Prctica de Teoria de Galois

Curs 97-98

Prctica 1. Extensions de cossos.

1. Racionalitzeu l'expressi
$$\frac{1}{\sqrt[3]{9}+\sqrt[3]{3}+2}$$

2. Considereu $\mathbb{Q}(u)$ l'extensi de $\mathbb{Q}$ generada per u, una arrel real del polinomi x^3-6x^2+9x+3. Expresseu cadascun dels segents elements en termes de la $\mathbb{Q}-$base $\{1,u,u^2\}$:
$$u^4, u^5, 3u^5-u^4+2, u^{-1}, (1+u)^{-1}, (u^2-6u+8)^{-1}.$$

3. Considerem el cos $K=\mathbb{Q}[x]/x^4-2$. Trobeu tots els cossos L isomorfs a K amb la propietat que $\mathbb{Q}\subset L\subset\mathbb{C}$. La mateixa pregunta per $K=\mathbb{Q}[x]/x^2+D$ amb D un enter lliure de quadrats.

4. Demostreu que $\sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}$ i $\sqrt{2+\sqrt[3]{3+\sqrt[5]{5}}}$ sn $\mathbb{Q}-$algebraics.

5. Proveu que $x^5-27x^3+15x+6$ s irreductible sobre $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

6. Sigui $K|\mathbb{Q}$ una extensi dels racionals de grau 2. Proveu que $\exists d\in\mathbb{Z}$ tal que $K\cong\mathbb{Q}(\sqrt{d})$. Intenteu si es posible generalitzar l'argument per L un cos base arbitari.

7. Siguin p i q dos nombres primers diferents i $F=\mathbb{Q}(\sqrt{p},\sqrt{q})$. Demostreu que:
   (a) $[F:\mathbb{Q}]=4$.
   (b) $\{1,\sqrt{p},\sqrt{q},\sqrt{pq}\}$ s una $\mathbb{Q}-$base de F.
   (c) $F=\mathbb{Q}(\sqrt{p}+\sqrt{q})$.
   (d) $Irr(\sqrt{p}+\sqrt{q},\mathbb{Q})=x^4-2(p+q)x^2+(p-q)^2$.

8. Siguin $L|K, M|K$ extensions finites contingudes en un cos N. Definim LM com el mnim subcos de N que cont L i M. Suposem que $[LM:K]=[L:K][M:K]$. Proveu que es t $L\cap M=K$. Demostreu que val el recproc si un dels dos graus s 2, i doneu un exemple en el qual $L\cap M=K, [M:K]=[L:K]=3$ per en canvi $[ML:K]<9$.(Indicaci: considereu dues arrels cbiques).

9. Siguin $p_1,p_2,\ldots,p_n$ enters positius, primers i diferents. Demostreu que si $q_1,q_2,\ldots,q_r$ sn enters positius, primers dos a dos i tals que els $\sqrt{q_i}$ no siguin enters, i que $m.c.d(p_i,q_j)=1\quad\forall i,j$, aleshores $\sqrt{q_1q_2\ldots q_r}\notin\mathbb{Q}(\sqrt{p_1},\sqrt{p_2},\ldots,\sqrt{p_n})$. Generalitzeu al cas que els p_i noms siguin primers entre ells. Deduu que $[\mathbb{Q}(\sqrt{p_1},\sqrt{p_2},\ldots,\sqrt{p_n}):\mathbb{Q}]=2^n$.
   Com a aplicaci, calculeu els graus de les extensions
$$\mathbb{Q}(\sqrt{2},\sqrt{7},\sqrt{15})|\mathbb{Q},\quad \mathbb{Q}(\sqrt{14},\sqrt{15})|\mathbb{Q}\quad i\quad \mathbb{Q}(\sqrt{6},\sqrt{14})|\mathbb{Q}.$$

10. (Morfisme Frobenious) Considerem K un cos de caracterstica $p \neq 0$ finit. Definim:

$$\Phi_p : K \to K$$
$$x \mapsto x^p$$

(a) Proveu que $\mathbb{F}_p \subset K$ i $\Phi_p \in Aut_{\mathbb{F}_p}(K)$.
Denotem per $\mathbb{F}_{p^i}$ el cos finit de p^i elements.

(b) Construiu un cos de 4 elements. Proveu que tot cos de 4 elements s isomorf a
$$\mathbb{F}_2[x]/(x^2 + x + 1)$$

(c) Intenteu fer l'apartat anterior amb el cos de 16 elements, fent els canvis que corresponguin.

(d) Considerem l'extensi $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ i $K = \mathbb{F}_4$. Proveu llavors que $Aut_{\mathbb{F}_2}(\mathbb{F}_4) = \{id, \Phi_2\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.

(e) Considereu l'extensi $[\mathbb{F}_{16} : \mathbb{F}_4] = 2$ i definim

$$\delta : \mathbb{F}_{16} \to \mathbb{F}_{16}$$
$$x \mapsto x^4$$

Proveu que δ s un isomorfisme de cossos que t per cos fix $\mathbb{F}_4$.
Proveu $Aut_{\mathbb{F}_4}(\mathbb{F}_{16}) = \{id, \delta\}$.
Penseu $\delta = \Phi_2 \circ \Phi_2$ com un $Aut_{\mathbb{F}_2}(\mathbb{F}_{16})$. Proveu

$$Aut_{\mathbb{F}_2}(\mathbb{F}_{16}) =< \Phi_2 >\cong \frac{\mathbb{Z}}{4\mathbb{Z}}$$

11. Proveu que si $L|K$ s una extenci de grau 2 amb $car(K) \neq 2$, es t que

$$\#Aut_K(L) = [L : K].$$

12. Pensem l'extensi $\mathbb{Q}(u)$ de $\mathbb{Q}$ dins $\mathbb{C}$

(a) on u s l'arrel real de $x^3+6x^2+9x+1998$. Observeu que $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Calculeu el grup $Aut_{\mathbb{Q}}(\mathbb{Q}(u))$.

(b) on u s una arrel complexa de $x^3 + 6x^2 + 9x + 1998$. Observeu $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Calculeu el grup $Aut_{\mathbb{Q}}(\mathbb{Q}(u))$.

Prctica de Teoria de Galois

Curs 97-98

Prctica 1. Extensions de cossos.

1. Racionalitzeu l'expressi
$$\frac{1}{\sqrt[3]{9}+\sqrt[3]{3}+2}$$

   Prova. Considerem l'isomorfisme de cossos
$$\varphi : \mathbb{Q}[x]/(x^3-3) \to \mathbb{Q}(\sqrt[3]{3})$$
$$p(x) \mapsto p(\sqrt[3]{3})$$
   Via φ buscar l'invers de $\sqrt[3]{9}+\sqrt[3]{3}+2$ es buscar el polinomi invers de x^2+x+2 en $\mathbb{Q}[x]/(x^3-3)$ i aplicar llavors φ amb aquest polinomi.
   Recordem que com $\mathbb{Q}$-espai vectorial $dim_{\mathbb{Q}}(\mathbb{Q}[x]/(x^3-3)) = [\mathbb{Q}[x]/(x^3-3) : \mathbb{Q}] = 3$ amb una $\mathbb{Q}$-base $\overline{1}, \overline{x}, \overline{x^2}$ per tant cal buscar $a, b, c \in \mathbb{Q}$ complint
$$\overline{(x^2+x+1)(ax^2+bx+c)} = \overline{1}$$
   en $\mathbb{Q}[x]/(x^3-3)$. Sabent que $\overline{x^3} = \overline{3}$ obtenim $a = -\frac{1}{2}, b = c = \frac{1}{2}$ per tant tenim que el polinomi invers s $\overline{\frac{1}{2}(-x^2+x+1)}$ i per tant la racionalitzaci de l'expressi s:
$$\varphi(\overline{\frac{1}{2}(-x^2+x+1)}) = \frac{1}{2}(-\sqrt[3]{9}+\sqrt[3]{3}+1)$$
   $\square$

2. Considereu $\mathbb{Q}(u)$ l'extensi de $\mathbb{Q}$ generada per u, una arrel real del polinomi x^3-6x^2+9x+3. Expresseu cadascun dels segents elements en termes de la $\mathbb{Q}-$base $\{1, u, u^2\}$:
$$u^4, u^5, 3u^5-u^4+2, u^{-1}, (1+u)^{-1}, (u^2-6u+8)^{-1}.$$

   Prova. L'argument es semblant al exercici anterior amb l'isomorfisme de cossos
$$\varphi : \mathbb{Q}[x]/(x^3-6x^2+9x-3) \to \mathbb{Q}(u)$$
$$p(x) \mapsto p(u)$$
   (u una arrel real que fixem del polinomi) i tan sols anoto els resultats:
$$u^4 = 27u^2-54u-18$$
$$u^5 = 105u^2-271u-81$$
$$3u^5-u^4+2 = 288u^2-756u-223$$
$$u^{-1} = -\frac{1}{3}(u^2-6u+9)$$
$$(1+u)^{-1} = \frac{1}{13}(u^2-7u+16)$$
$$(u^2-6u+8)^{-1} = \frac{1}{35}(u^2-9u+1)$$
   $\square$

3. Considerem el cos $K = \mathbb{Q}[x]/x^4 - 2$. Trobeu tots els cossos L isomorfs a K amb la propietat que $\mathbb{Q} \subset L \subset \mathbb{C}$. La mateixa pregunta per $K = \mathbb{Q}[x]/x^2 + D$ amb D un enter lliure de quadrats.

Prova. Observem que si tenim

$$\varphi : K \to L$$

$$\overline{x} \mapsto \alpha$$

on com $\overline{x}$ compleix $\overline{x}^4 = \overline{2}$ i com $\varphi(\overline{2}) = 2$ per ser φ en particular morfisme d'anells amb unitat obtenim que per fora L t un element α que s una arrel quarta de 2. Com $L \subset \mathbb{C}$ tenim que les uniques posibilitats per α son $\{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Observeu que $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(-\sqrt[4]{2})$ i $\mathbb{Q}(i\sqrt[4]{3}) = \mathbb{Q}(-i\sqrt[4]{2})$ per tant tenim que els L que busquem compleixen que $\mathbb{Q}(\sqrt[4]{2}) \subset L$ o b $\mathbb{Q}(i\sqrt[4]{2}) \subset L$ per observem que $Irr_{\mathbb{Q}}(\sqrt[4]{2}) = x^4 - 2 = Irr_{\mathbb{Q}}(i\sqrt[4]{2})$ on $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 = [\mathbb{Q}(i\sqrt[4]{2}) : \mathbb{Q}]$ i com $4 = [K : \mathbb{Q}] = [L : \mathbb{Q}]$ (via φ) tenim llavors que els L buscats sn:

$$\mathbb{Q}(\sqrt[4]{2}) \quad i \quad \mathbb{Q}(i\sqrt[4]{2})$$

Pel cas de $K = \mathbb{Q}[x]/(x^2 + D)$ amb D enter lliure de quadrats, l'argument es semblant i sol us anoto el resultat:

$$D < 0; \quad L = \mathbb{Q}(\sqrt{-D})$$

$$D > 0; \quad L = \mathbb{Q}(i\sqrt{D})$$

per tant en aquest cas sol hi ha una manera de pensar el cos $\mathbb{Q}[x]/x^2 + D$ dins de $\mathbb{C}$. $\square$

4. Demostreu que $\sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}$ i $\sqrt{2 + \sqrt[3]{3 + \sqrt[5]{5}}}$ sn $\mathbb{Q}-$algebraics.

Prova. Recordem que suma de nombres $\mathbb{Q}$-algebraics s $\mathbb{Q}$-algebraic. Tenim llavors com $\sqrt{2}, \sqrt[3]{3}$ i $\sqrt[5]{5}$ sn $\mathbb{Q}$-algebraics (satisfan polinomis sobre $\mathbb{Q}$: $x^2 - 2, x^3 - 3, x^5 - 5$ respectivament obtenim que $\sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}$ s $\mathbb{Q}$-algebraic.
Recordem igualment que tot element de tota extensi finita de cossos sobre K sn K-algebraics; per tant utilitzant suma d'algebraics s algebraic obtenim que $3 + \sqrt[5]{5}$ s $\mathbb{Q}$-algebraic com $\alpha = \sqrt[3]{3 + \sqrt[5]{5}}$ $\alpha^3 = 4 + \sqrt[5]{5}$ per tant $\mathbb{Q}(\alpha)|\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$ totes finites, on α s $\mathbb{Q}$-algebraic, un raonament semblant a l'ltim prova que $\sqrt{2 + \sqrt[3]{3 + \sqrt[5]{5}}}$. $\square$

5. Proveu que $x^5 - 27x^3 + 15x + 6$ s irreductible sobre $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Prova. Utilitzant el criteri de Eisentein pel primer $p = 3$ obtenim que el polinomi $P(x) = x^5 - 27x^3 + 15x + 6$ s irreductible sobre $\mathbb{Q}[x]$. Per un exercici de problemes de la 1era plana ens diu que si $P(x)$ s irreductible sobre $K[x]$ (K cos) i si tenim una extensi L finita de K amb $m = [L : K]$, llavors si $deg(P(x))$ s coprimer amb m s'obt que $P(x)$ s irreductible sobre $L[x]$.
Utilitzant aquest resultat que ja coneixeu i com $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ obtenim el resultat. $\square$

6. Sigui $K|k$ una extensi i $\alpha, \beta \in K$.
   Proveu que si $\alpha + \beta$ i $\alpha\beta$ sn algebraics sobre k, aleshores α i β tamb.

   Prova. Observem que α, β sn les solucions del polinomi

   $$x^2 - (\alpha + \beta)x + \alpha\beta$$

   en $k(\alpha + \beta, \alpha\beta)$, per tant tenim que $[k(\alpha, \beta) : k(\alpha + \beta, \alpha\beta)] < \infty$ s a dir una extensi algebraica i com $k(\alpha + \beta, \alpha\beta)|k$ era una extensi algebraica per hipptesi, tenint ,tot recordant que composici de extensions algebraiques s algebraica, l'enunciat; s a dir α, β sn algebraics sobre $\mathbb{Q}$. $\square$

7. Sigui $K|\mathbb{Q}$ una extensi dels racionals de grau 2. Proveu que $\exists d \in \mathbb{Z}$ tal que $K \cong \mathbb{Q}(\sqrt{d})$. Generalitzar l'argument per L cos base arbitari.

   Prova. Sigui $\alpha \in K \setminus \mathbb{Q}$. Com $[K : \mathbb{Q}] = 2$ tenim que α^2 compleix una relaci $\mathbb{Q}$-lineal amb $\alpha, 1$; s dir hi ha $b, c \in \mathbb{Q}$ on

   $$\alpha^2 = b\alpha + c$$

   Com $\alpha \notin \mathbb{Q}$ tenim que el polinomi $x^2 - bx - c$ no t arrels a $\mathbb{Q}$ per tant per ser de grau 2 s irreduible sobre $\mathbb{Q}[x]$; tenim llavors l'isomorfisme de cossos

   $$\gamma : \mathbb{Q}[x]/(x^2 - bx - c) \to K$$

   pel fet de ser $[K : \mathbb{Q}] = 2$. Igualment com tenim que podem escriure una arrel de $x^2 - bx - c$ com $\beta = \frac{+b+\sqrt{\Delta}}{2}$ i com $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{\Delta})$ i un isomorfisme β' de $\mathbb{Q}[x]/(x^2 - bx - c)$ a $\mathbb{Q}(\beta)$ que s avaluar en β obtenim un isomorfismde de

   $$\gamma \circ {\beta'}^{-1} : \mathbb{Q}(\sqrt{\Delta}) \to K$$

   (Nota: $\Delta = b^2 + 4c$).
   Per a un cos arbitrari l'argument anterior (canviant $\mathbb{Q}$ pr L) s vlid sempre que $car(K) \neq 2$ ja que l'expressi de β sempre s vlida algebraicament(per car$\neq 2$).
   Per $car(L)(= car(K)) = 2$ l'enunciat no s correcte, ja que $\mathbb{F}_4 = \mathbb{F}_2(\psi)$ on ψ s una arrel cbica de la unitat ψ s arrel de $x^3 - 1$ (el seu polinomi irreduible s $x^2 + x + 1$). $\square$

8. Siguin p i q dos nombres primers diferents i $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Demostreu que:

   (a) $[F : \mathbb{Q}] = 4$.
   (b) $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ s una $\mathbb{Q}-$base de F.
   (c) $F = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.
   (d) $Irr(\sqrt{p} + \sqrt{q}, \mathbb{Q}) = x^4 - 2(p + q)x^2 + (p - q)^2$.

Prova. (a) Veiem que $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2 = [F : \mathbb{Q}(\sqrt{p})]$ i llavors com $[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}) : \mathbb{Q})]$ obtindrem el resultat.

Recordem que si tenim una extensi algebraica simple $k(\alpha)|k$ s t $[k(\alpha) : k] = deg(Irr_k(k(\alpha))$ i t $k(\alpha)$ com a k-base $1, \alpha, \ldots, \alpha^{[k(\alpha):k]-1}$.

s clar que $Irr_{\mathbb{Q}}(\sqrt{p}) = x^2 - p$ (irreduible pel criteri Eisenstein) on obtenim que $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

Observem que $Irr_{\mathbb{Q}(\sqrt{p})}(\sqrt{q})|x^2 - q$ ja que $\sqrt{q}$ s arrel de $x^2 - q$ i aquest polinomi s de $\mathbb{Q}(\sqrt{p})[x]$. L'nica posibilitat que $x^2 - q$ no fos l'irreductible s que el polinomi irreductible fos de grau 1; s a dir que $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$. Anem a veure que aix no pasa. Si pases tindriem que hi ha $a, b \in \mathbb{Q}$ complint

$$\sqrt{q} = a + b\sqrt{p}$$

tenim llavors $q = a^2 + b^2p + 2ab\sqrt{p}$ on com $\sqrt{p} \notin \mathbb{Q}$ obtenim que $ab = 0$. Si $b = 0$ tenim $\sqrt{q} = a \in \mathbb{Q}$!! no pot ser; si $a = 0$ $\sqrt{q} = b\sqrt{p}$ on $\sqrt{pq} \in \mathbb{Q}$!!! no pot ser. Aix prova que $Irr_{\mathbb{Q}(\sqrt{p})}(\sqrt{q}) = x^2 - q$; provant aix que

$$[F : \mathbb{Q}] = 4$$

(b) Tenim que $\{1, \sqrt{p}\}$ s una $\mathbb{Q} - base$ de $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$; igualment sabem $\{1, \sqrt{q}\}$ s una $\mathbb{Q}(\sqrt{p})$-base de $F|\mathbb{Q}(\sqrt{p})$. Veiem que $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ s una $\mathbb{Q}$-base de F.

Veiem que sn $\mathbb{Q}$-linealment independents.

$$a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} = 0$$

$a, b, c, d \in \mathbb{Q}$. Escrivim l'anterior expressi per:

$$0 = (a + b\sqrt{p}) + \sqrt{q}(c + d\sqrt{p})$$

pel fet de ser $\{1, \sqrt{q}\}$ una $\mathbb{Q}(\sqrt{p})$-base obtenim

$$0 = a + b\sqrt{p} \quad 0 = c + d\sqrt{p}$$

pel fer de ser $\{1, \sqrt{p}\}$ una $\mathbb{Q}$-base obtenim $a = b = c = d = 0$ provant que $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ sn $\mathbb{Q}$-linealment independents. Per veure que sn una $\mathbb{Q}$-base de F cal veure que generem; per com tenim 4 elements de F $\mathbb{Q}$-linealment independents i $[F : \mathbb{Q}] = 4$ obtenim el resultat.

(c) Anotem $L = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. s clar que $\sqrt{p} + \sqrt{q} \in F$ per tant $\mathbb{Q} \subset L \subset F$. Per provar l'enunciat s suficient provar que $[L : \mathbb{Q}] = 4 = deg(Irr_{\mathbb{Q}}(\sqrt{p} + \sqrt{q}))$(on l'ltima igualtat prova del fet de ser L una extensi simple amb l'element $\sqrt{p} + \sqrt{q}$).

Anem a estudiar $deg(Irr_{\mathbb{Q}}(\sqrt{p} + \sqrt{q}))$ sabem que ha de dividir $4 = [F : \mathbb{Q}]$. Grau 1 no pot ser ja que llavors tindriem $\sqrt{p} + \sqrt{q} \in \mathbb{Q}$ on tindriem elevant al quadrat que $\sqrt{pq} \in \mathbb{Q}$ cosa que no pot ser. Per tant el grau nicament pot ser 2 o 4. Veiem que 2 no pot ser acavant aix aquest apartat.

Si $Irr_{\mathbb{Q}}(\sqrt{p} + \sqrt{q}) = x^2 + ax + b$ tenim llavors per definici de polinomi irreduible

$$(\sqrt{p} + \sqrt{q})^2 + a(\sqrt{p} + \sqrt{q}) + b = 0$$

on tenim del fet que $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ era $\mathbb{Q}$-base s'obt que $2 = 0$ mirant el coeficient de $\sqrt{pq}$; obtenim doncs que el polinomi irreduible no pot ser de grau 2. Provant aix que el grau s 4.

(d) s comprova que $\sqrt{p}+\sqrt{q}$ anul.la el polinomi i com en l'apartat anterior tenim que el polinomi irreduible s de grau 4 obtenim per unicitat d'aquests polinomis el resultat.

$\square$

9. Siguin $L|K, M|K$ extensions finites contingudes en un cos N. Definim LM com el mnim subcos de N que cont L i M. Suposem que $[LM : K] = [L : K][M : K]$. Proveu que es t $L \cap M = K$. Demostreu que val el recproc si un dels dos graus s 2, i doneu un exemple en el qual $L \cap M = K, [M : K] = [L : K] = 3$ per en canvi $[ML : K] < 9$.

Prova. Veiem primer que $L \cap M = K$.
Anotem $n = [L : K]$ i $m = [M : K]$. Sigui $\delta = [L \cap M : K]$, $\beta_1 = [M : L \cap M]$ $\beta_2 = [L : L \cap M]$, observem que tenim $m = \beta_1 \delta$ i $n = \beta_2 \delta$. Volem veure que $\delta = 1$, provant aix l'enunciat.
Com $[LM : K] = [LM : L][L : K] = [LM : M][M : K] = [L : K][M : K]$ tenim que $m = [LM : L]$ i $n = [LM : M]$. Provem que $[LM : M] \leq [L : L \cap M]$ provant aix que $\beta_2 = n$ on $\delta = 1$.
Tenim $L = (L \cap M)(\alpha_1, \ldots, \alpha_l)$, tenim que $M(\alpha_1, \ldots, \alpha_l)$ cont $(L \cap M)(\alpha_1, \ldots, \alpha_l)$ i M i com est dins LM tenim que $LM = M(\alpha_1, \ldots, \alpha_l)$ (raonant que fent extensions afegint cada α_i trobem el grau extensi i com els polinomis irreduibles α_i sobre $M(\alpha_1, \ldots, \alpha_{i-1})$ dividirant el polinomi irreductible de α_i sobre $L \cap M(\alpha_1, \ldots, \alpha_{i-1})$ tenim) per tant $[LM : M] \leq [L : L \cap M]$. On utilitzant comentaris anteriors acavem.
Veiem el recproc quan $[L : K] = 2$ o $[M : K] = 2$. Volem demostrar que $[LM : K = L \cap M] = [M : K][L : K]$. Sense perdua de generalitat podem suposar que $[M : K] = 2$. Hem demostrat abans que sempre tenim $[LM : L] \leq [M : L \cap M = K] = 2$. Denotem $\tau = [LM : L]$. Si $\tau = 1$ tenim $LM = L$ on $M \subset L$, per tant $L \cap M = L = LM$ i totes les extensions involucrades son de grau 1 i es clar que es t l'igualtat $[LM : K] = [M : K][L : K]$.
Si $\tau = 2$ si $n_1 = [L : K]$ tenim $[LM : K] = [LM : L][L : K] = 2n_1 = [M : K][L : K]$ com voliem veure.
Explicitem ara un exemple on $L \cap M = K$, $[M : K] = [L : K] = 3$ i $[ML : K] < 9$.

Es clar que $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\sqrt[3]{2}\xi) = \mathbb{Q}$ ja que un cos s totalment real i l'altre imaginari (ξ denota una arrel cbica complexa de la unitat)(Exercici al lector veure que la intersecci es $\mathbb{Q}$). $\square$

10. Siguin $p_1, p_2, ..., p_n$ enters positius, primers i diferents. Demostreu que si $q_1, q_2, ..., q_r$ sn enters positius, primers dos a dos i tals que els $\sqrt{q_i}$ no siguin enters, i que $m.c.d(p_i, q_j) = 1 \quad \forall i, j$, aleshores $\sqrt{q_1 q_2 ... q_r} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$. Generalitzeu al cas que els p_i noms siguin primers entre ells.

    Prova. Demostrem primer el primer apartat per inducci sobre n:
    Sigui $P(n) = \{\sqrt{q_1 q_2 ... q_r} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})\}$ Veiem primer que $P(1)$ s veritat. Suposem que $\sqrt{q_1 \dots q_r} \in \mathbb{Q}(\sqrt{p})$ llavors $\sqrt{q_1 \dots q_r} = a + b\sqrt{p}$ amb $a, b \in \mathbb{Q}$. D'aqu tenim

    $$q_1 \dots q_r = a^2 + b^2 p + 2ab\sqrt{p}$$

    per tant $ab = 0$,si $a = 0$ s'obt que $\sqrt{pq_1 \dots q_r} \in \mathbb{Q}$ cosa que no pot ser, si $b = 0$ tenim que $\sqrt{q_1 \dots q_r} \in \mathbb{Q}$ cosa que tampoc pot ser, provant aix que $P(1)$ s veritat.
    Suposem que es compleix $P(k-1)$ veiem que es compleix $P(k)$.
    Suposem que no es complis $P(k)$. Si

    $$\sqrt{q_1 \dots q_r} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k}) = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})(\sqrt{p_k})$$

    tenim $\sqrt{q_1 \dots q_r} = \iota + \tau\sqrt{p_k}$, $\iota, \tau \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})$ observem com $q_1 \dots q_r - 2\tau\sqrt{q_1 \dots q_r p_k} + \tau^2 p_k = \iota^2$ tenim com $\sqrt{q_1 \dots q_r p_k} \notin \mathbb{Q}(\sqrt{p_1}, \dots \sqrt{p_{k-1}})$(hiptesi inducci) s'ha de complir $\tau = 0$ on s'obtindria $\sqrt{q_1 \dots q_r} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})$ cosa que no pot ser per inducci; provant aix que $P(k)$ es dona si pasa $P(k-1)$. Provant aix per inducci que $P(n)$ s veritat per tot $n \in \mathbb{N}$.
    La mateixa prova serveix per la generalitzaci. $\square$

    Deduu que $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$.($p_i$ no quadrats)
    Com a aplicaci, calculeu els graus de les extensions

    $$\mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{15})|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{14}, \sqrt{15})|\mathbb{Q} \quad i \quad \mathbb{Q}(\sqrt{6}, \sqrt{14})|\mathbb{Q}.$$

    Prova. Provem per inducci $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$. Si $n = 1$ gracies al criteri de Eisenstein per p_1 obtenim que $Irr_{\mathbb{Q}}(\sqrt{p_1}) = x^2 - p_1$ i per tant $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$. Suposem certa la frmula per $k-1$ i veiem-ho per k.

    $$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})(\sqrt{p_k}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})][\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}}) : \mathbb{Q}]$$

    on obtenim aplicant l'hiptesi d'inducci:

    $$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k} : \mathbb{Q}] = 2^{k-1}[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})(\sqrt{p_k}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})]$$

    pel treball fet anteriorment en aquest exercici tenim que $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})$ per tant obtenim que $Irr_{\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{k-1}})}(\sqrt{p_k}) = x^2 - p_k$ provant aix la frmula pel cas k. Per tant per inducci obtenim la validesa del resultat per $n \in \mathbb{N}$.
    Utilitzant aquest resultat obtenim:

    $$[\mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{15}) : \mathbb{Q}] = 2^3 = 8$$

ja que $2, 7, 15$ no son quadrats i sn coprimers 2 a 2, igualment fent un comentari semblant per $14, 15$ tenim

$$[\mathbb{Q}(\sqrt{14}, \sqrt{15}) : \mathbb{Q}] = 4$$

. Pel clcul de $[\mathbb{Q}(\sqrt{6}, \sqrt{14}) : \mathbb{Q}]$ pel fet de ser $(6, 14) \neq 1$ no podem aplicar directament el resultat. Es clar que $[\mathbb{Q}(\sqrt{6} : \mathbb{Q}] = 2$. Per provar que l'extensi $[\mathbb{Q}(\sqrt{6}, \sqrt{14}) : \mathbb{Q}] = 4$ s suficient provar que $[\mathbb{Q}(\sqrt{14}, \sqrt{6}) : \mathbb{Q}(\sqrt{6})] = 2$, per aix s veure que $Irr_{\mathbb{Q}(\sqrt{6})}(\sqrt{14}) = x^2 - 14$ i per veure aix ltim es suficient veure que $\sqrt{14} \notin \mathbb{Q}(\sqrt{6})$ (exercici al lector). $\square$

11. (Morfisme Frobenious) Considerem K un cos de caracterstica $p \neq 0$ finit. Definim:

$$Frob_p : K \to K$$

$$x \mapsto x^p$$

   (a) Proveu que $\mathbb{F}_p \subset K$ i $Frob_p \in Aut_{\mathbb{F}_p}(K)$.

   (b) Considerem l'extensi $[\mathbb{F}_4 : \mathbb{F}_2] = 2$ i $K = \mathbb{F}_4$. Proveu llavors que $Aut_{\mathbb{F}_2}(\mathbb{F}_4) = \{id, Frob_2\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$.

   (c) Considereu l'extensi $[\mathbb{F}_{16} : \mathbb{F}_4] = 2$ i definim

$$\delta : \mathbb{F}_{16} \to \mathbb{F}_{16}$$

$$x \mapsto x^4$$

   Proveu que δ s un isomorfisme de cossos que t per cos fix $\mathbb{F}_4$.
   Proveu $Aut_{\mathbb{F}_4}(\mathbb{F}_{16}) = \{id, \delta\}$.
   Penseu $\delta = Frob_2 \circ Frob_2$ com un $Aut_{\mathbb{F}_2}(\mathbb{F}_{16})$. Proveu

$$Aut_{\mathbb{F}_2}(\mathbb{F}_{16}) =< Frob_2 >\cong \frac{\mathbb{Z}}{4\mathbb{Z}}$$

Prova. (a) Com K t caracterstica p tenim que

$$\iota : \mathbb{F}_p \to K$$

$$[a] \mapsto a$$

s injecci de cossos. Per tant podem pensar via ι que $\mathbb{F}_p \subset K$. Per provar que $Frob_p$ s un morfisme de cossos, s'utilitza que $p|\left(\binom{}{pk}\right)$ (exercici al lector). Recordeu com el nucli d'un morfisme d'anells s un ideal, i els unics ideals d'un cos s el zero i el total, tenim com $Frob_p$ no s nul que $Frob_p$ s injectiu. Veiem-ne l'exhaustivitat. Com tenim que K s un cos finit i com iota s injectiva $\#Frob_p(K) = \#K$ dient-nos que per fora el morfisme s exhaustiu. Per veure que $Frob_p \in Aut_{\mathbb{F}_p}(K)$; unicament ens falta comprovar que $Frob_p(a) = a$ per tot $a \in \mathbb{F}_p$; per aix s justament el teorema petit de Fermat. Per tant obtenim que $Frob_p \in Aut_{\mathbb{F}_p}(K)$.

(b) Grcies a l'apartat anterior tenim que $Frob_2 \in Aut_{\mathbb{F}_2}(\mathbb{F}_4)$. Per tant tenim que $id, Frob_2 \in Aut_{\mathbb{F}_2}(\mathbb{F}_4)$. Observem que $Frob_2^2 = id$; aix ve del fet que $\mathbb{F}_4$ sn les arrels cbiques de la unitat amb el zero i per tant $x^4 = x$ per tot $x \in \mathbb{F}_4$. Per tant unicament cal veure que tot automorfisme que no s la identitat en $Aut_{\mathbb{F}_2}(\mathbb{F}_4)$ s el Frobenious. Com $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ amb α complint l'igualtat

$$\alpha^2 + \alpha + 1 = 0$$

si $\sigma \in Aut_{\mathbb{F}_2}(\mathbb{F}_4)$ tenim llavors que $\sigma(\alpha)$ s una arrel de $x^2+x+1 = 0$; per tant pot ser α o l'altra arrel β (diferent, comproveu-ho); si $\sigma(\alpha) = \alpha$ tenim llavors $\sigma = id$. Si $\sigma(\alpha) = \beta$ com $\beta \in \mathbb{F}_4$ (raoneu perque) tenim dona un altre posible automorfisme, pero llavors obtenim que com a molt tenim dos automorfismes; per tant per fora $Aut_{\mathbb{F}_2}(\mathbb{F}_4) = \{id, Frob_2\}$.

(c)

$\square$

12. Proveu que si $L|K$ s una extenci de grau 2, $car(K) \neq 2$ es t que $\#Aut_K(L) = [L : K]$.

13. Pensem l'extensi $\mathbb{Q}(u)$ de $\mathbb{Q}$ dins $\mathbb{C}$

    (a) on u s l'arrel real de $x^3+6x^2+9x+1998$. Observeu que $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Calculeu el grup $Aut_{\mathbb{Q}}(\mathbb{Q}(u))$.

    (b) on u s una arrel complexa de $x^3 + 6x^2 + 9x + 1998$. Observeu $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Calculeu el grup $Aut_{\mathbb{Q}}(\mathbb{Q}(u))$.

Prctica de Teoria de Galois

Curs 97-98

Prctica 2. Grups finits.

1. **Grups Commutatius.** Descriu els reticles de subgrups dels segents grups:
$$C_n, \quad C_p, \quad C_{p^2}, \quad C_{p^n}, \quad C_2 \times C_2, \quad C_p \times C_p$$

2. **Grups d'ordre** 6
   (a) Descriu el reticle de subgrups de S_3.
   (b) Demostra que tot grup d'ordre 6 s isomorf a $\mathbb{Z}/6\mathbb{Z}$ o b a S_3.

3. **Grups Diedrals**
   (a) Descriu el reticle de subgrups de $D_4 = \{r, s | r^4 = s^2 = 1, srs = r^3\}$ grup d'isometries del quadrat.
   (b) Feu el mateix exercici amb $D_p = \{r, s | r^p = s^2 = 1, srs = r^{p-1}\}$ grup d'isometries del p-gon regular, p primer.

4. **Grup quaternionic.**
   Sigui H_8 el subgrup multiplicatiu que s'obt dels quaternions de Hamilton generat per $\{i, j\}$.
   (a) Doneu una presentaci amb generadors i relacions de l'anterior grup.
   (b) Comprova que H_8 s un grup no commutatiu de 8 elements.
   (c) Descriu el reticle de subgrups.

5. **Grups d'ordre** 8
   (a) Proveu que si grup G satisf $x^2 = 1 \quad \forall x \in G$, aleshores s abeli.
   (b) Proveu que tot grup no abeli de 8 elements s isomorf a D_4 o a H_8.

6. Descriu el reticle de subgrups de A_4

7. **Grups d'ordre** p^2
   (a) Sigui G un grup i H un subgrup del centre de G. Demostreu que si el grup quocient G/H s cclic, aleshores G s commutatiu.
   (b) Demostreu que tot grup d'ordre p^2 amb p primer s commutatiu.

8. En els problemes anteriors:
   (a) Calculeu l'ordre dels subgrups.
   (b) Calculeu els ndexos.
   (c) Dir quins subgrup sn normals.

   - **Algun estudi de** $Aut_K(L)$

9. Considereu el cos $\mathbb{Q}(\sqrt[3]{2}, \omega)$ on ω s una arrel cbica de la unitat. Calculeu $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$ i $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega))$. Considereu un subgrup d'ndex 2 de l'anterior grup. Intenteu trobar quins elements de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ queden fixats per aquest subgrup. Sn un cos?.

10. Considerem el cos $F = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ amb p, q primers diferents. Calculeu $Aut_{\mathbb{Q}}(F)$. Escriviu el reticle de l'anterior grup. Per cada subgrup intenteu trobar quins son els elements de F que queden fixats per subgrup que heu triat.

Prctica de Teoria de Galois

Curs 97-98

Prctica 3. La correspondncia de Galois.

1. Calculeu el reticle de subgrups i subcossos de les extensions obtingudes al adjuntar a $\mathbb{Q}$ les arrels dels segents polinomis de l'apartat a):

   (a) $X^n - 1, n \leq 8 \quad (X^2-2)^n(X^2-3)^m, \forall m, n \geq 0$

   (b) Demostra que els grups de Galois de l'apartat anterior sn commutatius.
   Descriu el Grup de Galois dels segents polinomis:

   (c) $X^6 + 3 \quad X^{15} - 2$

2. Expliciteu els cossos intermitjos que hi ha en l'extensi sobre $\mathbb{Q}(\pi)$ al adjuntar les arrels dels polinomis:

   (a) $(x^2-p)(x^2-q)$ on $p, q \in \mathbb{Z}$ sn nombres primers diferents.
   Descriu el Grup de Galois del polinomi $x^3 + nx + n$ amb $n \neq 1$ un natural no nul lliure de quadrats.

3. (a) Demostra que el conjunt format per les matrius

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \quad , \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

   quan $\zeta = \zeta_{q-1}$ s una arrel primitiva $(q-1)-$sima de la unitat i b recorre $\mathbb{F}_q^*$, s un sistema de generadors del grup lineal $GL_2(\mathbb{F}_q)$.

   (b) Demostreu que el grup de Galois G sobre $\mathbb{Q}$ del polinomi $X^p - a$, on p s un nombre primer i $a \neq \pm 1$ s un enter lliure de quadrats, s isomorf al subgrup de $GL_2(\mathbb{F}_p)$ format per les matrius

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$$

   tals que $x \in \mathbb{F}_p^*$ i $y \in \mathbb{F}_p$.

4. Recordeu que el cicle $(1, 2, ..., n)$ i la trasposici $(1, 2)$ generen el grup simtric S_n.

   (a) Sigui $f \in \mathbb{Q}[X]$ un polinomi irreductible de grau primer p. Suposem que f t exactament dues arrels complexes no reals. Demostreu que es seu grup de Galois sobre $\mathbb{Q}$,$G_{\mathbb{Q}}(f)$, s isomorf a S_p.

   (b) Determineu el grup de Galois sobre $\mathbb{Q}$ del polinomi $X^5 - 2pX + p$, p primer.

5. Sigui k un cos amb caracterstica $p > 0$, i sigui $K = k(x, y)$ el cos de les funcions racionals de dues variables sobre k. Posem $F = k(x^p, y^p)$.

   (a) Proveu $[K : F] = p^2$.

(b) Observeu que K s el cos de descomposici sobre F del polinomi $(X^p - x^p)(X^p - y^p)$. Proveu que $Aut_F(K) = \{id\}$.

(c) Veieu que $K^p \subset F$.

(d) Demostreu que no hi ha $\alpha \in K$ amb $K = F(\alpha)$.

(e) Doneu una infinitat de cossos intermitjos de $K|F$.

6. Sigui F un cos de caracterstica diferent de 2. Sigui K una extensi de Galois amb $[K : F] = 4$. Suposem que $Gal(K|F) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Proveu $K = F(\sqrt{a}, \sqrt{b})$ per algun $a, b \in F$.

Teoria de Galois

Prctica 5. Extensions radicals.

Curs 97-98

1. Doneu expressions radicals sobre $\mathbb{Q}$, en cas de poder-ho fer, per les solucions del polinomi:
   (a) $x^5 + x + 1$.
   (b) $x^9 - 15x^6 + 75x^3 - 127$.
   (c) $x^5 - 6x + 3$

2. Doneu l'expressio radical per $3e^{2\pi i/5}$.

3. Considerem la clausura algebraica M del cos finit $\mathbb{F}_p$. Considerem el cos $K = M(x)$. Considereu el polinomi $f(T) = T^p - T - x \in K[T]$. Proveu que $Gal_K(f)$ s un grup cclic (en particular un grup resoluble), per proveu que les solucions del polinomi $f(T)$ no sn radicals sobre K.

4. Construcci del polgon regular de 17 costats: [1]
   Siguin $\epsilon_k = cos(k\theta) + isin(k\theta)$ on $1 \leq k \leq 16$ i $\theta = 2\pi/17$ les arrels del polinomi ciclotomic $\phi_{17}(x)$
   (a) Calculeu $r_m = 3^m \quad mod \quad 17$ per $0 \leq m \leq 15$
   (b) Definim
   $$x_i = \sum_{m \equiv i \; mod \; 2} \epsilon_{r_m} \qquad y_j = \sum_{m \equiv j \; mod \; 4} \epsilon_{r_m}$$
   per $i = 0, 1 \quad j = 0, 1, 2, 3$. A partir de la igualtat $\epsilon_k + \epsilon_{17-k} = 2cos(k\theta)$ expreseu x_i, y_j en funci de $cos(k\theta)$
   (c) Comproveu que x_0, x_1 sn les solucions de $t^2 + t - 4$
   (d) Comproveu que y_0, y_2 sn les solucions de $t^2 - x_0 t - 1$ Comproveu que y_1, y_3 sn les solucions de $t^2 - x_1 t - 1$
   (e) Sigui $z_1 = 2cos\theta, z_2 = 2cos(4\theta)$ comproveu que z_1, z_2 sn les solucions de $t^2 - y_0 t + y_1$
   (f) Doneu una expressi radical per $cos\theta$ a partir dels apartats anteriors. Igualment doneu l'expressi radical per a $sin\theta$.

5. Dibuixeu la cissoide de Diocles, d'equaci $(X^2+Y^2)X - Y^2 = 0$, i expliqueu com es pot fer la duplicaci del cub amb regla i comps a partir d'aquesta corba.

[1] Aquest resultat s un dels resultats ms populars de Gauss, est publicat en el seu llibre "Disquisicions Aritmtiques", que est tradut al catal per Griselda Pascual, publicacions I.E.C.

Prctica de Teoria de Galois

Curs 97-98

Nombres trascendents sobre $\mathbb{Q}$

- **Objectiu**.

  L'objectiu d'aquesta prctica es demostrar que nombres que podem expressar de forma analtica sn nombres trascendents suposant cert un teorema de Lindemann o utilitzant tcniques de Lioville.

- **Trobem nombres que sn trascendents sobre $\mathbb{Q}$**

  En tota aquesta prctica suposarem que coneixem el segent resultat de l'any 1895

  Teorema 1 (Lindemann). *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$, $\mathbb{Q}$-linealment independents. Llavors les exponencials $e^{\alpha_1}, \ldots, e^{\alpha_n}$ compleixen que no hi ha cap polinomi no nul $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ complint*

  $$f(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0.$$

  Teorema 2. *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$ diferents. Llavors $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sn $\mathbb{Q}$-linealment independents.*

  Exercici 1. *Proveu que els dos teoremes anteriors sn equivalents.*

  Per una prova de l'anterior teorema podeu consultar la pagina 135 del llibre "Fields and Galois Theory" de P.Morandi, GTM 167.
  Recordem que sabeu que π i e sn nombres trascendents. El primer que va provar que e era trascendent va ser Hermite l'any 1873. π va ser demostrat que era trascendent per Lindemann l'any 1882.
  Proveu vosaltres, utilitzant l'anterior teorema que:

  Exercici 2. *Els nombres π i e sn nombres trascendents sobre $\mathbb{Q}$.*

  Anem a construir altres nombres trascendents.

  Exercici 3. *Proveu que si u s un nombre algebraic no zero, llavors $sin(u)$ i $cos(u)$ sn nombres trascendents.*

  Exercici 4. *Proveu que si u s un nombre trascendent llavors $sin(u)$ o $cos(u)$ poden ser algebraics o trascendents. Considerem u un nombre real, proveu llavors que si $sin(u)$ s trascendent llavors tamb ho s $cos(u)$ i viceversa. Si u s real, proveu que si $sin(u)$ s algebraic llavors tamb ho s $cos(u)$ i viceversa.*

  Intentem veure tamb que les funcions trigonomtriques aplicades a un nombre algebraic donen nombres trascendents. Intenteu provar:

  Exercici 5. *Si β s un nombre trascendent sobre un cos K arbitrari, llavors β^{-1} s trascendent sobre K. Igualment si α s un nombre algebraic sobre K no nul, tamb s algebraic α^{-1}.*

  Aplicant l'anterior exercici obseveu que tenim:

  Corol.lari 3. *Si u s un nombre algebraic no nul sobre $\mathbb{Q}$, llavors $sec(u)$ i $cosec(u)$ sn trascendents sobre $\mathbb{Q}$.*

  Apliquem igualment l'anterior exercici per provar:

  Exercici 6. *Si u s un nombre algebraic no nul sobre $\mathbb{Q}$, llavors $tan(u)$ i $cotan(u)$ sn nombres trascendents sobre $\mathbb{Q}$.*

  Veiem ms exemples de nombres trascendents.

  Exercici 7. *Sigui $u \neq 1$ un nombre algebraic no zero i f una de les funcions trigonomtriques inverses, proveu que el valor complex de $f(u)$ s trascendental sobre $\mathbb{Q}$.*

Finalment donem un altre exemple de nombres algebraics.

Exercici 8. *Sigui $u \neq 1$ un nombre algebraic qualsevol proveu que $log(u)$ s trascendental sobre $\mathbb{Q}$.*

- **s π algebraic sobre $\mathbb{Q}(e)$?**

  Hem demostrat suposant el teorema de Lindemann-Weierstass que els nombres π i e sn trascendents sobre $\mathbb{Q}$. s un problema obert saber si el nombre π s trascendent sobre $\mathbb{Q}(e)$ o si el nombre e s trascendent sobre $\mathbb{Q}(\pi)$. Per provar aix caldria veure que no existeix un polinomi no nul complint $f(x,y) \in \mathbb{Q}[x,y]$ amb $f(e,\pi) = 0$.

  Definici 4. *Sigui K una extensi sobre un cos F. Triem $a_1, \ldots, a_m \in K$. Diem que $a_1, \ldots, a_m$ sn algebraicament independents sobre F si tot polinomi $f \in F[x_1, \ldots, x_m]$ complint $f(a_1, \ldots, a_m) = 0$ llavors $f = 0$.*

  Reformulant el nostre problema obert amb el llenguatge de la definici, la pregunta oberta s demostrar si els nombres π, e sn algebraicament independents sobre $\mathbb{Q}$.
  En aquest camp matemtic hi ha la segent conjectura:

  Conjectura 5 (Schanuel). *Si $y_1, \ldots, y_m$ sn nombres complexos $\mathbb{Q}$-independents, llavors com a mnim m dels nombres $y_1, \ldots, y_m, e^{y_1}, \ldots, e^{y_m}$ sn algebraicament independents sobre $\mathbb{Q}$.*

  Llavors si suposem que l'anterior conjectura sigui certa llavors proveu llavors

  Exercici 9. *Suposant que fos certa la conjectura de Schanuel proveu que π s trascendent sobre $\mathbb{Q}(e)$, i que e s trascendent sobre $\mathbb{Q}(\pi)$.*

  Nota 1. *Es deixa com exercici suplementari al lector veure que π s trascendent sobre $\mathbb{Q}(e)$ s equivalent a e trascendent sobre $\mathbb{Q}(\pi)$ i equivalent a que e, π siguin algebraicament independents sobre $\mathbb{Q}$.*

- **El problema clssic de la quadratura del cercle**

  Un problema dels temps de la Grcia clssica, era:
  Es posible construir un quadrat d'rea π? s a dir sempre triant com una longitut fixada com a 1 podem construir en regla i compas el cercle de radi 1, el problema es si podem construir el quadrat d'rea π, s a dir si per regla i comps podem trobar una longitut de $\sqrt{\pi}$, el fet de poder aconseguir-ho s'anomenava la quadratura del cercle.
  Veureu a teoria que per construir un valor α mitjanant regla i compas s necessari i suficient que l'extensi $\mathbb{Q}(\alpha)|\mathbb{Q}$ sigui de grau una potncia de 2 i algebraica. Utilitzant aix proveu:

  Exercici 10. *s impossible la quadratura del cercle.*

- **Una prova on el nombre e s trascendent**

  Anem a fer aqu la prova de la trascendncia del nombre e sense utilitzar el resultat de Lindemann-Weierstrass. No obstant la prova que farem segueix en el cas particular per e les traces que se segueixen per la prova del teorema de Lindemann-Weierstrass.
  Suposeu que e no fos trascendent sobre $\mathbb{Q}$. Aix ens diu que tenim:

  $$a_m e^m + \ldots + a_1 e + a_0 = 0$$

  on podem triar els $a_i \in \mathbb{Z}$ complint que $a_0 \neq 0$.
  Definim:

  $$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \ldots (x-m)^p}{(p-1)!}$$

on p denota un nombre primer arbitrari. Observem que $deg(f) = mp + p - 1$.
Definim:

$$F(X) = f(x) + f'(x) + \ldots + f^{(mp+p-1)}(x)$$

Observeu que $f^{(mp+p)} = 0$ i que $\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x)$.
D'aqu obtenim per cada j

$$a_j \int_0^j e^{-x} f(x)dx = a_j F(0) - a_j e^{-j} F(j)$$

multiplicant per e^j i sumant sobre $j = 0, 1, \ldots, m$ obtenim

$$\sum_{j=0}^{m} (a_j e^j \int_0^j e^{-x} f(x)dx) = F(0) \sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j) = - \sum_{j=0}^{m} a_j \sum_{i=0}^{mp+p-1} f^{(i)}(j) \tag{1}$$

del fet que $\sum_{j=0}^{m} a_j e^j = 0$.
Proveu llavors que $f^{(i)}(j)$ sn enters, i s divisible per p a excepci per $j = 0$ i $i = p - 1$ i llavors $f^{(p-1)}(0) = (-1)^p \ldots (-m)^p$.
Llavors tenim que el valor de (2) s

$$Kp + a_0(-1)^p \ldots (-m)^p$$

per algun $K \in \mathbb{Z}$. Triant $p > max(m, |a_0|)$ l'enter $Kp + a_0(-1)^p \ldots (-m)^p$ no s divisible per p.
Per tant pels p suficientment grans el valor de (2) no s zero.
Estimem ara el valor de la integral. Observem que per $0 \leq x \leq m$ llavors

$$|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!}$$

on tenim llavors

$$|\sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x)dx| \leq \sum_{j=0}^{m} |a_j e^j| \int_0^j \frac{m^{mp+p-1}}{(p-1)!} dx$$

$$\leq \sum_{j=0}^{m} |a_j e^j| j \frac{m^{pm+p-1}}{(p-1)!}$$

compreveu que l'ltima expressi tendeix a 0 quan p tendeix a ∞, en contradicci amb el fet que hem vist que aquest valor s no nul pels p suficientment grans, provant aix:

Teorema 6 (Hermite). *El nombre real e s trascendent sobre $\mathbb{Q}$.*

- **Construcci de Lioville de nombres trascendents**
  Lioville, va ser el matemtic que primer va desxifr les notes d'Evariste Galois i fou el dia 4 de Juliol de 1843 que va comunicar a l'Academia de Cincies de Frana la importncia i profunditat dels resultats obtinguts per Evariste Galois.
  Igualment aquest matemtic t un paper destacat en els avenos en construcci de nombres trascendents, la idea de construcci fou que els nombres algebraics reals estan allunyats dels nombres racionals; s a dir

  Exercici 11 (Lioville,1851). *Sigui α una arrel real d'un polinomi irreductible de grau $n > 1$ amb coeficients enters. Llavors existeix una constant $c(\alpha)$ tal que*

  $$|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^n}$$

  per tot nombre racional $\frac{p}{q}$.

Indicaci: Observeu que $q^n f(\frac{p}{q}) \in \mathbb{Z}$ on $|q^n f(\frac{p}{q})| \geq 1$. Es pot pensar $|\alpha - \frac{p}{q}| \leq 1$. Utilitzar llavors el teorema del valor mig.

Exercici 12. *Proveu que el nombre* $\alpha = 0.11000100\ldots = \sum_{n=1}^{\infty} 10^{-n!}$ *s trascendent.*

Exercici 13. *Proveu que tot nombre real* α *que s'expressi mitjanant*

$$\sum_{n=1}^{\infty} \frac{k_n}{t^{n!}}$$

amb k_n *enters amb valor absolut acotat i* t *un enter arbitrari, s un nombre trascendent.*

Nota 2. *Els nombres reals* ψ *que sn aproximats per succesions racionals* p_n/q_n *on*

$$|\psi - \frac{p_n}{q_n}| < \frac{1}{q_n^{w_n}}$$

on $lim_{sup} w_n = +\infty$ *s'anomenem nombres de Lioville i sn trascendents.*

Prctica de Teoria de Galois

Curs 97-98

Nombres trascendents sobre $\mathbb{Q}$

- **Objectiu**.
  L'objectiu d'aquest recull es provar que nombres que els podem expressar de forma analtica sn nombres trascendents suposant cert un teorema de Lindemann o utilitzant tcniques de Lioville.
- **Trobem nombres que sn trascendents sobre $\mathbb{Q}$**
  En tota aquesta prctica suposarem que coneixem el segent resultat de l'any 1895

Teorema 7 (Lindemann). *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$-linealment independents. Llavors les exponencials $e^{\alpha_1}, \ldots, e^{\alpha_n}$ compleixen que no hi ha cap polinomi no nul $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ complint $f(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$.*

Teorema 8. *Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$ diferents. Llavors $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sn $\mathbb{Q}$-linealment independents.*

Proposici 9. *Els dos teoremes anteriors sn equivalents.*

Prova. Veiem primer que el teorema 1 implica el teorema 2. Siguin $\alpha_1, \ldots, \alpha_n$ nombres algebraics sobre $\mathbb{Q}$. Denotem per V el $\mathbb{Q}$-espai vectorial que generen, elegim-ne una base de V. Denotem-la per $\beta_1, \ldots, \beta_r$, $(r \leq n)$. Suposem que $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sn $\mathbb{Q}$-dependents. s a dir tenim

$$\sum_{i=1}^{n} r_i e^{\alpha_i} = 0$$

,$r_i \in \mathbb{Q}$ escrivim $\alpha_i = \sum_{j=1}^{r} r_{j,i}\beta_j$ tenim llavors que $e^{\alpha_i} = \prod_j (e^{\beta_j})^{r_{j,i}}$ per tant la relaci que $\mathbb{Q}$-dependncia ens dona una igualtat canviant $e^{\beta_i} := X_i$

$$\sum_{i=1}^{n} r_i (\prod_{j=1}^{r} X_j^{r_{j,i}}) = 0$$

escrivint el polinomi $f(X_1, \ldots, X_r) = \sum_{i=1}^{n} r_i (\prod_{j=1}^{r} X_j^{r_{j,i}}$ que s no nul tenim com $\beta_1, \ldots, \beta_r$ son $\mathbb{Q}$-linealment independent trobem un polinomi no nul f on $f(e^{\beta_1}, \ldots, e^{\beta_r}) = 0$ en contradicci amb el teorema 1.
Provem que el t2 implica el t1. Siguin ara $\alpha_1, \ldots, \alpha_n$ $\mathbb{Q}$-linealment independents. Suposem que existis un polinomi no nul $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ on $f(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$. Escrivim

$$f(x_1, \ldots, x_n) = \sum a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n}$$

considerem llavors els nombres algebraics $\beta_{a_{i_1, \ldots, i_n}} = \sum_k i_k \alpha_k$ que sn diferents entre ells per ser α_j $\mathbb{Q}$-linealment independents. Llavors tenim que f defineix una relaci $\mathbb{Q}$-lineal entre les $e^{\beta_{a_{i_1, \ldots, i_n}}}$ provant aix finalment l'enunciat. $\square$

Per una prova del teorema de Lindemann podeu consultar la pgina 135 del llibre "Fields and Galois Theory" de P.Morandi, GTM 167.
Recordem que sabeu que π i e sn nombres trascendents. El primer que va provar que e era trascendent va ser Hermite l'any 1873. π va ser demostrat que era trascendent per Lindemann l'any 1882.
Utilitzant l'anterior teorema tenim:

Corol.lari 10. *Els nombres π i e sn nombres trascendents sobre $\mathbb{Q}$.*

Prova. Una prova utilitzant el teorema 2 seria: suposem que π fos algebraic sobre $\mathbb{Q}$. Llavors tamb ho s $i\pi$. Considerem llavors els dos nombres algebraics sobre $\mathbb{Q}$: 0,π; aplicant el teorema de Lindemann obtenim llavors que $1 = e^0$ i $e^{\pi i} = -1$ sn $\mathbb{Q}$ linealment independents, cosa que s imposible per tant aix prova que π s un nombre trascendent.
Suposem ara que e fos algebraic sobre $\mathbb{Q}$. Aix per definici ens diu que existeixen $r_i \in \mathbb{Q}$ on

$$\sum_{i=0}^{m} r_i e^i = 0$$

Aix diu que els nombres $e^0, e^1, \ldots, e^m$ son $\mathbb{Q}$-dependents. Com $0, 1, \ldots, m$ sn nombres algebraics diferents, utilitzant el teorema de Lindemann obtenim que e ha de ser trascendent. □

Anem a construir altres nombres trascendents.

Corol.lari 11. *Proveu que si u s un nombre algebraic no zero, llavors $sin(u)$ i $cos(u)$ sn nombres trascendents.*

Prova. Recordeu que $sin(x) = \frac{e^{ix}-e^{-ix}}{2}$. Observem que si u s algebraic tenim llavors com que i s algebraic que el nombre iu s algebraic, observem llavors que el teorema de Lindemann diu que no existeix polinomi no nul f, complint $f(e^{ix}, e^{-ix}) = 0$. Suposem que $sin(u)$ fos algebraic; aix vol dir que existeix $g(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{Q}[x]$ on $g(sin(u)) = 0$, observem llavors que aix ens diu $g(\frac{e^{iu}-e^{iu}}{2}) = \sum_{i=0}^{r} a_r (\frac{e^{iu}-e^{-iu}}{2})^i = \sum_{j=v}^{s} b_j e^{iju} = 0$ amb $v, s \in \mathbb{Z}$ convenients($v < 0$,$s > 0$) i $b_j \in \mathbb{Q}$, per l'anterior expressi ens dona un polinomi $f(x, y) = \sum_{j=v}^{0} b_j y^{-j} + \sum_{j=0}^{s} x^j$ on $f(e^{iu}, e^{-iu}) = 0$ en contradicci, provant aix que $sin(u)$ s un nombre trascendent.
La prova en el cas del $cos(x)$ es semblant considerant que $cos(x) = \frac{e^{ix}+e^{-ix}}{2}$. □

Observem que si u s trascendent no poder dir res de $sin(u)$ o $cos(u)$ referent a la seva trascendialitat o no:

Lema 12. *Si u s un nombre trascendent llavors $sin(u)$ o $cos(u)$ poden ser algebraics o trascendents. Considerem u un nombre real, si $sin(u)$ s trascendent llavors tamb ho s $cos(u)$ i viceversa; igualment si $sin(u)$ s algebraic llavors tamb ho s $cos(u)$ i viceversa.*

Prova. s clar que com π s trascendent obtenim llavors que $cos(\pi)$ i $sin(\pi)$ sn nombres algebraics sobre $\mathbb{Q}$. Anem a veure que no forosament el sinus o cosinus d'un nombre trascendent sobre $\mathbb{Q}$ s algebraic. Considerem l'equaci $f(x) = cos(x) - x = 0$ per Bolzano sabem que t una soluci en $[0, \pi/2]$ aquest nombre α compleix $\alpha = cos(\alpha)$ observem que α no pot ser algebraic ja que llavors seria tamb trascendent pel corol.lari anterior, per tant obtenim que α s trascendent. Com tenim la relaci $cos^2 x + sin^2 x = 1$ tenim que si $sin(u)$ s algebraic tamb ho s $sin^2 u$ i per tant $cos^2 u$ i com una extensi que contingui $cosu$ referent a la de $cos^2 u$ s de grau 2 tenim que $cos(u)$ s algebraic. Un raonament similar per que cal escriure funcionaria pel cas trascendent(Exercici al lector). □

Veiem tamb que altres funcions trigonomtriques aplicades a un nombre algebraic donen nombres trascendents.

Lema 13. *Si β s un nombre trascendent sobre un cos K arbitrari, llavors β^{-1} s trascendent sobre K. Igualment si α s un nombre algebraic sobre K no nul, tamb s algebraic α^{-1}.*

Prova. Suposem que β^{-1} fos algebraic. Llavors tindriem que existeix un polinomi a $K[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$ complint $f(\beta{-}1) = 0$; s a dir

$$\sum_{i=0}^{n} a_i (\frac{1}{\beta})^i = 0$$

multiplicant l'anterior expressi per β^n obtenim llavors

$$\sum_{i=0}^{n} a_i \beta^{n-i} = 0$$

per tant tenim un polinomi $g(x) = \sum_{i=0}^{n} a_i x^{n-i}$ on $g(\beta) = 0$ dient-nos que β s algebraic en contra la hiptesi, provant aix l'enunciat. Si α s no nul la prova anterior mostra l'enunciat en el cas algebraic. $\square$

Aplicant l'anterior lema tenim:

Corol.lari 14. *Si u s un nombre algebraic no nul sobre $\mathbb{Q}$, llavors $sec(u)$ i $cosec(u)$ sn trascendents sobre $\mathbb{Q}$.*

Apliquem igualment l'anterior lema per provar:

Corol.lari 15. *Si u s un nombre algebraic no nul sobre $\mathbb{Q}$, llavors $tan(u)$ i $cotan(u)$ sn nombres trascendents sobre $\mathbb{Q}$.*

Prova. Com $cotang(u) = (tan(u))^{-1}$ utilitzant el lema si veiem el resultat per $tan(u)$ obtenim el resultat per $cotag(u)$. Anem doncs a demostrar que $tan(u)$ s un nombre trascendent quan u s un nombre algebraic no nul.
Recordem que $tan(u) = \frac{e^{iu} - e^{-iu}}{e^{iu} + e^{-iu}} = 1 - \frac{2}{1 + e^{-2iu}}$. Suposem que $tan(u)$ fos algebraic llavors $tan(u) - 1$ seria algebraic on tindriem que $-\frac{2}{1+e^{-2iu}}$ seria algebraic. Observeu per llavors que $1 + e^{-2iu}$ seria algebraic en particular tindriem que e^{-2iu} seria algebraic. Per aix entra en contradicci amb el teorema de Lindemann. Ja que $-2iu$ s un nombre algebraic no nul i el teorema de Lindemann en paticular ens diu llavors que e^{-2iu} s un nombre trascendent. $\square$

Veiem ms exemples de nombres trascendents.

Corol.lari 16. *Sigui $u \neq 1$ un nombre algebraic no zero i f una de les funcions trigonomtriques inverses, proveu que el valor complex de $f(u)$ s trascendental sobre $\mathbb{Q}$.*

Prova. Fem-ho per $arcsin(u)$. Per les altres es fan semblantment(exercici). Suposem que $arcsin(u)$ fos algebraic. Com $u \neq 0$ tenim que $arcsin(u) \neq 0$, apliquem-hi el sinus tenim llavors que utilitzant que el sinus d'un nombre algebraic no nul s trascendental tenim llavors:

$$u = sin(arcsin(u))$$

on u seria trascendental en contra de la hiptesi, provant-nos que $arcsin(u)$ s trascendentat. $\square$

Finalment donem un altre exemple de nombres algebraics.

Corol.lari 17. *Sigui $u \neq 1$ un nombre algebraic qualsevol llavors $log(u)$ s trascendental sobre $\mathbb{Q}$.*

Prova. Suposem que $log(u)$ fos un nombre algebraic, com $u \neq 1$ un nombre algebraic diferent s el 0. Aplicant el teorema de Lindemann obtenim que $e^{log(u)} = u$ no compleix cap equaci polinomial per u era algebraic, provant aix que $log(u)$ s trascendent sobre $\mathbb{Q}$, si $u \neq 1$ s un nombre algebraic. $\square$

- **s π algebraic sobre $\mathbb{Q}(e)$?**
  Hem demostrat suposant el teorema de Lindemann que els nombres π i e sn trascendents sobre $\mathbb{Q}$. s un problema obert saber si el nombre π s trascendent sobre $\mathbb{Q}(e)$ o si el nombre e s trascendent sobre $\mathbb{Q}(\pi)$. Per provar aix caldria veure que no existeix un polinomi no nul complint $f(x,y) \in \mathbb{Q}[x,y]$ amb $f(e,\pi)=0$.

  Definici 18. *Sigui K una extensi sobre un cos F. Triem $a_1,\dots,a_m \in K$. Diem que $a_1,\dots,a_m$ sn algebraicament independents sobre F si tot polinomi $f \in F[x_1,\dots,x_m]$ complint $f(a_1,\dots,a_m)=0$ llavors $f=0$.*

  Reformulant el nostre problema obert amb el llenguatge de la definici, la pregunta oberta s demostrar si els nombres π, e sn algebraicament independents sobre $\mathbb{Q}$.
  En aquest camp matemtic hi ha la segent conjectura:

  Conjectura 19 (Schanuel). *Si $y_1,\dots,y_m$ sn nombres complexos $\mathbb{Q}$-independents, llavors com a mnim m dels nombres $y_1,\dots,y_m,e^{y_1},\dots,e^{y_m}$ sn algebraicament independents sobre $\mathbb{Q}$.*

  Llavors si suposem que l'anterior conjectura sigui certa llavors obtenim

  Corol.lari 20. *Suposant que fos certa la conjectura de Schanuel llavors tenim que π s trascendent sobre $\mathbb{Q}(e)$, i que e s trascendent sobre $\mathbb{Q}(\pi)$.*

  Prova. Es deixa com exercici al lector veure que π s trascendent sobre $\mathbb{Q}(e)$ s equivalent a e trascendent sobre $\mathbb{Q}(\pi)$ i equivalent a que e,π siguin algebraicament independents sobre $\mathbb{Q}$.
  Considerem els dos nombres algebraics $1, i\pi$ que sn $\mathbb{Q}$-independents. Llavors considerem $i\pi, 1, e^{i\pi}=-1, e$ utilitzant llavors la conjectura tenim que per fora els nics dos valors que poden ser algebraicament independents sn $i\pi, e$ per tant obtenim que no existeix f no nul en $\mathbb{Q}[x,y]$ on $f(i\pi,e)=0$. Es clar llavors el mateix resultat per π, e provant el resultat, ja que si π fos algebraic sobre $\mathbb{Q}(e)$ com i s algebraic tamb seria $i\pi$ algebraic sobre $\mathbb{Q}(e)$ cosa que acavem de provar que no succeeix. $\square$

- **El problema clssic de la quadratura del cercle**
  Un problema dels temps de la Grcia clssica, era:
  Es posible construir un quadrat d'rea π? s a dir sempre triant com una longitut fixada com a 1 podem construir en regla i compas el cercle de radi 1, el problema es si podem construir el quadrat d'rea π, s a dir si per regla i comps podem trobar una longitut de $\sqrt{\pi}$, el fet de poder aconseguir-ho s'anomenava la quadratura del cercle.
  Veureu a teoria que per construir un valor α mitjanant regla i compas s necessari i suficient que l'extensi $\mathbb{Q}(\alpha)|\mathbb{Q}$ sigui de grau una potncia de 2 i algebraica. Utilitzant aix tenim:

  Teorema 21. *s impossible la quadratura del cercle.*

  Prova. Observem com π s trascendent, tenim que $\sqrt{\pi}$ s trascendent. Per tant l'extensi $\mathbb{Q}(\sqrt{\pi})|\mathbb{Q}$ no s algebraica, provant que no s construible. $\square$

- **Una prova on el nombre e s trascendent**
  Anem a fer aqu la prova de la trascendncia del nombre e sense utilitzar el resultat de Lindemann. No obstant la prova que farem segueix en el cas particular per e les traces que se segueixen per la prova del teorema de Lindemann.
  Suposeu que e no fos trascendent sobre $\mathbb{Q}$. Aix ens diu que tenim:

$$a_m e^m + \dots + a_1 e + a_0 = 0$$

on podem triar els $a_i \in \mathbb{Z}$ complint que $a_0 \neq 0$.
Definim:

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \dots (x-m)^p}{(p-1)!}$$

on p denota un nombre primer arbitrari. Observem que $deg(f) = mp + p - 1$.
Definim:

$$F(X) = f(x) + f'(x) + \dots + f^{(mp+p-1)}(x)$$

Observeu que $f^{(mp+p)} = 0$ i que $\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}f(x)$.
D'aqu obtenim per cada j

$$a_j \int_0^j e^{-x} f(x) dx = a_j F(0) - a_j e^{-j} F(j)$$

multiplicant per e^j i sumant sobre $j = 0, 1, \dots, m$ obtenim

$$\sum_{j=0}^{m}(a_j e^j \int_0^j e^{-x} f(x) dx) = F(0) \sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j) = - \sum_{j=0}^{m} a_j \sum_{i=0}^{mp+p-1} f^{(i)}(j) \tag{2}$$

del fet que $\sum_{j=0}^{m} a_j e^j = 0$.
Proveu llavors que $f^{(i)}(j)$ sn enters, i s divisible per p a excepci per $j = 0$ i $i = p - 1$ i llavors $f^{(p-1)}(0) = (-1)^p \dots (-m)^p$.
Llavors tenim que el valor de (2) s

$$Kp + a_0(-1)^p \dots (-m)^p$$

per algun $K \in \mathbb{Z}$. Triant $p > max(m, |a_0|)$ l'enter $Kp + a_0(-1)^p \dots (-m)^p$ no s divisible per p.
Per tant pels p suficientment grans el valor de (2) no s zero.
Estimem ara el valor de la integral. Observem que per $0 \leq x \leq m$ llavors

$$|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!}$$

on tenim llavors

$$|\sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x) dx| \leq \sum_{j=0}^{m} |a_j e^j| \int_0^j \frac{m^{mp+p-1}}{(p-1)!} dx$$

$$\leq \sum_{j=0}^{m} |a_j e^j| j \frac{m^{pm+p-1}}{(p-1)!}$$

compreveu que l'ltima expressi tendeix a 0 quan p tendeix a ∞, en contradicci amb el fet que hem vist que aquest valor s no nul pels p suficientment grans, provant aix:

Teorema 22 (Hermite). *El nombre real e s trascendent sobre $\mathbb{Q}$.*

- **Construcci de Lioville de nombres trascendents**
  Lioville, va ser el matemtic que primer va desxifr les notes d'Evariste Galois i fou el dia 4 de Juliol de 1843 que va comunicar a l'Academia de Cincies de Frana la importncia i profunditat dels resultats obtinguts per Evariste Galois.
  Igualment aquest matemtic t un paper destacat en els avenos en construcci de nombres trascendents, la idea de construcci fou que els nombres algebraics reals estan allunyats dels nombres racionals; s a dir

Proposici 23 (Lioville,1851). *Sigui α una arrel real d'un polinomi irreductible de grau $n > 1$ amb coeficients enters. Llavors existeix una constant $c(\alpha)$ tal que*

$$|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^n}$$

per tot nombre racional $\frac{p}{q}$.

Prova. Escrivim $f(x) \in \mathbb{Z}[x]$ el polinomi irreduible de grau n on $f(\alpha) = 0$. Observem que com $q^n f(p/q) \in \mathbb{Z}$, $|q^n f(p/q)| \geq 1$. Podem pensar $|\alpha - \frac{p}{q}| \leq 1$. Utilitzant el teorema del valor mig obtenim

$$|f(p/q)| = |f(\alpha) - f(p/q)| \leq |\alpha - \frac{p}{q}| sup_{|x-\alpha|\leq 1} |f'(x)|$$

obtenint aix el resultat. □

Com aplicaci veiem que **el nombre** $\alpha = 0.11000100\ldots = \sum_{n=1}^{\infty} 10^{-n!}$ **s trascendent.**

Anem a aplicar el resultat de Lioville per a provar que l'anterior nombre s trascendent. Per aix considerem $\alpha_r = \sum_{n=1}^{r} 10^{-n!} = p/q$ on $p = 10^{r!} \sum_{n=1}^{r} 10^{-n!}$, $q = 10^{r!}$ tenim llavors

$$|\alpha - \alpha_r| = |\alpha - \frac{p}{q}| = \sum_{n=r+1}^{\infty} 10^{-n!} < 10^{(r+1)!} \sum_{n=0}^{\infty} 10^{-n} < 10^{-(r+1)!} 2 = \frac{2 \cdot 10^{-r!}}{q^r}$$

Si $r \geq n$ i suficientment gran tenim $2 \cdot 10^{-r!} < c(\alpha)$ i

$$|\alpha - \frac{p}{q}| < \frac{c(\alpha)}{q^n} \tag{3}$$

, on llavors obtenim que hi ha una infinitat de nombres racionals satisfen l'inequaci 3 on amb el resultat de Lioville, aquest fet ens diu que α s trascendent.

Corol.lari 24. *Tot nombre real α que s'expressi mitjanant*

$$\sum_{n=1}^{\infty} \frac{k_n}{t^{n!}}$$

amb k_n enters amb valor absolut acotat i t un enter arbitrari, s un nombre trascendent.

Prova. La prova es unicament acotant les k_n per una constant i utilitzar el mateix argument que s'ha fet pel nombre $\alpha = 0.11000100\ldots$ sustituint $10 = t$ i els canvis convenients. □

Nota 3. *Els nombres reals ψ que sn aproximats per succesions racionals p_n/q_n on*

$$|\psi - \frac{p_n}{q_n}| < \frac{1}{q_n^{w_n}}$$

on $lim_{sup} w_n = +\infty$ s'anomenem nombres de Lioville i sn trascendents.

Prctica de Teoria de Galois.
curs 97-98
Extensions algebraiques.
Separabilitat e inseparabilitat.

- Objectiu
  Estudi dels elements que apareixen en extensions algebraiques. Un estudi sobre una descomposici d'extensions algebraiques $K|k$ en extensions on tots els seus elements sn purament inseparables o separables.

- Cossos perfectes

  Definici 25. *Diem que un cos k s perfecte si tota extenxi algebraica de k s separable.*

  Exercici 14. *Proveu que tota extensi algebraica sobre un cos k amb $car(k) = 0$ es t que s separable; s a dir si $car(k) = 0$ tenim llavors que k s un cos perfecte. En particular tenim que tota extensi algebraica de $\mathbb{Q}$ s separable. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sn cossos perfectes.*

  Exercici 15. *Proveu que si k s un cos algebraicament tancat, llavors s perfecte.*

  Falta doncs estudiar en profunditat les extensions algebraiques en un cos k amb $car(k) = p \neq 0$.

  Exercici 16. *Sigui k un cos amb $car(k) = p \neq 0$. Proveu: k s perfecte si i nomes si $k^p = k$.*

  Indicaci: Per $\Leftarrow$, si $F|k$ s una extensi algebraica $\alpha \in F$ i $g(x^{p^n})$ s el polinomi mnim de l'element α sobre k cal provar que $n = 0$, utilitzant aqu $k^p = k$.

  Exercici 17. *Proveu que si k s un cos de $car(k) = p \neq 0$ i t un nombre finit d'elements, llavors k s un cos perfecte.*

  Indicaci: Considereu el morfisme de cossos $\varphi : k \to k$ donat per $\varphi(a) = a^p$ i utilitzeu l'exercici anterior.

  Falta doncs estudiar els cossos de caracterstica p no finits.

  Exercici 18. *Doneu un exemple d'un cos no perfecte.*

  Evidentment l'anterior exemple ha de ser d'un cos de $car(k) = p \neq 0$ i no finit. No obstant tot cos complint aquestes condicions no s necessriament perfecte:

  Exercici 19. *Doneu un exemple d'un cos k de $car(k) = p \neq 0$ i que el seu nombre d'elements no sigui finit i que compleixi que k sigui un cos perfecte.*

- Extensions separables versus inseparables

  Considereu el cos $F = \mathbb{F}_2(x)$ i considerem l'extensi de cossos $K|F$ amb $K = \mathbb{F}_2(x^{\frac{1}{10}})$. Observeu que $K = \mathbb{F}_2(x^{1/5}, x^{1/2})$ proveu:

Exercici 20. *L'extensi* $\mathbb{F}_2(x^{1/5})|F$ *s separable i l'extensi* $\mathbb{F}_2(x^{1/2})|F$ *s purament inseparable.*

Observeu llavors que l'extensi algebraica $K|F$ cont elements separables i elements purament inseparables.

Definici 26. *Sigui* $K|k$ *una extensi. Anomenem clausura separable de* k *en* K *al conjunt* $S = \{a \in K | a \text{ separable sobre } k\}$.
Anomenem la clausura purament inseparable de k *en* K *al conjunt*

$$I = \{a \in K | a \text{ purament inseparable sobre } k\}.$$

Exercici 21. *Proveu que la clausura separable i la clausura inseparable sn cossos. Proveu* $S|k$ *s una extensi separable i* $I|F$ *s una extensi purament inseparable.*

Anem a fer un estudi donada una extensi $K|k$ algebraica, com sn referent a la inseparabilitat o no de l'extensi $K|S$; i la pregunta de si l'extensi $K|I$ s separable o no.

Qüesti 1. *Donada una extensi* $K|k$ *algebraica, existeix* K' *extensi de* k *continguda en* K *on* $K|K'$ *separable i* $K'|k$ *purament inseparable?*

Qüesti 2. *Donada una extensi* $K|k$ *algebraica, existeix* K'' *extensi de* k *continguda en* K *on* $K|K''$ *purament inseparable i* $K''|k$ *separable?*

Anem a resoldre la segona qesti plantejada.

Exercici 22. *Proveu que si* $K|k$ *s una extensi algebraica llavors* $K|S$ *s purament inseparable.*

Observeu que l'anterior exercici ens diu justament que la qesti 2 t resposta afirmativa per tota extensi algebraica. Observeu que s el millor resultat que un pot esperar.
Com aplicaci de l'anterior soluci positiva a la qesti 2

Exercici 23. *Sigui* $K|k$ *extensi algebraica finita i* $car(k) \nmid [K:k]$. *Proveu llavors que* $K|k$ *s separable.*

Definici 27. *Sigui* $K|k$ *una extensi finita. Anomenem el grau de inseparabilitat per la extensi* $K|k$ *com el grau* $[K:S]$ *i l'anotarem per* $[K:k]_i$. *Anomenem el grau de separabilitat per la extensi* $K|k$ *com el grau* $[S:k]$ *i l'anotarem* $[K:k]_s$.

Observeu que si $K|k$ una extensi finita tenim $[K:k] = [K:k]_s[K:k]_i$.

Exercici 24. *Sigui* $k \subset K \subset L$ *extensions de cossos finites. Proveu:*

$$[L:k]_s = [L:K]_s[K:k]_s$$

$$[L:k]_i = [L:K]_i[K:k]_i$$

Referent a la qesti 1, cal anotar que no es vlida en general per extensions algebraiques $K|k$ arbitrries havent-n'hi exemples explcits. No obstant si l'extensi $K|k$ s normal llavors s'obt un resultat afirmatiu a la qesti:

Teorema 28. *Sigui K una extensi normal de k, i siguin S i I les clausures separables i purament inseparable de k en K, respectivament. Llavors $S|k$ s Galois, $I = K^{Gal(K|k)}$ i $Gal(S/k) \cong Gal(K/I)$. Per tant K/I s Galois. A ms $K = SI$.*

Observem que el fet que K/I sigui Galois ens diu que en particular tenim que K/I s separable, donant una resposta afirmativa a la qesti 1.

1. Construu un exemple d'un cos k i un polinomi irreduible sobre k que tingui arrels mltiples i almenys dues arrels diferents.

2. Considerem K la clausura algebraica de $\mathbb{F}_p$, i $\varphi \in \Gamma(K/\mathbb{F}_p)$ l'aplicaci $\varphi(a) = a^p$.

   (a) Proveu que realment $\varphi \in \Gamma(K/\mathbb{F}_p)$ i t ordre infinit. Calculeu qui s $K^{<\varphi^n>}$.

   (b) Sigui $\phi \in \Gamma(K/\mathbb{F}_p)$. Proveu $\phi_{|\mathbb{F}_{p^n}} = \varphi^n$.

   (c) Proveu que existeix $\phi \in \Gamma(K/\mathbb{F}_p)$ on $\phi \notin < \varphi >$.

3. Considerem el polinomi $x^5 + x^4 + 1$. Calculeu la o les extensions radicals que fan resoluble per radicals aquest polinomi, en cas afirmatiu. Igualment si es posible expresseu de forma radical nica les solucions de l'anterior polinomi.

4. Proveu que l'extensi $\mathbb{Q}(cos(\frac{2\pi}{n})$ s Galois sobre $\mathbb{Q}$ per tot $n \in N$.
   s veritat l'anterior pregunta per $\mathbb{Q}(sin(\frac{2\pi}{n}))$ sobre $\mathbb{Q}$?

5. Sigui L/F una extensi de cossos. Fem les segents notacions: Donada una extensi de cossos L/K anotem S el conjunt de tots els elements de L que sn separables sobre K. Igualment anotem per I el conjunt d'elements purament inseparables sobre K, pensant que tot element de K s purament inseparable i separable.

   (a) Proveu que I i S son cossos sobre K.

   (b) Proveu que si L/F s algebraica llavors K/S s purament inseparable.

   (c) Si L/F s algebraica i finita amb $car(F) \nmid [L : F]$ llavors $L = S$, s a dir s una extensi separable.

6. s veritat que totes les extensions de grau 2 d'un cos finit de caracterstica $p > 0$ de grau 2 sn isomorfs com cossos? Responeu la mateixa pregunta sobre extensions de grau 2 sobre un cos de caracteristica p. La mateixa pregunta per caracterstica 0.Cal justificar la resposta.

7. Veure que las hiptesis del teorema principal de la teoria de Galois no es poden debilitar en el cas K/L d'una extensi finita.

8. .