Corpuri cu divizori primi

Costel Gabriel Bontea

September 11, 2012

Cuprins

Notaţii

Următoarele notaţii sunt folosite în text fără explicaţii:

$\mathbb{Z}$	=	mulţimea numerelor întregi
$\mathbb{Q}$	=	mulţimea numerelor raţionale
$\mathbb{R}$	=	mulţimea numerelor reale
$\mathbb{C}$	=	mulţimea numerelor complexe
E/F	=	E e o extindere a corpului F
$[E:F]$	=	gradul extinderii E/F
$P_{\alpha,F}$	=	polinomul minimal al lui α peste F
$P_{\alpha,E/F}$	=	polinomul caracteristic al lui $\alpha \in E$ în extinderea E/F
$\mathrm{N}_{E/F}(\alpha)$	=	norma lui α în extinderea E/F
$\mathrm{Tr}_{E/F}(\alpha)$	=	urma lui α în extinderea E/F
$\mathrm{Gal}(E/F)$	=	grupul F-automorfismelor lui E

Introducere

O bună cunoaştere a teoriei valuărilor este indispensabilă oricui ar vrea să se angajeze în studiul teoriei algebrice moderne a numerelor. Acesta a fost motivul care m-a făcut să aleg ca subiect pentru prezenta lucrare studiul corpurilor cu divizori primi. Din cauza limitărilor unei astfel de lucrări, însă, am fost nevoit să reduc studiul la rezultatele de bază ale teoriei.

Am început, aşadar, în capitolul 1, cu prezentarea noţiunii de valuare a unui corp şi a topologiei definite de o valuare. Folosindu-mă de cât mai multe exemple, am încercat să arăt că studiul unor astfel de obiecte merită întreprins. Am introdus, în continuare, relaţia de echivalenţa pe mulţimea valuărilor unui corp şi am caracterizat valuările echivalente. Apoi, după ce am definit noţiunea de divizor prim ca fiind o clasă de echivalenţa de valuări, am arătat că topologia definită de o valuare e o topologie metrică. La sfarşitul capitolului am definit primele noţiuni legate de extinderea divizorilor primi.

În capitolul următor am aprofundat studiul valuărilor nearhimediene şi a divizorilor primi nearhimedieni. Unui astfel de divizor i-am asociat un inel local şi am văzut cum arată acest inel în cazul exemplelor din primul capitol. Punând în evidenţă divizorii primi nearhimedieni ai unui corp de numere algebrice, am făcut cunoscută tema recurentă a lucrării: aceea de a aplica teoria la cazul corpurilor de numere algebrice. După o scurtă trecere în revistă a divizorilor primi discreţi, am definit indicele de ramificare şi gradul rezidual şi am făcut legătura cu ramificarea în corpuri de numere algebrice.

Capitolul 3 a fost devotat unei construcţii importante din teoria valuărilor, anume, aceea de completat al unui corp cu un divizor prim. Modelul pentru o astfel de construcţie poate fi luat corpul numerelor reale, care e completatul corpului numerelor raţionale în raport cu divizorul prim care conţine valoarea absolută. După ce am demonstrat existenţa şi unicitatea completatului, am studiat corpurile complete în raport cu divizori primi discreţi

şi corpurile complete în raport cu divizori primi arhimedieni. În cazul din urmă am demonstrat o importantă teoremă a lui Ostrowski care afirmă că, până la un izomorfism de corpuri cu divizori primi, $(\mathbb{R}, P_\infty)$ şi $(\mathbb{C}, P_\infty)$, unde P_∞ e divizorul prim care conţine valoarea absolută, sunt singurele corpuri complete în raport cu divizori primi arhimedieni. În final, am profitat de prilej pentru a determina toţi divizorii primi arhimedieni ai unui corp de numere algebrice.

În capitolul 4 am început studiul extinderilor divizorilor primi, considerând cazul în care corpul de bază e complet. Pentru a demonstra unicitatea extinderii am introdus noţiunea de spaţiu normat peste un corp valuat şi am arătat echivalenţa normelor pe un astfel de spaţiu. Pentru existenţa extinderii am făcut apel la lema lui Hensel şi am văzut alte câteva consecinţe ale acestei leme. Am studiat apoi extinderea divizorilor primi discreţi şi am demonstrat următorul rezultat fundamental: gradul unei extinderi finite a unui corp complet în raport cu un divizor prim discret e produsul indicelui de ramificare cu gradul rezidual. Datorită rezultatelor obţinute am putut, apoi, clasifica corpurile locale.

În ultimul capitol am trecut la studiul extinderilor divizorilor primi în cazul general. Folosindu-ne de informaţiile obţinute în capitolul precedent, am putut dovedi existenţa extinderilor şi, totodată, am putut stabili numărul lor. Am încheiat capitolul cu câteva consecinţe, dintre care mai importantă e identitatea fundamentală a teoriei valuărilor, care, la nivelul corpurilor de numere algebrice se reduce la identitatea fundamentală clasică din teoria ramificării.

Capitolul 1

Valuări şi divizori primi

1.1 Valuări şi topologia definită de o valuare

Noţiunea fundamentală care ne va ajuta să vedem într-o altă perspectivă corpurile de numere algebrice este aceea de *valuare*.

Definiţie 1.1.1. *Fie F un corp. O* ***valuare*** *pe F este o funcţie $\varphi : F \to \mathbb{R}$ pentru care există $C \in \mathbb{R}$ astfel încât următoarele condiţii să fie îndeplinite:*

(i) $\varphi(x) \geq 0$*, pentru orice* $x \in F$*, şi* $\varphi(x) = 0 \Leftrightarrow x = 0$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$*, pentru orice* $x, y \in \mathbb{R}$

(iii) $\varphi(x) \leq 1 \Rightarrow \varphi(1 + x) \leq C$

Să observăm că o valuare φ pe F induce un morfism de grupuri de la $(F^*, \cdot)$ în $(\mathbb{R}_{>0}, \cdot)$, unde s-a notat prin $\mathbb{R}_{>0}$ mulţimea numerelor reale pozitive. Prin urmare, $\varphi(1) = 1$ şi $\varphi(x^{-1}) = 1/\varphi(x)$, pentru orice $x \in F^*$. Cum $\varphi(-1)^2 = \varphi(1) = 1$, avem $\varphi(-1) = 1$ şi $\varphi(-x) = \varphi(-1)\varphi(x) = \varphi(x)$, pentru orice $x \in F$.

Mai observăm că, dacă φ e o valuare pe F, iar C e constanta care apare în condiţia (iii), atunci, oricare ar fi $\alpha > 0$, φ^α rămâne valuare pe F, constanta putând fi aleasă, în cazul acesta, C^α. Dăm în continuare câteva exemple de valuări.

Exemple: (1) Cel mai simplu exemplu de valuare este valuarea pentru care morfismul de la F^* în $\mathbb{R}_{>0}$ este cel trivial, i.e. $\varphi : F \to \mathbb{R}$, $\varphi(0) = 0$ şi $\varphi(x) = 1$, oricare ar fi $x \in F^*$. Numim această valuare, *valuarea trivială*.
(2) Funcţia valoare absolută determină o valuare pe mulţimea numerelor reale $\mathbb{R}$ şi o valuare pe mulţimea numerelor complexe $\mathbb{C}$. În ambele cazuri putem alege $C = 2$.

(3) Pe mulţimea numerelor raţionale $\mathbb{Q}$ putem asocia oricărui număr prim p o infinitate de valuări. Pentru aceasta, se consideră funcţia *ordinal*, $\mathrm{ord}_p : \mathbb{Q}^* \to \mathbb{Z}$, care asociază fiecărui număr raţional nenul x puterea la care apare p în scrierea lui x ca produs de numere prime din $\mathbb{Z}$. Aşadar, dacă $x \in \mathbb{Q}^*$, avem

$$x = \mathrm{sgn}(x) \prod_p p^{\mathrm{ord}_p(x)}$$

unde produsul se face după toate numerele prime (pozitive) ale lui $\mathbb{Z}$, iar sgn e funcţia semn, $\mathrm{sgn}(x) = 1$ dacă $x > 0$ şi $\mathrm{sgn}(x) = -1$ dacă $x < 0$. Cu ajutorul funcţiei ordinal putem defini o valuare pe $\mathbb{Q}$ de îndată ce fixăm $0 < c < 1$. Mai precis, funcţia

$$\varphi_{p,c} : \mathbb{Q} \to \mathbb{R},\ \varphi_{p,c}(x) = \begin{cases} 0 & \text{daca} \quad x = 0 \\ c^{\mathrm{ord}_p(x)} & \text{daca} \quad x \neq 0 \end{cases}$$

este o valuare pe $\mathbb{Q}$. Într-adevăr, condiţiile (i) şi (ii) ale definiţiei 1.1.1 sunt trivial satisfăcute, cea din urmă datorită relaţiei: $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$, pentru orice x, $y \in \mathbb{Q}^*$. Să arătăm că (iii) are loc pentru $C = 1$. Fie $x \in \mathbb{Q}$ astfel încât $\varphi_{p,c}(x) \leq 1$. Dacă $x = 0$ sau $x = -1$ atunci (iii) e verificată. Dacă $x \neq 0, -1$ considerăm a, $b \in \mathbb{Z}$ astfel încât $x = p^{\mathrm{ord}_p(x)} a/b$ şi $p \nmid b$. Atunci $1 + x = (b + p^{\mathrm{ord}_p(x)} a)/b$. Observăm că numărătorul e un număr întreg, deoarece $\mathrm{ord}_p(x) \geq 0$. Cum numitorul e prim cu p, deducem că $\mathrm{ord}_p(1 + x) \geq 0$, deci $\varphi_{p,c}(1 + x) \leq 1$.
(4) Să generalizăm exemplul (3) la cazul corpurilor de numere algebrice. Fie, aşadar, F un corp de numere algebrice, şi $\mathcal{O}_F$ inelul său de întregi algebrici. Ne reamintim că mulţimea idealelor fracţionare nenule ale lui $\mathcal{O}_F$, $\mathcal{I}_F$, formează un grup abelian în raport cu înmulţirea idealelor. Mai mult, $(\mathcal{I}_F, \cdot)$ e grupul abelian liber generat de mulţimea idealelor prime nenule ale lui $\mathcal{O}_F$, i.e. dacă I e un ideal fracţionar nenul al lui $\mathcal{O}_F$, atunci

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)}$$

unde produsul se face după toate idealele prime nenule ale lui $\mathcal{O}_F$, iar $\mathrm{ord}_{\mathfrak{p}}(I)$ sunt numere întregi unic determinate de I şi, mai puţin un număr finit, toate sunt nule.

Fie $\mathfrak{p}$ un ideal prim nenul al lui $\mathcal{O}_F$ şi $v_{\mathfrak{p}} : F^* \to \mathbb{Z}$, funcţia definită prin $v_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_F)$, oricare ar fi $x \in F^*$. Idealului $\mathfrak{p}$ îi putem asocia o infinitate de valuări pe F în felul următor: dacă $0 < c < 1$, atunci

$$\varphi_{\mathfrak{p},c} : F \to \mathbb{R},\ \varphi_{\mathfrak{p},c}(x) = \begin{cases} 0 & \text{daca} \quad x = 0 \\ c^{v_{\mathfrak{p}}(x)} & \text{daca} \quad x \neq 0 \end{cases}$$

e o valuare pe F. Într-adevăr, condiţia (i) din definiţia 1.1.1 e automat satisfacută, iar condiţia (ii) rezultă din relaţia $\mathrm{ord}_{\mathfrak{p}}(IJ) = \mathrm{ord}_{\mathfrak{p}}(I)\mathrm{ord}_{\mathfrak{p}}(J)$, oricare ar fi $I,\ J \in \mathcal{I}_F$. În ceea ce priveşte relaţia (iii) arătăm, ca şi în exemplul (3) că ea e satisfăcută pentru $C = 1$. Fie $x \in F$, $x \neq 0, -1$, astfel încât $\varphi_{\mathfrak{p},c}(x) \leq 1$. Atunci $\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_F) \geq 0$. Fie $\mathfrak{a}$ şi $\mathfrak{b}$ ideale întregi ale lui $\mathcal{O}_F$ astfel încât $x\mathcal{O}_F = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_F)}\mathfrak{a}\mathfrak{b}^{-1}$ si $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0$. Atunci

$$(1+x)\mathcal{O}_F \subseteq \mathcal{O}_F + x\mathcal{O}_F = (\mathfrak{b} + \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_F)}\mathfrak{a})\mathfrak{b}^{-1}$$

Ne reamintim acum că, dacă $I,\ J \in \mathcal{I}_F$, atunci $I \subseteq J$ dacă şi numai dacă $J|I$, i.e. $I = J\mathfrak{c}$, unde $\mathfrak{c}$ e un ideal întreg al lui $\mathcal{O}_F$. Aşadar, $I \subseteq J$ dacă şi numai dacă $\mathrm{ord}_{\mathfrak{p}}(I) \geq \mathrm{ord}_{\mathfrak{p}}(J)$ pentru orice ideal prim nenul $\mathfrak{p}$, al lui $\mathcal{O}_F$. Cum $(1+x)\mathcal{O}_F \subseteq \mathcal{O}_F + x\mathcal{O}_F$, avem $v_{\mathfrak{p}}(1+x) \geq \mathrm{ord}_{\mathfrak{p}}(\mathcal{O}_F + x\mathcal{O}_F)$. Dar $\mathfrak{b} + \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_F)}\mathfrak{a}$ e un ideal intreg al lui $\mathcal{O}_F$, iar $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) = 0$. Prin urmare, $v_{\mathfrak{p}}(1+x) \geq \mathrm{ord}_{\mathfrak{p}}(\mathcal{O}_F + x\mathcal{O}_F) \geq 0$, deci $\varphi_{\mathfrak{p},c}(1+x) \leq 1$. Dacă $x = 0$ sau $x = -1$ atunci (iii) e îndeplinită, după cum se poate verifica cu uşurinţă.
(5) Exemplul de la (3) mai poate fi generalizat într-un mod. Pentru aceasta, fie R un inel factorial cu corpul de fracţii F şi fie $\mathcal{P}$ un sistem reprezentabil de elemente prime asociat lui R. Orice element $x \in F^*$ se scrie atunci în mod unic sub forma

$$x = u\prod_{p\in\mathcal{P}} p^{\mathrm{ord}_p(x)}$$

unde u e element inversabil în R şi $\{\mathrm{ord}_p(x)\}_{p\in\mathcal{P}}$ e o familie de numere întregi de suport finit. La fel de uşor ca în exemplul (3) se arată că, dacă $p \in \mathcal{P}$ şi $0 < c < 1$, atunci funcţia

$$\varphi_{p,c} : F \to \mathbb{R},\ \varphi_{p,c}(x) = \begin{cases} 0 & \text{daca} \quad x = 0 \\ c^{\mathrm{ord}_p(x)} & \text{daca} \quad x \neq 0 \end{cases}$$

e o valuare pe F. Dacă $R = \mathbb{Z}$ şi $\mathcal{P}$ e mulţimea numerelor prime, pozitive, ale lui $\mathbb{Z}$, atunci obţinem valuările din exemplul (3). Dacă F e un corp, $R = F[X]$ e inelul de polinoame în nedeterminata X şi $\mathcal{P}$ e mulţimea polinoamelor monice şi ireductibile ale lui $F[X]$ atunci, pentru fiecare astfel de polinom obţinem o familie de valuări pe $F(X)$ indexate după intervalul $(0,1)$.

Aşa cum corpurile $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ au o topologie naturală indusă de valuarea absolută, la fel se întâmplă cu orice corp pe care e definită o valuare. Avem următoarea

Propoziţie 1.1.1. *Fie φ o valuare a unui corp F. Există o unică topologie τ_φ pe F care admite ca sistem fundamental de vecinătăţi pentru $x \in F$ sistemul format din mulţimile*

$$B(x,\varepsilon) = \{y \in F\ :\ \varphi(x-y) < \varepsilon\},\ \varepsilon > 0$$

Demonstraţie. Fie, pentru orice $x \in F$, $\mathcal{V}_x = \{V \subseteq F : \exists\, \varepsilon > 0$ astfel incat $B(x, \varepsilon) \subseteq V\}$. Atunci $\mathcal{V}_x$ verifică proprietăţile unui sistem de vecinătăţi pentru x:

(1) Dacă $V \in \mathcal{V}_x$, atunci $x \in V$.

(2) Dacă $V \in \mathcal{V}_x$ şi $W \supseteq V$, atunci $W \in \mathcal{V}_x$.

(3) Dacă $V, W \in \mathcal{V}_x$, atunci $V \cap W \in \mathcal{V}_x$.

(4) Dacă $V \in \mathcal{V}_x$, atunci există $W \in \mathcal{V}_x$ astfel încât $W \in \mathcal{V}_y$, pentru orice $y \in V$.

Într-adevăr, (1), (2) şi (3) sunt triviale, iar (4) are loc deoarece, dacă $V \in \mathcal{V}_x$, atunci $W = \bigcup_{y \in V} B(y, \varepsilon)$, unde $\varepsilon > 0$, are proprietatea dorită.

Fie $\tau_\varphi = \{G \subseteq F : G \in \mathcal{V}_x, \text{pentru orice } x \in G\}$. E binecunoscut faptul că τ_φ e unica topologie pe F care admite ca sistem de vecinătăţi pentru $x \in F$ pe $\mathcal{V}_x$. Prin urmare, τ_x e unica topologie pe F care admite ca sistem fundamental de vecinătăţi pentru $x \in F$ sistemul format din mulţimile $B(x, \varepsilon)$, $\varepsilon > 0$. □

Corolar 1.1.1. *Fie φ o valuare a unui corp F, $\{x_n\}$ un şir de elemente din F şi $x \in F$. Atunci*

$$x_n \to x \text{ relativ la } \tau_\varphi \Leftrightarrow \varphi(x_n - x) \to 0$$

Demonstraţie. Ţinând seama de definiţia convergenţei şirurilor în spaţii topologice, şirul $\{x_n\}$ converge la x în topologia definită de φ dacă şi numai dacă, pentru orice $\varepsilon > 0$, există $N \geq 1$ astfel încât $\varphi(x_n - x) < \varepsilon$, oricare ar fi $n \geq N$, i.e. dacă şi numai dacă $\varphi(x_n - x) \to 0$. □

Definiţie 1.1.2. *Spunem că două valuări ale lui F, φ_1 şi φ_2, sunt* ***echivalente****, şi notăm aceasta prin $\varphi_1 \sim \varphi_2$, dacă $\tau_{\varphi_1} = \tau_{\varphi_2}$. Clasele de echivalenţă de valuări în raport cu $\sim$ se numesc* ***divizori primi*** *ai lui F. Divizorul prim care conţine valuarea trivială se numeşte* ***divizorul prim trivial****, iar restul divizorilor primi se numesc* ***divizori primi netriviali***

Vom nota divizorii primi ai lui F prin literele P, Q, etc.

1.2 Caracterizarea valuarilor echivalente

Următoarea teoremă oferă condiţii necesare şi suficiente ca două valuări netriviale să fie echivalente.

Teoremă 1.2.1. *Fie φ_1 şi φ_2 două valuări netriviale pe F. Următoarele afirmaţii sunt echivalente:*

(i) $\varphi_1 \sim \varphi_2$

(ii) $\varphi_1(x) < 1 \Rightarrow \varphi_2(x) < 1$

(iii) $\varphi_1(x) \leq 1 \Rightarrow \varphi_2(x) \leq 1$

(iv) $\varphi_2 = \varphi_1^\alpha$, *unde* $\alpha > 0$

Demonstraţie. (i) $\Rightarrow$ (ii) Dacă $\varphi_1(x) < 1$ atunci $\lim\limits_{n\to\infty} \varphi_1(x^n) = \lim\limits_{n\to\infty} \varphi_1(x)^n = 0$, deci $x^n \to 0$ în topologia definită de φ_1. Cum $T_{\varphi_1} = T_{\varphi_2}$, $x^n \to 0$ în topologia definită de φ_2. Prin urmare, $\lim\limits_{n\to\infty} \varphi_2(x)^n = \lim\limits_{n\to\infty} \varphi_2(x^n) = 0$, de unde deducem că $\varphi_2(x) < 1$.
(ii) $\Rightarrow$ (iii) E de ajuns să arătăm că $\varphi_1(x) = 1 \Rightarrow \varphi_2(x) = 1$. Fie $y \in F$ astfel încât $0 < \varphi_1(y) < 1$ (un astfel de y există, întrucât φ_1 e netrivială). Pentru orice $n \geq 1$, avem $\varphi_1(x^n y) < 1$, deci şi $\varphi_2(x^n y) < 1$. Cum $\varphi_2(x) < \left(\varphi_2(y^{-1})\right)^{1/n}$, pentru orice $n \geq 1$, rezultă, prin trecere la limită, că $\varphi_2(x) \leq 1$. În mod similar, $\varphi_2(x^{-1}) \leq 1$, deci $\varphi_2(x) = 1$.
(iii) $\Rightarrow$ (ii) Fie $x \in F$ astfel încât $\varphi_1(x) < 1$. Deoarece φ_2 nu e trivială, există $y \in F$ astfel încât $0 < \varphi_2(y) < 1$. Ţinând cont de faptul că $\varphi_1(x)^n \to 0$, există n astfel incat $\varphi_1(x)^n \leq \varphi_1(y)$. Aşadar, $\varphi_1(x^n y^{-1}) \leq 1$, deci $\varphi_2(x^n y^{-1}) \leq 1$. Cum $\varphi_2(x)^n \leq \varphi_2(y) < 1$, deducem că $\varphi_2(x) < 1$.
(ii) $\Rightarrow$ (iv) Deoarece φ_1 e netrivială, există $x \in F^*$ astfel încât $\varphi_1(x) < 1$. Conform ipotezei, avem şi $\varphi_2(x) < 1$. Fie $\alpha > 0$ astfel încât $\varphi_2(x) = \varphi_1(x)^\alpha$. Vom demonstra că $\varphi_2 = \varphi_1^\alpha$.

Fie, aşadar, $y \in F^*$. Dorim să arătăm că $\varphi_2(y) = \varphi_1(y)^\alpha$. Să observăm că, atunci când $\varphi_1(y) \neq 1$, ceea ce vrem să arătăm este echivalent cu

$$\frac{\log \varphi_2(y)}{\log \varphi_1(y)} = \alpha = \frac{\log \varphi_2(x)}{\log \varphi_1(x)} \tag{1.1}$$

Fie $\gamma \in \mathbb{R}$ astfel încât $\varphi_1(y) = \varphi_1(x)^\gamma$. Dacă arătăm că $\varphi_2(y) = \varphi_2(x)^\gamma$ atunci vom fi terminat, fiindcă vom avea

$$\frac{\log \varphi_1(y)}{\log \varphi_1(x)} = \gamma = \frac{\log \varphi_2(y)}{\log \varphi_2(x)}$$

şi egalitatea 1.1 va fi satisfăcută când $\gamma \neq 0$ Când $\gamma = 0$, vom avea $\varphi_2(y) = 1 = 1^\alpha = \varphi_1(y)^\alpha$.

Arătăm că $\varphi_2(y) = \varphi_2(x)^\gamma$ prin dubla inegalitate. Fie m/n un număr raţional cu numitorul pozitiv astfel încât $m/n > \gamma$. Atunci, din $\varphi_1(y) =$

$\varphi_1(x)^\gamma > \varphi_1(x)^{m/n}$, rezultă că $\varphi_1(x^m y^{-n}) < 1$. Prin urmare, $\varphi_2(x^m y^{-n}) < 1$, de unde $\varphi_2(y) > \varphi_2(x)^{m/n}$. Alegând convenabil un şir de numere raţionale care să convergă la γ, găsim că $\varphi_2(y) \geq \varphi_2(x)^\gamma$. Fie acum m/n un număr raţional cu numitorul pozitiv astfel încât $m/n < \gamma$. Atunci $\varphi_1(y) = \varphi_1(x)^\gamma < \varphi_1(x)^{m/n}$, deci $\varphi_1(y^n x^{-m}) < 1$. Folosind ipoteza, deducem că $\varphi_2(y^n x^{-m}) < 1$, deci $\varphi_2(y) < \varphi_2(x)^{m/n}$. Alegem, din nou, în mod convenabil, un şir de numere raţionale care să conveargă la γ pentru a deduce că $\varphi_2(y) \leq \varphi_2(x)^\gamma$. Astfel, $\varphi_2(y) = \varphi_2(x)^\gamma$ şi implicaţia (ii) $\Rightarrow$ (iv) e demonstrată.
(iv) $\Rightarrow$ (i) e trivială. □

Corolar 1.2.1. *Fie P un divizor prim al lui F. Atunci, pentru orice $\varphi \in P$,*

$$P = \{\varphi^\alpha \,:\, \alpha > 0\}$$

Demonstraţie. Dacă P e divizorul prim netrivial, afirmaţia rezultă din teorema 1.2.1. Dacă P conţine valuarea trivială, atunci afirmaţia se menţine şi în acest caz, deoarece P nu mai conţine nici o altă valuare. Într-adevăr, fie φ o valuare echivalentă cu valuarea trivială. Dacă, prin absurd, φ nu e trivială, atunci există $x \in F \setminus \{0\}$ astfel încât $\varphi(x) < 1$. Şirul $\{x^n\}$ converge la 0 în topologia definită de φ, deci şi în topologia definită de valuarea trivială. Cum aceasta din urmă e topologia discretă, $x^n = 0$ pentru n suficient de mare. Prin urmare, $x = 0$, o contradicţie cu faptul că $x \neq 0$. □

In cadrul exemplului (5), divizorul prim de care aparţine $\varphi_{p,c}$ este

$$\{\varphi_{p,c}^\alpha \,:\, \alpha > 0\} = \{\varphi_{p,c^\alpha} \,:\, \alpha > 0\} = \{\varphi_{p,d} \,:\, 0 < d < 1\}$$

Pe de altă parte, dacă p, $q \in \mathcal{P}$ sunt distincte, atunci $\varphi_{p,c} \not\sim \varphi_{q,d}$ pentru orice $0 < c, d < 1$, întrucât $\varphi_{p,c}(p) = c < 1$, pe când $\varphi_{q,d}(p) = 1$. Prin urmare, fiecărui element $p \in \mathcal{P}$ îi corespunde un divizor prim netrivial al lui F, pe care îl vom nota tot cu p. Similar, în exemplul (4), fiecărui ideal prim nenul $\mathfrak{p}$ al inelului de întregi algebrici $\mathcal{O}_F$, îi corespunde un divizor prim netrivial al corpului de numere algebrice F, care va fi notat tot prin $\mathfrak{p}$. În cazul acesta, pentru a vedea că divizorii primi asociaţi idealelor prime nenule distincte, $\mathfrak{p}$ şi $\mathfrak{q}$, sunt distincţi e de ajuns să observăm că există $x \in \mathfrak{p} \setminus \mathfrak{q}$. Pentru acest x avem $\varphi_{\mathfrak{p},c}(x) < 1$ şi $\varphi_{\mathfrak{q},d}(x) = 1$, pentru orice $0 < c, d < 1$. Pentru orice subcorp al lui $\mathbb{C}$ vom nota cu P_∞ divizorul prim care conţine valoarea absolută.

1.3 Topologia definită de o valuare e topologie metrică

Vom arăta în continuare că topologia definită de o valuare e o topologie metrică. Pentru aceasta, vom arăta că orice valuare e echivalentă cu o valuare φ care satisface ***inegalitatea triunghiului***:

$$\varphi(x+y) \leq \varphi(x) + \varphi(y)$$

Înainte de toate, ne va fi de folos următoarea

Propoziţie 1.3.1. *În definiţia valuării,* (iii) *poate fi înlocuită cu*

$$\varphi(x+y) \leq C \max\{\varphi(x), \varphi(y)\}$$

pentru orice x, $y \in F$.

Demonstraţie. Presupunem întâi că φ e o valuare pe F. Fie x, $y \in F$ astfel încât $\varphi(x) = \max\{\varphi(x), \varphi(y)\}$. Dacă $\varphi(x) = 0$ atunci $x = y = 0$ şi condiţia din enunţ e verificată. Dacă $\varphi(x) \neq 0$ atunci, ţinând cont că $\varphi(1 + y/x) \leq C$, avem

$$\varphi(x+y) = \varphi(x)\varphi(1+y/x) \leq C \max\{\varphi(x), \varphi(y)\}$$

Reciproc, dacă φ e o funcţie cu proprietăţile (i) şi (ii) din definiţia 1.1.1 şi verifică, în plus, condiţia din enunţ, atunci $\varphi(1) = 1$ şi

$$\varphi(1+x) \leq C \max\{\varphi(1), \varphi(x)\} = C$$

pentru orice $x \in F$ cu $\varphi(x) \leq 1$. □

Pentru o valuare φ putem considera mulţimea tuturor constantelor C care pot apărea în condiţia (iii) din definiţia 1.1.1. Această mulţime e nemărginită superior şi e mărginită inferior de 1. Într-adevăr, dacă φ verifică (iii) cu C, atunci φ verifică (iii) cu $C' > C$ şi, întrucât $\varphi(0) = 0 \leq 1$, $1 = \varphi(1+0) \leq C$. Marginea inferioară a acestei mulţimi face parte din mulţime, se notează cu $\|\varphi\|$ şi se numeşte ***norma*** lui φ. Aşadar, $1 \leq \|\varphi\| = \inf C = \min C$, unde C parcurge mulţimea constantelor ce pot apărea în (iii). Dacă $\alpha > 0$, atunci rezultă imediat că $\|\varphi^\alpha\| = \|\varphi\|^\alpha$. Prin urmare, dacă P e un divizor prim, atunci există $\varphi \in P$ astfel încât $\|\varphi\| \leq 2$. Astfel de valuări satisfac inegalitatea triunghiului aşa cum vom vedea după următoarea lemă.

Lemă 1.3.1. *Fie φ o valuare pe F astfel încât $\|\varphi\| \leq 2$. Atunci*

$$\varphi(x_1 + \cdots + x_n) \leq 2n \max\{\varphi(x_1), \ldots, \varphi(x_n)\}$$

oricare ar fi $n \geq 1$ şi $x_1, \ldots, x_n \in F$. În particular, $\varphi(n) \leq 2n$ pentru orice întreg pozitiv, n.

Demonstraţie. Conform propoziţiei 1.3.1, avem $\varphi(x_1+x_2) \leq 2 \max\{\varphi(x_1), \varphi(x_2)\}$ oricare ar fi x_1, $x_2 \in F$. Folosind inducţia, deducem că

$$\varphi(x_1 + \cdots + x_{2^r}) \leq 2^r \max\{\varphi(x_1), \ldots, \varphi(x_{2^r})\}$$

oricare ar fi $r \geq 1$ şi $x_1, \ldots, x_{2^r} \in F$.

Fie acum $n \geq 2$ si $x_1, \ldots, x_n \in F$. Considerând $r \geq 1$ astfel încât $2^r \leq n < 2^{r+1}$, avem

$$\begin{aligned} \varphi(x_1 + \cdots + x_n) &= \varphi(x_1 + \cdots + x_n + 0 + \cdots + 0) \qquad (2^{r+1}\text{termeni}) \\ &\leq 2^{r+1} \max\{\varphi(x_1), \ldots, \varphi(x_n)\} \\ &\leq 2n \max\{\varphi(x_1), \ldots, \varphi(x_n)\} \end{aligned}$$

În particular, dacă $x_1 = \cdots = x_n = 1$, obţinem $\varphi(n) \leq 2n$. □

Propoziţie 1.3.2. *Fie φ o funcţie definită pe F cu valori în mulţimea numerelor reale care verifică condiţiile* (i) *şi* (ii) *din definiţia valuării. Atunci φ verifică inegalitatea triunghiului dacă şi numai dacă φ e o valuare şi $\|\varphi\| \leq 2$.*

Demonstraţie. Necesitatea rezultă din propoziţia 1.3.1 şi observaţia că

$$\varphi(x + y) \leq \varphi(x) + \varphi(y) \leq 2 \max\{\varphi(x), \varphi(y)\}$$

pentru orice x, $y \in F$.

Pentru a demonstra suficienţa ne folosim de lema anterioară. Fie x şi y elemente ale lui F şi n un număr întreg pozitiv. Atunci

$$\begin{aligned} \varphi(x+y)^n &= \varphi\left[x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + y^n\right] \\ &\leq 2(n+1) \max_i \left\{\varphi\left[\binom{n}{i}x^{n-i}y^i\right]\right\} \\ &\leq 2(n+1) \sum_i \varphi\left[\binom{n}{i}\right] \varphi(x^{n-i})\varphi(y^i) \\ &\leq 4(n+1) \sum_i \binom{n}{i} \varphi(x)^{n-i}\varphi(y)^i \\ &= 4(n+1)[\varphi(x) + \varphi(y)]^n \end{aligned}$$

Prin urmare,

$$\varphi(x+y) \leq \sqrt[n]{4(n+1)}[\varphi(x)+\varphi(y)]$$

Lăsând pe n să tindă către infinit obţinem inegalitatea triunghiului pentru x şi y. □

Teoremă 1.3.1. *Fie φ o valuare a corpului F cu proprietatea că $\|\varphi\| \leq 2$. Atunci τ_φ e o topologie metrică, în raport cu care F e un corp topologic şi φ e uniform continuă.*

Demonstraţie. Fie $d : F \times F \to \mathbb{R}$, aplicaţia definită prin

$$d(x,y) = \varphi(x-y)$$

pentru orice x, $y \in F$. Ţinând cont că φ verifică inegalitatea triunghiului, e uşor de văzut că d e o metrică pe F. În topologia τ_d definită de d, un sistem fundamental de vecinătăţi pentru $x \in F$ e format din mulţimile

$$\{y \in F \,:\, d(x,y) < \varepsilon\} = B(x,\varepsilon),\ \varepsilon > 0$$

prin urmare, ţinând seama de propoziţia 1.1.1, $\tau_d = \tau_\varphi$. Aşadar, τ_φ e o topologie metrică.

Faptul că φ e uniform continuă rezultă din observaţia că, pentru orice x, $y \in F$, $\varphi(x) \leq \varphi(x-y)+\varphi(y)$ şi $\varphi(y) \leq \varphi(y-x)+\varphi(x)$, deci

$$|\varphi(x)-\varphi(y)| \leq \varphi(x-y)$$

Ca să arătăm că F e corp topologic în raport cu τ_φ trebuie să probăm faptul că aplicaţiile $(x,y) \to x-y$, $(x,y) \to xy$ şi $x \to x^{-1}$ sunt continue. Ţinând seama că topologia produs de pe $F \times F$ e topologia metrică dată de

$$d'\big((x_1,x_2),(y_1,y_2)\big) = \max\{\varphi(x_1-y_1),\varphi(x_2-y_2)\}$$

verificările care rămân sunt de rutină. □

In virtutea faptului că orice divizor prim conţine o valuare care verifică inegalitatea triunghiului, vom considera de acum încolo doar valuări de acest tip.

1.4 Extinderi de corpuri cu divizori primi

În cazul unei extinderi de corpuri E/F se pune problema studierii legăturii dintre divizorii primi ai lui F şi cei ai lui E. O primă observaţie care se poate face este că orice divizor prim al lui E induce, în mod natural, un divizor prim al lui F. Pentru aceasta, să considerăm Q un divizor prim al lui E. Atunci

$$P = \{\psi|_F \,:\, \psi \in Q\}$$

e un divizor prim al lui F. Într-adevăr, dacă $\psi \in Q$ atunci $\psi|_F$ e o valuare a lui F, iar divizorul prim al lui F care îl conţine pe $\psi|_F$ e $\{(\psi|_F)^\alpha \,:\, \alpha > 0\} = \{\psi^\alpha|_F \,:\, \alpha > 0\} = P$. Spunem că P este ***restricţia*** lui Q la F, iar Q e o ***extindere*** a lui P la E. Nu este exclus ca un divizor prim să admită mai multe extinderi, dupa cum nu e exclus ca el sa nu admită nici o extindere. Studiul privind existenţa şi numărul extinderilor unui divizor prim îl vom întreprinde în secţiunile 4 şi 5 ale prezentei lucrări.

Definiţie 1.4.1. *Atunci când E/F e o extindere de corpuri, iar Q e un divizor prim al lui E a cărui restricţie la F e P, spunem că (E, Q) e o **extindere** a lui (F, P). Despre divizorul prim Q mai spunem că **stă deasupra** lui P sau că îl **divide** pe P, iar acest lucru îl notăm cu $Q|P$.*

Procedeul de restricţie a unui divizor prim e un caz particular al următoarei situaţii. Fie $\mu : F \to E$ un morfism de corpuri şi Q un divizor prim al lui E. Atunci

$$P = \{\psi\mu \,:\, \psi \in Q\}$$

e un divizor prim al lui F. Într-adevăr, dacă $\psi \in Q$, atunci $\psi\mu$ e o valuare a lui F, iar divizorul prim al lui F care îl conţine pe $\psi\mu$ e $\{(\psi\mu)^\alpha \,:\, \alpha > 0\} = \{\psi^\alpha\mu \,:\, \alpha > 0\} = P$. Notând divizorul prim P cu $\mu^*(Q)$ şi mulţimile divizorilor primi ai lui F, respectiv E, cu $\mathcal{D}(F)$, respectiv $\mathcal{D}(E)$, obţinem o aplicaţie

$$\mu^* : \mathcal{D}(E) \to \mathcal{D}(F),\ Q \to \mu^*(Q)$$

Dacă $\nu : E \to L$ e un alt morfism de corpuri, atunci se verifică cu uşurinţă că $(\nu\mu)^* = \mu^*\nu^*$. Totodată, dacă $E = F$ şi $\mu = \mathrm{Id}_F$, atunci $\mathrm{Id}_F^* = \mathrm{Id}_{\mathcal{D}(F)}$. Prin urmare, dacă $\mu : F \to E$ e un izomorfism de corpuri, atunci $\mu^* : \mathcal{D}(E) \to \mathcal{D}(F)$ e o bijecţie de mulţimi şi $\left(\mu^*\right)^{-1} = \left(\mu^{-1}\right)^*$.

Definiţie 1.4.2. *In situaţia în care $\mu : F \to E$ e un morfism de corpuri, Q e un divizor prim al lui E şi $P = \mu^*(Q)$, vom spune că (E, Q, μ) e o **extindere** a lui (F, P).*

Atunci când E/F e o extindere de corpuri şi $\mu = i_{F\to E}$ e morfismul de incluziune a lui F în E, faptul că $(E, Q, i_{F\to E})$ e o extindere a lui (F, P) e echivalent cu faptul că (E, Q) e o extindere a lui (F, P).

Pentru o extindere (E, Q, μ) a lui (F, P) e uşor de văzut că $\mu : F \to E$ e o aplicaţie continuă. De fapt, dacă $\psi \in Q$, atunci $\psi\mu \in P$ şi

$$\psi\big(\mu(x) - \mu(y)\big) = \psi\mu(x - y)$$

pentru orice x, $y \in F$.

Capitolul 2

Valuări nearhimediene şi divizori primi nearhimedieni

Definiţie 2.0.3. *Fie φ o valuare a unui corp F. Spunem că φ e* ***arhimediană*** *dacă $\|\varphi\| > 1$ şi* ***nearhimediană*** *dacă $\|\varphi\| = 1$.*

Întrucât valuările echivalente cu φ sunt φ^α, $\alpha > 0$, iar $\|\varphi^\alpha\| = \|\varphi\|^\alpha$, pentru orice $\alpha > 0$, vedem că dacă φ e arhimediană/nearhimediană atunci orice valuare echivalentă cu φ e arhimediană/nearhimediană. Vom spune, prin urmare, că un divizor prim e ***arhimedian***, respectiv ***nearhimedian***, dacă conţine o valuare arhimediană, respectiv, nearhimediană.

În cadrul exemplelor din secţiunea 1, valuările de la (2) sunt arhimediene, iar cele de la (1), (3), (4) şi (5) nearhimediene.

Vom studia în aceast capitol valuările nearhimediene şi divizorii primi nearhimedieni.

2.1 Valuări nearhimediene

Începem cu următoarea caracterizare a valuărilor nearhimediene.

Propoziţie 2.1.1. *Fie φ o valuare pe F. Următoarele afirmaţii sunt echivalente:*

(i) *φ e nearhimediană.*

(ii) *$\varphi(x+y) \leq \max\{\varphi(x), \varphi(y)\}$, pentru orice $x, y \in F$.*

(iii) *$\varphi(n \cdot 1) \leq 1$, pentru orice $n \in \mathbb{Z}$.*

(iv) *Există $M > 0$ astfel încât $\varphi(n \cdot 1) \leq M$, pentru orice $n \in \mathbb{Z}$.*

Demonstraţie. (i) $\Rightarrow$ (ii) rezultă din definiţia normei.
(ii) $\Rightarrow$ (iii) e imediată din observaţia că

$$\varphi(x_1 + \cdots + x_n) \leq \max\{\varphi(x_1), \ldots, \varphi(x_n)\}$$

pentru orice $n \geq 1$ şi orice $x_1, \ldots, x_n \in F$, deci $\varphi(n \cdot 1) \leq \varphi(1) = \varphi(-1) = 1$, pentru orice $n \in \mathbb{Z}$.
(iii) $\Rightarrow$ (iv) e trivială.
(iv) $\Rightarrow$ (i) Fie x, $y \in F$ astfel încât $\varphi(x) \leq \varphi(y)$. Ţinând cont de lema 1.3.1, avem, pentru orice $n \geq 1$,

$$\begin{aligned}
\varphi(x+y)^n &= \varphi[(x+y)^n] \\
&= \varphi\left[x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + y^n\right] \\
&\leq 2(n+1)\max\left\{\varphi\left[\binom{n}{i}x^{n-i}y^i\right]\right\} \\
&\leq 2(n+1)M\max_i\left\{\varphi(x)^{n-i}\varphi(y)^i\right\} \\
&\leq 2(n+1)M\varphi(y)^n
\end{aligned}$$

Aşadar, $\varphi(x+y) \leq \sqrt[n]{2(n+1)M}\varphi(y)$, oricare ar fi $n \geq 1$. Făcând $n \to \infty$, obţinem $\varphi(x+y) \leq \varphi(y) = \max\{\varphi(x), \varphi(y)\}$. □

Corolar 2.1.1. *Fie F un subcorp al lui E şi φ o valuare pe E. Dacă φ e arhimediană, respectiv nearhimediană, pe F atunci φ e arhimediană, respectiv nearhimediană, pe E. În particular, un corp de caracteristică $p > 0$ nu poate avea decât valuări nearhimediene.*

Următorul rezultat va fi invocat destul de des în demonstraţii.

Propoziţie 2.1.2. *Fie φ o valuare nearhimediană pe F. Atunci*

$$\varphi(x) \neq \varphi(y) \Rightarrow \varphi(x+y) = \max\{\varphi(x), \varphi(y)\}$$

Demonstraţie. Să presupunem că $\varphi(x) < \varphi(y)$. Întrucât $\varphi(x+y) \leq \varphi(y)$, e de ajuns să arătăm inegalitatea opusă. Avem

$$\varphi(y) = \varphi(x+y-x) \leq \max\{\varphi(x+y), \varphi(x)\} = \varphi(x+y)$$

□

Corolar 2.1.2. *Fie φ o valuare nearhimediană pe F şi $x_1, \ldots, x_n \in F$.*

(i) *Dacă* $\varphi(x_i) > \varphi(x_j)$ *pentru orice* $j \neq i$, *atunci*

$$\varphi(x_1 + \cdots + x_n) = \varphi(x_i)$$

(ii) *Dacă* $x_1 + \cdots + x_n = 0$, *atunci există* $i \neq j$ *astfel încât*

$$\max\{\varphi(x_1), \ldots, \varphi(x_n)\} = \varphi(x_i) = \varphi(x_j)$$

Demonstraţie. (i) Rezultă din propoziţia 2.1.2, ţinând cont că

$$\varphi(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n) \leq \max_{j \neq i}\{\varphi(x_j)\} < \varphi(x_i)$$

(ii) Dacă ar exista un singur indice i pentru care $\max\{\varphi(x_1), \ldots, \varphi(x_n)\} = \varphi(x_i)$, atunci, ţinând cont de (i), am avea

$$0 = \varphi(x_1 + \cdots x_n) = \varphi(x_i)$$

Dar atunci $\varphi(x_j) < \varphi(x_i) = 0$ pentru orice $j \neq i$, o contradicţie. □

2.2 Divizori primi nearhimedieni

Trecem acum la studiul divizorilor primi nearhimedieni. În acest studiu, un rol important îl joacă bila închisă de centru 0 şi rază 1 din topologia asociată unui astfel de divizor. Propoziţia următoare arată că, în raport cu operaţiile induse de pe F, această mulţime e un inel local.

Propoziţie 2.2.1. *Fie* P *un divizor prim nearhimedian al lui* F. *Atunci mulţimile*

$$\mathcal{O}_P = \{x \in F : \varphi(x) \leq 1\}$$
$$\mathcal{P}_P = \{x \in F : \varphi(x) < 1\}$$
$$\mathcal{U}_P = \{x \in F : \varphi(x) = 1\}$$

nu depind de valuare $\varphi \in P$ *aleasă. Mai mult, în raport cu operaţiile induse de pe* F, $\mathcal{O}_P$ *e un inel local având corpul de fracţii* F, *idealul maximal* $\mathcal{P}_P$ *şi grupul unităţilor* $\mathcal{U}_P$

Demonstraţie. E clar că $\mathcal{O}_P$, $\mathcal{P}_P$ şi $\mathcal{U}_P$ nu depind decât de divizorul prim P. La fel de clar e că $\mathcal{O}_P$ e un subinel unitar al lui F. Deoarece, pentru orice $x \in F$, avem $x \in \mathcal{O}_P$ sau $x^{-1} \in \mathcal{O}_P$, corpul de fracţii al lui $\mathcal{O}_P$ e F. Grupul unităţilor lui $\mathcal{O}_P$ este

$$\{x \in F : x, x^{-1} \in \mathcal{O}_P\} = \{x \in F : \varphi(x) = 1\} = \mathcal{U}_P$$

E uşor de văzut acum că

$$\mathcal{O}_P \setminus \mathcal{U}_P = \{x \in F \,:\, \varphi(x) < 1\} = \mathcal{P}_P$$

e ideal al lui $\mathcal{O}_P$. Prin urmare, $\mathcal{O}_P$ e inel local, iar $\mathcal{P}_P$ e idealul său maximal. □

Definiţie 2.2.1. *Fie F un corp şi P un divizor prim al lui F. $\mathcal{O}_P$ se numeşte* ***inelul de valuare al lui F în P*** *sau* ***inelul de întregi al lui F în P****, $\mathcal{P}_P$ se numeşte* ***idealul prim în P****, iar $\mathcal{U}_P$* ***grupul unităţilor în P****. Corpul $\mathcal{F}_P = \mathcal{O}_P/\mathcal{P}_P$ se numeşte* ***corpul rezidual al lui F în P****.*

De exemplu, dacă P e trivial, atunci $\mathcal{O}_P = F$, $\mathcal{P}_P = \{0\}$ şi $\mathcal{U}_P = F^*$. Dacă R e un inel factorial, F e corpul său de fracţii şi p e divizorul prim asociat unui element prim p atunci

$$\begin{aligned}
\mathcal{O}_p &= \left\{\frac{a}{b} \,:\, a, b \in R,\, p \nmid b\right\} \\
\mathcal{P}_p &= \left\{\frac{a}{b} \,:\, a, b \in R,\, p \mid a, p \nmid b\right\} \\
\mathcal{U}_p &= \left\{\frac{a}{b} \,:\, b \in R,\, p \nmid ab\right\}
\end{aligned}$$

Aşadar, $\mathcal{O}_p = R_{(p)}$, localizatul inelului R în idealul prim (p). Prin urmare, corpul rezidual al lui F în p este $R_{(p)}/pR_{(p)} \simeq R/(p)$. În particular, corpul rezidual al lui $\mathbb{Q}$ în p e corpul cu p elemente.

Dacă F e un corp de numere algebrice şi $\mathfrak{p}$ divizorul prim asociat idealului prim nenul $\mathfrak{p}$ al lui $\mathcal{O}_F$, atunci

$$\mathcal{O}_\mathfrak{p} = (\mathcal{O}_F)_\mathfrak{p},\ \ \mathcal{P}_\mathfrak{p} = \mathfrak{p}(\mathcal{O}_F)_\mathfrak{p},\ \ \mathcal{F}_\mathfrak{p} \simeq \mathcal{O}_F/\mathfrak{p}$$

Să arătăm că, într-adevăr, $\mathcal{O}_\mathfrak{p}$ e localizatul inelului de întregi algebrici al lui F în idealul prim $\mathfrak{p}$, $(\mathcal{O}_F)_\mathfrak{p}$. Ţinând cont de descrierea elementelor din $\mathcal{O}_\mathfrak{p}$, respectiv $(\mathcal{O}_F)_\mathfrak{p}$, ceea ce vrem să arătăm e următoarea egalitate de mulţimi

$$\{x \in F \,:\, \mathrm{ord}_\mathfrak{p}(x) \geq 0\} = \left\{\frac{a}{b} \in F \,:\, a, b \in \mathcal{O}_F, b \notin \mathfrak{p}\right\}$$

Fie $a/b \in (\mathcal{O}_F)_\mathfrak{p}$. Deoarece $a,\ b \in \mathcal{O}_F$ si $b \notin \mathfrak{p}$, avem $\mathrm{ord}_\mathfrak{p}(a\mathcal{O}) \geq 0$ şi $\mathrm{ord}_\mathfrak{p}(b\mathcal{O}) = 0$, deci

$$\mathrm{ord}_\mathfrak{p}\big((a/b)\mathcal{O}\big) = \mathrm{ord}_\mathfrak{p}(a\mathcal{O}) - \mathrm{ord}_\mathfrak{p}(b\mathcal{O}) = \mathrm{ord}_\mathfrak{p}(a\mathcal{O}) \geq 0$$

Prin urmare, $(\mathcal{O}_F)_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}$. Fie acum $x \in \mathcal{O}_{\mathfrak{p}}$. Întrucât F e corpul de fracţii al inelului său de întregi algebrici, există $a,\ b \in \mathcal{O}_F,\ b \neq 0$, astfel încât $x = a/b$. Fie $\mathrm{ord}_{\mathfrak{p}}(a\mathcal{O}_F) = m \geq n = \mathrm{ord}_{\mathfrak{p}}(b\mathcal{O}_F)$ şi $\pi \in \mathfrak{p}^{-n} \setminus \mathfrak{p}^{-n+1}$. Atunci $\pi a,\ \pi b \in \mathcal{O}_F$ şi $\pi b \notin \mathfrak{p}$. Într-adevăr, considerând idealele întregi $\mathfrak{a}$, $\mathfrak{b}$ şi $\mathfrak{c}$ astfel încât

$$a\mathcal{O}_F = \mathfrak{p}^m\mathfrak{a},\ b\mathcal{O}_F = \mathfrak{p}^n\mathfrak{b},\ \pi\mathcal{O}_F = \mathfrak{p}^{-n}\mathfrak{c}$$

şi $\mathfrak{p} \nmid \mathfrak{abc}$, avem $(\pi b)\mathcal{O}_F = \mathfrak{bc}$ şi $(\pi a)\mathcal{O}_F = \mathfrak{p}^{m-n}\mathfrak{ac}$, de unde afirmaţia noastră. Aşadar, $x = \frac{\pi a}{\pi b} \in (\mathcal{O}_F)_{\mathfrak{p}}$ şi egalitatea $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_F)_{\mathfrak{p}}$ e demonstrată. Deoarece idealul maximal al lui $(\mathcal{O}_F)_{\mathfrak{p}}$ este $\mathfrak{p}(\mathcal{O}_F)_{\mathfrak{p}}$, afirmaţiile referitoare la idealul prim în $\mathfrak{p}$ şi corpul rezidual în $\mathfrak{p}$ rezultă imediat.

Pe baza acestor observaţii putem arăta că nu există alţi divizori primi nearhimedieni (netriviali) ai unui corp de numere algebrice în afară de cei asociaţi idealelor prime nenule din inelul de întregi algebrici. Vom începe cu cel mai simplu exemplu de corp de numere algebrice, anume $\mathbb{Q}$, după care vom trata cazul general.

Fie, aşadar, P un divizor prim nearhimedian (netrivial) al lui $\mathbb{Q}$ şi $\varphi \in P$. Întrucât $\varphi(n) \leq 1$, pentru orice număr întreg n, avem $\mathbb{Z} \subseteq \mathcal{O}_P$. Intersecţia lui $\mathbb{Z}$ cu idealul prim în P, $\mathcal{P}_P$, e un ideal prim al lui $\mathbb{Z}$, $p\mathbb{Z}$. Acest ideal e nenul, deoarece, în caz contrar, φ acţionează trivial pe mulţimea numerelor întregi nenule, deci şi pe mulţimea numerelor raţionale nenule. Ţinând cont că $\mathbb{Z} \setminus p\mathbb{Z} \subseteq \mathcal{U}_P$, avem

$$\mathbb{Z}_{(p)} \subseteq \mathcal{O}_P$$

Cum $\mathbb{Z}_{(p)}$ e inelul de valuare al lui $\mathbb{Q}$ în p, deducem din teorema 1.2.1 că $P = p$.

Raţionamentul folosit în cazul lui $\mathbb{Q}$ funcţionează pentru orice corp de numere algebrice, F. Singura observaţie care trebuie facută e că, dacă P e un divizor prim nearhimedian al lui F, atunci $\mathcal{O}_F \subseteq \mathcal{O}_P$. Într-adevăr, dacă α e un întreg algebric, atunci există întregii raţionali $a_0, \ldots, a_{n-1}$ astfel încât $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$. Considerând $\varphi \in P$, avem

$$\varphi(\alpha)^n \leq \max_i \{\varphi(a_i\alpha^i)\} \leq \max_i \{\varphi(\alpha)^i\}$$

de unde obţinem $\varphi(\alpha) \leq 1$, i.e. $\alpha \in \mathcal{O}_P$. Aşadar, dacă P e un divizor prim nearhimedian al lui F, atunci $\mathcal{O}_F \subseteq \mathcal{O}_P$. Fie $\mathfrak{p} = \mathcal{P}_P \cap \mathcal{O}_F$. Atunci $\mathfrak{p}$ e un ideal prim nenul al lui $\mathcal{O}_F$ şi $\mathcal{O}_F \setminus \mathfrak{p} \subseteq \mathcal{U}_P$. Prin urmare, $\mathcal{O}_{\mathfrak{p}} = (\mathcal{O}_F)_{\mathfrak{p}} \subseteq \mathcal{O}_P$, de unde rezultă că $P = \mathfrak{p}$.

Rezumând, am obţinut următoarea

Propoziţie 2.2.2. *Divizorii primi nearhimedieni (netriviali) ai unui corp de numere algebrice sunt în corespondenţă bijectivă cu idealele prime nenule ale inelului său de întregi algebrici.*

2.3 Valuări exponenţiale

Prezentăm în continuare o altă perspectivă asupra divizorilor primi nearhimedieni. Acest mod porneşte de la următoarea observaţie. Dacă φ e o valuare nearhimedianã a unui corp F, atunci funcţia

$$v : F \to \mathbb{R} \cup \{\infty\},\ v(x) = \begin{cases} -\log \varphi(x) & \text{daca} \quad x \neq 0 \\ \infty & \text{daca} \quad x = 0 \end{cases}$$

are următoarele proprietăţi:

(i) $v(x) = \infty \Leftrightarrow x = 0$

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$

pentru orice $x,\ y \in F$. Reciproc, dacă $v : F \to \mathbb{R} \cup \{\infty\}$ e o funcţie cu proprietăţile (i), (ii) şi (iii), atunci funcţia

$$\varphi : F \to \mathbb{R},\ \varphi(x) = \begin{cases} e^{-v(x)} & \text{dacă} \quad x \neq 0 \\ 0 & \text{dacă} \quad x = 0 \end{cases}$$

e o valuare nearhimedianã pe F. O verificare de rutină arată că asocierile $\varphi \to v$ şi $v \to \varphi$ sunt inverse una celeilalte. Numim funcţiile $v : F \to \mathbb{R} \cup \{\infty\}$ care satisfac condiţiile (i), (ii) şi (iii), ***valuări exponentiale*** ale lui F. Aşadar, valuările nearhimediene ale lui F sunt în corespondenţa bijectivă cu valuările exponenţiale ale lui F. Spunem că două valuări exponenţiale, v şi v', sunt ***echivalente*** şi scriem $v \sim v'$, dacă valuările nearhimediene corespunzătoare sunt echivalente, i.e. $e^{-v} = \varphi \sim \varphi' = e^{-v'}$. Aşadar, $v \sim v'$ dacă şi numai dacă $v' = \alpha v$, pentru un $\alpha > 0$. Clasa de echivalenţă a unei valuări exponenţiale v o vom identifica, în urma observaţiilor anterioare, cu clasa de echivalenţă a valuării nearhimediene e^{-v}. Prin urmare, dacă P e un divizor prim şi v e o valuare exponenţială cu proprietatea că $e^{-v} \in P$, atunci $P = \{\alpha v \,|\, \alpha > 0\}$. Inelul de întregi în P, idealul prim în P şi grupul unităţilor în P se exprimă în funcţie de $v \in P$ prin

$$\begin{aligned} \mathcal{O}_P &= \{x \in F \,:\, v(x) \geq 0\} \\ \mathcal{P}_P &= \{x \in F \,:\, v(x) > 0\} \\ \mathcal{U}_P &= \{x \in F \,:\, v(x) = 0\} \end{aligned}$$

Orice valuare exponenţială v a lui F determină un morfism de grupuri de la grupul multiplicativ al lui F în grupul aditiv al numerelor reale. Imaginea

lui F^* prin v se numeşte ***grupul de valuare*** al lui v şi se notează cu $\mathrm{G}(v)$. Atunci când $\mathrm{G}(v)$ e subgrup discret al lui $(\mathbb{R}, +)$ spunem că v e valuare ***discretă***. Întrucât grupurile de valuare a două valuări echivalente sunt izomorfe, definiţia se extinde pentru a cuprinde şi divizorii primi. Aşadar, un divizor prim e ***discret*** atunci când conţine o valuare exponenţială discretă.

E bine ştiut faptul că subgrupurile discrete ale lui $(\mathbb{R}, +)$ sunt cele de forma $a\mathbb{Z}$, cu $a \in \mathbb{R}$. Dacă $\mathrm{G}(v) = \{0\}$ atunci P e divizorul prim trivial. Dacă, pe de altă parte, $\mathrm{G}(v) = a\mathbb{Z}$, unde $a \neq 0$, atunci $\mathrm{G}(a^{-1}v) = \mathbb{Z}$. Aşadar, dacă P e un divizor prim discret netrivial, atunci P conţine o unică valuare exponenţială al cărei grup de valuare e $\mathbb{Z}$. Această valuare se notează cu v_P şi se numeşte ***valuarea exponenţială normalizată*** a lui P.

Propoziţie 2.3.1. *Fie P un divizor prim nearhimedian al lui F. Atunci P e discret dacă şi numai dacă $\mathcal{P}_P$ e ideal prim.*

Demonstraţie. Dacă P e discret atunci $v_P(F^*) = \mathbb{Z}$, deci există $\pi \in F^*$ astfel încât $v_P(\pi) = 1$. Avem

$$\begin{aligned}\mathcal{P}_P &= \{x \in F \,:\, v_P(x) \geq 1 = v_P(\pi)\} \\ &= \{x \in F \,:\, v_P(x\pi^{-1}) \geq 0\} \\ &= \{x \in F \,:\, x\pi^{-1} \in \mathcal{O}_P\} \\ &= \pi\mathcal{O}_P\end{aligned}$$

deci $\mathcal{P}_P$ e ideal principal.

Reciproc, dacă $\mathcal{P}_P = \pi\mathcal{O}_P$, atunci orice element nenul al lui F are o scriere unică de forma $u\pi^r$, cu $u \in \mathcal{U}_P$ şi $r \in \mathbb{Z}$. Alegând o valuare exponenţială $v \in P$, găsim că $v(F^*) = v(\pi)\mathbb{Z}$, deci P e discret. □

Dacă P e un divizor prim discret (netrivial) al lui F atunci generatorii idealului prim în P se numesc ***elemente prime*** ale lui F în raport cu P. Dacă π e un astfel de element atunci $F^* = \{u\pi^r \,:\, u \in \mathcal{U}_P, r \in \mathbb{Z}\}$ şi $\mathcal{O}_P = \{u\pi^r \,:\, u \in \mathcal{U}_P, r \geq 0\}$. De aici rezultă imediat că singurele ideale netriviale ale lui $\mathcal{O}_P$ sunt cele de forma

$$\mathcal{P}_P^r = \pi^r\mathcal{O}_P = \{x \in F \,:\, v_P(x) \geq r\},\ r \geq 1$$

Prin urmare, $\mathcal{O}_P$ e un inel principal cu $\mathcal{P}_P$ singurul său ideal prim nenul.

Am întâlnit deja exemple de valuări discrete şi de divizori primi discreţi. În exemplul (5) din secţiunea 1 funcţia ordinal, $\mathrm{ord}_p : F \to \mathbb{Z}$, care asociază unui element $x \in F$, puterea la care apare p în scrierea lui x ca produs de puteri de elemente prime, e o valuare exponenţială discretă, întrucât

$\varphi_{p,1/e}(x) = e^{-\mathrm{ord}_p(x)}$ e valuare nearhimediană şi $\mathrm{G}(\mathrm{ord}_p) = \mathbb{Z}$. Prin urmare, p e divizor prim discret al lui F, având ca valuare exponenţială normalizată chiar pe ord_p, iar ca element prim pe p. Din considerente similare, dacă F e corp de numere algebrice, atunci funcţia $v_{\mathfrak{p}} : F \to \mathbb{Z}$, $v_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(x\mathcal{O})$, oricare ar fi $x \in F$, e valuarea exponenţială normalizată a divizorului prim discret $\mathfrak{p}$ al lui F.

2.4 Indicele de ramificare şi gradul rezidual

Fie (E, Q) o extindere a lui (F, P). E clar că P e arhimedian (nearhimedian) dacă şi numai dacă Q e arhimedian (nearhimedian). În cazul nearhimedian avem

$$\mathcal{O}_P = \mathcal{O}_Q \cap F \text{ si } \mathcal{P}_P = \mathcal{P}_Q \cap F$$

Într-adevăr, dacă $\psi \in Q$ şi $\varphi = \psi_F$, atunci

$$\mathcal{O}_Q \cap F = \{x \in F \,:\, \psi(x) \leq 1\} = \{x \in F \,:\, \varphi(x) \leq 1\} = \mathcal{O}_P$$

şi, similar $\mathcal{P}_P = \mathcal{P}_Q \cap F$. Datorită incluziunilor $\mathcal{O}_P \subseteq \mathcal{O}_Q$ şi $\mathcal{P}_P \subseteq \mathcal{P}_Q$, corpul rezidual al lui F în P se scufundă în corpul rezidual al lui E în Q prin intermediul aplicaţiei

$$\mathcal{F}_P = \mathcal{O}_P/\mathcal{P}_P \ni a + \mathcal{P}_P \to a + \mathcal{P}_Q \in \mathcal{O}_Q/\mathcal{P}_Q = \mathcal{E}_Q$$

Privind corpul $\mathcal{F}_P$ ca subcorp al lui $\mathcal{E}_Q$, putem vorbi de gradul extinderii $\mathcal{E}_Q/\mathcal{F}_P$.

Definiţie 2.4.1. ***Gradul lui*** Q ***peste*** P *sau* ***gradul rezidual al lui*** E ***peste*** F ***în*** Q *este*

$$f(Q/P) = [\mathcal{E}_Q : \mathcal{F}_P]$$

Fie acum $w \in Q$ o valuare exponenţială a lui E şi $v = w|_F \in P$. Atunci $w(F^*) = v(F^*)$ e subgrup al lui $w(E^*)$ şi, în plus, $[w(E^*) : w(F^*)] = [(\alpha w)(E^*) : (\alpha w)(F^*)]$, pentru orice $\alpha > 0$. Aşadar, indicele lui $w(F^*)$ în $w(E^*)$ nu depinde decât de divizorul prim Q.

Definiţie 2.4.2. ***Indicele de ramificare al lui*** Q ***peste*** P *este*

$$e(Q/P) = [w(E^*) : w(F^*)]$$

Gradele reziduale şi indicii de ramificare se bucură de următoarea proprietate:

Propoziţie 2.4.1. *Fie P un divizor prim nearhimedian al lui F, (E, Q) o extindere a lui (F, P) şi (K, R) o extindere a lui (E, Q). Atunci*

$$e(R/P) = e(R/Q)\, e(Q/P)$$

$$f(R/P) = f(R/Q)\, f(Q/P)$$

Demonstraţie. Rezultă uşor din faptul că indicii grupurilor şi gradele extinderilor de corpuri sunt multiplicativi. □

Atunci când Q e discret, indicele de ramificare capătă interpretarea clasică. Mai precis, în cazul discret, $\mathcal{O}_Q$ e inel Dedekind cu un singur ideal prim nenul, $\mathcal{P}_Q$. Aceeaşi afirmaţie e valabilă şi pentru $\mathcal{O}_P$, căci, la rândul său, P e discret. Singurul ideal prim nenul al lui $\mathcal{O}_P$ e $\mathcal{P}_P$. Deoarece $\mathcal{P}_P \subseteq \mathcal{P}_Q$, există $e \geq 1$ astfel încât $\mathcal{P}_P\mathcal{O}_Q = \mathcal{P}_Q^e$. Pretindem că $e = e(Q/P)$. Fie, pentru aceasta, π_Q un element prim pentru Q şi π_P un element prim pentru P. Atunci $w(E^*) = w(\pi_Q)\mathbb{Z}$ si $w(F^*) = w(\pi_P)\mathbb{Z}$. Deoarece $[w(\pi_Q)\mathbb{Z} : w(\pi_P)\mathbb{Z}] = e(Q/P)$, avem $w(\pi_P) = e(Q/P)w(\pi_Q)$, deci $w\big(\pi_Q^{e(Q/P)}\big) = w(\pi_P)$. Atunci

$$\mathcal{P}_P\mathcal{O}_Q = (\pi_P\mathcal{O}_P)\mathcal{O}_Q = \pi_P\mathcal{O}_Q = \pi_Q^{e(Q/P)}\mathcal{O}_Q = \mathcal{P}_Q^{e(Q/P)}$$

de unde rezultă afirmaţia noastră.

Legătura dintre indicii de ramificare clasici si cei definiţi aici e, însă, ceva mai strânsă. Următoarea propoziţie e revelatoare.

Propoziţie 2.4.2. *Fie E/F o extindere de corpuri de numere algebrice. Dacă $\mathfrak{p}$ e un ideal prim nenul al lui $\mathcal{O}_F$ şi*

$$\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

e descompunerea în produs de ideale prime nenule distincte a lui $\mathfrak{p}\mathcal{O}_E$, atunci divizorii primi ai lui E care stau deasupra lui $\mathfrak{p}$ sunt $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. Mai mult,

$$e(\mathfrak{P}_i/\mathfrak{p}) = e_i \text{ si } f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}_E/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}]$$

pentru orice $i \in \{1, \ldots, r\}$

Demonstraţie. Fie P un divizor prim al lui E care stă deasupra lui $\mathfrak{p}$. Deoarece P e nearhimedian, există, conform propoziţiei 2.2.2, un ideal prim nenul $\mathfrak{P}$ al lui $\mathcal{O}_E$ astfel încât $P = \mathfrak{P}$. Avem atunci

$$\mathfrak{p} = \mathcal{O}_F \cap \mathcal{P}_\mathfrak{p} = \mathcal{O}_F \cap (F \cap \mathcal{P}_\mathfrak{P}) = \mathcal{O}_F \cap \mathcal{P}_\mathfrak{P} = \mathcal{O}_F \cap (\mathcal{O}_E \cap \mathcal{P}_\mathfrak{P}) = \mathcal{O}_F \cap \mathfrak{P}$$

ceea ce arată că idealul prim $\mathfrak{P}$ divide $\mathfrak{p}$. Pe de altă parte, dacă $x \in F$, atunci, din $x\mathcal{O}_F = \mathfrak{p}^{v_\mathfrak{p}(x)} \prod_{\mathfrak{q}\neq\mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(x)}$, deducem că

$$\begin{aligned} x\mathcal{O}_E &= (\mathfrak{p}\mathcal{O}_E)^{v_\mathfrak{p}(x)} \prod_{\mathfrak{q}\neq\mathfrak{p}} (\mathfrak{q}\mathcal{O}_E)^{v_\mathfrak{q}(x)} \\ &= \prod_{i=1}^{r} \mathfrak{P}_i^{e_i v_\mathfrak{p}(x)} \prod_{\mathfrak{P}\neq\mathfrak{P}_1,\ldots,\mathfrak{P}_r} \mathfrak{P}^{v_\mathfrak{P}(x)} \end{aligned}$$

Prin urmare, $v_{\mathfrak{P}_i}(x) = e_i v_\mathfrak{p}(x)$, pentru orice $x \in F$ şi orice $i \in \{1,\ldots,r\}$. Rezultă că divizorii primi $\mathfrak{P}_i$ stau deasupra lui $\mathfrak{p}$ şi, în plus, $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$, pentru orice $i = 1,\ldots,r$. Afirmaţia referitoare la gradele reziduale e o consecinţă imediată a faptului că $\mathcal{E}_{\mathfrak{P}_i} \simeq \mathcal{O}_E/\mathfrak{P}_i$ si $\mathcal{F}_\mathfrak{p} \simeq \mathcal{O}_F/\mathfrak{p}$. □

Revenind la cazul general, următoarea propoziţie arată că, în cazul unei extinderi finite, indicele de ramificare şi gradul rezidual sunt amândouă finite. Mai precis, avem

Propoziţie 2.4.3. *Fie (E,Q) o extindere a lui (F,P) cu P nearhimedian. Fie $\omega_1,\ldots,\omega_r \in \mathcal{O}_Q$ astfel încât $\overline{\omega_1},\ldots,\overline{\omega_r}$ sunt liniar independente peste $\mathcal{F}$ şi fie $\pi_0,\ldots,\pi_s \in E^*$ astfel încât, dacă $v \in Q$, clasele determinate de $v(\pi_0),\ldots,v(\pi_s)$ în $v(E^*)/v(F^*)$ sunt distincte. Atunci*

$$\{\omega_i\pi_j \mid i = 1,\ldots,r,\ j = 0,\ldots,s\}$$

e un sistem liniar independent peste F. În particular,

$$e(Q/P)\, f(Q/P) \leq [E:F]$$

Demonstraţie. Fie $a_{ij} \in F$ astfel încât $\sum_{i,j} a_{ij}\omega_i\pi_j = 0$. Notăm cu $d_j = \sum_{i=1}^{r} a_{ij}\omega_i$ şi observăm că $v(d_j) = \min\{v(a_{1j}),\ldots,v(a_{rj})\}$. Într-adevăr, fie $v(a_{kj}) = \min\{v(a_{1j}),\ldots,v(a_{rj})\}$. Dacă $a_{kj} = 0$, atunci nu avem nimic de demonstrat. Dacă $a_{kj} \neq 0$, atunci, împărţind pe d_j la a_{kj}, obţinem că $a_{kj}^{-1}d_j$ e o combinaţie liniară de $\omega_1,\ldots,\omega_r$ cu coeficienţi în inelul $\mathcal{O}_P$. Coeficientul lui ω_r fiind 1 şi $\overline{\omega_1},\ldots,\overline{\omega_r}$ fiind liniar independente peste $\mathcal{F}$, $a_{kj}^{-1}d_j$ nu poate fi decât un element inversabil din $\mathcal{O}_Q$. Prin urmare, $v(d_j) = v(a_{kj}) = \min\{v(a_{1j}),\ldots,v(a_{rj})\}$.

Dacă, prin absurd, există coeficienţi a_{ij} nenuli, atunci cel puţin doi termeni din suma $\sum_{j=0}^{s} d_j\pi_j$ sunt nenuli. Deoarece $\sum_{j=0}^{s} d_j\pi_j = 0$, există $j \neq k$ astfel încât $v(d_j\pi_j) = v(d_k\pi_k)$. Cum $v(\pi_j) - v(\pi_k) = v(d_k) - v(d_j) \in v(F^*)$, am obţinut o contradicţie. □

Capitolul 3

Completatul unui corp cu un divizor prim

Fie F un corp şi P un divizor prim al lui F. Un şir de elemente din F, $\{a_n\}$, se numeşte ***şir Cauchy*** dacă $a_m - a_n \to 0$, când $m, n \to \infty$, în topologia definită de P. Mai precis, $\{a_n\}$ e şir Cauchy dacă, alegând $\varphi \in P$, găsim pentru orice $\varepsilon > 0$ un număr întreg pozitiv N astfel încât $\varphi(a_m - a_n) < \varepsilon$ îndată ce $m,\ n \geq N$. Orice şir convergent e un şir Cauchy, însă nu întotdeauna un şir Cauchy e convergent. Spunem că F e ***complet*** în raport cu P dacă orice şir Cauchy de elemente din F e un şir convergent.

Un exemplu de corp care nu e complet e, dupa cum se ştie, $(\mathbb{Q}, P_\infty)$. Mulţimea numerelor raţionale poate fi, însă, "completată" cu o mulţime de elemente astfel încât, noua mulţime să aibă o structură de corp valuat, iar în acest corp şirurile Cauchy să fie convergente. Aceasta e una din metodele de construcţie a mulţimii numerelor reale, iar ideea din spatele ei va fi folosită în cele ce urmează pentru a "completa" orice corp valuat.

3.1 Existenţa şi unicitatea completatului

Definiţie 3.1.1. *Fie P un divizor prim al corpului F. Un **completat** al lui F în raport cu P este o extindere $(\widetilde{F}, \widetilde{P}, \mu)$ a lui (F, P) cu următoarele proprietăţi:*

(i) *$\widetilde{F}$ e complet în raport cu $\widetilde{P}$*

(ii) *$\mu(F)$ e dens în $\widetilde{F}$*

Aşadar, dacă $i : \mathbb{Q} \to \mathbb{R}$ e morfismul de incluziune, atunci $(\mathbb{R}, P_\infty, i)$ e un completat al lui $(\mathbb{Q}, P_\infty)$. Orice corp e complet în raport cu divizorul prim

trivial, prin urmare, în cele ce vor urma, vom considera doar divizori primi netriviali.

Următoarea teoremă ne asigură de existenţa completatului unui corp cu un divizor prim.

Teoremă 3.1.1. *Dacă F e un corp şi P e un divizor prim al lui F atunci există un completat al lui F în raport cu P.*

Demonstraţie. Fie $\varphi \in P$ astfel încât $\|\varphi\| \leq 2$. Notăm cu $\mathcal{R}$ mulţimea şirurilor Cauchy din F şi cu $\mathcal{I}$ mulţimea şirurilor din F convergente la zero. Se verifică uşor că, în raport cu adunarea şi înmulţirea punctuală, $\mathcal{R}$ e un inel comutativ şi unitar, având ca element unitate şirul constant $(1, 1, \ldots, 1, \ldots)$.

În inelul $\mathcal{R}$, $\mathcal{I}$ e un ideal maximal. Într-adevăr, ţinând cont că şirurile Cauchy sunt mărginite, singurul lucru netrivial de demonstrat e că $\mathcal{I}$ e maximal. Fie, pentru aceasta, $\{a_n\}$ un şir Cauchy care nu converge la zero şi să arătăm că există $\delta > 0$ şi N un număr întreg pozitiv astfel încât $\varphi(a_n) > \delta$ pentru orice $n \geq N$. Presupunem, prin absurd, că, oricare ar fi $\delta > 0$ şi oricare ar fi $N \geq 1$, există $n \geq N$ astfel încât $\varphi(a_n) \leq \delta$. Fie $\varepsilon > 0$ arbitrar. Cum $\{a_n\}$ e şir Cauchy, există $N \geq 1$ astfel încât $\varphi(a_n - a_m) < \varepsilon/2$, pentru orice $n, m \geq N$. Ţinând cont de ipoteza noastră, există $n \geq N$ astfel încât $\varphi(a_n) \leq \varepsilon/2$. Pentru orice $m \geq N$ avem atunci

$$\varphi(a_m) \leq \varphi(a_m - a_n) + \varphi(a_n) < \varepsilon$$

fapt ce arată că $a_n \to 0$, o contradicţie. Aşadar, există $\delta > 0$ şi $N \geq 1$ astfel încât $\varphi(a_n) > \delta$ pentru orice $n \geq N$. Fie $\{b_n\}$ şirul definit prin

$$b_n = \begin{cases} 1 & \text{daca} \quad n < N \\ \frac{1}{a_n} & \text{daca} \quad n \geq N \end{cases}$$

Întrucât, pentru n, $m \geq N$,

$$\varphi(b_m - b_n) = \frac{\varphi(a_n - a_m)}{\varphi(a_m)\varphi(a_n)} < \frac{1}{\delta^2}\,\varphi(a_n - a_m)$$

$\{b_n\}$ e un şir Cauchy. Cum $\{a_n\}\{b_n\} \equiv \{1\} \pmod{\mathcal{I}}$, rezultă că $\mathcal{I}$ e, într-adevăr, un ideal maximal al lui $\mathcal{R}$.

Fie corpul $\widetilde{F} = \mathcal{R}/\mathcal{I}$. Funcţia $\widetilde{\varphi} : \widetilde{F} \to \mathbb{R}$ definită prin $\widetilde{\varphi}(\{a_n\} + \mathcal{I}) = \lim\limits_{n\to\infty} \varphi(a_n)$, oricare ar fi $\{a_n\} \in \mathcal{R}$, e bine definită şi reprezintă o valuare pe $\widetilde{F}$. Într-adevăr, dacă $\{a_n\}$ e un şir Cauchy din F, atunci $\{\varphi(a_n)\}$ e un şir Cauchy în $\mathbb{R}$, datorită relaţiei

$$|\varphi(a_m) - \varphi(a_n)| \leq \varphi(a_m - a_n)$$

Cum $\mathbb{R}$ e complet, există şi e unică limita şirului $\{\varphi(a_n)\}$. Dacă $\{b_n\}$ e un alt şir Cauchy cu proprietatea că $\{a_n\} \equiv \{b_n\} \pmod{\mathcal{I}}$, atunci $\{a_n - b_n\} \in \mathcal{I}$, deci $\varphi(a_n - b_n) \to 0$. Cum şirurile $\{\varphi(a_n)\}$ şi $\{\varphi(b_n)\}$ au limită şi $|\varphi(a_n) - \varphi(b_n)| \leq \varphi(a_n - b_n)$, rezultă că $\lim\limits_{n\to\infty} \varphi(a_n) = \lim\limits_{n\to\infty} \varphi(b_n)$. Prin urmare, $\widetilde{\varphi}$ e bine definită. Faptul că $\widetilde{\varphi}$ e o valuare pe $\widetilde{F}$ care verifică inegalitatea triunghiului rezultă uşor din proprietăţile limitelor de şiruri.

Fie $\widetilde{P}$ divizorul prim al lui $\widetilde{F}$ determinat de $\widetilde{\varphi}$ şi $\mu : F \to \widetilde{F}$, funcţia definită prin $\mu(a) = (a, a, \dots, a, \dots) + \mathcal{I}$, pentru orice $a \in F$. Vom arăta în cele ce urmează că $(\widetilde{F}, \widetilde{P}, \mu)$ reprezintă un completat al lui (F, P).

În primul rând, $(\widetilde{F}, \widetilde{P}, \mu)$ e o extindere al lui (F, P), întrucât μ e, în mod clar, un morfism de corpuri, şi $\mu^*(\widetilde{P}) = P$. Pentru ultima afirmaţie e de ajuns să observăm că, oricare ar fi $a \in F$,

$$\widetilde{\varphi}(\mu(a)) = \lim_{n\to\infty} \varphi(a) = \varphi(a)$$

În al doilea rând, $\mu(F)$ este dens în $\widetilde{F}$, deoarece, dacă $\alpha = \{a_n\} + \mathcal{I} \in \widetilde{F}$ atunci $\alpha = \lim\limits_{n\to\infty} \mu(a_n)$. Într-adevăr,

$$\lim_{n\to\infty} \widetilde{\varphi}\big(\alpha - \mu(a_n)\big) = \lim_{n\to\infty} \Big(\lim_{m\to\infty} \varphi(a_m - a_n)\Big) = 0$$

În ultimul rând, $\widetilde{F}$ este complet în raport cu $\widetilde{P}$. Pentru aceasta, fie $\{\alpha_n\}$ un şir Cauchy de elemente din $\widetilde{F}$. Deoarece $\mu(F)$ e dens în $\widetilde{F}$, există, pentru orice $n \geq 1$, $a_n \in F$ astfel încât $\widetilde{\varphi}\big(\alpha_n - \mu(a_n)\big) < 1/n$. Aşadar, şirurile $\{\alpha_n\}$ şi $\{\mu(a_n)\}$ diferă printr-un şir convergent la zero. Cum $\{\alpha_n\}$ e Cauchy, la fel trebuie să fie şi $\{\mu(a_n)\}$. Dar atunci şi $\{a_n\}$ e şir Cauchy, întrucât

$$\varphi(a_m - a_n) = \widetilde{\varphi}\big(\mu(a_m - a_n)\big) = \widetilde{\varphi}\big(\mu(a_m) - \mu(a_n)\big)$$

Fie $\alpha = \{a_n\} + \mathcal{I}$. Deoarece şirul $\{\mu(a_n)\}$ converge către α, aceeaşi proprietate o are şi $\{\alpha_n\}$. Prin urmare, F este complet în raport cu $\widetilde{P}$ şi teorema e complet demonstrată. □

Pentru unicitate avem nevoie de următoarea propoziţie.

Propoziţie 3.1.1. *Fie (E, Q, σ) o extindere a lui (F, P). Dacă $(\widetilde{F}, \widetilde{P}, \mu)$ e un completat al lui (F, P) şi $(\widetilde{E}, \widetilde{Q}, \lambda)$ e un completat al lui (E, Q), atunci există un unic morfism de corpuri $\widetilde{\sigma} : \widetilde{F} \to \widetilde{E}$ cu proprietăţile:*

(i) $(\widetilde{\sigma})^*\big(\widetilde{Q}\big) = \widetilde{P}$

(ii) $\widetilde{\sigma}\mu = \lambda\sigma$

Demonstraţie. Fie $\alpha \in \widetilde{F}$. Deoarece $\mu(F)$ e dens în $\widetilde{F}$, există un şir de elemente $\{a_n\}$ din F astfel încât $\lim\limits_{n\to\infty} \mu(a_n) = \alpha$. Dacă $\widetilde{\sigma} : \widetilde{F} \to \widetilde{E}$ are proprietăţile (i) şi (ii) din teoremă atunci $\widetilde{\sigma}$ e continuă datorită proprietăţii (i) şi, ţinând seama şi de proprietatea (ii),

$$\widetilde{\sigma}(\alpha) = \widetilde{\sigma}\big(\lim_{n\to\infty} \mu(a_n)\big) = \lim_{n\to\infty} \big(\widetilde{\sigma}\mu(a_n)\big) = \lim_{n\to\infty} \big(\lambda\sigma(a_n)\big)$$

Aşadar, proprietăţile (i) şi (ii) determină, în mod unic, morfismul $\widetilde{\sigma}$.

Să arătăm acum că $\widetilde{\sigma} : \widetilde{F} \to \widetilde{E}$ definită prin

$$\widetilde{\sigma}(\alpha) = \lim_{n\to\infty} \lambda\sigma(a_n)$$

unde $\{a_n\}$ e un şir din F cu proprietatea că $\mu(a_n) \to \alpha$, e bine definită şi e un morfism de corpuri care verifică (i) şi (ii). Fixăm, înainte de toate, $\psi \in Q$, $\varphi \in P$, $\widetilde{\psi} \in \widetilde{Q}$ şi $\widetilde{\varphi} \in \widetilde{P}$ astfel încât $\widetilde{\psi}\lambda = \psi$, $\psi\sigma = \varphi$ şi $\widetilde{\varphi}\mu = \varphi$. Deoarece $\{\mu(a_n)\}$ e un şir Cauchy, iar

$$\widetilde{\psi}\big(\lambda\sigma(a_m) - \lambda\sigma(a_n)\big) = \psi\big(\sigma(a_m) - \sigma(a_n)\big) = \varphi(a_m - a_n) = \widetilde{\varphi}\big(\mu(a_m) - \mu(a_n)\big)$$

şirul $\{\lambda\sigma(a_n)\}$ e şi el Cauchy. Cum $\widetilde{E}$ e complet, $\{\lambda\sigma(a_n)\}$ e un şir convergent, deci are sens să vorbim de limita lui. Dacă $\{b_n\}$ e un alt şir din F cu proprietatea că $\mu(b_n) \to \alpha$, atunci din

$$\widetilde{\psi}\big(\lambda\sigma(a_n) - \lambda\sigma(b_n)\big) = \psi\big(\sigma(a_n) - \sigma(b_n)\big) = \varphi(a_n - b_n) = \widetilde{\varphi}\big(\mu(a_n) - \mu(b_n)\big)$$

rezultă că $\lim\limits_{n\to\infty} \lambda\sigma(a_n) = \lim\limits_{n\to\infty} \lambda\sigma(b_n)$. Aşadar, $\widetilde{\sigma}$ e bine definită.

Faptul că $\widetilde{\sigma}$ e morfism de corpuri rezultă după o verificare de rutină, aşa ca nu vom mai arăta decât (i) şi (ii). Pentru (i), ţinem cont că $\widetilde{\psi}$ şi $\widetilde{\varphi}$ sunt continue pentru a deduce că

$$\begin{aligned}\widetilde{\psi}\widetilde{\sigma}(\alpha) &= \widetilde{\psi}\big(\lim_{n\to\infty} \lambda\sigma(a_n)\big) = \lim_{n\to\infty} \widetilde{\psi}\lambda\sigma(a_n) = \lim_{n\to\infty} \psi\sigma(a_n) \\ &= \lim_{n\to\infty} \varphi(a_n) = \lim_{n\to\infty} \widetilde{\varphi}\mu(a_n) = \widetilde{\varphi}(\lim_{n\to\infty} \mu(a_n)) = \widetilde{\varphi}(\alpha)\end{aligned}$$

relaţie ce arată că $(\widetilde{\sigma})^*\big(\widetilde{Q}\big) = \widetilde{P}$. Pentru (ii) avem, $\mu(a) = \lim\limits_{n\to\infty} \mu(a)$, deci $\widetilde{\sigma}\mu(a) = \lim\limits_{n\to\infty} \lambda\sigma(a) = \lambda\sigma(a)$, pentru orice $a \in F$. □

Corolar 3.1.1. *Dacă $(\widetilde{F}, \widetilde{P}, \mu)$ şi $(\widehat{F}, \widehat{P}, \nu)$ sunt doi completaţi ai lui (F, P), atunci există şi e unic un F-izomorfism de corpuri $\sigma : \widetilde{F} \to \widehat{F}$ astfel încât $\sigma^*(\widehat{P}) = \widetilde{P}$.*

În virtutea teoremei 3.1.1 şi corolarului 3.1.1, putem vorbi de "completatul" unui corp cu un divizor prim. Dacă (F, P) e un corp cu un divizor prim, vom privi completatul său ca pe o extindere a lui (F, P) şi îl vom nota cu (F_P, P).

Propoziţie 3.1.2. *Fie E un corp complet în raport cu divizorul prim Q. Dacă (E, Q) e o extindere a lui (F, P) atunci închiderea $\overline{F}$ a lui F în E e un corp şi $(\overline{F}, i^*_{\overline{F}\to E}(Q), i_{F\to\overline{F}})$ e un completat al lui (F, P).*

Demonstraţie. Fie α, $\beta \in \overline{F}$. Există atunci şirurile de elemente din F, $\{x_n\}$ si $\{y_n\}$, astfel încât $x_n \to \alpha$ şi $y_n \to \beta$. Cum E e un corp topologic, avem $\alpha - \beta = \lim_n (x_n - y_n) \in \overline{F}$, $\alpha\,\beta = \lim_n (x_n\, y_n) \in \overline{F}$ şi, dacă $\alpha \neq 0$, atunci există $N \geq 1$ astfel încât $x_n \neq 0$, pentru orice $n \geq N$, şi $1/\alpha = \lim_n 1/x_n \in \overline{F}$. Prin urmare, $\overline{F}$ e subcorp al lui E. Fie $\overline{P} = i^*_{\overline{F}\to E}(Q)$. Deoarece topologia indusă de $\overline{P}$ pe $\overline{F}$ e urma pe $\overline{F}$ a topologiei induse de Q pe E, $(\overline{F}, \overline{P})$ e corp complet. Cum $i^*_{F\to\overline{F}}(\overline{P}) = i^*_{F\to\overline{F}}\, i^*_{\overline{F}\to E}(Q) = i^*_{F\to E}(Q) = P$ si F e dens în $\overline{F}$, rezultă că $(\overline{F}, \overline{P}, i_{F\to\overline{F}})$ e un completat al lui (F, P). □

3.2 Corpuri complete în raport cu divizori primi discreţi

Vom vedea în această secţiune că, în cazul discret, avem o descriere mai precisă a elementelor completatului. Următoarea propoziţie ne va fi de folos.

Propoziţie 3.2.1. *Fie (E, Q) un completat al lui (F, P) cu P nearhimedian. Atunci*

$$e(Q/P) = f(Q/P) = 1$$

În particular, dacă P e discret atunci Q e discret. Mai mult, $\mathcal{O}_Q$ e închiderea lui $\mathcal{O}_P$ în E şi $\mathcal{P}_Q$ e închiderea lui $\mathcal{P}_P$ în E.

Demonstraţie. Fie v o valuare exponenţială care aparţine lui Q şi $\alpha \in E^*$. Cum F este dens în E, există $a \in F$ astfel încât $v(a - \alpha) > v(\alpha)$. Atunci $v(\alpha) = v(a - \alpha + \alpha) = v(a) \in v(F^*)$. Prin urmare, $v(E^*) = v(F^*)$ si $e(Q/P) = 1$.

Pentru a arăta că $f(Q/P) = 1$ e suficient să găsim pentru $\alpha \in \mathcal{O}_Q$ un $a \in \mathcal{O}_P$ astfel încât $v(a - \alpha) > 0$. Ştim că F e dens în E, deci există $a \in F$ astfel încât $v(a-\alpha) > 0$. Cum $v(a) = v(a-\alpha+\alpha) \geq \min\{v(a-\alpha), v(\alpha)\} \geq 0$, $a \in \mathcal{O}_P$. □

Lemă 3.2.1. *Fie P un divizor prim nearhimedian al lui F. Relativ la topologia definită de P, un şir $\{x_n\}$ de elemente ale lui F e şir Cauchy dacă şi numai dacă $x_n - x_{n-1} \to 0$.*

Demonstraţie. Necesitatea fiind evidentă, demonstrăm suficienţa. Fie $\varphi \in P$ şi $\varepsilon > 0$. Există $N \geq 1$ astfel încât $\varphi(x_{n+1} - x_n) < \varepsilon$, oricare ar fi $n \geq N$. Pentru $n \geq N$ şi $p \geq 1$ avem atunci

$$\begin{aligned}\varphi(x_{n+p} - x_n) &= \varphi(x_{n+p} - x_{n+p-1} + \cdots + x_{n+1} - x_n) \\ &\leq \max_{i=1,\ldots,p} \{\varphi(x_{n+i} - x_{n+i-1})\} \\ &< \varepsilon\end{aligned}$$

fapt ce arată ca şirul $\{x_n\}$ e Cauchy. □

Lemă 3.2.2. *Fie F un corp complet în raport cu divizorul prim nearhimedian P. Dacă $\{x_n\}$ e un şir de elemente din F, atunci seria $\sum_n x_n$ e convergentă dacă şi numai dacă $x_n \to 0$.*

Demonstraţie. Fie $\{s_n\}$ şirul sumelor parţiale asociat seriei $\sum_n x_n$. Deoarece F e complet în raport cu P, şirul $\{s_n\}$ e convergent dacă şi numai dacă $\{s_n\}$ e şir Cauchy. Ţinând cont de lema precedentă, ultima afirmaţie e echivalentă cu faptul că $x_n = s_n - s_{n-1} \to 0$. □

Teoremă 3.2.1. *Fie F un corp complet în raport cu divizorul prim discret P. Daca $\mathcal{R}$ e un sistem complet de reprezentanţi pentru $\mathcal{F}_P = \mathcal{O}_P/\mathcal{P}_P$ cu proprietatea că $0 \in \mathcal{R}$, iar $\pi_n \in F$, $n \in \mathbb{Z}$, sunt astfel încât $v_P(\pi_n) = n$, atunci orice element $\alpha \in F^*$ admite o reprezentare unică de forma*

$$\alpha = \sum_{n=r}^{\infty} a_n \pi_n$$

unde $a_n \in \mathcal{R}$ şi $a_r \neq 0$.

Demonstraţie. Fie $\alpha \in F^*$ şi $r = v_P(\alpha)$. Atunci $v_P(\alpha\pi_r^{-1}) = 0$, deci $\alpha\pi_r^{-1} \in \mathcal{U}_P$. Fie $a_r \in \mathcal{R} \setminus \{0\}$ astfel încât $\alpha\pi_r^{-1} - a_r \in \mathcal{P}_P$. Avem

$$v_P(\alpha - a_r\pi_r) \geq r + 1 = v_P(\pi_{r+1})$$

deci $(\alpha - a_r\pi_r)\pi_{r+1}^{-1} \in \mathcal{O}_P$. Fie $a_{r+1} \in \mathcal{R}$ astfel încât $(\alpha - a_r\pi_r)\pi_{r+1}^{-1} - a_{r+1} \in \mathcal{P}_P$. Atunci

$$v_P\big(\alpha - (a_r\pi_r + a_{r+1}\pi_{r+1})\big) \geq r + 2 = v_P(\pi_{r+2})$$

deci există $a_{r+2} \in \mathcal{R}$ astfel încât $[\alpha - (a_r\pi_r + a_{r+1}\pi_{r+1})]\pi_{r+2}^{-1} - a_{r+2} \in \mathcal{P}_P$. Continuând procedeul, obţinem un şir $\{a_n\}_{n\geq r}$ cu proprietatea că

$$v_P\big(\alpha - (a_r\pi_r + \cdots + a_m\pi_m)\big) \geq m+1$$

pentru orice $m \geq r$. Deducem de aici că seria $\sum_{n\geq r} a_n\pi_n$ e convergentă şi suma ei este $\sum_{n=r}^{\infty} a_n\pi_n = \alpha$.

Pentru unicitate să observăm că, dacă $\{a_n\}_{n\geq r}$ e un şir de elemente din $\mathcal{O}_P$ cu $a_r \in \mathcal{U}_P$, atunci seria $\sum_{n\geq r} a_n\pi_n$ e convergentă şi $v_P(\sum_{n=r}^{\infty} a_n\pi_n) = r$. Într-adevăr, deoarece $a_n\pi_n \to 0$, seria $\sum_{n\geq r} a_n\pi_n$ e convergentă, conform lemei 3.2.2. Mai mult, pentru orice $m \geq r$,

$$v_P(a_r\pi_r + \cdots + a_m\pi_m) = v(a_r\pi_r) = r$$

de unde, prin trecere la limită, obţinem $v_P(\sum_{n=r}^{\infty} a_n\pi_n) = r$. Aşadar, dacă α admite reprezentările $\alpha = \sum_{n=r}^{\infty} a_n\pi_n$ şi $\sum_{n=s}^{\infty} b_n\pi_n$, atunci $r = s = v_P(\alpha)$ şi $\sum_{n=r}^{\infty}(a_n - b_n)\pi_n = 0$. Ultima egalitate are loc doar dacă $a_n = b_n$, pentru orice $n \geq r$, fapt ce încheie demonstraţia. □

Corolar 3.2.1. *Fie F un corp complet în raport cu un divizor prim discret P, $\pi \in F$ e un element prim al lui F în raport cu P şi $\mathcal{R}$ un sistem complet de reprezentanţi pentru $\mathcal{F}_P = \mathcal{O}_P/\mathcal{P}_P$ astfel încât $0 \in \mathcal{R}$. Orice element nenul al lui F admite o unică reprezentare ca* ***serie formală Laurent***

$$\sum_{n=r}^{\infty} a_n\pi^n$$

unde $a_n \in \mathcal{R}$ şi $a_r \neq 0$.

Daca (F, P) e un corp cu un divizor prim discret şi $(\widetilde{F}, \widetilde{P})$ e un completat al lui (F, P), atunci corolarul 3.2.1 ne oferă posibilitatea de a exprima elementele lui $\widetilde{F}$ în funcţie de elementele lui F. Mai precis, conform propoziţiei 3.2.1, $\widetilde{P}$ e discret şi orice element prim al lui F în raport cu P e element prim al lui $\widetilde{F}$ în raport cu $\widetilde{P}$. Mai mult, deoarece corpul rezidual al lui F în P coincide cu corpul rezidual al lui $\widetilde{F}$ în $\widetilde{P}$, putem alege ca sistem complet de reprezentanţi pentru $\mathcal{O}_{\widetilde{P}}/\mathcal{P}_{\widetilde{P}}$ un sistem complet de reprezentanţi pentru $\mathcal{O}_P/\mathcal{P}_P$. Aşadar, în virtutea corolarului 3.2.1, elementele lui $\widetilde{F}$ se pot scrie în mod unic ca serii formale Laurent $\sum_{n=r}^{\infty} a_n\pi_P^n$ cu a_n făcând parte dintr-un sistem complet de reprezentanţi pentru $\mathcal{O}_P/\mathcal{P}_P$ şi π_P un element prim al lui F în P.

De exemplu, în cazul lui $(\mathbb{Q}, p)$, un sistem complet de reprezentanţi pentru $\mathcal{O}_p/\mathcal{P}_p \simeq \mathbb{Z}/(p)$ e $\{0, 1, \ldots, p-1\}$ şi un element prim al lui $\mathbb{Q}$ in p e p. Prin urmare, elementele nenule ale lui $\mathbb{Q}_p$ se scriu, în mod unic, sub forma

$$\sum_{n=r}^{\infty} a_n p^n$$

unde $a_n \in \{0, 1, \ldots, p-1\}$, $r \in \mathbb{Z}$ şi $a_r \neq 0$. Întrucât, $v_p\big(\sum_{n=r}^{\infty} a_n p^n\big) = r$, elementele inelului de valuare al lui $\mathbb{Q}_p$ în p sunt serii de forma

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

cu $a_n \in \{0, 1, \ldots, p-1\}$, pentru orice $n \geq 0$. Elementele lui $\mathbb{Q}_p$ se numesc ***numere p-adice***, iar $\mathbb{Q}_p$ se numeşte ***corpul numerelor p-adice***. Inelul de valuare al lui $\mathbb{Q}_p$ în p se notează cu $\mathbb{Z}_p$, iar elementele lui se numesc ***întregi p-adici***.

Fie F un corp şi $F[X]$ inelul de polinoame în nedeterminata X, cu coeficienţi in F. $F[X]$ e un inel factorial cu corpul de fracţii $F(X)$. Dacă X e divizorul prim al lui $F(X)$ asociat polinomului ireductibil $X \in F[X]$, atunci un sistem complet de reprezentanţi pentru $\mathcal{O}_X/\mathcal{P}_X \simeq F[X]/(X)$ e format din elementele lui F, iar un element prim al lui $F(X)$ în X e X. Prin urmare, elementele completatului lui $F(X)$ în raport cu X se scriu, în mod unic, sub forma

$$\sum_{n=r}^{\infty} a_n X^n$$

unde $a_n \in F$, $r \in \mathbb{Z}$ şi $a_r \neq 0$, iar elementele inelului de valuare $\mathcal{O}_X$ al lui $F(X)_X$ în X sunt serii de forma

$$a_0 + a_1 X + a_2 X^2 + \cdots$$

cu $a_n \in F$, pentru orice $n \geq 0$. Se observă că $F(X)_X = F\big((X)\big)$, corpul de serii formale Laurent, iar $\mathcal{O}_X = F\big[[X]\big]$, inelul de serii formale în nedeterminata X, cu coeficienţi în F.

3.3 Valuari arhimediene si teorema lui Ostrowski

Vom demonstra în această secţiune o teoremă a lui Ostrowski care afirmă că, până la un izomorfism de corpuri cu divizori primi, $(\mathbb{R}, P_\infty)$ şi $(\mathbb{C}, P_\infty)$ sunt singurele corpuri complete în raport cu divizori primi arhimedieni. Folosindu-ne de acest rezultat, vom determina apoi toţi divizorii primi arhimedieni ai unui corp de numere algebrice. Pentru corpul numerelor raţionale, însă, lucrurile sunt ceva mai simple.

Propoziţie 3.3.1. *P_∞ e singurul divizor prim arhimedian al lui $\mathbb{Q}$.*

Demonstraţie. Fie P un divizor prim arhimedian al lui $\mathbb{Q}$ şi $\varphi \in P$ astfel încât $\|\varphi\| \leq 2$. Să considerăm doi întregi supraunitari, m şi n. Pentru orice $t > 0$, există $s \geq 0$ şi $a_0, \ldots, a_s \in \{0, \ldots, n-1\}$, $a_s \neq 0$, astfel încât

$$m^t = a_0 + a_1 n + \cdots + a_s n^s$$

Deoarece $a_s \geq 1$, avem $n^s \leq m^t$, deci $s \leq t(\log m / \log n)$. Ţinând cont de faptul că $\varphi(a_i) \leq a_i < n$, pentru orice $i \in \{0, \ldots, n-1\}$, avem

$$\begin{aligned}
\varphi(m)^t &\leq \varphi(a_0) + \varphi(a_1)\varphi(n) + \cdots + \varphi(a_s)\varphi(n)^s \\
&\leq n\big(1 + \varphi(n) + \cdots + \varphi(n)^s\big) \\
&\leq n(s+1)\max\{1, \varphi(n)\}^s \\
&\leq n\left(1 + t\frac{\log m}{\log n}\right)\max\{1, \varphi(n)\}^{t(\log m/\log n)}
\end{aligned}$$

Luând rădăcina de ordin t şi făcând pe t să tindă către ∞, obţinem

$$\varphi(m) \leq \max\{1, \varphi(n)\}^{\log m/\log n}$$

Inegalitatea obţinută e valabilă pentru orice m, $n > 1$ şi ea implică faptul că $\varphi(n) > 1$ pentru orice $n > 1$. Într-adevăr, dacă ar exista $n_0 > 1$ cu proprietatea că $\varphi(n_0) \leq 1$, atunci, înlocuind în inegalitatea de mai sus pe n cu n_0, am obţine $\varphi(m) \leq 1$, pentru orice $m \in \mathbb{Z}$, o contradicţie cu faptul că φ e arhimediană. Aşadar, $\max\{1, \varphi(n)\} = \varphi(n)$, pentru orice $n > 1$, şi inegalitatea de mai sus devine $\varphi(m)^{1/\log m} \leq \varphi(n)^{1/\log n}$, pentru orice m, $n > 1$. Cum relaţia e simetrică în m şi n, avem

$$\varphi(m)^{1/\log m} = \varphi(n)^{1/\log n}$$

pentru orice m, $n > 1$. Considerând $\alpha > 0$ astfel încât $\varphi(n)^{1/\log n} = e^\alpha$, pentru $n > 1$, găsim că $\varphi(n) = n^\alpha$, oricare ar fi $n > 1$. Aşadar, $\varphi(n) = |n|^\alpha$ pentru orice număr întreg n, deci şi pentru orice număr raţional. Cum $\varphi = |\cdot|^\alpha$, tragem concluzia că $P = P_\infty$. □

Următoarele două leme au caracter ajutător.

Lemă 3.3.1. *Fie φ o valuare pe mulţimea numerelor complexe $\mathbb{C}$ astfel încât $\varphi(a) = |a|$ pentru orice $a \in \mathbb{R}$. Atunci $\varphi(a) = |a|$, pentru orice $a \in \mathbb{C}$.*

Demonstraţie. Deoarece $\|\varphi\| = \max\{\varphi(1), \varphi(2)\} = 2$, φ verifică inegalitatea triunghiului. Totodată, $\varphi(i) = 1$, întrucât $1 = \varphi(i)^4$. Prin urmare, dacă $\alpha = a + bi$, unde $a, b \in \mathbb{R}$, atunci

$$\varphi(\alpha) \leq \varphi(a) + \varphi(b) = |a| + |b| \leq \sqrt{2}\sqrt{|a|^2 + |b|^2} = \sqrt{2}\,|\alpha|$$

Fie $f : \mathbb{C}^* \to \mathbb{R}$, $f(\alpha) = \varphi(\alpha)/|\alpha|$, oricare ar fi $\alpha \in \mathbb{C}^*$. Vom arăta că f e funcţia constantă 1, ceea ce va termina demonstraţia. Avem, pentru $\alpha \neq 0$, $0 < f(\alpha) \leq \sqrt{2}$ şi $f(\alpha)^n = f(\alpha^n) \leq \sqrt{2}$ pentru orice întreg pozitiv, n. Deoarece $f(\alpha) \leq 2^{\frac{1}{2n}}$, oricare ar fi $n = 1, 2, 3, \ldots$, obţinem, prin trecere la limită, $f(\alpha) \leq 1$. Cum α a fost ales arbitrar, avem şi inegalitatea $f(1/\alpha) \leq 1$, deci $f(\alpha) = 1$, pentru orice $\alpha \neq 0$. □

Lemă 3.3.2. *Dacă (F, φ) este o extindere a lui $(\mathbb{R}, |\cdot|)$ atunci $(F, \varphi) = (\mathbb{R}, |\cdot|)$ sau $(F, \varphi) = (\mathbb{C}, |\cdot|)$.*

Demonstraţie. E de ajuns să arătăm că F e algebric peste $\mathbb{R}$ fiindcă atunci, considerând pe F ca subcorp al lui $\mathbb{C}$ şi ţinând cont că $[\mathbb{C} : \mathbb{R}] = 2$, vom avea $F = \mathbb{R}$ sau $F = \mathbb{C}$. Luând în considerare lema 3.3.1 demonstraţia va fi incheiată.

Fie $\xi \in F$. Vom arăta că ξ e rădăcina unui polinom monic, de grad 2, cu coeficienţi în $\mathbb{R}$, iar pentru aceasta, vom dovedi că funcţia $f : \mathbb{C} \to \mathbb{R}$ definită prin

$$f(z) = \varphi\big(\xi^2 - (z + \overline{z})\xi + z\overline{z}\big)$$

pentru orice $z \in \mathbb{C}$, atinge valoarea 0. Să observăm întâi că f este continuă şi că $\lim_{z\to\infty} f(z) = \infty$. Avem

$$\begin{aligned} |f(z) - f(z_0)| &= |\varphi\big(\xi^2 - (z + \overline{z})\xi + z\overline{z}\big) - \varphi\big(\xi^2 - (z_0 + \overline{z_0})\xi + z_0\overline{z_0}\big)| \\ &\leq \varphi\big(z\overline{z} - z_0\overline{z_0} + (z_0 + \overline{z_0} - z - \overline{z})\xi\big) \\ &\leq |z\overline{z} - z_0\overline{z_0}| + |z_0 + \overline{z_0} - z - \overline{z}|\varphi(\xi) \end{aligned}$$

Cum cantitatea din dreapta inegalităţii tinde la 0 când z tinde la z_0, rezultă că f este continuă. Pe de altă parte,

$$\begin{aligned} f(z) &\geq \varphi(z\overline{z}) - \varphi(\xi^2) - \varphi(z + \overline{z})\varphi(\xi) \\ &\geq |z|^2 - \varphi(\xi^2) - 2|z|\varphi(\xi) \end{aligned}$$

deci, $\lim_{z\to\infty} f(z) = \infty$. Arătăm acum că f are o valoare minimă, care se va dovedi în final a fi 0. Fie $m = \inf f(\mathbb{C})$. Evident, $m \geq 0$. Fie $M > m$. Cum $\lim_{z\to\infty} f(z) = \infty$, există $r > 0$ astfel încât $f(z) > M$, oricare ar fi $z \in \mathbb{C} \setminus \overline{B}(0, r)$, unde am notat prin $\overline{B}(0, r)$, bila închisă de centru 0 şi

rază r. Deoarece f este continuă şi $\overline{B}(0,r)$ e o mulţime compactă, există z' astfel încât $f(z') = \min\{f(z) \mid z \in \overline{B}(0,r)\}$. De fapt, $f(z') = m$, căci $f(z') \leq f(z)$, oricare ar fi $z \in \mathbb{C}$. Într-adevăr, există $z'' \in \overline{B}(0,r)$ astfel încât $m \leq f(z'') < M$, de unde deducem că

$$f(z') \leq f(z'') < M < f(z)$$

pentru orice $z \in \mathbb{C} \setminus \overline{B}(0,r)$.

Aşadar, f are o valoare minimă, m. Arătăm în continuare că $m = 0$ raţionând prin absurd. Să presupunem, deci, că $m > 0$. Fie $\mathcal{S} = \{z \in \mathbb{C} \mid f(z) = m\}$. Evident, $\mathcal{S}$ este o mulţime nevidă, închisă şi mărginită. Cum $\mathcal{S}$ e nevidă şi compactă, există $z_0 \in \mathcal{S}$ astfel încât $|z_0| \geq |z|$, pentru orice $z \in \mathcal{S}$. Fie ε astfel încât $0 < \varepsilon < m$ şi polinomul cu coeficie@nti reali, $g(X) = X^2 - (z_0 + \overline{z_0})X + z_0\overline{z_0} + \varepsilon$. Deoarece discriminantul lui g e negativ, g are ca rădăcini un număr complex şi conjugatul său, z_1 şi $\overline{z_1}$. Cum $z_1\overline{z_1} = z_0\overline{z_0} + \varepsilon$, avem $|z_1| > |z_0|$, deci $z_1 \notin \mathcal{S}$.

Fie, pentru $n \geq 1$ fixat, polinomul cu coeficienţi reali

$$G(X) = \big(g(X) - \varepsilon\big)^n - (-\varepsilon)^n$$

Dacă notăm cu $\alpha_1, \ldots, \alpha_{2n} \in \mathbb{C}$ rădăcinile sale, atunci

$$G(X) = \prod_{i=1}^{2n}(X - \alpha_i) = \prod_{i=1}^{2n}(X - \overline{\alpha_i})$$

Deoarece $G(z_1) = 0$, z_1 este unul dintre α_i, să zicem $z_1 = \alpha_1$. Evaluând în ξ relaţia

$$G(X)^2 = \prod_{i=1}^{2n}\big(X^2 - (\alpha_i + \overline{\alpha_i})X + \alpha_i\overline{\alpha_i}\big)$$

şi aplicând φ obţinem

$$\varphi\big(G(\xi)^2\big) = \prod_{i=1}^{2n} f(\alpha_i) \geq f(\alpha_1)m^{2n-1}$$

Pe de altă parte,

$$\varphi\big(G(\xi)\big) \leq \varphi\big(\xi^2 - (z_0 + \overline{z_0})\xi + z_0\overline{z_0}\big)^n + \varphi(-\varepsilon)^n = f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n$$

Din cele două inegalităţi rezultă că

$$f(\alpha_1)m^{2n-1} \leq \varphi\big(G(\xi)\big)^2 \leq (m^n + \varepsilon^n)^2$$

de unde obţinem că

$$\frac{f(\alpha_1)}{m} \leq \left[1 + \left(\frac{\varepsilon}{m}\right)^n\right]^2$$

Făcând pe n să tindă către infinit, găsim că $f(\alpha_1)/m \leq 1$, deci $f(\alpha_1) = m$, o contradicţie cu $\alpha_1 = z_1 \notin \mathcal{S}$. □

Teoremă 3.3.1. (Teorema lui Ostrowski) *Dacă F e un corp complet în raport cu un divizor prim arhimedian P, atunci (F, P) e izomorf cu $(\mathbb{R}, P_\infty)$ sau cu $(\mathbb{C}, P_\infty)$, i.e. există un izomorfism σ definit pe F cu valori în $\mathbb{R}$ sau $\mathbb{C}$, astfel încât $P = \sigma^*(P_\infty)$.*

Demonstraţie. Deoarece F admite un divizor prim arhimedian, F are caracteristica zero. Prin urmare, corpul prim al lui F e $\mathbb{Q}$. Restricţia lui P la $\mathbb{Q}$ e P_∞, întrucât acesta e singurul divizor prim arhimedian al lui $\mathbb{Q}$. Fie $\overline{\mathbb{Q}}$ închiderea lui $\mathbb{Q}$ în F şi $\overline{P}$ restricţia lui P la $\overline{\mathbb{Q}}$. Atunci, conform propoziţiei 3.1.2, $(\overline{\mathbb{Q}}, \overline{P}, i_{\mathbb{Q}\to\overline{\mathbb{Q}}})$ e un completat al lui $(\mathbb{Q}, P_\infty)$. Cum $(\mathbb{R}, P_\infty, i_{\mathbb{Q}\to\mathbb{R}})$ e şi el un completat al lui $(\mathbb{Q}, P_\infty)$, există un izomorfism $\tau : \overline{\mathbb{Q}} \to \mathbb{R}$ astfel încât $\overline{P} = \tau^*(P_\infty)$. Considerăm acum o mulţime F' şi o aplicaţie $\sigma : F \to F'$ cu proprietăţile: $\mathbb{R} \subseteq F'$, σ e bijecţie de mulţimi şi $\sigma|_{\overline{\mathbb{Q}}} = \tau$. De exemplu, putem lua $F' = \mathbb{R} \cup (F \setminus \overline{Q})$ şi σ aplicaţia care coincide cu τ pe $\overline{\mathbb{Q}}$ şi cu identitatea pe $F \setminus \overline{Q}$. Deoarece σ e o bijecţie de mulţimi, există pe F' o unică structură de corp astfel încât σ e morfism de corpuri. Relativ la această structură, $\mathbb{R}$ e subcorp al lui F' şi σ extinde izomorfismul τ. Fie $P' = (\sigma^{-1})^*(P)$. Atunci

$$i^*_{\mathbb{R}\to F'}(P') = i^*_{\mathbb{R}\to F'}(\sigma^{-1})^*(P) = (\sigma^{-1}\, i_{\mathbb{R}\to F'})^*(P) = (i_{\overline{\mathbb{Q}}\to F}\tau^{-1})^*(P) = P_\infty$$

ceea ce inseamnă că P' stă deasupra lui P_∞. Considerând $\varphi \in P'$ astfel încât restricţia lui φ la $\mathbb{R}$ e valoarea absolută, deducem din lema 3.3.2 că $(F', P') = (\mathbb{R}, P_\infty)$ sau $(F', P') = (\mathbb{C}, P_\infty)$. □

Definiţie 3.3.1. *Un divizor prim arhimedian P al unui corp F se numeşte **real**, respectiv **complex**, dacă completatul lui (F, P) e izomorf cu $(\mathbb{R}, P_\infty)$, respectiv $(\mathbb{C}, P_\infty)$.*

Împreună cu teorema 2.2.2, teorema următoarea sfârşeşte clasificarea divizorilor primi ai unui corp de numere algebrice.

Teoremă 3.3.2. *Fie F un corp de numere algebrice. Dacă $\sigma_1, \ldots, \sigma_{r_1}$ sunt scufundările reale ale lui F şi $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ sunt scufundări complexe ale lui F alese astfel încât fiecare pereche conjugată de scufundări complexe e reprezentată o singură dată, atunci divizorii primi arhimedieni ai lui F sunt $\sigma_1^*(P_\infty), \ldots, \sigma_{r_1+r_2}^*(P_\infty)$.*

Demonstraţie. Fie P un divizor prim arhimedian al lui F şi $(\widetilde{F},\widetilde{P})$ un completat al lui (F,P). Conform teoremei 3.3.1, $(\widetilde{F},\widetilde{P})$ e izomorf cu $(\mathbb{R},P_\infty)$ sau cu $(\mathbb{C},P_\infty)$. Dacă $\sigma:\widetilde{F}\to\mathbb{R}$ e astfel încât $\sigma^*(P_\infty)=\widetilde{P}$, atunci $\sigma\, i_{F\to\widetilde{F}}$ e o scufundare reală a lui F cu proprietatea că

$$(\sigma\, i_{F\to\widetilde{F}})^*(P_\infty)=i^*_{F\to\widetilde{F}}\sigma^*(P_\infty)=i^*_{F\to\widetilde{F}}(\widetilde{P})=P$$

În mod similar, dacă $\sigma:\widetilde{F}\to\mathbb{C}$ e astfel încât $\sigma^*(P_\infty)=\widetilde{P}$, atunci $\sigma\, i_{F\to\widetilde{F}}$ e o scufundare complexă a lui F cu proprietatea că $(\sigma\, i_{F\to\widetilde{F}})^*(P_\infty)=P$. Aşadar, divizorii primi arhimedieni ai lui F sunt de forma $\sigma^*(P_\infty)$, unde σ e o scufundare a lui F în corpul numerelor complexe. Să arătăm că $\sigma_1^*(P_\infty),\ldots,\sigma^*_{r_1+r_2}(P_\infty)$ sunt toţi divizorii primi ai lui F.

În primul rând, dacă $(\sigma_{r_1+i},\overline{\sigma}_{r_1+i})$ e o pereche conjugată de scufundări complexe ale lui F, atunci e uşor de văzut că $\sigma^*_{r_1+i}(P_\infty)=\overline{\sigma}^*_{r_1+i}(P_\infty)$. În al doilea rând, să observăm că, dacă $\overline{\sigma_i(F)}$ e închiderea lui $\sigma_i(F)$ în $\mathbb{C}$, atunci $(\overline{\sigma_i(F)},P_\infty,\sigma_i)$ e un completat al lui $(F,\sigma_i^*(P_\infty))$ şi $\overline{\sigma_i(F)}=\mathbb{R}$, pentru $i=1,\ldots,r_1$, şi $\overline{\sigma_i(F)}=\mathbb{C}$, pentru $i=r_1+1,\ldots,r_1+r_2$. Într-adevăr, dacă $i\in\{1,\ldots,r_1\}$, atunci $\mathbb{R}=\overline{\mathbb{Q}}\subseteq\overline{\sigma_i(F)}\subseteq\mathbb{R}$, iar dacă $i\in\{r_1+1,\ldots,r_1+r_2\}$, atunci $\overline{\sigma_i(F)}$ e o extindere strictă a lui $\mathbb{R}$, prin urmare, $\overline{\sigma_i(F)}=\mathbb{C}$.

Să presupunem acum că $\sigma_i^*(P_\infty)=\sigma_j^*(P_\infty)$. Atunci $\overline{\sigma_i(F)}=\overline{\sigma_j(F)}$. Fie izomorfismul $\theta:\sigma_i(F)\to\sigma_j(F)$, $\theta\big(\sigma_i(x)\big)=\sigma_j(x)$, pentru orice $x\in F$. Ţinând cont de propoziţia 3.1.1, există un izomorfism continuu $\rho:\overline{\sigma_i(F)}\to\overline{\sigma_j(F)}$ care extinde pe θ. Dacă $\overline{\sigma_i(F)}=\mathbb{R}$, atunci ρ nu poate fi decât morfismul identitate al lui $\mathbb{R}$, iar dacă $\overline{\sigma_i(F)}=\mathbb{C}$, atunci ρ e sau morfismul identitate al lui $\mathbb{C}$ sau morfismul de luare a conjugatului. În ambele cazuri avem $i=j$ şi teorema e demonstrată. □

Capitolul 4

Extinderea valuărilor - cazul corpului de bază complet

Ne ocupăm în aceast capitol şi în următorul de problema extinderii: dat un corp F, un divizor prim P al lui F şi E/F o extindere finită de corpuri, se cere să se determine dacă există divizori primi ai lui E care stau deasupra lui P şi, în caz afirmativ, să se stabilească numărul lor. În cazul în care P e divizorul prim trivial, răspunsul e şi el trivial. Mai general, avem următoarea

Propoziţie 4.0.2. *Fie P divizorul prim trivial al corpului F. Dacă E e o extindere algebrică a lui F atunci P are o unică extindere la E, anume, divizorul prim trivial.*

Demonstraţie. Evident, divizorul prim trivial al lui E e o extindere a lui P la E. Să arătăm că e unica. Fie Q un divizor prim al lui E care divide P şi $\varphi \in Q$. E uşor de văzut că orice element algebric peste F face parte din inelul de valuare al lui E în Q. De exemplu, dacă $\alpha^n = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, unde $a_0, \ldots, a_{n-1} \in F$, atunci

$$\varphi(\alpha)^n \leq \max_i \{\varphi(a_i\alpha^i)\} = \max_i \{\varphi(\alpha)^i\}$$

deci $\varphi(\alpha) \leq 1$. Cum E e algebric peste F, avem că $E = \mathcal{O}_Q$. Dar asta atrage după sine faptul că Q e trivial, fiindcă, dacă $\alpha \in E^*$ atunci $\varphi(\alpha) \leq 1$ şi $\varphi(\alpha^{-1}) \leq 1$ implică $\varphi(\alpha) = 1$. □

În baza acestui rezultat, vom exclude din discuţiile ce vor veni divizorul prim trivial. Vom arăta, în cele ce urmează, că, dacă F e complet în raport cu P, atunci există şi e unică o extindere a lui P la E.

4.1 Spaţii normate. Unicitatea extinderii

Pentru a arăta unicitatea extinderii, se dovedeşte util următorul concept.

Definiţie 4.1.1. *Fie (F, φ) un corp valuat. Un **spaţiu normat** peste (F, φ) este o pereche $(V, \|\cdot\|)$ formată dintr-un F-spaţiu vectorial, V, şi o funcţie, numită **normă**, $\|\cdot\| : V \to \mathbb{R}$, având următoarele proprietăţi:*

(i) $\|v\| \geq 0$, *oricare ar fi* $v \in V$ *şi* $\|v\| = 0 \Leftrightarrow v = 0$

(ii) $\|av\| = \varphi(a)\|v\|$, *oricare ar fi* $a \in F$ *si* $v \in V$

(iii) $\|v + w\| \leq \|v\| + \|w\|$, *oricare ar fi* v, $w \in V$

Dacă $(V, \|\cdot\|)$ este un spaţiu normat peste (F, φ) atunci avem, în mod natural, o topologie metrică pe V, definită de funcţia

$$d : V \times V \to \mathbb{R},\ d(v, w) = \|v - w\|,\ \ v, w \in V$$

În raport cu această topologie $(V, +)$ e un grup topologic, după cum se poate uşor constata.

Orice F-spaţiu vectorial finit dimensional V poate fi înzestrat cu o structură de spaţiu normat peste (F, φ) dacă $\|\varphi\| \leq 2$. O normă pe V, în acest caz, poate fi definită în felul următor: se alege o bază arbitrară, $\{e_1, \ldots, e_n\}$, a lui V şi, pentru $v = a_1e_1 + \cdots + a_ne_n$ se pune

$$\|v\| = \max\{\varphi(a_1), \ldots, \varphi(a_n)\}$$

O verificare de rutină arată că $(V, \|\cdot\|)$ este un spaţiu normat peste (F, φ). Norma $\|\cdot\|$ se numeşte **norma canonică** asociată bazei $\{e_1, \ldots, e_n\}$. Următoarea teoremă afirmă că, în cazul în care F e complet în raport cu topologia definită de φ, atunci orice altă normă pe V defineşte aceeaşi topologie pe V ca şi $\|\cdot\|$.

Teoremă 4.1.1. *Fie (F, φ) e un corp valuat complet astfel încât $\|\varphi\| \leq 2$. Dacă $(V, |\cdot|)$ e un spaţiu normat peste (F, φ), finit dimensional, atunci există constantele D_1, $D_2 > 0$ astfel încât, considerând norma canonică $\|\cdot\|$ asociată bazei $\{e_1, \ldots, e_n\}$ a lui V, să avem*

$$D_1\|v\| \leq |v| \leq D_2\|v\|$$

oricare ar fi $v \in V$. În particular, orice două norme pe V induc aceeaşi topologie pe V şi V e complet în raport cu această topologie.

Demonstraţie. Vom demonstra întâi că V e complet relativ la topologia definită de $\|\cdot\|$. Fie $\{v_k = a_1^{(k)}e_1 + \cdots + a_n^{(k)}e_n\}_{k\geq 1}$ un şir Cauchy de elemente din V. Atunci $\{a_i^{(k)}\}_{k\geq 1}$ e un şir Cauchy de elemente din F pentru orice $i = 1, \ldots, n$, întrucât

$$\varphi\big(a_i^{(j)} - a_i^{(k)}\big) \leq \|v_j - v_k\|$$

Cum F e complet în raport cu φ, există $a_i \in F$, $i = 1, \ldots, n$, astfel încât $a_i^{(k)} \to a_i$. Punând $v = a_1e_1 + \cdots + a_ne_n$ şi ţinând seama că

$$\|v_k - v\| = \max_i \{\varphi\big(a_i^{(k)} - a_i\big)\} \to 0$$

găsim că $(v_k)_k$ e un şir convergent la v, deci V e, într-adevăr, complet în topologia normei canonice.

Pentru restul demonstraţiei folosim inducţia după n. Dacă $n = 1$, atunci orice element al lui V e de forma ae_1, unde $a \in F$. Ţinând cont de proprietăţile unei norme, avem

$$|ae_1| = \varphi(a)|e_1| = \|ae_1\| \cdot |e_1|$$

oricare ar fi $a \in F$, şi putem lua $D_1 = D_2 = |e_1|$.

Presupunem acum că teorema e adevărată în cazul spaţiilor normate peste (F, φ), $(n-1)$-dimensionale, şi o demonstrăm pentru spaţiile de dimensiune n. Fie, pentru $i = 1, \ldots, n$,

$$V_i = Fe_i + \cdots + Fe_{i-1} + Fe_{i+1} + \cdots + Fe_n$$

Din ipoteza de inducţie, V_i e complet în raport cu topologia indusă de $|\cdot|$, prin urmare, e o submulţime închisă a lui V. Tot submulţime închisă e şi $V_i + e_i$, deoarece translaţiile lui V sunt homeomorfisme. Cum $\bigcup_{i=1}^n (V_i + e_i)$ e închisă şi $0 \notin \bigcup_{i=1}^n (V_i + e_i)$, există $D_1 > 0$ astfel încât

$$|v_i + e_i| \geq D_1$$

pentru orice $v_i \in V_i$ şi orice $i \in \{1, \ldots, n\}$.

Fie acum $v = a_1e_1 + \cdots + a_ne_n \in V \setminus \{0\}$ şi $r \in \{1, \ldots n\}$ astfel încât $\|v\| = \varphi(a_r)$. Atunci $a_r \neq 0$ şi

$$|a_r^{-1}v| = \left|\frac{a_1}{a_r}e_1 + \cdots + e_r + \cdots + \frac{a_n}{a_r}e_r\right| \geq D_1$$

deci, $|v| \geq D_1\varphi(a_r) = D_1\|v\|$. Cum

$$|v| = |a_1e_1 + \cdots + a_ne_n| \leq \varphi(a_1)|e_1| + \cdots + \varphi(a_n)|e_n| \leq D_2\|v\|$$

unde $D_2 = |e_1| + \cdots + |e_n|$, demonstraţia e încheiată. □

Corolar 4.1.1. *Fie F un corp complet în raport cu divizorul prim P şi E/F o extindere finită de corpuri. Dacă $\varphi \in P$ admite o extindere la E, atunci aceasta este unică şi, relativ la topologia definită de ea, E este complet. Aşadar, P admite cel mult o extindere la E, şi, în caz că această extindere există, E e complet.*

Demonstraţie. Fie ψ_1 şi ψ_2 două extinderi ale lui φ la E. Deoarece ψ_1^α şi ψ_2^α sunt extinderi ale lui φ^α, ne putem reduce la cazul $\max\{\|\psi_1\|, \|\psi_2\|, \|\varphi\|\} \leq 2$. În acest caz, (E, ψ_1) şi (E, ψ_2) sunt spaţii normate finit dimesionale peste (F, φ) şi putem aplica teorema 4.1.1 pentru a deduce că topologiile definite de ψ_1 şi ψ_2 coincid, iar E e complet în raport cu această topologie. Folosindu-ne de teorema 1.2.1 deducem că $\psi_2 = \psi_1^\alpha$ pentru un $\alpha > 0$, deci, prin restricţie, $\varphi = \varphi^\alpha$. Cum φ nu e trivială, avem $\alpha = 1$ şi $\psi_1 = \psi_2$. □

Corolar 4.1.2. *Fie F un corp complet în raport cu divizorul prim P şi Ω o extindere algebrică a lui F. Dacă $\varphi \in P$ admite o extindere la Ω, atunci aceasta este unică. Prin urmare, P admite cel mult o extindere la Ω.*

Demonstraţie. Fie ψ_1 şi ψ_2 două extinderi ale lui φ la Ω şi $\alpha \in \Omega$ un element arbitrar. Deoarece $F(\alpha)$ este o extindere finită a lui F, iar restricţiile lui ψ_1 şi ψ_2 la $F(\alpha)$ sunt extinderi ale lui φ la $F(\alpha)$, avem, conform corolarului precedent, că $\psi_1(\alpha) = \psi_2(\alpha)$. □

4.2 Lema lui Hensel. Existenţa extinderilor

Vom arăta acum că, dacă F e complet în raport cu P şi E e o extindere finită a lui F, atunci există o extindere a lui P la E. Să observăm, însă, inainte, că, dacă P e arhimedian, atunci teorema lui Ostrowski ne asigură de existenţa şi unicitatea extinderii. Prin urmare, ne rămâne de studiat cazul în care P e nearhimedian. În acest caz, vom face apel la următoarea lemă, pentru care introducem următoarea definiţie.

Definiţie 4.2.1. *Fie P un divizor prim nearhimedian al lui F şi $v \in P$ o valuare exponenţială. Dacă $f = a_0 + a_1X + \cdots + a_nX^n \in F[X]$, atunci*

$$\overline{v}(f) = \min\{v(a_0), \ldots, v(a_n)\}$$

*Un polinom $f \in \mathcal{O}_P[X]$ se numeşte **polinom primitiv** dacă $\overline{v}(f) = 0$.*

Dacă $f \in \mathcal{O}_P[X]$, atunci vom nota cu $\overline{f}$ imaginea sa prin morfismul canonic $\mathcal{O}_P[X] \to \mathcal{F}_P[X]$.

Lemă 4.2.1. (Lema lui Hensel) *Fie F un corp complet în raport cu divizorul prim nearhimedian P şi $f \in \mathcal{O}_P[X]$ un polinom primitiv. Dacă $\overline{f} \in \mathcal{F}_P[X]$ admite descompunerea*

$$\overline{f}(X) = \mathcal{G}(X)\mathcal{H}(X)$$

unde $\mathcal{G}$, $\mathcal{H} \in \mathcal{F}_P[X]$ sunt polinoame relativ prime între ele, atunci f admite descompunerea

$$f(X) = g(X)h(X)$$

unde g, $h \in \mathcal{O}_P[X]$ sunt astfel încât

$$\overline{g} = \mathcal{G}, \qquad \overline{h} = \mathcal{H}, \qquad \deg g = \deg \mathcal{G}$$

Demonstraţie. Fie $s = \deg f$ şi $r = \deg \mathcal{G}$. Este clar că $\deg \overline{f} \leq s$ şi $\deg \mathcal{H} \leq s - r$.

Fie g_1, $h_1 \in \mathcal{O}_P[X]$ astfel încât $\overline{g}_1 = \mathcal{G}$, $\deg g_1 = \deg \mathcal{G}$, $\overline{h}_1 = \mathcal{H}$ şi $\deg h_1 = \deg \mathcal{H}$. Deoarece $\overline{f} = \mathcal{G}\mathcal{H}$, avem $f - g_1h_1 \in \mathcal{P}_P[X]$. Mai ştim că $\mathcal{G}$ şi $\mathcal{H}$ sunt relativ prime între ele, deci există a, $b \in \mathcal{O}_P[X]$ astfel încât $\overline{a}\mathcal{G} + \overline{b}\mathcal{H} = 1$. Aşadar, $ag_1 + bh_1 - 1 \in \mathcal{P}_P[X]$. Fie

$$\varepsilon = \min\{\overline{v}(f - g_1h_1), \overline{v}(ag_1 + bh_1 - 1)\}$$

Dacă $\varepsilon = \infty$, atunci $f = g_1h_1$ şi nu mai avem nimic de demonstrat. Dacă $\varepsilon \neq \infty$, atunci există $\pi \in \mathcal{P}_P$ astfel încât $v(\pi) = \varepsilon$. Relaţia $\overline{v}(f - g_1h_1) \geq \varepsilon = v(\pi)$ este echivalentă atunci cu faptul că $f - g_1h_1 \in \pi\mathcal{O}_P[X]$.

Vom construi în cele ce urmează, pornind de la g_1 şi h_1, polinomele g_i, $h_i \in \mathcal{O}_P[X]$, $i = 1, 2, 3, \ldots$, cu următoarele proprietăţi:

$$f \equiv g_ih_i \,(\mathrm{mod}\, \pi^i) \tag{4.1}$$

$$g_i \equiv g_{i-1} \,(\mathrm{mod}\pi^{i-1}),\ h_i \equiv h_{i-1} \,(\mathrm{mod}\pi^{i-1}) \qquad (i > 1) \tag{4.2}$$

$$\overline{g}_i = \mathcal{G},\ \overline{h}_i = \mathcal{H} \tag{4.3}$$

$$\deg g_i = \deg \mathcal{G} = r,\ \deg h_i \leq s - r \tag{4.4}$$

Construcţia fiind realizată pentru $i = 1$, să presupunem că am găsit polinoamele $g_1, \ldots, g_{n-1}, h_1, \ldots, h_{n-1} \in \mathcal{O}_P[X]$ cu proprietăţile cerute şi să construim g_n şi h_n. Luând în considerare relaţia (4.2), g_n şi h_n trebuie să fie de forma

$$g_n = g_{n-1} + \pi^{n-1}u$$
$$h_n = h_{n-1} + \pi^{n-1}v$$

unde $u,\ v \in \mathcal{O}_P[X]$. Căutăm, aşadar, $u,\ v \in \mathcal{O}_P[X]$ astfel încât relaţiile (4.1), (4.3) şi (4.4) să aibă loc pentru $i = n$. Deoarece

$$g_n h_n = g_{n-1}h_{n-1} + \pi^{n-1}(g_{n-1}v + h_{n-1}u) + \pi^{2n-2}uv$$

şi $2n-2 \geq n$, relaţia (4.1) e satisfăcută dacă şi numai dacă $f \equiv g_{n-1}h_{n-1} + \pi^{n-1}(g_{n-1}v + h_{n-1}u) \pmod{\pi^n}$. Folosindu-ne de ipoteza de inducţie, avem că $w = (f - g_{n-1}h_{n-1})/\pi^{n-1} \in \mathcal{O}_P[X]$. Aşadar, $f \equiv g_n h_n \pmod{\pi^n}$ dacă şi numai dacă $w \equiv g_{n-1}v + h_{n-1}u \pmod{\pi}$. Deoarece $g_i \equiv g_{i-1} \pmod{\pi^{i-1}}$, oricare ar fi $i \in \{1, \ldots, n-1\}$, avem $g_{n-1} \equiv g_1 \pmod{\pi}$ şi, în mod similar, $h_{n-1} \equiv h_1 \pmod{\pi}$. Prin urmare, trebuie să determinăm u şi v astfel încât $w \equiv g_1 v + h_1 u \pmod{\pi}$ şi (4.3) şi (4.4) să aibă loc.

Ne reamintim că $g_1 a + h_1 b \equiv 1 \pmod{\pi}$, deci $g_1 aw + h_1 bw \equiv w \pmod{\pi}$. Deoarece coeficientul dominant al lui g_1 e un element inversabil în $\mathcal{O}_P$, putem împărţi cu rest în $\mathcal{O}_P[X]$ pe bw la g_1. Vom lua pe postul lui u restul acestei împărţiri. Aşadar, $bw = qg_1 + u$, unde $q \in \mathcal{O}_P[X]$ şi $\deg u < \deg g_1 = r$. Relaţia $g_1 aw + h_1 bw \equiv w \pmod{\pi}$ devine atunci

$$g_1(aw + h_1 q) + h_1 u \equiv w \pmod{\pi}$$

Fie v polinomul obţinut din $aw + h_1 q$ prin eliminarea monoamelor ale căror coeficienţi sunt multipli de π. Atunci $aw + h_1 q \equiv v \pmod{\pi}$, deci $g_1 v + h_1 u \equiv w \pmod{\pi}$. În plus, $\deg v \leq s - r$. Într-adevăr, din faptul că $g_1 v + h_1 u - w \in \pi\mathcal{O}_P[X]$, iar coeficientul dominant al lui $g_1 v$ nu se află în $\pi\mathcal{O}$, deducem că

$$r + \deg v = \deg g_1 v \leq \deg(h_1 u - w) \leq \max\{\deg(h_1 u), \deg w\} \leq s$$

de unde afirmaţia noastră. Este acum uşor de văzut că $g_n = g_{n-1} + \pi^{n-1}u$ şi $h_n = h_{n-1} + \pi^{n-1}v$ verifică condiţiile (4.3) şi (4.4).

Fie, pentru $i = 1, 2, 3, \ldots$, $g_i(X) = a_0^{(i)} + a_1^{(i)}X + \cdots + a_r^{(i)}X^r$, unde $a_j^{(i)} \in \mathcal{O}_P$. Ţinând cont de relaţia (4.2), avem, pentru $j = 0, 1, \ldots, r$, $a_j^{(i+1)} \equiv a_j^{(i)} \pmod{\pi^i}$, oricare ar fi $i \geq 1$. Aşadar, conform propoziţiei 3.2.1, $\{a_j^{(i)}\}_i$ e un şir Cauchy pentru orice $j \in \{0, \ldots, r\}$. Cum F e complet, există $a_j \in F$, $j = 0, \ldots, r$, astfel încât $a_j^{(i)} \to a_j$. Din continuitatea lui φ rezultă că $a_j \in \mathcal{O}_P$, pentru orice $j \in \{0, \ldots, r\}$. Fie $g(X) = a_0 + a_1 X + \cdots + a_r X^r$. Să observăm că, deoarece $a_j^{(i+n)} \equiv a_j^{(i)} \pmod{\pi^i}$, oricare ar fi $n \geq 1$, rezultă, prin trecere la limită, că $a_j \equiv a_j^{(i)} \pmod{\pi^i}$, oricare ar fi j şi i. Prin urmare, $g \equiv g_i \pmod{\pi^i}$, $i = 1, 2, 3, \ldots$. În mod similar, găsim $h(X) = b_0 + b_1 X + \cdots + b_{s-r}X^{s-r} \in \mathcal{O}_P[X]$ astfel încât $h \equiv h_i \pmod{\pi^i}$, pentru orice i. Deoarece

$$f \equiv g_i h_i \equiv gh \pmod{\pi^i}$$

oricare ar fi $i \geq 1$, avem $f = gh$. În fine, $\overline{g} = \overline{g}_i = \mathcal{G}$, $\overline{h} = \overline{h}_i = \mathcal{H}$ şi, din $s = \deg f = \deg g + \deg h \leq r + s - r = s$, rezultă $\deg g = r = \deg \mathcal{G}$. □

Din demonstraţie se poate observa că, dacă $\mathcal{G}$, respectiv $\mathcal{H}$, e monic atunci polinomul g, respectiv h, poate fi ales monic.

Prezentăm în continuare câteva aplicaţii ale lemei lui Hensel. Pe baza lor vom putea demonstra teoremă 4.2.1.

Corolar 4.2.1. *Dacă $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ e ireductibil, atunci*

$$\overline{v}(f) = \min\{v(a_0), \ldots, v(a_n)\} = \min\{v(a_0), v(a_n)\}$$

În particular, dacă $a_n = 1$ şi $a_0 \in \mathcal{O}_P$, atunci $f \in \mathcal{O}_P[X]$.

Demonstraţie. Fie $\min\{v(a_0), \ldots, v(a_n)\} = v(a_i)$ şi $g(X) = a_i^{-1}f(X) = b_0 + b_1X + \cdots + b_nX^n$. Întrucât $b_j = a_i^{-1}a_j$ şi $v(a_i) \leq v(a_j)$, oricare ar fi $j \in \{0, \ldots, n\}$, $g \in \mathcal{O}_P[X]$ şi $\overline{v}(g) = 0$. Vom arăta că $\min\{v(b_0), v(b_n)\} = 0$, fapt ce ne va permite să deducem că $\min\{v(a_0), v(a_n)\} = v(a_i) = \overline{v}(f)$.

Presupunem, prin absurd, că $\min\{v(b_0), v(b_n)\} > 0$. Fie b_r primul, de la dreapta la stânga, dintre coeficienţii $b_0, b_1, \ldots, b_n$ cu proprietatea că $v(b_r) = 0$. Atunci $0 < r < n$ şi $\overline{g}$ admite în $\mathcal{F}_P[X]$ descompunerea

$$\overline{g}(X) = X^r(\overline{b}_r + \overline{b}_{r+1}X^{r+1} + \cdots + \overline{b}_nX^n)$$

Conform lemei lui Hensel, g e divizibil cu un polinom de grad r, lucru contrazis de ireductibilitatea lui f. □

Corolar 4.2.2. *Fie E o extindere finită a lui F şi $\alpha \in E$. Atunci $P_{\alpha,F} \in \mathcal{O}_P[X]$ dacă şi numai dacă $N_{E/F}(\alpha) \in \mathcal{O}_P$.*

Demonstraţie. Deoarece $N_{E/F}(\alpha) = \pm P_{\alpha,F}(0)^{[E:F(\alpha)]}$, avem $N_{E/F}(\alpha) \in \mathcal{O}_P$ dacă şi numai dacă $P_{\alpha,F}(0) \in \mathcal{O}_P$. Ţinând cont de corolarul 4.2.1, obţinem rezultatul dorit. □

Corolar 4.2.3. *Dacă $f \in \mathcal{O}_P[X]$ e monic şi ireductibil peste F, atunci $\overline{f}$ e o putere a unui polinom ireductibil din $\mathcal{F}_P[X]$.*

Demonstraţie. Dacă, prin absurd, $\overline{f}$ nu ar fi o putere a unui polinom ireductibil din $\mathcal{F}_P[X]$ atunci, aplicând lema lui Hensel, după o alegere convenabilă a polinoamelor $\mathcal{G}$ şi $\mathcal{H}$, ar rezulta că f nu e ireductibil. □

Corolar 4.2.4. *Fie $f \in \mathcal{O}_P[X]$ un polinom primitiv. Dacă $\alpha \in \mathcal{F}_P$ e o rădăcină simplă a lui $\overline{f}$, atunci există $a \in \mathcal{O}_P$ astfel încât $\overline{a} = \alpha$ şi $f(a) = 0$.*

Demonstraţie. Fie $\mathcal{H} \in \mathcal{F}_P[X]$ astfel încât $\overline{f} = (X - \alpha)\mathcal{H}$. Cum $X - \alpha$ şi $\mathcal{H}$ sunt prime între ele, lema lui Hensel ne asigură de existenţa unui polinom monic, de gradul întâi, $g \in \mathcal{O}_P[X]$, astfel încât $g \mid f$ şi $\overline{g} = X - \alpha$. Dacă $g = X - a$, atunci a verifică proprietăţile din enunţ. □

O consecinţă imediată a acestui corolar e faptul că $\mathbb{Q}_p$ conţine $(p-1)$-rădăcinile unităţii. Pentru aceasta, e de ajuns să observăm că $X^{p-1} - 1$ se descompune în factori liniari în corpul rezidual al lui $\mathbb{Q}_p$, care e corpul cu p elemente.

Corolar 4.2.5. *Fie p e un număr prim impar şi α un întreg p-adic inversabil. Atunci*

$$\alpha \in \mathbb{Q}_p^2 \Leftrightarrow \overline{\alpha} \in \mathcal{F}_p^2$$

Demonstraţie. Dacă $\alpha \in \mathbb{Q}_p^2$, atunci $\alpha = \beta^2$, pentru un întreg p-adic inversabil, β. Trecând la clase modulo idealul prim în p, găsim că $\overline{\alpha} = \overline{\beta}^2 \in \mathcal{F}_p^2$. Reciproc, dacă există $\beta \in \mathbb{Z}_p$ astfel încât $\overline{\alpha} = \overline{\beta}^2$, atunci, în $\mathcal{F}_p[X]$, avem

$$X - \overline{\alpha} = (X - \overline{\beta})(X + \overline{\beta})$$

Cum $\overline{\beta} \neq -\overline{\beta}$ şi $X^2 - \alpha$ e polinom primitiv, deducem din corolarul 4.2.4 că $\alpha \in \mathbb{Q}_p^2$. □

Suntem acum în măsură să demonstrăm următoarea

Teoremă 4.2.1. *Fie F un corp complet în raport cu divizorul prim nearhimedian P şi E o extindere finită, de grad n, a lui F. Atunci:*

(i) *P are o unică extindere, Q, la E şi E e complet în raport cu Q. Dacă $\varphi \in P$, atunci unica sa extindere la E e $\varphi' \in Q$, unde*

$$\varphi'(\alpha) = \sqrt[n]{\varphi[N_{E/F}(\alpha)]}$$

oricare ar fi $\alpha \in E$.

(ii) *P e discret dacă şi numai dacă Q e discret.*

(iii) *$\mathcal{O}_Q$ e închiderea întreagă a lui $\mathcal{O}_P = \mathcal{O}_Q \cap F$ în E.*

Demonstraţie. (i) În virtutea corolarului 4.1.1, nu trebuie să arătăm decât că φ' extinde pe φ la E. Ţinând cont de proprietăţile normei,

$$N_{E/F}(\alpha) = 0 \Leftrightarrow \alpha = 0$$

$$N_{E/F}(\alpha\,\beta) = N_{E/F}(\alpha)N_{E/F}(\beta),\ \alpha,\beta \in E$$
$$N_{E/F}(\alpha) = \alpha^n,\ \alpha \in F$$

singurul lucru netrivial de demonstrat e condiţia (iii) din definiţia 1.1.1. O demonstrăm pentru $C = 1$.

Fie $\alpha \in E$ astfel încât $\varphi'(\alpha) \leq 1$. Atunci $N_{E/F}(\alpha) \in \mathcal{O}_P$, deci, luând în considerare corolarul 4.2.2, $P_{\alpha,F} \in \mathcal{O}_P[X]$. Polinomul $f(X) = P_{\alpha,F}(X-1)$ e polinomul minimal al lui $1+\alpha$ peste F, deoarece e monic, e ireductibil în $F[X]$ şi se anulează în $1+\alpha$. Notând cu $m = [E : F(\alpha)]$, avem

$$N_{E/F}(1+\alpha) = [\pm f(0)]^m = [\pm P_{\alpha,F}(-1)]^m \in \mathcal{O}_P$$

deci $\varphi'(1+\alpha) \leq 1$.
(ii) Rezultă din relaţia

$$\log\,\varphi'(\alpha) = \frac{1}{n}\log\,\varphi[N_{E/F}(\alpha)]$$

(iii) În primul rând, elementele lui $\mathcal{O}_Q$ sunt întregi peste $\mathcal{O}_P$. Într-adevăr, dacă $\alpha \in \mathcal{O}_Q$ atunci $N_{E/F}(\alpha) \in \mathcal{O}_P$, deci $P_{\alpha,F} \in \mathcal{O}_P[X]$, conform corolarului 4.2.2. Cum $P_{\alpha,F}(\alpha) = 0$, rezultă că α e întreg peste $\mathcal{O}_P$. Reciproc, dacă α e întreg peste $\mathcal{O}_P$, atunci α verifică o relaţie de forma

$$\alpha^r + a_{r-1}\alpha^{r-1} + \cdots + a_0 = 0$$

unde $a_0, \ldots, a_{r-1} \in \mathcal{O}_P$. Prin urmare,

$$\varphi'(\alpha)^r = \varphi'(a_{r-1}\alpha^{r-1} + \cdots + a_0) \leq \max_{i=0,\ldots,r-1}\{\varphi'(\alpha)^i\}$$

de unde rezultă uşor că $\varphi'(\alpha) \leq 1$, i.e. $\alpha \in \mathcal{O}_Q$.

În fine,

$$\mathcal{O}_Q \cap F = \{\alpha \in F\,:\,\varphi'(\alpha) \leq 1\} = \{\alpha \in F\,:\,\varphi(\alpha) \leq 1\} = \mathcal{O}_P$$

□

Corolar 4.2.6. *Fie F un corp complet în raport cu un divizor prim P. Dacă Ω e o extindere algebrică a lui F, atunci P are o unică extindere la Ω.*

Demonstraţie. Unicitatea rezultă din corolarul 4.1.2. Să arătăm existenţa extinderii. Dacă P e arhimedian, atunci, ţinând cont de teorema lui Ostrowski, nu avem nimic de demonstrat. Presupunem, aşadar, că P e nearhimedian. Fie $\varphi \in P$ şi, pentru fiecare extindere finită E a lui F, inclusă în Ω, fie φ_E unica extindere a lui φ la E. E clar că, dacă E şi E' sunt extinderi finite ale lui F incluse în Ω, atunci $\varphi_E|_{E\cap E'} = \varphi_{E'}|_{E\cap E'} = \varphi_{E\cap E'}$. Prin urmare, funcţia $\varphi_\Omega : \Omega \to \mathbb{R}$, definită prin $\varphi_\Omega(\alpha) = \varphi_E(\alpha)$, unde $E \subseteq \Omega$ e o extindere finită a lui F care conţine pe α, e bine definită. O verificare de rutină arată că φ_Ω e o valuare pe Ω care extinde pe φ, deci P admite o extindere la Ω. □

4.3 Extinderea divizorilor primi discreţi. Corpuri locale.

În această secţiune, ne întoarcem la studiul extinderilor de corpuri cu divizori primi discreţi pentru a stabili o relaţie fundamentală între gradul extinderii, indicele de ramificare şi gradul rezidual.

Propoziţie 4.3.1. *Fie (E, Q) o extindere a lui (F, P) astfel încât Q şi P sunt discrete, F e complet în raport cu P şi $f(Q/P) < \infty$. Dacă $e = e(Q/P)$, $f = f(Q/P)$, π_Q e un element prim al lui Q şi $\{\omega_1, \ldots, \omega_f\}$ e o ridicare la $\mathcal{O}_Q$ a unei $\mathcal{F}_P$-baze a lui $\mathcal{E}_Q$, atunci*

$$\{\omega_i \pi_Q^j \,:\, i = 1, \ldots, f,\ j = 0, \ldots, e-1\}$$

e o $\mathcal{O}_P$-bază a lui $\mathcal{O}_Q$. În particular, E e o extindere finită a lui F, de grad

$$[E : F] = ef$$

Demonstraţie. Conform propoziţiei 2.4.3, $B = \{\omega_i \pi_Q^j \,:\, i = 1, \ldots, f,\ j = 0, \ldots, e-1\}$ e un sistem liniar independent peste F. Să arătăm că $\mathcal{O}_Q = \sum_{i,j} \mathcal{O}_P \omega_i \pi_Q^j$.

Deoarece $\{\overline{\omega_1}, \ldots, \overline{\omega_f}\}$ e o $\mathcal{F}_P$-bază a lui $\mathcal{E}_Q$, avem că $\mathcal{O}_Q = \mathcal{O}_P\omega_1 + \cdots + \mathcal{O}_P\omega_f + \pi_Q\mathcal{O}_Q$. Fie $N = \mathcal{O}_P\omega_1 + \cdots + \mathcal{O}_P\omega_f$. Atunci

$$\begin{aligned}
\mathcal{O}_Q &= N + \pi_Q\mathcal{O}_Q \\
&= N + \pi_Q N + \pi_Q^2\mathcal{O}_Q \\
&\ \ \vdots \\
&= N + \pi_Q N + \cdots + \pi_Q^{e-1}N + \pi_Q^e\mathcal{O}_Q \\
&= M + \pi_Q^e\mathcal{O}_Q
\end{aligned}$$

unde $M = N + \pi_Q N + \cdots + \pi_Q^{e-1} N = \sum_{i,j} \mathcal{O}_P \omega_i \pi_Q^j$. Fie π_P un element prim al lui P. Ţinând cont de definiţia indicelui de ramificare, avem $\pi_P \mathcal{O}_Q = \pi_Q^e \mathcal{O}_Q$. Aşadar,

$$\begin{aligned}\mathcal{O}_Q &= M + \pi_P \mathcal{O}_Q \\ &= M + \pi_P M + \pi_P^2 \mathcal{O}_Q \\ &\vdots \\ &= M + \pi_P M + \cdots + \pi_P^{n-1} M + \pi_P^n \mathcal{O}_Q\end{aligned}$$

pentru orice $n \geq 1$.

Fie acum $\alpha \in \mathcal{O}_Q$ şi $x_k = \sum_{i,j} a_{ijk} \omega_i \pi_Q^j \in M$, $k = 0, 1, \ldots$, astfel încât

$$\alpha - (x_0 + \pi_P x_1 + \cdots + \pi_P^{n-1} x_{n-1}) \in \pi_P^n \mathcal{O}_Q$$

pentru orice $n \geq 1$. Atunci

$$\alpha = \lim_{n\to\infty} \sum_{k=0}^{n-1} x_k \pi_P^k = \lim_{n\to\infty} \sum_{i,j} \Big(\sum_{k=0}^{n-1} a_{ijk} \pi_P^k \Big) \omega_i \pi_Q^j$$

Luând în considerare propoziţia 3.2.2, seria $\sum_k a_{ijk} \pi_P^k$ converge la un element $a_{ij} \in \mathcal{O}_P$. Prin urmare, $\alpha = \sum_{i,j} \alpha_{ij} \omega_i \pi_Q^j$ şi afirmaţia că B e $\mathcal{O}_P$-bază pentru $\mathcal{O}_Q$ e demonstrată.

Nu e greu de văzut acum că B e, de fapt, F-bază a lui E. Într-adevăr, dacă $\alpha \in E$, atunci, considerând un număr întreg r astfel încât $\pi_Q^{er} \alpha \in \mathcal{O}_Q$, găsim că $\alpha \in \pi_P^{-r} \mathcal{O}_Q$, deci α se poate scrie ca o combinaţie liniară de $\omega_i \pi_Q^j$ cu coeficienţi în F. Cum, pe de altă parte, $\omega_i \pi_Q^j$ sunt liniar independente peste F, propoziţia e complet demonstrată. □

Ţinând cont de propoziţia 2.4.3, de teorema 4.2.1 şi de propoziţia 4.3.1, avem următorul rezultat fundamental.

Teoremă 4.3.1. *Fie F un corp complet în raport cu divizorul prim discret P. Fie E e o extindere finită a lui F şi Q unica extindere a lui P la E. Atunci*

$$[E : F] = e(Q/P)\, f(Q/P)$$

Corolar 4.3.1. *In ipotezele teoremei* 4.3.1*, avem*

$$v_Q(\alpha) = \frac{1}{f(Q/P)} v_P\big(N_{E/F}(\alpha)\big)$$

pentru orice $\alpha \in E$*.*

Demonstraţie. Fie $\varphi' = e^{-v_Q}$ si φ restrictia lui φ' la F. Conform teoremei 4.2.1, avem $\varphi'(\alpha) = \Big(\varphi\big(\mathrm{N}_{E/F}(\alpha)\big)\Big)^{1/[E:F]}$, pentru orice $\alpha \in E$. Asadar, $v_Q(\alpha) = \frac{1}{[E:F]} v\big(\mathrm{N}_{E/F}(\alpha)\big)$, unde $v = -\log\varphi$ e restrictia lui v_Q la F. Dar $v_Q|_F = e(Q/P)v_P$, deci

$$v_Q(\alpha) = \frac{e(Q/P)}{e(Q/P)f(Q/P)} v_p\big(\mathrm{N}_{E/F}(\alpha)\big) = \frac{1}{f(Q/P)} v_P\big(\mathrm{N}_{E/F}(\alpha)\big)$$

pentru orice $\alpha \in E$. □

Cu ajutorul propoziţiei 4.3.1, putem clasifica corpurile complete în raport cu divizori primi discreţi, având corpurile reziduale finite. Astfel de corpuri se numesc ***corpuri locale***.

Teoremă 4.3.2. *Corpurile locale sunt exact extinderile finite ale lui* $\mathbb{Q}_p$ *şi* $\mathbb{F}_p((X))$*, cu* p *parcurgând mulţimea numerelor prime.*

Demonstraţie. Fie p un număr prim. Dacă F e o extindere a lui $\mathbb{Q}_p$ sau $\mathbb{F}_p((X))$, atunci, ţinând cont de teorema 4.1.1, divizorul prim al lui $\mathbb{Q}_p$ sau $\mathbb{F}_p((X))$ se extinde în mod unic la un divizor prim discret al lui F şi, în raport cu acesta, F e complet. Mai mult, conform propoziţiei 2.4.3, corpul rezidual al lui F în acest divizor prim e finit. Prin urmare, orice extindere finită a lui $\mathbb{Q}_p$ sau $\mathbb{F}_p((X))$ e un corp local.

Fie acum (F, P) un corp local şi p caracteristica corpului rezidual al lui F în P. Dacă corpul prim al lui F e $\mathbb{Q}$, atunci restricţia lui P la $\mathbb{Q}$ e p. Mai mult, ţinând cont de propoziţia 3.1.2, închiderea lui $\mathbb{Q}$ în F e un completat al lui $(\mathbb{Q}, p)$. Aşadar, (F, P) e o extindere a lui $(\mathbb{Q}_p, p)$. Considerând propoziţia 4.3.1, $F/\mathbb{Q}_p$ e finită. Dacă, pe de altă parte, corpul prim al lui F e finit, atunci el e izomorf cu corpul prim al lui $\mathcal{F}_P$, i.e. e corpul cu p elemente. Fie t un element prim al lui F în P. E uşor de văzut că t e transcendent peste $\mathbb{F}_p$ şi că restricţia lui P la $\mathbb{F}_p(t)$ e divizorul prim t asociat elementului prim $t \in \mathbb{F}_p[t]$. Deoarece închiderea lui $\mathbb{F}_p(t)$ în F e un completat al lui $(\mathbb{F}_p(t), t)$, avem că (F, P) e o extindere a lui $\big(\mathbb{F}_p((t)), t\big)$. Ţinând cont de propoziţia 4.3.1, $F/\mathbb{F}_p((t))$ e finită. □

Capitolul 5

Extinderi - cazul general

5.1 Existenţa şi numărul extinderilor

Fie E/F o extindere finită de corpuri şi P un divizor prim al lui E. Am văzut în secţiunea precedentă că, dacă F e complet în raport cu P, atunci există o unică extindere a lui P la E. Ce se poate spune dacă renunţăm la condiţia de completitudine? Folosinde-ne de rezultatul obţinut în cazul corpului de bază complet putem da rapid un răspuns la problema existenţei extinderilor. În condiţii puţin mai generale avem următoarea

Propoziţie 5.1.1. *Fie (F, P) un corp cu un divizor prim, $(\widetilde{F}, \widetilde{P})$ un completat al lui (F, P), Ω o închidere algebrică a lui $\widetilde{F}$ şi R extinderea lui $\widetilde{P}$ la Ω. Dacă E e o extindere algebrică a lui F şi $\mu : E \to \Omega$ e un F-morfism, atunci $Q_\mu = \mu^*(R)$ e o extindere a lui P la E. Mai mult, orice extindere a lui P la E se obţine în felul acesta.*

Demonstraţie. E clar că $Q_\mu = \mu^*(R)$ e un divizor prim al lui E ce stă deasupra lui P, întrucât

$$i^*_{F\to E}(Q_\mu) = i^*_{F\to E}\mu^*(R) = (\mu\, i_{F\to E})^*(R) = i^*_{F\to\Omega}(R) = P$$

Fie acum Q o extindere a lui P la E şi să arătăm că există un F-morfism $\mu : E \to \Omega$ astfel încât $Q = \mu^*(R)$. Fie $(\widetilde{E}, \widetilde{Q})$ un completat al lui (E, Q) şi fie $\overline{F}$ închiderea lui F în $\widetilde{E}$. Dacă $\overline{P}$ e restricţia lui $\widetilde{Q}$ la $\overline{F}$, atunci, ţinând seama de propozitia 3.1.2, $(\overline{F}, \overline{P}, i_{F\to\overline{F}})$ e un completat al lui (F, P). Conform propoziţiei 3.1.1, există un F-morfism $\rho : \overline{F} \to \widetilde{F}$ astfel încât $\rho^*(\widetilde{P}) = \overline{P}$.

Întrucât E/F e algebrică, la fel este şi $E\overline{F}/\overline{F}$. Cum Ω e algebric închis, există $\tau : E\overline{F} \to \Omega$ astfel încât $\tau\, i_{\overline{F}\to E\overline{F}} = i_{\widetilde{F}\to\Omega}\rho$. Pretindem că $\mu =$

$\tau\, i_{E\to E\overline{F}} : E \to \Omega$ e un F-morfism cu proprietatea că $\mu^*(R) = Q$. Într-adevăr, e de ajuns să vedem că $\tau^*(R) = i^*_{E\overline{F}\to\widetilde{E}}(\widetilde{Q})$, căci vom avea atunci

$$\mu^*(R) = i^*_{E\to E\overline{F}}\tau^*(R) = i^*_{E\to E\overline{F}} i^*_{E\overline{F}\to\widetilde{E}}(\widetilde{Q}) = i^*_{E\to\overline{E}}(\widetilde{Q}) = Q$$

Observăm că $\tau^*(R)$ e un divizor prim al lui $E\overline{F}$ cu proprietatea

$$\begin{aligned} i^*_{\overline{F}\to E\overline{F}}\big(\tau^*(R)\big) &= (\tau\, i_{\overline{F}\to E\overline{F}})^*(R) \\ &= (i_{\widetilde{F}\to\Omega}\,\rho)^*(R) \\ &= \rho^*\, i^*_{\widetilde{F}\to\Omega}(R) \\ &= \rho^*(\widetilde{P}) \\ &= \overline{P} \end{aligned}$$

Pe de altă parte, $\overline{P}$ admite o unică extindere la $E\overline{F}$, iar aceasta este $i^*_{E\overline{F}\to\widetilde{E}}(\widetilde{Q})$. Aşadar, $\tau^*(R) = i^*_{E\overline{F}\to\widetilde{E}}(\widetilde{Q})$ şi demonstraţia e terminată. □

Corolar 5.1.1. *Dacă E e o extindere algebrică a lui F şi P e un divizor prim al lui F, atunci există o extindere a lui P la E.*

Având un răspuns afirmativ la întrebarea privind existenţa extinderilor, ne punem, în mod firesc, problema de a determina numărul extinderilor unui divizor prim. Pentru a rezolva această problemă vom fixa următorul cadru de lucru şi vom da următoarele definiţii.

Fie F un corp, E o extindere finită a lui F, $\widetilde{F}$ o extindere arbitrară a lui F astfel încât $E \cap \widetilde{F} = f$ şi Ω o închidere algebrică a lui $\widetilde{F}$. Mulţimea F-morfismelor $E \to \Omega$ o notăm cu $\Gamma(F, E \to \Omega)$, iar elementele ei le numim ***aplicaţii de compoziţie*** pentru $(E, F, \widetilde{F}, \Omega)$. Dacă μ e o aplicaţie de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$, atunci corpul $\widetilde{F}\mu(E)$ se numeşte ***extinderea compozită*** asociată lui μ. Spunem că două aplicaţii de compoziţie, μ_1 şi μ_2, sunt ***echivalente***, şi scriem asta $\mu_1 \sim \mu_2$, dacă există $\sigma \in \mathrm{Gal}(\Omega/\widetilde{F})$ astfel încât $\mu_2 = \sigma\,\mu_1$.

Lemă 5.1.1. *Fie E^S închiderea separabilă a lui F în E şi $\mu \in \Gamma(F, E \to \Omega)$ o aplicaţie de compoziţie. Atunci:*

(i) *Închiderea separabilă a lui $\widetilde{F}$ în $\widetilde{F}\mu(E)$ e $\widetilde{F}\mu(E^S)$.*

(ii) *Numărul $g_\mu = \dfrac{[E:F]_{\mathrm{ins}}}{[\widetilde{F}\mu(E):\widetilde{F}]_{\mathrm{ins}}}$ e 1 sau o putere a unui număr prim.*

Demonstraţie. (i) Închiderea separabilă a lui F în $\mu(E)$ e $\mu(E^S)$, prin urmare, închiderea separabilă a lui $\widetilde{F}$ în $\widetilde{F}\mu(E)$ e $\widetilde{F}\mu(E^S)$.

(ii) Dacă $E^S = E$, atunci $[E : F]_{\text{ins}} = [\widetilde{F}\mu(E) : \widetilde{F}]_{\text{ins}} = 1$. Dacă $E^S \neq E$ şi caracteristica lui F e $p > 0$, atunci, ţinând cont că $[E : F]_{\text{ins}}$ şi $[\widetilde{F}\mu(E) : \widetilde{F}]_{\text{ins}}$ sunt puteri ale lui p şi

$$[\widetilde{F}\mu(E) : \widetilde{F}]_{\text{ins}} = [\widetilde{F}\mu(E) : \widetilde{F}\mu(E^S)] \leq [\mu(E) : \mu(E^S)] = [E : E^S] = [E : F]_{\text{ins}}$$

ajungem la concluzia dorită. □

Lemă 5.1.2. *Fie $\mu_1, \ldots, \mu_r$ un sistem complet de reprezentanţi pentru clasele de echivalenţă de aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$. Dacă $G = \text{Gal}(\Omega/\widetilde{F})$ şi $G_i = \text{Gal}(\Omega/\widetilde{F}\mu_i(E))$, pentru $i = 1, \ldots, r$, atunci mulţimea $\Gamma(\widetilde{F}, \widetilde{F}\mu_i(E) \to \Omega)$ are $m_i = [G : G_i]$ elemente. În plus, dacă $\sigma_{i,1}, \ldots, \sigma_{i,m_i}$ e un sistem complet de reprezentanţi pentru relaţia de congruenţă la stânga modulo G_i, atunci*

$$\Gamma(F, E \to \Omega) = \{\sigma_{i,j}\,\mu_i \,:\, i = 1, \ldots, r,\ j = 1, \ldots, m_i\}$$

Demonstraţie. Prima afirmaţie rezultă în urma faptului uşor de verificat că

$$\big(G/G_i\big)_s \ni \sigma G_i \to \sigma|_{\widetilde{F}\mu_i(E)} \in \Gamma(\widetilde{F}, \widetilde{F}\mu_i(E) \to \Omega)$$

e o bijecţie de mulţimi.

Pentru cea de-a doua afirmaţie, dacă $\mu \in \Gamma(F, E \to \Omega)$, atunci există $i \in \{1, \ldots, r\}$ şi $\sigma \in G$ astfel încât $\mu = \sigma\,\mu_i$. Considerând $j \in \{1, \ldots, m_i\}$ şi $\tau \in G_i$ astfel încât $\sigma = \sigma_{i,j}\tau$, avem $\mu = \sigma_{i,j}\,\tau\,\mu_i = \sigma_{i,j}\mu_i$. În fine, aplicaţiile $\sigma_{i,j}\,\mu_i$ sunt distincte două câte două, întrucât, dacă $\sigma_{i,j}\,\mu_i = \sigma_{k,l}\,\mu_k$, atunci $\mu_i = \sigma_{i,j}^{-1}\,\sigma_{k,l}\,\mu_k$, deci $\mu_i \sim \mu_k$. Aşadar, $i = k$ şi $\sigma_{i,j}\,\mu_i = \sigma_{i,l}\,\mu_i$. Cum $\sigma_{i,j}$ şi $\sigma_{i,l}$ coincid pe $\widetilde{F}\mu_i(E)$, avem $\sigma_{i,j}^{-1}\sigma_{i,l} \in G_i$, de unde rezultă $j = l$. □

Propoziţie 5.1.2. *Păstrând notaţiile din lema precedentă, fie $[E : F] = n$, $[\widetilde{F}\mu_i(E) : \widetilde{F}] = n_i$ şi $[E : F]_{\text{ins}}/[\widetilde{F}\mu_i(E) : \widetilde{F}]_{ins} = g_i$. Atunci, pentru orice*

$\alpha \in E$,

$$\begin{aligned} \mathrm{N}_{E/F}(\alpha) &= \prod_{i=1}^{r} \mathrm{N}_{\widetilde{F}\mu_i(E)/\widetilde{F}}\big(\mu_i(\alpha)\big)^{g_i} && (5.1)\\ \mathrm{Tr}_{E/F}(\alpha) &= \sum_{i=1}^{r} g_i \mathrm{Tr}_{\widetilde{F}\mu_i(E)/\widetilde{F}}\big(\mu_i(\alpha)\big) && (5.2)\\ P_{\alpha,E/F}(X) &= \prod_{i=1}^{r} P_{\mu_i(\alpha),\widetilde{F}\mu_i(E)/\widetilde{F}}(X)^{g_i} && (5.3)\\ n &= \sum_{i=1}^{r} g_i n_i && (5.4) \end{aligned}$$

Demonstraţie. Ne folosim de formulele pentru normă, urmă şi polinom caracteristic. Avem

$$\begin{aligned} P_{\alpha,E/F}(X) &= \prod_{\mu\in\Gamma(F,E\to\Omega)} \big(X-\mu(\alpha)\big)^{[E:F]_{\mathrm{ins}}}\\ &= \prod_{i,j} \big(X-\sigma_{i,j}\,\mu_i(\alpha)\big)^{[\widetilde{F}\mu_i(E):\widetilde{F}]_{\mathrm{ins}}\,g_i}\\ &= \prod_{i=1}^{r}\left[\prod_{j=1}^{m_i}\Big(X-\sigma_{i,j}\big(\mu_i(\alpha)\big)\Big)^{[\widetilde{F}\mu_i(E):\widetilde{F}]_{\mathrm{ins}}}\right]^{g_i}\\ &= \prod_{i=1}^{r} P_{\mu_i(\alpha),\widetilde{F}\mu_i(E)/\widetilde{F}}(X)^{g_i} \end{aligned}$$

şi, în mod similar, se obţin (5.1) şi (5.2). Formula (5.4) rezultă din (5.3) egalând gradele polinoamelor. □

Propoziţie 5.1.3. *Dacă $E = F(\alpha)$, atunci există o corespondenţă bijectivă între clasele de echivalenţă de aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$ şi factorii ireductibili ai lui $P_{\alpha,F}$ în $\widetilde{F}[X]$.*

Demonstraţie. Întrucât $E = F(\alpha)$, avem $P_{\alpha,E/F} = P_{\alpha,F}$. Mai mult, pentru $i = 1,\dots,r$, $\widetilde{F}\mu_i(E) = \widetilde{F}\big(\mu_i(\alpha)\big)$, deci $P_{\mu_i(\alpha),\widetilde{F}\mu_i(E)/\widetilde{F}} = P_{\mu_i(\alpha),\widetilde{F}}$. Ţinând cont de (5.3), descompunerea în factori ireductibili a lui $P_{\alpha,F}$ în $\widetilde{F}[X]$ este

$$P_{\alpha,F}(X) = \prod_{i=1}^{r} P_{\mu_i(\alpha),\widetilde{F}}(X)^{g_i}$$

Pentru a termina demonstraţia mai trebuie să arătăm că factorii ireductibili $P_{\mu_i(\alpha),\widetilde{F}}$ sunt distincţi. Dacă $P_{\mu_i(\alpha),\widetilde{F}} = P_{\mu_j(\alpha),\widetilde{F}}$, atunci $\mu_i(\alpha)$ şi $\mu_j(\alpha)$ sunt conjugate peste $\widetilde{F}$. Prin urmare, există un $\widetilde{F}$-izomorfism $\rho : \widetilde{F}\big(\mu_i(\alpha)\big) \to \widetilde{F}\big(\mu_j(\alpha)\big)$ astfel încât $\rho\big(\mu_i(\alpha)\big) = \mu_j(\alpha)$. Extinzând pe ρ la un morfism $\sigma : \Omega \to \Omega$, avem că $\sigma \in \mathrm{Gal}(\Omega/\widetilde{F})$ şi $\sigma\mu_i = \mu_j$. Rezultă că $\mu_i \sim \mu_j$, deci $i = j$. □

Teoremă 5.1.1. *Fie (F, P) un corp cu un divizor prim, $(\widetilde{F}, \widetilde{P})$ un completat al lui (F, P), Ω o închidere algebrică a lui $\widetilde{F}$ şi R extinderea lui $\widetilde{P}$ la Ω. Dacă E/F e o extindere finită de corpuri, atunci numărul extinderilor lui P la E e acelaşi cu numărul claselor de echivalenţa de aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$.*

De fapt, dacă $\mu_1, \ldots, \mu_r$ e un sistem complet de reprezentanţi pentru clasele de echivalenţă de aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$, atunci

$$Q_i = \mu_i^*(R),\ i = 1, \ldots, r$$

sunt toţi divizorii primi ai lui E care stau deasupra lui P.

Mai mult, dacă S_i e unica extindere a lui $\widetilde{P}$ la $\widetilde{E}_i = \widetilde{F}\mu_i(E)$, atunci $(\widetilde{E}_i, S_i, \mu_i)$ e un completat al lui (E, Q_i).

În fine, dacă $[E : F] = n$, $[\widetilde{E}_i : \widetilde{F}] = n_i$ şi $[E : F]_{\mathrm{ins}}/[\widetilde{E}_i : \widetilde{F}]_{\mathrm{ins}} = g_i$, atunci, pentru orice $\alpha \in E$, avem

$$\mathrm{N}_{E/F}(\alpha) = \prod_{i=1}^{r} \mathrm{N}_{\widetilde{E}_i/\widetilde{F}}\big(\mu_i(\alpha)\big)^{g_i} \tag{5.5}$$

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{i=1}^{r} g_i \mathrm{Tr}_{\widetilde{E}_i/\widetilde{F}}\big(\mu_i(\alpha)\big) \tag{5.6}$$

$$P_{\alpha,E/F}(X) = \prod_{i=1}^{r} P_{\mu_i(\alpha),\widetilde{E}_i/\widetilde{F}}(X)^{g_i} \tag{5.7}$$

$$n = \sum_{i=1}^{r} g_i n_i \tag{5.8}$$

Demonstraţie. Fără a restrânge generalitatea, putem presupune că $E \cap \widetilde{F} = F$. Fie $\mu \in \Gamma(F, E \to \Omega)$ o aplicaţie de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$. Conform propoziţiei 5.1.1, $Q_\mu = \mu^*(R)$ e o extindere a lui P la E. Să arătăm că, dacă $S_\mu = i^*_{\widetilde{F}\mu(E)\to\Omega}(R)$ e unica extindere a lui $\widetilde{P}$ la $\widetilde{F}\mu(E)$, atunci $(\widetilde{F}\mu(E), S_\mu, \mu)$ e un completat al lui (E, Q_μ).

În primul rând, deoarece $(\widetilde{F}\mu(E), S_\mu)$ e o extindere finită a corpului complet $(\widetilde{F}, \widetilde{P})$ rezultă, conform corolarului 4.1.1, că $\widetilde{F}\mu(E)$ e complet în raport cu S_μ. Fie $\overline{\mu(E)}$ închiderea lui $\mu(E)$ în $\widetilde{F}\mu(E)$. Atunci $\overline{\mu(E)}$ e un subcorp al lui $\widetilde{F}\mu(E)$ care conţine pe $\mu(E)$. Mai mult, $\widetilde{F} \subseteq \overline{\mu(E)}$, deoarece $F \subseteq \mu(E)$ şi închiderea lui F în $\widetilde{F}\mu(E)$ e $\widetilde{F}$. Aşadar, $\overline{\mu(E)} = \widetilde{F}\mu(E)$, ceea ce arată că $\mu(E)$ e dens în $\widetilde{F}\mu(E)$. În fine,

$$\mu^*(S_\mu) = \mu^*\, i^*_{\widetilde{F}\mu(E)\to\Omega}(R) = (i_{\widetilde{F}\mu(E)\to\Omega}\,\mu)^*(R) = \mu^*(R) = Q_\mu$$

deci, $(\widetilde{F}\mu(E), S_\mu, \mu)$ e, într-adevăr, un completat al lui (E, Q_μ).

Arătăm în continuare că, dacă μ_1 şi μ_2 sunt aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$, atunci $\mu_1 \sim \mu_2$ dacă şi numai dacă $Q_{\mu_1} = Q_{\mu_2}$. Împreună cu propoziţia 5.1.1 şi propoziţia 5.1.2, teorema va fi atunci demonstrată. Să presupunem întâi că $\mu_1 \sim \mu_2$. Există atunci $\sigma \in \mathrm{Gal}(\Omega/\widetilde{F})$ astfel încât $\mu_2 = \sigma\mu_1$. Ţinând cont că

$$i^*_{\widetilde{F}\to\Omega}\sigma^*(R) = (\sigma\, i^*_{\widetilde{F}\to\Omega}) = i^*_{\widetilde{F}\to\Omega}(R) = \widetilde{P}$$

şi R e unica extindere a lui $\widetilde{P}$ la Ω, avem $\sigma^*(R) = R$. Aşadar,

$$Q_{\mu_2} = \mu_2^*(R) = \mu_1^*\sigma^*(R) = \mu_1^*(R) = Q_{\mu_1}$$

Reciproc, dacă $Q_{\mu_1} = Q_{\mu_2}$, atunci $(\widetilde{F}\mu_1(E), S_{\mu_1}, \mu_1)$ şi $(\widetilde{F}\mu_2(E), S_{\mu_2}, \mu_2)$ sunt doi completaţi ai lui $(E, Q_{\mu_1} = Q_{\mu_2})$. Prin urmare, există un izomorfism de corpuri $\rho : \widetilde{F}\mu_1(E) \to \widetilde{F}\mu_2(E)$ astfel încât $S_{\mu_1} = \rho^*(S_{\mu_2})$ şi $\rho\,\mu_1 = \mu_2$. Cum ρ e un homeomorfism care acţionează identic pe F şi $\widetilde{F}$ e închiderea lui F în $\widetilde{F}\mu_1(E)$ şi în $\widetilde{F}\mu_2(E)$, avem că ρ acţionează identic pe $\widetilde{F}$. Extinzând pe ρ la un $\widetilde{F}$-morfism al lui Ω, găsim că $\mu_1 \sim \mu_2$. □

Pentru numerele g_i se mai foloseşte notaţia $g(Q_i/P)$. Gradul extinderii $\widetilde{E}_i/\widetilde{F}$ se mai numeşte ***gradul local*** al lui E/F în Q_i şi se mai notează cu $n(Q_i/P)$. În general, noţiunile şi obiectele legate de extinderea $\widetilde{E}_i/\widetilde{F}$ sunt însoţite de calificativul "locale", spre deosebire de noţiunile şi obiectele extinderii E/F care au calificativul de "globale". În termenii aceştia, atunci când $g_i = 1$, $i = 1, \ldots, r$, (cum e cazul când E/F e separabilă), formulele (5.5),(5.6), (5.7) şi (5.8) se exprimă, respectiv, în felul următor: norma globală e produsul normelor locale, urma globală e suma urmelor locale, polinomul caracteristic global e produsul polinoamelor caracteristice locale şi gradul global e suma gradelor locale. Renunţând la a face referire la μ_i,

formulele (5.5) - (5.8) se pot exprima succint în formele următoare:

$$\mathrm{N}_{E/F}(\alpha) = \prod_{Q|P} \mathrm{N}_{E_Q/F_P}(\alpha) \tag{5.9}$$

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{Q|P} \mathrm{Tr}_{E_Q/F_P}(\alpha) \tag{5.10}$$

$$P_{\alpha,E/F}(X) = \prod_{Q|P} P_{\alpha,E_Q/F_P}(X) \tag{5.11}$$

$$n = \sum_{Q|P} n(Q/P) \tag{5.12}$$

5.2 Consecinţe

Ne ocupăm în această secţiune de câteva aplicaţii ale rezultatelor din secţiunea precedentă. Vom descoperi, printre altele, câteva rezultate binecunoscute din teoria algebrică a numerelor. Începem cu un rezultat care aminteşte de teorema 3.3.2.

Propoziţie 5.2.1. *Fie P un divizor prim arhimedian al lui F, E o extindere finită, de grad n, a lui F şi $Q_1, \ldots, Q_r$ extinderile lui P la E.*

Dacă P e complex atunci $r = n$. Mai mult, fiecare Q_i e complex şi $n(Q_i/P) = 1$.

Dacă P e real atunci $r = r_1 + r_2$, unde r_1 e numărul extinderilor reale, iar r_2 e numărul extinderilor complexe. Ordonând Q_i astfel încât $Q_1, \ldots, Q_{r_1}$ sunt reale şi $Q_{r_1+1}, \ldots, Q_{r_1+r_2}$ sunt complexe, avem

$$n(Q_i/P) = \begin{cases} 1 & \text{pentru} \quad i = 1, \ldots, r_1 \\ 2 & \text{pentru} \quad i = r_1 + 1, \ldots, r_1 + r_2 \end{cases}$$

şi $r_1 + 2r_2 = n$.

Demonstraţie. Ne vom folosi de teorema 5.1.1. Observăm, înainte, că F are caracteristica 0, deci E/F e separabilă. În particular, $\Gamma(F, E \to \Omega)$ are $[E : F]$ elemente. Fără a restrânge generalitatea, presupunem că $\Omega = \mathbb{C}$.

Dacă P e complex, atunci $\Omega = \widetilde{F}$ şi $\mathrm{Gal}(\Omega/\widetilde{F}) = \{1\}$. Prin urmare, numărul claselor de echivalenţă de aplicaţii de compoziţie pentru $(E, F, \widetilde{F}, \Omega)$ coincide cu numărul elementelor mulţimii $\Gamma(F, E \to \Omega)$, deci, cu gradul extinderii E/F. Aşadar, $r = n$. Evident, fiecare extindere a lui P la E e complexă, de grad local egal cu 1.

Dacă P e real, atunci $\mathrm{Gal}(\Omega/\widetilde{F})$ e un grup ciclic de ordin 2 generat de morfismul de conjugare, σ. Aşadar, dacă $\mu_1,\ \mu_2 \in \Gamma(F, E \to \Omega)$, avem

$$\mu_1 \sim \mu_2 \Leftrightarrow \mu_1 = \mu_2 \,\mathrm{sau}\, \sigma\mu_1 = \mu_2 \Leftrightarrow \mu_1 = \mu_2 \,\mathrm{sau}\, \overline{\mu}_1 = \mu_2$$

Alegând reprezentanţii $\mu_1, \ldots, \mu_{r_1+r_2}$ pentru clasele de echivalenţă de aplicaţii de compoziţie pentru $\Gamma(F, E \to \Omega)$ astfel încât $\mu_1, \ldots, \mu_{r_1}$ reprezintă clase cu un singur element şi $\mu_{r_1+1}, \ldots, \mu_{r_1+r_2}$ reprezintă clase cu două elemente, găsim că $Q_i = \mu_i^*(P_\infty)$ sunt reali pentru $i = 1, \ldots, r_1$ şi complecşi pentru $i = r_1 + 1, \ldots, r_1 + r_2$. Pentru ultima afirmaţie ne folosim de formula (5.12). □

Propoziţie 5.2.2. *Fie P un divizor prim nearhimedian al lui F şi E/F o extindere finită de corpuri de grad n. Dacă Q e o extindere a lui P la E şi $\widetilde{P}$, respectiv $\widetilde{Q}$, sunt divizorii primi ai lui F_P, respectiv E_Q, atunci*

$$e(\widetilde{Q}/\widetilde{P}) = e(Q/P) \ \ si \ \ f(\widetilde{Q}/\widetilde{P}) = f(Q/P)$$

Aşadar,

$$\sum_{Q|P} g(Q/P)\, e(Q/P)\, f(Q/P) \leq \sum_{Q|P} g(Q/P)\, n(Q/P) = n$$

Demonstraţie. Luând în considerare propoziţia 2.4.1 si propoziţia 3.2.1, avem

$$e(\widetilde{Q}/\widetilde{P}) = e(\widetilde{Q}/\widetilde{P})\, e(\widetilde{P}/P) = e(\widetilde{Q}/P) = e(\widetilde{Q}/Q)\, e(Q/P) = e(Q/P)$$

şi, în mod similar, $f(\widetilde{Q}/\widetilde{P}) = f(Q/P)$. Ultima afirmaţie rezultă uşor dacă ţinem cont de propoziţia 2.4.3 şi de relaţia

$$e(Q/P) f(Q/P) = e(\widetilde{Q}/\widetilde{P}) f(\widetilde{Q}/\widetilde{P}) \leq [E_Q : F_P] = n(Q/P)$$

□

Propoziţie 5.2.3. *Fie P un divizor prim discret al lui F şi E/F o extindere de corpuri de grad n. Atunci*

(i) *Orice extindere a lui P la E e discretă*

(ii) $n = \sum_{Q|P} g(Q/P)\, e(Q/P)\, f(Q/P)$

Mai mult, există următoarele relaţii între valuările exponenţiale normalizate:

(iii) $v_Q(a) = e(Q/P)v_P(a)$, *pentru orice* $a \in F$

(iv) $v_P\big(N_{E/F}(\alpha)\big) = \sum_{Q|P} g(Q/P)\, f(Q/P)\, v_Q(\alpha)$, *pentru orice* $\alpha \in E$

Demonstraţie. (i) Fie Q o extindere a lui P la E şi $\widetilde{P}$, respectiv $\widetilde{Q}$, divizorii primi ai lui F_P, respectiv E_Q. Deoarece P e discret avem că $\widetilde{P}$ e discret. Cum $(E_Q, \widetilde{Q})$ e o extindere finită a lui $(F_P, \widetilde{P})$ şi F_P e complet în raport cu $\widetilde{P}$, rezultă, conform teoremei 4.2.1, că $\widetilde{Q}$ e discret. Aşadar, Q e discret.
(ii) Ţinând cont de teorema 4.3.1, de propoziţia 5.2.2 şi de (5.8), avem

$$\begin{aligned} n &= \sum_{Q|P} g(Q/P)\, n(Q/P) \\ &= \sum_{Q|P} g(Q/P)\, e(\widetilde{Q}/\widetilde{P})\, f(\widetilde{Q}/\widetilde{P}) \\ &= \sum_{Q|P} g(Q/P)\, e(Q/P)\, f(Q/P) \end{aligned}$$

(iii) $v_Q(a) = v_{\widetilde{Q}}(a) = e(\widetilde{Q}/\widetilde{P})\, v_{\widetilde{P}}(a) = e(Q/P)\, v_P(a)$.
(iv) Identificând în (5.5) pe $\mu_i(\alpha)$ cu α şi ţinând cont de corolarul 4.3.1, avem

$$\begin{aligned} v_P\big(\mathrm{N}_{E/F}(\alpha)\big) &= v_{\widetilde{P}}\big(\mathrm{N}_{E/F}(\alpha)\big) \\ &= v_{\widetilde{P}}\left(\prod_{Q|P} \mathrm{N}_{E_Q/F_P}(\alpha)^{g(Q/P)}\right) \\ &= \sum_{Q|P} g(Q/P)\, v_{\widetilde{P}}\big(\mathrm{N}_{E_Q/F_P}(\alpha)\big) \\ &= \sum_{Q|P} g(Q/P)\, f(\widetilde{Q}/\widetilde{P})\, v_{\widetilde{Q}}(\alpha) \\ &= \sum_{Q|P} g(Q/P)\, f(Q/P)\, v_Q(\alpha) \end{aligned}$$

□

Corolar 5.2.1. *Dacă* P *e un divizor prim discret al lui* F *şi* E *e o extindere finită şi separabilă a lui* F *atunci are loc* ***identitatea fundamentală a***

teoriei valuărilor

$$[E:F] = \sum_{Q|P} e(Q/P) f(Q/P) \tag{5.13}$$

Dacă E/F e o extindere de corpuri de numere algebrice, atunci (5.13) nu e altceva decât identitatea fundamentală clasică. Într-adevăr, ţinând cont de propoziţia 2.4.2, avem următorul

Corolar 5.2.2. *Fie E/F o extindere de corpuri de numere algebrice, $\mathfrak{p}$ un ideal prim nenul al lui $\mathcal{O}_F$ şi $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, descompunerea în produs de ideale prime nenule distincte a lui $\mathfrak{p}\mathcal{O}_E$. Dacă $f_i = [\mathcal{O}_E/\mathfrak{P}_i : \mathcal{O}_F/\mathfrak{p}]$, atunci:*

(i) $[E:F] = \sum_{i=1}^{r} e_i f_i$

(ii) $v_{\mathfrak{P}_i}(a) = e_i\, v_{\mathfrak{p}}(a)$, *pentru orice* $a \in F$

(iii) $v_{\mathfrak{p}}\big(\mathrm{N}_{E/F}(\alpha)\big) = \sum_{i=1}^{r} f_i\, v_{\mathfrak{P}_i}(\alpha)$, *pentru orice* $\alpha \in E$

Observăm că egalitatea de la punctul (iii) al precedentului corolar nu este altceva decât afirmaţia că $\mathrm{N}_{E/F}(\alpha\mathcal{O}_E) = \mathrm{N}_{E/F}(\alpha)\mathcal{O}_F$. Pentru aceasta, reamintim că norma unui ideal fracţionar nenul, $J = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}}(J)}$, al lui $\mathcal{O}_E$ este

$$\mathrm{N}_{E/F}(J) = \prod_{\mathfrak{P}} \left(\mathfrak{P} \cap \mathcal{O}_F\right)^{f_{\mathfrak{P}}\, \mathrm{ord}_{\mathfrak{P}}(J)}$$

unde $f_{\mathfrak{P}} = [\mathcal{O}_E/\mathfrak{P} : \mathcal{O}_F/(\mathfrak{P} \cap \mathcal{O}_F)]$. Aşadar, din punctul (iii) al corolarului 5.2.2, deducem că

$$\begin{aligned}
\mathrm{N}_{E/F}(\alpha)\mathcal{O}_F &= \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}\left(\mathrm{N}_{E/F}(\alpha)\right)} \\
&= \prod_{\mathfrak{p}} \prod_{\mathfrak{P}|\mathfrak{p}} \left(\mathfrak{P} \cap \mathcal{O}_F\right)^{f_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha)} \\
&= \prod_{\mathfrak{P}} \left(\mathfrak{P} \cap \mathcal{O}_F\right)^{f_{\mathfrak{P}}\, \mathrm{ord}_{\mathfrak{P}}(\alpha\mathcal{O}_E)} \\
&= \mathrm{N}_{E/F}(\alpha\mathcal{O}_E)
\end{aligned}$$

Bibliografie

[1] T. Albu, I.D. Ion, *Capitole de teoria algebrică a numerelor*, Universitatea din Bucureşti, 1979

[2] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, Science Publishers, Inc., 1967.

[3] N. Childress, *Class Field Theory*, Springer - Universitext, 2009.

[4] L.J. Goldstein, *Analytic Number Theory*, Prentice-Hall, Inc., 1971.

[5] G.J. Janusz, *Algebraic Number Fields*, Academic Press, Inc., 1973.

[6] J. Neukirch, *Algebraic Number Theory*, Springer - Grundlehren der mathematischen Wissenschaften 322, 1999.

[7] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Book Company, Inc., 1963.