Teorie Galois

July 25, 2021

1 Curs 1 - Corpuri şi spaţii liniare

Definiţii: inel, corp, exemple, morfism de corpuri; izomorfism, automorfism.

Observaţie 1.1 *$f : F \to E$ morfism de corpuri implică*

$$\forall\ k \in \mathbb{Z},\ x \in F,\ f(kx) = kf(x),\ f\left(x^k\right) = (f(x))^k.$$

Teorema 1.1 *Un corp comutativ este un domeniu de integritate.*

Teorema 1.2 *Orice morfism de corpuri este injectiv.*

Teorema 1.3 *$\sigma : F \simeq E$, izomorfism corpuri $\Rightarrow \sigma^* : F[X] \to E[X]$, izomorfism de inele.*

(σ^* morfism surjectiv; $\sigma^*(f) = 0 \Rightarrow \sigma(a_k) = 0 \Rightarrow a_k = 0$)
$F \leq K$, subgrup :

$$\begin{cases} (F,+) \leq (F,+) \\ (F^*,\cdot) \leq (K^*,\cdot), \text{ subgrup} \end{cases}$$

Exemplu 1.1 $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

$d \in \mathbb{Z} - \{0,1\}$, d liber de pătrate ($\nexists\ p$ prim : $\mathrm{p}^2 | d$)

$$\mathbb{Q}\left(\sqrt{d}\right) \leq \mathbb{C}, \mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}, Aut\,\mathbb{Q}\left(\sqrt{d}\right) = \left\{1_{\mathbb{Q}(\sqrt{d})},\ u\right\}.$$

$$u\left(a + b\sqrt{d}\right) = a - b\sqrt{d} \Rightarrow \left(u\left(\sqrt{d}\right)\right)^2 = u(d) = d \Rightarrow u\left(\sqrt{d}\right) = \pm\sqrt{d}.$$

Teorema 1.4 *$\mathbb{Q}$ este cel mai mic subcorp al lui $\mathbb{C}$.*

(F subcorpul prim al lui $\mathbb{C} \Rightarrow 1 \in F \Rightarrow \mathbb{Z} \subset F \Rightarrow \mathbb{Q} \subseteq F$)

Caracteristica unui corp

F corp comutativ
$car\ F = p$, dacă $p \cdot 1 = 0$, p minim, altfel $car\ F = 0$.

i) p prim;

ii) $n \cdot 1 = 0$ în $F \Rightarrow p|n$.

Demonstraţie.

i) Presupunem că $p = rq \Rightarrow \underbrace{p \cdot 1}_{=0} = (r \cdot 1)(q \cdot 1) \overset{\text{dom}}{\underset{\text{integr}}{\Longrightarrow}} r \cdot 1 = 0$ sau $q \cdot 1 = 0$, fals!

ii) Fie $r \neq 0$ şi $r < p$, $n = pq + r \Rightarrow \underbrace{n \cdot 1}_{=0} = \underbrace{pq \cdot 1}_{=0} + r \cdot 1 \Rightarrow r \cdot 1 = 0$, fals!

■

Teorema 1.5 *F grup de caracteristică $p \Rightarrow (x \pm y)^p = x^p \pm y^p$.*

Demonstraţie. $(x \pm y)^p = x^p + \sum_{k=1}^{p-1} \underbrace{C_p^k}_{=0} x^{p-k}(-y)^k \pm y^p$ şi inducţie. ■

Teorema 1.6

i) *$car\ F = 0 \Rightarrow \mathbb{Q} \subseteq F$*, până la izomorfism.

ii) *$car\ F = P \Rightarrow \mathbb{Z}_P \subseteq F$*, până la izomorfism.

Demonstraţie.

i) $\forall\ n \in \mathbb{N}^*$, $n \cdot 1 \neq 0 \Rightarrow (n \cdot 1)^{-1} \in P$ subcorpul prim $\Rightarrow$

$$(m \cdot 1)(n \cdot 1)^{-1} \in P \Rightarrow \mathbb{Q} \subseteq \underbrace{P \subseteq \mathbb{Q}}_{\text{def } P}.$$

ii) $F' = \{0, 1, 2, ..., p-1\} \simeq \mathbb{Z}_{p.}$, $x \cdot 1 \longleftarrow \hat{x}$. Aşadar rezultă că F‘izom.

$\mathbb{Z}_p$ nu are subcorpuri proprii. ($F'' \subseteq \mathbb{Z}_p \Rightarrow |F''|\ \ |p \Rightarrow F'' = \mathbb{Z}_p$).

■

Teorema 1.7 *Fie f ireductibil, $f \in K[X] \Rightarrow K \leq K[X]/_{(f)} = K_1$, K_1 este corp.*

Demonstraţie. $K[X]$ euclidian $\Rightarrow K[X]$ principal.

Arăt că (f) este maximal.

$$(f) \subseteq \underbrace{(h)}_{I} \subseteq K[X] \Rightarrow h|f,\ f \text{ ireductibil, avem:}$$

$$h \sim 1 \Rightarrow (h) = K[X] \text{ sau } h \sim f \Rightarrow (f) = (h).$$

$$k \rightsquigarrow k + (f),\ f \text{ are rădăcina } x + (f) \text{ în } K_1$$

Reciproca (f) maximal $\Rightarrow f$ ireductibil. Presupunem că:

$$f = gh \in (f) \Rightarrow g \in (f) \text{ sau } h \in (f),\ (f) \text{ prim.}$$

$$\Rightarrow f|g \text{ sau } f|h \Rightarrow f \sim g \text{ sau } f \sim h \Rightarrow f \text{ ired .}$$

■

Extindere finită: $F \underset{finită}{\leq} E$ dacă dim ${}_FE$ $(= [E\colon F]) < \infty$, unde F este subcorp al lui E.

Teorema 1.8

$$F \leq L \leq E$$

$$[L\colon F] < \infty,\ [E\colon L] < \infty \Rightarrow [E\colon F] < \infty \text{ şi } [E\colon F] = [L\colon F] \cdot [E\colon L].$$

Demonstraţie.

$$B_1 = \{e_i\}_i \text{ bază în } {}_LE$$

$$B_2 = \{f_j\}_j \text{ bază în } {}_FL$$

$$\Rightarrow B = \{e_i\ f_j\}_{(i,j)} \text{ bază în } {}_FE.$$

Liniara independenţă:

$$\sum_{i,j}^{*} a_{ij} e_i f_j = 0,\ a_{i,j} \in F \ \Rightarrow\ \sum_{i}^{*} \left(\sum_{j}^{*} a_{ij} f_j \right) e_i = 0$$

Sistem de generatori:

$$z \in E \Rightarrow z = \sum_{i}^{*} b_i e_i, b_i \in L \Rightarrow b_i = \sum_{j}^{*} a_{ij} f_j.$$

■

Consecinţe:

1) $[E\colon F] = 1 \Rightarrow E = F$.

2) $F \leq L \leq E, [E\colon F] = [L\colon F] \nrightarrow E = L.$

3) $[E\colon F] = p$ (prim) $\Rightarrow$ nu sunt corpuri intermediare .

2 Seminar 1

Exerciţiu 2.1 $F \leq E,\ [E\colon F] = 1 \Rightarrow E = F$.

Soluţie 2.1

$$\forall x \in E,\ \exists\ f \in F\ : x = f \cdot 1 \in F \Rightarrow x \in F\ .$$

Exerciţiu 2.2 $\left.\begin{array}{c} F \leq L \leq E \\ [E\ :\ F] = [L\ :\ F] \end{array}\right\} \Rightarrow E = L.$

Soluţie 2.2 *Avem* $[E\ :\ F] = [L : F] \cdot [E\ :\ L] \overset{ip}{\Rightarrow} [E\ :\ L] = 1 \overset{ex.1}{\Rightarrow} E = L.$

Exerciţiu 2.3 ${}_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})$ *spaţiu liniar cu baza* $\{1, \sqrt{2}\}$.

sau: $\sqrt{2}$ rădăcina lui $X^2 - 1$, $\left(\sqrt{2}\right)^2 = 1 \Rightarrow {}_{\mathbb{Q}}\mathbb{Q}\left(\sqrt{2}\right)$ are baza $\{1, \sqrt{2}\}$.

Exerciţiu 2.4 *Fie* $f = X^4 + X + 1 \in \mathbb{Z}_2[X]$.

i) Arătaţi că f este ireductibil în $\mathbb{Z}_2[X]$;

ii) Construiţi tabelele de compoziţie în $\mathbb{Z}_2(y)$, unde y este rădăcină a lui f.

Soluţie 2.3

i) f nu are rădăcină în $\mathbb{Z}_2$ $\left(\ f(\hat{0}) \neq \hat{0},\ f(\hat{1}) \neq \hat{0}\right)$.

Presupunem că $f = gh$ cu $g = X^2 + a_1X + a_2$ şi $h = X^2 + b_1X + b_2$, $a_i, b_i \in \mathbb{Z}_2\ \Rightarrow$

$$\Rightarrow \begin{cases} a_1 + b_1 = \hat{0} \\ a_1b_1 + a_2 + b_2 = \hat{0} \\ a_1b_2 + a_2b_1 = \hat{1} \\ a_2b_2 = \hat{1}\ \Rightarrow a_2 = b_2 = \hat{1} \Rightarrow a_1b_1 = \hat{0},\ \underset{fals!}{a_1 + b_1 = \hat{1}}. \end{cases}$$

ii) Avem $y^4 = y + 1$.

Observăm că ${}_{\mathbb{Z}_2}\mathbb{Z}_2(y)$ are baza $\{1, y, y^2, y^3\}$.

Obţinem $\mathbb{Z}_2(y) = \{\hat{0}, \hat{1}, y, y + \hat{1}, y^2, y^2 + \hat{1}, y^2 + y, y^2 + y + 1, y^3, y^3 + \hat{1}, y^3 + y, y^3 + y^2, y^3 + y^2 + y, y^3 + y + \hat{1}, y^3 + y^2 + y + \hat{1}\}$.

$|\mathbb{Z}_2(y)| = 16$.

Exerciţiu 2.5 ${}_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{3})$ *are baza* $\{1, \sqrt[3]{3}, \sqrt[3]{3^2}\}$ *pentru că* $\left(\sqrt[3]{3}\right)^3 = 3$.

Exerciţiu 2.6 $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt{7}\right) \geq \left(\mathbb{Q}\left(\sqrt{2}\right)\right)\left(\sqrt[3]{3}\right) \geq \mathbb{Q}\left(\sqrt{2}\right) \geq \mathbb{Q}$.

Soluţie 2.4

${}_{\mathbb{Q}}\mathbb{Q}\left(\sqrt{2}\right)$ are baza $\left\{1, \sqrt{2}\right\} = B_1$.
${}_{\mathbb{Q}\left(\sqrt{2}\right)}\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}\right)$ are baza $\left\{1, \sqrt[3]{3}, \sqrt[3]{9}\right\} = B_2$.
${}_{\mathbb{Q}\left(\sqrt{2},\ \sqrt[3]{3}\right)}\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt{7}\right)$ are baza $\left\{1, \sqrt{7}\right\} = B_3$.
Atunci ${}_{\mathbb{Q}}\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt{7}\right)$ are baza $B = B_1B_2B_3$.

Exerciţiu 2.7 *Să se studieze ireductibilitatea lui* $f = X^2 + aX + b$, $a, b \in K$. $K \in \{\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Q}\}$.

Soluţie 2.5 *Fie* α *o rădăcină pentru* f.

Atunci
$$(2\alpha + a)^2 = a^2 - 4b, \ \left(\alpha^2 + a\alpha + b = 0 | 4\right).$$

f ired în $K[X] \iff a^2 - 4b \notin K^2 = \left\{k^2 | k \in K\right\}$.
Pentru $\mathbb{Z}_3$,

$$K^2 = \{0, 1\}.$$
$$a^2 - 4b \notin K^2 \iff a^2 - 4b = 2 \text{ în } \mathbb{Z}_3$$

Pentru $\mathbb{Z}_5$,

$$K^2 = \{0, 1, 4\}.$$
$$a^2 - 4b \notin K^2 \iff a^2 - 4b = 2 \text{ sau} = 3 \text{ în } \mathbb{Z}_5$$

Se determină a, b.

Exerciţiu 2.8 *Arătaţi că mulţimea subcorpurilor lui* $\mathbb{R}$ *este infinită.*

Soluţie 2.6
$$\mathbb{Q}\left(\sqrt[n]{2}\right) \leq \mathbb{R}, \ \left[\ \mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = n.$$

Exerciţiu 2.9 *Arătaţi că* $\forall\, n \in \mathbb{N}^*, \exists\, K\colon\ \mathbb{Q} \leq K \leq \mathbb{R}, [K\colon \mathbb{Q}] = n, \left(K = \mathbb{Q}\left(\sqrt[n]{z}\right)\right)$. *Rezultă ext.* $\mathbb{Q} \leq \mathbb{R}$ *infinită.*

Exerciţiu 2.10 *Determinaţi subcorpurile lui* $\mathbb{C}$ *care conţin pe* $\mathbb{R}$.

Soluţie 2.7 $\mathbb{R} \leq K \leq \mathbb{C}$ *şi* $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{C} : \mathbb{R}] \Rightarrow K = \mathbb{R}$ *sau* $K = \mathbb{C}$.

3 Curs 2 - Elemente algebrice

Fie $F \leq E$, $a \in E$.

Definiţie 3.1 *Spunem că a* $alg/_F$ *dacă* $\exists\, f \in F[X]$, $f \neq 0$,*astfel încât,* $f(a) = 0$.

Definiţie 3.2 *Spunem că a* $transc/_F$ *dacă a nu e* $alg/_F$.

Definiţie 3.3 *Extinderea* $F \leq E$ *este algebrică dacă* $\forall\, a \in E$, a $alg/_{F.}$

1) $\forall\, a \in F$, a $alg/_F$, fiind rădăcină pentru $X - a$.

2) $\mathbb{Q} \leq \mathbb{R}$, $\sqrt{2}$ $alg/_{\mathbb{Q}}$, $f = X^2 - 2$, e, Π $\text{transc}/_{\mathbb{Q}}$.

3) $K \leq K(X)$, X $transc/_K$.

4) $\mathbb{R} \leq \mathbb{C}$ alg : $\forall\, a = x + i\, y$ e rădăcină pentru $X^2 - 2xX + x^2 + y^2$.

4 Polinom minimal

Fie $F \leq E$, a $alg/_F$, $a \in E$. Vom face următoarea notaţie:

$$m_a \overset{not}{=} Irr(a,\ F),$$

unde prin $Irr\ (a,\ F)$ înţelegem: ireductibil în $F[X]$, coeficient dominant 1 şi are pe a rădăcină. (m_a ireductibil sau de grad minim).

Teorema 4.1 *Fie* $f \in F[X]$ *cu* $f(a) = 0$ *şi* $g = m_a$. *Atunci* $g \mid f$.

Demonstraţie.

Vom folosi metoda reducerii la absurd, aşa că vom presupune că $g \nmid f$.
Din faptul că g este ireductibil rezultă că:

$$(g,\ f) = 1 \Rightarrow \exists\, h_1, h_2 \in F[X] \text{ astfel încât:}$$
$$h_1 g + h_2 f = 1, \text{ pentru } X = a.$$

Adică $0 = 1$, fals! ■

Teorema 4.2

$$\begin{cases} \mathbf{1})\ \alpha \text{ alg}/_K \Rightarrow K(\alpha) = K[\alpha] \\ \mathbf{2})\ K(\alpha) = K[\alpha] \Rightarrow \alpha \text{ alg}/_K \end{cases}$$

Demonstraţie.

1)

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

Fie $h = m_\alpha$. Cum $g(\alpha) \neq 0 \Rightarrow h \nmid g$, h *ired* $\Rightarrow (h, g) = 1$.

$$\begin{aligned} &\Rightarrow \exists\ u, v \in K[X] :\ uh + vg = 1 \Rightarrow v(\alpha)\, g(\alpha) = 1 \Rightarrow \\ &\Rightarrow \frac{1}{g(\alpha)} = v(\alpha) \Rightarrow \frac{f(\alpha)}{g(\alpha)} = f(\alpha)\, v(\alpha) \in K[\alpha] \Rightarrow \\ &\Rightarrow K(\alpha) \subseteq K[\alpha] \subseteq K(\alpha). \end{aligned}$$

2) Din $K(\alpha) = K[\alpha] \Rightarrow \forall\ \frac{f(\alpha)}{g(\alpha)} \in K[\alpha]$. Iau g cu $grad \geq 1 \Rightarrow$

$$\frac{1}{g(\alpha)} = v(\alpha) \in K[X].$$

Fie $\overline{f} = v\ g - 1$ cu rădăcina α. $\overline{f} \in K[X]$, $\overline{f} \neq 0$ altfel

$$vg = 1 \Rightarrow g \in v \in (K[X]) = K^*$$

contradicţie cu $grad\ g \geq 1$.

Aşadar $\alpha\ alg|_K$. ■

Teorema 4.3 *Orice extindere finită e algebrică.*

Demonstraţie. Fie $K \leq L$ cu $[L\colon K] = n$ şi $a \in L$.

Avem $\{1, a, ..., a^n\}$ lin. dep. în ${}_KL \Rightarrow \exists\ k_0, k_1, ..., k_n \in K$ nu toate nule, astfel încât:

$$\sum_{i=0}^{n} k_i a^i = 0 \Rightarrow a \text{ rădăcina polinomului.}$$

$$f = \sum_{i=0}^{n} k_i X^i \neq 0 \Rightarrow a\ alg/_K.$$

■

Teorema 4.4 $\alpha\ alg/_F \Rightarrow \dim_F F(\alpha) = \text{grad } m_\alpha$.

Demonstraţie. Fie $m_\alpha = X^n + a_{n-1}X^{n-1} + ... + a_0 \in F[X]$. Atunci rezultă că:

$$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_0.$$

$$\alpha^{n+i} = \sum_{0 \le K \le n-1} b_K \alpha^K \Rightarrow B = \left\{1, \alpha, ..., \alpha^{n-1}\right\} \text{ sistem de generatori în } {}_F F(\alpha).$$

B lin. indep., altfel grad $m_\alpha < n$. Deci B bază în ${}_F F(\alpha)$. ■

Teorema 4.5 *Fie $K \le L$ şi $[L\colon K] = n$. Atunci $\exists\ \alpha_1, ..., \alpha_n$ $alg/_K$, astfel încât $L = K(\alpha_1, ..., \alpha_n)$.*

Demonstraţie. Fie B bază în ${}_K L = \{\alpha_1, ..., \alpha_n\}$. Atunci

$$L = \left\{ \sum_1^n k_i \alpha_i \mid k_i \in K, \forall i \right\} \subseteq K[\alpha_1, ..., \alpha_n] \underset{\alpha_i\ alg}{=} K(\alpha_1, ..., \alpha_n) \subseteq L.$$

pentru că $[L\colon K] < \infty$ ■

5 Extinderi prin adjuncţionare

Fie $F \le E$, $S \subseteq E$.

$$F(S) = \bigcap_{\substack{K \le E \\ F \cup S \subseteq K}} K \textbf{ corpul obţinut prin adjuncţionare}.$$

$$S = \{x_1, ..., x_n\} \Rightarrow F(S) = F(x_1, ..., x_n) \text{ şi } F(S_1 \cup S_2) = (F(S_1))(S_2).$$

$$F[S] = \bigcap_{\substack{R \text{ subinel în } E \\ F \cup S \subseteq K}} R \quad \textbf{subinel obţinut prin adjuncţionare}.$$

$F(S)$ este **corpul de fracţie al lui** $F[S]$.

$$F(S) = \left\{ \frac{A}{B} \mid A \in F[S],\ B \in F[S],\ B \neq 0 \right\}.$$

Definiţie 5.1 *$K \le L$ este **extindere simplă** dacă $\exists\ \alpha \in L :\ L = K(\alpha)$. α: element primitiv al lui L peste K.*

Teorema 5.1 *(Teoremă de structură)*

Fie $L = K(\alpha)$. *Arătaţi că:*
1) α $alg/_K \Rightarrow K(\alpha) \simeq K[X]/_{(m_\alpha)}$.
2) α $transc/_K \Rightarrow K(\alpha) \simeq K(X)$.

Demonstraţie.

$$\begin{aligned} f\colon\ K[X] &\to K(\alpha) \\ k &\rightsquigarrow k \\ X &\rightsquigarrow \alpha \end{aligned}$$

Rezultă că Im $f = K[\alpha]$.
1)

$$\begin{aligned} Kerf &= \{P \in K[X] \mid f(P) = P(\alpha) = 0\} = (m_\alpha) \\ &(\ P(\alpha) = 0 \Rightarrow m_\alpha | P) \end{aligned}$$

Obţinem $K[X]/_{(m_\alpha)} \simeq K[\alpha] \overset{\alpha \text{ alg}}{=} K(\alpha)$.
2)

$$Kerf = \{P|\ P(\alpha) = 0\} = 0 \Rightarrow \underset{\text{dom. integritate}}{K[X] \simeq K[\alpha].}$$

■

6 Seminar 2

Exerciţiu 6.1 *Fie a o rădăcină pentru $f = X^3 - X + 1 \in \mathbb{Q}[X]$*

$$\begin{cases} \textbf{a}) \text{ Determinaţi } b^{-1} \text{ în } \mathbb{Q}(a) \text{ şi } a^{-1} \text{ în } \mathbb{Q}(a), \text{ unde } b = 1 - 2a + 3a^2 \in \mathbb{Q}(a). \\ \textbf{b}) \text{ Determinaţi } m_c \in \mathbb{Q}[X],\ c = 1 + a - 2a^2. \\ \textbf{c}) \text{ Arătaţi că } \mathbb{Q}(a) = \mathbb{Q}(c). \end{cases}$$

Soluţie 6.1

a) f ired, altfel ar avea un factor de grad 1 cu coeficient în $\mathbb{Q}$, fals!
Deci

$$m_a = f \Rightarrow_{\mathbb{Q}} \mathbb{Q}(a) \text{ are baza} \{1, a, a^2\}.$$

$$f(a) = 0 \Rightarrow a(a^2 - 1) = -1 \Rightarrow a(1 - a^2) = 1 \Rightarrow a^{-1} = 1 - a^2.$$

$$\begin{aligned} b^{-1} &= x + ya + za^2,\ x, y, z \in \mathbb{Q}. \\ bb^{-1} &\Rightarrow \left(1 - 2a + 3a^2\right)\left(x + ya + za^2\right) = 1 \end{aligned}$$

Din indentificarea coeficienţilor, obţinem:

$$x = \frac{6}{11},\ y = -\frac{7}{11},\ z = -\frac{8}{11}$$

b) Obţinem m_c astfel:

$$\begin{cases} 1 + a - 2a^2 = c \ \mid a \\ a^3 - a + 1 = 0 \ \mid 2 \end{cases} \Rightarrow \begin{cases} ac = a + a^2 - 2a^3 \\ 0 = 2a^3 - 2a + 2 \\ \quad -----(+) \end{cases}$$

$$\begin{cases} ac = a^2 - a + 2 \ \mid 2 \\ c = 1 + a - 2a^2 \end{cases} \Rightarrow \begin{cases} 2ac = 2a^2 - 2a + 4 \\ c = 1 + a - 2a^2 \\ \quad -----(+) \end{cases}$$

$$2ac + c = 1 - a + 4 \Rightarrow a(2c+1) = 5 - c$$

$$\Rightarrow a = \frac{5-c}{2c+1} \quad (c \neq -\frac{1}{2})$$

$$c = -\frac{1}{2} \Rightarrow c = 5, fals!$$

$$f = m_a \Rightarrow \left(\frac{5-c}{2c+1}\right)^3 - \frac{5-c}{2c+1} + 1 = 0 \Rightarrow m_c = X^3 + X^2 - 8X + 11.$$

c)

$$\left.\begin{array}{l} a = \frac{5-c}{2c+1} \in \mathbb{Q}(c) \Rightarrow \mathbb{Q}(a) \subseteq \mathbb{Q}(c) \\ c = 1 + a - 2a^2 \in \mathbb{Q}(a) \Rightarrow \mathbb{Q}c) \subseteq \mathbb{Q}(a) \end{array}\right\} \Rightarrow \mathbb{Q}(a) = \mathbb{Q}(c).$$

Sau: $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq \mathbb{Q}(a)$
$[\mathbb{Q}(a) : \mathbb{Q}] = 3 = \text{grad } m_a = \text{grad } m_c = [\mathbb{Q}(c) : \mathbb{Q}] \Rightarrow \mathbb{Q}(a) = \mathbb{Q}(c)$.

Exerciţiu 6.2

Fie $X^3 - X + 1 \in \mathbb{Q}[X]$ şi a o rădăcină a sa.

Determinaţi. : $\begin{cases} \textbf{i)} \ \frac{3a^2+2}{a^2+4} \text{ în } \mathbb{Q}(a) \\ \textbf{ii)} \ \text{Irr } (\beta^{-1},\ \mathbb{Q}), \text{ unde } \beta = 2 - a + a^2 \ . \end{cases}$

Soluţie 6.2

i)

$$\frac{3a^2+2}{a^2+4} = x + ya + za^2, \text{ cu } x, y, z \in \mathbb{Q}.$$

Folosim $a^3 - a + 1 = 0$.
Obţinem: $x = \frac{53}{101}$, $y = \frac{10}{101}$, $z = \frac{50}{101}$.

ii) Ca mai sus, obţinem:

$$\beta^{-1} = \frac{7}{11} + \frac{a}{11} - \frac{2a^2}{11}.$$

Şi scriu a în funcţie de β^{-1}.

$$\begin{cases} 11\beta^{-1} = 7 + a - 2a^2 \\ 0 = a^3 - a + 1 \end{cases} \Rightarrow \begin{cases} 11\beta^{-1}a = 7a + a^2 - 2a^3 \\ 0 = 2a^3 - 2a + 2 \\ \quad ----(+) \end{cases}$$

$$\begin{cases} 11\beta^{-1}a = 5a + a^2 + 2 \\ 11\beta^{-1} = 7 + a - 2a^2 \end{cases} \Rightarrow \begin{cases} 22\beta^{-1}a = 10a + 2a^2 + 4 \\ 11\beta^{-1} = 7 + a - 2a^2 \end{cases} \Big| \overset{(+)}{\Rightarrow} 11a+11 = 11(\beta^{-1}+2a\beta^{-1})$$

Aşadar avem:

$$a + 1 = \beta^{-1} + 2a\beta^{-1} \Rightarrow a(1 - 2\beta^{-1}) = \beta^{-1} - 1$$

$$\left.\begin{array}{l} \Rightarrow a = \frac{\beta^{-1}-1}{1-2\beta^{-1}} \text{ , } \beta^{-1} \neq \frac{1}{2} \\ a^3 - a + 1 = 0 \end{array}\right\} \Rightarrow \left(\frac{\beta^{-1} - 1}{1 - 2\beta^{-1}}\right)^3 + \frac{1 - \beta^{-1}}{1 - 2\beta^{-1}} + 1 = 0 \Rightarrow \text{...grad } Irr\ \beta^{-1} = 3.$$

Exerciţiu 6.3

Fie a răd. ptr. $X^3 - X + 1 \in \mathbb{Q}[X]$.
i) $b = 1 - a + a^2$, $c = 2 + a - 2a^2$ din $\mathbb{Q}(a)$. Determinaţi $Irr\ \left(b^{-1}c,\ \mathbb{Q}\right)$.
ii) $b = 2 + a - a^2$, $c = 1 + 3a + 2a^2$. Determinaţi $Irr\ \left(bc^{-1},\ \mathbb{Q}\right)$.

Soluţie 6.3

i)

$$d = b^{-1}c = -4a^2 - a + 5.$$

Scriu a în funcţie de d, astfel:

$$a = \frac{d + 11}{4d - 5}.$$

ii)

$$d = \frac{-10}{11}a^2 + \frac{5}{11}a + \frac{2}{11} \Rightarrow a = \frac{2 - d}{2d + 1}$$

$$Irr\ (d, \mathbb{Q}) = 13X^3 + 14X^2 - 13X + 7.$$

Exerciţiu 6.4

Fie $z = a + bi \in \mathbb{C}$. Să se arate că z alg/$_{\mathbb{Q}} \iff \begin{cases} a \text{ alg}/\mathbb{Q} \\ b \text{ alg}/\mathbb{Q} \end{cases}$.

Soluţie 6.4

$\Rightarrow$" Fie A corpul numerelor algebrice peste $\mathbb{Q}$.
z alg/$_{\mathbb{Q}} \Rightarrow$

$$\exists\ f \in \mathbb{Q}[X],\ f \neq 0,\ f(z) = 0.$$

$$\overline{z} \in A \Longleftarrow f(\overline{z}) = 0,\ f(z) \Rightarrow f(\overline{z}).$$

$$a = \frac{z + \overline{z}}{2},\ b = \frac{z - \overline{z}}{2i} \Rightarrow a, b \in A.$$

$\Leftarrow$" a, b, $i \in A \Rightarrow z \in A$.

Observaţie
$A = \{a \in \mathbb{C} \mid a \text{ alg}/_{\mathbb{Q}}\}$ este corp.
Mai general, dacă $K \leq L$, $A = \{\alpha \in L \mid \alpha \text{ alg}/_K\}$,
Atunci A este corp.
$\alpha, \beta \in A$

$$\Rightarrow [K(\alpha,\ \beta) : K] < \infty \Rightarrow K \leq K(\alpha,\ \beta) \text{ alg} \Rightarrow K(\alpha,\ \beta) \subseteq A.$$
$$\Rightarrow \alpha \pm \beta,\ \alpha\beta,\ \beta^{-1}(\ \beta \neq 0) \in A \Rightarrow A \text{ corp.}$$

Exerciţiu 6.5

Fie $F \leq L$. $A = \{a \in L \mid a \text{ alg}/_K\}$ şi fie $u \in L$. Fie $f \in K[X]$, grad $f \geq 1$.
Atunci $u \in A \iff f(u) \in A$.

Soluţie 6.5

$\Rightarrow$"

$$\left.\begin{matrix} u \in A \\ A \text{ corp} \end{matrix}\right\} \Rightarrow f(u) \in A.$$

$\Leftarrow$"

$$f(u) \in A \Rightarrow \exists\ g \in K[X],\ g \neq 0, \text{astfel încât } g(f(u)) = 0.$$

Fie $h = gf$, deci avem că $h(u) = 0$. Folosim faptul că $g \neq 0 \Rightarrow h \neq 0$.($f$ are grad $f \geq 1$) rezultă că $u \in A$.

Exerciţiu 6.6

Fie $f \in \mathbb{Q}[X]$, grad $f \geq 1$. Atunci $f(\Pi)$ $transc/_{\mathbb{Q}}$ şi $f(e)$ $transc/_{\mathbb{Q}}$.

Exerciţiu 6.7

Determinaţi $\mathbb{R}\left(\sqrt{2}+i\sqrt{3}\right)$.

Soluţie 6.6

Mai mult, dacă $z \in \mathbb{C}-\mathbb{R}$, $\mathbb{R}(z)=\mathbb{C}$.
$\mathbb{R} \leq \mathbb{R}(z) \leq \mathbb{C} \Rightarrow \mathbb{R}(z)=\mathbb{R} \Rightarrow z \in \mathbb{R}$ fals! sau $\mathbb{R}(z)=\mathbb{C}$.

Exerciţiu 6.8

Determinaţi $Irr\left(1+\sqrt{2},\ \mathbb{Q}\right)$.

Soluţie 6.7

Notăm $a=1+\sqrt{2}$.

$\Rightarrow (a-1)=2 \Rightarrow a^2-2a-1 \Rightarrow a$ soluţie pentru $X^2-2X-1 \in \mathbb{Q}[X]$ ired.
$\Rightarrow Irr(1+\sqrt{2})=X^2-2X-1$.

Exerciţiu 6.9

Arătaţi că $\mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt{2}}\right)=\mathbb{Q}\left(\sqrt{6}\right)$.

Soluţie 6.8

$$\frac{\sqrt{3}}{\sqrt{2}}=\frac{\sqrt{6}}{2} \in \mathbb{Q}\left(\sqrt{6}\right).$$
$$\sqrt{6}=2\cdot\frac{\sqrt{3}}{\sqrt{2}} \in \mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt{2}}\right)$$

În general, dacă $\left.\begin{array}{c} u \in \mathbb{Q} \\ \sqrt{u} \notin \mathbb{Q} \end{array}\right\} \Rightarrow \exists\ d$ liber pătrate. $\mathbb{Q}(\sqrt{u})=\mathbb{Q}\left(\sqrt{d}\right)$.
$u=\frac{p}{q}$, $q \neq 0$, $p,q \in \mathbb{Z} \Rightarrow \sqrt{u}=\sqrt{\frac{p}{q}}=\frac{\sqrt{pq}}{q} \Rightarrow q\sqrt{u}=\sqrt{pq}$.

$$pq=a^2d \Rightarrow q\sqrt{u}=a\sqrt{d} \Rightarrow \mathbb{Q}(\sqrt{u})=\mathbb{Q}\left(\sqrt{d}\right)$$

7 Curs 3 - Tranzitivitatea extinderii algebrice

Teorema 7.1

Fie $K \leq L \leq F$. Avem $F\ alg/_K \Leftrightarrow F\ alg/_L$ şi $L\ alg/_K$.

Demonstraţie. $\Rightarrow$" Din $K \leq L \Rightarrow F$ alg$/_L$.

$$\left.\begin{array}{c} \alpha \in L \subseteq F \\ F \text{ alg}/_K \end{array}\right| \Rightarrow \alpha\ alg/_K.$$

$\Leftarrow$" Fie $\alpha \in F \Rightarrow \alpha\ alg/_L \Rightarrow$

$$\exists\ f = \sum_i^* \beta_i X^i,\ f \neq 0,\ f(\alpha) = 0,\ \beta_i \in L, \forall i \Rightarrow \alpha\ alg/_{K(\beta_0, ...,\ \beta_n)}$$

$$\beta_i \in L,\ L\ alg/_K \Rightarrow \beta_i\ alg/_K, \forall i \Rightarrow [K(\beta_0,\ ...,\ \beta_n) : K] < \infty. \qquad (\mathbf{1})$$

Cum α alg$/_{K(\beta_0, ...,\ \beta_n)} \Rightarrow [K(\alpha,\ \beta_0, ...,\ \beta_n)\ :\ K(\beta_0, ...,\ \beta_n)] < \infty$ şi împreună cu (**1**) rezultă că $K(\alpha, \beta_0, ..., \beta_n)\colon K] < \infty \Rightarrow \alpha\ alg/_K \Rightarrow F\ alg/_K$. ■

K - **izomorfisme**

Fie $K \leq L$, $K \leq L_2$.

Definiţie 7.1 *Funcţia $f\ :\ L_1 \longrightarrow L_2$ este K - **izom** dacă* **1**) *f izomorfism de corpuri;* **2**)$\forall\ a \in K,\ f(a) = a$.

Observaţie 7.1 *Pentru α transc.$/_K \Rightarrow K(\alpha) \overset{K-izom}{\simeq} K(X)$.*

Teorema 7.2 *Fie $K \leq L$; α, $\beta \in L$.*

I) α, β alg$/_K \Rightarrow$

$$\mathbf{1})\ Irr(\alpha, K) = Irr(\beta,\ K) \Leftrightarrow \mathbf{2})\ \exists\ f\colon K(\alpha) \to K(\beta)$$

cu $K-$izom , $f(\alpha) = \beta$

II) α, β transc$/_K \Rightarrow \exists\ f\ :\ K(\alpha) \to K(\beta)$, K- izom, unde $f(\alpha) = \beta$.

Demonstraţie. *I)* Vom arăta că **1**) $\Rightarrow$ **2**). Avem

$$K(\alpha) \simeq K[X]/(Irr(\alpha,\ K))\ \simeq K(\beta).$$
$$P(\alpha) \leftarrow P + (Irr(\alpha, K)) \to P(\beta).$$

2) $\Rightarrow$ **1**) Fie $Irr\ (\alpha,\ K) = f$; $Irr(\beta,\ K) = g$. Avem K- izom :

$\varphi\colon K(\alpha) \longrightarrow K(\beta)$ cu $\varphi(\alpha) = \beta$.

$\varphi(f(\alpha)) = f(\beta) \Rightarrow f(\beta) = 0 \Rightarrow g/f;\ g,\ f$ ired. $\Rightarrow f = g$.

II) Avem $K(\alpha) \simeq K(X) \simeq K(\beta)$. ■

Exemplu 7.1

$$f\colon \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}\left(-\sqrt{2}\right) = \mathbb{Q}\left(\sqrt{2}\right).$$
$$a + b\sqrt{2} \rightsquigarrow a - b\sqrt{2}.$$

Exemplu 7.2

$$f\colon \mathbb{C} \to \mathbb{C},\ z \to \overline{z}.$$

Exemplu 7.3

$$f\colon \mathbb{Q}\left(\sqrt[3]{3}\right) \to \mathbb{Q}\left(\epsilon\sqrt[3]{3}\right) \text{ cu } \epsilon \text{ rădăcină pentru } X^2 + X + 1.$$
$$a + b\sqrt[3]{3} + c\sqrt[3]{9} \rightsquigarrow a + \epsilon b\sqrt[3]{3} + \epsilon^2 c\sqrt[3]{9}.$$

Observăm că $\sqrt[3]{3}$, $\epsilon\sqrt[3]{3}$, $\epsilon^2\sqrt[3]{3}$ rădăcină pentru $X^3 - 3 \in \mathbb{Q}[X]$.

Exemplu 7.4

Dacă $f \in K[X]$ ireductibil şi $\{x_i\}_{i=\overline{1,\,n}}$ sunt rădăcinile sale, atunci:
$f_{ij}\ :\ K(x_i) \to K(x_j)$ este K- izom.

8 Închiderea algebrică a unui corp

$K \leq L$ şi $A = \{\alpha \in L \mid \alpha\ alg/_K\}$. A corp ($\alpha,\ \beta \in A \Rightarrow K(\alpha,\ \beta) \subseteq A$, pentru că:

$$[K(\alpha,\ \beta) : K] < 0 \Rightarrow \alpha\beta,\ \alpha \pm \beta,\ \beta^{-1} \in A), \beta \neq 0, \forall\ \beta \notin A, \beta\ transc/A.$$

A: închiderea algebrică a lui K în L.

Exemplu 8.1 *Mulţimea A, a numerelor algebrice din $\mathbb{C} \to$ are cardinal χ_0.*

$$(\alpha \in \mathbb{C}, \alpha\ alg/_{\mathbb{Q}} \to P = Irr\ \alpha \in \mathbb{Q}[X]).$$

Mulţimea $A_1 = A \cap \mathbb{R}$ a numerelor algebrice din $\mathbb{R}$.

$$\mathbb{Q} \leq A_1 \leq A \overset{\text{teorema Bernstein}}{\Longrightarrow} card\ A_1 = \chi_0.$$

Definiţie 8.1 *$\overline{K}$ este **închidere algebrică** a lui K dacă: $K \underset{alg}{\leq} \overline{K}$ şi*

$$(\forall \alpha \notin \overline{K}, \alpha\ transc/_{\overline{K}}) \Leftrightarrow (\forall\ \alpha\ alg/_{\overline{K}},\ \alpha \in \overline{K}).$$

Definiţie 8.2 *K **algebric închis** dacă $\overline{K} = K$.*

Teorema 8.1 *Fie K corp comutativ, $f \in K[X]$, grad $f \geq 2$. Atunci $\exists\ L$, $K \leq L$, astfel încât f are o rădăcină în L.*

Demonstraţie. Din lema lui **Krull**, $\exists\ M$ ideal maximal, astfel încât

$$(f) \subseteq M \subseteq K[X].$$

$K[X]$ inel principal $\Rightarrow$ $\left.\begin{array}{c} M = (g) \\ M \text{ maximal} \end{array}\right\} g$ ired.

Fie $L = K[X]/_M$.

$$\sigma : K \to L,\ \sigma(a) = a + M,\ \sigma \text{ injectiv.,fiind morfism de corpuri.}$$

$f(x + M) = f(X) + M = M = O_L \Rightarrow x + M$ rădăcină pentru f în L.

■

Corolar 1

1) Dacă $\{f_1, ..., f_n\} \subseteq K[X]$, atunci $\exists\ L$, $K \leq L$ astfel încât $\forall\ f_i$, fi are o rădăcină în L.

2) Fie $f \in K[X]$. Atunci $\exists\ L$, $K \leq L$,astfel încât f se descompune în $L[X]$ în factori de gradul I.

Lemma 1 *Fie $K \leq L$, L algebric închis. Atunci $\overline{K}_L = \{\alpha \in L \mid \alpha\ alg/_K\}$ e algebric închis şi $\overline{K}_L\ alg/_K$.*

Demonstraţie.

$$\left.\begin{array}{c} \text{Fie } f \in \overline{K}_L[X],\ grad\ f \geq 1 \\ L \text{ algebric închis} \end{array}\right\} \Rightarrow \exists\ \alpha \in L,\ f(\alpha) = 0$$

$$\Rightarrow \alpha\ alg/_{\overline{K}_L},\ \overline{K}_L\ alg/_K \Rightarrow \alpha\ alg/_K$$

$$\Rightarrow \alpha \in \overline{K}_L, \text{adică } \overline{K}_L \text{ algebric închis.}$$

■

Teorema 8.2 ***(Teorema de existenţă a închiderii algebrice)*** *$\forall\ K$ corp comutativ, $\exists\ \overline{K} \geq K$ închidere algebrică a lui K.*

Demonstraţie. Construim $\overline{K}_1$, astfel încât $K \leq \overline{K}_1$ şi $\overline{K}_1$ algebric închis.

Fie

$$T = \{f \in K[X] \mid grad\ f \geq 1\} \subseteq K[X].$$

($T = K[X] - K$). Căutăm un corp în care $\forall\ f \in T$, f are o rădăcină în acel corp.

Introduc variabilele $(X_f)_{f \in T}$. (Câte una pentru fiecare polinom f).

Fie

$$G = \{f(X_f) \mid f \in T\} \subset K[X_f \mid f \in T].$$

Dacă T este infinită, atunci

$$K[X_f |\ f \in T] = \bigcup_{\substack{J \subseteq T \\ J \text{ finit}}} K[X_j |\ j \in J]$$

Deci, $G \subsetneq K[X_f \mid f \in T]$ şi fie $\underset{\text{maximal}}{M} \supseteq (G)$.

Observaţie: $(G) \neq K[X_f \mid f \in T]$, altfel $1 = f_1(X_{f_1})\, g, + \ ... \ + f_n(X_{f_n})\, g_n$.

Iau o extindere $\widetilde{K}$ a lui K, astfel încât f_1, ..., f_n, au rădăcinile α_1, ..., α_n în $\widetilde{K}$.

Înlocuiesc X_{f_i} cu α_i şi obţin $1 = 0$, fals! ■

Fie $L_1 = K[X_f \mid f \in T]\ /M$ corp. $\forall\ f \in T$, f are o rădăcină în $L_1 : X_f + M$.

Continuând astfel,obţinem:

$$K \subseteq L_1 \subseteq ... \subseteq L_n \subseteq L_{n+1} \subseteq ...,$$

unde orice polinom din L_n are o rădăcină în L_{n+1}.

Fie

$$\overline{K}_1 = \bigcup_{i \in \mathbb{N}^*} L_i.$$

Avem: **1**) $K \subseteq \overline{K}_1$;

2) $\overline{K}_1$ corp $(\alpha \in L_i,\ \beta \in L_j\ (\ i \leq j) \Rightarrow \alpha,\ \beta \in L_j \Rightarrow \alpha - \beta,\ \alpha\ \beta,$ α^{-1}(pentru $\alpha \neq 0$) $\in L_j < \overline{K}_1$)

3) $\overline{K}_1$ algebric închis.

(Fie $f \in \overline{K}_1[X]$,

$$f = a_0 + a_1 X + ... + a_n X^n\ ;\ a_0 \in L_{i_0},\ a_1 \in L_{i_1}, ..., a_n \in L_{i_n}$$

şi $j_0 = max\ (i_0, ..., i_n) \Rightarrow f \in L_{j_0}[X] \Rightarrow$

$$\Rightarrow \left.\begin{array}{c} \exists\ \alpha \in L_{j_0+1} \subseteq \overline{K}_1 \\ f(\alpha) = 0 \end{array}\right\} \Rightarrow f = (X - \alpha)\, f_1$$

Repet pentru f_1, ...$\Rightarrow f$ are toate rădăcinile în $\overline{K}_1$.).

Aplicând apoi Lema rezultă teorema.

Proposition 2 *Orice corp finit nu este algebric închis.*

Demonstraţie. Fie $K = \{0, 1, a_1, ..., a_n\}$ şi

$$f = X(X-1)\prod_{i=1}^{n}(X - a_i) + 1\ \in K[X].$$

f nu are rădăcini în K, pentru că $f(x) = 1$, $\forall\ x \in K$. ■

9 Seminar 3

Exerciţiu 9.1 $[K : \mathbb{Q}] = 2 \Leftrightarrow K = \mathbb{Q}\left(\sqrt{d}\right)$ *(d liber de pătrate,* $\sqrt{d} \notin \mathbb{Q}$.)

Soluţie 9.1

$\Leftarrow$" $\left[\mathbb{Q}\left(\sqrt{d}\right) : \mathbb{Q}\right] = grad\ Irr\ \sqrt{d} = 2$, pentru că $Irr\ \sqrt{d} = X^2 - d$.

$\Rightarrow$" Fie $u \in K - \mathbb{Q}, [K : \mathbb{Q}] = 2$, $dim_{\mathbb{Q}} K = 2 \Rightarrow \{1, u\}$ bază în ${}_{\mathbb{Q}}K$

$$\Rightarrow K = \{a + bu |\ a, b \in \mathbb{Q}\} \Rightarrow K = \mathbb{Q}(u).$$

(sau direct: $u \in K - \mathbb{Q}, [K : \mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(u)$).
În particular,

$$u^2 \in K = \mathbb{Q}(u) \Rightarrow \exists\ a, b \in \mathbb{Q} : u^2 = a + bu$$

$$\Rightarrow \underbrace{\left(u - \frac{b}{2}\right)^2}_{= v \notin \mathbb{Q}} = \underbrace{a^2 - \frac{b^2}{4}}_{= c \in \mathbb{Q}} .$$ Deci v răd. pentru $X^2 - c \in \mathbb{Q}[X]$ şi $\sqrt{c} \notin \mathbb{Q}$.

Aşadar, $K = \mathbb{Q}(u) = \mathbb{Q}(v) \quad = \mathbb{Q}(\sqrt{c}) = \mathbb{Q}\left(\sqrt{2}\right)$ cu d liber pătrate, unde $v = u - \frac{b}{2}$.

Exerciţiu 9.2 *Fie K corp finit, $|K| = q$:*

a) *Determinaţi numărul polinoamelor de grad 2, monice, ireductibile din* $K[X]$;
b) *Determinaţi numărul polinoamelor de grad 3, monice, ireductibile din* $K[X]$.

Soluţie 9.2

a) Fie $P = X^2 + aX + b \in K[X]$, monic.
$P \longrightarrow (a,\ b) \in K^2$.
Notăm:

$$P_2 = \{P |\ P \text{ de grad } 2, \text{monic}\}, |P_2| = |K^2| = q^2.$$

Să calculăm numărul polinoamelor reductibile din P_2.
P reductibil dacă:

$$P = (X - \alpha)^2 \text{ în număr de } q,\ \alpha \in K.$$

sau

$$P = (X-\alpha)(X-\beta) \text{ în număr de } C_q^2.\ \alpha, \beta \in K\ , \alpha \neq \beta.$$

Numărul cerut este:

$$q^2 - q - C_q^2 = q(q-1) - \frac{q(q-1)}{2} = \frac{q(q-1)}{2} = \frac{q^2-q}{2}.$$

b) Notă

$$P_3 = \{X^3 + aX^2 + bX + c |\ a, b, c \in K\} \Rightarrow |P_3| = q^3.$$

Calculăm numărul polinoamelor reductibile din P_3.
Polinoamele reductibile au forma:
• $P = (X-\alpha)\underbrace{\left(X^2 + aX + b\right)}_{ired}$, $\alpha,\ a, b \in K$
$P \longrightarrow$ în număr de $q \cdot \frac{q^2-q}{2}$ (pct. **a**)).
sau
•• $P = (X-\alpha)^2 (X-\beta)$, $\alpha,\ \beta \in K$
$P \longrightarrow$ sunt q^2.
sau
••• $P = (X-\alpha)(X-\beta)(X-\gamma)$ cu $\alpha,\ \beta, \gamma \in K$ distincte.
$P \longrightarrow$ în număr de $C_q^3 = \frac{q(q-1)(q-2)}{6}$.
Deci numărul cerut este:

$$q^3 - q \cdot \frac{q^2-q}{2} - q^2 - \frac{q(q-1)(q-2)}{6} = \frac{q^3}{2} - \frac{q^2}{2} - \frac{q^3 - 3q^2 + 2q}{6}$$
$$= \frac{2q^3 - 2q}{6} = \frac{q^3 - q}{3}.$$

Exerciţiu 9.3 *Să se construiască corpuri cu* 4, 8, 9 *elemente.*

Soluţie 9.3

Un corp finit nu are caracteristica $0 \Rightarrow \exists\ p$ prim, astfel încât:

$$\mathbb{Z}_p \leq K,\ dim_{\mathbb{Z}_p} K = n \Rightarrow |K| = p^n.$$

$\forall\ x \in K,\ x = \sum_{i=1}^{n} a_i e_i, a_i \in \mathbb{Z}_p.$

Pentru $|\ K\ | = 4$ sau $|\ K\ | = 8$, caut polinoamele ireductibile de *grad* 2 sau 3 peste $\mathbb{Z}_2$.

$$\mathbb{Z}_2 \leq K = \mathbb{Z}_2(\alpha).$$

$$dim_{\ \mathbb{Z}_2} K = [\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = grad\ Irr\ \alpha = 2 \text{ sau } Irr\ \alpha = 3.$$

• $X^2 + X + 1$ nu are rădăcini în $\mathbb{Z}_2 \Rightarrow$ este ireductibil.

$$\Rightarrow K = \mathbb{Z}_2(\alpha),\ \text{cu } \alpha \text{ răd.a lui } X^2 + X + 1,\ \text{are 4 elemente.}$$

•• X^3+X+1 nu are rădăcini în $\mathbb{Z}_3 \Rightarrow$ este ireductibil

.

$$\Rightarrow K=\mathbb{Z}_2(\beta),\ \text{cu } \beta \text{ rădăcinăa lui } X^3+X+1,\ \text{are 8 elemente.}$$

••• $\mid K \mid = 9 = 3^2 \Rightarrow$ caut un polinom ireductibil de grad 2 peste $\mathbb{Z}_3$.

$$f = X^2+1 \ ired \text{ în } \mathbb{Z}_3[X].$$
$$K = \mathbb{Z}_3(\gamma), \gamma \text{ rădăcină pentru } f.$$

10 Curs 4 - Corp de descompunere

Fie K corp comutativ. Avem echivalenţa:

$$\begin{cases} \text{- } K \text{ corp algebric închis;} \\ \text{- } K \text{ nu are ext. alg. proprii;} \\ \text{- orice polinom din } K[X] \text{ are o rădăcină în } K; \\ \text{- orice polinom din } K[X] \text{ are toate rădăcinile în } K; \\ \text{- orice polinom din } K[X] \text{ se descompune în factori liniari în } K[X]; \\ \text{- singurele polinoame ireductibile din } K[X] \text{ au gradul 1.} \end{cases}$$

Definiţie 10.1 *Fie $f \in K[X]$, grad $f \geq 1$.* ***Corpul de descompunere*** *al lui f este o extindere algebrică a lui K, astfel încât:*

$$\begin{cases} \text{- conţine toate rădăcinile lui } f; \\ \text{- } f \text{ nu are toate rădăcinile în niciun subcorp propriu} \end{cases}$$

Notaţie: $\mathcal{C}_f$

$$\mathcal{C}_f = K(\alpha_1, ..., \alpha_n) \ cu \ \alpha_1, ..., \alpha_n \text{ rădăcinile lui } f.$$

Exemple
1)

$$f = X^2-2 \in \mathbb{Q}[X].\ \mathcal{C}_f = \mathbb{Q}\left(\sqrt{2}\right).$$

2)

$$f = X^4-2 \in \mathbb{Q}[X],\ f \text{ are rădăcini } \pm\sqrt[4]{2};\ \pm\ i\sqrt[4]{2}.\ \mathcal{C}_f = \mathbb{Q}\left(\sqrt[4]{2},\ i\right).$$

3)

$$f = X^4-2 \in \mathbb{R}[X] \Rightarrow \mathcal{C}_f = \mathbb{R}\left(\sqrt[4]{2},\ i\right) = \mathbb{C}.$$

Rădăcini de ordin n ale unităţii:

Fie $f = X^n - 1 \in K[X]$.

$$U_n = \{\alpha \in L |\ \alpha^n = 1\} \text{ (gradul rădăcinii).}$$

$$(U_n, \cdot) \underset{\text{finit}}{\leq} (L^*,\ \cdot).$$

U_n e generat de o rădăcină primitivă de grad n (ordin) a lui 1.
• Dacă *car* $K = 0$ sau car $K = p \nmid n$, atunci f are rădăcini distincte.
•• Dacă *car* $K = p \mid n$, atunci $f = (X^m - 1)^{p^k}$. $n = p^k m$, $p \nmid m$.

Rădăcinile lui f sunt rădăcinile lui $X^m - 1$, cu ordinul de multiplicitate p^k.
Problema se reduce la cazul $p \nmid n$.
$(U_n, \cdot)$ grup ciclic.
Numărul rădăcinilor primitive (generatori de ordin n) este:

$$\varphi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) cun = p_1^{\alpha_1}...p_k^{\alpha_k}.$$

$$x^k \text{ are ordin } n \Leftrightarrow (n,\ k) = 1. \text{ (de la grupuri ciclice).}$$

Fie α o rădăcină primitivă a lui 1.

$$Irr(\alpha,\ \mathbb{Q}) = F_n |\ X^n - 1.$$

Teorema 10.1

1) $F_n \in \mathbb{Z}[X]$;
2) *grad* $F_n = \varphi(n)$;
3) *orice rădăcină a lui* F_n *e rădăcină primitivă şi reciproc.*

Proposition 3 $X^n - 1 = \prod_{d \mid n} F_d(X)$, *pentru că* $F_d \mid \left(X^d - 1\right) \mid (X^n - 1)$ *şi* $n = \sum_{d \mid n} \underset{\text{grad } F_d}{\varphi(d)}$.

Exerciţiu 10.1 *Determinaţi diverse polinoame ciclotomice.*

$$X^2 - 1 = \underset{F_1}{(X-1)}\underset{F_2}{(X+1)}$$
$$grad\ F_2 = \varphi(2) = 2 \cdot \left(1 - \frac{1}{2}\right) = 1.$$

$$X^3-1=(X-1)\ \left(X^2+X+1\right)=F_1F_3.$$
$$grad\ F_3=3\left(1-\frac{1}{3}\right)=2.$$

$$X^4-1=(X-1)(X+1)\left(X^2+1\right)=F_1F_2F_4$$
$$grad\ F_4=4\cdot\left(1-\frac{1}{2}\right)=2\Rightarrow F_4=X^2+1.$$

$$X^5-1=(X-1)\left(X^4+X^3+X^2+X+1\right)=F_1F_5.$$
$$grad\ F_5=5\left(1-\frac{1}{5}\right)=4\Longrightarrow F_5=X^4+X^3+X^2+X+1.$$

$$X^6-1=(X-1)(X+1)\left(X^2+X+1\right)\left(X^2-X+1\right)=F_1F_2F_3F_6$$
$$grad\ F_6=6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=2\Rightarrow F_6=X^2-X+1.$$

$$X^7-1=(X-1)(X^6+X^5+...+X+1)=F_1F_7.$$
$$\text{grad}\ \ F_7=7\left(1-\frac{1}{7}\right)\Rightarrow F_7=X^6+X^5+...+X+1.$$

11 Seminar 4

Exerciţiu 11.1

i) Determinaţi polinoamele de *grad* 2 şi 3, ireductibile în $\mathbb{Z}_2[X]$.
ii) Determinaţi polinoamele de *grad* 2, ireductibile în $\mathbb{Z}_3[X]$.

Soluţie 11.1

i) $f=X^2+aX+b\in\mathbb{Z}_2[X]$, de *grad* 2.

$$f \text{ ireductibil} \Leftrightarrow\ f \text{ nu are rădăcini în } \mathbb{Z}_2.$$

$$\left.\begin{array}{l} a=b=0 \\ a=0,\ b=1\rightarrow X^2+1=(X+1)^2 \\ a=1,\ b=0 \end{array}\right\} \text{reductibile.}$$

$$a=1=b\rightarrow X^2+X+1 \textbf{ ireductibil}.$$

$f = X^3 + aX^2 + bX + c \in \mathbb{Z}_2[X]$, de *grad* 3.

$$f \text{ ireductibil} \Leftrightarrow f \text{ nu are rădăcini în } \mathbb{Z}_3.$$

$a = b = c = 0 \rightarrow$ reductibil.
$a = b = 0,\ c = 1 \rightarrow X^3 + 1$ reductibil.
$a = 0,\ b = 1,\ c = 0 \rightarrow$ reductibil.
$a = 1,\ b = c = 0 \rightarrow$ reductibil.
$a = 1,\ b = 1,\ c \in \{0, 1\} \rightarrow$ reductibil.

$$a = 0,\ b = 1,\ c = 1 \Rightarrow f = X^3 + X + 1 \textbf{ ireductibil}.$$
$$a = 1,\ b = 0,\ c = 1 \Rightarrow f = X^3 + X^2 + 1 \textbf{ ireductibil}.$$

ii) $f = X^2 + aX + b \in \mathbb{Z}_3[X]$

$$a = b = 0 \rightarrow \textbf{reductibil}.$$
$$a = 0,\ b = 1 \rightarrow X^2 + 1 \textbf{ ireductibil}.$$

$$f \text{ ireductibil} \Leftrightarrow f \text{ nu are rădăcini în } \mathbb{Z}_3.$$

$a = 1,\ b \in \{0, 1\} \rightarrow (X = -2X \text{ în } \mathbb{Z}_3[X])$ reductibil.
$a = 0,\ b = 2,\ f = X^2 + 2 = X^2 - 1$ reductibil.

$$a = 1,\ b = 2 \Rightarrow f = X^2 + X + 2 \textbf{ ireductibil.}$$

$a = 2,\ b \in \{0, 1\} \rightarrow$ reductibil.

$$a = 2,\ b = 2 \rightarrow f = X^2 + 2X + 2 \textbf{ ireductibil}.$$

Mai sunt şi alte polinoame, cu coeficientul dominant 2, asociate în divizibilicu cele de mai sus.

$$\left.\begin{array}{l} 2X^2 + 2 \\ 2X^2 + 2X + 1 \\ 2X^2 + X + 1 \end{array}\right\} \textbf{ireductibile}$$

Exerciţiu 11.2 *Rădăcinile lui* $X^n - a \in K[X]$.

Soluţie 11.2

Fie α o rădăcină a lui $X^n - a \Longrightarrow$

$$\alpha^n = a.$$

Facem substituţia $X = \alpha\ y$

$$\Rightarrow X^n - a = \alpha^n y^n - a = a\,(y^n - 1).$$

Fie ε o rădăcină primitivă a lui 1.
Atunci celelalte rădăcini ale lui 1 sunt $\{1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}\}$.
Deci

$$\mathcal{C}_{X^n-a,\ K} = K(\alpha,\ \varepsilon).$$

.

Rădăcinile lui $X^n - a$ sunt α, $\alpha\varepsilon$, ..., $\alpha\varepsilon^{n-1}$.

Exerciţiu 11.3 *Fie $K \subseteq L$ cu $[L\ :\ K] = 2$.*

i) Dacă car $K \neq 2$, atunci $\exists\ \alpha$ rădăcină pentru

$$\underset{\text{ired}}{X^2 - a} \in K[X]\ :\ L = K(\alpha);$$

ii) Dacă car $K = 2$, atunci $\exists\ \alpha$ rădăcină pentru

$$\underset{\text{ired}}{X^2 + a} \text{ sau } \underset{\text{ired}}{X^2 + X + a} \in K[X]$$

astfel încât $L = K(\alpha)$.

Soluţie 11.3

Fie $K \leq K(\beta) \leq L$, cu $\beta \notin K \Rightarrow 2 = [L\ :\ K(\beta)] \cdot \underbrace{[K(\beta) : K]}_{\neq 1}$.

$L = K(\beta)$, $[L\colon K] = 2 \Rightarrow grad\ Irr\ \beta = 2$.

$$Irr\beta = a_0 + a_1X + X^2.$$

i) *car $K \neq 2$.*

$$a_0 + a_1X + X^2 = a_0 - \underbrace{\frac{a_1^2}{4}}_{-a} + \underbrace{\left(\frac{a_1}{2} + X\right)^2}_{Y}$$

$\alpha = \beta + \frac{a_1}{2}$ rădăcina ecuaţiei $Y^2 - a = 0$.

$$L = K(\beta) = K(\alpha).$$

ii)
$$\begin{cases} a_1 = 0 \Rightarrow Irr\ \beta = a_0 + X^2 \\ a_1 \neq 0 \Rightarrow a_0 + a_1X + X^2 = a_1^2 \left(\underbrace{\frac{a_0}{a_1^2}}_{a} + \underbrace{\frac{X}{a_1}}_{Y} + \frac{X^2}{a_1^2} \right) \end{cases}$$

$\alpha = \frac{\beta}{a_1}$ rădăcină pentru $a + Y + Y^2$.

$$K(\alpha) = K(\beta).$$

Exerciţiu 11.4 *Determinaţi corpurile de descompunere pentru:*

i) $f = X^2 + 1 \in \mathbb{Z}_3[X]$ $(\mathbb{Z}_5[X],\ \mathbb{Q}[X])$;
ii) $f = X^2 - 2 \in \mathbb{Q}[X]$ $(\mathbb{R}[X])$;
iii) $f = X^4 + 1 \in \mathbb{Z}_3[X]$.

Soluţie 11.4

i) f ireductibil în $\mathbb{Z}_3[X]$ (nu are rădăcini).
$\mathbb{Z}_3[X]/_{(f)}$ corp în care are o rădăcină, deci le are pe ambele.

În $\mathbb{Z}_5[X]$:
$$f\left(\hat{2}\right) = \hat{0} \Rightarrow \hat{2} \text{ rădăcină}$$
$$f\left(\hat{3}\right) = \hat{0} \Rightarrow \hat{3} \text{ rădăcină}$$

Deci
$$\mathcal{C}_{f,\,\mathbb{Z}_5} = \mathbb{Z}_5.$$

În $\mathbb{Q}[X]$: f ireductibil $\Rightarrow$
$$\mathcal{C}_{f,\,\mathbb{Q}} = \mathbb{Q}[X]/(f) \simeq \mathbb{Q}(i).$$

ii) $f = X^2 - 2$.

În $\mathbb{Q}[X]$:
$$\mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}\left(\sqrt{2}\right).$$

În $\mathbb{R}[X]$:
$$\mathcal{C}_{f,\,\mathbb{R}} = \mathbb{R}\left(\sqrt{2}\right) = \mathbb{R}.$$

iii) $f = X^4 + 1 \ \in \mathbb{Z}_3[X]$.
$$f = \left(X^2 + X + 1\right)\left(X^2 + 2X + 2\right) \in \mathbb{Z}_3[X].$$
Fie α rădăcină pentru $X^2 + X + 2 \Rightarrow \alpha + 1$ rădăcină pentru $X^2 + 2X + 2$
$$\Rightarrow \mathcal{C}_f = \mathbb{Z}_3(\alpha) = \mathbb{Z}_3[X]/\left(X^2 + X + 2\right).$$

12 Curs 5 - Închiderea algebrică a unui corp. Corpul de descompunere al unui polinom

Teorema 12.1 ***(Teorema de unicitate)***

Fie $\sigma: K \longrightarrow K^{'}, \overline{\sigma}: K[X] \longrightarrow K^{'}[X]$, *unde* σ *izomorfism şi* $\overline{\sigma}$ *izomorfism de inele. Fie* $Q \neq S \subset K[X] \rightsquigarrow \overline{\sigma}(S)$, *astfel încât* $\forall\ f \in S$, cu *grad* $f > 0$. *Fie* $F = C_S$ *şi* $F^{'} = C_{\overline{\sigma}(S)}$. *Atunci* $\exists\ \tau : F \to F^{'}$, *astfel încât* $\tau|_K = \sigma$.

Demonstraţie. I) Pentru $S = \{f\}$, demonstrăm prin inducţie după gradul lui f.

• *grad* $f = 1 \Rightarrow \left\{ \begin{array}{l} F = K \\ F^{'} = K^{'} \end{array} \right.$ şi $\tau = \sigma$.

•• *grad* $f = n > 1$. Presupunem afirmaţia adevărată pentru polinoame de *grad* $\leq n-1$.

Fie α rădăcină a lui f, $\alpha \in F - K$. $\alpha^{'}$ rădăcină pentru $\overline{\sigma}(f)$, $\alpha^{'} \in F^{'} - K^{'}$.

Aplicaţia $\tau_1 :\ K(\alpha) \longrightarrow K^{'}\left(\alpha^{'}\right)$

$$k \rightsquigarrow\ \sigma(k)$$
$$\alpha \rightsquigarrow \alpha^{'}$$

τ_1 izomorfism, deoarece $[K(\alpha)\ :\ K] = \left[K^{'}\left(\alpha^{'}\right)\ :\ K^{'}\right]$. τ_1 extinde σ.

Atunci:

$$f = (X - \alpha)\, h \in K(\alpha)[X].$$

$$\overline{\tau}_1(f) = \left(X - \alpha^{'}\right)\overline{\tau}_1(h).$$

$$grad\ h = grad\ f - 1.$$

Conform ipotezei inductive,

$$\exists\ \tau:\ F \longrightarrow F^{'}, \quad \left.\begin{array}{l} \tau/_{K(\alpha)} = \tau_1 \\ \text{Dar } \tau_1/_K = \sigma \end{array}\right\} \Rightarrow \tau/_K = \sigma.$$

II) Fie

$$\mathcal{S} = \{\left(E, E^{'}, \tau\right) | K \leq E \leq F, K^{'} \leq E^{'} \leq F^{'},\ \exists \tau: E \to E^{'}, \tau/_K = \sigma\}$$

Ordonăm $\mathcal{S}$ astfel:

$$\left(E_1, E_1^{'}, \zeta_1\right) \leq \left(E_2,\ E_2^{'}, \zeta_2\right) \Leftrightarrow \left\{ \begin{array}{l} E_1 \leq E_2 \\ E_1^{'} \leq E_2^{'} \\ \tau_2/_{E_1} = \tau_1 \end{array} \right.$$

Arătăm că orice lanţ al lui $(\mathcal{S},\ \leq)$ admite un majorant.

Fie lanţul $\left(E_1, E_1^{'}, \zeta_1\right) \leq \left(E_2, E_2^{'}, \zeta_2\right) \leq ...$

şi $\left\{ \begin{array}{l} \left.\begin{array}{c} E^* = \underset{i \geq 1}{\cup} E_i \\ E^{'*} = \underset{i \geq 1}{\cup} E_i^{'} \end{array}\right\} \text{corpuri} \quad K \leq E^* \leq F\ ,\ K^{'} \leq E^{'*} \leq F^{'}. \\ \tau^*(x) = \tau_i(x) \text{ pentru } x \in E_i \text{ } (i \text{ minim cu această proprietate}),\ \tau^*(x) \text{ izomorfism.} \end{array} \right.$

Rezultă că: $\left(E^*, E^{'*}, \zeta^*\right)$ este majorant pentru lanţul dat.

Conform lemei lui Zorn, $\left(F_1, F_1^{'}, \varphi\right)$ este element maximal în $\mathcal{S}$.

Arătăm că: $F_1 = F;\ F_1^{'} = F^{'}$.

Vom proceda prin reducere la absurd**.**

Presupunem $F_1 \subsetneq F = \mathcal{C}_S \Rightarrow \exists\ f \in S$ astfel încât f nu are toate rădăcinile în F_1. Rezultă că:

$$F_1^{'} \lneq \mathcal{C}_f \leq F \quad (f \in S \subset K[X] \subset F_1[X])$$

Analog, $F_1^{'} \lneq \mathcal{C}_{\overline{\varphi} f} \leq F^{'}$ unde φ: $F_1 \longrightarrow F_1^{'}$.Conform primei părţi,

$$\exists\ \tau\colon\ \tau_f \simeq \mathcal{C}_{\overline{\varphi} f},\ \tau/_{F_1} = \varphi.$$

Dar$(\mathcal{C}_f,\ \mathcal{C}_{\overline{\varphi} f},\ \tau)$ depăşeşte strict elementul maximal, fals!

Deci, $F_1 = F$, $F_1^{'} = F$! ■

Corolar 2 *Fie $f \in K[X]$, grad $f \geq 2$. Atunci oricare două corpuri de descompunere ale lui f sunt K- izomorfisme.*

Demonstraţie. Iau $K^{'} = K$, $S = \{f\}$. $\sigma = 1_K \Rightarrow \exists\ \tau\ :\ F \longrightarrow F^{'}$ ■

$F, F^{'}$ corpuri de descompunere pentru f.

$\tau/_K = 1_K \Rightarrow \tau \quad K-$izom.

Corolar 3 *Fie K corp comutativ. Atunci oricare două închideri algebrice ale lui K sunt K - izom.*

Demonstraţie. Fie $\sigma = 1_K$ şi $S = K[X] - K$. ■

Tipuri de extinderi algebrice

Separabilă : Fie $K \leq L$, $a \in L$. a **sep**$/_K$ dacă $a\ alg/_K$ şi m_a nu are rădăcini multiple. Spunem că $K \leq L$ **separabil** dacă $\forall a \in L$, $a\ sep/_K$.

Normală: Fie $K \leq L$. L **normală** peste K dacă:

$$L\ alg/_K \text{ şi } \left.\begin{array}{l} \forall\ f \in K[X],\ f \text{ ireductibil} \\ f(\alpha) = 0,\ \alpha \in L \end{array}\right\} \Rightarrow \mathcal{C}_f \subseteq L.$$

Galois: Spunem că extinderea $K \leq L$ este **Galois** dacă este finită, separabilă şi normală.

Radicală: Extinderea $K \leq L$ este **radicală** dacă este: **simplă**:

$$K \leq \mathcal{C}_{X^n - a, K}$$

şi

$$K \leq L\colon\ \exists\ K_0 = K,\ K_1, ..., K_n = L;\ K_i \leq K_{i+1} \text{ radicală simplă.}$$

Corpuri finite

Fie K corp finit, *car* $K = p$. $\mathbb{Z}_p \leq K$.
Dacă *dim* $_{\mathbb{Z}_p} K = n$, atunci $\mid K \mid = p^n$.
(elementele lui K sunt combinaţii liniare din elementele bazei; coeficienţi din $\mathbb{Z}_p$).

Teorema 12.2 *Fie K corp finit, car $K = p \Leftrightarrow K = \mathcal{C}_{X^{p^n}-X,\ \mathbb{Z}_p}$.*

Demonstraţie. $\Rightarrow$"$(K^*,\ \cdot)$ are $p^n - 1$ elemente $\Rightarrow$

$$\alpha^{p^n-1} = 1,\ \forall\ \alpha \in K^* \Rightarrow \alpha^{p^n} = \alpha,\ \forall\ \alpha \in K \Rightarrow K \subseteq \mathcal{C}_{X^{p^n}-X,\ \mathbb{Z}_p}.$$

Polinomul $X^{p^n} - X$ are derivata -1, deci are p^n rădăcini distincte. Mai mult,

$$\mathcal{C}_{X^{p^n}-X,\ \mathbb{Z}_p} = \{\text{rădăcinile lui } X^{p^n} - X\}.$$

corp: α, β rădăcini pentru $X^{p^n} - X \Rightarrow$

$$\alpha^{p^n} = \alpha,\ \beta^{p^n} = \beta \Rightarrow (\alpha \div \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$$
$$(\alpha\ \beta)^{p^n} = \alpha^{p^n}\beta^{p^n},\ \alpha \neq 0 \Rightarrow \alpha^{-1} \text{ rădăcină.}$$

În puls,

$$|\mathcal{C}_{X^{p^n}-X}|\ = p^n,\ |K|\ = p^n,\ K \subseteq \mathcal{C}_{X^{p^n}-X} \Rightarrow K = \mathcal{C}_{X^{p^n}-X}.$$

$\Leftarrow$" Ca mai sus, $\mathcal{C}_{X^{p^n}-X}$ are p^n elemente. ■

Consecinţe:

1. $\forall\ p$ prim, $\forall\ n \in \mathbb{N}$ există corpuri cu p^n elemente;
2. Oricare două corpuri cu p^n elemente sunt izomorfe (corpuri de descompunere pentru acelaşi polinom).

Subcorpurile unui corp finit

Teorema 12.3 *Fie K corp finit, $\mid K \mid = p^n$, $K_1 \leq K$. Atunci $\exists\ s \mid n :\ \mid K_1 \mid = p^s$ şi reciproc.*

Demonstraţie.

$$\mathbb{Z}_p \leq K_1 \leq K \Rightarrow \underbrace{[K_1\ :\ \mathbb{Z}_p]}_{s} \mid \underbrace{[K\ :\ \mathbb{Z}_p]}_{n}$$
$$K_1 = \mathcal{C}_{X^{p^s}-X, \mathbb{Z}_p}.$$

. ■

Teorema 12.4 ***(Wedderburn)*** *Orice corp finit este comutativ.*

13 Seminarii 5, 6

Exerciţiu 13.1 *Să se determine corpurile de descompunere peste* $\mathbb{Q}$ *şi peste* $\mathbb{R}$ *pentru polinoamele:*

$$X^3+1,\ X^4-2,\ X^4+2,\ X^4+X^2+1.$$

Soluţie 13.1

a)

$$X^3+1=(X+1)\left(X^2-X+1\right) \text{ cu rădăcinile } -1,\ \frac{1\pm i\sqrt{3}}{2}.$$
$$\mathcal{C}_{f,\,\mathbb{Q}}=\mathbb{Q}\left(i\sqrt{3}\right),\ \mathcal{C}_{f,\,\mathbb{R}}=\mathbb{R}\left(i\sqrt{3}\right)=\mathbb{C}.$$

b)

$$X^4-2 \text{ cu rădăcinile } \pm\sqrt[4]{2},\ \pm i\sqrt[2]{4}.$$
$$\mathcal{C}_{f,\mathbb{Q}}=\mathbb{Q}\left(\sqrt[4]{2},\ i\right),\ \mathcal{C}_{f,\,\mathbb{R}}=\mathbb{R}\left(\sqrt[4]{2},\ i\right)=\mathbb{C}$$

c)

$$X^4+2=0\Rightarrow X^4=-2=2i^2\Rightarrow X^2=\pm i\sqrt{2}.$$

Caz **I** : Dacă $X^2=i\sqrt{2}$.

$$a+bi\in\mathbb{C}:\ \ (a+bi)^2=i\sqrt{2}.$$
$$\Rightarrow\left\{\begin{array}{l}a^2=b^2\\2ab=\sqrt{2}\end{array}\right.\Rightarrow\left\{\begin{array}{l}a=\pm\,b\\a=\frac{1}{b\sqrt{2}}\end{array}\right.$$

.

Pentru $a=b\Rightarrow$

$$a^2=\frac{1}{\sqrt{2}}\Rightarrow a=b=\pm\frac{1}{\sqrt[4]{2}}.$$

Pentru $a=-b\Rightarrow$

$$a^2=-\frac{1}{\sqrt{2}}\Rightarrow a\notin\mathbb{R} \text{ fals!}$$

Obţinem soluţiile:

$$x_{1,\,2}=\pm\frac{1}{\sqrt[4]{2}}(1+i).$$

Caz **II** : Dacă $X^2=-i\sqrt{2}$.

$$a+bi\in\mathbb{C}\ :(a+bi)^2=-i\sqrt{2}.$$
$$\Rightarrow\left\{\begin{array}{l}a^2=b^2\\2ab=-\sqrt{2}\end{array}\right.\Rightarrow\begin{array}{l}a=\pm\,b\\a=-\frac{1}{b\sqrt{2}}\end{array}\ .$$

Pentru $a = b \Rightarrow$

$$a^2 = -\frac{1}{\sqrt{2}} \Rightarrow a \notin \mathbb{R} \text{ fals!}$$

Pentru $a = -b \Rightarrow$

$$a^2 = \frac{1}{\sqrt{2}} \Rightarrow a = -b = \pm\frac{1}{\sqrt[4]{2}}.$$

Obţinem soluţiile:

$$x_{3,\,4} = \pm\frac{1}{\sqrt[4]{2}}(1-i).$$

Observăm că:

$$\frac{x_1}{x_3} = \frac{1+i}{1-i} = \frac{(1+i)^2}{2} = i.$$

$$\mathcal{C}_{f,\,\mathbb{Q}} = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}\left(i,\ \sqrt[4]{2}\right)$$
$$\mathcal{C}_{f,\,\mathbb{R}} = \mathbb{R}\left(i,\ \sqrt[4]{2}\right) = \mathbb{C}.$$

d) $X^4 + X^2 + 1$.
Facem substituţia

$$X^2 = Y \Rightarrow Y^2 + Y + 1 = 0$$

cu rădăcinile:

$$y_{1,\,2} = \frac{-1 \pm i\sqrt{3}}{2}.$$

Fie acum $X = a + bi \in \mathbb{C} \Rightarrow (a+bi)^2 = \frac{-1\pm i\sqrt{3}}{2}$.

$$\Rightarrow \begin{cases} a^2 - b^2 = -\frac{1}{2} \\ 2ab = \pm\frac{\sqrt{3}}{2} \Rightarrow b = \pm\frac{\sqrt{3}}{4a} \end{cases} \Rightarrow a^2 - \frac{3}{16a^2} = -\frac{1}{2}$$

$$\Rightarrow 16a^4 + 8a^2 - 3 = 0 \Rightarrow \left(4a^2+1\right)^2 = 4 \Rightarrow\ 4a^2 + 1 = \pm 2 \Rightarrow$$

$$\Rightarrow 4a^2 = 1 (\text{pentru că } a \in \mathbb{R}).$$

$$\Rightarrow a = \pm\frac{1}{2} \Rightarrow b = \pm\frac{\sqrt{3}}{2}.$$

Obţinem soluţiile:

$$x_{1,\,2} = \pm\frac{1}{2}\left(1+\sqrt{3}i\right),\ x_{3,\,4} = \pm\frac{1}{2}\left(1-\sqrt{3}i\right).$$
$$\mathcal{C}_{f,\,\mathbb{Q}} = \mathbb{Q}\left(i\sqrt{3}\right),\ \mathcal{C}_{f,\,\mathbb{R}} = \mathbb{R}\left(i\sqrt{3}\right) = \mathbb{C}.$$

Exerciţiu 13.2 *Să se arate că* $\mathbb{Q}\left(\sqrt{2}\right) \ncong \mathbb{Q}\left(\sqrt{3}\right)$.

Soluţie 13.2 *Presupunem că* $\exists\ f : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}\left(\sqrt{3}\right)$, *f izomorfism.*

$$f\left(\sqrt{2}\right) = a + b\sqrt{3}.$$

$$2 = f(2) = \left(a + b\sqrt{3}\right)^2 \Rightarrow \begin{cases} a^2 + 3b^2 = 2 \\ ab = 0 \end{cases} \Rightarrow a = 0 \text{ sau } b = 0 \text{ fals!}$$

Exerciţiu 13.3 *Să se arate că:* $\forall\ n \in \mathbb{N}^*$, $\forall\ p \in \mathbb{N}$, *prim.*

i) $\exists$ *polinom de grad n, ireductibil peste* $\mathbb{Z}_p$;
ii) $\exists$ *extinderea* $\mathbb{Z}_p \leq K$, *astfel încât* $[K : \mathbb{Z}_p] = n$.

Soluţie 13.3

Consider $K = \mathcal{C}_{X^{p^n}-X,\ \mathbb{Z}_p}$, $\mid K \mid = p^n$ (rădăcina lui $X^{p^n} - X$).
K corp finit $\Rightarrow (K^*,\ \cdot)$ grup ciclic.

$$K^* = [a] \Rightarrow K = \mathbb{Z}_p(a).$$

Din $[K : \mathbb{Z}_p] = n \Rightarrow$

$$[\mathbb{Z}_p(a) : \mathbb{Z}_p] = n \Rightarrow grad\ Irr\,(a, \mathbb{Z}_p) = n.$$

Polinomul căutat este $Irr\ a$, unde $[a] = K^*$.

Exerciţiu 13.4 *Fie P un corp prim şi fie* $n \in \mathbb{N}^*$. *Atunci:*

i) $\exists$ *polinom ireductibil de grad n din* $P[X]$;
ii) $\exists$ *extindere* $P \leq K$ *de grad n.*

Soluţie 13.4

Avem $P \simeq \mathbb{Q}$ sau $P \simeq \mathbb{Z}_p$ (exerciţiul precedent).
Pentru $\mathbb{Q}$. Fie

$$f = X^n + pX^{n-1} + ... + pX + p\ ,\ p \text{ prim.}$$

Aplic **Eisenstein** $\Rightarrow f$ ireductibil. $grad\ f = n$. (sau $f = X^n - 2$).
Fie a rădăcină pentru $f \Rightarrow$

$$f = Irr\ a \text{ şi } K = \mathbb{Q}(a).$$

Exerciţiu 13.5 *Determinaţi corpul de descompunere pentru:*

$$\underbrace{\left(X^3+X^2+1\right)}_{g}\underbrace{\left(X^3+X+1\right)}_{h}\in\mathbb{Z}_2\left[X\right]\ .$$

Soluţie 13.5

Polinoamele g, h sunt ireductibile în $\mathbb{Z}_2\left[X\right]$. Fie α o rădăcină a lui g. Verific dacă şi celelalte două rădăcini ale lui g sunt în $\mathbb{Z}_2\left(\alpha\right)$.

$$\alpha^3+\alpha^2+1=0\Rightarrow\alpha^3=\alpha^2+1 \qquad (\mathbf{1})$$

Elementele lui $\mathbb{Z}_2\left(\alpha\right)$ au forma:

$$a+b\alpha+c\alpha^2,\ a,b,c\in\mathbb{Z}_2\ (grad\ Irr\ \alpha=3).$$

Avem:

$$\alpha^6=\left(\alpha^2+1\right)^2=\alpha^4+1\underset{(\mathbf{1})}{=}\alpha^3+\alpha+1.$$
$$\alpha^4=\alpha^3+\alpha\Rightarrow g\left(\alpha^2\right)=\alpha^6+\alpha^4+1=0\Rightarrow\alpha^2\text{ rădăcină.}$$

Aşadar rezultă că g are toate rădăcinile în $\mathbb{Z}_3\left(\alpha\right)$.
Ca mai sus, dacă β e rădăcină pentru h, atunci β^2 rădăcină pentru $h\Rightarrow$

$$\mathcal{C}_{h,\ \mathbb{Z}_2}=\mathbb{Z}_2\left(\beta\right).$$

$$(\beta^3=\beta+1\Rightarrow\beta^6+\beta^2+1=\left(\beta+1\right)^2+\beta^2+1=0).$$

Legătura între β şi α. β poate fi $\alpha+1$.
Deci $\mathcal{C}_{gh,\ \mathbb{Z}_2}=\mathbb{Z}_2\left(\alpha\right)$.

Exerciţiu 13.6 *Fie $\mathbb{R}\leq K$ extindere finită. Atunci $\exists\ n\ :\ [K\ :\ \mathbb{R}]=2n$.*

Soluţie 13.6 *Presupunem $[K\ :\ \mathbb{R}]=2n+1,\ \ n\neq0$ şi fie $a\in K-\mathbb{R}\Rightarrow$*

$$\mathbb{R}\leq\mathbb{R}\left(a\right)\leq K\Rightarrow2n+1=[K\ :\ \mathbb{R}\left(a\right)]\cdot\underbrace{[\mathbb{R}\left(a\right)\ :\ \mathbb{R}]}_{\text{grad }Irr\ a}$$

$\Rightarrow$ *grad Irr a* impar$\Rightarrow$ *Irr a* are rădăcină reală, contradicţie (*Irr a* ireductibil).

Exerciţiu 13.7 *Fie $f=X^8-X$. Determinaţi $\mathcal{C}_{f,\ \mathbb{Q}}$ şi $\mathcal{C}_{f,\ \mathbb{Z}_2}$.*

Soluţie 13.7

a)

$$f = X(X-1)\left(X^6+X^5+X^4+X^3+X^2+X+1\right).$$

Pentru $f \in \mathbb{Q}[X]$,

$$f = X(X-1)F_7.$$

$$\mathcal{C}_{f,\,\mathbb{Q}} = \mathbb{Q}(\varepsilon),$$

ε rădăcină pentru F_7 şi $Irr\ \varepsilon = F_7$. (ε rădăcină primitivă pentru X^7-1).

b)

$$f = X(X-1)\underbrace{\left(X^6+X^5+X^4+X^3+X^2+X+1\right)}_{gh},$$

unde

$$g = X^3+X^2+1 \text{ şi } h = X^3+X+1.$$

Deci $\mathcal{C}_{f,\,\mathbb{Z}_2} = \mathbb{Z}_2(\alpha)$, cu α rădăcina lui X^3+X+1.

Exerciţiu 13.8 *Arătaţi că* $\mathbb{Q}\left(\sqrt{3},\ i\right) = \mathbb{Q}\left(\sqrt{3}+i\right)$.

Soluţie 13.8

$\dim_{\mathbb{Q}} \mathbb{Q}\left(\sqrt{3},\ i\right) = 4$ şi $\sqrt{3}+i \in \mathbb{Q}\left(\sqrt{3},\ i\right)$.

Arăt că $\dim_{\mathbb{Q}} \mathbb{Q}\left(\sqrt{3}+i\right) = 4$ adică $grad\ Irr\left(\sqrt{3}+i\right) = 4$.

$$a = \sqrt{3}+i \Rightarrow \left(a-\sqrt{3}\right)^2 = -1 \Rightarrow 2\sqrt{3}a = a^2+4$$

$$\Rightarrow a \text{ rădăcină pentru } X^4-4X^2+16 \in \mathbb{Q}[X] \text{ ireductibil } (R.A)$$

Exerciţiu 13.9 *Fie* $\alpha\ alg/_K$ *cu grad* $Irr\ \alpha = n$ *şi* $\beta \in K(\alpha)$. *Atunci grad* $Irr\ \beta \mid n$.

Soluţie 13.9

$$K \leq K(\beta) \leq K(\alpha).$$

$$\underbrace{[K(\alpha)\ :\ K]}_{n=\text{grad } Irr\ \alpha} = [K(\alpha)\ :\ K(\beta)]\ \cdot \underbrace{[K(\beta)\ :\ K]}_{\text{grad } Irr\ \beta}$$

Exerciţiu 13.10 *Fie* $K \leq L \leq E$, $\alpha \in E$, $\alpha\ alg/_K$. *Atunci*

$$[L(\alpha)\ :\ L] \leq [K(\alpha)\ :\ K].$$

Soluţie 13.10

$$[L(\alpha)\ :\ L] = grad\ Irr(\alpha,\ L),\ [K(\alpha)\ :\ K] = \text{grad } Irr(\alpha,\ K).$$

$$K \leq L \Rightarrow Irr(\alpha,\ L) \mid \underbrace{Irr(\alpha,\ K)}_{\in\ K[X] \subset L[X]}$$

Rezultă că:

$$\text{grad } Irr(\alpha,\ L) = [L(\alpha) : L] \leq [K(\alpha) : K] = \text{grad } Irr(\alpha,\ K).$$

14 Cursuri 6, 7 - Extinderi separabile

$K \leq L$, $a \in L$.

Definiţie 14.1 *Spunem că a este* ***separabil*** *peste K şi notăm: a* $\mathbf{sep}/_K$, *dacă a* $alg/_K$ *şi Irr a nu are rădăcini multiple.*

Observaţie 14.1

a rădăcină multiplă pentru f de multiplicitate $t \Rightarrow (X-a)^t \mid f$ şi $(X-a)^{t+1} \nmid f$

Teorema 14.1 *Dacă avem car* $K = 0$, *atunci a* $sep/_K \Leftrightarrow a\ alg/_K$.

Lemma 4 $f \in K[X]$ *nu are rădăcini multiple* $\Leftrightarrow \left(f,\ f'\right) \neq 1$ *(nu contează car K).*

Demonstraţie.

$\Rightarrow$"

$f = (X-a)^t g \Rightarrow f' = t(X-a)^{t-1} g + (X-a)^t g \Rightarrow f(a) = f'(a) = 0.(t \geq 2)$

Obţinem că $(X-a) \mid \left(f,\ f'\right)$.

$\Leftarrow$" $\exists\ a$ astfel încât $(X-a) \mid \left(f,\ f'\right) \Rightarrow f(a) = f'(a) = 0.$

$$\Downarrow$$

$$(X-a) \mid g \Rightarrow (X-a)^2 \mid f. \qquad \blacksquare$$

Demonstraţie. (teoremă) $a\ alg/_K \Rightarrow a\ sep/_K$. $\blacksquare$

Observaţie 14.2 f *ired. din* $K[X] \Rightarrow f$ *nu are rădăcini multiple.*

Într-adevăr, dacă presupunem că f *are rădăcini multiple* $\Rightarrow$

$$\left(f,\ f'\right) \neq 1.$$

Cum f *ireductibil şi grad* $f' <$ *grad* f *rezultă că* $f \mid f'$. *Aşadar* $f' = 0$.

Dar $f = a_n X^n + ... \Rightarrow n\ a_n = 0$ *şi car* $K = 0$ *fals.* $a_n \neq 0$.

Deci, f *nu are rădăcini multiple* $\Rightarrow a\ sep/_K$.

În particular, $f = Irr\ a$.

Teorema 14.2 *car* $K = p$, $f \in K[X]$, f *ireductibil (nu neaparat Irr a).* f *are rădăcini multiple* $\Leftrightarrow \exists\ g \in K[X]$, $f = g(X^p)$

Demonstraţie. $\Rightarrow$" f are rădăcini multiple $\Rightarrow f^{'}=0$ (ca mai sus).

$$f=a_nX^n+...+a_2X^2+a_1X+a_0$$
$$f'=n\ a_nX^{n-1}+...+2a_2X+a_1.$$

Cum $f'=0\Rightarrow i\ a_i=0,\ \forall\ i=1,\ n$ şi folosind ipoteza,

$$carK=p\Rightarrow a_i=0,\ \text{dacă}\ p\nmid i.$$

Rezultă că:

$$f=a_{p^t}X^{p^t}+...+a_pX^p+a_0.$$

Fie

$$g=a_{p^t}X+...+a_pX+a_0\in K[X]\Rightarrow f=g\left(X^p\right).$$

$\Leftarrow$" Din $f=g\left(X^p\right)\Rightarrow$

$$f=a_{p^t}X^{p^t}+...+a_pX^p+a_0\Rightarrow f^{'}=0\Rightarrow\left(f,\ f^{'}\right)=f\neq 1$$
$$\Rightarrow f \text{ are rădăcini multiple.}$$

■

Definiţie 14.2 *Un **corp perfect** este un corp comutativ, în care orice element algebric este separabil.*

Teorema 14.3 *Fie K corp comutativ, car $K=p$. K perfect $\overset{RA}{\underset{RA}{\Leftrightarrow}}$ $K^p=K$.*

Demonstraţie.
$\Rightarrow$" Fie

$$\nu:\ K\longrightarrow K$$
$$x\rightsquigarrow x^p.$$

ν morf $\Rightarrow K^p\leq K$. Presupunem:

$$K^p\neq K\Rightarrow\exists\ a\in K,\ a\neq b^p,\ \forall\ b\in K.$$

Rezultă că X^p-a nu are rădăcini în K.
Fie $\beta\notin K\Rightarrow$

$$a=\beta^p\Rightarrow X^p-a=(X-\beta)^p.$$

Atunci $Irr\ \beta=(X-\beta)^t$, cu $2\leq t\leq p$.
$\Rightarrow p\ alg$, dar nu e sep (pentru că $\beta\notin K$) $\Rightarrow K$ nu e perfect, fals.
Deci, $K^p=K$.
$\Leftarrow$" Presupunem $\exists\ a\ alg/_K, a$ nu e $sep/_K\Rightarrow Irr\ a$ are rădăcini multiple.

Din teorema anterioară, rezultă că

$$Irr\ a = X^{np} + ... + a_1 X^p + a_0 \text{ şi } K^p = K \Rightarrow a_i = b_i^p$$
$$\Rightarrow Irr\ a = (b_n X^n + ... + b_1 X + b_0)^p,$$

unde $b_n = 1$ şi $X^n + ... + b_1 X + b_0 \in K[X]$.
Deci, K perfect. ■

Corolar 4 *Orice corp finit este perfect.*

Demonstraţie.

$$\nu:\ K \longrightarrow K$$
$$x \rightsquigarrow x^p$$

ν este injectiv, fiind morfism şi cum $\mid K \mid$ finit $\Rightarrow \nu$ surjectiv $\Rightarrow K^p = K$.
Deci, K perfect. ■

Exemplu de corp care nu este perfect: $\mathbb{Z}_p(X)$.

Fie

$$f = Y^p - X \in \mathbb{Z}_p(X)[Y],\ f \text{ ireductibil.}$$

Aplicăm criteriul lui **Eisenstein,** $X \in \mathbb{Z}_p[X]$ prim.
f are rădăcini multiple, $f = Irr\ y$, cu rădăcini pentru $f \Rightarrow$

$$y \text{ nu e } sep/_{\mathbb{Z}_p(X)}$$

sau:

$$(\mathbb{Z}_5(X))^5 = \mathbb{Z}_5\left(X^5\right) \Rightarrow \mathbb{Z}_5(X).$$

Avem $\mathbb{Z}_5^5 = \mathbb{Z}_5$.

Lemma 5 $K \underset{alg}{\leq} L_1 \underset{alg}{\leq} L_2$, $\alpha \in L_2, \alpha\ sep/_K$. *Atunci* $\alpha\ sep/_{L_1}$

$(\Rightarrow L_2\ sep/_K \Rightarrow L_2\ sep/L_1)$

Demonstraţie.

$$Irr(\alpha, L_1)\ \mid Irr(\alpha,\ K),$$

$Irr(\alpha,\ K)$ nu are rădăcini multiple.
Rezultă că $Irr(\alpha, L_1)$ n-are rădăcini multiple. ■

Corolar 5 *Orice extindere algebrică a unui corp perfect este un corp perfect.*

Demonstraţie. Fie K corp perfect, $K \underset{alg}{\leq} L_1$. Să arătă că L_1 perfect, adică:

$$L_2 \ alg/_{L_1} \Rightarrow L_2 \ sep/_{L_1}.$$

Avem $K \underset{alg}{\leq} L_1 \underset{alg}{\leq} L_2$.
K perfect $\Rightarrow$

$$L_2 sep/_K \overset{\text{Lemă}}{\Longrightarrow} L_2 sep/_{L_1}.$$

■

Lemma 6 *car* $K = p$, $a \in K$, $X^p - a$ *nu are rădăcini în* K. *Atunci* $X^p - a$ *ired în* $K[X]$.

Teorema 14.4 $K \underset{alg}{\leq} L$, *car* $K = p$.

a) $L \ sep/_K \overset{\text{RA}}{\Longrightarrow} L = K(L^p)$;
b) $[L : K] = n$ *şi* $L = K(L^p) \overset{\text{RA}}{\Longrightarrow} L \ sep/_K$.

Demonstraţie. a) $K \leq K(L^p) \leq L \ sep/_K \overset{\text{Lema 1}}{\Longrightarrow} L \ sep/_{K(L^p)}$.
Presupunem $K(L^p) \neq L \Rightarrow$

$$\exists \ a \in L - K(L^p), \ a^p \in K(L^p).$$

Fie $f = X^p - a^p \in K(L^p)[X]$ nu are rădăcini în $K(L^p) \overset{\text{Lema 2}}{\Longrightarrow} f$ ireductibil în $K(L^p)[X]$.

$$f = g(X^p) \in \underset{car\ p}{K(L^p)[X]}.$$

Rezultă că f are rădăcini multiple, $f = Irr \ a \Rightarrow a$ nu e $sep|_K$, fals!
b) Presupunem

$$\exists \ b \in L, \ b \ nesep/_K, \ b \ alg/_K \Rightarrow m_b = Irr \ b$$

$$Irr \ b = g(X^p) \Rightarrow grad \ Irr \ b = p \cdot m \Rightarrow \{1, b, b^2, ..., b^m\} \text{ liniar independente}|_K$$

$$[L : K] = n \text{ o completez la o bază în } {}_K L.$$

$$\underset{\text{bază}}{B} = \{1, b, ..., b^m, y_1, ..., y_k\}.$$

$L = K(L^p) \Rightarrow B^p$ e sistem de generatori în L, pentru că $K(L^p) = L$ e format din combinaţii liniare de elemente din L^p, cu coeficienţi din K.
Deoarece $|B^p| = n \ \Rightarrow B^p$ bază în ${}_K L$,

$$B^p = \{1, b^p, ..., b^{p^m}, \ y_1^p, ..., \ y_k^p\}.$$

$$grad \ Irr \ b = p^m \Rightarrow 1, b^p, ..., b^{p^m} \text{ liniar independente.}$$

■

Corolar 6 *$K \leq L$, car $K = p$. $\alpha \in L$, $\alpha\ alg/_K$. Atunci:*

1) $\alpha\ sep/_K \Leftrightarrow K(\alpha) K(\alpha^p)$.
2) $\alpha\ sep/_K \Rightarrow K(\alpha)\ sep/_K$.
Demonstraţie. 1) $\Rightarrow$"

$$K \leq K(\alpha^p) \leq L,\ \alpha\ sep/_K \Rightarrow \alpha\ sep/_{K(\alpha^p)}.$$

Presupunem că $\alpha \notin K(\alpha^p)$.
Fie $f = X^p - \alpha^p = (X-\alpha)^p \Rightarrow Irr \mid f$, ireductibil.(Lema 2). (f nu are rădăcini în $K(\alpha^p)$)
Rezultă că $Irr\ \alpha = f$, f are rădăcină multiple pe α, fals!.
Aşadar

$$\alpha \in K(\alpha^p) \Rightarrow K(\alpha) \leq K(\alpha^p) \leq K(\alpha) \Rightarrow\ =\ "$$

$\Leftarrow$" Fie $L = K(\alpha)$. Atunci

$$K(L^p) = K(K(\alpha))^p \subseteq K(\alpha) = L$$
$$L = K(\alpha) = K(\alpha^p) \subset K(L^p).$$

Din cele două relaţii obţinem $L = K(L^p)$. Extinderea $K \leq L$ finită pentru că $\alpha\ alg/_K$, rezultă din teorema precedentă **b**) că

$$L\ sep/_K \Rightarrow \alpha\ sep/_K.$$

2)

$$\alpha\ sep/_K \overset{1)}{\Leftrightarrow} K(\alpha) = K(\alpha^p) \overset{\text{th. ant.}}{\Rightarrow} K(\alpha)\ \ sep/_K.$$

■

Teorema 14.5 ***(fundamentală a elementului primitiv)***

$L = K(\alpha_1, ..., \alpha_n)$, $\alpha_i\ sep/_K (alg/_K)$. Atunci $\exists\ \theta \in L$ (element primitiv), $L = K(\theta)$, $\theta\ sep/_K\ (alg/_K)$.

.

15 Curs 8– Extinderi normale

Definiţie 15.1 *Fie $K \subseteq L$. Spunem că L este **extindere normală** a lui K dacă $L\ alg|_K$ şi $\forall\ f \in K[X]$, f ireductibil (nu minimal) cu $f(\alpha) = 0, \alpha \in L$, atunci $\mathcal{C}_f \subseteq L$.*

Observaţie 15.1 *$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nu este normală, pentru că $\epsilon\sqrt[3]{2}, \epsilon^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$, cu $\epsilon^2 + \epsilon + 1 = 0$.*

Teorema 15.1 ***(de caracterizare)*** *Fie $K \leq L$, K algebric peste L. Următoarele afirmaţii sunt echivalente:*

1. *L normală$|_K$;*

2. *L corp de descompunere pentru o familie de polinoame din $K[X]$;*

3. *$K \leq L \leq \overline{K}$ (închidere algebrică) $\sigma : \overline{K} \to \overline{K}, K - izomorfism \Longrightarrow \sigma(L) \subseteq L$.*

Demonstraţie. **1**) $\Rightarrow$ **2**)

Fie $\{\beta_j\}_{j\in J}$ o bază pentru ${}_KL$ şi $f_j = Irr\ \beta_j$. Vrem să demonstrăm că $L = \mathcal{C}_{\{f_j|\ j\in J\}}$

Din faptul că L normală rezultă că

$$\mathcal{C}_T \subseteq L. \qquad (bf*)$$

Invers, fie $a \in L$, atunci

$$a = \sum_{j\in J} \alpha_j\beta_j, \alpha_j \in K,$$

dar

$$\beta_j \in \mathcal{C}_T \Rightarrow a \in \mathcal{C}_T$$

Deci $L \subseteq \mathcal{C}_T$ şi conform $(*)$, obţinem

$$L = \mathcal{C}_T.$$

2) $\Rightarrow$ **3**)

Avem $L = \mathcal{C}_T$, unde T reprezintă o familie de polinoame.

Fie $\sigma : \overline{K} \to \overline{K}, K-$izomorfism şi vrem să arătăm că $\sigma(L) \subseteq L$.

Fie α o rădăcină a unui polinom f din T, unde f este un polinom ireducitibil.

$$f = \sum a_i x^i$$

şi obţinem

$$\sum a_i\alpha^i = 0 \Rightarrow \sum a_i\sigma(\alpha)^i = 0 \Rightarrow \sigma(\alpha) \text{ rădăcină pentru } f \Rightarrow \sigma(\alpha) \in L.$$

Să observăm că este suficient să demonstrăm pentru α rădăcină a unui polinom din T, pentru că $\mathcal{C}_T = K$ (rădacina lui T).

Deci

$$\sigma(L) \subseteq L,\ \sigma \text{ injectiv} \Rightarrow \sigma(L) = L.$$

3) $\Rightarrow$ **1**)

Fie

$$f \in K[X],\ f \text{ ireductibil } f(\alpha) = 0,\ \alpha \in L.$$

Arătăm că $\mathcal{C}_f \subseteq L$.

Fie β o altă rădăcină a lui f rezultă că α, β au acelaşi polinom minimal. Atunci conform teoremei anterioare avem:

$$K(\alpha) \overset{\sigma_1}{\simeq} K(\beta),\ \sigma_1(\alpha) = \beta.$$

σ_1 $K-$ izomorfism.

Prelungesc σ_1 la $\overline{\sigma_1} : \overline{K} \to \overline{K}$ şi folosim că $\overline{\sigma_1}$ este K-izomorfism, atunci:

$$\overline{\sigma_1}(L) \subseteq L \Rightarrow \underbrace{\sigma_1(\alpha)}_{=\beta} \in L \Rightarrow \mathcal{C}_f \subseteq L.$$

■

Corolar 7 *Toate corpurile de descompunere (pentru familii de polinoame din $K[X]$) sunt extinderi normale ale lui K.*

Corolar 8 *$\overline{K}$, închiderea algebrică a lui K, este normală.*

Teorema 15.2 ***(de construcţie a închiderii normale)***

Fie $K \leq L$ o extindere finită. Atunci există o extindere normală minimală N a lui L. Dacă, în plus, L este separabilă peste K, atunci şi N este separabilă peste K.

Demonstraţie. Fie $dim_K L < \infty$ şi $\{\alpha_1, ..., \alpha_n\}$ bază în ${}_K L$.

Obţinem

$$L = K(\alpha_1, ..., \alpha_n).$$

Fie

$$f_i = Irr(\alpha_i, K),\ i = \overline{1,n}.$$

Definim

$$N = \mathcal{C}_{\{f_i | i=\overline{1,n}\}} = \mathcal{C}_{\prod_{i=1}^{n} f_i}$$

N este normală şi minimală pentru că $\{\alpha_i\}_{i=1}^n$ este bază în ${}_K L$.

N se obţine prin adjuncţia unui număr finit de elemente algebrice, deci N este finită peste K.

Dacă L $sep|_K$, atunci α_i $sep|_K$, $\forall\ i = \overline{1,n}$, deci toate rădăcinile ale lui f_i sunt separabile $\Rightarrow N$ $sep|_K$. ■

16 Extinderi Galois. Grup Galois

Definiţie 16.1 *$K \leq L$ se numeşte **Galois** dacă este finită, separabilă şi normală.*

Grupul lui Galois: $G(K;L)$ este grup $K-autom.$ lui L.
$G(K;L) = \{\sigma : L \to L |\ \sigma\ K-autom.\}$.

Observaţie 16.1 $G(K;L) \leq Aut\ L$.

Teorema 16.1 *Fie $K \leq L = K(\theta)$ extindere Galois. Atunci $|G(K;L)| = [L : K] = grad\ Irr(\theta, K)$.*

Demonstraţie. Stabilim o bijecţie între mulţimea K-autom.şi mulţimea rădăcinilor lui $Irr(\theta, K)$.

Fie $u \in G(K;L)$ şi arătăm că $u(\theta)$ este rădăcină pentru $Irr(\theta, K)$.

Fie

$$\begin{aligned} Irr(\theta,K) &= a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n. \\ &\Rightarrow a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1} + \theta^n = 0 \\ &\Rightarrow a_0 + a_1u(\theta) + ... + a_{n-1}(u(\theta))^{n-1} + (u(\theta))^n = 0 \\ &\Rightarrow u(\theta) \text{ rădăcină pentru } Irr(\theta,K). \end{aligned}$$

Invers, dacă β rădăcină pentru $Irr(\theta, K)$, atunci $u : K(\theta) \to K(\beta)$.
K izomorfism $\theta \longrightarrow \beta k \longrightarrow k$ şi vrem să arătăm că $u \in G(K;L)$.
Din faptul că extinderea $K \leq K(\theta)$ este normală, avem:

$$\beta \in K(\theta) \Rightarrow K(\beta) \leq K(\theta). \qquad (1)$$

β şi θ au acelaşi polinom minimal de unde rezultă că:

$$[K(\beta) : K] = [K(\theta) : K]. \qquad (2)$$

Din (1) şi (2) obţinem $K(\beta) = K(\theta)$.
Aşadar $u \in G(K;L)$. ■

Exemplu 16.1 *$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ extindere Galois. Determinaţi $G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}))$.*

Soluţie 16.1 *$Irr(\sqrt{2}) = X^2 - 2$ cu rădăcinile $\sqrt{2}$, $-\sqrt{2}$.*

$$\{.u_1 : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}),\ u_1(\sqrt{2}) = -\sqrt{2} \qquad u_2 = 1_{\mathbb{Q}(\sqrt{2})}$$

$\Rightarrow$ *$G(\mathbb{Q}, \mathbb{Q}(\sqrt{2})) \simeq \mathbb{Z}_2$ (are 2 elemente).*

Exemplu 16.2 *Fie $\mathbb{Q} \leq \mathbb{Q}(\epsilon)$ cu ϵ rădăcină pentru $F_8 = X^4 + 1$.Determinaţi $G(\mathbb{Q}, \mathbb{Q}(\epsilon))$.*

Soluţie 16.2 *Celelalte soluţii ale lui F_8 sunt ϵ^3, ϵ^5, ϵ^7. ($F_8 = Irr\ \epsilon$).*

Obţinem 4 automorfisme:

$$\begin{aligned} u_i &: \mathbb{Q}(\epsilon) \to \mathbb{Q}(\epsilon) \\ u_1(\epsilon) &= \epsilon,\ u_2(\epsilon) = \epsilon^3 \\ u_3(\epsilon) &= \epsilon^5, u_4(\epsilon) = \epsilon^7. \end{aligned}$$

Deoarece

$$\epsilon^4 = -1 \Rightarrow \epsilon^5 = -\epsilon \Rightarrow (\epsilon^5)^5 = \epsilon \text{ şi } (\epsilon^7)^7 = \epsilon.$$

Obţinem $u_i^2 = 1_{\mathbb{Q}(\epsilon)}$, deci $G(\mathbb{Q}, \mathbb{Q}(\epsilon))$ este grupul lui Klein.

Exemplu 16.3 *Determinaţi* $G(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}))$.

Extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nu este normală.

Fie $u \in G(\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2}))$. Atunci $u(\sqrt[3]{2})$ este rădăcină din $\mathbb{Q}(\sqrt[3]{2})$ a lui $Irr(\sqrt[3]{2}, \mathbb{Q})$, deci $u(\sqrt[3]{2}) = \sqrt[3]{2}$.

Rezultă $G\left(\mathbb{Q}, \mathbb{Q}\left(\sqrt[3]{2}\right)\right) = \{1_{\mathbb{Q}(\sqrt[3]{2})}\}$.

Teorema 16.2 *Fie* $K \leq L$ *extindere Galois. Atunci* $G(K, L) \leq \mathcal{S}_n$, *unde* $n = [L : K]$.

Demonstraţie. Avem $L = K(\alpha)$, $f = Irr(\alpha, K)$ are n rădăcini.

Dacă $u, v \in G(K, L)$ şi $u \neq v$, atunci $u(\alpha) \neq v(\alpha)$.

(pentru că *răd.* $f \in K(\alpha)$ şi dacă $u(\alpha) = v(\alpha)$, atunci

$$u(\forall \text{ răd.} f) = v(\forall \text{ răd.} f) \Rightarrow u = v \text{ fals!})$$

Fie

$$\begin{array}{rcl} g & : & G(K, L) \longrightarrow \mathcal{S}_n \\ g(u) & = & \begin{pmatrix} \alpha = \alpha_1 & . & . & . & \alpha_n \\ u(\alpha) & . & . & . & u(\alpha_n) \end{pmatrix}. \end{array}$$

Din faptul că $u \neq v \Rightarrow u(\alpha) \neq v(\alpha) \Rightarrow g(u) \neq g(v) \Rightarrow g$ injectivă.

g morfism:

$$g(u_1 \circ u_2) = \begin{pmatrix} \alpha_1 & . & . & . & \alpha_n \\ u_1 \circ u_2(\alpha_1) & . & . & . & u_1 \circ u_2(\alpha_n) \end{pmatrix}$$

$$g(u_1) \circ g(u_2) = \begin{pmatrix} u_2(\alpha_1) & . & . & . & u_2(\alpha_n) \\ u_1(u_2(\alpha_1)) & & & & u_1(u_2(\alpha_n)) \end{pmatrix} \circ \begin{pmatrix} \alpha_1 & . & . & . & \alpha_n \\ u_2(\alpha_1) & . & . & . & u_2(\alpha_n) \end{pmatrix} = g(u_1 \circ u_2).$$

În concluzie $G(K, L) \leq \mathcal{S}_n$. ■

17 Seminar 8

Exerciţiu 17.1 *Să se studieze grupul Galois al extinderii* $\mathbb{Q} \leq \mathbb{Q}(\epsilon) = \mathcal{C}_{X^n - 1, \mathbb{Q}}$, *unde* ϵ *este rădăcină primitivă.*

Rezolvare 17.1

Extinderea $\mathbb{Q} \leq \mathbb{Q}(\epsilon)$ este extindere Galois, pentru că:

- este finită : $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = grad\ F_n$;
- este separabilă, pentru că: $car\ \mathbb{Q} = 0$;
- este normală, pentru că: $\mathbb{Q}(\epsilon) = \mathcal{C}_{X^n - 1, \mathbb{Q}}$.

Deci

$$|G(\mathbb{Q},\mathbb{Q}(\epsilon))| = [\mathbb{Q}(\epsilon):\mathbb{Q}] = gradF_n = \varphi(n).$$

Elementele lui $G(\mathbb{Q},\mathbb{Q}(\epsilon))$ sunt $u_1, u_2, ...u_{\varphi(n)}$ cu:

$$u_1(\epsilon) = \epsilon,\ u_2(\epsilon) = \epsilon^{k_2} ... u_{\varphi(n)} = \epsilon^{k_{\varphi(n)}},$$

unde $(k;n) = 1$ şi ϵ^{k_i}este rădăcină primitivă.
Dar

$$\begin{aligned}(u_i \circ u_j)(\epsilon) &= u_i(\epsilon^{k_j}) = \epsilon^{k_i k_j} = (u_j \circ u_i)(\epsilon), \forall\ i,j \\ &\Rightarrow G(\mathbb{Q},\mathbb{Q}(\epsilon)) \text{ comutativă.}\end{aligned}$$

Exerciţiu 17.2 *Determinaţi grupul Galois corespunzător polinomului*

$X^3 - 2 \in \mathbb{Q}[X]$.

Rezolvare 17.2

$\mathcal{C}_{X^3-2,\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, \epsilon) = \mathbb{Q}(\sqrt[3]{2} + \epsilon)$.
Extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2} + \epsilon)$ este Galois, deoarece:

- este separabila, $car\ \mathbb{Q} = 0$;
- este finită, pentru că $\sqrt[3]{2} + \epsilon\ alg|_{\mathbb{Q}}$;
- este normală, pentru că e un corp de descompunere.

Să determinăm celelalte rădăcini ale lui $Irr(\theta,\mathbb{Q})$, $\theta = \sqrt[3]{2} + \epsilon$.

- ϵ şi ϵ^2 sunt conjugate, fiind rădăcini pentru $X^2 + X + 1$;
- $\sqrt[3]{2}$, $\epsilon\sqrt[3]{2}$, $\epsilon^2\sqrt[3]{2}$ sunt conjugate, fiind rădăcinile lui $X^3 - 2$.

Rădăcinile lui $Irr(\theta,\mathbb{Q})$ sunt:

$$\sqrt[3]{2} + \epsilon,\ \epsilon\sqrt[3]{2} + \epsilon,\ \epsilon^2\sqrt[3]{2} + \epsilon,\ \sqrt[3]{2} + \epsilon^2,\ \epsilon\sqrt[3]{2} + \epsilon^2,\ \epsilon^2\sqrt[3]{2} + \epsilon^2.$$

Elementele lui $G(\mathbb{Q},\mathbb{Q}(\theta))$ sunt:

$$u_1 : \{\epsilon \longrightarrow \epsilon;\ \sqrt[3]{2} \longrightarrow \sqrt[3]{2};\quad u_2 : \{\epsilon \longrightarrow \epsilon^2;\ \sqrt[3]{2} \longrightarrow \sqrt[3]{2};\quad u_3 : \{\epsilon \longrightarrow \epsilon;\ \sqrt[3]{2} \longrightarrow \epsilon\sqrt[3]{2};$$

$$u_4 : \{.\epsilon \longrightarrow \epsilon^2;\ \sqrt[3]{2} \longrightarrow \epsilon\sqrt[3]{2};\ u_5 : \{\epsilon \longrightarrow \epsilon;\ \sqrt[3]{2} \longrightarrow \epsilon^2\sqrt[3]{2};\ u_6 : \{\epsilon \longrightarrow \epsilon^2;\ \sqrt[3]{2} \longrightarrow \epsilon^2\sqrt[3]{2}.$$

Notăm cu $u_2 = u$ şi $u_3 = v$ şi obţinem următoarele relaţii:

$$u^2 = \epsilon,\ v^2 = u_5, v^3 = \epsilon,\ uv = u_4,\ uv^2 = u_6.$$

$$G(\mathbb{Q},\mathbb{Q}(\theta)) = \{1, u, v, v^2, uv, vu, uv^2\} \simeq \mathcal{S}_3 \text{ (nu e abelian).}$$

Exerciţiu 17.3 *Fie extinderea* $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Să se determine* $G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}, \sqrt{3}))$.

Rezolvare 17.3

$$u_1 \ : \ \{\sqrt{2} \longrightarrow \sqrt{2}; \sqrt{3} \longrightarrow \sqrt{3};\ u_2 : \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow \sqrt{3};$$
$$u_3 \ : \ \{\sqrt{2} \longrightarrow \sqrt{2}; \sqrt{3} \longrightarrow -\sqrt{3};\ u_4 : \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow -\sqrt{3}.$$

Notăm cu $u_2 = u$, $u_3 = v$ şi obţinem:

$$u_4 = uv,\ u_i^2 = 1 \Rightarrow G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}, \sqrt{3})) \simeq \text{Gr.Klein}.$$

Observaţie 17.1 *Fie* $\mathbb{Q} \leq \mathbb{Q}(\alpha, \beta)$ *şi* $u \in Aut\ \mathbb{Q}(\alpha, \beta)$, $u|_{\mathbb{Q}} = 1_{\mathbb{Q}}$.

$u(\alpha + \beta) = u(\alpha) + u(\beta)$, $u(\alpha)$ este altă rădăcină pentru $Irr\ \alpha$ şi $u(\beta)$ este altă rădăcină pentru $Irr\ \beta$.

Aşadar avem

$u(\alpha + \beta) = \alpha_i + \beta_j; \alpha_i$ rădăcină pentru $Irr\ \alpha;\ \beta_j$, rădăcină pentru $Irr\ \beta$.

Deci, dacă $\alpha + \beta$ e rădăcină pentru $Irr(\alpha + \beta, \mathbb{Q})$, atunci celelalte rădăcini sunt $\alpha_i + \beta_j$.

Exerciţiu 17.4 *Determinaţi grupul Galois al corpului de descompunere peste* $\mathbb{Q}$, *al polinomului* $f = X^4 - 3$.

Rezolvare 17.4 *Fie*

$$X = \sqrt[4]{3}Y \Rightarrow f = 3(Y^4 - 1) = 3(Y - 1)(Y + 1)(Y^2 + 1) \Rightarrow \mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt[4]{3}, i).$$

Extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{3}, i)$ este extindere Galois.

$$u_1 : \{i \longrightarrow i; \sqrt[4]{3} \longrightarrow \sqrt[4]{3};\quad u_2 : \{i \longrightarrow i\ \ ; \sqrt[4]{3} \longrightarrow -\sqrt[4]{3};$$

$$u_3 : \{i \longrightarrow i; \sqrt[4]{3} \longrightarrow i\sqrt[4]{3};\quad u_4 : \{i \longrightarrow i\ \ ; \sqrt[4]{3} \longrightarrow -i\sqrt{3};$$

$$u_5 : \{i \longrightarrow -i; \sqrt[4]{3} \longrightarrow \sqrt[4]{3}\ \ ;\ u_6 : \{i \longrightarrow -i;\ \sqrt[4]{3} \longrightarrow -\sqrt[4]{3};$$

$$u_7 : \{i \longrightarrow -i; \sqrt[4]{3} \longrightarrow i; \sqrt[4]{3}\ ;\ u_8 : \{i \longrightarrow -i\ ; \sqrt[4]{3} \longrightarrow -i\sqrt{3}\ .$$

Notăm $u_3 = a$, $u_5 = b$ şi obţinem: $ord\ a = 4$, $ord\ b = 2$, $ab = ba^3$.

$$G = G(\mathbb{Q}; \mathbb{Q}(\sqrt[4]{3}, i)) \simeq \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}.$$

G: grupul izometriilor unui pătrat.

- a : rotaţie de unghi $\frac{\pi}{2}$ în jurul centrului pătratului;

- b : simetria faţă de mediatoarea unei laturi.

G: grupul diedral D_4 nu e comutativ.
Grupurile cu 8 elemnte:

- abeliene: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$.
- neabeliene: D_4, grupul cuaternionilor Q: $j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$; $k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $ord\ j = ord\ k = 4 : j^2 = k^2$, $jkj = k$; $kjk = j$. $Q =< j, k >$ în raport cu " . ".

Exerciţiu 17.5 *Determinaţi grupul Galois al extinderilor:*

i) $\mathbb{Q} \leq \mathbb{R}$;

ii) $\mathbb{R} \leq \mathbb{C}$;

iii) $\mathbb{Q} \leq \mathbb{Q}(i)$.

Rezolvare 17.5

i) $G(\mathbb{Q}, \mathbb{R}) = Aut\ \mathbb{R}$. Fie $u \in G(\mathbb{Q}, \mathbb{R})$ şi $x \in \mathbb{R} - \mathbb{Q}$.

Fie $a_n \nearrow x$, $b_n \searrow x$, a_n, $b_n \in \mathbb{Q}$.
Avem

$$a_n \leq x \leq b_n. \qquad (bf*)$$

Verific că u este monotonă, iar pentru acest lucru, consider $z \geq 0$ şi obţinem:

$$z = (\sqrt{z})^2 \Rightarrow u(z) = (u(\sqrt{z}))^2 \geq 0.$$

Deci, dacă:

$$x \leq y \Rightarrow \exists\ z \geq 0 : y = x + z \Rightarrow u(y) = u(x) + u(z) \geq u(x).$$

Aplic u pentru $(*) : \{.u(a_n) \leq u(x) \leq u(b_n) u(a_n) = a_n,\ u(b_n) = b_n,\ a_n \nearrow x, b_n \searrow x \Rightarrow u(x) = x$.
Deci, $Aut\ \mathbb{R} = \{1_{\mathbb{R}}\}$.

ii) $\mathbb{R} \leq \mathbb{C} = \mathbb{R}(i) = \mathcal{C}_{X^2+1,\mathbb{R}}$.

Rădăcinile lui $X^2 + 1$ sunt $\pm\ i$.

$$u_1(i) = i;\ u_2(i) = -i \Rightarrow G(\mathbb{R}, \mathbb{C}) = \{u_1, u_2\} \simeq \mathbb{Z}_2.$$

Similar pentru $\mathbb{Q} \leq \mathbb{Q}(i)$.

Exerciţiu 17.6 *Fie* $f = X^3 - 2 \in \mathbb{Q}[X]$. *Determinaţi* $G(\mathbb{Q}, \mathcal{C}_{f,\mathbb{Q}})$.

Rezolvare 17.6

Rădăcinile lui f sunt: $\sqrt[3]{2}, \epsilon\sqrt[3]{2}, \epsilon^2\sqrt[3]{2}$, unde ϵ răd. pentru X^2+X+1.
$\mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\epsilon, \sqrt[3]{2})$. Avem $[\mathbb{Q}(\epsilon, \sqrt[3]{2}) : \mathbb{Q}] = 6 \Rightarrow |G(\mathbb{Q}, \mathcal{C}_{f,\mathbb{Q}})| = 6$.
Fie $u_i \in G(\mathbb{Q}, \mathbb{Q}(\epsilon, \sqrt[3]{2}))$, iar u_i este dat de $u_i(\epsilon)$ şi $u_i(\sqrt[3]{2})$.

$$u_1 \ : \ \{\epsilon \longrightarrow \epsilon; \sqrt[3]{2} \longrightarrow \sqrt[3]{2}; \ \ u_2 : \{\epsilon \longrightarrow \epsilon^2; \sqrt[3]{2} \longrightarrow \sqrt[3]{2}; \quad u_3 : \{.\epsilon \longrightarrow \epsilon; \sqrt[3]{2} \longrightarrow \epsilon\sqrt[3]{2}$$

$$u_4 \ : \ \{\epsilon \longrightarrow \epsilon^2; \sqrt[3]{2} \longrightarrow \epsilon\sqrt[3]{2}; \ u_5 : \{\epsilon \longrightarrow \epsilon; \sqrt[3]{2} \longrightarrow \epsilon^2\sqrt[3]{2}; \ u_6 : \{\epsilon \longrightarrow \epsilon^2; \sqrt[3]{2} \longrightarrow \epsilon^2\sqrt[3]{2}.$$

Avem $u_2u_3 \neq u_3u_2$, pentru că:

$$u_2u_3(\sqrt[3]{2}) = u_2(\epsilon\sqrt[3]{2}) = \epsilon^2\sqrt[3]{2} \ u_3u_2(\sqrt[3]{2}) = u_3(\sqrt[3]{2}) = \epsilon\sqrt[3]{2}$$

Deci, $G_f(\mathbb{Q}) = G(\mathbb{Q}, \mathbb{Q}(\epsilon, \sqrt[3]{2}) \simeq \mathcal{S}_3$.

18 Cursuri $9, 10$ - Grupul Galois al unei extinderi Galois

Teorema 18.1 ***(curs trecut)***

$K \leq L$, extindere Galois $\Rightarrow G(K, L) = \mathcal{C}_f \leq \mathcal{S}_n$, unde $n = grad\ f$. (f ireductibil).

Teorema 18.2 *Există extinderea Galois, pentru care* $G(K; L) \simeq \mathcal{S}_n$.

Demonstraţie. Notăm $E = K(X_1, ..., X_n)$.

$$\sigma_1 = X_1 + ... + X_n, \ \sigma_2 = \sum_{1 \leq i < j \leq n} X_iX_j, ..., \ \sigma_n = X_1 \cdot ... \cdot X_n \ .F = K(\sigma_1, ..., \sigma_n)$$

Atunci $F \leq E$ extindere Galois, pentru că x_i răd. pentru

$$f = \prod_{i=1}^{n}(X - X_i) = X^n - \sigma_1X^{n-1} + ... + (-1)^n\sigma_n.$$

$f \in F[X]$, f ireductibil cu rădăcinile distincte.
$[E : F] < \infty$, pentru că X_i, $i = \overline{1, n}$ sunt alg. (răd. lui f) ; $E = \mathcal{C}_{f,F}$; rădăcini distincte $\Rightarrow F \leq E$ sep.
Rezultă $F \leq E$ extindere Galois.
Fie $\alpha \in \mathcal{S}_n$. Obţinem : $u_\alpha : \ \underset{\downarrow}{X_i} \ , u_\alpha(\sigma_i) = \sigma_i, \forall\ i \Rightarrow u_\alpha|_F = 1_F$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad X_{\alpha(i)}$
Asocierea $\alpha \longrightarrow u_\alpha$ este injectivă $\Rightarrow |\mathcal{S}_n| \leq |G(F; E)| \leq |\mathcal{S}_n|$ (teorema anterioară), unde $n = grad\ f$, f ireductibil şi $E = C_f$.
Rezultă că $G(F; E) \simeq \ \mathcal{S}_n$. ■

Observaţie 18.1 $[K(X_1, X_2, ..., X_n) : K(\sigma_1, ..., \sigma_n)] = n!$, *unde:*

$K(X_1, X_2, ..., X_n) = C_{f,,K(\sigma_1,...,\sigma_n)}$ şi $K(\sigma_1, ..., \sigma_n) = F$.

Problemă 1 *Fie* $f \in F[X]$, *grad* $f = n$. *Atunci* $[C_{f,K} : K] \leq n!$.

Teorema 18.3 ***(Teorema fundamentală a teoriei lui Galois)***

Teorema 18.4 ***(Elementului primitiv)***

$K(\alpha_1, ..., \alpha_n) = K(\theta)$, unde θ $sep|_K$ şi α_i $sep|_K$.
Fie $K \leq L$ şi consider $G(K; L)$.
Fie $\mathcal{K}$: mulţimea subcorpurilor lui L, ce includ K.
$\mathcal{L}$: mulţimea subgrupurilor lui $G(K; L)$.

Teorema 18.5 *Dacă* $K \leq L$ *extindere Galois, atunci există o bijecţie între* $\mathcal{K}$ *şi* $\mathcal{L}$.

Demonstraţie. Fie

$$\begin{aligned} \Phi &: \mathcal{L} \longrightarrow \mathcal{K} \\ H &\leq G(K, L) \rightsquigarrow L^H = \{x \in L |\ u(x) = x,\ \forall\ u \in H\}. \end{aligned}$$

Avem $K \leq L^H \leq L$. L^H corp :

$$\begin{aligned} x, y &\in L^H \Rightarrow u(x - y) = x - y;\ u(xy) = xy;\ u(x^{-1}) = x^{-1};\ \forall\ u \in H \\ x, y &\in L^H \Rightarrow\ x - y;\ xy;\ x^{-1} \in L^H. \end{aligned}$$

Fie

$$\begin{aligned} \Psi &: \mathcal{L} \longrightarrow \mathcal{K} \\ K &\leq L_1 \leq L \rightsquigarrow G(L_1, L) \leq G(K; L). \end{aligned}$$

Observăm că ϕ şi Ψ sunt antimonotone.

$$\begin{aligned} H_1 &\leq H_2 \Rightarrow L^{H_1} \geq L^{H_2} \\ L_1 &\leq L_2 \Rightarrow G(L_2; L) \leq G(L_1; L). \end{aligned}$$

Dacă $H \in \mathcal{L}$, arătăm că $H = \Psi\Phi(H) \Leftrightarrow H = G(L^H; L)$.
Avem $H \leq G(L^H; L)$ şi demonstrăm că $L^H \leq L$ extindere Galois.

$$K \leq L, \text{ finită} K \leq L^H \leq L \Rightarrow L^H \leq L \text{ finită}.$$

În cele ce urmează, vom arăta că L $normală|_{L^H}$.
Fie $x \in L$. Avem x $alg|_K$ de unde $\exists\ Irr(x, K) = f$
$K \leq L$ normală $\Rightarrow \mathcal{C}_f \subseteq L, x$ $alg|_{L^H}$ deci$Irr(x, L^H) \Rightarrow C_{Irr(x,L^H)} \subseteq L$.
L $sep|_K \Rightarrow L$ $sep|_{L^H}$.

Deci, $L^H \leq L$ extindere Galois$\Rightarrow \exists\ \theta \in L;\ L = L^H(\theta)$.
Fie $h = \prod_{u \in H} (X - u(\theta))$, el are pe θ ca rădăcină. (pentru $u = 1_L$).
Observăm că:

$$\forall\ v \in H,\ v(h) = h \Rightarrow h \in L^H[X] \Rightarrow Irr(\theta, L^H)|h.$$

Avem

$$|G(L^H; L)| = [L : L^H] = gradIrr(\theta, L^H) \leq gradh = |H|.$$

Obţinem:

$$|G(L^H, L)| \leq |H| \text{ şi } H \leq G(L^H, L).$$

Rezultă $H = G(L^H, L)$.
Pe de altă parte, $L_1 \leq L^{G(L_1;L)}$.
Arătăm că $[L : L_1] = [L : L^{G(L_1;L)}]$.
Din prima parte a demonstraţiei, $G(L^{G(L_1;L)}; L) = G(L_1; L)$.
Din $K \leq L$ ext. Galois$\Rightarrow L^{G(L_1,L)} \leq L$ ext. Galois.
$L_1 \leq L$ ext. Galois.
Aşadar obţinem $[L : L^{G(L_1;L)}] = [L : L_1] \Rightarrow L_1 = L^{G(L_1,L)}$.
Deci Φ şi Ψ sunt una inversa celeilalte. ■

Observaţie 18.2 *K, L corpuri finite$\Rightarrow K \leq L$ extindere Galois:*

- este finită
- este normală pentru că $L = \mathcal{C}_{X^{P^n} - X,\ K}$.
- este separabilă, pentru că K finit$\Rightarrow K$ perfect.

Teorema 18.6 ***(Galois)*** *Fie $K \leq L$ extindere Galois şi $K \leq L_1$ normală. Atunci $\{L_1 | K \leq L_1 \leq L\} \overset{bij}{\longleftrightarrow} \{H |\ H \rhd G(K, L)\}$. $(H = G(L, L))$.*

Corolar 9 *Fie $H \leq \mathcal{S}_n$, $\exists\ T \leq E$ extindere Galois: $G(T, E) \simeq H$.*

Demonstraţie. $\exists$ o ext. Galois $F \leq E$, astfel încât

$$G(F; E) \simeq \mathcal{S}_n \geq H \Rightarrow \exists H_1 \simeq H \text{ şi } H_1 \leq G(F, E).$$

Fie $T = E^{H_1}$, atunci rezultă că $G(E^{H_1}, E) = H_1$. ■

Exerciţiu 18.1 *Să se găsească $G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}, \sqrt{3}))$ şi corpurile intermediare corespunzătoare.*

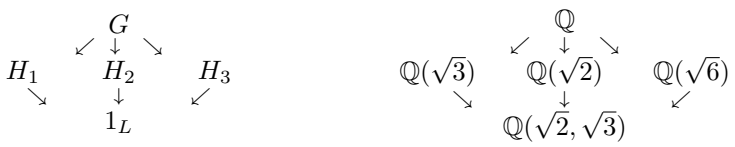
Rezolvare 18.1 *$G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}, \sqrt{3})) \simeq K$, K grupul lui Klein.*

$u_1 : \{\sqrt{2} \longrightarrow \sqrt{2}; \sqrt{3} \longrightarrow \sqrt{3};\quad u_2 : \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow \sqrt{3};$
$u_3 : \{\sqrt{2} \longrightarrow \sqrt{2}; \sqrt{3} \longrightarrow -\sqrt{3};\ u_4 : \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow -\sqrt{3}.$

Notăm $u_2 = u$ şi $u_3 = v$.

Subgrupurile lui G sunt: $\{1\}$, $H_1 = \{1, u\} \lhd G$, $H_2 = \{1, v\} \lhd G$, $H_3 = \{1, uv\} \lhd G$, $G \lhd G$.

Subgrupurile lui G: Subcorpurile intermediare:



$$\begin{aligned} L^{H_1} &= \{x \in L|\ \varphi(x) = x, \forall \varphi \in H_1\} = \{x \in L|\ u(x) = x\} = \mathbb{Q}(\sqrt{3}). \\ L^{H_2} &= \{x \in L|\ v(x) = x\} = \mathbb{Q}(\sqrt{2}). \\ L^{H_3} &= \{x \in L|\ uv(x) = x\} = \mathbb{Q}(\sqrt{6}). \end{aligned}$$

$$uv : \{.\sqrt{2} \xrightarrow{v} \sqrt{2} \xrightarrow{u} -\sqrt{2}\sqrt{3} \xrightarrow{v} -\sqrt{3} \longrightarrow -\sqrt{3}$$

Dacă nu observ cine e L^H, atunci:

$$L = \{x|\ x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ a, b, c, d \in \mathbb{Q}\}.$$

$$u(x) = a + bu(\sqrt{2}) + cu(\sqrt{3}) + du(\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

Temă 1 *Fie $\mathbb{Q} \leq \mathcal{C}_{X^3-2,\mathbb{Q}}$. Determinaţi $G(\mathbb{Q}, \mathcal{C}_{X^3-2,\mathbb{Q}})$ şi subcorpurile coresp.*

18.1 Seminar nr. 9

Exerciţiu 18.2 *Fie $f = X^3 - 2 \in \mathbb{Q}(\epsilon)[X]$ cu ϵ rădăcină pentru $X^2 + X + 1$. Să se determine $G_f(\mathbb{Q}(\epsilon))$.*

Rezolvare 18.2

$\mathcal{C}_{f,\mathbb{Q}(\epsilon)} = \mathbb{Q}(\epsilon, \sqrt[3]{2})$. Notăm $K = \mathbb{Q}(\epsilon)$.

Avem $K \leq K(\sqrt[3]{2})$ cu baza $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. $u \in G(K, \mathcal{C}_{f,K})$ e unic determinat de $u(\sqrt[3]{2})$.

$u(\sqrt[3]{2})$ e răd. pentru $X^3 - 2$, rezultă:

$$u(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \epsilon\sqrt[3]{2}, \epsilon^2\sqrt[3]{2}\} \Rightarrow |G(K, \mathcal{C}_{f,K})| = 3 \Rightarrow G_f(K) \simeq \mathbb{Z}_3.$$

Exerciţiu 18.3 *Fie p prim, $\epsilon \neq 1$, ϵ rădăcină pentru $X^p - 1$. $f = X^p - 2 \in K[X]$ cu $K = \mathbb{Q}(\epsilon)$. Determinaţi $G_f(K)$.*

Rezolvare 18.3

Rădăcinile lui f sunt:

$$\sqrt[p]{2},\ \epsilon\sqrt[p]{2},...,\ \epsilon^{p-1}\sqrt[p]{2} \Rightarrow \mathcal{C}_{f,K} = K(\epsilon,\ \sqrt[p]{2}) = K(\ \sqrt[p]{2}).$$

$$Irr(\epsilon,\mathbb{Q}) = X^{p-1} + ... + X + 1,\ Irr(\sqrt[p]{2},\mathbb{Q}) = X^p - 2.$$

Fie $u \in G_f(K)$. Atunci u e unic determinat de $u(\sqrt[p]{2})$. Rezultă:

$$u(\sqrt[p]{2}) \in \{\sqrt[p]{2}, \epsilon\sqrt[p]{2}, ..., \epsilon^{p-1}\sqrt[p]{2}\} \Rightarrow |G_f(K)| = p,\ p \text{ prim} \Rightarrow G_f(K) \simeq \mathbb{Z}_p.$$

Exerciţiu 18.4 *Fie $f = X^4 - 2 \in K[X]$, cu $K = \mathbb{Q}(i)$. Să se determine $G_f(K)$.*

Rezolvare 18.4

Rădăcinile lui f sunt: $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. f ireductibil în $K[X]$ şi $\mathcal{C}_{f,K} = K(\sqrt[4]{2})$.

Dacă $u \in G_f(K)$, atunci $u(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Obţinem 4 automorfisme:

$$u_1(\sqrt[4]{2}) = \sqrt[4]{2};\ u_2(\sqrt[4]{2}) = -\sqrt[4]{2};\ u_3(\sqrt[4]{2}) = i\sqrt[4]{2};\ u_4(\sqrt[4]{2}) = -i\sqrt[4]{2}.$$

Observăm că $u_4^2 = u_2$; $u_4^3 = u_3 \Rightarrow G_f(K) \simeq \mathbb{Z}_4$.

Exerciţiu 18.5 *Fie $f = X^3 - 2 \in \mathbb{Q}[X]$. Avem $G_f(\mathbb{Q}) = \mathcal{S}_3$.*

i) Determinaţi diagrama laticii subgrupurilor lui $G_f(\mathbb{Q})$.

ii) Determinaţi diagrama laticii subcorpurilor $\mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$ $(= L)$

Rezolvare 18.5

i) Subgrupurile lui $\mathcal{S}_3$ sunt:

$H_1 = \{1_L\};\ H_2 = \langle u_1\rangle;\ u_1 : \{\epsilon \longrightarrow \epsilon^2\ \sqrt[3]{2} \longrightarrow \sqrt[3]{2}\quad, u_1 \text{ transpoziţie},$

$H_3 = \langle u_2\rangle;\ u_2 : \{\epsilon \longrightarrow \epsilon\ \sqrt[3]{2} \longrightarrow \epsilon\sqrt[3]{2},\ H_3 \lhd \mathcal{S}_3,\ H_3 = \{1, u_2, u_2^2\},\ u_2$ ciclu de lungime 3.

$H_4 = \langle u_2u_1\rangle; H_5 = \langle u_2^2u_1\rangle$ transpoziţie, $H_6 = \mathcal{S}_3$

$H_3 \lhd \mathcal{S}_3 \Rightarrow \mathbb{Q} \leq L^{H_3}$ normală.

ii) $L^{H_I} \overset{not}{=} L_i = \{x \in L|\ u(x) = x,\ \forall\ u \in H_i\}$. $H_i \longleftrightarrow L_i$ antiizomorfism între cele doua latici.

$$\begin{aligned} L_1 &= \{x|u(x) = x, \forall u \in H_1 = \{1\}\} = L = \mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, \epsilon). \\ L_2 &= \{x|u_1(x) = x, u_1 \in H_2\} = \mathbb{Q}(\sqrt[3]{2}). \\ L_3 &= \{x|u_2(x) = x, u_2 \in H_3\} = \mathbb{Q}(\epsilon). \\ L_4 &= \{x|u_2u_1(x) = x, u_2u_1 \in H_4\}. \end{aligned}$$

$$u_2u_1 : \{\sqrt[3]{2} \longrightarrow \epsilon; \sqrt[3]{2}\epsilon \longrightarrow \epsilon^2; \quad u_2u_1(\epsilon\sqrt[3]{2}) = u_2(\epsilon^2\sqrt[3]{2}) = \epsilon^2\epsilon\sqrt[3]{2} = \sqrt[3]{2}.$$

$$u_2u_1(\epsilon^2\sqrt[3]{2}) = u_2(\epsilon^4; \sqrt[3]{2}) = \epsilon\epsilon\sqrt[3]{2} = \epsilon^2\sqrt[3]{2}.$$

Deci

$$L_4 = \mathbb{Q}(\epsilon^2\sqrt[3]{2}).$$

$$L_5 = \{x|\ u_2^2u_1(x) = x,\ u_2u_1 \in H_5\}.$$

$$u_2^2u_1 :\ \{\sqrt[3]{2} \longrightarrow \epsilon^2; \sqrt[3]{2}\epsilon \longrightarrow \epsilon \quad ,\ u_2^2u_1(\epsilon\sqrt[3]{2}) = \epsilon^2\epsilon^2\sqrt[3]{2} = \epsilon\sqrt[3]{2}.\ L_5 = \mathbb{Q}(\epsilon\sqrt[3]{2}).$$

$$L_6 = \{x|u(x) = x, \forall u \in \mathcal{S}_3\} = \mathbb{Q}.$$

Exerciţiu 18.6 *Aceeaşi problemă pentru* $f = X^3 - 2 \in \mathbb{Q}(\epsilon)[X]$, $G_f(K) \simeq \mathbb{Z}_3$

$(u(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \epsilon\sqrt[3]{2}, \epsilon^2\sqrt[3]{2}\})$. $K = \mathbb{Q}(\epsilon)$.

Subgrupuri: $H_1 = \{1\}$, $H_2 = \mathbb{Z}_3$.
Subgrupurile corespunzătoare: $L^{H_1} = \mathcal{C}_{f,K} = \mathbb{Q}(\epsilon, \sqrt[3]{2})$, $L^{H_2} = \mathbb{Q}(\epsilon) = K$.

Temă 2 *Fie* $f = X^4 - 2 \in \mathbb{Q}[X]$. *Avem* $G_f(\mathbb{Q}) = D_4$.

i) Determinaţi laticea subgrupurilor lui D_4.

ii) Determinaţi laticea subcorprurilor corespunzătoare.

19 Curs 11 - Extinderi radicale

Fie K cu *car* $K = 0$. Fie $\overline{K}$ închiderea algebrică a lui K.

Definiţie 19.1 $\alpha \in \overline{K}$ *este* ***radical*** *peste* K, *dacă* α *e rădăcina unui polinom de forma* $X^n - a$, $a \in K$.(*polinom care nu are rădăcini multiple pentru că car* $K = 0$).

Rădăcinile lui $X^n - a$ sunt $\theta\epsilon^i$, $i = \overline{0, n-1}$, ϵ^i rădăcină pentru $X^n - 1$.

Definiţie 19.2 *Extindere* ***radicală simplă :*** $K \leq K(\theta, \epsilon) = \mathcal{C}_{X^n-a,K}$.

Definiţie 19.3 *Extindere* ***radicală:*** $K \leq L$ *dacă* $\exists\ K_i$:

$$K = \underset{rad.simplă}{K_0} \leq K_1 \leq ... \leq \underset{rad.simplă}{K_{n-1}} \leq K_n = L.$$

1. Are loc tranzitivitatea extinderii radicale.

2. Orice extindere radicală e finită.

3. Extinderi radicale simple sunt normale, dar cele care nu sunt simple, nu sunt neaparat normale.

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt[4]{3}),\ \mathbb{Q}(\sqrt{3}) = \mathcal{C}_{X^2-3},\ \mathbb{Q}(\sqrt[4]{3}) = \mathcal{C}_{X^2-\sqrt{3}}.$$

($\sqrt[4]{3}$ e rădăcină pentru $X^4 - 3$, celelalte rădăcini sunt: $-\sqrt[4]{3}, \pm i\sqrt[4]{3} \notin \mathbb{R}$.)

Teorema 19.1 *Orice extindere radicală este inclusă într-o extindere radicală normală.*

Exemplu 19.1

$$\mathbb{Q} \leq \underset{rad.normală}{\mathbb{Q}(\sqrt[4]{3})} \leq \mathbb{Q}(\sqrt[4]{3}, i),\ \mathbb{Q}(\sqrt[4]{3}, i) = \mathcal{C}_{X^4-1, \mathbb{Q}(\sqrt[4]{3})}.$$

.

Definiţie 19.4 *Fie $f \in K[X]$, car $K = 0$. Ecuaţia $f = 0$ este **rezolubilă** sau (**rezolvabilă**) prin radicali dacă $\exists\ K \leq L$, astfel încât: L radicală (deci şi o extindere radicală normală) şi $\mathcal{C}_f \subseteq L$.*

Teorema 19.2 *Fie $K \leq L$ extindere Galois, car $K = 0$.$\exists\ L' : L \leq L'$ radicală $\Leftrightarrow G(K, L)$ grup rezolubil.*

Deci, ecuaţia $f = 0$ e rezolvabilă prin radicali $\Leftrightarrow G_f(K) = Gal(K, \mathcal{C}_f)$ este rezolubil. ($K \leq \mathcal{C}_f$ e extindere Galois).

19.1 Grupuri Galois

Definiţie 19.5 *Grupul $(G, \cdot)$ este **rezolubil** dacă $\exists$ lanţul normal:*

$$\{e\} = H_n \lhd H_{n-1} \lhd ... \lhd H_1 \lhd H_0 = G \ a.î \ \forall\ i,\ H_{i-1}|_{H_i} \ abelian.$$

Teorema 19.3 ***(C.N.S)*** *Fie $H \lhd G$. G rezolubil$\Leftrightarrow$ H şi $G|_H$ rezolubile.*

Studiul grupului $(\mathcal{S}_n, \circ)$

Teorema 19.4 *Pentru $n \leq 4$, $\mathcal{S}_n$ este rezolubil.*

Demonstraţie. $\mathcal{S}_2 \simeq \mathbb{Z}_2$, abelian, deci rezolubil.

$$\mathcal{S}_3 : \mathcal{A}_3 \lhd \mathcal{S}_3,\ |\mathcal{A}_3| = 3,\ |\mathcal{S}_3| = 6,\ \mathcal{A}_3 \simeq \mathbb{Z}_3 \text{ abelian.}$$

Avem $1 \lhd \mathcal{A}_3 \lhd \mathcal{S}_3$ cu $\mathcal{A}_3$ abelian şi $\mathcal{S}_3|\mathcal{A}_3 \simeq \mathbb{Z}_2$ abelian $\Rightarrow \mathcal{S}_3$ rezolubil.
$\mathcal{S}_4$: Avem $1 \lhd K \lhd \mathcal{A}_4 \lhd \mathcal{S}_4$.

K grup Klein,

$$K = \{1, (12)(34), (13)(24), (14)(23)\},\ \underset{\text{distincte}}{[(ij)|(kl)]^2} = (ij)^2(kl)^2 = 1$$

$$|K| = 4;\ |A_4| = \frac{4!}{2} = 12 \Rightarrow |\frac{A_4}{K}|=3 \Rightarrow \frac{A_4}{K} \text{ abelian şi } K \text{ abelian.}$$

Demonstrăm $K \lhd \mathcal{A}_4$.
Fie $\sigma \in \mathcal{A}_4$, $(ij)(kl) \in K$. Arătăm că $\sigma(ij)(kl)\sigma^{-1} \in K$.
$s \notin \{i, j, k, l\}$,

$$\sigma(s) \xrightarrow{\sigma^{-1}} s \xrightarrow{(ij)(kl)} s \xrightarrow{\sigma} \sigma(s)$$

$$\sigma(i) \xrightarrow{\sigma^{-1}} i \xrightarrow{(ij)(kl)} j \xrightarrow{\sigma} \sigma(j)$$

$$\sigma(j) \xrightarrow{\sigma^{-1}} j \xrightarrow{(ij)(kl)} i \xrightarrow{\sigma} \sigma(i)$$

$$\sigma(k) \xrightarrow{\sigma^{-1}} k \xrightarrow{(ij)(kl)} l \xrightarrow{\sigma} \sigma(l)$$

$$\sigma(l) \xrightarrow{\sigma^{-1}} l \xrightarrow{(ij)(kl)} k \xrightarrow{\sigma} \sigma(k)$$

Deci, $\sigma(ij)(kl)\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l)) \in K \Rightarrow K \lhd \mathcal{A}_4$.
Aşadar $\mathcal{S}_4$ este rezolubil. ■

Teorema 19.5 *Pentru $n \geq 5$, $\mathcal{S}_n$ nu este rezolubil.*

Demonstraţie. Presupunem $\mathcal{S}_n$ rezolubil rezultă că

$$\exists 1 = H_n \lhd H_{n-1} \lhd ... \lhd H_0 = \mathcal{S}_n.$$

Arătăm că dacă:

$$H_s \supset \{(ijk)|\ \forall\ i, , j,\ k \text{ distincte}\},$$

atunci

$$H_{s+1} \supset \{(ijk)|\ \forall\ i,\ j, k \text{ distincte}\}, \forall s,$$

ceea ce se reduce la

$$H_n = 1 \supset \{(ijk)|\ \forall\ i,\ j,\ k \text{ distincte}\} \text{ fals!}$$

Observăm că: $(jit)^{-1}(kip)^{-1}(jit)(kip) = (ijk)$, deoarece ($\exists\ i, j, k, t, p$ distincte).

$$p \xrightarrow{(kip)} k \xrightarrow{(kip)^{-1}} p$$

$$t \xrightarrow{(jit)} j \xrightarrow{(jit)^{-1}} t$$

$$i \xrightarrow{(kip)} p \xrightarrow{(jit)} p \xrightarrow{(kip)^{-1}} i \xrightarrow{(jit)^{-1}} j$$

$$j \xrightarrow{(jit)} i \xrightarrow{(kip)^{-1}} k$$

$$k \xrightarrow{(kip)} j \xrightarrow{(jit)} t \xrightarrow{(jit)^{-1}} i.$$

Deci,

$$(jit)^{-1}H_{s+1}(kip)^{-1}H_{s+1}(jit)H_{s+1}(kip)H_{s+1} = (ijk)H_{s+1}.$$

Dar $H_{s+1} \lhd H_s$, iar $H_s|_{H_{s+1}}$ abelian, iar $(jit), (kip) \in H_s \Rightarrow$ membrul stang este $H_{s+1} \Rightarrow H_{s+1} = (ijk)H_{s+1} \Rightarrow (ijk) \in H_{s+1}$.

Presupunerea făcută este falsă$\Rightarrow \mathcal{S}_n$ nu este rezolubil. ■

Concluzie

$f \in K[X]$, *car* $K = 0$. $f = 0$ rezolvabilă prin radicali$\Leftrightarrow \exists\, L' \geq K$, $L' \geq \mathcal{C}_f = L \geq K$ (normală, finită, separabilă) $\Leftrightarrow G(\underset{\text{rezolubil}}{K, \mathcal{C}_f}) \leq \mathcal{S}_n$, $n = grad\ f$.

Deci, $f = 0$ rezolvabil prin radicali, dacă $grad\ f \leq 4$.

Teorema 19.6 *Dacă* $f \in \mathbb{Q}[X]$, f *ireductibil, grad* $f = p$, p *prim,* f *are exact* 2 *rădăcini (conjugate) în* $\mathbb{C} - \mathbb{R}$, *atunci* $G_f(\mathbb{Q}) \simeq \mathcal{S}_p$.

Demonstraţie. Avem

$$G_f(\mathbb{Q}) \leq \mathcal{S}_p,\ \mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\underset{\text{răd. lui } f}{\alpha_1, ...\alpha_p}) \geq \mathbb{Q}(\alpha_1) \geq \mathbb{Q}.$$

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = gradf = p \Rightarrow [\mathcal{C}_{f,\mathbb{Q}} : \mathbb{Q}]$$

se divide cu

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p \Rightarrow p||G_f(\mathbb{Q})| = [\mathcal{C}_{f,\mathbb{Q}} : \mathbb{Q}].$$

Conform teoremei lui **Cauchy** rezultă $\exists\ \sigma \in G_f(\mathbb{Q})$, $ord\ \sigma = p$. Pot presupune $\sigma = (i_1, ..., i_p)$ ciclu, $\{i_1, ...i_p\} = \{1, ..., p\}$.

Fie

$$u : \mathbb{C} \to \mathbb{C},\ u(a + bi) = a - bi,\ u|_{\mathbb{R}} = 1_{\mathbb{R}}.$$

$u(\alpha_i) = \alpha_j,\ u(\alpha_j) = \alpha_i,\ \alpha_i, \alpha_j$ sunt unicele răd. din $\mathbb{C} - \mathbb{R}$ conjugate.

u lasă pe loc rădăcinile reale.

De unde rezultă că $G_f(\mathbb{Q})$ conţine o transpoziţie pe care o notăm (ab).

Dar

$$\sigma = (i_1...i_p) = (i_2i_3, ...i_pi_1) = ...$$

$\Rightarrow \sigma$ poate fi scris $\sigma = (a\ j_2...j_p) \Rightarrow \exists\ k \geq 1$ astfel încât

$$\sigma^k = (abl_3...l_p) \in G_f(\mathbb{Q}).$$

Putem presupune $\tau = (12)$, $\sigma = (1\ 2\ 3...p) \in G_f(\mathbb{Q})$

$$\Rightarrow \underbrace{< \tau, \sigma >}_{S_p} \leq G_f(\mathbb{Q}) \Rightarrow \mathcal{S}_p \leq G_f(\mathbb{Q}) \leq \mathcal{S}_p \Rightarrow G_{\ f}(\mathbb{Q}) = \mathcal{S}_p\ .$$

■

Problemă 2 *Fie $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$, f ireductibil. (criteriul lui **Eisenstein**). Să se arate că $f = 0$ nu e rezolvabilă prin radicali.*

Făcând graficul, se observă că f are 3 rădăcini reale. $G_f(\mathbb{Q}) \simeq \mathcal{S}_5$ nu e rezolubil.

Rezultă că $f = 0$ nu este rezolvabilă prin radicali.

Problemă 3 *Fie $f = X^5 - 6X + 3 \in \mathbb{Q}[X]$. Să se arate că $f = 0$ nu este rezolvabilă prin radicali (similar).*

Problemă 4 *Fie $f = 15X^7 - 84X^5 - 35X^3 + 420X + 7 \in \mathbb{Q}[X]$. Să se arate că f=0 nu este rezolvabilă prin radicali. ($p = 7$, crit. Eisenstein)*

Alte exemple de grupuri rezolubile

D_n (grup diedral): grupul izometriilor poligonului regulat cu n laturi.

$D_n = \langle \rho, s \rangle$, ρ : rotaţie de unghi $\frac{2\pi}{n}$ în jurul centrului.

s : simetrie relativ la o axă de simetrie.

$|D_n| = 2n$. Avem

$$\{1\} \leq \underset{\text{abelian}}{\langle \rho \rangle} \lhd D_n, \ |D_n/\rho| = 2.$$

Obţinem că D_n este rezolubil.

Alte rezultate importante cu privire la grupurile rezolubile

Teorema 19.7 *G grup, $|G| = p^n$, p prim. Atunci G rezolubil.*

Demonstraţie. Inducţie după n. Pentru $n \in \{0, 1\}$, G abelian. Dacă $Z(G) \neq G$, atunci $Z(G)$, $G/Z(G)$ au ordin p^m, $m < n \Rightarrow$ sunt rezolubile$\Rightarrow$ G rezolubil. ■

Teorema 19.8 *Dacă G grup, $|G| = \prod_{i=1}^{k} p_i$, p_i prime distincte, atunci G rezolubil.*

Teorema 19.9 *(**Burnside**, 1904) Fie p,q numere prime şi G grup cu $|G| = p^k q^k$, atunci G rezolubil.*

Teorema 19.10 *(**Feit-Thompson**) G grup, $|G|$ impar rezultă G rezolubil.*

Teorema 19.11 *Fie G grup finit. G rezolubil $\Leftrightarrow \exists$ serie normală ciclică, $\forall i$, $|H_{i-1}|_{H_i}| =$prim.*

Observaţie 19.1 *Cel mai mic grup nerezolubil este A_5, $|A_5| = 60$.*

19.2 Seminar nr. 10

Exerciţiu 19.1 *Fie* $f = X^4 - 2 \in \mathbb{Q}[X]$. *Avem* $G_f(\mathbb{Q}) = D_4$.

i) Determinaţi laticea subgrupurilor lui D_4;

ii) Determinaţi laticea subcorpurilor corespunzătoare.

Rezolvare 19.1

i) $a^4 = 1$ (a rotaţie de 90° în jurul centrului pătratatului)

$b^2 = 1$ (b simetrie relativ la o axă de simetrie).

$D_4 = \langle a, b\rangle$, $aba = b$.

$$a = \sigma_7 : \{i \longrightarrow i; \quad \sqrt[4]{2} \longrightarrow -i\sqrt[4]{2},\ b = \sigma_2 : \{i \longrightarrow -i;\ \sqrt[4]{2} \longrightarrow \sqrt[4]{2} \quad ,\ |D_4| = 8.$$

Subgrupurile proprii au ordinele 2 şi 4.
Subgrupurile de ordin 2 sunt generate de elementele de ordin 2:

$$H_1 = 1,\ b \to H_2 = \{b\},\ a^2 \to H_3 = \langle a^2\rangle.$$

$$ab \to H_4 = \langle ab\rangle,\ a^2b \to H_5 = \langle a^2b\rangle,\ a^3b \to H_6 = \langle a^3b\rangle\ .$$

Subgrupuri cu 4 elemente: $H_7 = \langle a\rangle$ şi subgrupuri de tip Klein

$$H_8 = \langle a^2, b\rangle = \langle a^2, a^2b\rangle,\ H_9 = \langle a^2, ab\rangle = \langle a^2, a^3b\rangle,\ H_{10} = D_4.$$

ii) Subcorpurile corespunzătoare:

$$Li = L^{H_i} = \{x|\ \sigma(x) = x, \forall \sigma \in H_i\};$$

$$L_1 = \mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt[4]{2}, i),\ L_{10} = \mathbb{Q};$$

$$L_2 = \{x|\ (b = \sigma_2)(x) = x\} = \mathbb{Q}(\sqrt[4]{2});$$

$$L_3 = \{x|\ a^2(x) = x\} = \mathbb{Q}(i, \sqrt[4]{2});$$

$$a : \{i \longrightarrow i; \quad \sqrt[4]{2} \longrightarrow -i\sqrt[4]{2} \Rightarrow a^2 : \{i \longrightarrow i\ ; \sqrt[4]{2} \longrightarrow -\sqrt[4]{2};$$

$$L_4 = \{x|\ (ab)(x) = x\},\ ab : \{i \xrightarrow{b} -i \xrightarrow{a} -i\ ; \sqrt[4]{2} \xrightarrow{b} \sqrt[4]{2} \xrightarrow{a} -i\sqrt[4]{2};$$

$$x \in \mathbb{Q}(\sqrt[4]{2}, i) \Rightarrow x = a^1 + b^1 i + c\sqrt[4]{2} + d\sqrt[4]{4} + ei\sqrt[4]{4} + fi\sqrt[4]{2} + g\sqrt[4]{8} + hi\sqrt[4]{8}.$$

O bază în ${}_{\mathbb{Q}}\mathbb{Q}(\sqrt[4]{2}, i) : \{1, i\}\ \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$.
Aşadar

$$\begin{aligned}(ab)(x) &= a^1 - b^1 i - ci\sqrt[4]{2} - d\sqrt[4]{4} + ei\sqrt[4]{4} - f\sqrt[4]{2} + gi\sqrt[4]{8} + h\sqrt[4]{8}\ .\\ (ab)(x) &= x \Rightarrow b^1 = 0,\ f = -c,\ d = 0,\ g = h.\end{aligned}$$

De unde rezultă că:

$$\begin{aligned}L_4 &= \{a^1 + c\sqrt[4]{2} + ei\sqrt[4]{4} - ci\sqrt[4]{2} + g\sqrt[4]{8} + gi\sqrt[4]{8}/\ a^1, c, e, g \in \mathbb{Q}\}\\ &= \{a^1 + c(1-i)\sqrt[4]{2} + ei\sqrt[4]{4} + g(1+i)\sqrt[4]{8}/\ a, c, e, g \in \mathbb{Q}\}.\end{aligned}$$

Avem

$$\begin{aligned}\left((1-i)\sqrt[4]{2}\right)^2 &= (1-i)^2\sqrt[4]{4} = -2i\sqrt[4]{4}\ .\\ \left((1-i)\sqrt[4]{2}\right)^3 &= (1-i)^3\sqrt[4]{8} = -2(1+i)\sqrt[4]{8}.\end{aligned}$$

Rezultă

$L_4 = \mathbb{Q}((1-i)\sqrt[4]{2})$.

Similar,

$$L_6 = \{x|\ (a^3b)(x) = x\} \Rightarrow L_6 = \mathbb{Q}((1+i)\sqrt[4]{2});$$

$$L_5 = \{x|\ (a^2b)(x) = x\} = \mathbb{Q}(i\sqrt[4]{2}),\ a^2b : \{i \longrightarrow -i;\ \sqrt[4]{2} \longrightarrow -\sqrt[4]{2};$$

$$L_7 = \{x|\ a(x) = x\} = \mathbb{Q}(i),\ a : \{i \longrightarrow i\ \ ;\sqrt[4]{2} \longrightarrow -i\sqrt[4]{2};$$

$$L_8 = \{x|\ a^2(x) = x \text{ şi } b(x) = x\} = L_3 \cap L_2 = \mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(i, \sqrt[4]{4}) \Rightarrow L_8 = \mathbb{Q}(\sqrt[4]{4}).$$

$$L_9 = \{x|a^2(x) = x \text{ şi } (ab)(x) = x\} = L_3 \cap L_4 = \mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}((1+i)\sqrt[4]{2}) = \mathbb{Q}(i\sqrt[4]{2}).$$

Exerciţiu 19.2 *Fie* $f = X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$.

i) Să se determine $G_f(\mathbb{Q})$;

ii) Determinaţi laticea subgrupurilor lui $G_f(\mathbb{Q})$;

iii) Determinaţi laticea subcorpurilor corespunzătoare.

Rezolvare 19.2

i) $f = (X^2 - 2)(X^2 - 3)$, $\mathcal{C}_f(\mathbb{Q}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Extinderea $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ este Galois.
Elementele lui $G(\mathbb{Q}, \mathbb{Q}(\sqrt{2}, \sqrt{3})$ sunt:

$$u_1 \quad : \quad \{\sqrt{2} \longrightarrow \sqrt{2}; \sqrt{3} \longrightarrow; \sqrt{3}; \quad u_2 : \{\sqrt{2} \longrightarrow \sqrt{2} \ ; \sqrt{3} \longrightarrow -\sqrt{3};$$

$$u_3 \quad : \quad \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow; \sqrt{3} \ ; \ u_4 : \{\sqrt{2} \longrightarrow -\sqrt{2}; \sqrt{3} \longrightarrow -\sqrt{3}.$$

Pentru $\forall\ i$, $u_i^2 = 1 \Rightarrow G_f(\mathbb{Q}) \simeq K$, K grupul lui Klein.

ii), *iii*)

$$H_1 = \{1\} \longrightarrow L_1 = \mathcal{C}_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

$$H_2 = \{1, u_2\} \longrightarrow L_2 = \{x|\ u_2(x) = x\} = \mathbb{Q}(\sqrt{2}).$$

$$H_3 = \{1, u_3\} \longrightarrow L_3 = \{x|\ u_3(x) = x\} = \mathbb{Q}(\sqrt{3}).$$

$$H_4 = \{1, u_4\} \longrightarrow L_4 = \{x|\ u_4(x) = x\} = \mathbb{Q}(\sqrt{6}).$$

$$H_5 = G_f(\mathbb{Q}) \longrightarrow L_5 = \mathbb{Q}.$$

Exerciţiu 19.3 *Aceeaşi problemă pentru* $f = (X^2 + 3)(X^3 - 3)$.

Rezolvare 19.3

i) $\mathcal{C}_f(\mathbb{Q}) = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}(\epsilon, \sqrt[3]{3})$.

Rădăcinile lui $X^2 + 3 : \pm\ i\ \sqrt{3}$;
Rădăcinile lui $X^3 - 3 : \sqrt{3}$, $\epsilon\sqrt[3]{3}$, $\epsilon^2\sqrt[3]{3}$. Unde $\epsilon = \frac{-1 \pm i\sqrt{3}}{2}$, ϵ răd. pentru $X^2 + X + 1$.
Elementele lui $G_f(\mathbb{Q})$ sunt:

$$u_1 : \{\epsilon \longrightarrow \epsilon \ ; \sqrt[3]{3} \longrightarrow \sqrt[3]{3} \ ; \quad u_2 : \{\epsilon \longrightarrow \epsilon \ \ ; \sqrt[3]{3} \longrightarrow \epsilon\sqrt[3]{3}; \quad u_3 : \{\epsilon \longrightarrow \epsilon \quad ; \sqrt[3]{3} \longrightarrow \epsilon^2\sqrt{3}$$

$$u_4 : \{\epsilon \longrightarrow \epsilon^2 \ ; \sqrt[3]{3} \longrightarrow \sqrt[3]{3} \ \ ; \ u_5 : \{\epsilon \longrightarrow \epsilon^2 \ \ ; \sqrt[3]{3} \longrightarrow \epsilon\sqrt[3]{3} \ \ ; \ u_6 : \{\epsilon \longrightarrow \epsilon^2 \quad ; \sqrt[3]{3} \longrightarrow \epsilon^2\sqrt{3} \ .$$

$u_2u_4 \neq u_4u_2 \Rightarrow G_f(\mathbb{Q}) \simeq \mathcal{S}_3$.

$u_4^2 = 1 \Rightarrow u_4$ transpoziţie.
$u_2^3 = 1 \Rightarrow u_2$ ciclu.

ii) Subgrupurile sunt:

$$H_1 = \{1\} \longrightarrow L_1 = \mathcal{C}_f(\mathbb{Q}),\ L_1 = \mathbb{Q}(\epsilon, \sqrt[3]{3});$$

$$H_2 = \{1, u_2, u_2^2 = u_3\} \lhd G_f(\mathbb{Q}),\ L_2 = \{x|\ u_2(x) = x\} = \mathbb{Q}(\epsilon);$$

$$H_3 = \{1, u_4\} \longrightarrow L_3 = \{x|\ u_4(x) = x\} = \mathbb{Q}(\sqrt[3]{3});$$

$$H_4 = \{1, u_6\} \longrightarrow L_4 = \{x|\ u_6(x) = x\} = \mathbb{Q}(\epsilon\sqrt[3]{3});$$

$$H_5 = \{1, u_5\} \longrightarrow L_5 = \{x|\ u_5(x) = x\} = \mathbb{Q}(\epsilon^2\sqrt[3]{3});$$

$$H_6 = G_f(\mathbb{Q}) \longrightarrow\ L_6 = \mathbb{Q}.$$

Observaţie 19.2 *Elementele lui* $\mathbb{Q}(\epsilon, \sqrt[3]{3}) : \mathbb{Q} \leq \mathbb{Q}(\epsilon) \leq \mathbb{Q}(\epsilon, \sqrt[3]{3})$. $B_1 = \{1, \epsilon\}$, $B_2 = \{1, \sqrt[3]{3}, \sqrt[3]{9}\}$, $B = B_1B_2$.

20 Curs 13 - Nr. Liouville

Euler a definit numărele transcendente. **Liouville** a demonstrat existenţa numerelor transcendente.

Definiţie 20.1 $x \in \mathbb{R}$ *se numeşte* ***număr Liouville*** *dacă* $\forall\ n \in \mathbb{N}^*$, $\exists\ p, q \in \mathbb{Z}$, $q > 1$, *astfel încât:*

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}.$$

Un număr Liouville poate fi aproximat destul de bine de un şir de numere raţionale.

1844 : Liouville a demonstrat că toate numerele Liouville sunt transcendente, deci iraţionale.

Teorema 20.1 *Fie* $f \in \mathbb{Z}[X]$, f *ireductibil peste* $\mathbb{Q}$, *grad* $f \geq 2$. *Fie* $\alpha \in \mathbb{R}$, $f(\alpha) = 0$. *Fie* $p, q \in \mathbb{Z}$, $q > 0$ *fixate. Atunci* $\exists\ c > 0$ $(c \in \mathbb{R})$, *astfel încât:*

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^{grad\ f}},\ c \text{ independent de } p \text{ şi } q.$$

Demonstraţie.

Fie $f = a_0 + a_1X + ... + a_rX^r$ şi $\alpha = \alpha_1,\ \alpha_2, ..., \alpha_r$ rădăcinile lui f, într-o extindere a lui $\mathbb{Q}$. Cazuri:

1. $\left|\alpha - \frac{p}{q}\right| \geq 1$, atunci iau $c = 1$ (sau puţin mai mic decât $q = 1$).

2. $\left|\alpha - \frac{p}{q}\right| < 1$, atunci:

$$\left|\alpha_i - \frac{p}{q}\right| = \left|\alpha_i - \alpha + \alpha - \frac{p}{q}\right| < |\alpha_i| + |\alpha| + 1, \forall i.$$

Fie $f = a_r(X - \alpha_1)(X - \alpha_2)...(X - \alpha_r) \Rightarrow$

$$f\left(\frac{p}{q}\right) = |a_r| \cdot \left|\frac{p}{q} - \alpha\right| \cdot \prod_{i=2}^{r} \left|\frac{p}{q} - \alpha_i\right| < |a_r| \cdot \left|\alpha - \frac{p}{q}\right| \cdot \prod_{i=2}^{r} (|\alpha_i| + |\alpha| + 1).$$

$|a_r| \cdot \prod_{i=2}^{r} (|\alpha_i| + |\alpha| + 1) = c^{-1} \Rightarrow c > 0$ şi c independent de p şi q.

Obţinem:

$$\left|f\left(\frac{p}{q}\right)\right| < c^{-1} \left|\alpha - \frac{p}{q}\right|. \tag{1}$$

Pe de altă parte,

$$\begin{aligned} f\left(\frac{p}{q}\right) &= \frac{1}{q^r} \underbrace{(a^r p^r + a^{r-1}p^{r-1}q + ... + a_o q^r)}_{\in \mathbb{Z}} \Rightarrow \\ \left|f\left(\frac{p}{q}\right)\right| &= \frac{1}{q^r} \underbrace{|a^r p^r + ... + a_0 q^r|}_{\geq 1}, \end{aligned}$$

dacă $\frac{p}{q} \neq \alpha_i$ $\left(\text{altfel } f\left(\frac{p}{q}\right) = 0\right)$, iar f ired$|_{\mathbb{Q}}$.

Rezultă

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^r} \tag{2}$$

Din (1) şi (2) rezultă:

$$\frac{1}{q^r} < c^{-1} \left|\alpha - \frac{p}{q}\right| \Rightarrow \frac{c}{q^r} < \left|\alpha - \frac{p}{q}\right|.$$

■

20.1 Criteriul Liouville

Numerele Liouville sunt transcendente

Demonstraţie.

Fie α nr. Liouville $\Rightarrow \forall\ n\ (> grad\ f),\ \exists\ p,q \in \mathbb{Z},\ q > 1$ astfel încât: $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$.

Presupun α algebric $\Rightarrow \exists\ f = Irr(\alpha, \mathbb{Q}) \overset{\text{Teor. ant.}}{\Longrightarrow} \exists\ c > 0 : \left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{grad\ f}}$.

Aşadar obţinem

$$\frac{c}{q^{grad\ f}} < \frac{1}{q^n} \Rightarrow c < q^{\overbrace{grad\ f - n}^{< 0}},$$

pentru că n este foarte mare. Contradicţie!

Deci $\alpha\ trans|_{\mathbb{Q}}$. ■

Exerciţiu 20.1 *Să se arate că* $c = \sum\limits_{n=1}^{\infty} \frac{1}{10^{n!}}$ *(constanta Liouville) este transcendent peste* $\mathbb{Q}$.

p

Rezolvare 20.1

Arăt că c este număr Liouville.

Fie $n \in \mathbb{N}^*$. Definim:

$$p_n = \sum_{j=1}^{n} 10^{n!j!},\ q_n = 10^{n!} > 0.$$

Atunci:

$$\begin{aligned} \left|c - \frac{p_n}{q_n}\right| &= \left|c - \sum_{j=1}^{n} 10^{-j}\right| = \sum_{j=n+1}^{\infty} \frac{1}{10^{j!}} \leq \sum_{j=(n+1)!}^{\infty} \frac{1}{10^j} \\ &= 10^{-(n+1)!} \sum_{j\ \geq 0} 10^{-j}. \end{aligned}$$

Dar

$$\sum_{k\ \geq 0} \frac{1}{b^k} = \frac{b}{b-1} \Rightarrow \sum_{j\ \geq 0} 10^{-j} = \frac{10}{9}.$$

Deci,

$$\left|c - \frac{p_n}{q_n}\right| \leq \frac{10}{9} 10^{-(n+1)!}.$$

Verific că:

$$\left| c - \frac{p_n}{q_n} \right| < \frac{1}{(10^{n!})^n}.$$

$n!n = n!n + n! - n! = n!(n+1) - n! = (n+1)! - n!$.
Trebuie ca:

$$\frac{10}{9} 10^{-(n+1)!} < 10^{-(n+1)!+n!} \Leftrightarrow \frac{10}{9} < 10^{n!} \text{ (adevărat)}$$

Observaţie 20.1 $\underset{poziţia}{c} = 0.\underset{1!}{1}\underset{2!}{1}\underset{3!}{0}0\underset{4!}{1}0...010$

Alte numere Liouville:

- $3.1400\underset{3!}{1}0...0\underset{4!}{5}0...0\underset{5!}{9}...\underset{6!}{2}...$ (unde $\pi = 3.141592...$)
- Similar putem proceda cu orice alt număr infinit, punând zecimale nenule pe poziţia $n!$ ($\forall n \geq 1$) şi 0 în rest. De exemplu, pornind de la 12.299...9..., aşez zecimalele pe poziţa $n!$.
- Cardinalul mulţimii nr. Liouville este c (ca mulţimea tututror şirurilor infinite de zecimale nenule). Totuşi această mulţime are măsura Lebesgue nulă (1980, **J. Oxtoby**)

Numere transcendente celebre

1) $\pi = 3.141592...$(1882, **Lindemann**)

2) e (1873, **Hermite**)

3) 0.123456789101112... (Nr. **Chapernowne**)

4) lg 2 (în baza 10)

5) e^{π}

6) $2^{\sqrt{2}}$ (Nr. **Hilbert**)

Teorema 20.2 ***(Gelfond-Schneider)***

Dacă a, b algebrice, $a \neq 0, 1$, $b \in \mathbb{Q}$, atunci a^b transcendent. (i^i exemplu)

7) $\sum\limits_{k \geq 0} \frac{(-1)^k}{(2k+1)^2}$ (**Constanta lui Catalan**)

8) $\gamma = \lim\limits_{n \to \infty} \left(1 + \frac{1}{2} + ... + \frac{1}{n} - \ln n\right) = 0.577215...$ (**Constanta lui Euler**)

Revenim la exemplul de la **6**), $i^i = e^{i \ln i}$, ln este .....(se ia o determinare principală)

Sau: $e^{ix} = \cos x + i \sin x$, $x = \frac{\pi}{2} \Rightarrow e^{i\frac{\pi}{2}} = i \Rightarrow e^{-\frac{\pi}{2}} = i^i$.

Din teorema **Gelfond-Schneider** rezultă ca dacă a, c algebrice, $a \neq 0, 1$, atunci $\log_a c$ transcendent. (Exemplu: $\log_{10} 2$).

Fie $c = a^b$ cu a, c algebrice, $a \neq 0, 1 \Rightarrow b$ transcendent (altfel, b algebric $\underset{T.G.S}{\Longrightarrow} c$ transcendent)$\Rightarrow \log_a c$ transcendent.

Despre π

Să ne imaginăm o rasă de furnici vorbitoare. Acestea se aşează una în spatele celeilalte, formând un şir infinit.

Prima furnică strigă "3" în $\frac{1}{2}$ min.

A doua "1" în $\frac{1}{4}$ min.

A treia "4" în $\frac{1}{8}$ min.

Fiecare furnică are pe spate numărul strigat de următoarea, dar $\sum_{i \geq 1} \frac{1}{2^i} = 1$, deci într-un minut, toate furnicile vor vorbi, ceea ce ar însemna că la sfârşitul minutului aflăm ultima cifră a lui π! Dar π nu are o ultimă cifră!

Istoric: Hermite, Lindemann, Liouville, Wantzel, Wedderburn, Abel, Galois.

20.2 Seminar nr. 12

Probleme Grupuri rezolubile

Exerciţiu 20.2 *Fie $K \leq L$ ext. Galois, $[L : K] = p^m$, p prim. Atunci $\exists$ $F_i : K = F_0 \leq F_1 \leq ... \leq F_m = L$ astfel încât $\forall$ i $[F_i : F_{i-1}] = p$ şi $K \leq F_i$ ext. Galois.*

Rezolvare 20.2

Avem $|G(K, L)| = [L : K] = p^m \Rightarrow G$ p-grup finit$\Rightarrow G$ rezolubil (finit)

$$\Rightarrow \exists \{e\} \leq H_1 \leq ... \leq H_k = G,$$

cu $\forall$ i, $Hi \lhd G$ şi $[H_i : H_{i-1}] = p$.

Datorită coresp. Galois, obţinem:

$$L^{\{e\}} = L \geq L^{H_1} \geq ... \geq L^{H_k} = K.$$

Verificăm că $\forall$ i, $[L^{H_i} : L^{H_{i+1}}] = p$.

Avem

$$G(L^H, L) = H \Rightarrow [L : L^{H_1}] = [G(L^{H_1}, L)] = |H_1| = p.$$

Apoi,

$$|H_2| \ = |H_1| \cdot |H_2 : H_1| = p^2 \Rightarrow [L : L^{H_2}] = p^2.$$

$$[L : L^{H_2}] = [L : L^{H_1}] \cdot [L^{H_1} : L^{H_2}] = p^2 \Rightarrow [L^{H_1} : L^{H_2}] = p.$$

Exerciţiu 20.3 *Fie $n \geq 1$, α rădăcină primitivă de grad n a lui 1. Determinaţi $G(\mathbb{Q}, \mathbb{Q}(\alpha))$, subgrupurile sale, subcorpurile corespunzătoare.*
Caz particular $n = p$.

Rezolvare 20.3

$\mathbb{Q} \leq \mathbb{Q}(\alpha)$.
Fie $u \in G(\mathbb{Q}, \mathbb{Q}(\alpha)) \Rightarrow u(\alpha)$ răd. primitivă a lui $1 \Rightarrow |G(\mathbb{Q}, \mathbb{Q}(\alpha))| = \varphi(n)$.

Grupul $G(\mathbb{Q}, \mathbb{Q}(\alpha))$ e abelian, pentru că $u_1(\alpha) = \alpha^{k_1},\ (k_1, n) = 1$;
$u_2(\alpha) = \alpha^{k_2},\ (k_2, n) = 1$.
Rezultă că:

$$G(\mathbb{Q}, \mathbb{Q}(\alpha)) \simeq (U(\mathbb{Z}_n), \cdot)$$

$$u \rightsquigarrow k, (k, n) = 1, u(\alpha) = \alpha^k.$$

f izomorfism.
Subgrupurile lui $G(\mathbb{Q}, \mathbb{Q}(\alpha))$ corespund subgrupurilor lui $(U(\mathbb{Z}_n), \cdot)$.
Subcorpurile se determină din teorema fundamentală Galois.

Exerciţiu 20.4 *Fie $n \geq 1$, n par, α răd. primitivă de grad n a lui 1. Demonstraţi echivalenţele:*

i) $|G(\mathbb{Q}, \mathbb{Q}(\alpha))| = \frac{n}{2}$;

ii) $n = 2^k$, adică orice extindere normală $\mathbb{Q} \leq \mathbb{Q}(\theta)$ de grad n conţine doar elemente construibile cu rigla şi compasul.

Rezolvare 20.4

Din $|G(\mathbb{Q}, \mathbb{Q}(\alpha))| = \varphi(n)$, rezultă că avem de arătat echivalenţa:

$$\varphi(n) = \frac{n}{2} \Leftrightarrow n = 2^k,\ k \in \mathbb{N}^*.$$

" $\Longrightarrow$ "

$$n = p_1^{\alpha_1} ... p_s^{\alpha_s} \Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) ... \left(1 - \frac{1}{p_s}\right) \varphi(n) = \frac{n}{2} \qquad \Rightarrow 2\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) = 1.$$

Presupun $s \geq 2$ şi obţinem:

$$1 = 2\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right) \Rightarrow 2(p_1-1)...(p_s-1) = p_1...p_s \text{ cu } p_1 < p_2 < ... < p_s.$$

Aşadar $p_s|2(p_1-1)...(p_s-1)$, dar p_s este mai mare faţă de toţi termenii. Ceea ce rezultă că:

$$s = 1 \Rightarrow n = p_1^{\alpha_1} \Rightarrow 2\left(1-\frac{1}{p_1}\right) = 1 \Rightarrow p_1 = 2 \Rightarrow n = 2^{\alpha_1}.$$

Sau: $2(p_1-1)...(p_s-1) = p_1...p_s \Rightarrow \exists\, i : p_i = 2$.
Fie $p_1 = 2 \Rightarrow (p_2-1)...(p_s-1) = p_2...p_s$ (fals!).

" $\Longleftarrow$ "

$$n = 2^k \Rightarrow \varphi(n) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1}.$$

Exerciţiu 20.5 *Fie $P = X^4+X^3+X^2+X+1$ şi $f = X^2P+P^2 \in \mathbb{Q}[X]$. Ce puteţi spune despre rădăcinile lui f ?*

Rezolvare 20.5

$$\begin{aligned} f &= P(X^2+P) = P(X^4+X^3+2X^2+X+1) \\ &= P(X^2+1)(X^2+X+1) = F_5 \cdot F_4 \cdot F_3 \end{aligned}$$

unde F_5 are gradul 4, F_4 şi F_3 au gradul 2.
Rădăcinile sunt numere construibile cu rigla şi compasul, pentru că

$$\mathbb{Q} \leq \mathbb{Q}(\epsilon) = \mathcal{C}_{F_{2^k}}.$$

Exerciţiu 20.6 *Fie $f = 15X^7-84X^5-35X^3+420X+7 \in \mathbb{Q}[X]$. Stabiliţi dacă $f=0$ e rezolvabilă prin radicali*

Rezolvare 20.6

f ireductibil (crit. **Eisenstein**, $p=7$). Să vedem dacă f are 2 răd. în $\mathbb{C}-\mathbb{R}$ conjugate.

Calculăm derivata:

$$\begin{aligned} f'(X) &= 105X^6-420X^4-105X^2+420 \\ &= 105(X^6-4X^4-X^2+4) \\ &= 105(X^2+1)(X-1)(X+1)(X-2)(X+2). \end{aligned}$$

f' are 4 răd. reale: ± 1, ± 2 şi 2 răd. complexe.

Calculând $f(\pm 1)$, $f(\pm 2)$ aflăm punctele de maxim şi de minim.

$$f(-2) = 215,\ f(1) = 323,\ f(-1) = -309,\ f(2) = -201.$$

f are 2 minime relative negative şi 2 maxime relative pozitive şi deci f schimbă semnul de 5 ori $\left(\lim_{x\to-\infty} f(x) = -\infty, \lim_{x\to\infty} f(x) = +\infty\right)$.

Aşadar f are 5 răd. reale şi 2 complexe conjugate$\Rightarrow$ $G_f(\mathbb{Q}) \simeq \mathcal{S}_5$ nu e rezolubil $\Rightarrow$ f nu e rezolvabilă prin radicali.

21 Curs 14

Extinderi transcendente. Gradul de transcendenţă

Definiţie 21.1 *Fie $K \leq L$. L este* ***extindere transcendentă*** *a lui K, dacă L nu este $alg|_K$.*

Exemplu 21.1 $\mathbb{Q} \leq \mathbb{R}$ *(*$\exists\ e,\ \pi \in \mathbb{R}$, *e,*$\pi$ *transc*$|_{\mathbb{Q}}$*)*

$$K \leq K(X),\ K \leq K(X_1, ..., X_n).$$

Independenţa algebrică

Fie $\underset{\text{mulţime}}{S} \subseteq L$ şi $K \leq L$.

Definiţie 21.2 *S se numeşte* ***alg. independentă*** *peste K dacă elem. lui S nu sunt răd. ale unui polinom nenl, în mai multe nedeterminate, cu coeficienţii din K.*

Rezultă că S este format doar din elemente transcendente.

Aşadar $\forall\{a_1, ..., a_n\} \subset S$, dacă $f(a_1, ..., a_n) = 0$, f cu coeficienţi în K obţinem $f = 0$.

1. $\{a\}$ *indep*$|_K \Leftrightarrow a$ *transc*$|_K$.

2. Nu orice mulţime de elemente transcendente este independentă.

De exemplu, $\{\sqrt{\pi}, 2\pi + 1\} \subseteq \mathbb{R}$ nu e alg indep$|_{\mathbb{Q}}$,deoarece

$$\begin{aligned} f(X_1, X_2) &= 2X_1^2 - X_2 + 1 \neq 0 \\ f(\sqrt{\pi}, 2\pi + 1) &= 2\pi - 2\pi - 1 + 1 = 0. \end{aligned}$$

Definiţie 21.3 *Fie $K \leq L$ ext. transcendentă. Extinderea se numeşte* ***pură*** *dacă $L = K(S)$, unde S alg indep$|_K$.*

Fie $K \leq L$ şi $\underset{\text{mulţime}}{S} \subseteq L$.

Definiţie 21.4 *S se numeşte **bază de transcendenţă** a lui L peste K dacă:*

1. S alg indep$|_K$ şi
2. $K(S) \underset{\text{alg}}{\leq} L$ (mai spunem că S generează alg pe L)

- Pentru $K \leq K(X)$, o bază tr. este $\{X\}$.

Observăm că $\{X, X^2\}$ nu sunt alg indep, pentru că $\exists\ f(U,U) = U^2 - V$ cu răd. X, X^2.

- Pentru $K \leq K(X_1, ..., X_n)$, o bază trans. este $\{X_1, ..., X_n\}$.

Teorema 21.1 *Fie $K \leq L$ extindere transcendentă. Atunci, oricare două baze de transcendenţă ale lui L peste K sunt cardinal echivalente.*

Definiţie 21.5 *Cardinalul unei baze de transcendenţă a lui L peste K se numeşte **gradul de transcendenţă** şi este notat: grad $tr_K L$.*

- Dacă L nu are o bază de transcendenţă finită, atunci *grad* $tr_K L = \infty$.
- Dacă *grad* $tr_K L = 0 \Rightarrow K \underset{\text{alg}}{\leq} L$ şi baza tr. este $\varnothing$.

Exemple
1. Fie $\mathbb{Q} \leq \mathbb{Q}(e, \pi)$. Atunci *grad* $tr_{\mathbb{Q}}\mathbb{Q}(e, \pi) \in \{1, 2\}$. (nu se ştie dacă π şi e sunt alg. independente).

2. Fie $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \pi)$. Atunci *grad* $tr_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \pi) = 1$, pentru că $\sqrt{2}$ *alg*$|_{\mathbb{Q}}$.

3. $\{a \in \mathbb{C}$ sau $a \in \mathbb{R} |\ a$ *alg*$|_{\mathbb{Q}}\}$ numărabilă$\Rightarrow \mathbb{Q} \leq \mathbb{C}$ (sau $\mathbb{Q} \leq \mathbb{R}$) au grad tr. Gradul de transcendenţă oferă o idee intuitivă despre mărimea corpului L.

Teorema 21.2 *Fie $K \leq L$ şi $\underset{\text{submulţimi}}{M, N} \subset L$, M alg indep$|_K$. Echivalenţa:*

i) $M \dot{\cup} N$ alg. indep$|_K$; (unde $\dot{\cup}$ reuniune disjunctă)

ii) N alg. indep$|_{K(M)}$.

Demonstraţie. i) $\Rightarrow$ **ii**) Fie f cu coeficienţi în $K(M)$, $f(n_1, ..., n_s) = 0, n_i \in N$. $\exists$ g cu coeficienţi în K, astfel încât

$$f = g(m_1, ..., m_r) \Rightarrow g(m_1, ..., m_r)(n_1, ..., n_s) = 0 \overset{\text{i)}}{\Rightarrow} g = 0 \Rightarrow f = 0.$$

ii) $\Rightarrow$ **i**) Fie h cu coeficienţi în K şi $h(m_1, ..., m_r, n_1, ..., n_s) = 0$.
Notăm $h(m_1, ..., m_r) = f$.
$\Rightarrow$.}f are coef în $K(M) f(n_1, ..., n_s) = 0 \quad \overset{\text{ii)}}{\Rightarrow} f = 0 \Rightarrow h = 0$.
Folosim acest rezultat în demonstrarea următoarei teoreme. ■

Teorema 21.3 *Fie $K \leq F \leq L$ extindere transcendentă. Atunci :*

$$gradtr_K L = gradtr_K F + gradtr_F L.$$

Demonstraţie. Fie M bază $tr_K F$, N bază $tr_K L$, $M \cap N = \varnothing \Rightarrow$
N alg. indep$|_F \Rightarrow N$ alg. indep$|_{K(M) \subseteq F}$.
Arătăm că $M \cup N$ bază $tr_K L$.
Conform teoremei anterioare, $M \cup N$ alg indep$|_K$.
Să mai arătăm că $K(M \cup N) \underset{\text{alg}}{\leq} L$.
Avem

$$F(N) \underset{\text{alg}}{\leq} L \text{ şi } K(M) \underset{\text{alg}}{\leq} F$$

$$\Rightarrow \quad K(M)(N) = K(M \cup N) \underset{\text{alg}}{\leq} F(N) \underset{\text{alg}}{\leq} L \Rightarrow K(M \cup N) \underset{\text{alg}}{\leq} L.$$

Deci, $M \cup N$ bază $tr_K L$. ■

Observaţie 21.1 *Fie $K \leq L$ şi $y_1, ..., y_n \in L$ astfel încât $y_1, ..., y_n$ alg. indep$|_K$. Atunci $\exists$ izom*

$$K(X_1, ..., X_n) \overset{\varphi}{\simeq} K(y_1, ..., y_n)$$
$$X_i \longrightarrow y_i$$

$Ker\varphi = 0$ din definiţia alg. indep.

Teorema 21.4 *Fie S bază tr. a lui L peste K (unde $K \leq L$). Atunci S este o mulţime maximală alg. indep$|_K$ şi reciproc.*

Demonstraţie.
" $\Longrightarrow$ " S este alg. indep$|_K$.
Să mai arătăm că S este maximală alg.indep.
Fie $y \in L - S$. Cum y alg$|_{K(S)} \Rightarrow .\}\exists\ f \neq 0,\ f(y) = 0 f$ cu coef în $K(S) \Rightarrow$ $S \cup \{y\}$ alg. dep.
Deci S e maximală alg. indep.
" $\Longleftarrow$ " Arătăm că $K(S) \underset{\text{alg}}{\leq} L$.
Fie $y \in L - S \overset{\text{ip}}{\Rightarrow} S \cup \{y\}$ alg. dep $\Rightarrow$

$$\exists\ f \neq 0,\ f(s_1, ..., s_n, y) = 0 \Rightarrow y \text{ alg}|_{K(S)}.$$

■

Teorema 21.5 *Fie $K \leq L$, $\underset{submulţime}{S \subseteq L}$. Echivalenţa:*

1. *S bază tr. a lui L peste K*;
2. *S minimală, astfel încât* $K(S) \underset{\text{alg}}{\leq} L$.
(*S mulţime minimală de gen. alg ai lui L peste K*)

Demonstraţie.
1) $\Rightarrow$ **2**) Arăt că $\forall\, a \in S$, $S - \{a\}$ nu generează alg peste L, adică

$$K(S - \{a\}) \underset{\text{transc}}{\leq} L\ .$$

S alg indep$\Rightarrow$ a transc$|_{K(S-\{a\})} \Rightarrow K(S - \{a\}) \underset{\text{transc}}{\subseteq} L$.
Presupunem a alg$|_{K(S-\{a\})} \Rightarrow \exists\, f \neq 0$, $f(a) = 0$, f cu coeficienţi în $K(S - \{a\}) \Rightarrow S$ alg dep, fals!
2) $\Rightarrow$ **1**) Vrem să arătăm că S alg. indep$|_K$.
Preusupunem S alg. dep$|_K \Rightarrow \exists\, s_1, ..., s_n \in S$,

$$\begin{aligned} f \quad &\in \quad K[X_1, ..., X_n],\ f \neq 0,\ f(s_1, ..., s_n) = 0 \\ &\Rightarrow \quad f(s_2, ..., s_n)(s_1) = 0 \Rightarrow s_1 \text{ alg}|_{K(s_2,...,s_n)}, \end{aligned}$$

unde

$$f(s_2, ..., s_n) \in K[s_2, ..., s_n] - \{0\}.$$

Aşadar obţinem că

$$\begin{aligned} s_1 \text{ alg}|_{K(S-\{s_1\})} \quad &\Rightarrow \quad K(S - \{s_1\}) \underset{\text{alg}}{\subseteq} K(S) \underset{\text{alg}}{\subseteq} L \Rightarrow \\ &\Rightarrow \quad K(S - \{s_1\}) \underset{\text{alg}}{\subseteq} L \text{ (contrazice } \mathbf{2}\text{)}. \end{aligned}$$

■

Problemă 5 *Fie* $K = \mathbb{C}$ *şi* $F = \mathbb{C}[X][Y]/(f(X,Y))$, *unde* $f(X,Y) = Y^2 - (X-a)(X-b)(X-c)$, f *ireductibil,* $f \neq 0$ *în* $\mathbb{C}[X,Y] \Rightarrow F$ *corp.* $\{\hat{X}\}$, $\{\hat{Y}\}$ *baze tr. pentru* $F \Rightarrow$ *grad* $tr_{\mathbb{C}}F = 1$. $\left(f(\hat{X}, \hat{Y}) = 0\right)$.

21.1 Seminarii nr. 13, 14

Istoric:

Tartaglia (Nicola Fontana)
Cardano
Ferrari
Euler, Gauss.

Exerciţiu 21.1 *Arătaţi că următoarele sisteme sunt sisteme de generatori pentru* $\mathcal{S}_n$:

i) $A = \{(1\ 2),\ (1\ 3), ...,\ (1\ n)\}$;

ii) $B = \{(1\ 2),\ (2\ 3), ...,\ (n-1\ n),\ (n\ 1)\}$;

iii) $C = \{(1\ 2),\ (1\ 2...\ n)\}$;

iv) $D = \{(1\ 2),\ (2\ 3...\ n)\}$.

Rezolvare 21.1

i) $\forall\ \sigma \in \mathcal{S}_n$, $\sigma = (i_1,\ j_1)(i_2\ ,j_2)...(i_k\ ,j_k)$.

Dar, $(i_r,\ j_r) = (1\ i_r)(1\ j_r)(1\ i_r)$ (introduc 1 peste tot).

ii) Arătăm că $A \subset [B]$.

Fie $(1\ k) \in A$.

$$\begin{aligned}(1\ k) &= (1\ 2)(2\ k)(1\ 2) \text{ (introduc 2 peste tot)}\\ (2\ k) &= (2\ 3)(3\ k)(2\ 3) \text{ (introduc 3 peste tot)}\\ &...\\ (k-2\ k) &= (k-2\ k-1)(k-1\ k)(k-2\ k-1) \text{ (introduc } k-1 \text{ peste tot)}\end{aligned}$$

Conform celor de mai sus, rezultă că $(1\ k) \in [B]$.

iii) Arătăm că $B \subset [C]$.

Notăm $\alpha = (1\ 2...\ n)$, $\sigma_1 = (1\ 2)$.
Avem

$$\sigma_2 = \alpha\sigma_1\alpha^{-1} = (\alpha(1)\ \alpha(2)) = (2\ 3) \in [C]\text{bf}*$$

$$\begin{aligned}&(2)\\ \sigma_3 &= \alpha\sigma_2\alpha^{-1} = (\alpha(2)\ \alpha(3)) = (3\ 4)\\ &...\\ \sigma_s &= \alpha\sigma_s\alpha^{-1} = (\alpha(s-1)\ \alpha(s)) = (s\ s+1).\end{aligned}$$

Deci $B \subset [C]$.

iv) $C \cap D = \{(1\ 2)\}$.

$(1\ 2\ 3...\ n) = (1\ 2)(2\ 3...\ n) \Rightarrow C \subset [D]$.

Observaţie 21.2 $(*)$ *Pentru* $\sigma = (i_1...i_r)$ *şi* $\alpha \in \mathcal{S}_n$.

$$\alpha\sigma\alpha^{-1} = (\alpha(i_1)...\alpha(i_r))$$

Verific astfel:

$$\alpha\sigma\alpha^{-1}(\alpha(i_s)) = \alpha\sigma(i_s) = \alpha(i_{s+1}).$$