ASUPRA UNOR EXTINDERI PĂTRATICE

MARCEL ŢENA[1)]

Abstract. The article analises the set of the fixed points of an involutive automorphism of a commutative field.

Keywords: field, automorphism.
MSC : 13B02

Considerăm un corp comutativ K şi un automorfism $i : K \to K$, diferit de automorfismul identic 1_K, dar care este involutiv, adică $i \circ i = 1_K$.

Notăm cu F mulţimea formată din punctele fixe ale automorfismului i adică $F = \{x \in K \mid i(x) = x\}$. Cu aceste ipoteze şi notaţii, avem următoarea:

Teoremă. a) *F este un subcorp al lui K şi $[K : F] = 2$, unde $[K : F]$ este gradul extinderii $F \subset K$ (dimensiunea spaţiului liniar K peste corpul F).*

b) *i este o aplicaţie F– liniară, având ca matrice asociată într-o anumită bază*:

$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *când corpul K are caracteristica diferită de* 2, *respectiv*

$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *când corpul K are caracteristica* 2.

Demonstraţie. Începem cu următoarea:

Lemă. *Există un element $x_0 \in K$ cu $x_0 + i(x_0) \neq 0$.*

Demonstraţia lemei. Presupunem prin absurd că pentru orice $x \in K$ avem $x + i(x) = 0$, deci $i(x) = -x$, $\forall\, x \in K$. Când $\mathrm{Char}(K) \neq 2$, avem $i(1) = -1$ şi cum $i(1) = 1$, rezultă $1 = -1$, absurd. Când $\mathrm{Char}(K) = 2$, egalitatea $i(x) = -x$ devine $i(x) = x$, $\forall\, x \in K$, adică $i = 1_K$, absurd.

Demonstraţia propriu-zisă a teoremei. a) Faptul că F este subcorp al lui K este o simplă verificare. Deoarece $i \neq 1_K$, există $\alpha \in K$ cu $i(\alpha) \neq \alpha$, deci $\alpha \in K \setminus F$. Atunci mulţimea $\{1, \alpha\}$ este liniar independentă peste F (căci o relaţie de liniar dependenţă ar duce la $\alpha \in F$). Deoarece dimensiunea unui spaţiu vectorial reprezintă numărul maxim de vectori liniari independenţi rezultă $[K : F] \geq 2$.

Pentru a dovedi inegalitatea contrară $[K : F] \leq 2$, este suficient să arătăm că orice mulţime cu 3 elemente din K este liniar dependentă peste F. Fie $\{\alpha, \beta, \gamma\} \subseteq K$. Considerăm sistemul liniar omogen peste K cu necunoscutele $x, y, z \in K$:

$$\begin{cases} \alpha x \quad +\beta y \quad +\gamma z = 0 \\ i(\alpha)x + i(\beta)y + i(\gamma)z = 0. \end{cases}$$

Deoarece necunoscutele sunt mai multe decât ecuaţiile, sistemul are cel puţin o soluţie nenulă $(x_1, y_1, z_1) \in K^3$; să zicem că $x_1 \neq 0$. Conform lemei există $x_0 \in K$ cu $x_0 + i(x_0) \neq 0$. Pentru orice $\lambda \in K$, $(\lambda x_1, \lambda y_1, \lambda z_1)$

[1)]Profesor dr., Colegiul Naţional „Sf. Sava“, Bucureşti.

rămâne soluţie a sistemului şi luând $\lambda = \dfrac{x_0}{x_1}$ obţinem soluţia (x_2, y_2, z_2), unde $x_2 = \lambda x_1 = x_0$, $y_2 = \lambda y_1$, $z_2 = \lambda z_1$. Scriind că $(x_2 = x_0, y_2, z_2)$ verifică sistemul, avem:

$$\begin{cases} \alpha x_0 \quad +\beta y_2 \quad +\gamma z_2 = 0 & (1) \\ i(\alpha)x_0 + i(\beta)y_2 + i(\gamma)z_2 = 0. & (2) \end{cases}$$

Aplicând automorfismul i în (2) obţinem:

$$i(x_0)\alpha + i(y_2)\beta + i(z_2)\gamma = 0. \tag{3}$$

Adunând (1) cu (3) rezultă:

$$[x_0 + i(x_0)]\,\alpha + [y_2 + i(y_2)]\,\beta + [z_2 + i(z_2)]\,\gamma = 0. \tag{4}$$

Dar $x_0 + i(x_0), y_2 + i(y_2), z_2 + i(z_2) \in F$ şi cum $x_0 + i(x_0) \neq 0$, egalitatea (4) arată liniar dependenţa mulţimii $\{\alpha, \beta, \gamma\}$ peste F.

Observaţie. Deoarece $[K : F] = 2$, rezultă că pentru orice $\alpha \in K \setminus F$ mulţimea $B = \{1, \alpha\}$ este o bază a lui K peste F (deoarece este liniar independentă şi are cardinalul unei baze).

b) Faptul că i este aplicaţie $F-$liniară rezultă imediat din aceea că i este morfism de corpuri.

Cazul I. $\mathrm{Char}(K) \neq 2$. Considerăm un element $\alpha \in K \setminus F$ şi formăm elementele $s = \alpha + i(\alpha) \in F$, $p = \alpha i(\alpha) \in F$, $d = \alpha - i(\alpha) \in K \setminus F$ (aceste apartenenţe sunt imediate, căci $i(s) = s$, $i(p) = p$, iar dacă am presupune $i(d) = d$, ar rezulta $-d = d$ şi cum $1 + 1 \neq 0$, ar însemna că $d = 0$, adică $i(\alpha) = \alpha$, prin urmare $\alpha \in F$, absurd). Conform observaţiei, mulţimea $B = \{1, d\}$ este o bază a lui K peste F. Dar $d^2 = s^2 - 4p \in F$, deci $i(d^2) = d^2$, adică $(i(d))^2 = d^2$ şi cum $i(d) \neq d$ (deoarece $d \notin F$), rezultă $i(d) = -d$. Aşadar:

$$\begin{cases} i(1) = 1 \cdot 1 + 0 \cdot d \\ i(d) = 0 \cdot 1 + (-1) \cdot d \end{cases}$$

ceea ce arată că matricea asociată aplicaţiei F-liniare i în baza $\{1, d\}$ este

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Cazul II. $\mathrm{Char}(K) = 2$. Conform lemei putem alege $\alpha \in K$ astfel încât $s = \alpha + i(\alpha) \neq 0$ şi atunci $\alpha \notin F$ (căci $\alpha \in F$ duce la $i(\alpha) = \alpha$, adică $\alpha + i(\alpha) = 0$, absurd). Egalitatea $s = \alpha + i(\alpha)$ înmulţită cu $\dfrac{1}{s}$ devine $1 = \dfrac{\alpha}{s} + \dfrac{i(\alpha)}{s}$ şi cum $s \in F$, putem scrie mai departe:

$$1 = \frac{\alpha}{s} + i\left(\frac{\alpha}{s}\right) \quad \text{sau} \quad i\left(\frac{\alpha}{s}\right) = 1 + \frac{\alpha}{s}.$$

Cum $\frac{\alpha}{s} \in K \setminus F$, conform observaţiei rezultă că mulţimea $B = \left\{1, \frac{\alpha}{s}\right\}$ este o bază a lui K peste F. Aşadar:

$$\begin{cases} i(1) = 1 \cdot 1 + 0 \cdot \frac{\alpha}{s} \\ i\left(\frac{\alpha}{s}\right) = 1 \cdot 1 + 1 \cdot \frac{\alpha}{s} \end{cases}$$

ceea ce arată că matricea asociată aplicaţiei F-liniare i în baza $\left\{1, \frac{\alpha}{s}\right\}$ este

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Teorema este complet demonstrată.

Comentarii. 1. Ilustrăm teorema precedentă prin patru exemple, primele două pentru corpuri de caracteristică 0, al treilea pentru un corp de caracteristică $p \neq 2$ şi al patrulea pentru un corp de caracteristică 2.

• Luând $K = \mathbb{C}$, $i : \mathbb{C} \to \mathbb{C}$, $i(z) = \overline{z}$ (conjugarea complexă), avem $F = \mathbb{R}$ şi $[\mathbb{C} : \mathbb{R}] = 2$; o bază a lui $\mathbb{C}$ peste $\mathbb{R}$ este $B = \{1, \mathrm{i}\}$, i fiind unitatea imaginară şi cum $i(1) = 1$, $i(\mathrm{i}) = -\mathrm{i}$, rezultă că matricea asociată aplicaţiei liniare i este

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

• Luând $K = \mathbb{Q}\left(\sqrt{d}\right)$ un corp pătratic, unde $d \in \mathbb{Z} \setminus \{1\}$ este un întreg liber de pătrate, $i : \mathbb{Q}\left(\sqrt{d}\right) \to \mathbb{Q}\left(\sqrt{d}\right)$, $i\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$, $\forall\, a, b \in \mathbb{Q}$ (conjugarea pătratică), avem $F = \mathbb{Q}$ şi $\left[\mathbb{Q}\left(\sqrt{d}\right) : \mathbb{Q}\right] = 2$; o bază a lui $\mathbb{Q}\left(\sqrt{d}\right)$ peste $\mathbb{Q}$ este $B = \left\{1, \sqrt{d}\right\}$ şi deoarece $i(1) = 1$, $i\left(\sqrt{d}\right) = -\sqrt{d}$, rezultă că matricea asociată este

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

• Luând $K = \mathbb{F}_{p^2}$ un corp cu p^2 elemente, care are caracteristica p (p =prim, $p \neq 2$) şi $i : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$, $i(x) = x^p$ (automorfismul lui *Frobenius*) avem $i \circ i = 1_K$, $F = \{x \in K \mid x^p = x\} = \mathbb{F}_p \simeq \mathbb{Z}_p$ care este un corp cu p elemente şi $\left[\mathbb{F}_{p^2} : \mathbb{F}_p\right] = 2$. Polinomul $f = X^{p^2} - X \in \mathbb{F}_p[X]$ are ca rădăcini toate elementele corpului K, iar polinomul $g = X^p + X \in \mathbb{F}_p[X]$ divide polinomul f (căci rădăcinile lui g sunt rădăcini pentru f). Polinomul g nu are însă rădăcini în $\mathbb{F}_p^*$, căci o eventuală rădăcină $x_0 \in \mathbb{F}_p^*$ a lui g ar duce la $x_0^p = x_0$ şi $x_0^p = -x_0$, deci $x_0 = -x_0$, absurd, în caracteristică $p \neq 2$. Alegem atunci o rădăcină $\alpha \in K^*$ a polinomului g, deci $\alpha \in K \setminus \mathbb{F}_p$ şi atunci $B = \{1, \alpha\}$ este o bază a lui K peste $\mathbb{F}_p$. Deoarece $i(1) = 1$ şi $i(\alpha) = \alpha^p = -\alpha$,

rezultă că matricea asociată aplicaţiei liniare i în baza B este

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

• Luând $K = \mathbb{F}_4 = \{0, 1, \alpha, 1+\alpha\}$ un corp cu 4 elemente, care are caracteristica 2, iar $i : \mathbb{F}_4 \to \mathbb{F}_4$, $i(x) = x^2$ (automorfismul lui *Frobenius*) avem $i \circ i = 1_K$, $F = \left\{x \in \mathbb{F}_4 \mid x^2 = x\right\} = \{0, 1\} = \mathbb{F}_2 \simeq \mathbb{Z}_2$ care este un corp cu 2 elemente şi $[\mathbb{F}_4 : \mathbb{F}_2] = 2$; o bază a lui $\mathbb{F}_4$ peste $\mathbb{F}_2$ este $B = \{1, \alpha\}$ şi deoarece $i(1) = 1$, iar $i(\alpha) = \alpha^2 = 1 + \alpha$ (a se vedea tabla înmulţirii în corpul $\mathbb{F}_4$), rezultă că matricea asociată lui i este

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

2. Punctul a) al teoremei precedente, este un caz particular al unui rezultat mai general ([1], teorema 14) şi anume:

Fie K un corp comutativ şi G un grup format din n automorfisme ale corpului K. Dacă F este mulţimea „invarianţilor“ grupului G, adică:

$$F = \{x \in K \mid \sigma(x) = x,\ \forall\, \sigma \in G\},$$

atunci F este un subcorp al corpului K şi avem $[K : F] = n$.

În cazul nostru $G = \{1_K, i\}$ este un grup cu 2 automorfisme ale corpului K, prin urmare $[K : F] = 2$.

3. Este valabil, în ipotezele teoremei, următorul rezultat:

Singurele F-automorfisme (automorfisme pentru care elementele lui F sunt puncte fixe) ale corpului K sunt 1_K şi i.

Într-adevăr, fie $f : K \to K$ un F–automorfism, adică $f(x) = x, \forall\, x \in F$. Dacă $B = \{1, \alpha\}$ este o bază a lui K peste F, am văzut că $s = \alpha + i(\alpha) \in F$, $p = \alpha i(\alpha) \in F$. Atunci $f(s) = s$, $f(p) = p$, adică $f(\alpha) + f(i(\alpha)) = s$, $f(\alpha) f\left(i(\alpha)\right) = p$. Înseamnă că polinomul $X^2 - sX + p \in F[X]$ are, pe de o parte, rădăcinile α şi $i\alpha$, iar pe de altă parte, rădăcinule $f(\alpha)$ şi $f\left(i(\alpha)\right)$, adică $\{\alpha, i(\alpha)\} = \{f(\alpha), f\left(i(\alpha)\right)\}$. Dacă $f(\alpha) = \alpha$ rezultă $f = 1_K$, iar dacă $f(\alpha) = i(\alpha)$ rezultă $f = i$.

4. La Olimpiada Naţională de Matematică din anul 1998, semnatarul acestor rânduri a propus la clasa a XII-a următoarea problemă:

Un corp $K \subset \mathbb{C}$ în care operaţiile sunt cele obişnuite cu numere complexe, satisface ipotezele:

a) *Corpul K are exact două endomorfisme f şi g.*

b) $f(x) = g(x) \Rightarrow x \in \mathbb{Q}$.

Să se demonstreze că există un întreg liber de pătrate $d \neq 1$ astfel încât $K = \mathbb{Q}\left(\sqrt{d}\right)$.

Dăm aici o soluţie bazată pe teorema din acest articol.

Mai întâi de toate, este clar că unul din endomorfisme este 1_K; să zicem că $g = 1_K$. Nu putem avea $f \circ f = f$, căci f fiind injectiv (morfismele de corpuri sunt injective) ar rezulta $f = 1_K = g$, absurd. Aşadar $f \circ f = 1_K$, deci f este un automorfism involutiv al corpului K. Ipoteza b) din problemă se scrie $f(x) = x \Rightarrow x \in \mathbb{Q}$ şi pentru că implicaţia reciprocă este evidentă, rezultă că $\mathbb{Q} = \{x \in K \mid f(x) = x\}$. Conform teoremei avem $[K : \mathbb{Q}] = 2$. Dacă $\alpha \in K \setminus \mathbb{Q}$, am văzut că $\alpha - f(\alpha) \in K \setminus \mathbb{Q}$. Dar $\alpha - f(\alpha) = \sqrt{s^2 - 4p}$, unde $s = \alpha + f(\alpha) \in \mathbb{Q}$, $p = \alpha f(\alpha) \in \mathbb{Q}$ şi unde prin $\sqrt{A}$ înţelegem una din rădăcinile polinomului $X^2 - A \in \mathbb{Q}[X]$. Scriind $s^2 - 4p = q^2 d$, cu $q \in \mathbb{Q}$ şi $d \in \mathbb{Z} \setminus \{1\}$ liber de pătrate, rezultă $\alpha - f(\alpha) = q\sqrt{d}$, deci $\sqrt{d} \in K \setminus \mathbb{Q}$. Atunci $B = \left\{1, \sqrt{d}\right\}$ este o bază a lui K peste $\mathbb{Q}$, prin urmare:

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

5. Autorul este recunoscător colegului său, prof. *Dinu Şerbănescu* şi lui *Andrei Ciupan*, student la Harvard University (USA), pentru punerea problemei.

BIBLIOGRAFIE

[1] Artin E., *Galoissche Theorie*, B. G. Teubner Verlagsgeselschaft, Leipzig, 1959.