracteristică p care nu este corp perfect. Dacă $b \in K \setminus \mathrm{Im}\, u$, atunci polinomul $f = X^p - b$ este ireductibil în $K[X]$.*

Demonstraţie. Fie $\overline{K}$ închiderea algebrică a lui K şi $\alpha \in \overline{K}$ o rădăcină a lui f. Ca şi mai sus, rezultă $f = (X-\alpha)^p$. Deoarece $K[X]$

este inel factorial, f este produs de factori ireductibili. Putem presupune că aceşti factori ireductibili sunt unitari. Fiecare dintre aceşti factori este polinom minimal al lui α. Notând cu s numărul factorilor, $f = p_\alpha^{\,s}$. Rezultă $p = d^\circ f = s \cdot d^\circ p_\alpha$. Cum p este număr prim, rezultă $s = p$ sau $s = 1$. Dacă $s = p$, atunci $p_\alpha = X - \alpha \in K[X]$, deci $b = \alpha^p \in \operatorname{Im} u$, contradicție.

Rezultă, $s = 1$ şi $f = p_\alpha$ este ireductibil în $K[X]$. □

3. Rădăcini primitive ale unității

Fie K un corp comutativ. Vom începe cu o proprietate pe care o au subgrupurile finite ale lui K^*.

3.1. **Propoziție.** *Fie K un corp comutativ şi G un subgrup finit al lui* $(K^*, \cdot)$. *Atunci, G este ciclic.*

Demonstrație. Fie $n = |G|$ şi $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ descompunerea în factori primi a lui n ($p_i \neq p_j$ pentru $i \neq j$). Este suficient să arătăm că în subgrupul G există un element de ordin n.

Fie $i \in \overline{1,r}$, o valoare fixată. Polinomul $f = X^{\frac{n}{p_i}} - 1 \in K[X]$ are cel mult $\dfrac{n}{p_i}$ rădăcini în K. Rezultă că există $x_i \in G$, astfel încât $x_i^{\frac{n}{p_i}} \neq 1$. Notăm $y_i = x_i^{\frac{n}{p_i^{\alpha_i}}}$.

Vom arăta că elementul y_i are ordinul $p_i^{\alpha_i}$.

Din $y_i^{p_i^{\alpha_i}} = x_i^{\,n} = x_i^{|G|} = 1$, obținem $ordy_i \mid p_i^{\alpha_i}$. Deci, $ordy_i = p_i^{\,k}$, $k \leq \alpha_i$. Dacă $k < \alpha_i$, atunci $x_i^{\frac{n}{p_i}} = \left(y_i^{p_i^k}\right)^{p_i^{\alpha_i - 1 - k}} = 1$, contradicție cu alegerea lui x_i. Deci, $k = \alpha_i$ şi $ordy_i = p_i^{\alpha_i}$.

Cu elementele $y_1, \ldots, y_r$ determinate ca mai sus, notăm $y = y_1 \ldots y_r$. Deoarece G este grup comutativ şi $\left(ordy_i, ordy_j\right) = 1$, pentru $i \neq j$, $ordy = ordy_1 \cdot \ldots \cdot ordy_r = n$. Rezultă $G = (y)$. □

Fie în continuare K un corp comutativ algebric închis şi $n \in \mathbb{N}^*$.

În cazul $carK = p \neq 0$, presupunem în plus, $p \nmid n$.

Polinomul $f = X^n - 1$ are în K exact n rădăcini. În ipoteza făcută, $f' = nX^{n-1}$ are în K numai rădăcina 0. Polinoamele f şi f' nu au rădăcini comune şi ca urmare, f are numai rădăcini simple. Notăm

(1) $$U_n = \left\{ \alpha \in K \middle| \alpha^n = 1 \right\}.$$

U_n, fiind mulțimea rădăcinilor lui f în K, are exact n elemente.

Dacă $\alpha, \beta \in U_n$, atunci $(\alpha\beta)^n = \alpha^n \beta^n = 1$ şi $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1$, adică $\alpha\beta \in U_n$, $\alpha^{-1} \in U_n$.

Prin urmare, U_n este un subgrup al lui $(K^*, \cdot)$.

U_n poartă numele de ***grup multiplicativ al rădăcinilor de grad n ale unității***, din corpul algebric închis K.

Conform 3.1., U_n este grup ciclic.

Un generator ξ al grupului U_n poartă numele de ***rădăcină primitivă de gradul n a unității***.

$$U_n = \left\{ 1, \xi, \xi^2, ..., \xi^{n-1} \right\}.$$

Din proprietățile grupurilor finite se ştie că elementul ξ^k este şi el un generator al grupului U_n dacă şi numai dacă $(n,k) = 1$.

Prin urmare, există exact $\varphi(n)$ rădăcini primitive de grad n ale unității, unde funcția φ este indicatorul lui Euler.

Vom considera în continuare, în locul lui K, corpul $\mathbb{C}$ al numerelor complexe. U_n poartă în acest caz numele de ***grup multiplicativ al rădăcinilor complexe de grad n ale unității***.

$$U_n = \left\{ \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \middle| k \in \overline{0, n-1} \right\}.$$

O rădăcină primitivă de grad n a unității este, în acest caz,

$$\xi = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Mai sunt rădăcini primitive de grad *n* ale unității, toate puterile ξ^k cu $(n,k)=1$.

Dacă ξ este o rădăcină complexă, primitivă de grad *n* a unității, atunci $\mathbb{Q}(\xi)$ poartă numele de ***al n – lea corp ciclotomic***. Denumirea provine de la faptul că imaginile geometrice ale elementelor lui U_n taie cercul unitate din planul complex în *n* părți egale.

Rădăcinile unității sunt numere algebrice. Putem vorbi despre polinomul lor minimal.

3.2. **Teoremă.** *Fie ξ o rădăcină primitivă complexă de grad n a unității şi f polinomul minimal al lui ξ peste $\mathbb{Q}$. Atunci*:

a) $f \in \mathbb{Z}[X]$;

b) *Dacă* $f(\eta)=0$, *atunci* η *este rădăcină primitivă de grad n a unității*;

c) *Dacă* η *este o rădăcină primitivă de grad n a unității*, *atunci* $f(\eta)=0$;

d) $d^\circ f = \varphi(n)$;

e) $\left[\mathbb{Q}(\xi):\mathbb{Q}\right]=\varphi(n)$.

Demonstrație. a) ξ este o rădăcină a polinomului $X^n-1\in\mathbb{Z}[X]$. Prin urmare, $f \mid X^n-1$. Deoarece $\mathbb{Z}[X]$ este inel factorial, X^n-1 se descompune în $\mathbb{Z}[X]$ în produs de factori ireductibili. Putem presupune că toți aceşti factori sunt unitari. Datorită unicității descompunerii în factori, *f* coincide cu unul din factori.

b) Dacă η este o altă rădăcină a lui *f*, atunci conform III.7.4., există un izomorfism $\mathbb{Q}(\xi)\to\mathbb{Q}(\eta)$ care invariază elementele lui $\mathbb{Q}$ şi duce ξ în η. În particular, $\xi^m=1\Leftrightarrow\eta^m=1,\ m\in\mathbb{N}$.

Rezultă $ord\,\xi = ord\,\eta = n$, deci η este rădăcină primitivă de grad *n* a unității.

c) Fie η altă rădăcină primitivă de grad *n* a unității şi *g* polinomul minimal al lui η peste $\mathbb{Q}$. Trebuie demonstrat că $f=g$.

Deoarece *f* şi *g* sunt polinoame ireductibile unitare, este suficient să demonstrăm că $(f,g)\neq 1$. Presupunem, prin reducere la absurd,

că $(f,g)\sim 1$. Din $f \mid X^n-1$ şi $g \mid X^n-1$, rezultă că există h, polinom din $\mathbb{Z}[X]$, astfel încât

(2) $$X^n-1=fgh.$$

Deoarece η este rădăcină primitivă de grad n a unității, există k, $1\le k\le n-1$, $(k,n)=1$, astfel încât $\eta=\xi^k$.

Repetând eventual raționamentul, este suficient să tratăm cazul $\eta=\xi^p$ unde p este număr prim şi $p\nmid n$.

Fie $g_p=g(X^p)$. Din $g_p(\xi)=g(\eta)=0$, rezultă că $f \mid g_p$. Deci există $f_1\in\mathbb{Z}[X]$, astfel încât $g_p=ff_1$. Fie $\pi:\mathbb{Z}\to\mathbb{Z}_p$ surjecția canonică şi $\overline{\pi}:\mathbb{Z}[X]\to\mathbb{Z}_p[X]$ unicul morfism de inele care extinde π cu proprietatea că $\overline{\pi}(X)=X$. Pentru un polinom oarecare $t\in\mathbb{Z}[X]$, notăm $\bar{t}=\overline{\pi}(t)$. Din relațiile de mai sus, rezultă:

$$X^n-\hat{1}=\overline{f}\cdot\overline{g}\cdot\overline{h} \text{ şi } \overline{g_p}=\overline{f}\cdot\overline{f_1}.$$

Datorită teoremei lui Fermat, $a^p=a$, $\forall a\in\mathbb{Z}_p$ şi

$$\overline{g_p}=\overline{g(X^p)}=\overline{g}^p=\overline{f}\cdot\overline{f_1}.$$

Rezultă că $\overline{f}$ şi $\overline{g}$ au rădăcini comune, deci $X^n-\hat{1}$ are rădăcini multiple. Dar, $\left(X^n-\hat{1}\right)'=n\cdot\hat{1}\cdot X^{n-1}$ are numai rădăcina 0 care nu este şi rădăcină pentru $X^n-\hat{1}$. Am obținut o contradicție. Ipoteza făcută, $(f,g)\sim 1$ este falsă. Prin urmare, $f=g$.

d) Conform b) şi c), gradul lui f este egal cu numărul rădăcinilor primitive de grad n ale unității, deci $d^\circ f=\varphi(n)$.

e) $\left[\mathbb{Q}(\xi):\mathbb{Q}\right]=d^\circ f=\varphi(n)$. □

3.3. **Definiție.** *Polinomul minimal al unei rădăcini primitive de grad n a unității se numeşte* ***al n – lea polinom ciclotomic*** *şi se notează cu* F_n.

Deoarece $U_1=\{1\}$, $F_1=X-1$.

Deoarece $U_2 = \{-1,1\}$ şi -1 este rădăcină primitivă de gradul doi a unității, $F_2 = X + 1$.

Deoarece $U_3 = \{1, \varepsilon, \varepsilon^2\}$, unde $\varepsilon^2 + \varepsilon + 1 = 0$, $\varepsilon \in \mathbb{C}$ şi ε este o rădăcină primitivă de gradul 3 a unității, $F_3 = X^2 + X + 1$.

3.4. **Consecință.** *Fie* $n \in \mathbb{N}^*$. *Atunci*:

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

(*în ultima egalitate, ca şi în continuare, considerăm numai divizorii pozitivi*).

Demonstrație. Dacă $d \mid n$, atunci $F_d \mid X^n - 1$. Dacă d_1 şi d_2 sunt doi divizori distincți ai lui *n*, atunci F_{d_1} şi F_{d_2} nu au rădăcini comune, deci $\left(F_{d_1}, F_{d_2}\right) \sim 1$. Rezultă $\prod_{d|n} F_d \mid X^n - 1$. Reciproc, fie *f* un factor ireductibil în $\mathbb{Z}[X]$, unitar, al lui $X^n - 1$ şi α o rădăcină a lui *f*. Din $\alpha^n = 1$ rezultă $ord\,\alpha = d \mid n$. α este o rădăcină primitivă de grad *d* a unității şi $f = F_d$. Rezultă $X^n - 1 = \prod_{d|n} F_d$. □

3.5. **Consecință.** *Fie* $n \in \mathbb{N}^*$. *Atunci*:

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

Demonstrație. Din (3), rezultă $n = \sum_{d|n} d^\circ F_d = \sum_{d|n} \varphi(d)$. □

4. Corpuri finite

Structura de corp finit are o serie de proprietăți remarcabile.

4.1. **Propoziție.** *Fie L un corp finit şi K un subcorp al său. Atunci:*

$$|L| = |K|^{[L:K]}.$$

Demonstrație. Deoarece *L* este corp finit, *K* este corp finit şi extinderea $L \supseteq K$ este finită. Fie $[L:K] = n$ şi $(e_1, ..., e_n)$ o bază în ${}_K L$. Pentru $y \in L$, există şi sunt unici $c_1, ..., c_n \in K$ astfel încât

$$y = \sum_{i=1}^{n} c_i e_i .$$

Rezultă că aplicația:

$$K^n \to L,\ (c_1,...,c_n) \to \sum_{i=1}^{n} c_i e_i$$

este o bijecție. Deci, $|L| = |K^n| = |K|^n = |K|^{[L:K]}$. □

4.2. **Consecință.** *Fie K un corp finit. Există un număr prim p şi* $n \in \mathbb{N}^*$, *astfel încât*

$$|K| = p^n .$$

Demonstrație. Fie $p = carK$. Deoarece *K* este corp finit, *p* este număr prim şi $K \supseteq \mathbb{Z}_p$. Fie $n = [K : \mathbb{Z}_p]$. Din 4.1., rezultă:

$$|K| = |\mathbb{Z}_p|^n = p^n . \quad \square$$

Consecința 4.2. este o proprietate de cardinalitate a corpurilor finite. Nu pentru orice număr *m* poate exista un corp cu *m* elemente. Dacă există un astfel de corp, atunci, obligatoriu *m* este de forma p^n cu *p* prim şi $n \in \mathbb{N}^*$. Vom vedea în continuare că relația $m = p^n$ este şi o condiție suficientă de existență a unui corp finit cu *m* elemente.

4.3. **Teorema lui Weddeburn.** *Orice corp finit este comutativ.*

Demonstrație. Fie *K* un corp finit. Notăm

$$C = \{a \in K \mid ax = xa, \forall x \in K\}.$$

C este subcorp al lui *K*, numit ***centrul*** lui *K*.

Dacă $p = carK$, atunci *C* include subcorpul prim $\mathbb{Z}_p$ al lui *K*.

Corpul *K* este comutativ dacă şi numai dacă $C = K$.

Fie $[K : C] = n$. Să presupunem că $n > 1$. Aplicăm ecuația claselor pentru grupul $(K^*, \cdot)$ unde $K^* = K \setminus \{0\}$:

$$|K^*| = |C^*| + \sum_{a \in S} (K^* : C(a)^*) \qquad (4)$$

unde *S* este un sistem de reprezentanți ai claselor de elemente conjugate care nu aparțin centrului (peste tot * înseamnă excluderea ele-

mentului 0) iar $C(a)=\{y\in K \mid ay=ya\}$. $C(a)$ este de asemenea un subcorp al lui K, $C(a)\supseteq C$ şi $C(a)\neq K$ pentru $a\notin C$.

Notăm $[C(a):C]=d(a)$. Din $C\subseteq C(a)\subseteq K$ rezultă $d(a)\mid n$. Pentru $a\notin C$, $d(a)<n$. Fie $q=|C|$. Din 4.1., rezultă

$$|K|=q^n,\quad |C(a)|=q^{d(a)}.$$

$$(K^*:C(a)^*)=\frac{|K^*|}{|C(a)^*|}=\frac{q^n-1}{q^{d(a)}-1}>1,\ \text{pentru } a\notin C.$$

Din (4) rezultă:

$$q^n-1=q-1+\sum_{a\in S}\frac{q^n-1}{q^{d(a)}-1}. \tag{5}$$

Dacă F_n este al n – lea polinom ciclotomic, atunci din $F_n \mid X^n-1$ în $\mathbb{Z}[X]$, rezultă

$$F_n(q)\mid q^n-1. \tag{6}$$

Dacă $d(a)<n$, atunci $X^{d(a)}-1$ şi F_n nu au rădăcini comune, deci $\left(X^{d(a)}-1,F_n\right)\sim 1$. Rezultă $F_n \mid \frac{X^n-1}{X^{d(a)}-1}$ în $\mathbb{Z}[X]$ şi

$$F_n(q)\mid \frac{q^n-1}{q^{d(a)}-1}. \tag{7}$$

Din (5), (6) şi (7), rezultă $F_n(q)\mid q-1$.

Vom arăta că ultima relaţie nu este posibilă.

Dacă $n=2$, atunci $F_2=X+1$, $F_2(q)=q+1 \nmid q-1$.

Dacă $n>2$ şi ξ este o rădăcină a lui F_n, atunci $\xi=a+bi$, $a\in\mathbb{R}$, $b\in\mathbb{R}^*$. În plus, $|\xi|=\sqrt{a^2+b^2}=1$, deci $|a|<1$.

$$|q-\xi|=|q-a-bi|=\sqrt{q^2-2aq+1}>q-1.$$

$$F_n=\prod_{\xi}(X-\xi). \tag{8}$$

În (8) ξ parcurge rădăcinile primitive de grad n ale unităţii.

$$\left|F_n(q)\right| = \prod_{\xi} \left|q - \xi\right| > q - 1.$$

Deci $F_n(q) \nmid q - 1$. Ipoteza $n > 1$ ne-a condus la o contradicție. Rezultă $n = 1$, $K = C$ şi K corp comutativ. □

4.4. **Consecință.** *Două corpuri finite cu acelaşi număr de elemente sunt izomorfe.*

Demonstrație. Fie K un corp finit. Conform teoremei 4.3., K este corp comutativ. Fie $n = \left|K\right|$. $(K^*, \cdot)$ este grup cu $n - 1$ elemente.

Pentru orice $x \in K^*$, $x^{n-1} = 1$.

Rezultă că toate elementele lui K sunt rădăcini ale polinomului $f = X^n - X \in \mathbb{Z}_p[X]$ unde $p = carK$.

Prin urmare, K este corp de descompunere pentru f. Acum 4.4. rezultă din III.7.6. □

Consecință 4.4. este o proprietate de unicitate a corpurilor finite.

4.5. **Consecință.** *Fie K un corp finit. Atunci grupul $(K^*, \cdot)$ este grup ciclic.*

Demonstrație. Conform teoremei lui Wedderburn, K este corp comutativ, deci $(K^*, \cdot)$ este grup abelian. Din 3.1., rezultă că grupul menționat este grup ciclic. □

4.6. **Teoremă.** *Pentru orice număr prim p şi orice $n \in \mathbb{N}^*$, există un corp cu p^n elemente.*

Demonstrație. Fie p un număr prim şi L o închidere algebrică a lui $\mathbb{Z}_p$. Polinomul $f = X^{p^n} - X \in \mathbb{Z}_p[X]$ are toate rădăcinile în L. Deoarece $f' = -1$, rădăcinile lui f sunt distincte. Fie

$$K = \left\{\alpha \in L \middle| f(\alpha) = 0\right\}.$$

K are p^n elemente. Pentru $\alpha \in L$:

$$\alpha \in K \Leftrightarrow u^n(\alpha) = \alpha$$

unde $u : L \to L$ este endomorfismul lui Frobenius.

Dacă $\alpha, \beta \in K$, atunci: $u^n(\alpha) = \alpha$, $u^n(\beta) = \beta$.

$u^n(\alpha + \beta) = u^n(\alpha) + u^n(\beta) = \alpha + \beta$, $u^n(-\alpha) = -u^n(\alpha) = -\alpha$,

$u^n(\alpha\beta) = u^n(\alpha)u^n(\beta) = \alpha\beta,\ \ u^n(\alpha^{-1}) = u^n(\alpha)^{-1} = \alpha^{-1},\ \ \alpha \neq 0.$

Prin urmare, K este un subcorp al lui L şi $|K| = p^n$. □

4.7. **Consecinţă.** *Fie K un corp finit cu p^n elemente, $p = carK$. Atunci K are un subcorp cu p^d elemente, dacă şi numai dacă $d \mid n$* ($n, d \in \mathbb{N}^*$).

Demonstraţie. Să presupunem că există un subcorp K_1 al lui K cu p^d elemente. Din $\mathbb{Z}_p \subseteq K_1 \subseteq K,\ \ [K_1 : \mathbb{Z}_p] = d,\ \ [K : \mathbb{Z}_p] = n$ şi din proprietatea de tranzitivitate a extinderilor finite, rezultă $d \mid n$.

Reciproc, fie $d \in \mathbb{N}^*$ un divizor al lui n. Fie L o închidere algebrică a lui K. Conform teoremei 4.6., există un subcorp K_1 al lui L cu p^d elemente şi

$$K_1 = \left\{\alpha \in L \middle| u^d(\alpha) = \alpha\right\},\ \ K = \left\{\alpha \in L \middle| u^n(\alpha) = \alpha\right\}.$$

Din $d \mid n$ rezultă $K_1 \subseteq K$. □

5. Problema rădăcinilor multiple ale unui polinom ireductibil

Fie K un corp comutativ şi $f \in K[X]$, un polinom ireductibil. Vom cerceta în ce condiţii f poate avea rădăcini multiple.

Conform propoziţiei III.6.8., f are rădăcini multiple (într-o extindere a lui K), dacă şi numai dacă $(f, f') \neq 1$. Deoarece f este ireductibil, aceasta revine la $f \mid f'$. Deoarece $d^\circ f > d^\circ f'$, rezultă $f' = 0$.

Fie $f = \sum_{i=0}^{n} a_i X^i,\ \ n \geq 1,\ \ f' = \sum_{i=1}^{n} i a_i X^{i-1}$.

$$f' = 0 \Leftrightarrow ia_i = 0,\ i \in \overline{1,n} \Leftrightarrow \left(i \cdot 1 = 0 \text{ sau } a_i = 0\right),\ i \in \overline{1,n}.$$

Distingem două cazuri.

I. *Corpul K are caracteristica zero*: $carK = 0$.

În acest caz, $i \cdot 1 = 0 \Rightarrow i = 0$. Condiţia $f' = 0$ implică $f = a_0 \in K^*$, deci f inversabil, contradicţie cu f ireductibil în $K[X]$. Prin urmare, f nu poate avea rădăcini multiple.

II. *Corpul K are caracteristică nenulă*: $carK = p \neq 0$ (Se ştie că *p* este număr prim).

În acest caz, $i \cdot 1 = 0 \Rightarrow p \mid i$. Deci, dacă $p \nmid i$, atunci $a_i = 0$ şi

$$f = a_0 + a_p X^p + a_{2p} X^{2p} + ... + a_{kp} X^{kp} \in K[X^p].$$

Putem formula:

5.1. **Teoremă.** *Fie K un corp comutativ şi* $f \in K[X]$, *un polinom ireductibil. Pentru* $carK = 0$, *polinomul f nu are rădăcini multiple. Pentru* $carK = p \neq 0$, f *are rădăcini multiple dacă şi numai dacă* $f \in K[X^p]$.

Să considerăm în continuare $carK = p \neq 0$ şi $f \in K[X^p]$.

Fie $r \in \mathbb{N}^*$, astfel încât $f \in K[X^{p^r}]$ şi $f \notin K[X^{p^{r+1}}]$. Există atunci $h \in K[X]$, astfel încât $f = h(X^{p^r})$. Deoarece *f* este ireductibil, *h* este ireductibil. Afirmăm că *h* nu are rădăcini multiple. Altfel, $h \in K[X^p]$ şi $f \in K[X^{p^{r+1}}]$, contradicție.

Fie $d^\circ h = m$ şi *L* o extindere a lui *K* în care *h* are toate rădăcinile $\beta_1, ..., \beta_m$ (distincte).

$$h = \prod_{i=1}^{m} (X - \beta_i), \quad f = \prod_{i=1}^{m} (X^{p^r} - \beta_i).$$

Fie L' o extindere a corpului *L* în care fiecare polinom $X^{p^r} - \beta_i$ are o rădăcină α_i, $i \in \overline{1,m}$. Deoarece $\beta_1, ..., \beta_m$ sunt distincte, rădăcinile $\alpha_1, ..., \alpha_m$ sunt distincte.

Cum $\alpha_i^{p^r} = \beta_i$, rezultă $X^{p^r} - \beta_i = X^{p^r} - \alpha_i^{p^r} = (X - \alpha_i)^{p^r}$, adică:

$$f = \prod_{i=1}^{m} (X - \alpha_i)^{p^r}. \tag{1}$$

5.2. **Teoremă.** *Dacă* $f \in K[X]$ *este polinom ireductibil, atunci toate rădăcinile lui f au acelaşi ordin de multiplicitate.*

Demonstrație. În cazul $carK = 0$, toate rădăcinile lui *f* sunt simple. În cazul $carK = p \neq 0$, afirmația rezultă din (1). □

Cu notațiile din (1), *m* poartă numele de ***grad redus*** al polinomului *f* şi *r* poartă numele de ***exponent*** al polinomului *f* sau al rădăcinilor lui *f*. Dacă *r* este exponentul polinomului ireductibil *f*, atunci toate rădăcinile lui *f* au ordinul de multiplicitate egal cu p^r. Gradul redus al unui polinom ireductibil este egal cu numărul rădăcinilor distincte ale polinomului.

Gradul *n* al polinomului ireductibil *f*, gradul redus *m* şi exponentul *r* sunt legați prin relația:

$$n = mp^r .$$

5.3. **Definiție.** *Fie K un corp comutativ şi* $f \in K[X]$ *un polinom ireductibil. Se spune că f este* ***separabil*** *dacă toate rădăcinile lui f sunt simple. În caz contrar, se spune că polinomul f este* ***neseparabil****.*

Din teorema 5.1., rezultă că, în cazul $carK = 0$, toate polinoamele ireductibile din $K[X]$ sunt separabile.

În cazul $carK = p \neq 0$, polinomul ireductibil *f* este neseparabil dacă şi numai dacă $f \in K[X^p]$.

6. Extinderi algebrice separabile

6.1. **Definiție.** *Fie* $L \supseteq K$ *o extindere de corpuri şi* $\alpha \in L$ *un element algebric peste K. Se spune că* α *este* ***separabil*** *peste K dacă polinomul său minimal* $p_\alpha \in K[X]$ *este separabil. În caz contrar, se spune că* α *este* ***neseparabil*** *peste K.*

Din teorema 5.1. şi din definiția 5.3., rezultă că toate elementele algebrice peste un corp *K* de caracteristică 0 sunt separabile. În cazul $carK = p \neq 0$, elementul α, algebric peste corpul *K*, este neseparabil peste *K* dacă şi numai dacă $p_\alpha \in K[X^p]$.

6.2. **Definiție.** *Fie* $L \supseteq K$ *o extindere algebrică de corpuri. Se spune că extinderea* $L \supseteq K$ *este* ***separabilă*** *dacă toate elementele lui L sunt separabile peste K. În caz contrar, se spune că* $L \supseteq K$ *este o extindere* ***neseparabilă****.*

Din comentariile de mai sus, rezultă că orice extindere algebrică a unui corp de caracteristică 0 este şi o extindere separabilă.

Noțiunea de extindere separabilă este legată de noțiunea de corp perfect.

6.3. **Propoziție.** *Corpul K este perfect dacă şi numai dacă orice element algebric peste K este separabil peste K.*

Demonstrație. Afirmația este evidentă în cazul $carK = 0$.

Fie K un corp perfect de caracteristică $p \neq 0$ şi $\alpha \in L \supseteq K$ un element algebric. Să presupunem că α este neseparabil peste K. Rezultă că polinomul său minimal $p_\alpha \in K[X^p]$:

$$p_\alpha = \sum_{k=0}^{r} b_k X^{kp}, \ b_r = 1.$$

Deoarece K este corp perfect, pentru orice $k \in \overline{0,r}$, există $a_k \in K$ astfel încât $b_k = u(a_k) = a_k{}^p$ (u fiind endomorfismul lui Frobenius).

$$p_\alpha = \sum_{k=0}^{r} a_k{}^p X^{kp} = \left(\sum_{k=0}^{r} a_k X^k \right)^p,$$

contradicție cu faptul că p_α este ireductibil peste K.

Fie acum K un corp care nu este perfect. Rezultă că endomorfismul lui Frobenius nu este surjectiv. Atunci, există $b \in K$, astfel încât, $u(a) \neq b, \ \forall a \in K$.

Conform propoziției 2.2., polinomul $f = X^p - b$ este ireductibil în $K[X]$. Fie $\overline{K}$ închiderea algebrică a lui K şi $\alpha \in \overline{K}$ o rădăcină a lui f. Atunci, f este polinomul minimal al lui α peste K şi $f = (X - \alpha)^p$. Deci, α este neseparabil peste K. □

6.4. **Consecință.** *Orice extindere algebrică a unui corp finit este extindere separabilă.*

Demonstrație. Rezultă din faptul că orice corp finit este perfect şi din 6.3. □

6.5. **Propoziție.** *Fie $L \supseteq K$ o extindere algebrică separabilă şi $E \in \mathscr{L}(L;K)$. Atunci, $L \supseteq E$ este extindere separabilă.*

Demonstrație. Fie $\alpha \in L$ şi $p_\alpha \in K[X]$, polinomul minimal al lui α peste K. Deoarece α este separabil peste K, p_α are numai rădăcini simple. Fie $f_\alpha \in E[X]$, polinomul minimal al lui α peste E. Din

$f_\alpha \mid p_\alpha$, rezultă că f_α are numai rădăcini simple. Deci α este separabil peste *E*. Cum $\alpha \in L$ este arbitrar, extinderea $L \supseteq E$ este separabilă. □

Reamintim că se spune că extinderea $L \supseteq K$ este ***simplă*** dacă există $\alpha \in L$, astfel încât, $L = K(\alpha)$. Elementul α din această relație poartă numele de ***element primitiv*** al extinderii.

6.6. **Teoremă** (**a elementului primitiv**). *Orice extindere finită şi separabilă este simplă.*

Demonstrație. Fie $L \supseteq K$ o extindere finită şi separabilă.

În cazul *K* corp finit, din $|L| = |K|^{[L:K]}$, rezultă că şi *L* este finit. Conform 3.1., $(L^*, \cdot)$ este grup ciclic. Dacă *x* este un element generator al lui L^*, atunci $L = K(x)$.

Rămâne să tratăm cazul *K* corp infinit.

Fie $[L:K] = \dim_K L = n$ şi $(e_1, ..., e_n)$ o bază în ${}_K L$. Rezultă că are loc egalitatea:

$$L = K(e_1, ..., e_n).$$

Raționând prin inducție după *n*, este suficient să demonstrăm că dacă $\alpha, \beta \in L$, atunci există $\gamma \in L$, astfel încât:

$$K(\alpha, \beta) = K(\gamma).$$

Fie p_α şi p_β polinoamele minimale ale lui α, respectiv β, peste *K*. Considerăm $\overline{K}$, o închidere algebrică a lui *K*, astfel încât $\overline{K} \supseteq L$.

Fie $\alpha_1 = \alpha, \alpha_2, ..., \alpha_r \in \overline{K}$, rădăcinile lui p_α. Deoarece α este separabil peste *K*, $\alpha_1, \alpha_2, ..., \alpha_r$ sunt distincte.

Fie $\beta_1 = \beta, \beta_2, ..., \beta_s \in \overline{K}$, rădăcinile lui p_β. Deoarece β este separabil peste *K*, $\beta_1, \beta_2, ..., \beta_s$ sunt distincte.

Fiecare ecuație de forma:

(1) $$\alpha + x\beta = \alpha_i + x\beta_j, \quad i \in \overline{1,r}, \quad j \in \overline{2,s}$$

are cel mult o rădăcină în *K*.

Deoarece *K* este infinit, există $c \in K$, care nu este rădăcină a niciunei ecuații de forma (1). Fie

$$\gamma = \alpha + c\beta \text{ şi } f = p_\alpha(\gamma - cX) \in K(\gamma)[X].$$

Din $f(\beta) = p_\alpha(\gamma - c\beta) = p_\alpha(\alpha) = 0$, rezultă că f şi p_β au rădăcina comună β. Arătăm că β este singura rădăcină comună. Într-adevăr, fie β_j una dintre rădăcinile lui p_β, astfel încât:

$$f(\beta_j) = p_\alpha(\gamma - c\beta_j) = 0.$$

Există $i \in \overline{1,r}$, astfel încât $\gamma - c\beta_j = \alpha_i$, sau $\gamma = \alpha + c\beta = \alpha_i + c\beta_j$.
Conform alegerii lui c, rezultă $i = j = 1$ şi $\beta_j = \beta$.

Deducem:

$$(p_\beta, f) \sim X - \beta.$$

Din $f, p_\beta \in K(\gamma)[X]$, rezultă că $\beta \in K(\gamma)$. Deoarece $\alpha = \gamma - c\beta$, $\alpha \in K(\gamma)$. Prin urmare, $K(\alpha, \beta) \subseteq K(\gamma)$.
Cum incluziunea inversă este evidentă, $K(\alpha, \beta) = K(\gamma)$. □

7. Elemente conjugate

7.1. **Definiție.** *Fie $L \supseteq K$ o extindere de corpuri şi $\alpha, \beta \in L$, elemente algebrice peste K. Se spune că α şi β sunt **conjugate** peste K dacă au acelaşi polinom minimal peste K*:

$$p_\alpha = p_\beta.$$

În extinderea $\mathbb{C} \supseteq \mathbb{R}$, elementele $1+i$ şi $1-i$ sunt conjugate. Polinomul lor minimal peste $\mathbb{R}$ este $X^2 - 2X + 2$.

În extinderea $\mathbb{C} \supseteq \mathbb{Q}$, elementele $\sqrt[3]{2}, \sqrt[3]{2}\varepsilon$ şi $\sqrt[3]{2}\varepsilon^2$ sunt conjugate peste $\mathbb{Q}$ ($\varepsilon \in \mathbb{C}$ şi $\varepsilon^2 + \varepsilon + 1 = 0$), deoarece polinomul lor minimal peste $\mathbb{Q}$ este $X^3 - 2$.

7.2. **Consecință.** *Fie K un corp comutativ şi $\overline{K}$, o închidere algebrică a lui K. Fie $\alpha \in \overline{K}$. Numărul conjugaților în $\overline{K}$ ai lui α (peste K) este egal cu numărul rădăcinilor distincte ale polinomului minimal p_α. În cazul $carK = 0$, acest număr este egal cu $d^\circ p_\alpha$. În cazul $carK = p \neq 0$, acest număr este egal cu gradul redus al lui p_α.*

Demonstrație. A se vedea paragraful 5. □

Vom arăta în continuare că elementele conjugate sunt legate de automorfismele din grupul Galois.

7.3. **Teoremă.** *Fie K un corp comutativ şi* $\overline{K}$ *o închidere algebrică a lui K. Fie* $\alpha \in \overline{K}$. *Numărul conjugaților în* $\overline{K}$ *ai lui* α *(peste K) este egal cu numărul morfismelor de corpuri*

(2) $$\sigma : K(\alpha) \to \overline{K},$$

cu proprietatea $\sigma(a) = a, \ \forall a \in K$.

Demonstrație. Fie $p_\alpha = \sum_{i=0}^{n} a_i X^i \in K[X]$, polinomul minimal al lui α. Fie A mulțimea morfismelor de forma (2) şi B mulțimea conjugaților lui α în $\overline{K}$. Fie $\sigma \in A$.

$$0 = \sigma\left(p_\alpha(\alpha)\right) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = p_\alpha\left(\sigma(\alpha)\right).$$

Prin urmare, $\sigma(\alpha)$ este un conjugat al lui α, $\sigma(\alpha) \in B$.

Definim aplicația:

$$F : A \to B, \ \ F(\sigma) = \sigma(\alpha), \ \ \forall \sigma \in A.$$

Dacă $\sigma, \tau \in A$ şi $F(\sigma) = F(\tau)$, atunci $\sigma(\alpha) = \tau(\alpha)$. Deoarece pentru orice $a \in K$, $\sigma(a) = \tau(a) = a$, rezultă $\sigma = \tau$. Deci F este injectivă. Fie $\beta \in B$. Din III.7.4., rezultă că există un izomorfism

$$v : K(\alpha) \to K(\beta)$$

astfel încât $v(a) = a, \ \forall a \in K$ şi $v(\alpha) = \beta$.

Dacă $j : K(\beta) \to \overline{K}$ este morfismul incluziune, atunci $\sigma = j \circ v \in A$ şi $F(\sigma) = \beta$. Deci F este bijectivă şi $|A| = |B|$. □

7.4. **Consecință.** *Fie K un corp comutativ şi* $\overline{K}$ *închiderea sa algebrică. Elementele* $\alpha, \beta \in \overline{K}$ *sunt conjugate peste K, dacă şi numai dacă există* $\sigma \in G\left(\overline{K} \mid K\right)$, $\sigma(\alpha) = \beta$.

Demonstrație. Dacă α şi β sunt conjugate peste K, atunci, conform 7.3., există un morfism de corpuri $\sigma : K(\alpha) \to \overline{K}$, astfel încât

$\sigma(\alpha)=\beta$. Conform III.9.5., există un morfism $\tau:\overline{K}\to\overline{K}$ care prelungeşte σ, $\tau\in G\left(\overline{K}\mid K\right)$ şi $\tau(\alpha)=\sigma(\alpha)=\beta$.

Reciproc, dacă $\sigma(\alpha)=\beta$, unde $\sigma\in G\left(\overline{K}\mid K\right)$, atunci, urmând calculul din demonstraţia lui 7.3., rezultă:

$$p_\alpha(\beta)=\sigma\left(p_\alpha(\alpha)\right)=\sigma(0)=0.$$

Deci, β este un conjugat al lui α. □

8. Extinderi algebrice normale

8.1. **Definiţie.** *Fie* $L\supseteq K$ *o extindere algebrică de corpuri, unde* $L\subseteq\overline{K}$. *Se spune că* $L\supseteq K$ *este o* ***extindere normală*** *dacă din* $\alpha\in L$ *şi* $\beta\in\overline{K}$, β *conjugat cu* α *peste K, rezultă* $\beta\in L$.

Deci, o extindere algebrică este normală dacă odată cu un element conţine orice conjugat al acestuia peste corpul de bază.

Extinderea $K\supseteq K$ este extindere normală deoarece pentru orice $a\in K$, singurul element conjugat cu *a* peste *K* este *a*.

Extinderea $\overline{K}\supseteq K$ este evident extindere normală.

8.2. **Propoziţie.** *Fie* $L\supseteq K$ *o extindere de corpuri,* $L\subseteq\overline{K}$. *Sunt echivalente condiţiile:*

a) $L\supseteq K$ *este o extindere normală*;

b) $\forall\sigma\in G\left(\overline{K}\mid K\right)$, $\sigma(L)\subseteq L$;

c) $\forall\sigma\in G\left(\overline{K}\mid K\right)$, $\sigma|_L\in G\left(L\mid K\right)$.

Demonstraţie. "a)$\Rightarrow$b)" Fie $\sigma\in G\left(\overline{K}\mid K\right)$ şi $\alpha\in L$. Din 7.4., $\beta=\sigma(\alpha)$ este un conjugat al lui α peste *K*. Deoarece $L\supseteq K$ este extindere normală, $\beta\in L$. Deci, $\sigma(L)\subseteq L$.

"b)$\Rightarrow$c)" Fie $\sigma\in G\left(\overline{K}\mid K\right)$. Conform b), putem vorbi despre restricţia $\sigma|_L:L\to L$. Este suficient să demonstrăm că $\sigma|_L$ este surjectivă. Fie $y\in L$ şi p_y polinomul minimal al lui *y* peste *K*. Fie

$$A=\left\{\alpha\in L\,\middle|\,p_y(\alpha)=0\right\}.$$

Mulţimea A este finită, conţine y şi, dacă $\alpha\in A,$ atunci $\sigma(\alpha)\in A.$ Deoarece restricţia lui σ la A este injectivă, este şi surjectivă. Există $x\in A\subseteq L,$ astfel încât $\sigma(x)=y.$

"c) $\Rightarrow$ a)" Fie $\alpha\in L$ şi $\beta\in\overline{K},$ un conjugat al lui α peste K. Conform 7.4., există $\sigma\in G\left(\overline{K}\mid K\right)$ astfel încât $\sigma(\alpha)=\beta.$ Conform c), $\sigma(\alpha)\in L.$ □

8.3. **Propoziţie.** *Orice corp de descompunere al unui polinom este extindere normală a corpului de bază.*

Demonstraţie. Considerăm f un polinom din $K[X],$ $d^\circ f=n\geq 1$ şi fie $L=K(\alpha_1,...,\alpha_n)\subseteq\overline{K}$ un corp de descompunere al lui f. Dacă $\sigma\in G\left(\overline{K}\mid K\right),$ atunci, pentru orice $i\in\overline{1,n},$ $f(\sigma(\alpha_i))=0,$ deci există $j\in\overline{1,n},$ astfel încât $\sigma(\alpha_i)=\alpha_j\in L.$ Rezultă $\sigma(L)\subseteq L$ şi, conform 8.2.b), $L\supseteq K$ este o extindere normală. □

În particular, deoarece $\mathbb{Q}\left(\sqrt{3}\right)$ este corp de descompunere al polinomului $f=X^2-3\in\mathbb{Q}[X],$ $\mathbb{Q}\left(\sqrt{3}\right)\supseteq\mathbb{Q}$ este extindere normală.

8.4. **Propoziţie.** *Dacă $L\supseteq K$ este o extindere finită şi normală, atunci L este corp de descompunere al unui polinom $f\in K[X]$.*

Demonstraţie. Fie $(\alpha_1,...,\alpha_n)$ o bază în ${}_KL$. Atunci rezultă că $L=K(\alpha_1,...,\alpha_n).$ Fie $p_{\alpha_i}\in K[X]$ polinomul minimal al lui α_i peste $K,$ $i\in\overline{1,n}.$ Deoarece $L\supseteq K$ este extindere normală şi p_{α_i} are o rădăcină în L, rezultă că p_{α_i} are toate rădăcinile în $L,$ $i\in\overline{1,n}.$ Notăm

$$f=\prod_{i=1}^{n}p_{\alpha_i}\in K[X].$$

L este corp de descompunere al polinomului f. □

8.5. **Propoziție.** *Fie* $L \supseteq K$ *extindere algebrică şi* $E \in \mathscr{L}(L;K)$. *Dacă* $L \supseteq K$ *este extindere normală, atunci* $L \supseteq E$ *este extindere normală.*

Demonstrație. $L \supseteq K$ este extindere algebrică. Fie $\overline{K}$ o închidere algebrică a lui *K*, astfel încât $\overline{K} \supseteq L$. $\overline{K}$ este şi închidere algebrică a lui *E*. Fie $\sigma \in G\left(\overline{K} \mid E\right)$. Rezultă $\sigma \in G\left(\overline{K} \mid K\right)$ şi, deoarece $L \supseteq K$ este extindere normală, $\sigma(L) \subseteq L$. Conform 8.2., $L \supseteq E$ este extindere normală. □

8.6. **Propoziție.** *Fie* $L \supseteq K$ *o extindere algebrică de corpuri şi* $E_1, E_2 \in \mathscr{L}(L;K)$. *Atunci*:

a) *Dacă* $E_1 \supseteq K$ *şi* $E_2 \supseteq K$ *sunt extinderi normale, atunci extinderile* $E_1E_2 \supseteq K$ *şi* $E_1 \cap E_2 \supseteq K$ *sunt normale*:

b) *Dacă* $E_1 \supseteq K$ *este extindere normală, atunci* $E_1E_2 \supseteq E_2$ *este extindere normală*.

Demonstrație. a) Fie $\overline{K}$ o închidere algebrică a lui *K*, $\overline{K} \supseteq L$. Dacă $\sigma \in G\left(\overline{K} \mid K\right)$, atunci, deoarece $E_1 \supseteq K$ şi $E_2 \supseteq K$ sunt extinderi normale, $\sigma(E_1) \subseteq E_1$ şi $\sigma(E_2) \subseteq E_2$. Rezultă:

$$\sigma(E_1E_2) = \sigma\left(K(E_1 \cup E_2)\right) \subseteq K\left(\sigma(E_1) \cup \sigma(E_2)\right) \subseteq K(E_1 \cup E_2) = E_1E_2$$

$$\sigma(E_1 \cap E_2) = \sigma(E_1) \cap \sigma(E_2) \subseteq E_1 \cap E_2.$$

Deci, $E_1E_2 \supseteq K$ şi $E_1 \cap E_2 \supseteq K$ sunt extinderi normale.

b) $\overline{K}$ este închidere algebrică şi pentru E_2. Dacă $\sigma \in G\left(\overline{K} \mid E_2\right)$, atunci $\sigma(E_2) = E_2$ şi $\sigma \in G\left(\overline{K} \mid K\right)$, deci $\sigma(E_1) \supseteq E_1$ ($E_1 \supseteq K$ este extindere normală). Ca şi mai sus, se obține $\sigma(E_1E_2) \subseteq E_1E_2$. Deci, extinderea $E_1E_2 \supseteq E_2$ este normală. □

8.7. **Teoremă.** *Dacă* $L \supseteq K$ *este o extindere finită, normală şi separabilă, atunci* $G(L \mid K)$ *este finit şi*:

$$\left|G(L \mid K)\right| = [L:K].$$

Demonstrație. Conform teoremei elementului primitiv, extinderea $L \supseteq K$ este simplă. Fie α un element primitiv al său. Deci,

$$L = K(\alpha) \text{ şi } d^{\circ} p_{\alpha} = [L : K]$$

unde $p_{\alpha} \in K[X]$ este polinomul minimal al lui α.

Considerăm, ca de obicei, $\overline{K}$ o închidere algebrică a lui K care include L. Notăm cu $A = \left\{ \beta \in \overline{K} \,\middle|\, p_{\alpha}(\beta) = 0 \right\}$ mulțimea conjugaților lui α peste K. Deoarece $L \supseteq K$ este o extindere normală, $A \subseteq L$. Cum α este separabil peste K, $|A| = d^{\circ} p_{\alpha}$. Este suficient să demonstrăm că $|G(L \mid K)| = |A|$.

Fie $\sigma \in G(L \mid K)$. $\sigma(\alpha)$ este o rădăcină a lui p_{α}. Aplicația:

$$\lambda : G(L \mid K) \to A, \ \lambda(\sigma) = \sigma(\alpha), \ \forall \sigma \in G(L \mid K)$$

este bine definită.

Dacă $\sigma, \tau \in G(L \mid K)$ şi $\lambda(\sigma) = \lambda(\tau)$, atunci $\sigma = \tau$. Prin urmare, aplicația λ este injectivă şi $G(L \mid K)$ este finit.

Dacă $\beta \in A$, atunci, conform III.7.4., există un izomorfism

$\sigma : K(\alpha) \to K(\beta)$ astfel încât $\sigma(a) = a, \ \forall a \in K$ şi $\sigma(\alpha) = \beta$.

Din $K \subseteq K(\beta) \subseteq L = K(\alpha)$ şi $[K(\beta) : K] = [K(\alpha) : K] = d^{\circ} p_{\alpha}$, rezultă $K(\beta) = L$. Deci, $\sigma \in G(L \mid K)$ şi $\sigma(\alpha) = \beta$, adică aplicația λ este bijectivă. Rezultă $|G(L \mid K)| = |A|$. □

8.8. **Consecință.** *Fie L un corp finit şi K un subcorp al său. Atunci $G(L \mid K)$ este ciclic.*

Demonstrație. Fie $carL = p$ şi $\overline{K}$ o închidere a lui K astfel încât

$$\mathbb{Z}_p \subseteq K \subseteq L \subseteq \overline{K}.$$

Fie $d = [K : \mathbb{Z}_p], \ m = [L : \mathbb{Z}_p], \ n = [L : K]$.

Extinderea $L \supseteq K$ este finită, normală (fiind corp de descompunere) şi separabilă (conform 6.4.). Din 8.7., rezultă:

(9) $$|G(L \mid K)| = [L : K] = n.$$

Fie $u:\overline{K}\to\overline{K}$ endomorfismul lui Frobenius. Deoarece $L\supseteq\mathbb{Z}_p$ este extindere normală, putem vorbi despre restricția u_1 a lui *u* la *L*.

Fie $v=u_1^{\,d}$. Din demonstrația teoremei 4.6., rezultă $v(\alpha)=\alpha$, $\forall\alpha\in K$. Prin urmare, $v\in G(L\,|\,K)$. Vom arăta că:

$$G(L\,|\,K)=\{1_L,v,v^2,...,v^{n-1}\}.$$

Ținând seama de (9), este suficient să arătăm că $ordv=n$.

Pentru orice $\alpha\in L$, $v^n(\alpha)=u^m(\alpha)=\alpha$. Deci, $v^n=1_L$. Dacă ar exista *i*, $0<i<n$, astfel încât $v^i=1_L$, atunci, pentru orice $\alpha\in L$:

$$\alpha=v^i(\alpha)=u^{di}(\alpha)=\alpha^{p^{di}}.$$

Polinomul $f=X^{p^{di}}-X$ ar avea în L $p^m>p^{di}$ soluții, contradicție. Deci, $ordv=n$. □

9. Teorema fundamentală a teoriei lui Galois

În acest paragraf sunt studiate condițiile în care corespondențele între laticea subgrupurilor grupului Galois şi laticea corpurilor intermediare ale unei extinderi sunt bijective.

9.1. **Teoremă.** *Fie* $L\supseteq K$ *o extindere finită, normală şi separabilă. Fie* $G=G(L\,|\,K)$, $\mathscr{L}(G)=\{H\,|\,H\le G\}$ *şi*

$$\mathscr{L}(L;K)=\{E\,|\,E\text{ subcorp al lui }L,\ E\supseteq K\}.$$

Am definit $F:\mathscr{L}(G)\to\mathscr{L}(L;K)$ *prin*

$$F(H)=L^H=\{\alpha\in L\,|\,\sigma(\alpha)=\alpha,\ \forall\sigma\in H\},\quad\forall H\in\mathscr{L}(G).$$

Atunci:

a) *F este bijectivă;*

b) *Fie* $H\in\mathscr{L}(G)$.

$$H\trianglelefteq G\Leftrightarrow L^H\supseteq K\ \textit{este extindere normală};$$

c) *Dacă* $H\trianglelefteq G$ *şi* $E=L^H$, *atunci*

$$G(E\,|\,K)\simeq G(L\,|\,K)/G(L\,|\,E).$$

Demonstrație. Considerăm şi cea de-a doua corespondență

$$\Phi : \mathcal{L}(L;K) \to \mathcal{L}(G)$$

definită prin $\Phi(E) = G(L \mid E),\ \forall E \in \mathcal{L}(L;K).$

Pentru a) este suficient să demonstrăm relațiile

$$\Phi \circ F = 1_{\mathcal{L}(G)} \text{ şi } F \circ \Phi = 1_{\mathcal{L}(L;K)}.$$

Fie $H \in \mathcal{L}(G).$ Din definițiile lui Φ şi F, rezultă:

(1) $$\left(\Phi \circ F\right)(H) = G\left(L \mid L^H\right) \supseteq H.$$

Deoarece extinderea $L \supseteq K$ este finită, normală şi separabilă, din 8.7., G este finit şi $\left|G(L \mid K)\right| = [L:K]$. Extinderea $L \supseteq L^H$ este şi ea finită, normală şi separabilă. Conform teoremei elementului primitiv, există $x \in L$ astfel încât $L = L^H(x).$ Conform 8.7.,

$$\left|G(L \mid L^H)\right| = [L:L^H] = d^\circ p_x$$

unde p_x este polinomul minimal al lui x peste L^H.

Subgrupul H este finit. Fie $\left|H\right| = n$ şi

$$H = \left\{\sigma_1, \sigma_2, ..., \sigma_n\right\},\ \sigma_1 = 1_L.$$

Notăm: $f = \prod_{i=1}^{n} (X - \sigma_i(x)) \in L[X].$

Fie $\sigma \in H$ şi f_σ polinomul obținut prin aplicarea lui σ asupra coeficienților lui f:

$$f_\sigma = \prod_{i=1}^{n} \left(X - (\sigma \circ \sigma_i)(x)\right) = \prod_{i=1}^{n} \left(X - \sigma_i(x)\right) = f$$

deoarece atunci când σ_i parcurge H şi $\sigma \circ \sigma_i$ parcurge H. Prin urmare, coeficienții lui f sunt invariați de automorfismele din H, adică $f \in L^H[X]$. În plus, $f(x) = 0,$ de unde rezultă $p_x \mid f$ şi $d^\circ p_x \le n.$ Deci,

$$\left|G(L \mid L^H)\right| \le n = \left|H\right|.$$

Ținând seama şi de relația (1), rezultă:

(2) $$G(L \mid L^H) = H.$$

Deci, $\Phi \circ F = 1_{\mathcal{L}(G)}.$

Fie acum $E \in \mathcal{L}(L;K)$. Din definiţiile lui Φ şi F, rezultă:

$$\big(F \circ \Phi\big)(E) = L^{G(L|E)} \supseteq E.$$

Deci,

$$K \subseteq E \subseteq L^{G(L|E)} \subseteq L.$$

Cum extinderile $E \subseteq L$ şi $L^{G(L|E)} \subseteq L$ sunt finite, normale şi separabile,

$$[L : L^{G(L|E)}] = \big|G(L \mid L^{G(L|E)})\big| = \big|G(L \mid E)\big| = [L : E]$$

(a două egalitate rezultă din (2)).

Din proprietatea de tranzitivitate a extinderilor finite, rezultă că $[L^{G(L|E)} : E] = 1$ sau $L^{G(L|E)} = E$ adică

$$F \circ \Phi = 1_{\mathcal{L}(L;K)}$$

şi se încheie demonstraţia lui a).

Să presupunem acum că H este subgrup normal în G. Fie $E = L^H$. Conform a), $G(L \mid E) = H$. Pentru a demonstra că $E \supseteq K$ este extindere normală, arătăm că E conţine odată cu un element x, orice conjugat al acestuia peste K.

Fie deci $x \in E$ şi x' un conjugat al său. Conform celor demonstrate în 8.7., există $\sigma \in G(L \mid K)$ astfel încât $\sigma(x) = x'$.

$$x' \in E = L^H \Leftrightarrow \tau(x') = x',\ \forall \tau \in H.$$

Deoarece H este subgrup normal în G, $\sigma H \sigma^{-1} = H$.

Fie $\tau \in H$. Există $\lambda \in H$ astfel încât $\tau = \sigma\lambda\sigma^{-1}$.

(3) $$\tau(x') = \sigma\Big(\lambda\big(\sigma^{-1}(x')\big)\Big) = \sigma\big(\lambda(x)\big) = \sigma(x) = x'.$$

Am ţinut seama că $x \in E$ şi $\lambda \in G(L \mid E)$, deci $\lambda(x) = x$.

Din (3) rezultă $x' \in E$ şi prin urmare, extinderea $E \supseteq K$ este normală.

Implicaţia reciprocă de la b) şi c) vor fi demonstrate simultan.
Fie deci $E \in \mathcal{L}(L;K)$ astfel încât $E \supseteq K$ să fie o extindere normală. Fie $H = G(L \mid E)$. Are loc şi egalitatea $L^H = E$. Definim aplicaţia:

$$\Lambda : G(L \mid K) \to G(E \mid K),\ \Lambda(\sigma) = \sigma|_E,\ \forall \sigma \in G(L \mid K).$$

Deoarece $E \supseteq K$ este o extindere normală, Λ este bine definită. Se verifică egalitatea:

$$(\sigma \circ \tau)|_E = \sigma|_E \circ \tau|_E, \ \forall \sigma, \tau \in G(L \mid K),$$

ceea ce arată că Λ este un morfism de grupuri.

Vom demonstra că Λ este morfism surjectiv.

Fie $u \in G(E \mid K)$. Fie $\overline{K}$ o închidere algebrică a lui K astfel încât $\overline{K} \supseteq L$. Conform III.9.5., există $\tau \in G\left(\overline{K} \mid K\right)$ care prelungeşte u. Deoarece $L \supseteq K$ este extindere normală, $\sigma = \tau|_L \in G(L \mid K)$.

$$\Lambda(\sigma) = \sigma|_E = \tau|_E = u,$$

deci Λ este morfism surjectiv.

Ne propunem să determinăm nucleul morfismului Λ.

Fie $\sigma \in G(L \mid K)$.

$$\sigma \in Ker\Lambda \Leftrightarrow \Lambda(\sigma) = \sigma|_E = 1_E \Leftrightarrow \sigma \in G(L \mid E) = H.$$

Deci, $Ker\Lambda = H$. De aici rezultă $H \trianglelefteq G$ şi, aplicând teorema fundamentală de izomorfism pentru morfismul Λ:

$$G\left(E \mid K\right) = \mathrm{Im}\,\Lambda \simeq G\left(L \mid K\right)/H = G\left(L \mid K\right)/G\left(L \mid E\right).$$

Se observă că izomorfismul de la c) este indus de aplicația de restricționare a automorfismelor din G la E. □

Probleme propuse

1. Dacă $E, F \in \mathscr{L}(L;K)$ şi $\alpha \in L$ element algebric peste E, arătați că $\left[EF(\alpha) : EF\right] \leq \left[E(\alpha) : E\right]$.

2. Dacă $E, F, G \in \mathscr{L}(L;K)$ şi extinderea $F \supseteq E$ este finită, atunci $FG \supseteq EG$ este o extindere finită şi $\left[FG : EG\right] \leq \left[F : E\right]$.

3. Fie $L \supseteq K$ o extindere de corpuri şi E, F două corpuri intermediare. Dacă $\left[E : K\right]$ şi $\left[F : K\right]$ sunt numere prime între ele, arătați că:

$$\left[EF : K\right] = \left[E : K\right] \cdot \left[F : K\right].$$

4. Să se determine:
a) rădăcinile complexe de gradul 10 ale unității;
b) rădăcinile primitive de gradul 10 ale unității;
c) polinomul ciclotomic F_{10}.
d) descompunerea în factori ireductibili în $\mathbb{Q}[X]$ a polinomului:

$$f = X^{10} - 1.$$

5. Considerăm funcția lui Möbius, $\mu : \mathbb{N}^* \to \mathbb{Z}$ definită prin:

$$\mu(n) = \begin{cases} 1, & n = 1; \\ (-1)^s, & n = p_1 p_2 \ldots p_s,\ p_i \text{ prime, distincte;} \\ 0, & \text{altfel } (\exists p \text{ prim, astfel ca } p^2 \mid n). \end{cases}$$

Arătați că:
a) $\mu(mn) = \mu(m)\mu(n)$ dacă $(m,n) = 1$;

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

c) Fie $(G,+)$ grup comutativ. Considerăm funcțiile:

$$f, g : \mathbb{N}^* \to G \text{ astfel încât } f(n) = \sum_{d|n} g(d).$$

Arătați că are loc egalitatea (*formula de inversiune a lui Möbius*):

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right),$$

d) Dacă $(G,\cdot)$ este grup abelian şi funcțiile $f, g : \mathbb{N}^* \to G$ verifică relația $f(n) = \prod_{d|n} g(d)$, atătați că $g(n) = \prod_{d|n} f\left(\frac{n}{d}\right)^{\mu(d)}$.

e) Să se arate că $F_n = \prod_{d|n} \left(X^{\frac{n}{d}} - 1 \right)^{\mu(d)}$.

f) Folosind e), să se calculeze în mod direct F_6, F_{10}, F_{12}, F_{15}.

6. Fie p şi q numere prime distincte. Arătați că:

$$F_{p^n} = F_p\left(X^{p^{n-1}}\right),\ F_{p^n q^m} = F_{pq}\left(X^{p^{n-1}q^{m-1}}\right).$$

Folosind aceste relații, calculați F_{27} și F_{36}.

7. Arătați că pentru un corp finit K, grupul $Aut(K)$ este abelian.

8. Să se arate că $L = \mathbb{Z}_2[X]/\left(X^4 + X^3 + \hat{1}\right)$ este un corp cu 16 elemente. Construiți apoi un corp cu 8 respectiv, 27 elemente.

9. Fie K un corp finit și $a \in K$. Determinați a astfel încât polinomul f să fie ireductibil în $K[X]$ dacă:

a) $f = X^3 + aX + 2 \in K[X],\ |K| = 3;$

b) $f = X^4 + aX + 1 \in K[X],\ |K| = 5.$

10. Fie p număr prim și $a, b, c \in \mathbb{Z}_p$ cu $a \neq \hat{0}$. Să se rezolve în $\mathbb{Z}_p$ ecuația $ax^2 + bx + c = \hat{0}$. În cazul în care există, găsiți soluțiile ecuațiilor: $\hat{2}x^2 + \hat{3}x + \hat{5} = \widehat{10},$ respectiv, $x^2 + \hat{3}x + \hat{3} = \hat{0},$ în $\mathbb{Z}_{11}$.

11. Fie K un corp finit de caracteristică p, număr prim și n număr natural. Arătați că polinomul $f = X^{p^n} - a \in K[X]$ are cel mult o rădăcină în K.

12. Se consideră un corp finit K cu $car(K) = p,$ număr prim. Să se arate că:

a) Pentru orice număr natural n, există polinoame ireductibile de grad n în $K[X]$.

b) Pentru orice polinom ireductibil $f \in K[X],$ există un număr natural n astfel ca $f \mid X^{p^n} - X$.

13. Fie corpul finit (fixat) K, cu q elemente.

a) Stabiliți numărul de polinoame ireductibile, de grad n, neasociate în divizibilitate din $K[X]$.

b) Arătați că numărul polinoamelor unitare, ireductibile, de grad p, număr prim, din $K[X]$ este egal cu $\frac{q^p - q}{p}$.

c) Precizați toate extinderile de grad p, număr prim, ale lui K.

14. Arătați că următoarele extinderi sunt simple şi, pentru fiecare dintre ele, precizați un element primitiv:

a) $\mathbb{Q}\left(\sqrt{5}, \sqrt{3}\right) \supseteq \mathbb{Q}$;

b) $\mathbb{Q}\left(\sqrt[3]{2}, i\sqrt{3}\right) \supseteq \mathbb{Q}$.

15. Demonstrați că o extindere finită de corpuri $L \supseteq K$ este normală dacă şi numai dacă L este corp de descompunere al unui polinom $f \in K[X]$.

16. Considerăm extinderile de corpuri $E \supseteq L \supseteq K$ astfel încât $L \supseteq K$ este normală şi E este corpul de descompunere peste L al unui polinom $f \in K[X]$. Arătați că $E \supseteq K$ este extindere normală.

Se menține adevărată afirmația dacă $f \in L[X]$? Au extinderile normale proprietatea de tranzitivitate?

17. Să se arate că orice extindere pătratică este normală. Este ea şi separabilă?

18. Fie K un corp finit şi $f \in K[X]$, polinom ireductibil. Arătați că $L = K[X]/(f)$ este un corp de descompunere al lui f peste K.

19. Precizați care dintre următoarele extinderi sunt normale:

a) $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$, unde α este o rădăcină a lui $f = X^3 - 2 \in \mathbb{Q}[X]$;

b) $\mathbb{Q}\left(i, \sqrt{3}, \alpha\right) \supseteq \mathbb{Q}\left(i, \sqrt{3}\right)$, cu α definit ca mai înainte;

c) $\mathbb{Z}_2[X]/\left(X^3 + X + \hat{1}\right) \supseteq \mathbb{Z}_2$.

20. Fie K un corp finit cu p^s elemente (p număr prim, $s \geq 1$). Fie $L \supseteq K$ o extindere finită de grad n. Pentru $k \in \overline{0, n-1}$ definim morfismele $u_k : L \to L$ prin $u_k(x) = x^{p^{ks}}$, $\forall x \in L$. Arătați că pentru orice k, $u_k \in G(L \mid K)$.

21. Fie K un corp finit cu p^s elemente (p număr prim şi $s \geq 1$) şi α o rădăcină a lui $f \in K[X]$, polinom ireductibil de grad n.
Arătați că rădăcinile lui f din $K(\alpha)$ sunt: α, α^{p^s}, $\alpha^{p^{2s}}$, ... , $\alpha^{p^{(n-1)s}}$.

22. Pentru polinomul $f = X^4 + X^3 + \hat{1} \in \mathbb{Z}_2[X]$, stabiliți corpul de descompunere L şi precizați rădăcinile sale.

23. Fie K un corp comutativ, de caracteristică p, număr prim şi $f = X^p - X + a \in K[X]$, un polinom ireductibil. Fie α o rădăcină a lui f într-o închidere algebrică a lui K. Determinați $G(K(\alpha) \mid K)$.

24. Pentru fiecare polinom $f \in \mathbb{Q}[X]$, definit la următoarele subpuncte, notăm cu L un corp de descompunere al său şi cu G_f grupul Galois asociat extinderii $L \supseteq \mathbb{Q}$. Determinați:

$$G_f, \ \mathcal{L}(G_f) \text{ şi } \mathcal{L}(L;\mathbb{Q}),$$

precizând care corpuri intermediare $E \in \mathcal{L}(L;\mathbb{Q})$ sunt extinderi normale ale lui $\mathbb{Q}$.

a) $f = X^2 + 3 \in \mathbb{Q}[X]$;

b) $f = (X^2 + 2)(X^2 - 5) \in \mathbb{Q}[X]$;

c) $f = X^3 - 2 \in \mathbb{Q}[X]$;

d) $f = X^4 - 2 \in \mathbb{Q}[X]$.

Capitolul VI

APLICAȚII ALE TEORIEI LUI GALOIS

În acest capitol vom aplica elementele de teorie Galois din capitolul precedent la două probleme clasice. În primul rând este vorba de rezolvarea ecuațiilor algebrice prin radicali, problemă centrală pentru matematica secolelor XVI – XIX. Caracterizarea ecuațiilor algebrice rezolvabile prin radicali se face cu ajutorul grupului Galois al corpului de descompunere asociat acestui polinom.

A doua problemă tratată este aceea a constructibilității cu rigla şi compasul. Urmărind bijecția obişnuită dintre punctele unui plan, în care s-a fixat un sistem de coordonate carteziene ortogonale şi elementele lui $\mathbb{C}$, se realizează transpunerea problemei construcțiilor geometrice în domeniul extinderilor de corpuri. Pe această cale se dă un răspuns simplu unor probleme clasice ca: dublarea cubului, cuadratura cercului, trisecțiunea unghiului, construcția poligoanelor regulate.

1. Extinderi radicale.

Fie K un corp de caracteristică zero şi $\overline{K}$ închiderea sa algebrică. Considerăm polinomul

(1) $$f = X^n - a \in K[X], \quad n \geq 1.$$

Fie $\theta \in \overline{K}$ o rădăcină a lui f. Se spune că θ este un ***radical de ordin n*** peste K. Dacă $\xi \in \overline{K}$ este o rădăcină primitivă de grad n a unității, atunci $\theta\xi^i$, $i \in \mathbb{N}$, este de asemenea o rădăcină a lui f. Astfel,

(2) $$\theta, \theta\xi, ..., \theta\xi^{n-1}$$

sunt toate rădăcinile lui f.

1.1. **Definiție.** *Numim* ***extindere radicală simplă*** *a corpului K, orice corp de descompunere al unui polinom*

$$f = X^n - a \in K[X], \quad n \geq 1.$$

$\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$ este o extindere radicală simplă fiind un corp de descompunere al polinomului $f = X^2 - 2 \in \mathbb{Q}[X]$.

$\mathbb{C} \supseteq \mathbb{R}$ este o extindere radicală simplă fiind un corp de descompunere al polinomului $f = X^2 + 1 \in \mathbb{R}[X]$.

Orice corp de descompunere al unui polinom de gradul doi este o extindere radicală simplă. Într-adevăr, fie $f = X^2 + aX + b \in K[X]$, $\Delta = a^2 - 4b$ şi $\theta \in \overline{K}$ astfel încât $\theta^2 = \Delta$. Elementele $\frac{-a \pm \theta}{2}$ sunt rădăcinile lui f. Corpul de descompunere al lui f coincide cu corpul de descompunere al polinomului $X^2 - \Delta \in K[X]$.

În particular, orice extindere de gradul doi este o extindere radicală simplă.

Din considerațiile de mai sus, rezultă că orice extindere radicală simplă este de forma

(3) $$K(\theta, \xi) \supseteq K$$

unde $\theta^n \in K$ (pentru un anumit $n \in \mathbb{N}^*$) şi ξ este rădăcină primitivă de grad n a unității.

Pentru $\varepsilon = \frac{-1 + i\sqrt{3}}{2}$, extinderea $\mathbb{Q}\left(\sqrt[3]{2}, \varepsilon\right) \supseteq \mathbb{Q}$ este radicală simplă, fiind corpul de descompunere al polinomului $X^3 - 2 \in \mathbb{Q}[X]$.

Orice extindere radicală simplă este o extindere normală deoarece este corp de descompunere.

Deoarece θ şi ξ din (3) sunt elemente algebrice peste K, din (3) rezultă că orice extindere radicală simplă este o extindere finită, deci algebrică.

1.2. **Definiție.** *Spunem că* $L \supseteq K$ *este* ***extindere radicală*** *dacă există lanțul de extinderi*

(4) $$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = L$$

unde $K_{i-1} \subseteq K_i$ *este extindere radicală simplă, pentru orice* $i \in \overline{1,s}$.

Din definiție, rezultă că extinderile radicale au proprietatea de tranzitivitate.

Orice extindere radicală este o extindere finită, deci şi o extindere algebrică.

Deoarece extinderile normale nu au proprietatea de tranzitivitate, nu rezultă că orice extindere radicală este o extindere normală.

1.3. **Teoremă.** *Dacă* $L \supseteq K$ *este o extindere radicală, atunci există o extindere* L' *a lui L astfel încât* $L' \supseteq K$ *este extindere radicală şi normală.*

Demonstrație. În continuare, considerăm că toate extinderile lui *K*, care sunt extinderi algebrice, sunt incluse într-o închidere algebrică, $\overline{K}$. Fie $L \supseteq K$ o extindere radicală şi (4) un lanț de extinderi radicale simple. Vom raționa prin inducție după *s*.

Pentru $s = 1$, $L \supseteq K$ este extindere radicală simplă, deci şi o extindere normală. Putem lua $L' = L$.

Presupunem afirmația adevărată pentru valoarea $s-1$ şi considerăm extinderea radicală $L \supseteq K$ căreia îi corespunde lanțul (4), pentru valoarea *s*.

Conform ipotezei de inducție, există o extindere $L_1 \supseteq K_{s-1}$, astfel încât $L_1 \supseteq K$ este extindere radicală şi normală. $K_s \supseteq K_{s-1}$ este extindere radicală simplă, deci

$$K_s = K_{s-1}(\theta, \xi)$$

unde $\theta^n = \beta \in K_{s-1}$ (pentru un anumit $n \in \mathbb{N}^*$) şi ξ este rădăcină primitivă de grad *n* a unității.

Elementul $\beta \in K_{s-1} \subseteq L_1$ este algebric peste *K*. Fie $p_\beta \in K[X]$ polinomul său minimal şi $\beta_1 = \beta, \beta_2, ..., \beta_r$ toate rădăcinile lui p_β. Deoarece $L_1 \supseteq K$ este extindere normală, $\beta_i \in L_1$, $i \in \overline{1,r}$.

Fie $f = p_\beta(X^n) \in K[X]$ şi $\theta_i \in \overline{K}$ o rădăcină a polinomului

$$X^n - \beta_i,$$

$i \in \overline{1,r}$ cu $\theta_1 = \theta$. Toate rădăcinile lui *f* sunt de forma:

$$\theta_i \xi^j, \quad i \in \overline{1,r}, \quad j \in \overline{0,n-1}.$$

Fie L_2 corpul de descompunere al lui *f* peste *K*.

$$L_2 = K(\xi, \theta_1, ..., \theta_r).$$

$L_2 \supseteq K$ este o extindere normală. Notăm

$$L' = L_1 L_2 = K\left(L_1 \cup L_2\right) = K(L_1)(L_2) = L_1(L_2),$$

compozitul corpurilor L_1 şi L_2. Din V.8.6., rezultă că $L' \supseteq K$ este o extindere normală.

$$L' = L_1(\xi, \theta_1, ..., \theta_r).$$

$$L_1 \subseteq L_1(\xi) \subseteq L_1(\xi, \theta_1) \subseteq ... \subseteq L_1(\xi, \theta_1, ..., \theta_r).$$

Deoarece fiecare dintre extinderile ultimului lanţ este o extindere radicală simplă, $L_1 \subseteq L'$ este extindere radicală. Dar şi $K \subseteq L_1$ este o extindere radicală, deci $K \subseteq L'$ este o extindere radicală. În plus,

$$L' = L_1(\xi, \theta_1, ..., \theta_r) \supseteq K_{s-1}(\xi, \theta_1) = K_s = L. \qquad \square$$

2. Grupul Galois al unei extinderi radicale

Rezultatul principal al acestui paragraf este acela că grupul Galois al unei extinderi radicale şi normale este rezolubil.

2.1. **Lemă.** *Fie K un corp de caracteristică zero şi* $\xi \in \overline{K}$ *o rădăcină primitivă de grad n a unităţii. Atunci, grupul Galois*

$$G\left(K(\xi) \mid K\right)$$

este rezolubil.

Demonstraţie. Notăm $G = G\left(K(\xi) \mid K\right)$ şi fie $\sigma \in G$. Pentru *m*, număr natural,

$$\xi^m = 1 \Leftrightarrow \sigma(\xi)^m = 1.$$

Rezultă $ord(\xi) = ord\left(\sigma(\xi)\right) = n$, adică $\sigma(\xi)$ este, de asemenea, o rădăcină de grad *n* a unităţii. Există $q \in \mathbb{N}^*$, astfel încât $\sigma(\xi) = \xi^q$ şi $(q,n) = 1$. Dacă, în plus, $\sigma(\xi) = \xi^r$, atunci $ord\,\xi = n \mid (q-r)$.

Definim aplicaţia:

$$\lambda : G \to U(\mathbb{Z}_n),$$

prin $\lambda(\sigma)=\hat{q},$ dacă $\sigma(\xi)=\xi^q$.

Aplicația λ este bine definită.

Fie $\sigma,\tau\in G$ astfel încât $\sigma(\xi)=\xi^q$ şi $\tau(\xi)=\xi^r$. Atunci:

$$(\sigma\circ\tau)(\xi)=\sigma(\tau(\xi))=\sigma(\xi^r)=\xi^{qr}.$$

Deci, $\lambda(\sigma\circ\tau)=\widehat{qr}=\hat{q}\cdot\hat{r}=\lambda(\sigma)\lambda(\tau)$. Cu alte cuvinte, λ este un morfism de grupuri.

Dacă $\lambda(\sigma)=\hat{1},$ atunci $\sigma(\xi)=\xi$ şi rezultă $\sigma=1_{K(\xi)}$. Prin urmare, λ este un morfism injectiv.

Astfel, $G\simeq\operatorname{Im}\lambda\le U(\mathbb{Z}_n)$. Deoarece $\big(U(\mathbb{Z}_n),\cdot\big)$ este grup abelian, *G* este abelian, deci rezolubil. □

2.2. **Lemă.** *Fie K un corp de caracteristică zero. Fie* $\xi\in\overline{K}$ *o rădăcină primitivă de grad n a unității şi* $\theta\in\overline{K^*}$, *un radical de ordin n peste K. Atunci, grupul Galois*

$$G=G\big(K(\xi,\theta)\,|\,K(\xi)\big)$$

este rezolubil.

Demonstrație. Notăm: $\theta^n=a\in K,\ \ f=X^n-a.$

Pentru orice $\sigma\in G,\ \ \sigma(\theta)^n=a.$ Deoarece $\sigma(\theta)$ este, de asemenea, o rădăcină a lui *f*, există $m\in\mathbb{N},$ astfel încât $\sigma(\theta)=\theta\xi^m$. Dacă $\sigma(\theta)=\theta\xi^q,$ atunci $n\,|\,(m-q)$. Definim aplicația:

$$\lambda: G\to\mathbb{Z}_n,$$

prin $\lambda(\sigma)=\widehat{m},$ dacă $\sigma(\theta)=\theta\xi^m$.

Aplicația λ este bine definită.

Dacă, în plus, $\tau\in G$ şi $\tau(\theta)=\theta\xi^r,$ atunci:

$$(\sigma\circ\tau)(\theta)=\sigma(\tau(\theta))=\sigma(\theta)\xi^r=\theta\xi^{m+r}.$$

Deci,

$$\lambda(\sigma\circ\tau)=\widehat{m+r}=\widehat{m}+\hat{r}=\lambda(\sigma)+\lambda(\tau).$$

Cu alte cuvinte, λ este un morfism de grupuri.

Dacă $\lambda(\sigma)=\hat{0}$, atunci $\sigma(\theta)=\theta$ şi rezultă $\sigma=1_{K(\xi,\theta)}$. Morfismul λ este injectiv.

Astfel, $G\simeq \operatorname{Im}\lambda\leq\mathbb{Z}_n$. Rezultă *G* abelian, deci rezolubil. □

2.3. **Lemă.** *Fie K un corp de caracteristică zero şi* $L\supseteq K$ *o extindere radicală simplă. Atunci, grupul* $G=G\left(L\mid K\right)$ *este rezolubil.*

Demonstraţie. *L* este un corp de descompunere al unui polinom de forma $f=X^n-a\in K[X]$. Dacă $\theta\in L$ este o rădăcină a lui *f* iar $\xi\in L$ este o rădăcină primitivă de grad *n* a unităţii, atunci:

$$L=K(\theta,\xi).$$

$K(\xi)\supseteq K$ este extindere normală. Conform teoremei fundamentale a teoriei lui Galois, rezultă:

$$H=G\left(K(\xi,\theta)\mid K(\xi)\right)\trianglelefteq G \text{ şi } G/H\simeq G\left(K(\xi)\mid K\right).$$

Conform 2.1. şi 2.2., grupurile *H* şi G/H sunt rezolubile.

Rezultă că *G* este rezolubil. □

2.4. **Teoremă.** *Fie K un corp de caracteristică zero şi* $L\supseteq K$ *o extindere radicală şi normală. Atunci, grupul*

$$G=G\left(L\mid K\right)$$

este rezolubil.

Demonstraţie. Extinderea $L\supseteq K$ este o extindere finită, normală şi separabilă. Suntem în condiţiile aplicării teoremei fundamentale a teoriei lui Galois.

Fie lanţul de extinderi radicale simple:

(1) $$K=K_0\subseteq K_1\subseteq\ldots\subseteq K_s=L.$$

Notăm $H_i=G(L\mid K_i),\ i\in\overline{0,s}$.

$$H_0=G(L\mid K)=G,\ H_s=G(L\mid L)=(e).$$

Deoarece $K_{i-1}\subseteq K_i$ este extindere normală (fiind extindere radicală simplă), $H_i\trianglelefteq H_{i-1},\ i\in\overline{1,s}$. Prin urmare,

(2) $$G=H_0\supseteq H_1\supseteq\ldots\supseteq H_s=(e)$$

este un şir normal al lui *G*. Conform teoremei fundamentale a teoriei lui Galois,

$$H_{i-1}/H_i = G(L \mid K_{i-1})/G(L \mid K_i) \simeq G(K_i \mid K_{i-1}),\ \ i \in \overline{1,s}.$$

Aplicând 2.3., rezultă că H_{i-1}/H_i este grup rezolubil.

Grupul G este rezolubil, deoarece are un şir normal (2) cu factorii grupuri rezolubile. □

3. Ecuații algebrice rezolvabile prin radicali

3.1. **Definiție.** *Fie K un corp comutativ şi $f \in K[X],\ \ d^\circ f \geq 1$.*

O ecuație de forma

(1) $$f(x) = 0$$

se numeşte ***ecuație algebrică*** *peste K.*

În III.7. am văzut că există totdeauna o extindere L a lui K în care ecuația (1) are atâtea soluții cât este gradul lui f.

În acest paragraf urmărim modul de exprimare a rădăcinilor ecuației (1).

3.2. **Definiție.** *Spunem că* ***ecuația algebrică*** (1) ***este rezolvabilă prin radicali*** *dacă există o extindere radicală L a lui K care conține toate rădăcinile lui f.*

Condiția ca ecuația algebrică (1) să fie rezolvabilă prin radicali este echivalentă cu aceea că există o extindere radicală a lui K care include corpul de descompunere al lui f. Conform 1.3., se poate cere ca extinderea să fie radicală şi normală.

Conform celor discutate în VI.1., orice ecuație de gradul doi este rezolvabilă prin radicali.

Ecuațiile algebrice rezolvabile prin radicali se pot caracteriza folosind grupul Galois al corpului de descompunere al polinomului dat.

3.3. **Definiție.** *Fie K corp comutativ şi $f \in K[X],\ \ d^\circ f \geq 1$.*

Fie $L_f \supseteq K$ un corp de descompunere al polinomului f.

Grupul $G_f = G(L_f \mid K)$ poartă numele de ***grup Galois al polinomului f****.*

Aplicând teorema III.7.6., se deduce că grupul Galois al unui polinom este unic determinat, în afara unui izomorfism.

3.4. **Teoremă.** *Fie K corp comutativ de caracteristică zero şi* $f \in K[X]$, *cu* $d^{\circ} f \geq 1$. *Dacă ecuaţia algebrică* (1) *este rezolvabilă prin radicali, atunci grupul Galois al polinomului f este rezolubil.*

Demonstraţie. Fie L_f un corp de descompunere al lui *f*. Deoarece ecuaţia $f(x) = 0$ este rezolvabilă prin radicali, există o extindere radicală şi normală $L \supseteq K$ astfel încât $L \supseteq L_f$.

Conform 2.4., $G(L \mid K)$ este rezolubil. Deoarece $L_f \supseteq K$ este o extindere normală, conform teoremei fundamentale a teoriei lui Galois, rezultă că $H = G(L \mid L_f)$ este subgrup normal în *G* şi

$$G / H = G(L \mid K) / G(L \mid L_f) \simeq G(L_f \mid K) = G_f .$$

Grupul G_f este rezolubil ca grup factor al unui grup rezolubil. □

Conform teoremei 3.4., condiţia ca grupul Galois al polinomului *f* să fie rezolubil este o condiţie necesară ca ecuaţia algebrică (1) să fie rezolvabilă prin radicali.

În continuare, vom arăta că această condiţie este şi suficientă.

3.5. **Lemă.** *Fie K corp comutativ de caracteristică zero şi* $L \supseteq K$ *o extindere finită şi normală, astfel încât* $G(L \mid K)$ *este grup ciclic de ordin n şi K conţine o rădăcină primitivă de grad n a unităţii. Atunci,* $L \supseteq K$ *este o extindere radicală simplă.*

Demonstraţie. Fie $G = G(L \mid K)$ şi σ un generator al său:

$$G = \left\{1_L, \sigma, \sigma^2, ..., \sigma^{n-1}\right\}.$$

Fie $\xi \in K$ o rădăcină primitivă de grad *n* a unităţii. Pentru $p \in \mathbb{Z}$ şi $\alpha \in L$, notăm

(1) $\quad (\xi^p, \alpha) = \alpha + \xi^p \sigma(\alpha) + \xi^{2p} \sigma^2(\alpha) + ... + \xi^{(n-1)p} \sigma^{n-1}(\alpha)$

şi numim această expresie ***p-rezolventa Lagrange asociată lui*** α.

Să observăm că dacă $\alpha \in K$, atunci $\sigma^i(\alpha) = \alpha$, pentru orice *i* şi $(\xi^p, \alpha) = 0$.

Vom demonstra că *dacă* $(\xi, \alpha) \neq 0$, *atunci* α *este un element primitiv al extinderii* $L \supseteq K$, *adică* $L = K(\alpha)$.

Prin reducere la absurd, să presupunem $K(\alpha)\neq L.$ Conform teoremei fundamentale a teoriei lui Galois, $G\left(L\,|\,K(\alpha)\right)\neq(1_K).$ Există deci *d* un divisor pozitiv al lui *n*, $d<n,$ astfel încât

$$G\left(L\,|\,K(\alpha)\right)=(\sigma^d)=\left\{1_L,\sigma^d,\sigma^{2d},...,\sigma^{(m-1)d}\right\},\ \ n=md.$$

$$\sigma^{id}(\alpha)=\alpha,\ \text{pentru orice}\ i\in\overline{0,m-1}.$$

Orice $j\in\overline{0,n-1}$ se scrie $j=id+r$ cu $i\in\overline{0,m-1},\ \ r\in\overline{0,d-1}.$

Reevaluăm (1):

$$(\xi,\alpha)=\sum_{j=0}^{n-1}\xi^j\sigma^j(\alpha)=\sum_{i=0}^{m-1}\sum_{r=0}^{d-1}\xi^{id+r}\sigma^{id+r}(\alpha)=$$

$$=\sum_{r=0}^{d-1}\sum_{i=0}^{m-1}\xi^{id}\xi^r\sigma^r(\alpha)=\sum_{r=0}^{d-1}\xi^r\sigma^r(\alpha)\sum_{i=0}^{m-1}\xi^{id}=0.$$

Ultima egalitate rezultă din

$$\sum_{i=0}^{m-1}\xi^{id}=\frac{\xi^{md}-1}{\xi^d-1}=0$$

şi contrazice ipoteza $(\xi,\alpha)\neq 0.$

Demonstrăm în continuare că *există* $\alpha\in L$ *astfel încât* $(\xi,\alpha)\neq 0.$

Prin reducere la absurd, să presupunem că $(\xi,\alpha)=0,$ pentru orice $\alpha\in L.$ Extinderea $L\supseteq K$ fiind finită şi separabilă, este simplă. Fie θ un element primitiv al său.

În particular, $(\xi,\theta^i)=0,\ \ i\in\overline{0,n-1},$ sau $\sum_{j=0}^{n-1}\xi^j\sigma^j(\theta^i)=0,$ sau:

$$\sum_{j=0}^{n-1}\xi^j\left(\sigma^j(\theta)\right)^i=0,\ \ i\in\overline{0,n-1}. \tag{2}$$

Relaţiile (2) pot fi interpretate ca un sistem liniar şi omogen care admite soluţia nebanală $(1,\xi,\xi^2,...\xi^{n-1}).$ Prin urmare, determinantul său este nul:

$$\Delta = \begin{vmatrix} 1 & 1 & ... & 1 \\ \theta & \sigma(\theta) & ... & \sigma^{n-1}(\theta) \\ ..... & ..... & ... & ..... \\ \theta^{n-1} & \sigma(\theta)^{n-1} & ... & \sigma^{n-1}(\theta)^{n-1} \end{vmatrix}$$

Δ este un determinant Vandermonde şi

$$\Delta = \prod_{0 \le h < k \le n-1} \left(\sigma^k(\theta) - \sigma^h(\theta)\right) = 0.$$

Există h, k, $0 \le h < k \le n-1$, astfel încât $\sigma^k(\theta) = \sigma^h(\theta)$. Deoarece $L = K(\theta)$, rezultă $\sigma^h = \sigma^k$, contradicţie cu $ord\,\sigma = n$.

Fie în continuare $\alpha \in L$ astfel încât $(\xi, \alpha) \neq 0$. Notăm $\beta = (\xi, \alpha)$.

Vom demonstra că $\beta^n \in K$.

Să aplicăm σ relaţiei (1):

$$\sigma\left((\xi^p, \alpha)\right) = \sum_{j=0}^{n-1} \xi^{jp} \sigma^{j+1}(\alpha) = \xi^{-p} \sum_{j=0}^{n-1} \xi^{(j+1)p} \sigma^{j+1}(\alpha) =$$

$$= \xi^{-p} \sum_{j=0}^{n-1} \xi^{jp} \sigma^j(\alpha).$$

Deci,

(3) $$\sigma\left((\xi^p, \alpha)\right) = \xi^{-p}(\xi^p, \alpha), \quad p \in \mathbb{Z}.$$

În particular, pentru $p = 1$,

(4) $$\sigma(\beta) = \xi^{-1}\beta.$$

Ridicând (4) la puterea *p* şi împărţind (prin $\frac{a}{b}$ vom înţelege, ca de obicei ab^{-1}, $b \neq 0$) relaţiile (3) şi (4) rezultă:

$$\sigma\left(\frac{(\xi^p, \alpha)}{\beta^p}\right) = \frac{(\xi^p, \alpha)}{\beta^p}.$$

Cum σ este un generator al lui $G(L \mid K)$, rezultă:

$$\frac{(\xi^p, \alpha)}{\beta^p} = c_p \in K$$

sau:

(5) $$(\xi^p, \alpha) = c_p \beta^p, \quad p \in \mathbb{Z}.$$

Ridicând relația (4) la puterea *n* se obține $\sigma(\beta^n) = \beta^n$ şi, cu acelaşi argument ca mai sus, rezultă:

(6) $$\beta^n = a \in K.$$

Din relațiile (5) rezultă:

$$\sum_{p=0}^{n-1} c_p \beta^p = \sum_{p=0}^{n-1} (\xi^p, \alpha) = \sum_{p=0}^{n-1} \sum_{j=0}^{n-1} \xi^{jp} \sigma^j(\alpha) = \sum_{p=0}^{n-1} \sum_{j=1}^{n-1} \xi^{jp} \sigma^j(\alpha) + n\alpha =$$

$$= \sum_{j=1}^{n-1} \sigma^j(\alpha) \sum_{p=0}^{n-1} \xi^{jp} + n\alpha = n\alpha.$$

Deci

$$n\alpha = \sum_{p=0}^{n-1} c_p \beta^p \in K(\beta).$$

Cum $carK = 0, \ n \cdot 1 \neq 0,$ deci $\alpha \in K(\beta)$. Rezultă

$$L = K(\alpha) \subseteq K(\beta) \subseteq L$$

sau

$$K(\beta) = L.$$

Să considerăm polinomul $f = X^n - a \in K[X]$. Relația (6) arată că β este rădăcină a lui *f*. Cum *K* conține rădăcina primitivă ξ de grad *n* a unității, *L* este corpul de descompunere al lui *f*.

Deci, $L \supseteq K$ este o extindere radicală simplă. □

3.6. **Lemă.** *Fie K un corp de caracteristică zero şi* $L \supseteq K$ *o extindere finită şi normală, al cărei grup Galois este ciclic.*

Atunci, există o extindere $L' \supseteq L$ *astfel încât* $L' \supseteq K$ *este extindere radicală.*

Demonstrație. Fie $G = G(L \mid K)$ şi $n = |G|$. Se observă că, în raport cu lema 3.5., s-a renunțat la ipoteza *K* conține o rădăcină primitivă de grad *n* a unității.

Fie $\overline{K}$ o închidere algebrică a lui *K* astfel încât $L \subseteq \overline{K}$ şi $\xi \in \overline{K}$ o rădăcină primitivă de grad *n* a unității.

Extinderea $K(\xi) \subseteq L(\xi)$ este de asemenea finită şi normală.

Aplicația:

$$\Lambda : G\big(L(\xi) \mid K(\xi)\big) \to G(L \mid K),\ \ \Lambda(\sigma) = \sigma\,|_L,$$

este bine definită şi este un morfism de grupuri.

Dacă $\Lambda(\sigma) = 1_L$, atunci $\sigma = 1_{L(\xi)}$, deci Λ este morfism injectiv.

Ca urmare,

$$G\big(L(\xi) \mid K(\xi)\big)$$

este izomorf cu un subgrup al unui grup ciclic de ordin *n*.

Deci, $G\big(L(\xi) \mid K(\xi)\big)$ este grup ciclic de ordin *d*, $d \mid n$, $n = md$, $m \in \mathbb{N}^*$. Atunci, $\xi^m \in K(\xi)$ este o rădăcină primitivă de ordin *d* a unității. Din lema 3.5., rezultă că $L(\xi) \supseteq K(\xi)$ este o extindere radicală simplă. Cum

$$L(\xi) \supseteq K(\xi) \supseteq K \text{ şi } L(\xi) \supseteq L$$

rezultă că $L(\xi)$ este o extindere radicală a lui *K* şi $L(\xi) \supseteq L$.

Se poate lua $L' = L(\xi)$ şi lema este demonstrată. □

3.7. **Teoremă.** *Fie K un corp de caracteristică zero şi* $L \supseteq K$ *o extindere finită şi normală, astfel încât* $G(L \mid K)$ *este rezolubil.*

Atunci, există o extindere $L' \supseteq L$ *astfel încât* $L' \supseteq K$ *este extindere radicală.*

Demonstrație. Fie $G = G(L \mid K)$. Conform ipotezei, *G* este finit şi rezolubil. Prin urmare admite un şir normal ai cărui factori sunt grupuri ciclice. Fie acesta

(7) $$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_s = (e).$$

Să notăm $K_i = L^{H_i}$, $i \in \overline{0,s}$. $K_{i-1} \subseteq K_i$, $i \in \overline{1,s}$.

$$K_0 = L^{H_0} = L^{G(L|K)} = K,\ \ K_s = L^{H_s} = L^{(e)} = L.$$

Se obține următorul lanț de corpuri intermediare:

(8) $$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = L.$$

Conform teoremei fundamentale a teoriei lui Galois, din $H_i \trianglelefteq H_{i-1}$, rezultă $K_i \supseteq K_{i-1}$ extindere normală (şi finită) şi:

$G(K_i \mid K_{i-1}) \simeq G(L \mid K_{i-1}) / G(L \mid K_i) = H_{i-1} / H_i$ grup ciclic, $i \in \overline{1,s}$.

Vom demonstra teorema prin inducție după *s*.

Pentru $s = 1$, afirmația se obține din lema 3.6.

Să presupunem afirmația adevărată pentru valoarea $s-1$.

Conform ipotezei de inducție, există o extindere $L_1 \supseteq K_{s-1}$ astfel încât $L_1 \supseteq K$ este extindere radicală. Procedând ca în demonstrația lemei 3.6., se arată că $G(LL_1 \mid L_1)$ este izomorf cu un subgrup al lui $G(L \mid K_{s-1})$, deci este ciclic. Conform lemei 3.6., există o extindere $L' \supseteq LL_1$ astfel încât $L' \supseteq L_1$ este o extindere radicală. Din $L' \supseteq L_1$ şi $L_1 \supseteq K$ extinderi radicale, rezultă $L' \supseteq K$ extindere radicală. Evident, $L' \supseteq L$ şi teorema este demonstrată. □

3.8. **Teoremă.** *Fie K un corp de caracteristică zero şi* $f \in K[X]$, $d^\circ f = n \geq 1$. *Dacă grupul Galois* G_f *al polinomului f este rezolubil, atunci ecuația algebrică*

$$f(x) = 0$$

este rezolvabilă prin radicali.

Demonstrație. Fie L_f un corp de descompunere al lui *f*. Conform ipotezei, $G_f = G(L_f \mid K)$ este rezolubil. Extinderea $L_f \supseteq K$ este normală şi finită.

Conform teoremei 3.7., există o extindere $L' \supseteq L_f$ astfel încât $L' \supseteq K$ este extindere radicală. Prin urmare, ecuația $f(x) = 0$ este rezolvabilă prin radicali. □

Rezultatele anterioare pot fi reunite în următoarea teoremă:

3.9. **Teorema fundamentală asupra rezolvării ecuațiilor algebrice prin radicali.**

Fie K un corp de caracteristică zero şi $f \in K[X]$, $d^\circ f = n \geq 1$. *Ecuația algebrică*:

$$f(x) = 0$$

este rezolvabilă prin radicali, dacă şi numai dacă grupul Galois al polinomului f este rezolubil.

4. Ecuația generală de grad *n*

Fie K un corp de caracteristică zero şi $t_1, t_2, ..., t_n$, n nedeterminate care nu aparţin lui K. Fie:

$$f = X^n - t_1 X^{n-1} + t_2 X^{n-2} - ... + (-1)^n t_n \in K(t_1, t_2, ..., t_n)[X].$$

Ecuația $f(x) = 0$ se numeşte ***ecuație generală de grad n***.

4.1. **Teoremă.** *Cu notațiile de mai sus, polinomul f este ireductibil şi grupul său Galois este izomorf cu* $\mathscr{S}_n$.

Demonstrație. Fie $X_1, X_2, ..., X_n$, n nedeterminate peste K şi

$$f_0 = \prod_{i=1}^{n} (X - X_i) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - ... + (-1)^n s_n$$

unde $s_1, s_2, ..., s_n$ sunt polinoamele simetrice fundamentale în nedeterminatele $X_1, X_2, ..., X_n$. $f_0 \in K(s_1, s_2, ..., s_n)[X]$.

Arătăm că polinomul f_0 este ireductibil. Să presupunem că există $g, h \in K(s_1, s_2, ..., s_n)[X]$, astfel încât $f = gh$ şi $1 \le d^\circ g < n$. Există $i_1, i_2, ..., i_k$ astfel încât $1 \le i_1 < ... < i_k \le n$, $1 \le k < n$ şi

$$g = (X - X_{i_1})...(X - X_{i_k}) =$$
$$= X^k - (X_{i_1} + ... + X_{i_k}) X^{k-1} + ... + (-1)^n X_{i_1} ... X_{i_k}.$$

Rezultă $X_{i_1} ... X_{i_k} \in K(s_1, s_2, ..., s_n)$, contradicție.

Deoarece rădăcinile lui f_0 sunt $X_1, X_2, ..., X_n$, corpul de descompunere al lui f_0 este

$$K(s_1, s_2, ..., s_n)(X_1, ..., X_n) = K(X_1, ..., X_n).$$

Prin urmare, extinderea

$$K(X_1, ..., X_n) \supseteq K(s_1, s_2, ..., s_n)$$

este o extindere normală şi finită.

Notăm $L = K(X_1, ..., X_n)$ şi $F = K(s_1, s_2, ..., s_n)$.

Fie $\sigma \in \mathscr{S}_n$. Definim $\sigma^* : L \to L$ prin:

$$\sigma^*\left(\frac{g(X_1, X_2, ..., X_n)}{h(X_1, X_2, ..., X_n)}\right) = \frac{g(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)})}{h(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)})}, \quad \forall \frac{g}{h} \in L.$$

Aplicația σ^* este bine definită şi este chiar un morfism de corpuri. Din relațiile:

$$e^* = 1_L \text{ şi } (\sigma \circ \tau)^* = \sigma^* \circ \tau^*,$$

rezultă că există $(\sigma^*)^{-1} = (\sigma^{-1})^*$. Prin urmare, σ^* este un automorfism al lui *L*.

Fie

$$G = \left\{ \sigma^* \,\middle|\, \sigma \in \mathrm{S}_n \right\}.$$

G este un grup de automorfisme ale lui *L* care invariază corpul *F*.

Rezultă $G \subseteq G(L \mid F)$.

Din teorema fundamentală a polinoamelor simetrice, rezultă:

$$L^G = \left\{ \frac{g}{h} \in L \,\middle|\, \sigma^*\left(\frac{g}{h}\right) = \frac{g}{h},\ \forall \sigma^* \in G \right\} = K(s_1, ..., s_n) = F.$$

Din teorema fundamentală a teoriei lui Galois, rezultă:

$$G_{f_0} = G(L \mid F) = G(L \mid L^G) = G.$$

Aplicația:

$$\mathscr{S}_n \to G,\ \ \sigma \to \sigma^*,\ \ \forall \sigma \in \mathscr{S}_n,$$

este un izomorfism.

Prin urmare, $G_{f_0} \simeq \mathscr{S}_n$.

În continuare, vom transpune aceste proprietăți de la f_0 la *f*.

Fie $y_1, y_2, ..., y_n$, rădăcinile lui *f* într-o extindere a lui $K(t_1, t_2, ..., t_n)$. Rezultă:

$$\begin{aligned} t_1 &= y_1 + ... + y_n \\ t_2 &= \sum_{1 \le i < j \le n} y_i y_j \\ &\vdots \\ t_n &= y_1 ... y_n \end{aligned}$$

Corpul de descompunere al polinomului *f* este:

$$K(t_1, t_2, ..., t_n)(y_1, y_2, ..., y_n) = K(y_1, y_2, ..., y_n).$$

Fie aplicația:

$$\alpha : K(t_1, t_2, ..., t_n) \to K(s_1, s_2, ..., s_n),$$

$$\alpha\left(\frac{g(t_1,t_2,...,t_n)}{h(t_1,t_2,...,t_n)}\right)\overset{def}{=}\frac{g(s_1,s_2,...,s_n)}{h(s_1,s_2,...,s_n)},\quad \forall\frac{g}{h}\in K(t_1,t_2,...,t_n).$$

Aplicația α este bine definită. Se arată uşor că α este chiar un izomorfism de corpuri.

Fie

$$\overline{\alpha}: K(t_1,t_2,...,t_n)[X]\to K(s_1,s_2,...,s_n)[X],$$

unicul izomorfism care extinde α şi pentru care $\overline{\alpha}(X)=X$.

Din $\overline{\alpha}(f)=f_0$, rezultă că f este ireductibil. Din III.7.5., rezultă că există un izomorfism al corpurilor de descompunere ale polinoamelor f şi f_0:

$$\beta: K(y_1,y_2,...,y_n)\to K(X_1,...,X_n)$$

care prelungeşte pe α.

Considerăm diagrama:

$$\begin{array}{ccc} K(y_1,...,y_n) & \xrightarrow{\quad\lambda\quad} & K(y_1,...,y_n) \\ \beta^{-1}\uparrow & & \downarrow\beta \\ K(X_1,...,X_n) & \xrightarrow{\beta\circ\lambda\circ\beta^{-1}} & K(X_1,...,X_n) \end{array}$$

unde $\lambda\in G\big(K(y_1,y_2,...,y_n)\,|\,K(t_1,t_2,...,t_n)\big)$. Rezultă:

$$\beta\circ\lambda\circ\beta^{-1}\in G\big(K(X_1,X_2,...,X_n)\,|\,K(s_1,s_2,...,s_n)\big).$$

Aplicația:

$$G\big(K(y_1,y_2,...,y_n)\,|\,K(t_1,t_2,...,t_n)\big)\to G(L\,|\,F),\ \ \lambda\to\beta\circ\lambda\circ\beta^{-1}$$

este un izomorfism de grupuri. Rezultă:

$$G_f\simeq G_{f_0}\simeq\mathscr{S}_n.\quad\square$$

4.2. **Teorema lui Abel şi Ruffini.** *Ecuația generală de grad n, $n\geq 5$ nu este rezolvabilă prin radicali.*

Demonstrație. Rezultă din teorema fundamentală 3.9. privind rezolvarea ecuațiilor prin radicali, din 4.1. şi din faptul că grupul permutărilor de grad $n\geq 5$ nu este rezolubil. $\square$

4.3. **Observaţie.** Invocând aceleaşi teoreme şi faptul că grupul permutărilor de grad $n \le 4$ este rezolubil, deducem că ecuaţia generală de grad $n \le 4$ este rezolvabilă prin radicali.

5. Construcţii cu rigla şi compasul

În geometria elementară, în problemele de construcţii geometrice se dau un număr finit de puncte, drepte, unghiuri şi cercuri şi se cer elemente de aceeaţi natură. Având în vedere că o dreaptă este determinată de două puncte ale sale, un unghi este determinat de trei puncte (vârful său şi două puncte situate pe laturi) şi un cerc este determinat de centrul său şi un punct de pe circumferinţă, putem considera că toate elementele date sunt puncte. *Operaţiile admise* pentru determinarea elementelor cerute sunt *intersecţii de drepte şi* (*sau*) *cercuri* determinate de punctele deja cunoscute. Este motivul pentru care se vorbeşte despre *construcţii cu rigla şi compasul*.

Considerăm cunoscute următoarele construcţii din geometria elementară:

- construcţia mediatoarei unui segment;
- construcţia bisectoarei unui unghi;
- construcţia perpendicularei într-un punct al unei drepte sau dintr-un punct pe o dreaptă;
- construcţia paralelei la o dreaptă printr-un punct exterior dreptei.

În continuare vom arăta că se pot stabili condiţii necesare şi suficiente de *constructibilitate* folosind elemente de teorie Galois.

Fie π un plan şi $P_1, P_2, ..., P_r$ puncte fixate în plan, $r \in \mathbb{N}^*$. Definim un şir de mulţimi $\left(\mathcal{M}_n\right)_{n \ge 1}$, astfel:

a) $\mathcal{M}_1 = \{P_1, P_2, ..., P_r\}$;

b) Pentru orice $k \ge 1$, mulţimea $\mathcal{M}_{k+1}$ se obţine din $\mathcal{M}_k$, la care se adaugă puncte rezultate prin:

b1) Intersecţia a două drepte. Fiecare din cele două drepte este determinată de două puncte ale mulţimii $\mathcal{M}_k$;

b2) Intersecția dintre o dreaptă şi un cerc. Dreapta este determinată de două puncte din $\mathcal{M}_k$. Cercul are centrul într-un punct al lui $\mathcal{M}_k$ şi raza egală cu distanța între două puncte ale lui $\mathcal{M}_k$.

b3) Intersecția a două cercuri definite ca la b2).

Notăm:

(1) $$\mathcal{C}(P_1, P_2, ..., P_r) = \bigcup_{n=1}^{\infty} \mathcal{M}_n.$$

Un punct $P \in \mathcal{C}(P_1, P_2, ..., P_r)$ se spune că este ***constructibil cu rigla şi compasul din punctele*** $P_1, P_2, ..., P_r$.

Dacă $r = 1$, $\mathcal{M}_n = \{P_1\}$, pentru orice $n \in \mathbb{N}^*$ şi problema nu prezintă interes.

Mai departe, vom presupune $r \geq 2$.

În planul π vom fixa un sistem de coordonate carteziene xOy, astfel:

- Punctul P_1 este originea sistemului de coordonate:
- Punctul P_2 are coordonatele $(1, 0)$.

În acest mod, axa Ox are ca suport dreapta P_1P_2, P_1 este originea, P_2 se află pe semiaxa pozitivă, distanța dintre P_1 şi P_2 este luată ca unitate de măsură. Axa Oy este perpendiculară pe dreapta P_1P_2 în punctul P_1.

Fie:

(2) $$\theta : \pi \to \mathbb{C},$$

definită prin:

$$\theta\big(M(x, y)\big) = x + iy, \quad \forall M(x, y) \in \pi.$$

Aplicația θ este o bijecție.

Notăm $\theta(P_i) = z_i$, pentru orice $i \in \overline{1, r}$.

$$z_1 = \theta\big(P_1(0, 0)\big) = 0, \quad z_2 = \theta\big(P_2(1, 0)\big) = 1.$$

Fie:

$$\mathcal{C}(z_1, z_2, ..., z_r) = \theta\big(\mathcal{C}(P_1, P_2, ..., P_r)\big).$$

Un număr complex $z \in \mathscr{C}(z_1, z_2, ..., z_r)$ se spune că este ***construc-tibil cu rigla şi compasul din numerele complexe*** $z_1, z_2, ..., z_r$.

5.1. **Teoremă.** *Mulțimea* $\mathscr{C}(z_1, z_2, ..., z_r)$ *are proprietățile:*

a) *este subcorp al lui* $\mathbb{C}$;

b) *este închisă la conjugare, adică:*

$$\forall z \in \mathbb{C},\ z \in \mathscr{C}(z_1, z_2, ..., z_r) \Rightarrow \overline{z} \in \mathscr{C}(z_1, z_2, ..., z_r);$$

c) *este închisă la radicali de ordinul doi, adică:*

$$\forall z \in \mathbb{C},\ z \in \mathscr{C}(z_1, z_2, ..., z_r) \Rightarrow \sqrt{z}_{1,2} \in \mathscr{C}(z_1, z_2, ..., z_r);$$

d) *este cel mai mic subcorp al lui* $\mathbb{C}$ *care conține* $z_1, z_2, ..., z_r$ *şi este închis la conjugare şi la radicali de ordinul doi.*

Demonstrație. a) Evident, $\{z_1, z_2, ..., z_r\} \subseteq \mathscr{C}(z_1, z_2, ..., z_r)$.

Fie $z', z'' \in \mathscr{C}(z_1, z_2, ..., z_r)$. Atunci,

$z' = \theta(M'),\ z'' = \theta(M'')$, unde $M', M'' \in \mathscr{C}(P_1, P_2, ..., P_r)$.

Dacă $M \in \pi$, astfel încât $P_1M'MM''$ este paralelogram, atunci $\theta(M) = z' + z''$. Este uşor de arătat că $M \in \mathscr{C}(P_1, P_2, ..., P_r)$. Rezultă:

$$z' + z'' \in \mathscr{C}(z_1, z_2, ..., z_r).$$

Dacă N este simetricul lui M' față de P_1, atunci $\theta(N) = -z'$. Este uşor de arătat că $N \in \mathscr{C}(P_1, P_2, ..., P_r)$. Rezultă

$$-z' \in \mathscr{C}(z_1, z_2, ..., z_r).$$

Pentru închiderea la produs, apelăm la forma trigonometrică.

Fie $z' = \rho'(\cos t' + i \sin t')$, $z'' = \rho''(\cos t'' + i \sin t'')$. Atunci,

$$z'z'' = \rho'\rho''\big(\cos(t' + t'') + i \sin(t' + t'')\big).$$

Dacă $M \in \pi$ astfel încât $\theta(M) = z'z''$, atunci, raționând ca în manualele de liceu, se deduce că $M \in \mathscr{C}(P_1, P_2, ..., P_r)$.

Rezultă:

$$z'z'' \in \mathscr{C}(z_1, z_2, ..., z_r).$$

Dacă $z' \neq 0$, atunci, ținând seama că

$$\frac{1}{z'} = \frac{1}{\rho'}\big(\cos(-t') + i \sin(-t')\big),$$

se deduce analog că $(z')^{-1} \in \mathscr{C}(z_1, z_2, ..., z_r)$.

Prin urmare, $\mathscr{C}(z_1, z_2, ..., z_r)$ este subcorp al lui $\mathbb{C}$.

b) Fie $z \in \mathscr{C}(z_1, z_2, ..., z_r)$ şi $M \in \mathscr{C}(P_1, P_2, ..., P_r)$, cu $z = \theta(M)$.

Dacă M' este simetricul lui M faţă de Ox, atunci $\theta(M') = \bar{z}$. Se deduce uşor că $M' \in \mathscr{C}(P_1, P_2, ..., P_r)$. Rezultă

$$\bar{z} \in \mathscr{C}(z_1, z_2, ..., z_r).$$

c) Fie $z \in \mathscr{C}(z_1, z_2, ..., z_r)$ şi $M \in \mathscr{C}(P_1, P_2, ..., P_r)$, unde $z = \theta(M)$.

Dacă $z = \rho(\cos t + i \sin t)$, atunci una din valorile lui $\sqrt{z}$ este $\sqrt{\rho}\left(\cos\frac{t}{2} + i \sin\frac{t}{2}\right)$ (cealaltă este opusa acesteia). Apelând din nou la un raţionament din manualul de liceu, se deduce că punctul $P \in \pi$, astfel încât $\theta(P) = \sqrt{\rho}\left(\cos\frac{t}{2} + i \sin\frac{t}{2}\right)$, aparţine lui $\mathscr{C}(P_1, P_2, ..., P_r)$. Rezultă

$$\sqrt{z}_{1,2} \in \mathscr{C}(z_1, z_2, ..., z_r).$$

d) Fie K un subcorp al lui $\mathbb{C}$ care conţine $z_1, z_2, ..., z_r$ şi este închis la conjugare şi la radicali de ordinul doi.

$$1 \in K \Leftrightarrow -1 \in K \Rightarrow \sqrt{-1} = \pm i \in K.$$

Fie $z = a + bi \in K$. $\bar{z} = a - bi \in K$.

Deoarece K este subcorp al lui $\mathbb{C}$, rezultă:

$$a = \frac{1}{2}(z + \bar{z}) \in K, \quad b = \frac{1}{2i}(z - \bar{z}) \in K.$$

Deducem că, pentru orice $a, b \in \mathbb{R}$, $a + bi \in K \Leftrightarrow a, b \in K$.

Trebuie să demonstrăm relaţia $\mathscr{C}(z_1, z_2, ..., z_r) \subseteq K$. Dar,

$$\mathscr{C}(z_1, z_2, ..., z_r) = \bigcup_{n=1}^{\infty} \theta\left(\mathscr{M}_n\right).$$

Demonstrăm prin inducţie după n că $\theta\left(\mathscr{M}_n\right) \subseteq K$.

Pentru $n = 1$, $\theta\left(\mathscr{M}_1\right) = \{z_1, z_2, ..., z_r\} \subseteq K$, din ipoteză.

Presupunem $\theta\left(\mathscr{M}_k\right) \subseteq K$, pentru un anumit $k \in \mathbb{N}^*$.

Fie $M \in \mathcal{M}_{k+1}$, obținut ca la b1): $\{M\} = d_1 \cap d_2$.

Fie $N_1(a_1,b_1), N_2(a_2,b_2) \in \mathcal{M}_k$ care determină d_1. Conform ipotezei de inducție, $a_1,b_1,a_2,b_2 \in K$. Ecuația lui d_1 este:

$$\frac{x-a_1}{a_2-a_1} = \frac{y-b_1}{b_2-b_1} \text{ sau } ax+by+c=0$$

unde $a,b,c \in K$ (deoarece K este subcorp al lui $\mathbb{C}$).

În mod asemănător, ecuația lui d_2 este

$$a'x+b'y+c'=0$$

unde $a',b',c' \in K$.

Coordonatele lui M sunt soluția (x_0,y_0) a sistemului:

$$\begin{cases} ax+by+c=0 \\ a'x+b'y+c'=0. \end{cases}$$

Deoarece K este subcorp al lui $\mathbb{C}$, x_0 şi y_0 aparțin lui K şi

$$\theta(M) = x_0 + iy_0 \in K.$$

Fie acum $M \in d \cap \Gamma$ unde d este o dreaptă determinată de două puncte din $\mathcal{M}_k$ şi Γ este un cerc cu centrul într-un punct $C \in \mathcal{M}_k$, de rază $r = AB$, cu $A,B \in \mathcal{M}_k$. Ecuația lui d este de forma:

$$ax+by+c=0,\ a,b,c \in K.$$

Ecuația lui Γ este de forma:

$$x^2+y^2+mx+ny+p=0,\ m,n,p \in K.$$

Coordonatele (x_0,y_0) ale punctului M verifică sistemul

$$\begin{cases} ax+by+c=0 \\ x^2+y^2+mx+ny+p=0. \end{cases}$$

Deoarece K este închis la radicali de ordinul doi, rezultă $x_0,y_0 \in K$, deci $\theta(M) = x_0 + iy_0 \in K$.

Fie $M \in \Gamma \cap \Gamma'$ unde Γ şi Γ' sunt două cercuri determinate ca mai sus, de ecuații:

$$x^2+y^2+mx+ny+p=0,\ m,n,p \in K.$$
$$x^2+y^2+m'x+n'y+p'=0,\ m',n',p' \in K.$$

Deoarece corpul K este închis la radicali de ordinul doi, rezultă că, coordonatele x_0, y_0 ale lui M aparţin lui K, deci $\theta(M) \in K$.

În final, $\theta\left(\mathscr{M}_{k+1}\right) \subseteq K$. Deci, $\mathscr{C}(z_1, z_2, ..., z_r) \subseteq K$. □

Conform a), b) şi d) din 5.1., mulţimea $\mathscr{C}(z_1, z_2, ..., z_r)$ a numerelor complexe constructibile cu rigla şi compasul include corpul:

$$F = \mathbb{Q}(z_1, z_2, ..., z_r; \overline{z_1}, \overline{z_2}, ..., \overline{z_r}).$$

Conform c) din 5.1., dacă $E \subseteq \mathscr{C}(z_1, z_2, ..., z_r)$ şi $E' \supseteq E$ este o extindere finită de gradul doi, atunci $E' \subseteq \mathscr{C}(z_1, z_2, ..., z_r)$.

Putem deduce o nouă caracterizare a lui $\mathscr{C}(z_1, z_2, ..., z_r)$.

5.2. **Teoremă.** $z \in \mathscr{C}(z_1, z_2, ..., z_r)$ *dacă şi numai dacă:*

(*) *există extinderile* $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_m$, *astfel încât:*

$$[F_i : F_{i-1}] \leq 2, \ i \in \overline{1,m}, \text{ şi } z \in F_m.$$

Demonstraţie. Notăm cu E mulţimea numerelor complexe z care au proprietatea (*).

Folosind teorema 5.1., printr-un raţionament prin inducţie după m, rezultă $F_m \subseteq \mathscr{C}(z_1, z_2, ..., z_r)$. Deci, $E \subseteq \mathscr{C}(z_1, z_2, ..., z_r)$.

Vom demonstra şi incluziunea inversă.

Fie $z, z' \in E$. Există extinderile:

$$(4) \qquad F = F_0 \subseteq F_1 \subseteq ... \subseteq F_m, \ [F_i : F_{i-1}] \leq 2, \ i \in \overline{1,m}, \ z \in F_m.$$

$$F = E_0 \subseteq E_1 \subseteq ... \subseteq E_s, \ [E_i : E_{i-1}] \leq 2, \ i \in \overline{1,s}, \ z' \in E_s.$$

Rezultă $[F_m E_i : F_m E_{i-1}] \leq 2, \ i \in \overline{1,s}$ şi există extinderile:

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_m = F_m E_0 \subseteq F_m E_1 \subseteq ... \subseteq F_m E_s.$$

Din $z, z' \in F_m E_s$ şi $F_m E_s$ corp, rezultă $z - z', zz', z^{-1} \in F_m E_s$ $(z \neq 0)$. Deci, $z - z', zz', z^{-1} \in E$ şi, ca urmare, E este un subcorp al lui $\mathbb{C}$.

Raţionând prin inducţie după m, se deduce că E este închisă la conjugare.

Fie $z \in E$. Există extinderile de forma (4). Notăm $F_{m+1} = F_m\left(\sqrt{z}\right)$. $[F_{m+1} : F_m] \leq 2$. Rezultă $\sqrt{z} \in E$, adică E este închis la radicali de or-

dinul doi. Evident, $E \supseteq \{z_1, z_2, ..., z_r\}$. Conform teoremei 5.1., rezultă $\mathscr{C}(z_1, z_2, ..., z_r) \subseteq E$. În final, $\mathscr{C}(z_1, z_2, ..., z_r) = E$. □

5.3. **Consecinţă.** *Dacă numărul complex z este constructibil cu rigla şi compasul din* $z_1, z_2, ..., z_r$, *atunci z este algebric peste*

$$F = \mathbb{Q}(z_1, z_2, ..., z_r; \overline{z_1}, \overline{z_2}, ..., \overline{z_r}).$$

şi $d^\circ p_z = 2^t$, *pentru un anumit* $t \in \mathbb{N}$.

Demonstraţie. Fie $z \in \mathscr{C}(z_1, z_2, ..., z_r)$. Există extinderile de forma (4). Extinderea $F_m \supseteq F$ este finită, deci algebrică. Elementul $z \in F_m$ este algebric peste *F*. Din relaţiile:

$$F \subseteq F(z) \subseteq F_m \text{ şi } [F(z) : F] = d^\circ p_z$$

rezultă

$$d^\circ p_z \mid [F_m : F] = \prod_{i=1}^{m} [F_i : F_{i-1}] = 2^s, \quad s \le m.$$

Prin urmare, $d^\circ p_z = 2^t$, $t \le s$. □

Cu ajutorul consecinţei 5.3. vom trata câteva probleme celebre de construcţii cu rigla şi compasul.

5.4. **Problema dublării cubului.** Enunţul acestei probleme este următorul: "*Fiind dat un cub cu latura l*, *să se construiască* (*cu rigla şi compasul*) *un cub de volum dublu*."

Putem lua ca unitate de măsură latura *l* a cubului dat, $l = 1$.

În acest caz, $z_1 = 0$, $z_2 = 1$, $F = \mathbb{Q}\left(0,1;\overline{0},\overline{1}\right) = \mathbb{Q}$. Cubul de volum dublu are latura $l' = \sqrt[3]{2}$. Dar $\sqrt[3]{2}$ nu este constructibil cu rigla şi compasul din 0 şi 1 deoarece polinomul său minimal peste $\mathbb{Q}$ este $X^3 - 2$, al cărui grad nu este o putere a lui 2. Prin urmare, nu se poate construi cu rigla şi compasul, un cub cu volumul egal cu dublul volumului cubului dat. □

5.5. **Problema cuadraturii cercului.** Enunţul acestei probleme este următorul: "*Fiind dat un cerc*, *să se construiască* (*cu rigla şi compasul*) *un pătrat cu aceeaşi arie ca şi cercul*."

Vom lua ca unitate de măsură raza cercului. $r = 1$.

În acest caz, $z_1 = 0,\ z_2 = 1,\ F = \mathbb{Q}$. Pătratul cu aceeaşi arie cu cercul dat are latura $l = \sqrt{\pi}$. Dar $\sqrt{\pi}$ nu este constructibil cu rigla şi compasul din 0 şi 1 deoarece $\sqrt{\pi}$ nu este număr algebric peste $\mathbb{Q}$. Prin urmare, nu se poate construi cu rigla şi compasul, un pătrat cu aceeaşi arie cu cercul dat. □

5.6. **Problema trisecțiunii unghiului.** Enunțul acestei probleme este următorul: "*Fiind dat un unghi oarecare*, *să se împartă acest unghi* (*cu rigla şi compasul*) *în trei părți egale*."

Vom arăta că nici această construcție, în caz general, nu se poate realiza cu rigla şi compasul. Este suficient să arătăm că unghiul de $\frac{\pi}{3}$ nu se poate împărți, cu rigla şi compasul, în trei părți egale.

Unghiul de $\frac{\pi}{3}$ este determinat de trei puncte care formează un triunghi echilateral. În acest caz,

$$P_1(0,0), P_2(1,0), P_3\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right);$$

$$z_1 = 0, z_2 = 1, z_3 = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Împărțirea unghiului $\measuredangle P_2P_1P_3$ în trei părți egale revine la construcția punctului $P\left(\cos\frac{\pi}{9}, \sin\frac{\pi}{9}\right)$. Notăm $z = \cos\frac{\pi}{9} + i\sin\frac{\pi}{9}$.

Trebuie stabilit dacă $z \in \mathscr{C}(z_1, z_2, z_3)$. Deoarece $z_3 \in \mathscr{C}(z_1, z_2)$, este echivalent cu a stabili dacă $z \in \mathscr{C}(z_1, z_2)$. Şi în acest caz, $F = \mathbb{Q}$.

Din relația $\cos 3t = 4\cos^3 t - 3\cos t$, înlocuind $t = \frac{\pi}{9}$, rezultă:

$$4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} - \frac{1}{2} = 0,$$

sau $\cos\frac{\pi}{9}$ este rădăcină a polinomului

$$f = X^3 - \frac{3}{4}X - \frac{1}{8} \in \mathbb{Q}[X].$$

Deoarece *f* este ireductibil, rezultă că *f* este polinomul minimal al lui $\cos\frac{\pi}{9}$. Din 5.3., rezultă că $\cos\frac{\pi}{9} \notin \mathscr{C}(z_1, z_2)$.

Prin urmare, $z \notin \mathscr{C}(z_1, z_2)$. □

Din teorema 5.2., rezultă: condiţia ca *z* să aparţină unei extinderi de grad 2^t, $t \in \mathbb{N}$ a lui $F = \mathbb{Q}(z_1, z_2, ..., z_r; \overline{z_1}, \overline{z_2}, ..., \overline{z_r})$ este o condiţie necesară ca *z* să fie constructibil cu rigla şi compasul din $z_1, z_2, ..., z_r$. Vom arăta că este şi o condiţie suficientă.

5.7. **Lemă.** *Fie* $L \supseteq K$ *o extindere normală de subcorpuri ale lui* $\mathbb{C}$, *de grad* 2^t, $t \in \mathbb{N}^*$. *Atunci există extinderile*

(5) $\quad K = K_0 \subseteq K_1 \subseteq ... \subseteq K_t = L,\ [K_i : K_{i-1}] = 2,\ i \in \overline{1,t}.$

Demonstraţie. Deoarece extinderea $L \supseteq K$ este finită, normală şi separabilă,

$$\left|G(L \mid K)\right| = [L : K] = 2^t.$$

Notăm $G = G(L \mid K)$. Din exerciţiul IV.2., rezultă că *G* este rezolubil. Din IV.5.1., rezultă că *G* are un şir normal cu factorii ciclici. Factorii acestui şir normal au ordinele egale cu puteri ale lui 2. Se poate rafina acest şir normal, astfel încât toţi factorii să aibă ordinul doi. Deci există şirul normal:

$$G = H_0 \supseteq H_1 \supseteq ... \supseteq H_t = (e)$$

astfel încât $\left|H_{i-1} / H_i\right| = 2,\ i \in \overline{1,t}.$

Fie $K_i = L^{H_i},\ i \in \overline{0,t}.$

$$K_0 = L^G = K,\ K_t = L^{(e)} = L,\ K_{i-1} \subseteq K_i,\ i \in \overline{1,t}.$$

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_t = L,$$

Din teorema fundamentală a teoriei lui Galois, rezultă:

$$[K_i : K_{i-1}] = \left|G(K_i \mid K_{i-1})\right| = \frac{\left|G(L \mid K_{i-1})\right|}{\left|G(L \mid K_i)\right|} = \frac{\left|H_{i-1}\right|}{\left|H_i\right|} = 2,\ i \in \overline{1,t}.$$ □

5.8. **Teoremă.** *Numărul complex z este constructibil cu rigla şi compasul din numerele complexe* $z_1, z_2, ..., z_r$, *dacă şi numai dacă există o extindere normală* $L \supseteq F$, $F = \mathbb{Q}(z_1, z_2, ..., z_r; \overline{z_1}, \overline{z_2}, ..., \overline{z_r})$, *de grad egal cu o putere a lui 2, care conţine z.*

Demonstraţie. Să presupunem că *z* este constructibil cu rigla şi compasul din $z_1, z_2, ..., z_r$. Conform teoremei 5.2., există extinderile

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_m, \ [F_i : F_{i-1}] \leq 2, \ i \in \overline{1,m}, \ z \in F_m.$$

Repetând raţionamentul din teorema 1.3., rezultă că există extinderile

$$F_m \subseteq F_{m+1} \subseteq ... \subseteq F_{m+q}, \ [F_j : F_{j-1}] \leq 2, \ j \in \overline{m+1, m+q}$$

astfel încât $F_{m+q} \supseteq F$ este o extindere normală.

Putem lua $L = F_{m+q}$.

Reciproc, să presupunem că există $L \supseteq F$, o extindere normală de grad 2^t, care conţine *z*. Din lema 5.7., rezultă că există extinderile de forma (5). Din teorema 5.2., rezultă $z \in \mathscr{C}(z_1, z_2, ..., z_r)$. □

6. Construcţia poligoanelor regulate

Considerăm cunoscute construcţiile cu rigla şi compasul pentru: triunghiul echilateral, pătrat şi hexagonal regulat. Se pune problema de a caracteriza numerele naturale $n \geq 3$ pentru care poligonul regulat cu *n* laturi se poate construi cu rigla şi compasul.

6.1. **Teoremă.** *Poligonul regulat cu n laturi este constructibil cu rigla şi compasul dacă şi numai dacă n este de forma*:

(1) $$n = 2^{\alpha} p_1 p_2 ... p_s$$

unde $\alpha \in \mathbb{N}$ *şi* $p_1, p_2, ... p_s$ *sunt numere prime ale lui Fermat.*

Demonstraţie. În acest caz, $z_1 = 0, z_2 = 1, F = \mathbb{Q}$. Problema se reduce la construcţia poligonului regulat cu *n* laturi, înscris în cercul cu centrul în P_1, de rază $P_1P_2 = 1$. Dacă unul din vârfuri este plasat în $P_2(1,0)$, atunci următorul este plasat în $P\left(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}\right)$.

Problema revine la constructibilitatea lui $\xi = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ cu rigla şi compasul din z_1 şi z_2.

Dar ξ este rădăcină primitivă de grad *n* a unității, al cărei polinom minimal este F_n, de grad $\varphi(n)$ (vezi V.3.).

Fie $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$; cu $p_1, \ldots p_s$ numere prime distincte ≥ 3 şi $\alpha_i \in \mathbb{N}^*$, $i \in \overline{1,s}$.

$$\varphi(n) = 2^{\alpha-1} p_1^{\alpha_1-1}(p_1-1)\ldots p_s^{\alpha_s-1}(p_s-1).$$

Să presupunem ξ constructibil cu rigla şi compasul. Din 5.3., rezultă că $d^{\circ}F_n = \varphi(n)$ este o putere a lui 2.

Deci, $\alpha_i = 1$ şi $p_i - 1 = 2^{n_i}$, $n_i \in \mathbb{N}^*$, $i \in \overline{1,s}$.

Din $p_i = 2^{n_i} + 1$ număr prim, rezultă că $n_i = 2^{m_i}$. Cu alte cuvinte, $p_i = 2^{2^{m_i}} + 1$ este număr prim al lui Fermat, $i \in \overline{1,s}$. În final, *n* este de forma (1).

Reciproc, să presupunem că *n* este de forma (1). $\mathbb{Q}(\xi) \supseteq \mathbb{Q}$ este o extindere normală de grad egal cu o putere a lui 2. Din teorema 5.8., rezultă ξ constructibil cu rigla şi compasul. □

Din 6.1. rezultă că pentagonul regulat este constructibil cu rigla şi compasul, deoarece $5 = 2^{2^1} + 1$ este un număr prim al lui Fermat. De asemenea, decagonul regulat este constructibil cu rigla şi compasul, deoarece $10 = 2 \cdot 5$ satisface (1).

Construcția decagonului regulat se poate face ca în figura de mai jos, aplicând următorul raționament:

$$\mu(\measuredangle TOB) = \mu(\measuredangle TBO) = \mu(\measuredangle TBA) = \frac{\pi}{5}$$

$$OT = TB = BA = l_{10}.$$

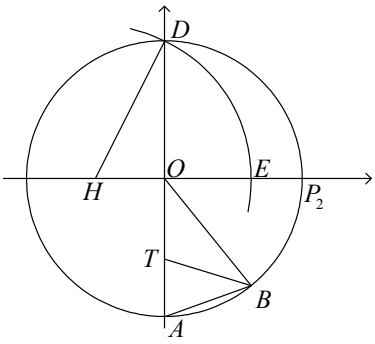
Din teorema bisectoarei, $\frac{TO}{TA} = \frac{BO}{BA}$. Notând $l_{10} = x$,

$$x^2 + x - 1 = 0, \quad x = -\frac{1}{2} + \frac{\sqrt{5}}{2}.$$

Dacă $H(-\frac{1}{2},0)$, atunci $HD=\frac{\sqrt{5}}{2}$.

Luând $E\in(OP_2$, astfel încât $HE=HD$,

$$OE=-\frac{1}{2}+\frac{\sqrt{5}}{2}=l_{10}=AB.$$



Heptagonul regulat (poligonul regulat cu 7 laturi) nu poate fi construit cu rigla şi compasul deoarece 7 nu este de forma (1).

Poligonul regulat cu 17 laturi este constructibil cu rigla şi compasul deoarece $17=2^{2^2}+1$ este un număr prim al lui Fermat.

Primul care a dat construcția poligonului regulat cu 17 laturi a fost Karl Friederick Gauss (1777 – 1855). De altfel, Gauss a fost primul care, în lucrarea sa "*Disquisitiones Arithmeticae*" (1801), a obținut expresia (1) a numerelor naturale *n* pentru care poligonul regulat cu *n* laturi este constructibil cu rigla şi compasul.

Probleme propuse

1. Fie $f \in \mathbb{Q}[X]$, L un corp de descompunere al polinomului f şi G_f, grupul Galois al extinderii $L \supseteq \mathbb{Q}$. Determinaţi:

$$G_f,\ \mathscr{L}\left(G_f\right) \text{ şi } \mathscr{L}(L;\mathbb{Q}),$$

precizând care corpuri intermediare ale extinderii $L \supseteq \mathbb{Q}$ sunt extinderi normale ale lui $\mathbb{Q}$ pentru $f = F_n \in \mathbb{Q}[X]$, $n \in \{5,7,12\}$.

2. Fie G un subgrup al grupului de permutări $\mathscr{S}_n$ ($n \geq 2$). G se numeşte *tranzitiv* dacă pentru orice $1 \leq i, j \leq n$ există $\sigma \in G$ astfel ca $\sigma(i) = j$.

Considerăm acum p, un număr prim, $G \leq \mathscr{S}_p$ subgrup tranzitiv care conţine o transpoziţie. Arătaţi că, în acest caz, $G = \mathscr{S}_p$.

3. Fie p un număr prim şi f un polinom ireductibil de grad p din $K[X]$ unde $K \subseteq \mathbb{R}$. Dacă f are doar două rădăcini complexe, arătaţi că grupul Galois al polinomului f este izomorf cu $\mathscr{S}_p$.

4. Arătaţi că, pentru orice număr prim $p \geq 5$, există un polinom de grad p din $\mathbb{Q}[X]$ pentru care grupul său Galois este izomorf cu $\mathscr{S}_p$.

5. Arătaţi că ecuaţia $x\left(x^2-4\right)\left(x^2+2\right)=2$ nu este rezolvabilă prin radicali peste $\mathbb{Q}$.

6. Exprimaţi prin radicali $\cos\frac{2\pi}{5}$ şi $\cos\frac{\pi}{5}$. Observaţi că pentagonul, respectiv decagonul regulat, este constructibil cu rigla şi compasul.

7. Arătați că $arc\cos\frac{11}{16}$ se poate împărți în trei părți egale folosind rigla şi compasul.

8. Exprimați prin radicali $\cos\frac{2\pi}{7}$ şi arătați că heptagonul regulat nu poate fi construit cu rigla şi compasul.

9. (*Problema celor trei bisectoare*) Se consideră triunghiul isoscel ΔABC în care se cunosc cele trei bisectoare ale sale i_a, i_b, i_c astfel încât $i_a = 3i_b$ şi $i_b = i_c$.

Arătați că, în acest caz, triunghiul ΔABC nu poate fi construit cu rigla şi compasul.

10. Dacă presupunem că se poate construi cu rigla şi compasul un poligon regulat cu *n* laturi, să se determine numerele prime *p* pentru care poligonul regulat cu $p^k n$ laturi, $k \geq 1$, este şi el constructibil cu rigla şi compasul.

11. Fie *n*, număr natural, $15 \leq n \leq 33$. Precizați pentru ce valori ale lui *n*, se poate construi cu rigla şi compasul un poligon regulat cu *n* laturi.

Capitolul VII

SOLUȚII

Capitolul I.

1. a) Se arată uşor că funcția precizată este injectivă şi păstrează incluziunea. Pentru a verifica faptul că aplicația este surjectivă, considerăm un ideal arbitrar J din $M_n(A)$. Pentru $1 \le s,t \le n$ definim mulțimea $J_{s,t} = \{x \in A \mid \exists (a_{i,j}) \in J, x = a_{s,t}\}$. Se demonstrează că $J_{s,t}$ este ideal bilateral în A şi $M_n(J_{s,t}) = J$. b) Se obține imediat că aplicația $f : M_n(A) \to M_n(A/I)$ definită prin $f\left((a_{i,j})_{i,j}\right) = \left(\widehat{a_{i,j}}\right)_{i,j}$ este morfism surjectiv de inele. Deoarece:

$$Kerf = \left\{(a_{i,j})_{i,j} \mid \left(\widehat{a_{i,j}}\right)_{i,j} = \left(\hat{0}\right)_{i,j}\right\} = \left\{(a_{i,j})_{i,j} \mid a_{i,j} \in I, (\forall) i,j\right\} = M_n(I),$$

folosind teorema fundamentală de izomorfism, rezultă relația cerută.

2. a) Pentru $a,b \in rad(A)$, fie $m,n \ge 1$ astfel încât $a^m = 0$, $b^n = 0$. Atunci,

$$(a-b)^{m+n} = \sum_{k=0}^{m+n} C_{m+n}^k a^k (-b)^{m+n-k} = 0 \text{ şi } (ax)^m = a^m x^m = 0, \ \forall x \in A.$$

Deci, $rad(A)$ este ideal în A.

Fie $n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m} \ge 2$. Rezultă:

$\hat{x} \in rad(\mathbb{Z}_n) \Leftrightarrow$ există $s \ge 1$ aşa încât $\widehat{x^s} = \hat{0} \Leftrightarrow n \mid x^s$. În concluzie, $\hat{x} \in rad(\mathbb{Z}_n) \Leftrightarrow p_1 p_2 \ldots p_m \mid x$ şi atunci $|rad(\mathbb{Z}_n)| = \dfrac{n}{p_1 p_2 \cdots p_m}$.

Inelul $\mathbb{Z}_n$ are doar un singur element nilpotent (pe cel nul) dacă şi numai dacă $n = p_1 p_2 ... p_m$, deci *n* este liber de pătrate.

b) Fie $a \in rad(A),\ u \in U(A)$. Atunci, $a + u = u(1 + u^{-1}a)$ unde $b = u^{-1}a$ este nilpotent. Este suficient să arătăm că $1 + b \in U(A)$. Deoarece *b* este nilpotent, fie *k* număr impar pentru care $b^k = 0$. Astfel, $1 = 1 + b^k = (1 + b)(1 - b + b^2 - ... + b^{k-1})$.

c) Fie $f \in rad\left(A[X]\right)$. Există $k \geq 1$ pentru care $f^k = 0$. În particular, $a_n{}^k = 0$, de unde a_n este nilpotent. Notăm $f_1 = f - a_n X^n$ care, conform a) este nilpotent. Fie $k_1 \geq 1$ astfel încât $f_1^{k_1} = 0$. Obţinem că a_{n-1} este nilpotent. Repetând acest raţionament, într-un număr finit de paşi, rezultă că toţi coeficienţii polinomului *f* sunt elemente nilpotente. Folosind a), rezultă imediat implicaţia reciprocă.

d) Presupunem că *f* este inversabil. Atunci, există $g = \sum_{i=0}^{m} b_i X^i$ astfel încât $gf = 1$. Rezultă sistemul:

$$\begin{cases} a_n b_m = 0 \\ a_n b_{m-1} + a_{n-1} b_m = 0 \\ a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m = 0 \\ ..... \\ a_0 b_0 = 1 \end{cases}$$

Astfel, a_0, b_0 sunt inversabile şi din $a_n{}^{m+1} b_0 = 0$ obţinem că a_n este nilpotent. Conform b), polinomul $f_1 = f - a_n X^n$ este inversabil şi reluăm raţionamentul. Implicaţia reciprocă rezultă din a) şi b).

e) Fie *f* divizor al lui zero. Considerăm $g = \sum_{i=0}^{m} b_i X^i$ polinomul nenul de grad minim ($b_m \neq 0$) pentru care $fg = 0$. Astfel, $a_n b_m = 0$. Din $f(a_n g) = 0$ şi $d^\circ(a_n g) < d^\circ g$, pentru a nu contrazice alegerea lui *g*, rezultă că $a_n g = 0$. Notând $f_1 = f - a_n X^n$ obţinem $f_1 g = 0$ şi

astfel $a_{n-1}b_m = 0$. Repetând procedeul, rezultă $a_i b_m = 0$, pentru $i \in \overline{0,n}$, deci $b_m f = 0$.

3. Fie $\pi : \mathbb{Z} \to \mathbb{Z}_n$ surjecția canonică. Aplicând teorema I.3.3. de corespondență și propoziția I.5.3., rezultă că $P \to \pi(P)$ stabilește o bijecție între mulțimea idealelor prime din inelul $\mathbb{Z}$ care include $Ker\pi = n\mathbb{Z}$ și mulțimea idealelor prime din $\mathbb{Z}_n$. Idealele prime din $\mathbb{Z}$ sunt (0) și $p\mathbb{Z}$, cu p număr prim. Dintre acestea, cele care includ $n\mathbb{Z}$ sunt doar cele de forma $p\mathbb{Z}$, unde p este divizor prim al lui n. Astfel, idealele prime din $\mathbb{Z}_n$ sunt cele de forma $p\mathbb{Z}_n$ cu p număr prim, $p \mid n$. $\mathbb{Z}_{16}$ are un singur ideal prim, pe $2\mathbb{Z}_{16}$; idealele prime ale inelului $\mathbb{Z}_{360}$ sunt $2\mathbb{Z}_{360}$, $3\mathbb{Z}_{360}$ și $5\mathbb{Z}_{360}$.

4. M este ideal maximal în A dacă și numai dacă A/M este corp. Această afirmație este echivalentă cu faptul că orice element nenul din A/M este inversabil, adică relația cerută în enunț.

5. I este ideal prim în $A \Leftrightarrow A/I$ este inel integru. Cum, din ipoteză, mulțimea A este finită și orice integru finit este corp, rezultă A/I corp, de unde I este ideal maximal.

6. Fie P un ideal prim; considerăm I ideal în A astfel încât $P \subsetneq I$. Din ipoteză, pentru $a \in I \setminus P$, există $n \geq 1$ astfel încât $a^n = a$. Deoarece $0 = a\left(a^{n-1} - 1\right) \in P$ și P este ideal prim, rezultă $a^{n-1} - 1 \in P \subsetneq I$. Cum și $a \in I$, $1 \in I \Leftrightarrow I = A$. Deci, P este ideal maximal.

7. a) Considerăm $\theta : A[X] \to A/(a)$ definit prin $\theta(f) = a_0 + (a)$, pentru $f = \sum_{i=0}^{n} a_i X^i \in A[X]$. Se arată ușor că θ este morfism surjectiv de inele cu $Ker\theta = \left\{ f = \sum_{i=0}^{n} a_i X^i \mid a_0 \in (a), n \in \mathbb{N} \right\} = (X, a)$ și aplicăm teorema fundamentală de izomorfism pentru inele.

b) rezultă din a), folosind consecințele I.5.4. și I.5.7.

c) Aplicăm b) pentru $A = \mathbb{Z}$, $a = 0$.

8. Fie P un ideal prim în A. Cum $P \neq A$, alegem $a \in A \setminus P$. Lanțul descendent de ideale $(a) \supseteq (a^2) \supseteq (a^3) \supseteq ... \supseteq ...$ este staționar, adică există $n \geq 1$ pentru care $(a^n) = (a^{n+1})$. Astfel, $a^n = ba^{n+1}$ unde $b \in A$. Deoarece A/P este integru şi $\hat{a} \neq \hat{0}$, $\widehat{a^n}\left(\widehat{ab} - \hat{1}\right) = \hat{0}$ implică $\hat{a}\hat{b} = \hat{1}$, deci $\hat{a} \in U\left(A/P\right)$. În concluzie, A/P este corp, de unde rezultă că idealul P este maximal.

9. Presupunem că $I \not\subseteq P_i$, pentru orice i. Vom presupune că idealele prime au fost alese astfel încât, pentru $i \neq j$, $P_i \not\subseteq P_j$ (în caz contrar, unul dintre ele se poate elimina din reuniune).

Pentru $i \in \overline{1,n}$ fixat considerăm idealul $J_i = I \cdot \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j$. Fie $b_j \in P_j \setminus P_i$, pentru toți $j \neq i$ şi $a_i \in I \setminus P_i$. În mod evident, $a = a_i \cdot \prod_{\substack{j=1 \\ j \neq i}}^{n} b_j \in J_i$.

Dacă $a \in P_i$, rezultă $a_i \in P_i$ sau un $b_j \in P_i$, fals. Astfel, $J_i \not\subseteq P_i$.

Fie $\alpha_i \in J_i \setminus P_i$, pentru fiecare i. Atunci, $\alpha = \alpha_1 + \alpha_2 + ... + \alpha_n \in I$ deoarece $J_i \subseteq I$, $(\forall) i \in \overline{1,n}$. Presupunem că există un indice i_0 pentru care $\alpha \in P_{i_0}$. În acest caz, cum $\alpha_k \in P_{i_0}$, pentru $k \neq i_0$, rezultă că $\alpha_{i_0} \in P_{i_0}$, ceea ce contrazice alegerea lui α_{i_0}. Astfel, $\alpha \notin P_i$, pentru orice i, adică $I \not\subseteq \bigcup_{i=1}^{n} P_i$, fals.

10. $P \neq A \Leftrightarrow 1 \notin P \Leftrightarrow 1 \in S$.

P este ideal prim în $A \Leftrightarrow$ pentru orice $a, b \in A$, ($ab \in P \Rightarrow a \in P$ sau $b \in P$) $\Leftrightarrow$ ($a \notin P$ şi $b \notin P \Rightarrow ab \notin P$) $\Leftrightarrow (a, b \in S \Rightarrow ab \in S)$.

11. Se arată uşor că $\theta : A[X] \to A_S$ definită prin $\theta(f) = f\left(\frac{1}{a}\right)$, pentru orice $f \in A[X]$, este morfism de inele. Pentru $\frac{b}{a^k} \in A_S$ există

$f = bX^k \in A[X]$ astfel încât $\theta(f) = \frac{b}{a^k}$, deci θ este surjectiv. Ţinând cont de teorema fundamentală de izomorfism pentru inele, este suficient să arătăm că $Ker\theta = (aX-1)$.

Incluziunea $(aX-1) \subseteq Ker\theta$ este imediată. Fie $f = \sum_{i=0}^{n} a_i X^i \in Ker\theta$.

Atunci, $X - \frac{1}{a} \mid f$ în $A_S[X]$, adică există $g \in A_S[X]$ astfel încât $f = g\left(X - \frac{1}{a}\right) \Leftrightarrow af = g(aX-1)$. Scriind relaţiile dintre coeficienţii polinoamelor, rezultă $g = ah$ cu $h \in A[X]$. Deoarece *a* este nondivizor al lui zero, $f = h(aX-1) \in (aX-1)$.

12. b) Fie $\rho_S : A \to A_S$ şi $\rho_{S'} : A \to A_{S'}$ morfismele structurale. Cum $S' \supseteq S$, $\rho_{S'}(s) \in U\left(A_{S'}\right)$, pentru orice $s \in S$. Din proprietatea de universalitate a inelelor de fracţii rezultă că există morfismul de inele $u : A_S \to A_{S'}$ astfel încât $u\left(\frac{a}{s}\right) = \rho_{S'}(a)\rho_{S'}(s)^{-1}$, $\frac{a}{s} \in A_S$ şi se arată că *u* este bijectivă.

Capitolul II

1. a) Fie $\overline{\alpha}$ conjugatul lui $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$. Atunci, $N(\alpha) = \alpha\overline{\alpha}$ şi de aici obţinem $N(\alpha\beta) = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha) \cdot N(\beta)$.

b) Dacă $\alpha \mid \beta$, atunci există $\gamma \in \mathbb{Z}\left[\sqrt{d}\right]$ astfel încât $\beta = \alpha\gamma$. Din a), rezultă $N(\alpha) \mid N(\beta)$.

c) Ţinem cont că $\alpha \sim \beta \Leftrightarrow \alpha \mid \beta$ şi $\beta \mid \alpha$; aplicăm apoi b).

d) Aplicăm c) ştiind că $\alpha \in U\left(\mathbb{Z}\left[\sqrt{d}\right]\right) \Leftrightarrow \alpha \sim 1$.

e) Cum $\beta = \alpha\gamma$ cu $\gamma \in \mathbb{Z}\left[\sqrt{d}\right]$ şi $N(\alpha) = \pm N(\beta)$, din a) rezultă că $N(\gamma) = \pm 1$, deci $\alpha \sim \beta$.

2. Fie $d = m + ni\sqrt{5}$ astfel încât $d \mid 3$ şi $d \mid 1 + i\sqrt{5}$. Cum $N(d) \mid 9$ şi $N(d) \mid 6$, rezultă că $N(d) \mid 3$. Deoarece ecuaţia $m^2 + 5n^2 = 3$ nu are soluţii întregi, în inelul $\mathbb{Z}\left[i\sqrt{5}\right]$ nu există elemente a căror normă este egală cu 3. Deci, $d \sim 1$.

Presupunem că există $d \sim \left(2\left(1 + i\sqrt{5}\right), 6\right)$. Atunci, cum $d \mid 6$ şi $d \mid 2\left(1 + i\sqrt{5}\right)$, obţinem $N(d) \mid 24$ şi $N(d) \mid 36$, deci $N(d) \mid 12$.

Deoarece $6 = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right)$, $1 + i\sqrt{5}$ şi 2 sunt divizori comuni ai celor două elemente. Rezultă $1 + i\sqrt{5} \mid d$ şi $2 \mid d$. Astfel, $6 \mid N(d)$ şi $4 \mid N(d)$, deci $12 \mid N(d)$. În concluzie, $N(d) = 12$. Pe de altă parte, ecuaţia $m^2 + 5n^2 = 12$ nu are soluţii în $\mathbb{Z}$, adică $N(d) \neq 12$, pentru orice d din $\mathbb{Z}\left[i\sqrt{5}\right]$. Această contradicţie arată că presupunerea făcută este falsă.

3. Pentru că $N(\alpha)$ este număr prim, $N(\alpha) \neq \pm 1$ şi $N(\alpha) \neq 0$, de unde rezultă $\alpha \neq 0$ şi $\alpha \neq 1$. Fie $d \mid \alpha$. Atunci, $N(d) \mid N(\alpha)$ implică $N(d) = \pm 1$ sau $N(d) = \pm N(\alpha)$, adică $d \sim 1$ sau $d \sim \alpha$.

4. Folosind exerciţiul II.1. pentru $d \in \{-1, -3, -5\}$, aflăm toate elementele z din $\mathbb{Z}\left[\sqrt{d}\right]$, cu $N(z) = \pm 1$. Astfel, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, $U\left(\mathbb{Z}\left[i\sqrt{3}\right]\right) = \{\pm 1\}$, $U\left(\mathbb{Z}\left[i\sqrt{5}\right]\right) = \{\pm 1\}$.

5. Presupunem că $f = X^2 + Y^2 \in \mathbb{Q}[X][Y]$ este reductibil. Atunci, $f = \left(a_1 X + b_1 Y + c_1\right)\left(a_2 X + b_2 Y + c_2\right)$ cu $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Q}$.

$$f = a_1 a_2 X^2 + b_1 b_2 Y^2 + \left(a_1 b_2 + a_2 b_1\right) XY + \left(a_1 c_2 + a_2 c_1\right) X +$$
$$+ \left(b_1 c_2 + b_2 c_1\right) Y + c_1 c_2.$$

Identificând coeficienții, vom obține: $c_1 = c_2 = 0,\ a_2 = a_1^{-1},\ b_2 = b_1^{-1}$ şi $a_1^2 + b_1^2 = 0,$ ultima relație fiind imposibilă. Astfel, f este un polinom ireductibil în $\mathbb{Q}[X,Y]$.

6. În $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$ iar $1 \pm i$ sunt elemente ireductibile deoarece $N(1 \pm i) = 2,$ număr prim. Din $d \mid 3$ rezultă $N(d) \in \{1,3,9\}$. Ecuația $a^2 + b^2 = 3$ nu are rădăcini întregi, deci în $\mathbb{Z}[i]$ nu există elemente de normă 3. Din cele două cazuri rămase, obținem $d \sim 1$ sau $d \sim 3$.

7. În $\mathbb{Z}\left[i\sqrt{n}\right]$, 2 este neinversabil. Fie $d = a + bi\sqrt{n}$, $a,b \in \mathbb{Z},$ un divizor al lui 2. Atunci, $N(d) = a^2 + b^2 n \in \{1,2,4\}$. Ecuația $N(d) = 2$ nu are soluții întregi; obținem $d \sim 1$ sau $d \sim 2$, deci 2 este ireductibil în $\mathbb{Z}\left[i\sqrt{n}\right]$. Deoarece n este impar, $2 \mid 1 + n = \left(1 + i\sqrt{n}\right)\left(1 - i\sqrt{n}\right)$ dar $2 \nmid 1 \pm i\sqrt{n},$ deci 2 nu este prim în $\mathbb{Z}\left[i\sqrt{n}\right]$.

8. Se aplică exercițiul II.3. pentru $d = -1$.

9. Fie p un număr prim, $p = \prod_{i=1}^{n} q_i$ unde q_i sunt elemente ireductibile în $\mathbb{Z}[i]$, $i \in \overline{1,n}.$ Pentru că $p^2 = \prod_{i=1}^{n} N(q_i)$ şi toți $N(q_i) \neq 1,$ rezultă $n \leq 2$.

10. a) Fie $z \in \mathbb{Z}[i]$ un element prim. Deoarece $N(z) = z\bar{z} > 1,$ el se poate scrie ca produs de numere prime: $N(z) = p_1 p_2 ... p_k$. Cum z este element prim şi $z \mid N(z),$ există un număr prim p_i astfel încât $z \mid p_i$.
b) p este număr prim, deci $p \neq 0$ şi $p \neq 1$. Fie $d = a + bi \in \mathbb{Z}[i]$, $d \mid p$. Atunci, $N(d) \in \{1, p, p^2\}$. Arătăm că, în condițiile din ipoteză, ecuația $a^2 + b^2 = p$ nu are soluții întregi. Pentru aceasta, observăm că, pentru orice numere întregi a şi b, $a^2 + b^2 \not\equiv 3 (\mathrm{mod}\, 4)$. Rezultă astfel că p este element ireductibil în $\mathbb{Z}[i]$, deci p este prim în $\mathbb{Z}[i]$.

c) Deoarece p este prim, putem aplica teorema lui Wilson şi rezultă $(p-1)!+1 \equiv 0 (\mathrm{mod}\, p)$. Pentru $1 \le k \le \frac{p-1}{2}$, $p-k \equiv -k (\mathrm{mod}\, p)$. Relaţia anterioară se scrie sub forma $\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0 (\mathrm{mod}\, p)$. Astfel, notând $\left(\frac{p-1}{2}\right)!$ cu x (din ipoteză, rezultă că p este număr impar şi astfel, x este număr natural), obţinem $p \mid (1+ix)(1-ix)$ în $\mathbb{Z}[i]$.
Dacă p este prim în $\mathbb{Z}[i]$, atunci $p \mid 1+ix$ sau $p \mid 1-ix$, fals. Deci, $p = p_1 p_2 ... p_k$ unde toţi p_i sunt primi în $\mathbb{Z}[i]$, iar $k \ge 2$. Refăcând raţionamentul de la exerciţiul II.9., obţinem $k \le 2$. Astfel, $k = 2$ şi $p = p_1 p_2$, de unde $\overline{p_1} = p_2$. Să observăm că $p_1 \neq p_2$ pentru că, în caz contrar, rezultă p nu este număr prim sau $p = 2 \not\equiv 1 (\mathrm{mod}\, 4)$.
d) Din rezultatele anterioare, orice element din P este prim în $\mathbb{Z}[i]$. Reciproc, fie z prim în $\mathbb{Z}[i]$. Conform a), există un număr prim p aşa încât $z \mid p$. Dacă $p = 2$, atunci $z \sim 1+i$. Pentru $p = 4k+3$, din b), $z = p \in A$ iar pentru $p = 4k+1$, din c) $z \in B$.

11. $21+3i = 3(7+i)$. Cum $N(7+i) = 50$, căutăm întâi divizori d cu $N(d) = 2$. Atunci, $d \sim 1+i$ şi obţinem $7+i = (1+i)(4-3i)$.
Din $N(4-3i) = 25$, rezultă că singurii săi divizori primi sunt de normă egală cu 5. Dar, $d \in \mathbb{Z}[i]$, $N(d) = 5 \Leftrightarrow d \sim 1+2i$ sau $d \sim 1-2i$.
Prin calcul, rezultă $1+2i \nmid 4-3i$, $4-3i = (1-2i)(2+i)$.
Astfel, $21+3i \sim 3(1+i)(1-2i)(2+i)$.
Analog obţinem descompunerile:
$60+90i \sim 3(1+i)(1-i)(1+2i)(1-2i)(2+3i)$, $8+11i \sim (1+2i)(6-i)$.
Folosind rezultatele obţinute în exerciţiile anterioare, se precizează, de fiecare dată, că factorii din descompuneri sunt primi în $\mathbb{Z}[i]$.

12. Aplicând algoritmul lui Euclid pentru numerele naturale nenule m şi n obţinem şirul de relaţii:

$$m = nq_1 + r_1$$
$$n = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_k = r_{k+1} q_{k+2}$$

în care ultimul rest nenul este r_{k+1}. Deci, $d = (m,n) = r_{k+1}$. Atunci, $m = dm_1$, $n = dn_1$ şi $(m_1, n_1) = 1$. Relaţia

$$a^m - b^m = \left(a^d - b^d\right)\left(a^{d(m_1-1)} + a^{d(m_1-2)}b^d + \ldots + b^{d(m_1-1)}\right)$$

implică $a^d - b^d \mid a^m - b^m$. În mod analog, rezultă $a^d - b^d \mid a^n - b^n$. Fie $c \in A$, $c \mid a^m - b^m$ şi $c \mid a^n - b^n$.

Din $a^m - b^m = a^{nq_1+r_1} - b^{nq_1+r_1} = a^{r_1}\left(a^{nq_1} - b^{nq_1}\right) + b^{nq_1}\left(a^{r_1} - b^{r_1}\right)$ rezultă $c \mid b^{nq_1}\left(a^{r_1} - b^{r_1}\right)$. Vom arăta că $\left(c, b^{nq_1}\right) \sim 1$. Pentru aceasta, presupunem că există $p \in A$, prim, astfel încât $p \mid c$ şi $p \mid b^{nq_1}$. Atunci, $p \mid a$ şi $p \mid b$, ceea ce contrazice ipoteza. Deci, c şi b^{nq_1} sunt relativ prime. Obţinem astfel $c \mid a^{r_1} - b^{r_1}$. Repetăm raţionamentul pentru $c \mid a^n - b^n$ şi $c \mid a^{r_1} - b^{r_1}$, utilizând a doua relaţie din algoritmul lui Euclid. Într-un număr finit de paşi, rezultă $c \mid a^d - b^d$.

13. Fie $a, b \in A$, $b \neq 0$ şi $b' \sim b$ astfel încât $\varphi'(b) = \varphi(b')$. Atunci, cum $b' \neq 0$, există $q, r \in A$ pentru care $a = b'q + r$ unde $r = 0$ sau $\varphi(r) < \varphi(b')$. Deoarece $b' = bu$ cu $u \sim 1$, obţinem $a = \left(uq\right)b + r$ cu $r = 0$ sau $\varphi'(r) \leq \varphi(r) < \varphi(b') = \varphi'(b)$. Deci, φ' verifică a doua condiţie din definiţia inelului euclidian. Considerăm acum $a, b \in A \setminus \{0\}$, $a \mid b$. Atunci, $b \in (a)$. Fie $a' \sim a$ cu $\varphi'(a) = \varphi(a')$. Astfel, $(a) = (a')$ şi $\varphi'(a) \leq \varphi(c)$, $(\forall) c \in (a)$. Dacă $b' \sim b$ astfel încât $\varphi'(b) = \varphi(b')$, obţinem $\varphi'(a) = \varphi(a') \leq \varphi(b') = \varphi'(b)$.

14. a) Folosind relaţiile lui Bézout, completăm tabelul următor:

k	0	1	2	3	4
t_k	375	-192	-9	-3	0
u_k	1	0	1	-21	64
v_k	0	1	2	-41	125
q_k	-	-	-2	21	3

şi obţinem: $(375,-192) \sim t_3 = -3 = 375(-21) - 192(-41)$.
Cum $-3 \mid 21$, ecuaţia are soluţii întregi. Din relaţia stabilită rezultă: $d = -3,\ u = -21,\ v = -41,\ a_1 = -125,\ b_1 = 64,\ c_1 = -7$. Soluţiile ecuaţiei sunt de forma: $x = 147 + 64t,\ y = 287 + 125t,\ t \in \mathbb{Z}$.
b) Determinăm câturile q_k din algoritmul lui Euclid aplicat pentru coeficienţii ecuaţiei: $r_0 = 35 - 35i$ şi $r_1 = -6 + 12i$ cu ajutorul cărora determinăm relaţiile lui Bézout şi completăm tabelul:

$$\frac{r_0}{r_1} = \frac{t_0}{t_1} = \frac{35-35i}{-6+12i} = -\frac{7}{2} - \frac{7}{6}i = (-4-i) + \left(\frac{1}{2} - \frac{1}{6}i\right),$$

$$q_2 = -4 - i;\ \ r_2 = r_0 - r_1 q_2 = -1 + 7i;$$

$$\frac{r_1}{r_2} = \frac{t_1}{t_2} = \frac{-6+12i}{-1+7i} = \frac{9}{5} + \frac{3}{5}i = (2+i) + \left(-\frac{1}{5} - \frac{2}{5}i\right),$$

$$q_3 = 2 + i;\ \ r_3 = r_1 - r_2 q_3 = 3 - i;$$

$$\frac{r_2}{r_3} = \frac{t_2}{t_3} = \frac{-1+7i}{3-i} = -1 + 2i,$$

$$q_4 = -1 + 2i.\ \ r_4 = r_2 - r_3 q_4 = 0$$

k	0	1	2	3	4
t_k	$35-35i$	$-6+12i$	$-1+7i$	$3-i$	0
u_k	1	0	1	$-2-i$	$-3+3i$
v_k	0	1	$4+i$	$-6-6i$	$-14+7i$
q_k	-	-	$-4-i$	$2+i$	$-1+2i$

Astfel, $(35-35i,-6+12i)\sim 3-i.$

Deoarece $1-7i=(3-i)(1-2i),$ obținem că $3-i\,|\,1-7i,$ adică ecuația admite soluții în $\mathbb{Z}[i]$. Rezultă: $d=3-i,\ u=-2-i,\ v=-6-6i,$ $a_1=14-7i,\ b_1=-3+3i,\ c_1=1-2i.$ Soluțiile ecuației sunt de forma:

$x=(1-2i)(-2-i)+(-3+3i)z=-4+3i+(-3+3i)z;$

$y=(1-2i)(-6-6i)+(-14+7i)z=-18+6i+(-14+7i)z;\ \ z\in\mathbb{Z}[i].$

15. a) rezultă imediat folosind definiția subinelului.

b) Deoarece θ şi θ' sunt rădăcinile ecuației de gradul al II-lea, rezultă $\theta+\theta'=-a\in\mathbb{Z}.$ De aici, $\theta\in\mathbb{Z}[\theta']$ şi $\theta'\in\mathbb{Z}[\theta]$.

$\mathbb{Z}[\theta]=\mathbb{Z}\Leftrightarrow\theta\in\mathbb{Z}.$ Arătăm că θ este număr întreg dacă şi numai dacă $d=a^2-4b$ este pătrat perfect. Într-adevăr, dacă $a^2-4b=k^2$ cu $k\in\mathbb{Z},$ k şi a au aceeaşi paritate, deci $-a\pm k$ este număr par, adică $\dfrac{-a\pm k}{2}\in\mathbb{Z}.$

c) Ținând cont de proprietățile funcției modul şi ale operației de conjugare, obținem că φ este funcție multiplicativă:

$\varphi(z_1z_2)=\left|z_1z_2\overline{z_1z_2}\right|=\left|z_1\overline{z_1}\right|\left|z_2\overline{z_2}\right|=\varphi(z_1)\varphi(z_2),$ pentru $z_1,z_2\in\mathbb{Z}[\theta].$

$z\in U\left(\mathbb{Z}[i]\right)\Leftrightarrow$ există $z'\in\mathbb{Z}[i],\ 1=zz'\Leftrightarrow 1=\varphi(z)\varphi(z')\Leftrightarrow 1=\varphi(z).$

d) Observăm că pentru $z=m+n\theta,\ \ \varphi(z)=0\Leftrightarrow z=0\Leftrightarrow m=n=0.$

$$\varphi(z)=\left|z\overline{z}\right|=\left|(m+n\theta)(m+n\theta')\right|=\left|m^2+n^2\theta\theta'+mn(\theta+\theta')\right|=$$
$$=\left|m^2-amn+bn^2\right|.$$

Funcția $N:\mathbb{Z}[\theta]\to\mathbb{Z},\ \ N(z)=z\overline{z},\ \ z\in\mathbb{Z}[\theta],$ este o funcție multiplicativă. Fie $z_1,z_2\in\mathbb{Z}[\theta],\ \ z_2\neq 0.$ $\dfrac{z_1}{z_2}=\dfrac{z_1\overline{z_2}}{z_2\overline{z_2}}=\dfrac{z}{N(z_2)}$ unde am notat $z=z_1\overline{z_2}=m+n\theta.$ Pentru m, respectiv n, şi $N(z_2)\neq 0,$ aplicăm teorema împărțirii cu rest. Rezultă că există $q_1,q_2,r_1,r_2\in\mathbb{Z}$ astfel încât:

$m=q_1N(z_2)+r_1,\ \ n=q_2N(z_2)+r_2,\ \ |r_1|\le\dfrac{1}{2}|N(z_2)|,\ \ |r_2|\le\dfrac{1}{2}|N(z_2)|.$

Atunci, $\frac{z_1}{z_2}=\frac{N(z_2)\left(q_1+q_2\theta\right)+\left(r_1+r_2\theta\right)}{N(z_2)}=\left(q_1+q_2\theta\right)+\frac{r_1+r_2\theta}{N(z_2)}$.

Dacă notăm $q=q_1+q_2\theta\in\mathbb{Z}[\theta]$ şi $r=\frac{z_2\left(r_1+r_2\theta\right)}{N(z_2)}$, din relaţia anterioară, rezultă $r=z_1-z_2q\in\mathbb{Z}[\theta]$. Deci există $q,r\in\mathbb{Z}[\theta]$ pentru care $z_1=z_2q+r$. Rămâne să calculăm $\varphi(r)$ pentru cazul $r\neq 0$.

Din $rN(z_2)=z_2\left(r_1+r_2\theta\right)$, rezultă $\varphi\left(rN\left(z_2\right)\right)=\varphi\left(z_2\left(r_1+r_2\theta\right)\right)$, ceea ce este echivalent cu $\varphi(r)\left(N\left(z_2\right)\right)^2=\left|N(z_2)\right|\left|r_1^2-ar_1r_2+br_2^2\right|$.

Astfel, $\varphi(r)=\frac{\left|r_1^2-ar_1r_2+br_2^2\right|}{\left|N\left(z_2\right)\right|}$. Observăm că:

$$\left|r_1^2-ar_1r_2+br_2^2\right|\le\left|r_1^2\right|+|a||r_1||r_2|+|b|\left|r_2^2\right|\le\frac{1}{4}\left|N(z_2)\right|^2\left(1+|a|+|b|\right).$$

Dacă $|a|+|b|<3$, obţinem $\varphi(r)<\varphi(z_2)$, adică $\mathbb{Z}[\theta]$ este inel euclidian. Pentru $a=0$, $|b|=1$ sau $|b|=2$; ecuaţia iniţială este de forma $x^2\pm1=0$ sau $x^2\pm2=0$. Găsim astfel inelele euclidiene $\mathbb{Z}[i]$, $\mathbb{Z}$, $\mathbb{Z}\left[i\sqrt{2}\right]$, $\mathbb{Z}\left[\sqrt{2}\right]$. Dacă $|a|=1$, $|b|=0$ sau $|b|=1$. Obţinem că inelele $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ şi $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ sunt euclidiene. Atunci când $|a|=2$, $b=0$, inelul rezultat este $\mathbb{Z}$.

16. Se procedează la fel ca la exerciţiul precedent.

17. Conform exerciţiului I.12., arătăm că $A_{S'}$ este inel euclidian. A fiind integru, $A_{S'}$ este tot integru. Folosind funcţia asociată inelului A, $\varphi:A\setminus\{0\}\to\mathbb{N}$, definim $N:A_{S'}\setminus\left\{\frac{0}{1}\right\}\to\mathbb{N}$ prin $N\left(\frac{a}{s}\right)=\varphi(a_1)$ cu $\frac{a_1}{s_1}=\frac{a}{s}$ şi $\frac{a_1}{s_1}$ este fracţie ireductibilă. Se observă că N este bine

definită. Folosind exercițiul II.13., pentru a demonstra că $A_{S'}$ este euclidian, este suficient să arătăm că funcția N verifică condiția b) din definiția inelului euclidian.

Fie $\frac{a}{s}, \frac{b}{t} \in A_{S'}$ cu $\frac{b}{t} \neq \frac{0}{1}$ și $\frac{a_1}{s_1}$, respectiv $\frac{b_1}{t_1}$ fracțiile ireductibile corespunzătoare. Cum $b_1 \neq 0$ și A este euclidian, există $q_1, r_1 \in A$ așa încât $a_1 = b_1 q_1 + r_1$ și $r_1 = 0$ sau $\varphi(r_1) < \varphi(b_1)$.

Din $\frac{a}{s} = \frac{a_1}{s_1} = \frac{b_1}{t_1} \cdot \frac{t_1 q_1}{s_1} + \frac{r_1}{s_1}$ rezultă că există $q = \frac{t_1 q_1}{s_1}$, $r = \frac{r_1}{s_1} \in A_{S'}$ pentru care $\frac{a}{s} = \frac{b}{t} \cdot q + r$. Mai mult, dacă $r_1 = 0$, $r = \frac{0}{1}$ iar în caz contrar, $N(r) \leq \varphi(r_1) < \varphi(b_1) = N\left(\frac{b}{t}\right)$.

18. Aplicăm exercițiul I.11. în care alegem $A = K[X]$, $a = X$, $X = Y$. Obținem $K[X,Y]/(XY-1) \simeq K[X]_S$ unde $S = \{1, X, X^2, ...\}$. Deoarece inelul $K[X]$ este euclidian, din exercițiul II.17., rezultă cerința problemei.

19. A_S este inel integru. Fie $\rho : A \to A_S$ morfismul structural. Arătăm că orice ideal I din A_S este principal. A fiind principal, există $a \in A$ astfel încât $\rho^{-1}(I) = (a)$. Arătăm că un generator al idealului I este $\rho(a) = \frac{a}{1}$. Cum $a \in \rho^{-1}(I)$, $\rho(a) \in I$, deci $(\rho(a)) \subseteq I$. Pentru $\frac{b}{s} \in I$, $\rho(b) = \frac{b}{1} = \frac{b}{s} \cdot \frac{s}{1} \in I$, adică $b \in \rho^{-1}(I)$. Astfel, există $c \in A$, astfel încât $b = ca$. Obținem $\frac{b}{s} = \frac{a}{1} \cdot \frac{c}{s} \in (\rho(a))$.

20. Deoarece $\mathbb{Z}$ este inel principal, există numerele naturale k și n pentru care $I = k\mathbb{Z}$ și $J = n\mathbb{Z}$. Astfel, $IJ = kn\mathbb{Z}$ iar $I \cap J = m\mathbb{Z}$ unde $m = [k,n]$. Folosind relația $kn = md$ cu $d = (k,n)$, din $I \cap J = IJ$ rezultă $d = 1$. Astfel, $I + J = d\mathbb{Z} = \mathbb{Z}$.

21. $\mathbb{Z}[i]$ este inel principal, deci I este principal. Pentru a găsi un generator al său, calculăm $d \sim (4+i, 1+i)$. $\mathbb{Z}[i]$ este şi inel euclidian, deci putem aplica algoritmul lui Euclid. Procedând ca la exercițiul II.14., rezultă relațiile:

$$4+i = (1+i)(2-2i)+i;$$
$$1+i = i(1-i)+0.$$

Astfel, $d \sim i$ şi $I = \mathbb{Z}[i]$.

22. Reducând la absurd, presupunem că în A există un număr finit de elemente ireductibile neasociate în divizibilitate, $q_1, q_2, ..., q_k$. Fie şirul $(a_n)_{n\geq 1}$ unde $a_n = 1 + q_1^n q_2^n ... q_k^n$, $n \geq 1$. Arătăm că toți termenii şirului sunt nenuli. Presupunem că există $n_0 \geq 1$ cu $a_{n_0} = 0$. Atunci, din $q_1\left(-q_1^{n_0-1} q_2^{n_0} ... q_k^{n_0}\right) = 1$ rezultă $q_1 \sim 1$, fals. Presupunem acum că există $m \neq n$ pentru care $a_m = a_n$. Considerăm cazul $m < n$. Deoarece $a_m = a_n \Leftrightarrow \left(q_1^m q_2^m ... q_k^m\right)\left(q_1^{n-m} q_2^{n-m} ... q_k^{n-m} - 1\right) = 0$, obținem ca înainte $q_1 \sim 1$, fals. Astfel, pentru orice $m \neq n$, $a_m \neq a_n$. Am arătat că $M = \{a_n \mid n \geq 1\}$ este mulțime infinită. Din ipoteză, $U(A)$ este mulțime finită; există atunci cel puțin un $n_0 \geq 1$ pentru care $a_{n_0} \neq 1$. Deoarece $a_{n_0} \neq 0$ şi A este inel factorial, fie $a_{n_0} = u\prod_{i=1}^{k} q_i^{\alpha_i}$, $\alpha_i \geq 0$, descompunerea canonică a lui a_{n_0}. Dacă toți $\alpha_i = 0$, $a_{n_0} \sim 1$, fals. Fără a restrânge generalitatea, putem alege $\alpha_1 > 0$.

Altfel, $q_1\left(uq_1^{\alpha_1 - 1} q_2^{\alpha_2} ... q_k^{\alpha_k} - q_1^{n_0 - 1} q_2^{n_0} ... q_k^{n_0}\right) = 1$, de unde $q_1 \sim 1$, fals.

23. Dacă A este mulțime infinită, pentru orice $a \in A$, polinoamele $f_a = X - a$ sunt ireductibile în $A[X]$ şi neasociate în divizibilitate. Dacă A este un integru finit, atunci A este corp. În acest caz, $A[X]$ este inel factorial şi $U\left(A[X]\right) = A^*$ este mulțime finită. Putem aplica exercițiul II.22.

24. Fie P un ideal prim, nenul, minimal în A şi $a \in P \setminus \{0\}$.

Atunci, $a \neq 1$, altfel $P = A$, fals (P este ideal prim). Fie $a = u\prod_{i=1}^{k} p_i^{\alpha_i}$ descompunerea canonică a lui a în inelul factorial A ($u \in U(A)$, toți p_i sunt primi iar $\alpha_i \geq 1$). Din $a \in P$, $u \notin P$ și P ideal prim, rezultă că există $i \in \overline{1,k}$ pentru care $p_i \in P$. Atunci, idealul (p_i) este prim și $(0) \subsetneq (p_i) \subseteq P$. Din minimalitatea lui P, obținem $P = (p_i)$, deci P este principal.

25. A_S este inel integru. Fie $\frac{a}{s} \in A_S \setminus \left\{\frac{0}{1}\right\}$, $\frac{a}{s} \neq \frac{1}{1}$. De aici, $a \neq 0$ și $a \neq 1$. A fiind factorial, $a = u\prod_{i=1}^{n} p_i^{\alpha_i}$ unde $u \in U(A)$, $\alpha_i \geq 1$ și p_i sunt elemente prime în A, pentru $i \in \overline{1,n}$. Obținem $\frac{a}{s} = \frac{u}{s}\prod_{i=1}^{n}\left(\frac{p_i}{1}\right)^{\alpha_i}$.

Să stabilim ce fel de element este $\frac{p}{1}$ în A_S, dacă p este prim în A. Considerăm două cazuri: (*i*) $p \nmid s$, $(\forall) s \in S$. Arătăm că $\frac{p}{1}$ este prim în A_S. Dacă $\frac{p}{1} \in U(A_S)$, există $\frac{b}{t} \in A_S$ cu $\frac{p}{1} \cdot \frac{b}{t} = \frac{1}{1}$, adică $t = pb$. Astfel, $p \mid t$, fals. Deci, $\frac{p}{1}$ nu este inversabil. Din $\frac{p}{1} \left| \frac{b_1}{t_1} \cdot \frac{b_2}{t_2} \right.$, rezultă că $t_1 t_2 bp = b_1 b_2 t$ cu $b \in A$, $t \in S$. Cum p este prim și $p \nmid t$, obținem $p \mid b_1$ sau $p \mid b_2$ și astfel, $\frac{p}{1} \left| \frac{b_1}{t_1} \right.$ sau $\frac{p}{1} \left| \frac{b_2}{t_2} \right.$. (*ii*) există $s \in S$ astfel încât $p \mid s$. În acest caz, fie $s = pc$ cu $c \in A$, Din $\frac{p}{1} \cdot \frac{c}{s} = \frac{1}{1}$, rezultă $\frac{p}{1} \in U(A_S)$. Dacă pentru orice $j \in \overline{1,n}$, p_j divid elemente din S, din

(*ii*), rezultă că toți $\frac{p_j}{1} \in U(A_S)$. Dar $\frac{u}{s} \in U(A_S)$, deci $\frac{a}{s} \sim \frac{1}{1}$, fals. Astfel, în descompunerea canonică a lui *a* există cel puțin un p_j cu proprietatea (*i*). Fie $k \in \overline{1,n}$ astfel încât, eventual după o renumerotare, avem: p_j verifică (*i*) dacă $j \le k$, iar pentru $k < j \le n$, p_j verifică (*ii*). Astfel, $q_j = \frac{p_j}{1}$ sunt elemente prime în A_S pentru $j \le k$ şi $v = \frac{u}{s} \prod_{j=k+1}^{n} \left(\frac{p_j}{1} \right)^{\alpha_j} \in U(A_S)$. Pentru că $\frac{a}{s} = v \prod_{i=1}^{k} q_i^{\alpha_i}$, inelul A_S este factorial.

26. Conform teoremei II.7.3., $\mathbb{Z}[X,Y] = \mathbb{Z}[X][Y]$ nu este principal, deci nici euclidian (teorema II.7.2.). Din consecința II.10.9., el este factorial. Procedând analog, obținem $\mathbb{Z}_5[X,Y]$ nu este euclidian şi nici principal, dar este factorial. Deoarece $\mathbb{Z}_6[X]$ nu este integru, el nu se încadrează în niciun tip de astfel de inele. În $\mathbb{Z}\left[i\sqrt{5}\right]$ obținem $6 = \left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$ şi $6 = 2 \cdot 3$. Se arată că factorii celor două descompuneri sunt elemente ireductibile, neasociate în divizibilitate. Deoarece 6 nu admite o descompunere unică în factori ireductibili în $\mathbb{Z}\left[i\sqrt{5}\right]$, acest inel nu este factorial, deci nu este nici principal, nici euclidian. Pentru celelalte două inele reluăm raționamentul. De exemplu, alegem descompunerile:
$10 = 2 \cdot 5 = \left(6+\sqrt{26}\right)\left(6-\sqrt{26}\right)$, în $\mathbb{Z}\left[\sqrt{26}\right]$ iar în $\mathbb{Z}\left[i\sqrt{3}\right]$, considerăm $4 = 2^2 = \left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)$.

27. Deoarece *A* este inel factorial, considerăm descompunerile canonice: $a = u\prod_{i=1}^{n} p_i^{\alpha_i}$, $b = v\prod_{i=1}^{n} p_i^{\beta_i}$, $c = w\prod_{i=1}^{n} p_i^{\gamma_i}$ unde $u,v,w \sim 1$, p_i

sunt prime în A, $\alpha_i, \beta_i, \gamma_i \geq 0$, $i \in \overline{1,n}$. Pentru a obține relațiile cerute, se folosește teorema II.9.3.. De exemplu, a) se reduce la a arăta că:

$$\max(\alpha_i, \beta_i, \gamma_i) + \min(\alpha_i, \beta_i) + \min(\alpha_i, \gamma_i) + \min(\beta_i, \gamma_i) =$$
$$= \alpha_i + \beta_i + \gamma_i + \min(\alpha_i, \beta_i, \gamma_i).$$

28. În inelul $\mathbb{C}[X]$ avem reprezentările:

$$f = X^m - 1 = \prod_{k=0}^{m-1}(X - x_k), \quad g = X^n - 1 = \prod_{l=0}^{n-1}(X - y_l),$$

unde $x_k = \cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m}$, $k \in \overline{0,m-1}$; $y_l = \cos\frac{2l\pi}{n} + i\sin\frac{2l\pi}{n}$, $l \in \overline{0,n-1}$. Fie $d = (m,n)$, $m = dm_1$, $n = dn_1$, unde $(m_1, n_1) = 1$.

$x_k = y_l \Leftrightarrow \frac{2k\pi}{m} = \frac{2l\pi}{n} \Leftrightarrow kn_1 = lm_1 \Rightarrow k = m_1 t$, $t \in \overline{0,d-1}$. Astfel,

$$(f,g) \sim \prod_{t=0}^{d-1}\left(X - x_{m_1 t}\right) = \prod_{t=0}^{d-1}\left(X - \left(\cos\frac{2t\pi}{d} + i\sin\frac{2t\pi}{d}\right)\right) = X^d - 1.$$

29. $f = X^{2n} - 1 = \prod_{k=0}^{2n-1}(X - x_k)$, unde $x_k = \cos\frac{k\pi}{n} + i\sin\frac{k\pi}{n}$, pentru $k \in \overline{0,2n-1}$ este descompunerea canonică a lui f în $\mathbb{C}[X]$. Rădăcinile reale ale polinomului sunt $x_0 = 1$, $x_n = -1$. Se arată uşor că $\overline{x_k} = x_{2n-k}$ pentru $k \neq 0$. Atunci, descompunerea canonică a lui f în $\mathbb{R}[X]$ este:

$$f = (X-1)(X+1)\prod_{k=1}^{n-1}(X - x_k)\left(X - \overline{x_k}\right) =$$
$$= (X-1)(X+1)\prod_{k=1}^{n-1}\left(X^2 - 2\cos\frac{k\pi}{n}X + 1\right).$$

30. Considerăm $f = X^2 + Y^2 - 1 \in K[Y][X]$. În $K[Y]$, inel factorial, $Y - 1$ este polinom ireductibil. Arătăm că $(Y-1)^2 \nmid Y^2 - 1$, apoi aplicăm criteriul lui Eisenstein. Dacă presupunem că $(Y-1)^2 \mid Y^2 - 1$, rezultă $(Y-1)^2 = Y^2 - 1$, deci $2 \cdot 1_K = 0 \Leftrightarrow car(K) = 2$, fals.

31. Pentru a demonstra necesitatea, să presupunem că n nu este număr prim. Atunci, $n = p \cdot q$, cu $p, q > 1$. Orice $j \in \overline{0, n-1}$ se poate scrie sub forma $j = p \cdot i + r$ cu $i \in \overline{0, q-1}$ şi $r \in \overline{0, p-1}$. Atunci, cum $f = \sum_{j=0}^{n-1} X^j = \sum_{i=0}^{q-1} \sum_{r=0}^{p-1} X^{pi+r} = \left(\sum_{i=0}^{q-1} X^{pi} \right) \left(\sum_{r=0}^{p-1} X^r \right)$, rezultă că polinomul f este reductibil în $\mathbb{Z}[X]$. Reciproc, considerăm acum n număr prim. În forma inițială a lui f nu se poate aplica criteriul lui Eisenstein. Deoarece $u : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $u(g) = g(X+1)$, pentru orice $g \in \mathbb{Z}[X]$, este izomorfism, este suficient să arătăm că $u(f)$ este ireductibil în $\mathbb{Z}[X]$.

$$u(f) = f(X+1) = \sum_{k=0}^{n-1} (X+1)^k = \frac{(X+1)^n - 1}{X} = X^{n-1} + \sum_{k=2}^{n-1} C_n^k X^{k-1} + n.$$

n fiind prim, $n \mid n$ şi $n^2 \nmid n$. Arătăm că $n \mid C_n^k$ pentru $k \in \overline{1, n-1}$. Considerăm relațiile $A_n^k = k! \cdot C_n^k$ şi $n \mid A_n^k = n(n-1)...(n-k+1)$.
Cum n este prim şi $(n, k!) = 1$, rezultă $n \mid C_n^k$, $k \in \overline{1, n-1}$. În mod evident, f este polinom primitiv în $\mathbb{Z}[X]$. Fiind îndeplinite toate condițiile din criteriul lui Eisenstein, rezultă că $u(f)$ este ireductibil în $\mathbb{Z}[X]$.

32. Dacă $g = f(X+1) = (X+1)^{p^n} + p - 1 = X^{p^n} + \sum_{k=1}^{p^n-1} C_{p^n}^k X^k + p$,
observăm că polinomul f este ireductibil în $\mathbb{Z}[X] \Leftrightarrow g$ este ireductibil în $\mathbb{Z}[X]$. Arătăm că numărul prim p verifică condițiile criteriului lui Eisenstein aplicat lui g. Pentru aceasta, demonstrăm că $p \mid C_{p^n}^k$, pentru $1 \le k \le p^n - 1$.

$$C_{p^n}^k = \frac{p^n \left(p^n - 1\right)...\left(p^n - k + 1\right)}{1 \cdot 2 \cdot ... \cdot k} = \frac{p^n}{k} \cdot \frac{p^n - 1}{1} \cdot ... \cdot \frac{p^n - (k-1)}{k-1}.$$

Pentru fiecare $1 \le j \le k-1$, scriem $j = p^{s_j} q_j$ cu $s_j < n$ şi $(q_j, p) = 1$. Deoarece $k < p^n$, $k = p^t q$ cu $t < n$ iar $(q, p) = 1$. Obținem astfel re-

laţia $C_{p^n}^k = \frac{p^{n-t}}{q}\prod_{j=1}^{k-1}\frac{p^{n-s_j}-q_j}{q_j} \Leftrightarrow p \mid qq_1...q_{k-1}C_{p^n}^k$. Din rezultatele stabilite anterior, rezultă $p \mid C_{p^n}^k$, pentru $1 \le k \le p^n - 1$.

33. $\mathbb{Z}_p$ este corp comutativ (p este prim). Fie $\pi : \mathbb{Z} \to \mathbb{Z}_p$ surjecţia canonică iar $\overline{\pi} : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ unicul morfism unitar de inele ce extinde π şi $\overline{\pi}(X) = X$. Atunci, $\overline{\pi}(f) = X^p - X + \hat{a} \in \mathbb{Z}_p[X]$. Deoarece $\mathbb{Z}_p$ este corp, există un corp L ce conţine $\mathbb{Z}_p$ ca subcorp (rezultă deci $car(L) = p$) în care $\overline{\pi}(f)$ are o rădăcină α (vezi lema III.7.1). Aplicând mica teoremă a lui Fermat, obţinem că $\hat{i} = \hat{i}^p$, pentru orice $\hat{i} \in \mathbb{Z}_p$. Deoarece

$$\overline{\pi}(f)(\alpha + \hat{i}) = (\alpha + \hat{i})^p - (\alpha + \hat{i}) + \hat{a} = (\alpha^p - \alpha + \hat{a}) + (\hat{i}^p - \hat{i}) = 0,$$

$\alpha, \alpha + \hat{1}, ..., \alpha + \widehat{p-1}$ sunt toate rădăcinile lui $\overline{\pi}(f)$ deci, în $L[X]$ are loc descompunerea $\overline{\pi}(f) = (X - \alpha)\left(X - \alpha - \hat{1}\right)...\left(X - \alpha - \widehat{p-1}\right)$.

Demonstrăm că $\overline{\pi}(f)$ este ireductibil în $\mathbb{Z}_p[X]$. Să presupunem, prin reducere la absurd, că $\overline{\pi}(f)$ este reductibil în $\mathbb{Z}_p[X]$. Există atunci $h \in \mathbb{Z}_p[X]$ astfel încât $h \mid \overline{\pi}(f)$ şi $1 \le d^\circ h = r < p = d^\circ \overline{\pi}(f)$.

Datorită unicităţii descompunerii în factori ireductibili din $L[X]$, există $i_1, ..., i_r \in \overline{0, p-1}$ pentru care :

$$h \sim h_1 = \left(X - \alpha - \hat{i}_1\right)...\left(X - \alpha - \hat{i}_r\right) \text{ în } \mathbb{Z}_p[X].$$

Putem considera $h = h_1 = X^r - \left(r\alpha + \hat{i}_1 + ... + \hat{i}_r\right)X^{r-1} + ... \in \mathbb{Z}_p[X]$. Rezultă $r\alpha \in \mathbb{Z}_p$, de unde $\alpha \in \mathbb{Z}_p$. Atunci, $\alpha^p = \alpha$.

Deoarece $\overline{\pi}(f)(\alpha)=\hat{0}$, rezultă $\hat{a}=\hat{0}$, adică $p \mid a$, relație ce contrazice ipoteza. Prin urmare, $\overline{\pi}(f)$ este ireductibil în $\mathbb{Z}_p[X]$. Conform criteriului reducției, f este ireductibil în $\mathbb{Z}[X]$.

34. Aplicăm criteriul reducției. Considerăm $\pi:\mathbb{Z}\to\mathbb{Z}_2$ surjecția canonică, pe care o extindem la morfismul $\overline{\pi}:\mathbb{Z}[X]\to\mathbb{Z}_2[X]$.

Notăm $g=\overline{\pi}(f)=X^5+X^2+\hat{1}$. Deoarece f este polinom primitiv şi $d^\circ f=d^\circ g$, rămâne să demonstrăm că g este polinom ireductibil în $\mathbb{Z}_2[X]$. Pentru aceasta, se observă că g nu are rădăcini în $\mathbb{Z}_2$, deci nu există în descompunerea sa canonică polinoame de gradul 1. Presupunem că g admite o descompunere de forma:

$$X^5+X^2+\hat{1}=\left(X^2+aX+b\right)\left(X^3+cX^2+dX+e\right),$$

cu $a,b,c,d,e\in\mathbb{Z}_2$. Identificând coeficienții, rezultă sistemul

$$\begin{cases} a+c=\hat{0} \\ ac+b+d=\hat{0} \\ ad+bc+e=\hat{1} \\ ae+bd=\hat{0} \\ be=\hat{1}. \end{cases}$$

Din ultima ecuație, $b=e=\hat{1}$, iar din prima $a=c$. Sistemul devine:

$$\begin{cases} a^2+d=\hat{1} \\ a(d+\hat{1})=\hat{0} \\ a+d=\hat{0}. \end{cases}$$

Astfel, dacă $a=\hat{0}$, rezultă $d=\hat{0}$, şi nu se verifică $a^2+d=\hat{1}$; dacă $d=\hat{1}$, $a=\hat{1}$ şi, la fel, $a^2+d\neq\hat{1}$. Deoarece sistemul nu are soluții în $\mathbb{Z}_2$, polinomul g este ireductibil în $\mathbb{Z}_2[X]$.

Capitolul III

1. a) Din propoziția III.3.3., rezultă $p=[L:K]=[L:E]\cdot[E:K]$. Obținem $[L:E]=1$ sau $[E:K]=1$, adică $E=L$ sau $E=K$.
b) Cum $\theta\in L\setminus K$, $K(\theta)\neq K$. Aplicăm a) și rezultă $L=K(\theta)$.

2. Considerăm extinderile $\mathbb{Q}\subseteq\mathbb{Q}\left(\sqrt{2}\right)\subseteq\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right)=K$. Pentru că $\sqrt{2}$ este algebric peste $\mathbb{Q}$ ($p_{\sqrt{2}}=X^2-2\in\mathbb{Q}[X]$), din propoziția III.4.7., obținem $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=d^\circ p_{\sqrt{2}}=2$ iar $\left\{1,\sqrt{2}\right\}$ formează o bază în ${}_{\mathbb{Q}}\mathbb{Q}\left(\sqrt{2}\right)$. $\sqrt{3}$ este algebric peste $\mathbb{Q}\left(\sqrt{2}\right)$; se verifică ușor că $p_{\sqrt{3}}=X^2-3$ este polinomul minimal al lui $\sqrt{3}$ peste $\mathbb{Q}\left(\sqrt{2}\right)$. Atunci, $\left[\mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]=2$ iar $\left\{1,\sqrt{3}\right\}$ este o bază a extinderii $K\supseteq\mathbb{Q}\left(\sqrt{2}\right)$. O bază a extinderii $K\supseteq\mathbb{Q}$ este $\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\}$ și $[K:\mathbb{Q}]=\left[K:\mathbb{Q}\left(\sqrt{2}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2\cdot2=4$. Deci,

$$\alpha\in K\Leftrightarrow\exists\, a,b,c,d\in\mathbb{Q},\ \alpha=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}.$$

3. Aplicând criteriul de ireductibilitate al lui Eisenstein, se verifică imediat că $f=X^n-2$ este ireductibil în $\mathbb{Q}[X]$. Astfel, $\alpha=\sqrt[n]{2}$ este algebric peste $\mathbb{Q}$, cu $p_\alpha=f$; obținem $\left[\mathbb{Q}\left(\sqrt[n]{2}\right):\mathbb{Q}\right]=n$.

4. a) Dacă α este algebric peste $\mathbb{Q}$, fie $p_\alpha\in\mathbb{Q}[X]$ polinomul său minimal. Atunci, din $p_\alpha\left(\overline{\alpha}\right)=0$, rezultă că $\overline{\alpha}$ este algebric peste $\mathbb{Q}$. Cum $\alpha,\overline{\alpha},i\in\mathbb{C}'$, rezultă $u=\dfrac{\alpha+\overline{\alpha}}{2}\in\mathbb{C}'$ și $v=\dfrac{\alpha-\overline{\alpha}}{2i}\in\mathbb{C}'$. Reciproca este imediată.
b) Fie $\alpha=|\alpha|(\cos t+i\sin t)$ cu $t\in[0,2\pi)$, un număr algebric.

Deoarece $|\alpha| = \alpha\overline{\alpha} \in \mathbb{Q}$, rezultă că $\overline{\alpha} \in \mathbb{Q}(\alpha)$, deci $u \in \mathbb{Q}(\alpha)$. Astfel, $\mathbb{Q}(u) \subseteq \mathbb{Q}(\alpha) \cap \mathbb{R}$. Notăm $d^\circ p_\alpha = n \geq 1$. Fie acum $x \in \mathbb{Q}(\alpha) \cap \mathbb{R}$. Există $a_0, a_1, ..., a_{n-1} \in \mathbb{Q}$, astfel încât $x = \sum_{k=0}^{n-1} a_k \alpha^k$ şi $x \in \mathbb{R}$. Obţinem

$$x = \sum_{k=0}^{n-1} a_k |\alpha|^k \cos kt.$$

Deoarece $\cos t = \frac{u}{|\alpha|} \in \mathbb{Q}(u)$ şi, pentru $k \in \overline{0, n-1}$, are loc relaţia:

$$\cos kt = \cos^k t - C_k^2 \cos^{k-2} t \sin^2 t + C_k^4 \cos^{k-4} t \sin^4 t - ... \in \mathbb{Q}(\cos t),$$

rezultă $x \in \mathbb{Q}(u)$.

5. a) $\Rightarrow$ b) Fie A un subinel al lui L, $A \supseteq K$ şi $a \in A \setminus \{0\}$. Deoarece $L \supseteq K$ este extindere algebrică, a este algebric peste K, deci $K[a]$ este corp. Atunci, există $a^{-1} \in K[a] \subseteq A$, adică A este corp.

b) $\Rightarrow$ a) Fie $a \in L$, arbitrar ales. Din ipoteză, cum $K \subseteq K[a] \subseteq L$, rezultă că inelul $K[a]$ este corp, deci a este algebric peste K.

6. f are gradul 3 şi nu are rădăcini raţionale, deci este polinom ireductibil în $\mathbb{Q}[X]$. Atunci $p_\alpha = f$.

Astfel, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ şi $\{1, \alpha, \alpha^2\}$ este bază a extinderii.

a) Din $\alpha^3 - 3\alpha + 1 = 0$ obţinem $\alpha^{-1} = 3 - \alpha^2$. Fie m, n, p raţionali cu $\beta^{-1} = m + n\alpha + p\alpha^2$. Din $\beta\beta^{-1} = 1$ rezultă:

$$1 = m + (2m + n)\alpha + (-2m + 2n + p)\alpha^2 + (-2n + 2p)\alpha^3 - 2p\alpha^4.$$

Înlocuind în relaţie $\alpha^3 = 3\alpha - 1$ şi $\alpha^4 = 3\alpha^2 - \alpha$, se obţine sistemul:

$$\begin{cases} m + 2n - 2p = 1 \\ 2m - 5n + 8p = 0 \\ -2m + 2n - 5p = 0 \end{cases}$$

cu soluţie unică $m = 1$, $n = p = -\frac{2}{3}$.

b) $\mathbb{Q}(\beta) \neq \mathbb{Q}$ deoarece $\beta \notin \mathbb{Q}$. Mai mult, din $\left[\mathbb{Q}(\alpha):\mathbb{Q}\right]=3$ rezultă $\mathbb{Q}(\beta)=\mathbb{Q}(\alpha)$. De aici, $d^{\circ}p_{\beta}=3$. Astfel,

$$p_{\beta}=X^3+sX^2+tX+v\in\mathbb{Q}[X] \text{ cu } p_{\beta}(\beta)=0.$$

Folosind relațiile de la a), rezultă:

$$\beta^2=3\left(3-8\alpha+4\alpha^2\right),\ \beta^3=3\left(-21+78\alpha-42\alpha^2\right).$$

Sistemul obținut din relația $p_{\beta}(\beta)=0$

$$\begin{cases} 9s+t+v=63 \\ -24s+2t=-234 \\ 12s-2t=126 \end{cases}$$

are soluția unică $s=9, t=-9, v=-9$.

7. Considerăm $p_{\alpha}, p_{\beta}\in K[X]$ polinoamele minimale peste K ale lui α, respectiv β. Atunci, $p_{\alpha}=\prod_{i=1}^{n}(X-\alpha_i)$ şi $p_{\beta}=\prod_{j=1}^{m}\left(X-\beta_j\right)$ cu $\alpha=\alpha_1$, $\beta=\beta_1$, reprezintă descompunerile lor canonice în $\overline{K}[X]$. Fie polinoamele:

$$f=p_{\alpha}(-X), g=\prod_{j=1}^{m}p_{\alpha}\left(X-\beta_j\right)=\prod_{i=1}^{n}\prod_{j=1}^{m}\left(X-\beta_j-\alpha_i\right),$$

$$h=\prod_{j=1}^{m}p_{\alpha}\left(\frac{X}{\beta_j}\right)=\prod_{i=1}^{n}\prod_{j=1}^{m}\left(\frac{X}{\beta_j}-\alpha_i\right) \text{ şi } r=X^n p_{\alpha}\left(\frac{1}{X}\right).$$

Este evident că $f, r\in K[X]$, $f(-\alpha)=0$, $r\left(\alpha^{-1}\right)=0$. De asemenea, $g(\alpha+\beta)=0$ şi $h(\alpha\beta)=0$.

În încheiere, arătăm că $g\in K[X]$ (pentru a demonstra că $h\in K[X]$ se procedează analog). Deoarece $\prod_{j=1}^{m}p_{\alpha}\left(X-\beta_j\right)$ rămâne invariant la orice permutare a mulțimii $\{\beta_1,...,\beta_m\}$, g este simetric în $\beta_1,...,\beta_m$. Aplicând teorema fundamentală a polinoamelor simetrice, rezultă $g\in K[X]$.

În cazul particular, $p_{\sqrt{2}} = X^2 - 2$, $p_{\sqrt[3]{3}} = X^3 - 3$ şi $\alpha = \alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\beta_1 = \sqrt[3]{3}$, $\beta_2 = \varepsilon\sqrt[3]{3}$, $\beta_3 = \varepsilon^2\sqrt[3]{3}$. Rezultă:

$$g_1 = \prod_{j=1}^{m} p_\alpha\left(X - \beta_j\right) = \prod_{i=1}^{2} p_\beta\left(X - \alpha_i\right) =$$
$$= X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1.$$

8. Fie $a \in K[\theta] \setminus \{0\}$, $a = f(\theta)$ cu $f \in K[X] \setminus \{0\}$. Pentru că polinomul p_θ este ireductibil şi $p_\theta \nmid f$, rezultă că f şi p_θ sunt relativ prime. Există atunci $g, h \in K[X]$ astfel ca $1 = f \cdot g + p_\theta \cdot h$. Obținem, $1 = a \cdot g(\theta)$, adică a este inversabil în $K[\theta]$.

9. Aplicînd teorema fundamentală a polinoamelor simetrice pentru $g \in K[X_1,...,X_n]$, polinom simetric, există $h \in K[X_1,...,X_n]$ astfel ca $g = h(s_1,...,s_n)$.

Deci, $g(\alpha_1,...,\alpha_n) = h\left(s_1(\alpha_1,...,\alpha_n),...,s_n(\alpha_1,...,\alpha_n)\right)$.

Folosind relațiile lui Viète, $s_k(\alpha_1,...,\alpha_n) \in K$, $k \in \overline{1,n}$. Astfel obținem $g(\alpha_1,...,\alpha_n) \in K$. Analog, cealaltă situație.

10. Fie $\alpha \in L$, transcendent peste K. Deoarece $K(\alpha) = K(-\alpha)$, iar $K(\alpha) = K(\alpha^{-1})$, elementele $-\alpha$ şi α^{-1} sunt transcendente peste K. Considerăm extinderile $K \subseteq K\left(\alpha^2 + \alpha\right) \subseteq K(\alpha)$. α fiind rădăcină a polinomului $f = X^2 + X - \left(\alpha^2 + \alpha\right) \in K\left(\alpha^2 + \alpha\right)[X]$, este algebric peste $K\left(\alpha^2 + \alpha\right)$, deci extinderea $K\left(\alpha^2 + \alpha\right) \subseteq K(\alpha)$ este finită. Dar, extinderea $K \subseteq K(\alpha)$ este infinită, deci $K \subseteq K\left(\alpha^2 + \alpha\right)$ este infinită. Astfel, $\alpha^2 + \alpha$ este transcendent peste K. Se procedează în mod analog pentru a arăta că α^n este transcendent peste K. Folosind aceste rezultate, observăm că nu putem preciza natura sumei, respectiv produsului a două elemente transcendente: $\alpha + (-\alpha) = 0$, $\alpha\alpha^{-1} = 1$, sunt algebrice peste K, dar $\alpha + \alpha^2$, α^2, sunt transcendente peste K. Fie $s = a + \beta$. Dacă presupunem că s este algebric

peste K, rezultă $\beta = s - a$ algebric peste K, fals. Deci s este transcendent peste K. Se arată la fel că, pentru $a \neq 0$, $a\beta$ este transcendent peste K.

11. $K \subseteq K(a) \subseteq K(X)$. Fie $F = f(Y) - ag(Y) \in K(a)[Y]$. X este algebric peste $K(a)$ deoarece $F(X) = 0$. Cum $d^\circ F = \max(d^\circ f, d^\circ g)$ este suficient să arătăm că F este ireductibil (adică $F \sim p_X$). Deoarece F este un polinom primitiv, conform lemei II.10.5., arătăm că F este ireductibil în $K[a,Y]$.

Reducem la absurd şi presupunem că F este reductibil şi anume $F = F_1F_2$, unde $F_1, F_2 \in K[a,Y]$, $d^\circ F_1, d^\circ F_2 \geq 1$. Din $d^\circ{}_a F = 1$ rezultă $d^\circ{}_a F_1 = 1$ şi $d^\circ{}_a F_2 = 0$ sau invers. Atunci, în primul caz (pentru celălalt se procedează la fel), $F_2 \in K[Y]$. Pentru că $F_2 \mid F$ rezultă că $F_2 \mid f$ şi $F_2 \mid g$ de unde $F_2 \sim 1$, adică $F_2 \in K^*$, fals.

Fie $a \in K(X) \setminus K$. Deoarece $K(X) \supseteq K(a)$ este extindere finită, iar extinderea $K(X) \supseteq K$ este infinită, rezultă că a este element transcendent peste K.

Astfel, K coincide cu închiderea sa algebrică în $K(X)$.

12. Considerăm două situații:

i) x este algebric peste K şi $g(x) \neq 0$.

Din $K(x) \supseteq K$ finită, rezultă că $K(x) \supseteq K\left(\dfrac{f(x)}{g(x)}\right)$ şi $K\left(\dfrac{f(x)}{g(x)}\right) \supseteq K$ sunt extinderi finite. Obținem $\dfrac{f(x)}{g(x)}$ este algebric peste K (s-a verificat a) pentru elementele algebrice $x \in L$, $g(x) \neq 0$ şi implicația reciprocă de la b)).

ii) x este transcendent peste K.

În acest caz, morfismul $u_x : K(X) \to K(x)$ este izomorfism. Cum $K\left(\dfrac{f(X)}{g(X)}\right) \simeq K\left(\dfrac{f(x)}{g(x)}\right)$, folosind rezultatul obținut în exercițiul an-

terior, obținem $\left[K(x):K\left(\frac{f(x)}{g(x)}\right)\right]=\max\left(d^{\circ}f,d^{\circ}g\right)$. Dar, extinderea $K(x)\supseteq K$ este infinită, deci extinderea $K\left(\frac{f(x)}{g(x)}\right)\supseteq K$ este infinită. Astfel, $\frac{f(x)}{g(x)}$ este transcendent peste *K* (am demonstrat a) pentru *x* transcendent peste *K* şi implicația directă de la b)).

13. Fie $\beta\in L$ o rădăcină a lui *f*. Atunci, $\beta^n=\alpha$. Dacă elementul β este transcendent peste *K*, din exercițiul III.10., rezultă că $\beta^n=\alpha$ este transcendent peste *K*. Fie acum α transcendent peste *K*. Dacă β este algebric peste *K*, rezultă că α algebric peste *K* şi contrazicem alegerea lui α. Deci β este transcendent peste *K*.

14. Pentru $a=\frac{f(\pi)}{g(\pi)}$ şi $b=h\left(\sqrt[30]{e}\right)$ unde $f=\sqrt{2}+\sqrt[3]{5}X-2X^2$, $g=\sqrt{7}-\sqrt[5]{3}X+(1+i)X^2$, $h=X^{15}+X^{10}+X^6$, aplicăm rezultatele obținute în exercițiile III.12 şi III.13.

15. Procedăm prin inducție matematică după *n*. Pentru $n=1$, inegalitatea este evidentă. Presupunem afirmația adevărată pentru polinoame de grad $\le n-1$ şi arătăm că ea rămâne adevărată pentru polinoame de grad *n*. Fie $f\in K[X]$ cu $d^{\circ}f=n$.

Dacă *f* este ireductibil, există o extindere $L_1\supseteq K$, de grad *n*, în care *f* are o rădăcină α. Deci $f=(X-\alpha)f_1\in L_1[X]$, cu $f_1\in L_1[X]$, $d^{\circ}f_1=n-1$. Din ipoteza de inducție, corpul de descompunere L_2 al lui f_1 are proprietatea că $[L_2:L_1]\le(n-1)!$. Rezultă că $L_2=L$ şi $[L:K]=[L:L_1][L_1:K]\le n!$.

Presupunem acum că *f* este reductibil în $K[X]$. Fie $g\in K[X]$ un factor ireductibil al său ($1\le d^{\circ}g<n$) şi $L'\supseteq K$ extinderea de grad egal cu $d^{\circ}g$ în care *g* are o rădăcină β.

Obținem $f=(X-\beta)g_1\in L'[X]$. Folosind ipoteza de inducție, corpul de descompunere L al polinomului g_1 verifică $[L:L']\le(n-1)!$ şi astfel, $[L:K]\le(n-1)!d^\circ g<n!$.

16. a) Se verifică imediat că f nu are rădăcini în $\mathbb{Z}_3$, deci în descompunerea sa în factori primi din $\mathbb{Z}_3[X]$ nu apar factori de gradul 1. Vedem dacă f se descompune în $\mathbb{Z}_3[X]$ sub forma $f=f_1f_2$ unde $f_1=X^2+aX+b\in\mathbb{Z}_3[X]$, $f_2=X^2+cX+d\in\mathbb{Z}_3[X]$, sunt ireductibile în $\mathbb{Z}_3[X]$. Rezultă sistemul:

$$\begin{cases}a+c=\hat{0}\\ b+d+ac=\hat{0}\\ ad+bc=\hat{0}\\ bd=\hat{1}.\end{cases}$$

Din ultima relație, $b=d=\hat{1}$ sau $b=d=\hat{2}$. În primul caz, sistemul nu are soluție în $\mathbb{Z}_3$, iar în a doua situație rezultă $a=\hat{1}$, $c=\hat{2}$.

Astfel, $f_1=X^2+X+\hat{2}$, $f_2=X^2+\hat{2}X+\hat{2}$.

Fie $L_1=\mathbb{Z}_3[X]/(f_1)\supseteq\mathbb{Z}_3$ extinderea în care f_1 are pe $\alpha=\widehat{X}$ ca rădăcină. Deci, $L_1=\mathbb{Z}_3(\alpha)$, $[L_1:\mathbb{Z}_3]=d^\circ f_1=2$ şi $\{1,\alpha\}$ este o bază a extinderii $L_1\supseteq\mathbb{Z}_3$. Cealaltă rădăcină a lui f_1 se obține folosind relațiile lui Viète; astfel $\beta=\hat{2}+\hat{2}\alpha\in L_1$. Verificăm dacă f_2 are rădăcini în L_1. Pentru aceasta, vedem dacă există $a,b\in\mathbb{Z}_3$ astfel încât $f_2(a+b\alpha)=0$. Ținând cont că $\alpha^2=\hat{1}-\alpha$, obținem sistemul:

$$\begin{cases}\hat{2}b(a+b+\hat{1})=\hat{0}\\ a^2+b^2+\hat{2}a+\hat{2}=\hat{0}.\end{cases}$$

$b\neq\hat{0}$ (altfel f_2 are rădăcini în $\mathbb{Z}_3$, ceea ce este imposibil) şi astfel rezultă $b=\hat{2}+\hat{2}a$, de unde $a=\hat{0}$, $b=\hat{2}$ sau $a=\hat{1}$, $b=\hat{1}$. Rădăcinile

lui f_2 sunt $x_1 = \hat{2}\alpha$, $x_2 = \hat{1} + \alpha$. În concluzie, corpul de descompunere este $L = \mathbb{Z}_3(\alpha, \beta, x_1, x_2) = \mathbb{Z}_3(\alpha)$.

b) $L = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$, L are 9 elemente.

Procedăm analog pentru $g = \left(X + \hat{1}\right)\left(X + \hat{4}\right)\left(X^2 + X + \hat{2}\right)$ şi pentru $h = \left(X^2 + \hat{1}\right)\left(X^2 + \hat{2}X + \hat{2}\right)$.

17. f are o singură rădăcină în $\mathbb{Z}_3$, pe $\hat{2}$. Astfel, $f = \left(X - \hat{2}\right) f_1$ cu $f_1 = X^2 + X + \hat{2}$ ireductibil în $\mathbb{Z}_3[X]$. În $L = \mathbb{Z}_3[X]/(f_1) \supseteq \mathbb{Z}_3$ f_1 are o rădăcină, pe $\alpha = \widehat{X}$. În plus, $[L : \mathbb{Z}_3] = 2$ şi $L = \mathbb{Z}_3(\alpha)$. Rezultă că $\{1, \alpha\}$ este o bază a lui ${}_{\mathbb{Z}_3}L$. Dacă β este cealaltă rădăcină a lui f_1, obținem $\beta = \hat{2} + \hat{2}\alpha \in L$. Deci, $L = \{a + b\alpha \mid a, b \in \mathbb{Z}_3\}$ este corp de descompunere al lui f.

Fie $\gamma = a + b\alpha \in L$ o rădăcină a lui g. Din $f_1(\alpha) = 0$, ştim că $\alpha^2 = \hat{1} + \hat{2}\alpha$. Rezultă $0 = g(\gamma) = \left(\hat{2}a^2 + \hat{2}b^2 + a + \hat{1}\right) + b\left(a + b + \hat{1}\right)\alpha$, de unde: $\hat{2}a^2 + \hat{2}b^2 + a = \hat{2}$ şi $b\left(a + b + \hat{1}\right) = \hat{0}$. Obținem că rădăcinile lui g sunt $\gamma_1 = \hat{2}\alpha$, $\gamma_2 = \hat{1} + \alpha$.

18. a) Folosim criteriul Eisenstein. Ecuația $f(x) = 0$ este echivalentă cu $y^2 - 2y - 2 = 0$ unde $y = x^3$. Rezultă $y_{1,2} = 1 \pm \sqrt{3}$. Vom nota $\alpha = \sqrt[3]{1 + \sqrt{3}}$, $\beta = \sqrt[3]{1 - \sqrt{3}}$. Rădăcinile lui f sunt rădăcinile cubice ale lui $y_{1,2}$: $x_1 = \alpha$, $x_2 = \alpha\varepsilon$, $x_3 = \alpha\varepsilon^2$, $x_4 = \beta$, $x_5 = \beta\varepsilon$, $x_6 = \beta\varepsilon^2$ unde $\varepsilon = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$.

b) $K = \mathbb{Q}(\alpha, \beta, \varepsilon) = \mathbb{Q}\left(\alpha, \beta, i\sqrt{3}\right)$ este corpul de descompunere al polinomului f. Din $\sqrt{3} = \alpha^3 - 1 \in K$, $i\sqrt{3} \cdot \sqrt{3} \in K$, adică $i \in K$.

c) $\alpha\beta = -\sqrt[3]{2}$, deci $\sqrt[3]{2} \in K$.

d) Se arată că au loc relaţiile:
$\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3,\left[\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right):\mathbb{Q}\left(\sqrt[3]{2}\right)\right]=2,\left[L:\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)\right]=2.$
Cum $1+\sqrt{3}\in L,$ folosind rezultatele obţinute la subpunctele anterioare, rezultă $K=\mathbb{Q}\left(\alpha,\sqrt[3]{2},i\sqrt{3}\right)=\mathbb{Q}\left(\alpha,\sqrt[3]{2},i,\sqrt{3}\right)=L(\alpha).$

19. a) Pentru orice $\hat{k}\in\mathbb{Z}_p,$ avem $\widehat{k^p}-\hat{k}=0.$ Ţinând cont că α este rădăcină a lui $f,$ $f\left(\alpha+\hat{k}\right)=\left(\alpha^p-\alpha+a\right)+\left(\hat{k}^p-\hat{k}\right)=0.$

b) Dacă f nu este ireductibil în $K[X],$ fie $f_1\in K[X]$ un factor ireductibil al său. Notăm cu L extinderea lui K în care f are o rădăcină $\alpha.$ Conform a), $\alpha+\hat{k}$ este rădăcină a lui $f,$ pentru orice $\hat{k}\in\mathbb{Z}_p,$ deci în $L[X]$ avem $f=\prod_{k=0}^{p-1}\left(X-\alpha-\hat{k}\right).$ Astfel, există $1\le s<p,$ $\widehat{k_i}\in\mathbb{Z}_p,$ $i\in\overline{1,s}$ pentru care $f_1=\prod_{i=1}^{s}\left(X-\alpha-\widehat{k_i}\right)\in K[X].$
Atunci, $s\alpha+\left(\widehat{k_1}+...+\widehat{k_s}\right)\in K,$ de unde $\alpha\in K.$ În concluzie, f se descompune în $K[X]$ în produs de factori de gradul 1 distincţi.

20. Notăm $f_1=X^2-a\in K[X]$ şi $f_2=X^2-b\in K[X].$ Deoarece $f=f_1f_2,$ rezultă că $L=K(u,v),$ cu u şi v elemente dintr-o extindere a lui K pentru care $u^2=a,$ $v^2=b.$ $K(u)$ şi $K(v)$ sunt corpuri intermediare ale extinderii $L\supseteq K$ şi $\left[K(u):K\right]\le 2,$ $\left[K(v):K\right]\le 2,$ $\left[L:K(u)\right]\le 2.$

Pentru $\left[L:K\right]=4,$ obţinem $\left[K(u):K\right]=2,$ $\left[K(v):K\right]=2,$ deci $u,v\notin K,$ adică a, b nu sunt pătrate perfecte în K. Din $\left[L:K(u)\right]=2,$ $v\notin K(u),$ de unde $uv\notin K,$ şi deci ab nu este pătrat perfect în K.

Reciproc, dacă a, b, ab nu sunt pătrate perfecte în K, polinoamele f_1 şi f_2 sunt ireductibile în $K[X]$. Dacă presupunem că f_2 este reductibil în $K(u)[X],$ fie $x=\alpha+\beta u$ o rădăcină a sa din $K(u)$. Din

$x^2 = b \Leftrightarrow b - \alpha^2 - a\beta^2 = 2\alpha\beta u$ şi $u \notin K$, rezultă $\alpha = 0$ sau $\beta = 0$. Dacă $\alpha = 0$, obţinem *ab* pătrat perfect în *K*, iar pentru $\beta = 0$, *b* este pătrat perfect în *K*, adică în fiecare caz este contrazisă ipoteza.
Deci, f_2 este ireductibil în $K(u)[X]$ şi obţinem că

$$[L:K] = [L:K(u)][K(u):K] = 2 \cdot 2 = 4.$$

21. Fie *L* extindere pătratică a lui *K*, deci $[L:K] = 2$. Conform exerciţiului III.1., fie $\alpha \in L \setminus K$ aşa încât $L = K(\alpha)$. Rezultă că polinomul p_α este de forma $p_\alpha = X^2 + aX + b \in K[X]$.

i) Presupunem $car(K) \neq 2$.

$\alpha^2 + a\alpha + b = 0 \Leftrightarrow \left(\alpha + \frac{1}{2}a\right)^2 + \frac{4b - a^2}{4} = 0$, de unde rezultă că α este rădăcină pentru $p_\alpha \Leftrightarrow \beta = \alpha + \frac{1}{2}a$ este rădăcină a polinomului $f = X^2 - c \in K[X]$ cu $c = \frac{a^2 - 4b}{4}$. *f* este ireductibil în $K[X]$ (altfel $\alpha \in K$) şi $K(\alpha) = K(\beta)$.

ii) Presupunem $car(K) = 2$.

Pentru $a \neq 0$, $\alpha^2 + a\alpha + b = 0 \Leftrightarrow \left(\alpha a^{-1}\right)^2 + \left(\alpha a^{-1}\right) + ba^{-2} = 0$. Astfel, α este rădăcină pentru $p_\alpha \Leftrightarrow \gamma = \alpha a^{-1}$ este rădăcină a polinomului ireductibil $f = X^2 + X - c \in K[X]$ unde $c = -ba^{-2}$. Cum $L = K(\gamma)$, *L* este corpul de descompunere al lui *f*.
Dacă $a = 0$, p_α este de forma cerută.

22. Considerăm polinomul:

$$f = \prod_{i=1}^{n} (X - X_i) = X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n \in K(s_1, \ldots, s_n)[X].$$

Corpul său de descompunere este:

$$E(X_1, \ldots, X_n) = K(X_1, \ldots, X_n)(s_1, \ldots, s_n) = K(X_1, \ldots, X_n) = L,$$

deci $L \supseteq E$ este extindere finită. Deoarece *f* este ireductibil în $E[X]$ şi $f(X_n) = 0$, rezultă $f = p_{X_n}$ şi $[E(X_n) : E] = n$.

Vom demonstra prin inducție după n că $\left[L:E\right]=n!$.

Pentru $n=2,\ K\left(X_1,X_2\right)$ este corpul de descompunere al lui $g=X^2-s_1X+s_2\in K\left(s_1,s_2\right)[X]$; deci $\left[K\left(X_1,X_2\right):K\left(s_1,s_2\right)\right]=2.$

Presupunem afirmația adevărată pentru $n-1$ nedeterminate, adică $\left[K\left(X_1,...,X_{n-1}\right):K\left(t_1,...,t_{n-1}\right)\right]=(n-1)!$ unde $t_1,...,t_{n-1}$ sunt polinoamele simetrice fundamentale în $X_1,...,X_{n-1}$. Arătăm că ea rămâne adevărată şi pentru n nedeterminate. Fie :

$$f_1=\prod_{i=1}^{n-1}\left(X-X_i\right)=X^{n-1}-t_1X^{n-2}+...+(-1)^{n-1}t_{n-1}.$$

Din $f=f_1\left(X-X_n\right),$ obținem:

$$s_1=t_1+X_n,\ \ s_n=t_{n-1}X_n \text{ şi } s_k=t_k+t_{k-1}X_n,\ \ k\in\overline{2,n-1}.$$

Fie $E_1=E\left(X_n\right)=K\left(X_n\right)\left(t_1,...,t_{n-1}\right)$. Aplicăm ipoteza de inducție şi obținem $\left[K(X_n)\left(X_1,...,X_{n-1}\right):K(X_n)\left(t_1,...,t_{n-1}\right)\right]=(n-1)!$ unde am înlocuit K cu corpul $K\left(X_n\right)$. În final, din $\left[E_1:K\left(s_1,...,s_n\right)\right]=n$ şi din $K(X_n)\left(t_1,...,t_{n-1}\right)=K\left(s_1,...,s_n\right)\left(X_n\right)=E_1$ rezultă $\left[L:E\right]=n!$.

23. Reducem la absurd şi presupunem corpul $K(X)$ algebric închis. În acest caz, polinoamele ireductibile din $K(X)[Y]$ sunt toate de gradul 1. Deci, $f=Y^2-X\in K(X)[Y]$ este reductibil. Fie $\alpha=\frac{g}{h}$ o rădăcină a sa din $K(X)$ cu $g,h\in K(X),\ h\neq 0,\ \left(g,h\right)\sim 1$. Atunci, $g^2=h^2X$. Din această relație rezultă că polinomul g^2 care are gradul un număr par este egal cu polinomul $h^2X,$ de grad impar, ceea ce este imposibil.

24. Vom proceda prin reducere la absurd şi presupunem că există $\alpha\in L\setminus K,$ element algebric peste K. Atunci, $p_\alpha\in K[X]$, polinomul său minimal, are gradul ≥ 2. Din ipoteză, p_α este polinom ireductibil în $L[X]$ ceea ce contrazice faptul că el are pe α rădăcină în L.

25. Fie $(E_i)_{i\in I}$ o familie de elemente din $\mathscr{L}_a$. Atunci, $K_0=\bigcap_{i\in I}E_i$ este un corp intermediar extinderii. Fie $\alpha\in L$ algebric peste K_0. Cum, pentru fiecare i, $K_0\subseteq E_i$, α este algebric peste E_i, $(\forall)i\in I$. Fiecare E_i este algebric închis în L, deci $\alpha\in K_0$. Astfel, $K_0\in\mathscr{L}_a$ şi $K_0=\inf_{i\in I}E_i$. Fie K_1 închiderea algebrică în L a corpului generat de $\bigcup_{i\in I}E_i$. Atunci, $K_1\in\mathscr{L}_a$. Dacă considerăm acum $F\in\mathscr{L}_a$ astfel încât $E_i\subseteq F$, pentru fiecare i, rezultă $K_1\subseteq F$, deci $K_1=\sup_{i\in I}E_i$. Pentru cazul particular, alegem $K=\mathbb{Q}$ şi $L=\mathbb{C}$.

26. Fie $\mathbb{C}'$ corpul numerelor algebrice. $\mathbb{C}'\supseteq\mathbb{Q}\left(\sqrt{2}\right)$.

$\mathbb{C}'$ este corp algebric închis şi $\mathbb{C}'\supseteq\mathbb{Q}\left(\sqrt{2}\right)$ este extindere algebrică. Deci $\mathbb{C}'$ este o închidere algebrică a lui $\mathbb{Q}\left(\sqrt{2}\right)$.

27. Din relația $\frac{1}{5^{n!}}\le\frac{1}{5^n}$, pentru $n\in\mathbb{N}$ şi din criteriul comparației, rezultă că seria $\sum_{n=0}^{\infty}\frac{1}{5^{n!}}$ este convergentă, deci $\alpha\in\mathbb{R}$.

Presupunem că $\alpha\in\mathbb{Q}$, deci $\alpha=\frac{p}{q}$, unde $p,q\in\mathbb{N}^*$. Fie $k\in\mathbb{N}^*$, ales arbitrar. Din $p\cdot 5^k=q\sum_{n=0}^{k}5^{k!-n!}+q\sum_{n=k+1}^{\infty}\frac{1}{5^{n!-k!}}$, rezultă

$$q\sum_{n=k+1}^{\infty}\frac{1}{5^{n!-k!}}\in\mathbb{N},\ \forall k\in\mathbb{N}^*.$$

Dar,

$$0<q\sum_{n=k+1}^{\infty}\frac{1}{5^{n!-k!}}=\frac{q}{5^{(k+1)!-k!}}\sum_{n=k+1}^{\infty}\frac{1}{5^{n!-(k+1)!}}<\frac{q}{5^{k\cdot k!}}\sum_{n=0}^{\infty}\frac{1}{5^n}=\frac{q}{5^{k\cdot k!}}\cdot\frac{5}{4}<1$$

pentru k suficient de mare, ceea ce contrazice relația anterioară.
Deci, $\alpha\notin\mathbb{Q}$.

Să presupunem acum că $\alpha \in \mathbb{C}'$ (α este algebric şi, deoarece $\alpha \notin \mathbb{Q},\ d^{\circ} p_{\alpha} = r > 1$). Aplicând criteriul lui Liouville, există $c > 0$ astfel încât, $(\forall)\, p, q \in \mathbb{Z},\ q > 0,$ să avem $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^r}$.

Alegem $k \in \mathbb{N}^*,$ arbitrar şi $\frac{p}{q} = \sum_{n=0}^{k} \frac{1}{5^{n!}} = \frac{p}{5^{k!}}$. Rezultă:

$$\left|\alpha - \frac{p}{5^{k!}}\right| = \sum_{n=k+1}^{k} \frac{1}{5^{n!}} > \frac{c}{5^{k!r}},$$

de unde obţinem că $c < \sum_{n=k+1}^{\infty} \frac{1}{5^{n!-k!r}},$ pentru orice $k \in \mathbb{N}^*$. Dar, pentru *k* suficient de mare,

$$\sum_{n=k+1}^{\infty} \frac{1}{5^{n!-k!r}} = \frac{1}{5^{k!(k+1-r)}} \sum_{n=k+1}^{\infty} \frac{1}{5^{n!-(k+1)!}} < \frac{1}{5^{k!(k+1-r)}} \cdot \frac{5}{4} < c,$$

ceea ce contrazice relaţia anterioară.

Prin urmare, α este transcendent.

Capitolul IV

1. Se arată prin calcul că operaţia definită este asociativă, are element neutru pe $e = (1,0) \in M(A)$ şi orice element $(a,b) \in M(A)$ este inversabil, inversul său fiind dat de $\left(a^{-1}, -ba^{-1}\right)$. Definim aplicaţia $f : M(A) \to U(A)$ prin $f\left((a,b)\right) = a,\ (a,b) \in M(A)$. Deducem uşor că f este un morfism surjectiv de grupuri iar nucleul său $Kerf = \{(1,b) \mid b \in A\}$ este izomorf cu $(A,+),$ grupul abelian subiacent structurii de inel a lui *A*. Astfel, $Kerf$ este grup rezolubil.

Aplicând teorema fundamentală de izomorfism pentru grupuri, $M(A)/Kerf \simeq U(A)$. Cum $(U(A),\cdot)$ este grup abelian, $M(A)/Kerf$ este şi el rezolubil. În final, aplicăm teorema IV.4.1. şi rezultă $M(A)$ grup rezolubil.

2. a) Conform ecuaţiei claselor de elemente conjugate,

$$|G| = |Z(G)| + \sum_{a \in S} |G : C(a)|$$

unde S este un sistem de reprezentanți pentru clasele de elemente conjugate care nu aparțin centrului şi $C(a)$ este centralizatorul elementului a. Atunci, $C(a) \neq G$ şi $p \mid |G : C(a)|$, pentru oricare $a \in S$. De aici, $p \mid |Z(G)|$, deci $|Z(G)| > 1$. Astfel, $Z(G) \neq (e)$.

b) Procedăm prin inducție matematică după n. Pentru $n = 1$, G este grup ciclic, deci abelian şi astfel, rezolubil. Presupunem că orice grup finit cu p^k elemente, $k < n$ este rezolubil şi considerăm un p – grup G cu $|G| = p^n$. Folosind a), rezultă că $Z(G)$ şi $G / Z(G)$ sunt p – grupuri cu mai puțin de p^n elemente. Conform ipotezei de inducție, aceste grupuri sunt rezolubile, de unde rezultă că G este grup rezolubil.

3. Considerăm şirurile rezolubile:

$G_1 = H_0 \supseteq H_1 \supseteq ... \supseteq H_m = (e)$ şi $G_2 = K_0 \supseteq K_1 \supseteq ... \supseteq K_n = (e)$.

Putem alege $m = n$. Atunci, pentru $i \in \overline{1,n}$ avem:

$H_i \trianglelefteq H_{i-1}$, $K_i \trianglelefteq K_{i-1}$, iar H_{i-1} / H_i şi K_{i-1} / K_i sunt factori abelieni. În aceste condiții:

$H_i \times K_i \trianglelefteq H_{i-1} \times K_{i-1}$, $(H_{i-1} \times K_{i-1}) / (H_i \times K_i) \simeq H_{i-1} / H_i \times K_{i-1} / K_i$,

pentru $i \in \overline{1,n}$. Cu alte cuvinte, şirul

$$G_1 \times G_2 = H_0 \times K_0 \supseteq H_1 \times K_1 \supseteq ... \supseteq H_n \times K_n = (e)$$

este rezolubil.

4. $D_n = \{1, \sigma, \sigma^2, ..., \sigma^{n-1}, \rho, \sigma\rho, ..., \sigma^{n-1}\rho\}$ unde σ este rotația de unghi $\frac{2\pi}{n}$ în jurul centrului O iar ρ este simetria în raport cu una din axele de simetrie ale lui P_n. $\sigma^n = 1$, $\rho^2 = 1$, $\rho\sigma = \sigma^{n-1}\rho$.

Fie $H = (\sigma)$, grup ciclic. Deoarece $(D_n : H) = 2$, $H \trianglelefteq D_n$. Factorii H şi $D_n / H \simeq \mathbb{Z}_2$ sunt abelieni, deci şirul $D_n \supseteq H \supseteq (1)$ este rezolubil.

5. a) evident. b) şi c) rezultă prin calcul direct; de exemplu, pentru b): $x[y,z]x^{-1}[x,z] = x(yzy^{-1}z^{-1})x^{-1}(xzx^{-1}z^{-1}) = (xy)z(xy)^{-1}z^{-1}$.

6. a) Definim $f: G/Z(G)\times G/Z(G)\to \mathscr{C}$ prin $f(\hat{x},\hat{y})=[x,y]$, $x,y\in G$, unde $\mathscr{C}=\{[x,y]\,|\,x,y\in G\}$. Arătăm că f este bine definită. Fie $u,v\in G$ astfel încât $\hat{x}=\hat{u}$ şi $\hat{y}=\hat{v}$. Atunci, $xu^{-1}, yv^{-1}\in Z(G)$. Obţinem:

$$f(\hat{x},\hat{y})=[x,y]=xyx^{-1}y^{-1}=(xu^{-1})u(yv^{-1})vu^{-1}(ux^{-1})v^{-1}(vy^{-1})=$$
$$=uv(xu^{-1})(ux^{-1})(yv^{-1})(vy^{-1})u^{-1}v^{-1}=[u,v]=f(\hat{u},\hat{v}).$$

Evident, f este surjectivă. Astfel, $|\mathscr{C}|\le|G/Z(G)\times G/Z(G)|=n^2$.

b) Prin calcul, rezultă $\left[yxy^{-1},y\right]^k=\left(y\left(xyx^{-1}y^{-1}\right)y^{-1}\right)^k=y[x,y]^k y^{-1}$, pentru $k\in\mathbb{N}^*$. Deoarece $|G/Z(G)|=n$, $[x,y]^n\in Z(G)$, deci:

$$[x,y]^{n+1}=xyx^{-1}[x,y]^n y^{-1}=xyx^{-1}xyx^{-1}y^{-1}[x,y]^{n-1}y^{-1}=$$
$$=\left(xy^2x^{-1}y^{-2}\right)\left(y[x,y]^{n-1}y^{-1}\right)=\left[x,y^2\right]\left[yxy^{-1},y\right]^{n-1}.$$

7. a) Deoarece $[x,y]^{-1}=[y,x]$, rezultă că elementele lui G' sunt produse finite de comutatori ai unor elemente din G.

b) evident, vezi exerciţiul IV.5.a).

c) Fie $x,y\in G$. y este conjugat cu $x\Leftrightarrow\exists a\in G$ cu $y=axa^{-1}$. Din

$$yxy^{-1}=zxz^{-1}\Leftrightarrow(z^{-1}y)x=x(z^{-1}y)\Leftrightarrow z^{-1}y\in C_G(x),$$

rezultă că $\left|\hat{x}\right|=\left(G:C_G(x)\right)$.

De asemenea, $y\in\hat{x}\Leftrightarrow y=axa^{-1}$, $a\in G\Leftrightarrow yx^{-1}=[a,x]\in G'$.

Obţinem în final,

$$\left|\hat{x}\right|=\left(G:C_G(x)\right)\le|G'|\Leftrightarrow\frac{|G|}{|C_G(x)|}\le\frac{|G|}{|G/G'|}\Leftrightarrow|G/G'|\le|C_G(x)|.$$

d) Fie $\sigma,\tau\in\mathscr{S}_n$. Obţinem $[\sigma,\tau]=\sigma\tau\sigma^{-1}\tau^{-1}\in\mathscr{A}_n$, deci, $\mathscr{S}_n'\subseteq\mathscr{A}_n$. Dacă $n\le 2$, $\mathscr{S}_n$ este grup comutativ, deci $\mathscr{S}_n'=(e)$. Pentru $n\ge 3$, fie $i,j,k\in\overline{1,n}$, distincte. $[(ij),(ik)]=(ij)(ik)(ij)^{-1}(ik)^{-1}=(ijk)$, deci $\mathscr{S}_n$ conţine toate ciclurile de lungime 3. Arătăm că aceste cicluri for-

mează un sistem de generatori pentru $\mathcal{A}_n$ şi, ca urmare, $\mathcal{A}_n \subseteq \mathcal{S}_n'$, adică $\mathcal{S}_n' = \mathcal{A}_n$. Ştim că orice pemutare pară se descompune în produs de un număr par de transpoziţii. Astfel, este suficient să demonstrăm că produsul a două transpoziţii este un produs de cicluri de lungime 3. Pentru aceasta, fie $i, j, k, l \in \overline{1,n}$, distincte. Obţinem:

$$(ik)(ij) = (ijk), \quad (ik)(jl) = (ik)(ij)(ij)(jl) = (ijk)(ijl).$$

e) Fie $i, j, k \in \overline{1,n}$ şi $s, t \in \overline{1,n} \setminus \{i, j, k\}$, distincte. $(sij), (tik) \in \mathcal{A}_n$ şi $\left[(sij), (tik)\right] = (sij)(tik)(sij)^{-1}(tik)^{-1} = (ijk)$. Deci $(ijk) \in \mathcal{A}_n'$. Deoarece ciclurile de lungime 3 generează $\mathcal{A}_n$, rezultă $\mathcal{A}_n' = \mathcal{A}_n$.

8. Deoarece comutatorii generează subgrupul G', este suficient să arătăm că $f\left([x, y]\right) \in \overline{G}'$, $x, g \in G$. Această afirmaţie rezultă din

$$f\left([x, y]\right) = f\left(xyx^{-1}y^{-1}\right) = f(x)f(y)f(x)^{-1}f(y)^{-1} = \left[f(x), f(y)\right].$$

Pentru a rezulta $f\left(G'\right) = \overline{G}'$, impunem condiţia ca f să fie surjectiv. Atunci, pentru orice $z, t \in \overline{G}$, există $x, y \in G$ cu $f(x) = z$, $f(y) = t$. Deci, $\left[z, t\right] = f\left([x, y]\right)$.

9. a) Pentru $a \in G$, fie $f_a : G \to G$, $f(x) = axa^{-1}$, $\forall x \in G$, automorfismul interior al lui G asociat lui a. Cum $H \trianglelefteq G$, $f_a(H) = H$. Astfel, restricţia $\overline{f_a} : H \to H$ este tot un automorfism. Din exerciţiul IV.8., $\overline{f_a}(H') = f_a(H') = H'$, deci $H' \trianglelefteq G$.

b) aplicăm a) pentru $H = G$.

10. a) Fie $g \in G$, $h \in H$. $ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in G'H \subseteq H$; deci $H \trianglelefteq G$. Din $\left[xH, yH\right] = xHyHx^{-1}Hy^{-1}H = \left[x, y\right]H \subseteq G'H \subseteq H$, pentru $x, y \in G$, rezultă G/H este abelian. Pentru $H = G'$, grupul G/G' este abelian.

b) Fie $x, y \in G$. G/H find abelian, $H = [xH, yH] = [x, y]H$, deci $[x, y] \in H$. Deoarece comutatorii $[x, y]$ formează un sistem de generatori pentru G', rezultă $H \supseteq G'$.

Observație. Din b) rezultă că G' este cel mai mic subgrup H al lui G pentru care G/H este abelian. Ca urmare, dintre toate grupurile factor abeliene G/H, G/G' are cardinalul cel mai mare.

11. a) Presupunem că G este grup rezolubil şi considerăm un şir rezolubil al său: $G = H_0 \supseteq H_1 \supseteq ... \supseteq H_n = (e)$. Folosind inducția matematică, arătăm că $H_k \supseteq G^{(k)}$, pentru orice $k \in \overline{1,n}$. Pentru $k = 1$, din $H_1 \trianglelefteq H_0$ şi H_0 / H_1 abelian, aplicând exercițiul IV.10. a), rezultă $H_1 \supseteq G^{(1)}$. Pentru $k \geq 2$, presupunem $H_{k-1} \supseteq G^{(k-1)}$. Din $H_k \trianglelefteq H_{k-1}$ şi H_{k-1} / H_k grup abelian, rezultă $H_k \supseteq (H_{k-1})' \supseteq (G^{(k-1)})' = G^{(k)}$. Deci, $H_k \supseteq G^{(k)}$, pentru orice $k \in \overline{1,n}$. Astfel, $(e) = H_n \supseteq G^{(n)}$, adică $G^{(n)} = (e)$.

Reciproc, fie n astfel încât $G^{(n)} = (e)$. Vom arăta că lanțul descendent de subgrupuri $G = G^{(0)} \supseteq G^{(1)} \supseteq ... \supseteq G^{(n)} = (e)$ este un şir rezolubil al lui G, deci grupul G este rezolubil. Pentru aceasta, din exercițiul IV.9., $G^{(1)} \trianglelefteq G$ şi, în general, $G^{(k)} \trianglelefteq G^{(k-1)}$, $k \in \overline{1,n}$. Astfel, şirul considerat este şir normal al lui G (de fapt, cum $G^{(1)} \trianglelefteq G$ implică $G^{(2)} \trianglelefteq G$, etc., toți $G^{(k)} \trianglelefteq G$). Conform exercițiului IV.8.a), $G/G^{(1)}$ este abelian. Mai mult, grupurile $G^{(k-1)} / G^{(k)}$, $k \in \overline{1,n}$, sunt abeliene. Astfel, şirul inițial este rezolubil.

b) Reluăm raționamentul făcut la a) şi obținem că $H_k \supseteq G^{(k)}$, pentru $k \in \overline{1,r}$. În particular, $G^{(r)} = (e)$. Cum n_0 este cel mai mic număr natural cu această proprietate, $r \geq n_0$.

c) Grupurile abeliene cu mai mult de un element au gradul de rezolubilitate 1. Grupul $\mathscr{S}_3$ este rezolubil şi $\mathscr{S}_3 \supseteq \mathscr{A}_3$. $\mathscr{A}_3$ fiind

abelian, $\mathscr{A}_3' = (e)$. Prin urmare, $\mathscr{S}_3^{(2)} = (e)$ şi gradul de rezolubilitate al lui $\mathscr{S}_3$ este 2.

12. Folosind exerciţiul anterior, arătăm că $\mathscr{S}_n^{(r)} \neq (e)$, pentru orice număr natural *r*. Acest rezultat se obţine din exerciţiul IV.7. d) şi e), deoarece, $\mathscr{S}_n^{(k)} = \mathscr{A}_n$, pentru orice $n \geq 5$ şi $k \geq 1$.

13. a) Presupunem că *G* este grup nilpotent, având şirul central

$$G = H_n \supseteq H_{n-1} \supseteq \ldots \supseteq H_0 = (e).$$

Prin inducţie matematică, arătăm că $H_i \leq Z_i(G)$, pentru $i \in \overline{0,n}$. $H_0 = (e) = Z_0(G)$. Fie $i \geq 1$. Presupunem $H_i \leq Z_i(G)$ şi demonstrăm că $H_{i+1} \leq Z_{i+1}(G)$. Fie $x \in H_{i+1}$, $y \in G$. Din $H_{i+1}/H_i \leq Z(G/H_i)$, rezultă $[xH_i, yH_i] = [x,y]H_i \in H_i$, deci $[x,y] \in Z_i(G)$. Atunci,

$$\left(H_{i+1}Z_i(G)\right)/Z_i(G) \leq Z\left(G/Z_i(G)\right) = Z_{i+1}(G)/Z_i(G).$$

Obţinem $H_{i+1} \leq H_{i+1}Z_i(G) \leq Z_{i+1}(G)$.

Deci $H_i \leq Z_i(G)$, pentru $i \in \overline{0,n}$. În particular, $G = H_n \leq Z_n(G)$, adică $G = Z_n(G)$.

Reciproc, fie şirul $G = Z_n(G) \supseteq \ldots \supseteq Z_1(G) \supseteq Z_0(G) = (e)$, unde *n* este un număr natural. Din modul de definire al subgrupurilor $Z_i(G)$, rezultă că acest şir este central, deci *G* este grup nilpotent.

b) Conform a), dacă *G* este grup nilpotent, putem considera şirul central $G = Z_n(G) \supseteq \ldots \supseteq Z_1(G) \supseteq Z_0(G) = (e)$. Pentru $i \in \overline{0,n-1}$, din $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$, rezultă că factorii şirului sunt grupuri abeliene, deci grupul *G* este rezolubil.

Am arătat în IV.2. că $\mathscr{S}_3$ este grup rezolubil. Obţinem uşor că $Z\left(\mathscr{S}_3\right) = \{e\}$. Astfel, în acest caz, nu există un număr natural *n* astfel încât $Z_n\left(\mathscr{S}_3\right) = \mathscr{S}_3$ şi, conform a), $\mathscr{S}_3$ nu este grup nilpotent. Am arătat că există grupuri rezolubile care nu sunt nilpotente, deci afirmaţia reciprocă de la b) este falsă.

Capitolul V

1. Fie $p_\alpha \in E[X]$ şi $g_\alpha \in EF[X]$ polinoamele minimale ale lui α peste E, respectiv EF. Deoarece $p_\alpha \in EF[X]$ şi $p_\alpha(\alpha)=0$, rezultă că $g_\alpha \mid p_\alpha$. Astfel, $\left[EF(\alpha):EF\right]=d^\circ g_\alpha \le d^\circ p_\alpha=\left[E(\alpha):E\right]$.

2. Presupunem că $\left[F:E\right]=n$ şi considerăm $\{e_1,e_2,...,e_n\}$ o bază a lui ${}_EF$. Atunci, $F=E\left(e_1,...e_n\right)$. Notăm $E_i=E\left(e_1,...e_i\right)$, $i\in\overline{1,n}$. $E=E_0\subseteq E_1\subseteq...\subseteq E_n=F$ reprezintă un lanț de extinderi finite. Formăm şirul de extinderi $EG=E_0G\subseteq E_1G\subseteq...\subseteq E_nG=FG$. Deoarece $E_{i+1}G=E_iG\left(e_{i+1}\right)$, pentru $i\in\overline{0,n-1}$, aplicând exercițiul V.1., rezultă $\left[E_{i+1}G:E_iG\right]=\left[E_iG\left(e_{i+1}\right):E_iG\right]\le\left[E_i\left(e_{i+1}\right):E_i\right]=\left[E_{i+1}:E_i\right]$. Aşadar,

$$\left[FG:EG\right]=\prod_{i=0}^{n-1}\left[E_{i+1}G:E_iG\right]\le\prod_{i=0}^{n-1}\left[E_i\left(e_{i+1}\right):E_i\right]=\left[F:E\right].$$

3. Observăm că $FK=K(F\cup K)=K(F)=F$; la fel, $EK=E$. Notăm $\left[E:K\right]=m$ şi $\left[F:K\right]=n$. Aplicând exercițiul V.2., rezultă: $\left[EF:F\right]=\left[EF:FK\right]\le\left[E:K\right]$ şi $\left[EF:E\right]=\left[EF:EK\right]\le\left[F:K\right]$, deci $EF\supseteq F\supseteq K$ şi $EF\supseteq E\supseteq K$ sunt extinderi finite. Considerăm relația:

(1) $$\left[EF:K\right]=\left[EF:E\right]\cdot\left[E:K\right]=\left[EF:F\right]\cdot\left[F:K\right].$$

Astfel, $m\mid\left[EF:K\right]$ şi $n\mid\left[EF:K\right]$. Din ipoteză, $(m,n)=1$, de unde $mn\mid\left[EF:K\right]$ adică $mn\le\left[EF:K\right]$.

Tot din (1), rezultă şi $\left[EF:K\right]\le mn$.

4. a) $x_k=\cos\frac{k\pi}{5}+\sin\frac{k\pi}{5}=\xi^k$, cu $\xi=\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}$ şi $k\in\overline{0,9}$.

b) ξ^k, $k\in\{1,3,7,9\}$.

c) $F_{10}=\frac{X^{10}-1}{F_1F_2F_5}=X^4-X^3+X^2-X+1$.

d) Descompunerea este dată de $X^{10}-1=F_1F_2F_5F_{10}$.

5. b) Fie $n=\prod_{i=1}^{k} p_i^{\alpha_i}$ descompunerea lui $n\geq 2$ în factori primi.

Mulțimea divizorilor d ai lui n pentru care $\mu(d)\neq 0$ este:

$$\left\{1, p_{i_1}p_{i_2}...p_{i_t} \mid 1\leq i_1<i_2<...<i_t\leq k;\ 1\leq t\leq k\right\}.$$

Rezultă:

$$\sum_{d|n}\mu(d)=\mu(1)+\sum_{i=1}^{k}\mu(p_i)+\sum_{1\leq i<j\leq k}\mu(p_ip_j)+\sum_{1\leq i<j<l\leq k}\mu(p_ip_jp_l)+...+$$

$$+...+\mu(p_1...p_k)=1+(-1)k+C_k^2(-1)^2+C_k^3(-1)^3+...+(-1)^k=$$

$$=(1-1)^k=0.$$

c) $$\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\sum_{d_1|\frac{n}{d}}g\left(d_1\right)=\sum_{dd_1|n}\mu(d)g\left(d_1\right)=$$

$$=\sum_{d_1|n}\left(\sum_{d|\frac{n}{d_1}}\mu(d)\right)g(d_1)=g(n).$$

d) analog cu c).

e) Fie $f,g:\mathbb{N}^*\to\mathbb{Q}[X]^*,\ \ f(n)=X^n-1,\ \ g(n)=F_n.$

Relația $X^n-1=\prod_{d|n}F_d$ se scrie $f(n)=\prod_{d|n}g(d).$ Aplicând d), rezultă

$$g(n)=\prod_{d|n}f\left(\frac{n}{d}\right)^{\mu(d)} \quad \text{sau} \quad F_n=\prod_{d|n}(X^{\frac{n}{d}}-1)^{\mu(d)}.$$

f) Din e) obținem:

$$F_6=\prod_{d|6}(X^{\frac{6}{d}}-1)^{\mu(d)}=\frac{\left(X^6-1\right)\left(X-1\right)}{\left(X^2-1\right)\left(X^3-1\right)}=X^2-X+1, \text{ etc.}$$

6. $$F_{p^n}=\prod_{d|p^n}(X^{\frac{p^n}{d}}-1)^{\mu(d)}=\left(X^{p^n}-1\right)^{\mu(1)}\left(X^{p^{n-1}}-1\right)^{\mu(p)}=$$

$$= \frac{\left(X^{p^{n-1}}\right)^p - 1}{X^{p^{n-1}} - 1} = F_p\left(X^{p^{n-1}}\right),\ F_{27} = F_{3^3} = F_3\left(X^9\right) = X^{18} + X^9 + 1.$$

7. K fiind corp finit, grupul $(K^*, \cdot)$ este ciclic. Fie a un generator al său. Atunci, $K = \left\{0, 1, a, a^2, ..., a^{n-2}\right\}$.

Fie $f \in Aut(K)$. $f(0) = 0,\ f(1) = 1$. Se observă că f este complet determinat de $f(a)$. Deoarece $a \neq 0,$ rezultă că $f(a) \in K^*$.

Fie $f_1, f_2 \in Aut(K)$ cu $f_1(a) = a^{k_1},\ f_2(a) = a^{k_2},\ 1 \leq k_1, k_2 \leq n-2$.

Atunci, $(f_1 \circ f_2)(a) = f_1\left(a^{k_2}\right) = a^{k_1 k_2} = (f_2 \circ f_1)(a),\ \forall a \in K,$ deci $f_1 \circ f_2 = f_2 \circ f_1$ şi astfel grupul $Aut(K)$ este comutativ.

8. Se demonstrează că $f = X^4 + X^3 + \hat{1} \in \mathbb{Z}_2[X]$ este ireductibil, deci L este corp. Cum $\left[L : \mathbb{Z}_2\right] = d^\circ f = 4,\ |L| = \left|\mathbb{Z}_2\right|^{[L:\mathbb{Z}_2]} = 2^4 = 16.$
Pentru un corp cu 8 elemente, putem alege $L = \mathbb{Z}_2[X]/(g)$ unde polinomul $g = X^3 + X + \hat{1} \in \mathbb{Z}_2[X]$ este ireductibil.
În mod analog, se arată că $L = \mathbb{Z}_3[X]/(h)$ este un corp cu 27 de elemente pentru $h = X^3 + \hat{2}X + \hat{2} \in \mathbb{Z}_3[X],$ polinom ireductibil.

9. a) Cum $d^\circ f = 3,\ f$ este ireductibil în $K[X] \Leftrightarrow f$ nu are rădăcini în K. Deoarece $|K| = 3,$ rezultă $x^3 = x,\ (\forall) x \in K$. Astfel, $f(x) \neq 0,\ \forall x \in K \Leftrightarrow (a+1)x + 2 \neq 0,\ \forall x \in K$. Rezultă $a = 2$.
b) $f(0) \neq 0$ şi $\forall x \in K^*,\ x^4 = 1$. Determinăm valorile lui a pentru care f nu are rădăcini în K, adică $f(x) = ax + 2 \neq 0,\ (\forall) x \in K^*$. Obţinem $a = 0$. Dar, în acest caz, $f = X^4 + 1 = \left(X^2 + 2\right)\left(X^2 + 3\right)$ este reductibil. Rezultă că, pentru orice $a \in K$, f este reductibil în $K[X]$.

10. Considerăm $p \geq 3$ (cazul în care $p = 2$ este imediat). În acest caz, $car\left(\mathbb{Z}_p\right) = p \neq 2$ şi obţinem $\left(2ax + b\right)^2 = b^2 - 4ac.$

Dacă $b^2 - 4ac$ nu este pătrat în $\mathbb{Z}_p,$ ecuaţia nu are soluţii în $\mathbb{Z}_p$.

Pentru $b^2-4ac=0$, soluțiile ecuației sunt $x_1=x_2=-b(2a)^{-1}$ iar dacă există $k\in\mathbb{Z}_p$ astfel încât $b^2-4ac=k^2$, $x_{1,2}=(-b\pm k)(2a)^{-1}$.

Pentru prima ecuație, $\hat{2}x^2+\hat{3}x-\hat{5}=\hat{0}\Leftrightarrow\left(\hat{4}x+\hat{3}\right)^2=\hat{5}=\left(\hat{4}\right)^2$ şi rezultă $x_1=\hat{1}$, $x_2=\hat{3}$. În al doilea caz, ecuația nu are soluții, deoarece $b^2-4ac=\hat{8}$ nu este pătrat în $\mathbb{Z}_{11}$.

11. Fie $u:K\to K$, endomorfismul lui Frobenius. Atunci, pentru orice $x\in K$, $u^n(x)=x^{p^n}$. Dacă presupunem că polinomul *f* are două rădăcini α şi β în *K*, rezultă $a=\alpha^{p^n}=\beta^{p^n}\Leftrightarrow u^n(\alpha)=u^n(\beta)$. Cum *u* este morfism injectiv, $\alpha=\beta$.

12. $|K|=p^s$ cu $s\geq 1$. a) Rădăcinile lui $f=X^{p^{sn}}-X\in K[X]$ formează un subcorp *L* al lui $\overline{K}$ cu p^{sn} elemente. Notăm cu *x* un generator al grupului ciclic $(L^*,\cdot)$. Astfel, $L=K(x)$. Din $[L:K]=n$, rezultă $d^\circ p_x=n$.

b) Fie $f\in K[X]$, polinom ireductibil de grad *m* şi $x\in\overline{K}$ o rădăcină a sa. Atunci, din $|K(x)|=p^{sm}$, rezultă că $y^{p^{sm}}-y=0$, pentru orice $y\in K(x)$. Deoarece $f\sim p_x$, obținem că $f\mid X^{p^n}-X$, unde $n=sm$.

13. a) Din $q=|K|$, rezultă că există $s\in\mathbb{N}^*$ astfel încât $q=p^s$. Notăm:

$I_n=\{f\in K[X]\mid f$ unitar şi ireductibil, $d^0f=n\}$ şi $N_n=|I_n|$.

Ca în exercițiul V.12., obținem că, pentru $f\in I_n$ şi $\alpha\in\overline{K}$, o rădăcină a lui *f*, corpul $L_f=K(\alpha)$ are q^n elemente. Deoarece rădăcinile lui $X^{p^{sn}}-X\in K[X]$ formează un subcorp *L* al lui $\overline{K}$ tot cu q^n elemente, obținem că $L_f=L=\{x\in\overline{K}\mid x^{q^n}-x=0\}$.

Din $f \mid X^{q^n} - X$, rezultă că toate rădăcinile lui f sunt distincte şi L conţine toate rădăcinile lui f. Notăm $A_f = \left\{ x \in \overline{K} \mid f(x) = 0 \right\}$.

Repetând raţionamentul pentru un alt polinom $g \in I_n$, rezultă că $\left| L_f \right| = \left| L_g \right|$ şi, deoarece în $\overline{K}$ există un singur subcorp cu un număr dat de elemente, $L_f = L_g$.

Dacă f şi g au o rădăcină comună, α, ţinând cont că polinomul minimal p_α este unic, rezultă $f = g$. Astfel, pentru $f \neq g$,

$$A_f \cap A_g = \varnothing.$$

Consecinţa V.4.7. precizează că, pentru $d \mid n$,

$$L' = \left\{ x \in \overline{K} \mid x^{q^d} - x = 0 \right\} \subseteq L.$$

Procedând analog, obţinem că pentru $h \in I_d$, cu $d \mid n$, L conţine toate rădăcinile lui h.

Fie $\beta \in L$. Cum extinderile $L \supseteq K(\beta) \supseteq K$ sunt finite şi $\left[L : K \right] = n$, există $d \mid n$, aşa încât $\left[K(\beta) : K \right] = d$, adică $d^\circ p_\beta = d$.

Aşadar, pentru $\beta \in L$, există $d \mid n$, $h \in I_d$, astfel încât $h(\beta) = 0$.

Din rezultatele obţinute până acum, $L = \bigcup_{d \mid n} \bigcup_{h \in I_d} A_h$.

Deoarece am arătat că reuniunea este disjunctă, $q^n = \sum_{d \mid n} d \cdot N_d$.

Pentru funcţiile $f, g : \mathbb{N}^* \to \mathbb{Z}$, definite prin $f(n) = q^n$, $g(n) = nN_n$, $\forall n \in \mathbb{N}^*$, avem $f(n) = \sum_{d \mid n} g(d)$. Aplicăm formula de inversiune a lui Möbius (vezi exerciţiul V.5.c)). Rezultă $N_n = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{\frac{n}{d}}$.

b) În cazul în care $n = p$, $N_p = \frac{1}{p}\left(q^p - q \right)$.

c) Extinderile de grad p ale lui K sunt de forma $K(\alpha)$ cu α o rădăcină a unui polinom ireductibil de grad p din $K[X]$.

14. Extinderile sunt finite şi separabile, deci sunt simple. a) Rădăcinile lui $p_{\sqrt{5}} = X^2 - 5$ sunt $\pm\sqrt{5}$, iar cele ale lui $p_{\sqrt{3}} = X^2 - 3$ sunt $\pm\sqrt{3}$. Căutăm $c \in \mathbb{Q}$ care nu este soluție pentru niciuna din ecuațiile $\sqrt{5} + c\sqrt{3} = \pm\sqrt{5} - c\sqrt{3}$. Rezultă $c \neq 0$. Alegem $c = 1$ şi găsim $\gamma = \sqrt{3} + \sqrt{5}$ un element primitiv al extinderii.

b) Rădăcinile polinomului $p_{i\sqrt{3}} = X^2 + 3$ sunt $x_1 = i\sqrt{3}$ şi $x_2 = -i\sqrt{3}$, iar $p_{\sqrt[3]{2}} = X^3 - 2$ are rădăcinile $y_1 = \sqrt[3]{2}$, $y_2 = \sqrt[3]{2} \cdot \varepsilon$, $y_3 = \sqrt[3]{2} \cdot \varepsilon^2$.

Determinăm $c \in \mathbb{Q}$ pentru care $x_1 + cy_1 \neq x_i + cy_j$, cu $i \in \{1,2\}$ şi $j \in \{2,3\}$. Rezultă $c \neq 0$. Astfel, $\gamma = i\sqrt{3} + \sqrt[3]{2}$ este element primitiv al extinderii.

15. Rezultă din propozițiile V.8.3. şi V.8.4..

16. $E = L(x_1, x_2, ..., x_n)$ este corpul de descompunere al lui *f* şi fie $\overline{K} \supseteq E \supseteq K$ o închidere algebrică a lui *K*. Considerăm $\sigma \in G(\overline{K} \mid K)$ şi arătăm că $\sigma(E) \subseteq E$. Extinderea $L \supseteq K$ fiind normală, $\sigma(L) \subseteq L$. Cum σ este un *K*- automorfism al lui $\overline{K}$, σ permută rădăcinile lui *f*. Astfel, $\sigma(E) \subseteq E$, adică $E \supseteq K$ este extindere normală.

Considerăm acum $f = X^2 - \sqrt{2} \in L[X]$, unde $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ şi $E = \mathbb{Q}(\sqrt[4]{2})$. Extinderea $L \supseteq K$ este normală (*L* este corpul de descompunere al polinomului $X^2 - 2 \in \mathbb{Q}[X]$) iar *E* este corpul de descompunere al lui *f* (deci tot extindere normală). Cu toate acestea, extinderea $\mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}$ nu este normală, deoarece polinomul ireductibil $X^4 - 2 \in \mathbb{Q}[X]$ nu are toate rădăcinile în $\mathbb{Q}(\sqrt[4]{2})$.

Astfel, am arătat că extinderile normale nu au proprietatea de tranzitivitate.

17. Aplicăm rezultatul obținut în exercițiul III. 21. şi obținem că aceste extinderi sunt normale. O extindere pătratică $L \supseteq K$ este separabilă dacă polinomul ireductibil al cărui corp de descompunere este

L, este separabil. Acest fapt se verifică în toate cazurile, mai puțin atunci când $car(K)=2$ şi $f=X^2-a\in K[X]$.

18. $L=K[X]/(f)$ este corp finit, $|L|=|K|^{[L:K]}=|K|^{d^\circ f}$ în care f are o rădăcină, pe α. De fapt, $L=K(\alpha)$. Deoarece extinderile de corpuri finite sunt normale, polinomul ireductibil f va avea toate rădăcinile în L. Astfel, L este un corp de descompunere al lui f peste K.

19. a) Extinderea nu este normală deoarece polinomul ireductibil f are o rădăcină în $\mathbb{Q}(\alpha)$, dar nu le are pe toate.

b) Extinderea este normală deoarece $\mathbb{Q}\left(i,\sqrt{3},\alpha\right)=\mathbb{Q}\left(i,\sqrt{3},\sqrt[3]{2}\right)$ este corpul de descompunere al polinomului f peste $\mathbb{Q}\left(i,\sqrt{3}\right)$.

c) Se arată uşor că polinomul $X^3+X+\hat{1}\in\mathbb{Z}_2[X]$ este ireductibil şi apoi aplicăm exercițiul V.18.

20. $u_0=1_L\in G(L\,|\,K)$. Fie $u:L\to L$ endomorfismul lui Frobenius. Pentru orice $x\in L$, $u_1(x)=x^{p^s}=u^s(x)$. Deoarece L este corp finit, u este automorfism, deci $u_1\in Aut(L)$. Pentru $x\in K$, $x^{p^s}=x$, de unde $u_1(x)=x$. Rezultă astfel, $u_1\in G(L\,|\,K)$. Demonstrația se încheie arătând că $u_k=u_1^k$, pentru $2\le k\le n-1$.

21. Conform exercițiului V.18., $K(\alpha)$ este un corp de descompunere pentru f. Mai mult, $|K(\alpha)|=p^{sn}$. Fie $G=G(K(\alpha)\,|\,K)$.
Din exercițiul V.20., rezultă că $u_1^{\,k}\in G$, $1\le k\le n-1$, $u_1=u^s$, unde $u\in Aut(K(\alpha))$ este endomorfismul lui Frobenius. Astfel, $|G|=n$ şi

$$G=\langle u_1\rangle=\left\{1_{K(\alpha)},u_1,...,u_1^{n-1}\right\}\simeq\mathbb{Z}_n.$$

Din V.7.4., toate rădăcinile lui f sunt de forma $u_1^{\,k}(\alpha)$, $0\le k\le n-1$.

Obținem astfel că

$$\alpha,\ u_1(\alpha)=\alpha^{p^s},\ u_1^2(\alpha)=\alpha^{p^{2s}},\ \ldots,\ u_1^{n-1}(\alpha)=\alpha^{p^{(n-1)s}}$$

sunt toate rădăcinile lui f.

22. Se arată că polinomul este ireductibil în $\mathbb{Z}_2[X]$.

Din exercițiul V.18., $L=\mathbb{Z}_2[X]/(f)\supseteq\mathbb{Z}_2$ este corp de descompunere al lui *f*. $\alpha=\widehat{X}\in L$ este o rădăcină a lui *f*. Aplicând exercițiul V.21. pentru $p=2,\ s=1,\ n=4,$ obținem că $\alpha,\ \alpha^2,\ \alpha^4$ şi α^8 sunt rădăcinile lui *f*.

23. $f(\alpha+j)=(\alpha^p-\alpha+a)+(j^p-j)=0,\quad j\in\overline{1,p-1}.$ Astfel, rădăcinile lui *f* sunt $\alpha,\alpha+1,...,\alpha+p-1$ şi $K(\alpha)$ este corp de descompunere pentru *f*, deci $K(\alpha)\supseteq K$ este normală. Extinderea este şi separabilă deoarece rădăcinile lui *f* sunt distincte. Din $\left[K(\alpha):K\right]=p$ rezultă că extinderea este finită. În final, $G=G\left(K(\alpha)\,|\,K\right)\simeq\mathbb{Z}_p$.

Ştim că orice $\sigma\in G$ permută rădăcinile lui *f*. Fie $\sigma_0\in G,$ definit prin $\sigma_0(\alpha)=\alpha+1.$ Obținem $G=\langle\sigma_0\rangle=\left\{1_{K(\alpha)},\sigma_0,...,\sigma_0^{p-1}\right\}$.

24. Deoarece *L* este corpul de descompunere al lui *f*, $L\supseteq K$ este finită şi normală. Corpurile având caracteristica egală cu 0, extinderea este şi separabilă. Astfel, $\left|G_f\right|=\left[L:K\right].$

a) $L=\mathbb{Q}\left(i\sqrt{3}\right)$ şi $\left\{1,i\sqrt{3}\right\}$ este o bază în ${}_KL$. Rezultă

$$G_f=\langle\sigma\rangle=\left\{1_L,\sigma\right\}\simeq\mathbb{Z}_2$$

unde $\sigma\in G_f$ este definit prin $\sigma\left(i\sqrt{3}\right)=-i\sqrt{3}.$

b) $L=\mathbb{Q}\left(\sqrt{5},i\sqrt{2}\right)$ şi $\left|G_f\right|=\left[L:K\right]=4.$ Atunci, G_f este izomorf cu grupul $\mathbb{Z}_4$ sau cu $\mathscr{K}$, grupul lui Klein.

Pentru a defini automorfismele $\sigma\in G_f,$ precizăm valorile posibile ale lui $\sigma(\alpha),$ pentru fiecare element adjuncționat $\alpha,$ ținând cont de faptul că $\sigma(\alpha)$ este un conjugat al lui $\alpha.$ Reunim rezultatele în tabelul următor:

	1_L	σ_1	σ_2	$\sigma_1\sigma_2$
$i\sqrt{3}$	$i\sqrt{3}$	$i\sqrt{3}$	$-i\sqrt{3}$	$-i\sqrt{3}$
$\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$

Obținem $\sigma_1^2=\sigma_2^2=(\sigma_1\sigma_2)^2=1_L$ și, cum orice grup de 4 elemente este comutativ, $\sigma_1\sigma_2=\sigma_2\sigma_1$. În acest caz, $G_f\simeq\mathcal{K}$.

Toate subgrupurile proprii ale lui G_f sunt ciclice şi anume:

$$H_1=\{1_L,\sigma_1\},\ H_2=\{1_L,\sigma_2\},\ H_3=\{1_L,\sigma_1\sigma_2\}.$$

Astfel, $\mathcal{L}(G_f)=\{(e),H_1,H_2,H_3,G_f\}$.

Cum G_f este comutativ, subgrupurile sale sunt normale, aşadar $E=L^H\supseteq\mathbb{Q}$ sunt extinderi normale. Observăm că $\mathbb{Q}(i\sqrt{3})\subseteq E_1$. Deoarece $[E_1:\mathbb{Q}]=2$, rezultă $E_1=\mathbb{Q}(i\sqrt{3})$. În mod analog, obținem că $E_2=\mathbb{Q}(\sqrt{5})$, $E_3=\mathbb{Q}(i\sqrt{15})$ de unde,

$$\mathcal{L}(L;\mathbb{Q})=\{\mathbb{Q},E_1,E_2,E_3,L\}.$$

c) $L=\mathbb{Q}(i\sqrt{3},\sqrt[3]{2})$, $[L:\mathbb{Q}]=6$. Atunci, $G_f\simeq\mathbb{Z}_6$ sau $G_f\simeq\mathcal{S}_3$.

Cele 6 automorfisme sunt definite în tabelul următor unde am notat $\varepsilon=\dfrac{-1+i\sqrt{3}}{2}$:

	1_L	σ_1	σ_1^2	σ_2	$\sigma_1\sigma_2$	$\sigma_1^2\sigma_2$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\varepsilon\sqrt[3]{2}$	$\varepsilon^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\varepsilon\sqrt[3]{2}$	$\varepsilon^2\sqrt[3]{2}$
$i\sqrt{3}$	$i\sqrt{3}$	$i\sqrt{3}$	$i\sqrt{3}$	$-i\sqrt{3}$	$-i\sqrt{3}$	$-i\sqrt{3}$

Obținem $\sigma_1^{\,3}=1_L$, $\sigma_2^{\,2}=1_L$, $\sigma_2\sigma_1=\sigma_1^2\sigma_2$.

De exemplu, pentru a verifica ultima relație, deoarece $\sigma_1(\varepsilon)=\varepsilon$ şi $\sigma_2(\varepsilon)=\varepsilon^2$, rezultă $\sigma_2\sigma_1(\sqrt[3]{2})=\sigma_2(\varepsilon\sqrt[3]{2})=\sigma_2(\varepsilon)\sigma_2(\sqrt[3]{2})=\varepsilon^2\sqrt[3]{2}$ iar $\sigma_2\sigma_1(i\sqrt{3})=\sigma_2(i\sqrt{3})=-i\sqrt{3}$.

Astfel, $G_f\simeq\mathcal{S}_3$.

$H_1=\{1_L,\sigma_1,\sigma_1^2\}$, $H_2=\{1_L,\sigma_2\}$, $H_3=\{1_L,\sigma_1\sigma_2\}$, $H_4=\{1_L,\sigma_1^2\sigma_2\}$

sunt toate subgrupurile proprii ale lui G_f.

Să determinăm acum corpurile intermediare ale extinderii.

Cum $\mathbb{Q}\left(i\sqrt{3}\right)\subseteq L^{H_1}=E_1$ şi $\left[E_1:\mathbb{Q}\right]=2=\left[\mathbb{Q}\left(i\sqrt{3}\right):\mathbb{Q}\right]$, rezultă $E_1=\mathbb{Q}\left(i\sqrt{3}\right)$. În mod analog, se obţine $E_2=\mathbb{Q}\left(\sqrt[3]{2}\right)$.

Să observăm că $\sigma_1\sigma_2\left(\varepsilon^2\sqrt[3]{2}\right)=\varepsilon^2\sqrt[3]{2}$, deci $\mathbb{Q}\left(\varepsilon^2\sqrt[3]{2}\right)\subseteq E_3$. Cum $\left[\mathbb{Q}\left(\varepsilon^2\sqrt[3]{2}\right):\mathbb{Q}\right]=3$, $E_3=\mathbb{Q}\left(\varepsilon^2\sqrt[3]{2}\right)$. La fel, $E_4=\mathbb{Q}\left(\varepsilon\sqrt[3]{2}\right)$.

Din exerciţiul V.17, rezultă că extinderea $E_1\supseteq\mathbb{Q}$ este normală şi, din exerciţiul V.19., obţinem că celelalte extinderi nu sunt normale.

d) $L=\mathbb{Q}\left(\sqrt[4]{2},i\right)$, $\left[L:\mathbb{Q}\right]=8$. Grupul G_f este format din următoarele automorfisme:

	1_L	σ_1	σ_2	σ_2^2	σ_2^3	$\sigma_2\sigma_1$	$\sigma_2^2\sigma_1$	$\sigma_2^3\sigma_1$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
i	i	$-i$	i	i	i	$-i$	$-i$	$-i$

unde, $\sigma_1^2=1_L$, $\sigma_2^4=1_L$, $\sigma_1\sigma_2=\sigma_2^3\sigma_1$.

Astfel, G_f este izomorf cu grupul diedral D_4.

Subgrupurile proprii ale lui G sunt:

$H_1=\left\{1_L,\sigma_1\right\}$, $H_2=\left\{1_L,\sigma_2^2\right\}$, $H_3=\left\{1_L,\sigma_2\sigma_1\right\}$, $H_4=\left\{1_L,\sigma_1\sigma_2\right\}$,

$H_5=\left\{1_L,\sigma_2^2\sigma_1\right\}$, $H_6=\left\{1_L,\sigma_2,\sigma_2^2,\sigma_2^3\right\}$, $H_7=\left\{1_L,\sigma_1,\sigma_2^2,\sigma_2^2\sigma_1\right\}$,

$H_8=\left\{1_L,\sigma_2\sigma_1,\sigma_2^2,\sigma_2^3\sigma_1\right\}$.

Procedând ca înainte, rezultă $E_1=L^{H_1}=\mathbb{Q}\left(\sqrt[4]{2}\right)$, $E_6=L^{H_6}=\mathbb{Q}\left(i\right)$.

Se observă că $\sigma_2^2\left(\sqrt{2}\right)=\sigma_2^2\left(\left(\sqrt[4]{2}\right)^2\right)=\sqrt{2}$, aşadar $\mathbb{Q}\left(\sqrt{2},i\right)\subseteq L^{H_2}$.

Din $\left[\mathbb{Q}\left(\sqrt{2},i\right):\mathbb{Q}\right]=4=\left[L^{H_2}:\mathbb{Q}\right]$, rezultă $E_2=L^{H_2}=\mathbb{Q}\left(\sqrt{2},i\right)$.

Cum $L\supseteq\mathbb{Q}$ este extindere simplă, găsim $\theta=i+\sqrt[4]{2}$ un element primitiv al ei şi notăm $\alpha=\theta+\sigma_2\sigma_1(\theta)=(1+i)\sqrt[4]{2}$.

Din $\sigma_2\sigma_1(\alpha)=\alpha$, rezultă $\mathbb{Q}(\alpha)\subseteq L^{H_3}$. Considerăm lanțul de extinderi $\mathbb{Q}\subseteq\mathbb{Q}\left(i\sqrt{2}\right)\subseteq\mathbb{Q}(\alpha)\subseteq L^{H_3}$.

Rădăcinile polinomului ireductibil $g=X^2-2i\sqrt{2}\in\mathbb{Q}\left(i\sqrt{2}\right)[X]$ sunt $\alpha,-\alpha$. Deci, $\mathbb{Q}(\alpha)$ este corp de descompunere al lui g peste $\mathbb{Q}\left(i\sqrt{2}\right)$. Deoarece

$$\left[\mathbb{Q}\left(i\sqrt{2}\right):\mathbb{Q}\right]=2,\ \left[\mathbb{Q}(\alpha):\mathbb{Q}\left(i\sqrt{2}\right)\right]=2,\ \left[L^{H_3}:\mathbb{Q}\right]=|G/H_3|=4,$$

rezultă $E_3=L^{H_3}=\mathbb{Q}(\alpha)$. Analog, $E_4=L^{H_4}=\mathbb{Q}\left((1-i)\sqrt[4]{2}\right)$.

Din definiția morfismului $\sigma_2^2\sigma_1$, știm că $\mathbb{Q}\left(i\sqrt[4]{2}\right)\subseteq L^{H_5}$. Pentru a obține E_5, observăm că $\mathbb{Q}\left(i\sqrt[4]{2}\right)$ este corp de descompunere pentru polinomul ireductibil $h=X^2+\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right)[X]$. Atunci,

$$\left[\mathbb{Q}\left(i\sqrt[4]{2}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]=\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2 \text{ şi } E_5=L^{H_5}=\mathbb{Q}\left(i\sqrt[4]{2}\right).$$

Pentru celelalte subgrupuri obținem:

$$E_7=L^{H_7}=\mathbb{Q}\left(\sqrt{2}\right) \text{ şi } E_8=L^{H_8}=\mathbb{Q}\left(i\sqrt{2}\right).$$

Dintre aceste corpuri intermediare, cum E_6, E_7 şi E_8 sunt extinderi pătratice ale lui $\mathbb{Q}$, ele sunt normale.

E_2 este extindere normală a lui $\mathbb{Q}$ deoarece E_2 este corp de descompunere al polinomului $f=(X^2+1)(X^2-2)\in\mathbb{Q}[X]$.

$E_1\supseteq\mathbb{Q}$ nu este extindere normală deoarece polinomul ireductibil $X^4-2\in\mathbb{Q}[X]$ cu toate că are rădăcini în E_1, nu le are pe toate. La fel, se motivează că extinderea $E_5\supseteq\mathbb{Q}$ nu este normală.

Extinderile $E_3\supseteq\mathbb{Q}$ şi $E_4\supseteq\mathbb{Q}$ nu sunt normale. Pentru a stabili acest rezultat, arătăm că H_3 şi H_4 nu sunt subgrupuri normale ale lui G_f. Această afirmație rezultă în urma unui calcul de forma:

$\sigma_2^{-1}(\sigma_2\sigma_1)\sigma_2=\sigma_1\sigma_2\notin H_3$.

Capitolul VI

1. În fiecare din aceste cazuri, $L=\mathbb{Q}(\xi)$, unde ξ este o rădăcină primitivă de grad *n* a unității. Considerăm $\lambda: G_f \to U(\mathbb{Z}_n)$, definit prin $\lambda(\sigma)=\hat{q}$, dacă $\sigma(\xi)=\xi^q$, conform demonstrației lemei VI.2.1. Obținem că G_f este izomorf cu $\operatorname{Im}\lambda$, subgrup al grupului $U\left(\mathbb{Z}_n\right)$.

Grupul G_f fiind comutativ, toate subgrupurile sale sunt normale, deci corpurile intermediare sunt extinderi normale.

a) ξ fiind rădăcină primitivă de ordin 5 a unității, $\left[\mathbb{Q}(\xi):\mathbb{Q}\right]=4$, cum $p_\xi = F_5 = X^4+X^3+X^2+X+1\in\mathbb{Q}[X]$. Atunci, $G_f \simeq \left(\mathbb{Z}_5^*,\cdot\right)$.

Deoarece $\hat{2}$ este un generator al grupului ciclic $\left(\mathbb{Z}_5^*,\cdot\right)$, vom defini $\sigma\in G_f$, un generator pentru G_f, prin $\sigma(\xi)=\xi^2$.

Astfel, $G_f=\left\{1_L,\sigma,\sigma^2,\sigma^3\right\}$. $H=\left\{1_L,\sigma^2\right\}$ este singurul său subgrup propriu, care este evident, subgrup normal.

Fie $\alpha=\xi+\sigma^2\left(\xi\right)=\xi+\xi^4$. Din $\sigma^2\left(\alpha\right)=\alpha$, $\mathbb{Q}\left(\alpha\right)\subseteq L^H$. Fie lanțul de extinderi finite: $\mathbb{Q}\subseteq\mathbb{Q}\left(\xi+\xi^4\right)\subseteq L^H\subseteq\mathbb{Q}\left(\xi\right)$.

Știm că $\left[\mathbb{Q}\left(\xi\right):L^H\right]=\left|H\right|=2$. Deoarece $\mathbb{Q}(\xi)$ este corp de descompunere al polinomului $X^2-\left(\xi+\xi^4\right)X+1$ peste corpul $\mathbb{Q}(\xi+\xi^4)$, rezultă $\left[\mathbb{Q}\left(\xi\right):\mathbb{Q}\left(\xi+\xi^4\right)\right]=2$. $L^H=\mathbb{Q}(\xi+\xi^4)$ este singurul corp intermediar, diferit de *L* şi de $\mathbb{Q}$, al extinderii.

b) Fie ξ o rădăcină primitivă de ordin 7 a unității cu $F_7\in\mathbb{Q}[X]$, polinomul său minimal. Procedând analog primului subpunct, obținem că G_f este grup ciclic, izomorf cu $\left(\mathbb{Z}_7^*,\cdot\right)=\left\langle\hat{3}\right\rangle$. Un generator al grupului Galois, $\sigma\in G_f$, este definit de relația $\sigma(\xi)=\xi^3$. Deci,

$$G_f=\left\{1_L,\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5\right\}.$$

$H_1 = \{1_L, \sigma^2, \sigma^4\}$ şi $H_2 = \{1_L, \sigma^3\}$ sunt singurele sale subgrupuri proprii.

$\theta = \xi + \sigma^2(\xi) + \sigma^4(\xi) = \xi + \xi^2 + \xi^4$ este invariat de subgrupul H_1 (folosim $\xi^7 = 1$ şi $\sigma^6 = 1_L$). Prin urmare, $\mathbb{Q}(\theta) \subseteq L^{H_1}$.

Considerăm polinomul

$$g = (X - \xi)(X - \xi^2)(X - \xi^4) = X^3 - \left(\xi + \xi^2 + \xi^4\right)X^2 +$$

$$+\left(\xi^3 + \xi^5 + \xi^6\right)X - \xi^7 = X^3 - \theta X^2 - (1 + \theta)X - 1 \in \mathbb{Q}(\theta)[X].$$

Deoarece $d^\circ g = 3$ şi g nu are rădăcini în $\mathbb{Q}(\theta)$, g este ireductibil în $\mathbb{Q}(\theta)[X]$, deci $\left[\mathbb{Q}(\xi) : \mathbb{Q}(\theta)\right] = 3$. Din $\left[\mathbb{Q}(\xi) : L^{H_1}\right] = |H_1| = 3$, rezultă $\mathbb{Q}(\theta) = L^{H_1} = E_1$.

Analog, $E_2 = L^{H_2} = \mathbb{Q}(\xi + \xi^6)$.

c) Dacă ξ este rădăcină de ordinul 12 a unității, $F_{12} = X^4 - X^2 + 1$ este polinomul său minimal şi astfel, $|G_f| = [\mathbb{Q}(\xi) : \mathbb{Q}] = 4$.

Rădăcinile polinomului ciclotomic F_{12} sunt $\xi, \xi^5, \xi^7, \xi^{11}$. Ştim că orice $\sigma \in G_f$ permută rădăcinile lui F_{12}. Deoarece $|G_f| = |U(\mathbb{Z}_{12})|$, morfismul injectiv $\lambda : G_f \to U(\mathbb{Z}_{12})$, definit la începutul exercițiului, prin $\lambda(\sigma) = \hat{q}$, $\sigma(\xi) = \xi^q$, $(q, 12) = 1$, este izomorfism.

$G_f = \{1_L, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ unde $\sigma_1(\xi) = \xi^5$, $\sigma_2(\xi) = \xi^7$ este izomorf cu grupul lui Klein. Subgrupurile proprii sunt:

$$H_1 = \{1_L, \sigma_1\}, \; H_2 = \{1_L, \sigma_2\}, \; H_3 = \{1_L, \sigma_1\sigma_2\}.$$

Deoarece $\alpha_1 = \xi + \sigma_1(\xi) = \xi + \xi^5$ este invariat de H_1, rezultă că $\mathbb{Q}(\alpha_1) \subseteq L^{H_1}$. Polinomul $g = X^2 - \left(\xi + \xi^5\right)X - 1 \in \mathbb{Q}(\alpha_1)[X]$ are ca rădăcină pe ξ (se arată că $\xi^6 = -1$), deci $\left[\mathbb{Q}(\xi) : \mathbb{Q}(\alpha_1)\right] = 2$. Cum şi $\left[\mathbb{Q}(\xi) : L^{H_1}\right] = 2$, obținem $L^{H_1} = \mathbb{Q}(\alpha_1)$.

În mod analog, $L^{H_3} = \mathbb{Q}(\alpha_2)$, unde $\alpha_2 = \xi + \sigma_1\sigma_2(\xi) = \xi + \xi^{11}$.

Din $\sigma_2(\xi)=\xi^7=-\xi$, rezultă că $\sigma_2(\xi^2)=\xi^2$, deci $\mathbb{Q}\left(\xi^2\right)\subseteq L^{H_2}$. Un corp de descompunere al polinomului $X^2-\xi^2\in\mathbb{Q}\left(\xi^2\right)[X]$ este $\mathbb{Q}(\xi)$, de unde $\left[\mathbb{Q}(\xi):\mathbb{Q}\left(\xi^2\right)\right]=2$. Din $\left[\mathbb{Q}(\xi):L^{H_2}\right]=2$, rezultă că $L^{H_2}=\mathbb{Q}\left(\xi^2\right)$.

2. Demonstrația parcurge mai multe etape:

(i) Fie (i_1i_2) o transpoziție din G. Notăm cu m $(m\le p)$ numărul maxim pentru care $(i_1i_2),(i_1i_3),...,(i_1i_m)\in G$. Pentru orice $1\le q,r\le m$, din $(i_qi_r)=(i_1i_q)(i_1i_r)(i_1i_q)\in G$ rezultă $(i_qi_r)\in G$.

(ii) Fie acum $1\le j\le p$, $j\notin\{i_1,...,i_m\}$ şi arătăm că $(ji_q)\notin G$. Într-adevăr, dacă presupunem $(ji_q)\in G$, cum $(i_1j)=(i_1i_q)(ji_q)(i_1i_q)$, rezultă $(i_1j)\in G$ ceea ce contrazice alegerea lui m.

(iii) Pentru că orice permutare din $\mathscr{S}_p$ se scrie ca produs de transpoziții, pentru a arăta că $G=\mathscr{S}_p$ este suficient să demonstrăm că G conține orice transpoziție din $\mathscr{S}_p$ adică, $m=p$.

Procedăm prin reducere la absurd şi presupunem că $m<p$. Există atunci $1\le j_1\le p$, $j_1\notin\{i_1,...,i_m\}$. G fiind grup tranzitiv, există $\sigma\in G$ astfel încât $\sigma(i_1)=j_1$.

Pentru $1\le k\le m$, notăm $\sigma(i_k)=j_k$ şi arătăm că

$$\{i_1,...,i_m\}\cap\{j_1,...,j_m\}=\varnothing.$$

Dacă presupunem $j_t\in\{i_1,...,i_m\}$, rezultă $(j_1j_t)=\sigma(i_1i_t)\sigma^{-1}\in G$, ceea ce contrazice (ii)

Pentru că cele două mulțimi sunt disjuncte, obținem $2m\le p$.

Dacă $2m<p$, repetăm procedeul şi alegem:

$$1\le k_1\le p,\ k_1\notin\{i_1,...,i_m\}\cup\{j_1,...,j_m\}.$$

G fiind tranzitiv, există $\tau\in G$ pentru care $\tau(i_1)=k_1$.

Notând $\tau(i_s)=k_s$, $1\le s\le m$, obținem:

$$\left(\{i_1,...,i_m\}\cup\{j_1,...,j_m\}\right)\cap\{k_1,...,k_m\}=\varnothing.$$

Astfel, $3m\le p$.

Continuând raționamentul, există $l>1$, număr natural, pentru care $ml=p$, deci p nu este număr prim, fals. Astfel, presupunerea făcută este greşită. Aşadar, $m=p$.

3. Fie $\alpha_1,...,\alpha_p$ rădăcinile lui f. Din ipoteză, putem considera α_1, $\alpha_2\in\mathbb{C}$, $\alpha_3,...,\alpha_p\in\mathbb{R}$. Cum $K\subseteq\mathbb{R}$, $\alpha_2=\overline{\alpha_1}$. Corpul de descompunere al lui f este $L=K(\alpha_1,...,\alpha_p)$. Fie $G=G(L|K)$ grupul Galois asociat extinderii şi $A=\{\alpha_1,...,\alpha_p\}$. Notăm cu $\mathscr{S}_A$ grupul de permutări al mulțimii A. Se verifică imediat că aplicația $\varphi:G\to\mathscr{S}_A$ definită prin $\varphi(\sigma)=\sigma|_A$, $\forall\sigma\in G$, este un morfism injectiv de grupuri. Deoarece $\mathscr{S}_p\simeq\mathscr{S}_A$, pentru a încheia demonstrația, este suficient să arătăm că φ este surjectiv, adică $G\simeq\operatorname{Im}\varphi=\mathscr{S}_A$.

Definim $u\in Aut(\mathbb{C})$, $u(a+bi)=a-bi$, $\forall a,b\in\mathbb{R}$ şi $v=u|_L$.

Din $v(\alpha_1)=\alpha_2$, $v(\alpha_2)=\alpha_1$ şi $v(\alpha_j)=\alpha_j$, $3\le j\le p$, obținem că $\varphi(v)=v|_A$ este o transpoziție. Cu alte cuvinte, $\operatorname{Im}\varphi$ conține o transpoziție. Arătăm acum că $\operatorname{Im}\varphi$ este subgrup tranzitiv. Fie $\alpha_i,\alpha_j\in A$.

Deoarece elementele sunt conjugate (ele au acelaşi polinom minimal), există $\sigma\in G$ pentru care avem $\sigma(\alpha_i)=\alpha_j$, deci $\operatorname{Im}\varphi$ este tranzitiv. Astfel, putem aplica rezultatul exercițiului anterior pentru $\operatorname{Im}\varphi$ şi va rezulta că $\operatorname{Im}\varphi=\mathscr{S}_A$.

4. Fie m, număr natural par, nenul şi $n_1<n_2<...<n_{k-2}$ numere întregi pare, unde $k>3$ este impar. Considerăm polinomul

$$f=\left(X^2+m\right)\left(X-n_1\right)\left(X-n_2\right)...\left(X-n_{k-2}\right).$$

Polinomul are $k-2$ rădăcini reale. Aplicând teorema lui Rolle, f are cel puțin $k-3$ extreme, dintre care $\frac{k-3}{2}$ sunt maxime şi $\frac{k-3}{2}$ sunt minime. Deoarece $m\ge 2$ şi $n_1,n_2,...,n_{k-2}$ sunt numere pare, rezultă

că, pentru orice h , număr impar, avem $|f(h)|>2.$ Astfel, valorile lui f în punctele de maxim sunt $>2.$

Notăm $g=f-2.$ Atunci, g are cel puțin $\frac{k-3}{2}$ maxime și $\frac{k-3}{2}$ minime iar valorile lui g în punctele de maxim sunt $>0.$ Pentru că sunt $\frac{k-3}{2}$ maxime și $\frac{k-3}{2}$ minime, rezultă că g are cel puțin $k-3$ rădăcini. Din $g(n_{k-2})=-2$ și $\lim_{x\to\infty} g(x)=\infty,$ obținem că g mai are o rădăcină reală $>n_{k-2}.$ Astfel, g are cel puțin $k-2$ rădăcini reale. Cum $d^{\circ}g=k,$ g va avea cel mult două rădăcini complexe.

Fie $\alpha_1,\alpha_2,...,\alpha_k$ toate rădăcinile lui g. Identificând coeficienții în relația $g=f-2,$ obținem:

$$\sum_{i=1}^{k}\alpha_i=\sum_{j=1}^{k-2}n_j,\quad \sum_{1\le i<j\le k}\alpha_i\alpha_j=\sum_{1\le s<t\le k-2}n_sn_t+m.$$

Atunci, $\sum_{i=1}^{k}\alpha_i^2=\left(\sum_{i=1}^{k}\alpha_i\right)^2-2\sum_{1\le i<j\le k}\alpha_i\alpha_j=\sum_{j=1}^{k-2}n_j^2-2m.$

Pentru o valoare suficient de mare a lui $m,$ $\sum_{i=1}^{k}\alpha_i^2=\sum_{j=1}^{k-2}n_j^2-2m<0.$

În acest caz, g va avea 2 rădăcini complexe (conjugate) și $k-2$ rădăcini reale.

Arătăm că polinomul g este ireductibil în $\mathbb{Q}[X].$ Pentru aceasta, scriem polinomul f sub forma $f=X^k+a_{k-1}X^{k-1}+...+a_1X+a_0$ unde a_i sunt numere pare, $\forall i\in\overline{0,k-1}.$

Cum $a_0=-mn_1n_2...n_{k-2}$ și $k>3,$ obținem $4\,|\,a_0$.

Astfel, $g=X^k+a_{k-1}X^{k-1}+...+a_1X+(a_0-2)$ are toți coeficienții pari (mai puțin cel dominant) și $4\nmid(a_0-2).$

Aplicând criteriul lui Eisenstein, g este ireductibil în $\mathbb{Q}[X].$

Acum, dacă alegem $k=p,$ cu p număr prim, $p>3,$ din exercițiul VI.3., rezultă $G\left(\mathbb{Q}(\alpha_1,...,\alpha_p)|\mathbb{Q}\right)\simeq\mathscr{S}_p.$

5. Polinomul

$$f = X\left(X^2-4\right)\left(X^2+2\right)-2 = X^5-2X^3-8X-2 \in \mathbb{Q}[X]$$

este ireductibil (se aplică criteriul de ireductibilitate al lui Eisenstein, pentru $p=2$). Deoarece $f'(x)=\left(x^2-2\right)\left(5x^2+4\right)$, folosind şirul lui Rolle, rezultă că f are doar două rădăcini complexe. De asemenea, $d^\circ f = 5$, număr prim. Conform exerciţiului VI.3., Grupul Galois asociat polinomului este izomorf cu $\mathscr{S}_5$, deci nu este rezolubil. Astfel, ecuaţia $f(x)=0$ nu este rezolvabilă prin radicali.

6. Fie $\xi = \cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$ o rădăcină primitivă de ordin 5 a unităţii. Cum $\xi^4 = \cos\frac{2\pi}{5}-i\sin\frac{2\pi}{5}$, avem $\xi+\xi^4 = 2\cos\frac{2\pi}{5}$.

La fel, $-2\cos\frac{\pi}{5} = \xi^2+\xi^3 = -1-\xi-\xi^4$.

Deoarece $\xi+\xi^2+\xi^3+\xi^4=-1$ şi $(\xi+\xi^4)(\xi^2+\xi^3)=-1$, rezultă că $2\cos\frac{2\pi}{5}$ şi $-2\cos\frac{\pi}{5}$ sunt rădăcini ale polinomului

$$g = \left(X-(\xi+\xi^4)\right)\left(X-(\xi^2+\xi^3)\right) = X^2+X-1$$

care este ireductibil în $\mathbb{Q}[X]$.

De aici, $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$, $\cos\frac{\pi}{5} = \frac{1+\sqrt{5}}{4}$. Folosind primul criteriu de constructibilitate, deducem că $\cos\frac{2\pi}{5}$ şi $\cos\frac{\pi}{5}$ se pot construi cu rigla şi compasul, deoarece polinoamele lor minimale sunt de grad egal cu 2. Astfel, $\sin\frac{2\pi}{5} = \sqrt{1-\cos^2\frac{2\pi}{5}}$ şi $\sin\frac{\pi}{5}$ sunt constructibile cu rigla şi compasul.

Unghiul de măsură $\frac{2\pi}{5}$ este determinat de punctele P_1, P_2, P_3 unde P_1 este originea sistemului de coordonate carteziene xOy ales în plan,

$P_2(1,0)$ şi $P_3\left(\cos\frac{2\pi}{5},\sin\frac{2\pi}{5}\right)$. Pentru unghiul de măsură $\frac{\pi}{5}$, este necesar punctul $P_4\left(\cos\frac{\pi}{5},\sin\frac{\pi}{5}\right)$. Astfel, P_3 şi P_4 se pot construi cu rigla şi compasul din P_1 şi P_2. Segmentele P_2P_3 şi P_2P_4 reprezintă laturile pentagonului, respectiv a decagonului regulat.

7. Unghiul $\alpha = arc\cos\frac{11}{16}$ este determinat de punctele:

$$P_1(0,0),\ P_2(1,0),\ P_3(\cos\alpha,\sin\alpha).$$

Pentru a stabili dacă unghiul α se poate împărţi în trei părţi egale cu rigla şi compasul, vedem dacă punctul $P\left(\cos\frac{\alpha}{3},\sin\frac{\alpha}{3}\right)$ se poate construi cu rigla şi compasul din punctele P_1,P_2,P_3. În acest caz,

$$z_1=0,\ z_2=1,\ z_3=\cos\alpha+i\sin\alpha=\frac{11}{16}+i\frac{3\sqrt{15}}{16}.$$

Deoarece $z_3\in\mathscr{C}(z_1,z_2)$, arătăm că $z\in\mathscr{C}(z_1,z_2)$. Avem $F=\mathbb{Q}$.

Relaţia $\cos\alpha=4\cos^3\frac{\alpha}{3}-3\cos\frac{\alpha}{3}$, arată că $\cos\frac{\alpha}{3}$ este rădăcină a polinomului $f=4X^3-3X-\frac{11}{16}=\frac{1}{16}(4X+1)(16X^2-4X-11)$.

Astfel, polinomul minimal al lui $\cos\frac{\alpha}{3}$ este:

$$g=16X^2-4X-11\in\mathbb{Q}[X].$$

Pentru că $d^\circ g=2,\ \cos\frac{\alpha}{3}\in\mathscr{C}(z_1,z_2)$.

8. Fie $\xi=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}$, rădăcină primitivă de ordinul 7 a unităţii. Pentru a construi cu rigla şi compasul un heptagon regulat, trebuie să poată fi posibilă construcţia unghiului de $\frac{2\pi}{7}$ folosind rigla şi

compasul. Verificăm dacă $\xi \in \mathscr{C}(z_1, z_2)$. Cum $\xi + \xi^6 = 2\cos\frac{2\pi}{7}$, rezultă $\mathbb{Q}(\xi + \xi^6) = \mathbb{Q}\left(\cos\frac{2\pi}{7}\right)$.

Aplicând VI.1.b), $\left[\mathbb{Q}(\xi + \xi^6) : \mathbb{Q}\right] = 3$. Astfel, polinomul minimal al lui $\cos\frac{2\pi}{7}$ peste $\mathbb{Q}$ este de grad 3, adică $\cos\frac{2\pi}{7}$ nu se poate construi cu rigla şi compasul, deci $\xi \notin \mathscr{C}(z_1, z_2)$.

Pentru a putea exprima prin radicali pe $\cos\frac{2\pi}{7}$, căutăm polinomul minimal g al lui $\xi + \xi^6$. Acesta este ireductibil, unitar, de grad 3. Orice altă rădăcină a sa este de forma $\sigma(\xi + \xi^6)$, $\sigma \in G$. Din exerciţiul VI.1.b), grupul Galois G al polinomului F_7 este ciclic, generat de $\sigma \in G$, definit prin $\sigma(\xi) = \xi^3$.
Deoarece $\sigma^3(\xi + \xi^6) = \xi + \xi^6$ şi g nu are rădăcini multiple, rădăcinile lui g sunt:
$\xi + \xi^6$, $\sigma(\xi + \xi^6) = \xi^3 + \xi^4$ şi $\sigma^2(\xi + \xi^6) = \xi^2 + \xi^5$.
Astfel,

$$g = \left(X - (\xi + \xi^6)\right)\left(X - \sigma(\xi + \xi^6)\right)\left(X - \sigma^2(\xi + \xi^6)\right) =$$
$$= X^3 + X^2 - 2X - 1$$

este polinomul minimal al lui $\xi + \xi^6$.

Cum $g\left(2\cos\frac{2\pi}{7}\right) = 0$, folosind formulele lui Cardano, putem exprima $\cos\frac{2\pi}{7}$ prin radicali.

9. Fie p semiperimetrul triunghiului. Dacă AA' este bisectoarea unghiului A, cu $A' \in BC$, lungimea segmentului $\left[AA'\right]$ este dată de:

$i_a = \dfrac{2p\sin\dfrac{B}{2}\sin\dfrac{C}{2}}{\cos\dfrac{A}{2}\cos\dfrac{B-C}{2}}$. Analog, $i_b = \dfrac{2p\sin\dfrac{C}{2}\sin\dfrac{A}{2}}{\cos\dfrac{B}{2}\cos\dfrac{C-A}{2}}$.

Din enunț, $\measuredangle B \equiv \measuredangle C$ şi $A + 2B = \pi$. Atunci,

$$i_a = 3i_b \Leftrightarrow \sin B\cos\frac{C-A}{2} = 3\sin A.$$

Cum $\sin A = \sin 2B$ şi $\cos\dfrac{C-A}{2} = \sin\dfrac{3B}{2}$, obținem $\sin\dfrac{3B}{2} = 6\cos B$.

Notând $\alpha = \sin\dfrac{B}{2}$, relația devine $3\alpha - 4\alpha^3 = 6(1-2\alpha^2)$ adică α este rădăcină a lui $f = 4X^3 - 12X^2 - 3X + 6$, polinom ireductibil în $\mathbb{Q}[X]$ (se aplică criteriul de ireductibilitate al lui Eisenstein pentru $p = 3$). Deoarece $d^\circ f = 3$, $\alpha \notin \mathscr{C}(z_1, z_2)$. Astfel, triunghiul ΔABC nu poate fi construit cu rigla şi compasul.

10. Deoarece poligonul regulat cu *n* laturi se poate construi cu rigla şi compasul, $n = 2^t p_1 p_2 ... p_m$ unde $t \in \mathbb{N}$ iar p_i, $1 \le i \le m$, sunt numere prime Fermat distincte. Pentru ca şi poligonul regulat cu $p^k n$ laturi, $k \ge 1$, să fie construibil cu rigla şi compasul, $p^k n$ trebuie să se scrie sub aceeaşi formă. Astfel, $p = 2$ este singura valoare care convine pentru orice $k > 1$, iar pentru cazul în care $k = 1$, $p = 2$ sau *p* poate fi orice număr prim Fermat diferit de fiecare p_i, $1 \le i \le m$.

11. Trebuie să determinăm numerele de forma $n = 2^t p_1 p_2 ... p_m$ cu $t \in \mathbb{N}$ iar p_i, $1 \le i \le m$, numere prime Fermat distincte, $15 \le n \le 33$. Singurele numere Fermat ≤ 33 sunt 3, 5, 17. Astfel, pentru ca poligonul regulat cu *n* laturi să se poată construi cu rigla şi compasul, $n \in \{15, 16, 17, 20, 24, 30, 32\}$.

BIBLIOGRAFIE

1. Atiyah, M., Mac Donald, I., *Introduction to Commutative Algebra*, Addison Wesley Publishing Company, 1969.
2. Barbilian, D., *Algebra*, Editura Didactică şi Pedagogică, Bucureşti, 1985.
3. Baumslag, B., Chandler, B., *Theory and Problems of Group Theory*, McGraw-Hill Inc., 1968.
4. Becheanu, M., Dincă, A., Ion, I.D., Niţă, C., Purdea, I., Radu, N., Ştefănescu, M., Vraciu, C., *Algebră*, Editura All, Bucureşti, 1998.
5. Bourbaki, N., *Algèbre*, chap. 3-5, Hermann, 1967.
6. Buşneag, D., *Capitole speciale de algebră*, Editura Universitaria, Craiova, 1977.
7. Dan., C., *Probleme de algebră*, *Inele, module, Teorie Galois*, Reprografia Universităţii din Craiova, 2000.
8. Dincă, A., *Lecţii de algebră*, Editura Universitaria, Craiova, 2000.
9. Faddéev, D., Sominski, I., *Recueil d' exercices d' algèbre supérieure*, Éditions Mir, Moscou,1972.
10. Ion, I.D., Niţă, C., *Elemente de aritmetică cu aplicaţii în tehnici de calcul*, Editura Tehnică, Bucureşti, 1978.
11. Ion, I.D., Niţă, C., Popescu, D., Radu, N., *Probleme de algebră*, Editura Didactică şi Pedagogică, Bucureşti, 1981.
12. Ion, I.D., Radu, N., *Algebră*, Editura Didactică şi Pedagogică, Bucureşti, 1981, 1991.
13. Jacobson, N., *Lectures in Abstract Algebra*, III. *Theory of Fields and Galois Theory*, Springer Verlag, New-York, 1964.
14. Kostrikin, A., *Introduction à l' algèbre*, Éditions Mir, Moscou, 1981.

15. Lang, S., *Algebra*, Addison Wesley Publishing Company, London, 1965.
16. Luchian, T., *Algebră abstractă*, Editura Didactică şi Pedagogică, Bucureşti, 1975.
17. Mignotte, M., *Mathématiques pour le calcul formel*, P.U.F., Paris, 1989.
18. Naudin, P., Quitté, C., *Algorithmique algèbrique*, Masson, Paris, 1992.
19. Năstăsescu, C., *Inele, module, categorii*, Editura Academiei, Bucureşti, 1976.
20. Năstăsescu, C., Niţă, C., *Teoria calitativă a ecuaţiilor algebrice*, Editura Tehnică, Bucureşti, 1979.
21. Năstăsescu, C., Niţă, C., Vraciu, C., *Bazele algebrei* I, Editura Academiei, Bucureşti, 1986.
22. Năstăsescu, C., Niţă, C., Vraciu, C., *Aritmetică şi algebră*, Editura Didactică şi Pedagogică, Bucureşti, 1993.
23. Pic, Gh., Purdea, I., *Tratat de algebră modernă*, Editura Academiei, Bucureşti, 1977.
24. Popovici, C.P., *Logică şi teoria numerelor*, Editura Didactică şi Pedagogică, Bucureşti, 1970.
25. Purdea, I., *Tratat de algebră modernă*, II, Editura Academiei, Bucureşti, 1982.
26. Radu, N., & colab., *Algebră pentru perfecţionarea profesorilor*, Editura Didactică şi Pedagogică, Bucureşti, 1983.
27. Rosen, K.H., *Elementary Number Theory and Its Applications*, Addison, Wesley Publishing Company, 1988.
28. Rotman, J.J., *The Theory of Groups*, *An Introduction*, Allyn and Bacon Inc., 1966.
29. Van der Waerden, *Algebra*, Springer Verlag, 1967.
30. Voïevodine, V., *Algèbre linèaire*, Éditions Mir, Moscou, 1976.

INDEX

NOTAȚII

$a \mid b$	a divide b
$a \sim b$	a asociat în divizibilitate cu b
(a)	idealul principal generat de a
$(a_1,...,a_n)$	cel mai mare divizor comun al elementelor $a_1,...,a_n$
$[a_1,...,a_n]$	cel mai mic multiplu comun al elementelor $a_1,...,a_n$
a/s	fracție
$\mathcal{A}_n$	grupul altern (al permutărilor pare) de grad n
$Aut(L)$	grupul automorfismelor corpului L
A/I	inelul factor al inelului A prin idealul său bilateral I
A_S	inelul de fracții al inelului A relativ la sistemul S
$car(A)$	caracteristica inelului A
$card(M)$	cardinalul mulțimii M
$c(f)$	conținutul polinomului f
$\mathcal{C}(P_1,...,P_n)$	mulțimea punctelor din plan constructibile cu rigla şi compasul din punctele $P_1,...,P_n$.
$\mathcal{C}(z_1,...,z_n)$	mulțimea numerelor complexe constructibile cu rigla şi compasul din numerele $z_1,...,z_n$.
$C(a)$	centralizatorul elementului a
$\mathbb{C}'$	corpul numerelor algebrice
$d^\circ f$	gradul polinomului f
D_n	grupul diedral de ordin n
Df	derivata formală a polinomului f

E_1E_2	compozitul corpurilor E_1 şi E_2
F_n	al n – lea polinom ciclotomic
$GL_n(R)$	grupul liniar de grad n peste R
$G(L \mid K)$	grupul Galois al extinderii $L \supseteq K$
G_f	grupul Galois al polinomului f
$(G:H)$	indicele subgrupului H în grupul G
G'	subgrupul derivat (comutant) al grupului G
$G^{(n)}$	al n – lea comutant al grupului G
$H \trianglelefteq G$	H este subgrup normal al grupului G
Im f	imaginea morfismului f
$I + J$	suma idealelor I şi J
IJ	produsul idealelor I şi J
$Kerf$	nucleul morfismului f
$K[M]$	subinelul generat de mulțimea M peste corpul K
$K(M)$	subcorpul de adjuncționare a mulțimii M la corpul K
$K[X]$	inelul polinoamelor cu coeficienți în corpul K
$K(X)$	corpul fracțiilor raționale
$\overline{K}$	închiderea algebrică a lui K
$[L:K]$	gradul extinderii $L \supseteq K$
L^H	subcorpul intermediar format din elementele corpului L, invariate de toate automorfismele din subgrupul H
${}_K L$	L este spațiu vectorial peste K
$\mathscr{L}(A)$	laticea idealelor bilaterale ale inelului A
$\mathscr{L}(A;Kerf)$	laticea idealelor bilaterale ale inelului A, care includ $Kerf$
$\mathscr{L}(L;K)$	laticea subcorpurilor intermediare între L şi K

$\mathscr{L}(G)$	laticea subgrupurilor grupului G
$\|M\|$	cardinalul mulțimii finite M
$M_n(R)$	inelul matricelor pătratice de ordin n cu elemente din inelul R
orda	ordinul elementului a
p_θ	polinomul minimal al elementului algebric θ
$\mathscr{S}(A)$	mulțimea subinelelor inelului A
$\mathscr{S}(A;Kerf)$	mulțimea subinelelor inelului A, care includ $Kerf$
$\mathscr{S}(M)$	grupul permutărilor mulțimii M
$\mathscr{S}_n$	grupul permutărilor de grad n
$U(A)$	grupul multiplicativ al unităților inelului A
U_n	grupul multiplicativ al rădăcinilor de grad n ale unității
$\hat{x}$	clasa elementului x
$[x,y]$	comutatorul elementelor x şi y
$\mathbb{Z}[i]$	inelul întregilor lui Gauss
$Z(G)$	centrul grupului G
$\mathbb{Z}_n$	inelul claselor de resturi modulo n
(ξ^p,α)	p – rezolventa Lagrange asociată lui α
$\varphi(n)$	indicatorul lui Euler pentru numărul natural n