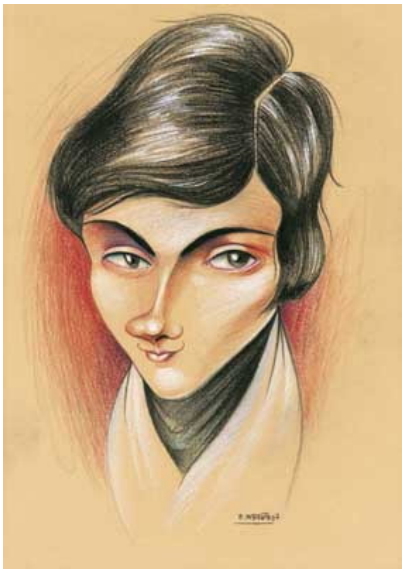
Universitat Autònoma de Barcelona

Correspondència bijectiva de Galois en extensions no finites



Autora: Jone Uria Albizuri
Tutor: Francesc Bars Cortina

Barcelona, 25 de Juny de 2012

Índex

Capítol 1

Introducció

La teoria de Galois, que porta nom d'un matemàtic francés, "Évariste Galois" (1811-1832), és la teoria que estudia propietats i característiques dels cossos, anomenada també teoria de cossos. L'aportació de Galois a la teoria de cossos va ser tan cabdal que va fer una revolució en aquest camp.

Sembla que la gran motivació de Galois era donar un criteri per a saber quan es poden expressar les arrels d'un polinomi en funció dels seus coeficients usant radicals. Abel (1802-1829) i Ruffini (1765-1822) ja van demostrar que per polinomis genèrics de grau més gran o igual que 5 no hi ha cap fórmula general per a expressar les arrels del polinomi en funció dels coeficients usant radicals. L'aportació de Galois és un mètode per donat un polinomi concret de grau n, saber quan es pot expressar per radicals les seves arrels a partir dels seus coeficients. Galois obté aquest resultat a partir d'una idea revolucionària, relacionant teoria de cossos i teoria de grups. Anem a explicitar-la una mica.

La idea principal de Galois va ser: enlloc d'estudiar els objectes (en el seu cas cossos) estudiem morfismes dels objectes (morfismes de cossos) i intentem caracteritzar els objectes a partir de les propietats dels morfismes. Aquesta idea innovadora de Galois es troba en l'actualitat en diverses rames de matemàtiques actuals, per exemple A. Grothendieck va fer una revolució similar amb el món de la Geometria, en particular de la Geometria Algebraica.

Amb aquesta idea, Galois va obtenir el que s'anomena actualment correspondència bijectiva de Galois en què caracteritzava els cossos intermedis entre dos cossos L i K via subgrups del grup de morfismes de cossos de L amb L deixant fix el cos K, sota certes condicions pels cossos L i K i sempre pensant que L com K-espai vectorial té dimensió finita. Ja hem comentat

que Galois amb aquest resultat va poder donar un criteri per donat un polinomi fixat $p(x)$ de grau n sobre un cos K decidir si podem expressar les seves arrels de forma exacta usant expressions radicals. La resposta es troba a travs que un grup de morfismes deixant el cos fix compleixi una propietat. Aquest grup de morfismes, realment són automorfismes i tenen estructura de grup amb composició, Galois és el primer en un estudi de teoria de grups i també l'estudi de cossos amb un nombre finit d'elements.

Al grau o llicenciatura de Matemàtiques estudiem gran part dels resultats anteriors. Aquest treball pretén obtenir certs resultats vers la filosofia iniciada per Galois quan L és un K-espai vectorial de dimensió no finita, en particular vol estudiar la correspondència bijectiva de Galois entre cossos i morfismes en aquesta situació.

Anem a descriure breument les diferents parts del treball que presentem a continuació. En el capítol 2 recordarem algunes definicions i resultats ja coneguts i molts d'ells donats en un curs bàsic de teoria de Galois en la titulació, per exemple en la §2.2 s'enuncia la correspondència bijectiva de Galois per a d'extensions L/K finites, és dir que L com a K-espai vectorial té dimensió finita. Un cop presentada la bijecció, hi les dues preguntes naturals següents (usualment no treballades en un curs bàsic de teoria de Galois):
* tot grup finit G és el grup d'automorfismes per a alguna extensió de cossos L/K? La resposta és que sí, i presentem la demostració en §2.3;
* fixat un grup finit G i un cos K, existeix un cos L que conté K que sigui Galois (recordeu la definició en el capítol 2) tal que el grup automorfismes de L deixant fix K és G? Resulta que aquesta pregunta és molt complicada i no es coneix la resposta general. Auesta pregunta se l'anomena el Problema Invers de la teoria de Galois, i per exemple per $K = \mathbb{Q}$ es conjectura que la resposta serà afirmativa per tot grup G. En §2.4 presentem aquest problema i donem alguns resultats e idees generals en atacar la pregunta, i també explicitem el grup simple més petit que no es coneix la resposta al problema invers de Galois quan el cos fixat és $\mathbb{Q}$.

En el capítol 3 ja entrem a estudiar la idea de Galois per a extensions L de K amb dimensió de L com K-espai vectorial no finita. En la §3.1 presentem un exemple que justifica que la correspondència com està plantejada en el cas finit no és correcta. En la construcció de l'exemple s'observa que el grup d'automorfismes, que s'involucra per extensions no finites, correspon a limits projectius d'objectes amb estructura de grups. El lector pot consultar l'apèndix per aprofundir amb aquest objectes. En la §3.2 donem les eines per poder obtenir una correspondència bijectiva entre cossos i automorfismes

de cossos, per obtenir-ho cal introduir topologia en els automorfismes i la bijecció que demostrarem en §3.3 és entre subcossos i subgrups tancats en el grup automorfisme de la extensió amb una topologia natural de ser aquest grup un límit projectiu, anomenats grups profinits. Finalment el treball per analogia a les dues preguntes naturals en la teoria de Galois per a extensions finites les traslladem en la situació no finita via:

* Donat un grup profinit qualsevol, existeix una extensió de cossos L/K Galois que li correspon aquest grup? La resposta és sí, és el conegut teorema de Waterhouse i en presentem una demostració en §3.5;

* Siguin fixats G un grup profinit i K un cos. Existeix una extensió L/K Galois amb grup de Galois G? En la §3.6 responem que no podem esperar que la resposta sigui sí, ni tan sols amb $K = \mathbb{Q}$ i G grup abelià profinit i lliure de torsió.

Finalment hem inclòs un apèndix sobre límits projectius per facilitar la lectura de resultats en els grups d'automorfismes involucrant extensions no finites, grups que tenen de forma natural una topologia i són grups topològics.

Capítol 2

Preliminaris d'extensions de Galois

2.1 Definicions i lemes previs

En aquesta secció recordarem les definicions bàsiques de teoria de Galois i un parell d'observacions que farem servir més endavant.

Definició 2.1.1. *Una extensió de cossos F/K és de Galois si és una extensió normal i separable.*

Definició 2.1.2. *Sigui F/K una extensió de cossos. Un element $\alpha \in F$ es diu algebraic sobre K si existeix un polinomi diferent de zero amb coeficients en K tal que s'anul·la en α.*
Diem que l'extensió és algebraica si tot element de F és algebraic sobre K.
(Es pot demostrar fàcilment que donat α algebraic sobre K, aleshores existeix un únic polinomi irreductible i mònic amb coeficients en K tal que s'anul·la en α, a aquest polinomi li diem polinomi irreductible de α sobre K i ho denotem per: $Irr(\alpha, K)[x]$).

Definició 2.1.3. *Una extensió de cossos F/K es diu normal si compleix les dues condicions següents:*
(i) F/K és una extensió algebraica,
(ii) qualsevol polinomi $q(x) \in K[x]$ irreductible en $K[x]$, si $q(x)$ té una arrel en F, llavors totes les arrels de $q(x)$ també estan en F. És a dir, tots els

polinomis irreductibles de $K[x]$ descomponen totalment en F o no tenen cap arrel en F.

Definició 2.1.4. *Si K és un cos i $\{f_i(x) \in K[x]\}_{i\in I}$ una familia de polinomis amb coeficients en K, es diu que F el cos de descompocició dels polinomis $\{f_i\}_{i\in I}$ sobre K, si és el cos més petit de manera que cada f_i descompon totalment en F (és a dir, totes les arrels de f_i són a F).*

Proposició 2.1.5. *F/K és normal si i només si, F és el cos de descomposició d'una familia de polinomis amb coeficients en K.*

Definició 2.1.6. *Diem que un polinomi irreductible $l(x) \in K[x]$ és separable si totes les seves arrels en una clausura algebraica de K són simples, és a dir, si no té cap arrel repetida. És equivalent a dir que el màxim comú divisor de $l(x)$ i $l'(x)$ és 1, on $l'(x)$ és la derivada formal de $l(x)$.*
Es diu que una extensió de cossos F/K és separable, si F/K és algebraica i per cada $\alpha \in F$ el polinomi $Irr(\alpha, K)[x]$ és separable.

Corol·lari 2.1.7. *Si F/K és de Galois i $K \subseteq E \subseteq F$, llavors F/E és de Galois.*

Demostració. Per la proposició 2.1.5 sabem que M/N normal si i només si M és el cos de descomposició d'una familia de polinomis amb coeficients en N.
Com F/K normal, és equivalent dir que F és el cos de descomposició d'una familia $(f_i)_{i\in I}$ de polinomis de $K[x]$, és a dir, $F = K((\alpha_{i,j_i})_{i,j_i})$ on α_{i,j_i} són arrels de f_i en una clausura algebraica de K fixada. Per tant, com que els $(f_i)_{i\in I} \in K[x] \subseteq E[x]$, F també és cos de descomposició de la mateixa familia de polinomis en $E[x]$ i per tant, F/E és normal.
El fet de ser F/E separable es dedueix de que F/K ho és, ja que $Irr(\alpha, E)[x]$ divideix $Irr(\alpha, K)[x]$ per tot $\alpha \in F$. □

Notació 2.1.8. *Si F un cos, $AutF$ és el grup d'automorfismes del cos F. Donat F/K una extensió de cossos, sempre podem considerar $Aut_K F = \{\sigma : F \longrightarrow F\ \sigma$ isomorfisme de cossos $\mid \sigma(k) = k, \forall k \in K\}$, els automorfismes del cos F que fixen el cos K. Si F/K és de Galois escriurem $Gal(F/K)$ en lloc de $Aut_K F$ i l'anomenarem el grup de Galois de F/K.*

2.2 Correspondència bijectiva de Galois per a extensions finites

En aquesta secció recordarem alguns resultats de teoria de Galois finita, en particular, el teorema de la correspondència bijectiva.

Donada F/K una extensió de cossos, sempre F és un K-espai vectorial. Diem que F/K és finita quan la dimensió de F com a K-espai vectorial és finit i anotem per $[F:K]$ aquesta dimensió. Si F/K finita, $Aut_K F$ sempre és un grup finit i sempre es té $[F:K] \geq |Aut_K F|$.

Teorema 2.2.1 (Artin)**.** *Si F/K és una extensió finita, F/K és de Galois $\Leftrightarrow [F:K] = |Aut_K F|$.*

Veieu [9] (capítol 1, secció 5) per una prova de l'anterior i el següent resultat.

Teorema 2.2.2 (Correspondència bijectiva de Galois)**.**
Sigui F/K una extensió finita de Galois. Denotem per
$\mathcal{A}$=$\{$ *E cos* $\mid K \subseteq E \subseteq F\}$ *i* $\mathcal{B}$=$\{H \mid H \leq Gal(F/K)\}$
i definim les aplicacions:
$\Psi : \mathcal{A} \longrightarrow \mathcal{B}$ *per* $\Psi(E) = Aut_E F = Gal(F/E)$
$\Theta : \mathcal{B} \longrightarrow \mathcal{A}$ *per* $\Theta(H) = F^H = \{\alpha \in F \mid h(\alpha) = \alpha, \forall h \in H\}$
Tenim
(i) Ψ i Θ són bijeccions, en particular, tenim una bijecció entre els subgrups de Gal(F/K) i els subcossos de F que contenen K.
(ii) Siguin $H_1, H_2 \leq Gal(F/K)$, i considerem F^{H_1} i F^{H_2}. Llavors, $\exists \sigma \in Gal(F/K)$ tal que $\sigma(F^{H_1}) = F^{H_2} \Leftrightarrow H_1 = \tau H_2 \tau^{-1}$, per cert $\tau \in Gal(F/K)$ (aquest τ és σ^{-1}).
A més,
F^H/K és de Galois $\Leftrightarrow H \trianglelefteq Gal(F/K)$.
I quan $H \trianglelefteq Gal(F/K)$ tenim, $Gal(F^H/K) \cong \frac{Gal(F/K)}{Gal(F/F^H)}$.

2.3 Tot grup finit G és grup de Galois per a certa extensió finita de cossos.

Veiem que per a tot grup finit G contruïm una extensió de cossos de manera que G és el grup de Galois que correspon a l'extensió.

Sigui G un grup finit qualsevol. Veiem [12], capítol 3, secció *Some Representation Theorems* per la prova del següent resultat.

Teorema 2.3.1. *(Teorema de Cayley) Si G és un grup finit d'ordre n, aleshores existeix un subgrup H de S_n (el grup simètric d'ordre n) tal que $G \cong H$.*

Sigui K un cos fixat, escrivim per $K(x_1, ..., x_n)$ al cos de fraccions de l'anell de polinomis en n variables amb coeficients en K. Escrivim per s_i el i-èssim polinomi simètric elemental que es defineixem com:

$s_0 := 1$

$s_1 := \sum_{i=1}^{n} x_i$

$s_2 := \sum_{i=1, i<j, j\leq n} x_i x_j$

$s_3 := \sum_{i=1, i<j<k, k\leq n} x_i x_j x_k$

...

$s_n := x_1 \cdots x_n$

Contruïm ara una extensió amb grup de Galois G. Per contruir-ho, és clau el teorema 2.3.1 i el teorema 2.3.3 on per aquest últim necessitem un resultat de teoria de Galois que recordem tot seguit.

Proposició 2.3.2. *Sigui F/K una extensió de cossos on F és el cos de descomposició sobre K d'un polinomi de grau n, aleshores, $[F : K] \leq n!$.*

Teorema 2.3.3. *En la notació anterior, $K(x_1, ..., x_n)/K(s_1, ..., s_n)$ és una extensió de Galois amb grup de Galois S_n i a més $K(s_1, ..., s_n)$ és isomorf al cos de fraccions de l'anell de polinomis en n variables amb coeficients en K.*

Demostració. El grup S_n actua sobre $K(x_1, ..., x_n)$ permutant el ordre de les variables de la manera següent. Si $\sigma \in S_n$ $\sigma(x_i) = x_{\sigma(i)}$ i obtenim $\sigma \in Aut_K K(x_1, ..., x_n)$. Fixem-nos que si s_i és un polinomi simètric, $\sigma(s_i) = s_i$ per tot $\sigma \in S_n$, per tant $\sigma \in Aut_{K(s_1,...,s_n)} K(x_1, ..., x_n)$.
Aleshores és clar que

$$K(s_1, ..., s_n) \subseteq K(x_1, ..., x_n)^{S_n} \subseteq K(x_1, ..., x_n)$$

Considerem el polinomi en x

$$p(x) = (x - x_1)...(x - x_n) = x^n - s_1 x^{n-1} + ... + (-1)^n s_n \in K(s_1, ..., s_n)[x]$$

Per tant, $K(x_1, ..., x_n)$ és el cos de descomposició de $p(x)$ sobre $K(s_1, ..., s_n)$. Com que $p(x)$ té grau n, per la proposició 2.3.2:

$$[K(x_1, ..., x_n) : K(s_1, ..., s_n)] \leq n!.$$

Observem, $S_n \leq Gal(K(x_1, ..., x_n)/K(x_1, ..., x_n)^{S_n})$ i tenim
$[K(x_1, ..., x_n) : K(x_1, ..., x_n)^{S_n}] \geq n!$.

Finalment, obtenim $[K(x_1,...,x_n)^{S_n} : K(s_1,...,s_n)] = 1$, i per tant, com $K(s_1,...,s_n) \subseteq K(x_1,...,x_n)^{K(s_1,...,s_n)} \subseteq K(x_1,...,x_n)$,
$[K(x_1,...,x_n) : K(s_1,...,s_n)] = n! = |S_n|$ obtenint el resultat. □

Teorema 2.3.4. *Donat G un grup finit, existeix una extensió finita de cossos de Galois L/M on $Gal(L/M) \cong G$.*

Demostració. Triem un cos K arbitrari. Pel teorema de Cayley podem pensar $G \leq S_n$. Considerem l'extensió de cossos $K(x_1,...,x_n)/K(s_1,...,s_n)$ amb la notiació anterior, (veiem teorema 2.3.3 i la seva demostració) que és finita i de Galois. Sabem que $Gal(K(x_1,...,x_n)/K(s_1,...,s_n)) \cong_\Psi S_n$. D'aquí, $\Psi^{-1}(G) \leq Gal(K(x_1,...,x_n)/K(s_1,...,s_n))$.
$K(x_1,...,x_n)/K(x_1,...,x_n)^{\Psi^{-1}(G)}$ és extensió de Galois pel corol·lari 2.1.7 amb grup de Galois $\Psi^{-1}(G) \cong G$ pel teorema 2.2.2. Per tant triant
$L = K(x_1,...,x_n)$ i $M = K(x_1,...,x_n)^{\Psi^{-1}(G)}$ obtenim el resultat. □

Observació 2.3.5. *Fixem-nos que en el teorema 2.3.4, donat G, L/M es construeix introduïnt el cos de fraccions de l'anell de polinomis en n variables per cert n.*
Si volem triar $M = K$ un cos fixat previament, el problema és molt més complicat, veieu la secció 2.4.

2.4 Problema invers de Galois

Després de la correspondència bijectiva de Galois i del teorema 2.3.4 es planteja la següent pregunta natural:

Qüestió 2.4.1. *Fixat un grup finit G i un cos K. Existeix una extensió L/K Galois amb $Gal(L/K) \cong G$?*

Aquesta pregunta és l'anomenat problema invers de Galois, que es va començar a estudiar a finals del segle XIX i encara manté linies d'interés d'investigació molt actives.

Evidentment si K és algebraicament tancat la resposta a la questió 2.4.1 tan sols es possible pel grup identitat.

En aquesta secció, per a simplificar, K sempre denota una extensió finita de $\mathbb{Q}$.

Conjectura 2.4.2. *Sigui K cos amb $[K : \mathbb{Q}] < \infty$. Sigui G un grup finit. Llavors existeix una extensió finita Galois L/K tal que $Gal(L/K) \cong G$.*

Hi ha molts resultats que demostren la conjectura per molts grups; no obstant, encara hi ha molts casos que encara no s'han demostrat. Anem a llistar alguns casos centrant-nos majoritàriament per $K = \mathbb{Q}$ i presentant dues direccions de treball.

Teorema 2.4.3. *Si G és un grup abelià finit llavors el problema invers de Galois té solució, és dir la conjectura 2.4.2 es compleix.*

La demostració usa la teoria de cossos de classe abstracta desenvolupada al segle XX, on caracteritza totes les extensions abelianes de K, és a dir extensions de Galois de K amb grup de Galois commutatiu, consulteu per exemple [10, Chp.IV-V-VI] per aquesta teoria.

És un problema obert per extensions finites de $\mathbb{Q}$ i diferents de $\mathbb{Q}$ trobar de manera explícita aquestes extensions abelianes [1]. Recordem sobre $\mathbb{Q}$ hi ha el teorema de Weber de 1886 (tot i que Kronecker va demostrar-ho en 1853 i Weber l'any 1886 i finalment Hilber l'any 1896 van completar diferents problemes deixats per la demostració de Kronecker)

Teorema 2.4.4 (Weber)**.** *Si $L/\mathbb{Q}$ és una extensió de Galois finita on $Gal(L/\mathbb{Q})$ és un grup abelià llavors existeix un $n \in \mathbb{N}$ on $L \subseteq \mathbb{Q}(\zeta_n)$ on ζ_n és una arrel n-èssima primitiva de 1, (és dir una arrel de $x^n - 1$ que no és arrel de $x^m - 1$ amb m divisor de n), en una clausura algebraica de $\mathbb{Q}$. En particular $Gal(L/K)$ és un quocient de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/(n))^*$.*

Considerem a partir d'ara G un grup finit no abelià.

Hi ha dos idees generals en atacar la conjectura, una usant un resultat de Hilbert "el teorema d'irreductibilitat" i l'altre resolent problemes d'inmersió. Anem a descriure-ho breument i a enunciar alguns resultats.

ffl Problemes d'inmersió, reducció a grups simples.

Definició 2.4.5. *Sigui H un grup. Un problema d'inmersió finit sobre un cos K consisteix en una extensió Galois finita L/K amb un morfisme exhaustiu $\phi : H \to Gal(L/K)$. Una solució al problema és una extensió Galois M/K amb $L \subseteq M$ conjuntament amb un isomorfisme $\beta : H \to Gal(M/K)$ complint $\phi = res_{M,L} \circ \beta$ on $res_{M,L}$ és el morfisme de restringir els automorfismes al cos L.*

Els matemàtics Scholz i Reichardt estudiaren aquests problemes durant la dècada del 1920 obtenint resultats sobre grups nilpotents, un cas concret

[1] Cal afegir que per extensions $[K : \mathbb{Q}] = 2$ de grau dos amb $K \not\subseteq \mathbb{R}$ també està resolt usant la teoria de corbes el.líptiques amb multiplicació complexa.

de grups resolubles. Recordem que hem vist en el curs de Galois la definició de grups resolubles.

Definició 2.4.6. *Un grup finit G s'anomena resoluble si existeix una cadena de subgrups H_i de G amb $0 \leq i \leq n$ complint:*

1. *$H_0 = \{e\}$ i $H_n = G$,*
2. *$H_i \lhd H_{i+1}$ per $i = 0, \ldots, n-1$,*
3. *H_{i+1}/H_i és un grup abelià per $i = 0, \ldots, n-1$.*

La cadena $H_0 \leq H_1 \leq \ldots \leq H_n = G$ direm que és una cadena resoluble per a G.

En 1954 Shafarevich va demostrar el següent resultat resolent una serie de problemes d'inmersió per la cadena de subgrups per un grup resoluble generalitzant el cas de grups nilpotents:

Teorema 2.4.7 (Shafarevich)**.** *Sigui G un grup resoluble. Llavors existeix $L/\mathbb{Q}$ Galois amb $Gal(L/\mathbb{Q}) \cong G$.*

Fixem-nos que el pas inicial del resultat de Shafarevich és donat G un grup resoluble amb $G = H_n$ i tenim el morfisme exhaustiu

$$\pi : G \to G/H_{n-1}$$

com G/H_{n-1} és un grup abelià és $Gal(L/\mathbb{Q})$ per cert cos L, i resoldre aquest problema d'inmersió per π és el resultat de Shafarevich respecte al problema d'inmersió.

Recordem la definició de grup simple:

Definició 2.4.8. *Sigui G un grup; diem que G és simple si els seus únics subgrups normals és l'element neutre i el grup G.*

Donat G un grup qualsevol triem H subgrup normal maximal més gran via inclusió en G, tenim el morfisme

$$\pi : G \to G/H$$

on G/H és un grup simple. Si podem resoldre el problema d'inmersió pels grups simples obtenim la conjectura per tot grup G. Per tant hi ha un interés primordial en resoldre la conjectura per tots els grups simples i el problema

d'inmersió en ells, pels grups abelians aquest problema està resolt per Shafarevich. [2]

- El teorema d'irreductibilitat de Hilbert.

Teorema 2.4.9 (Hilbert)**.** *Sigui $f(x_1, \ldots, x_n, X) \in \mathbb{Q}[x_1, \ldots, x_n, X]$ un polinomi en $n+1$ variables $x_1, \ldots, x_n, X$ sobre $\mathbb{Q}$. Denotem per $\mathbb{Q}(x_1, \ldots, x_n)$ el cos de fraccions de l'anell que polinomis amb coeficients a $\mathbb{Q}$ en la variable $x_1, \ldots, x_n$. Suposem que l'extensió de Galois sobre $\mathbb{Q}(x_1, \ldots, x_n)$ generada per $f(x_1, \ldots, x_n, X)$ té grup de Galois finit G. Llavors hi ha infinits $(b_1, \ldots, b_n) \in \mathbb{Q}^n$ complint que $f(b_1, \ldots, b_n, X)$ genera una extensió de Galois sobre $\mathbb{Q}$ amb grup de Galois G.*

Observació 2.4.10. *El problema del resultat de Hilbert és determinar els $(b_1, \ldots, b_n) \in \mathbb{Q}^n$ de manera explícita donat $f(x_1, \ldots, x_n, X)$; però no tractarem aquest problema aquí.*

Dels teoremes 2.4.9 i 2.3.1 es dedueïx que,

Corol·lari 2.4.11 (Hilbert, 1892)**.** *El grup alternat A_n i el grup simètric S_n es realitzen com grups de Galois sobre $\mathbb{Q}$, és a dir satisfan la conjectura 2.4.2.*

Amb la idea d'intentar construir G finits sobre $\mathbb{Q}(x_1, \ldots, x_n)$ per cert n usant el teorema 2.4.9 s'han obtingut diversos resultats, majoritàriament per grups simples:

Teorema 2.4.12 (Shih, circa 1970 i posterior)**.** *Fixem un primer p. Considerem el grup $G = PSL_2(\mathbb{F}_p)$ on $PSL_2(\mathbb{F}_p) = SL_2(\mathbb{F}_p)/\{\pm Id\}$ on $SL_n(F)$ són les matrius $n \times n$ a coeficients en F amb determinant igual a 1. Suposem que 2 o 3 o 5 o 7 no és un quadrat en $\mathbb{F}_p$. Llavors existeix $L/\mathbb{Q}$ Galois amb $Gal(L/\mathbb{Q}) \cong G$.*

I Beyli, Matzat, Malle i Thompson en els anys 1980 obtenen un criteri per grups G amb centre trivial sota certes hipòtesis en les classes de conjugació que s'aplica en:

[2] Es té el següent resultat respecte la classificació de grups simples finits de l'any 2004 de Aschbacher and Smith: Tot grup finit simple és isomorf a un dels següents grups:

1. un grup cíclic d'ordre primer,
2. un grup alternat A_n amb $n \geq 5$,
3. un grup simple corresponent a families de grups de Lie, hi ha 18 families,
4. els 26 grups simples esporàdics.

Corol·lari 2.4.13. *Sigui G un grup simple esporàdic, $G \neq M_{23}$ un dels grups de Mathieu. Llavors, existeix $L/\mathbb{Q}$ Galois amb grup de Galois isomorf G.*

Corol·lari 2.4.14. *Pels següents grups G,*

1. *$PSL_2(\mathbb{F}_p)$ per cada primer $p \not\equiv \pm 1 (mod\ 24)$;*
2. *$PSL_2(\mathbb{F}_{p^2})$ per cada primer $p \equiv \pm 2 (mod\ 5)$;*
3. *$PSL_3(\mathbb{F}_p)$ per cada primer $p \equiv 1 (mod\ 4)$*

existeix $L/\mathbb{Q}$ Galois amb $Gal(L/\mathbb{Q}) \cong G$.

Observació 2.4.15. *També hi ha resultats per altres families de grups Lie com el grup simplèctic, el grup especial unitari, grup ortogonal especial..., veieu per exemple el treball de Núria Vila [15].*

- Altres direccions.

Una idea per atacar el problema sobre $\mathbb{Q}$ és computacional. Hi ha tot un conjunt de treballs que estudien tots els grups que surten amb polinomis d'un grau fix. Hi ha resultats que s'han calculat tots els grups de Galois que surten d'introduir arrels de polinomis irreductibles sobre $\mathbb{Q}[x]$ de grau ≤ 15 [8] (i la correcció per a obtenir el grup $SL_2(\mathbb{F}_{16})$ d'ordre 4080 [1] que era el grup d'ordre més petit que no es coneixia la resposta a la conjectura 2.4.2 en l'any 2006).

Una altra idea de gran profunditat és usant Geometria Aritmética de Varietats algebraiques i les seves representacions de Galois. Les tècniques són molt més sofisticades però s'estan donant molts resultats importants en l'actualitat. Per veure un compendi de totes aquestes idees actuals via Geometria Aritmética, totes molt de moda després dels treballs d'Andrew Wiles referent a Fermat, suggerim la lectura de la tesis doctoral de Luis Dieulefait [5].

No obstant com a primera lectura, per aprofundir en el problema i resultats e idees, suggerim el llibre de J.P.Serre [13].

Com remarca final a aquesta secció en l'actualitat, Juny 2012, el grup simple més petit d'ordre en què no està publicada cap resposta és el grup de Lie $PSU(3, \mathbb{F}_9)$, el grup projectiu unitari del cos finit de 9 elements, segons la pàgina:

http://mathoverflow.net/questions/80359/which-small-finite-simple-groups-are-not-yet-known-to-be-galois-groups-over-q

Capítol 3

Correspondència de Galois per a extensiones no finites de Galois

3.1 Bijecció entre subcossos i subgrups?

Veurem en aquesta secció que la correspondència bijectiva del cas finit 2.2.2 no és certa per a extensions no finites.

Sigui F/K una extensió de Galois no necessàriament finita. Definim $\mathcal{A}$={E cos | $K \subseteq E \subseteq F$} i $\mathcal{B}$=$\{H \mid H \leq Gal(F/K)\}$ i igual que al cas finit podem definir les aplicacions
$\psi : \mathcal{A} \longrightarrow \mathcal{B}$ via $\psi(E) = Aut_E F = Gal(F/E)$ i
$\Theta : \mathcal{B} \longrightarrow \mathcal{A}$ via $\Theta(H) = F^H = \{\alpha \in F : \sigma(\alpha) = \alpha$,per tot $\sigma \in H\}$

Teorema 3.1.1. *Sigui F/K extensió de Galois no finita. L'aplicació Θ no és necessàriament bijectiva.*

Per justificar-ho contruirem una extensió concreta F/K de Galois i no finita on Θ no és bijectiva.
Considerem $\mathbb{F}_p$ el cos finit de p elements on p és un primer fix, i denotem per $\overline{\mathbb{F}_p}$ una clausura algebraica de $\mathbb{F}_p$ fixada. Considerem l'extensió de cossos $\mathbb{F}_{p^n}/\mathbb{F}_p$ on $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$ on és clar $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Definició 3.1.2. *Sigui l'aplicació:*
$Frob_{p,n} : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ *via* $Frob_{p,n}(x) = x^p$.

Aquesta aplicació és un morfisme de cossos, i s'anomena el morfisme de Frobenius.

Lema 3.1.3. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ és de Galois amb grup de Galois generat pel $Frob_{p,n}$.*

Demostració. Veiem primer de tot que és algebraica.
Sigui $\alpha \in \mathbb{F}_{p^n}$, com que $\alpha^{p^n} - \alpha = 0$ α és algebraic, i per tant $\mathbb{F}_{p^n}/\mathbb{F}_p$ algebraica.
Veiem que és separable:
Sigui $l(x) \in \mathbb{F}_p[x]$ irreductible i mònic on $l(\beta) = 0$ per cert $\beta \in \mathbb{F}_{p^n}$.
$l(x) = Irr(\beta, \mathbb{F}_p)[x] | (x^{p^n} - x) = m(x)$ i $mcd(m(x), m'(x)) = 1$, ja que $m'(x) = -1$. Per tant, $l(x)$ no té arrels repetides.
Veiem que $\mathbb{F}_{p^n}/\mathbb{F}_p$ normal:
Sigui $s(x) \in \mathbb{F}_p[x]$ mònic i irreductible i $\gamma \in \mathbb{F}_{p^n}$ una arrel de s.
$s(x) = Irr(\gamma, \mathbb{F}_p)[x] | (x^{p^n} - x)$, on $x^{p^n} - x$ té n arrels diferents perque la seva derivada és -1 i sabem que totes són a $\mathbb{F}_{p^n}$ (per construcció), per tant
$x^{p^n} - x = \prod_{\delta \in \mathbb{F}_{p^n}} (x - \delta)$.
Aleshores, $s(x)$ descompon totalment en $\mathbb{F}_{p^n}$.
Per acabar, considerant $Frob_{p,n} : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$, és facil demostrar que $Frob_{p,n}$ té ordre n i com $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] \geq |Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)|$,
obtenim $< Frob_{p,n} >= Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. □

Lema 3.1.4. *$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si $n \mid m$.*

Demostració. Sigui $\beta \in \mathbb{F}_{p^n}$, aleshores $\beta^{p^n} - \beta = 0$. Com que $n \mid m$, $m = nl$ per cert l. Tenim que $0 = (\beta^{p^n} - \beta)^{p^{n(l-1)}} = \beta^{p^{nl}} - \beta = \beta^{p^m} - \beta$, per tant $\beta \in \mathbb{F}_{p^m}$. □

Pensem ara en l'extensó de cossos $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ on $\mathbb{F}_{p^{p^\infty}} := \bigcup_{j \in \mathbb{N}} \mathbb{F}_{p^{p^j}}$.
Aquest és l'exemple que presentem per a F/K de Galois no finit on Θ no és bijectiva.
Es comprova que $\mathbb{F}_{p^{p^\infty}}$ és un cos on la suma i el producte els pensem de la següent manera: si $\alpha, \beta \in \mathbb{F}_{p^{p^\infty}}$, $\exists n, m \in \mathbb{N}$ tals que $\alpha \in \mathbb{F}_{p^{p^n}}$ i $\beta \in \mathbb{F}_{p^{p^m}}$.
Podem supossar $n \leq m$, i per tant pensem la suma i el producte en
$\mathbb{F}_{p^{p^m}} \subseteq \mathbb{F}_{p^{p^\infty}}$, ja que $p^n \mid p^m$ i pel lema 3.1.4, $\mathbb{F}_{p^{p^n}} \subseteq \mathbb{F}_{p^{p^m}}$.

Teorema 3.1.5. *L'extensió $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ és de Galois no finita.*

Demostració. • $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ algebraica:
Sigui $\alpha \in \mathbb{F}_{p^{p^\infty}} = \bigcup_{j \in \mathbb{N}} \mathbb{F}_{p^{p^j}} \Rightarrow \exists j \in \mathbb{N}$ tal que $\alpha \in \mathbb{F}_{p^{p^j}} \Leftrightarrow \alpha^{p^{p^j}} - \alpha = 0$; α és arrel del polinomi $x^{p^{p^j}} - x \in \mathbb{F}_p[x]$ i d'aqui α algebraic i $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ algebraica.

• $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ normal:
Sigui $m(x)$ un polinomi irreductible i monic i $\mu \in \mathbb{F}_{p^{p^\infty}}$ on $m(\mu) = 0$. Per contrucció de $\mathbb{F}_{p^{p^\infty}}$ $\mu \in \mathbb{F}_{p^{p^j}}$ per cert j.
$m(x) = Irr(\mu, \mathbb{F}_p)[x] \mid (x^{p^{p^j}} - x) = \prod_{\delta \in \mathbb{F}_{p^{p^j}}} (x - \delta)$.
I per tant en $\mathbb{F}_{p^{p^j}}$ $m(x)$ desconpon en producte de polinomis de grau 1, i com $\mathbb{F}_{p^{p^j}} \subseteq \mathbb{F}_{p^{p^\infty}}$, $m(x)$ desconpon en $\mathbb{F}_{p^{p^\infty}}$ en producte de polinomis de grau 1.
• $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ separable:
$\alpha \in \mathbb{F}_{p^{p^\infty}}$, $\alpha \in \mathbb{F}_{p^{p^j}}$ per cert j, i com abans, $Irr(\alpha, \mathbb{F}_p)[x] \mid (x^{p^{p^j}} - x)$ amb $x^{p^{p^j}} - x$ separable, perque la seva derivada val -1, d'on obtenim el resultat.
• $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ no finita:
Sabem que $[\mathbb{F}_{p^{p^j}} : \mathbb{F}_p] = p^j$, i $\mathbb{F}_{p^{p^{j+1}}}/\mathbb{F}_{p^{p^j}}/\mathbb{F}_p$ on $[\mathbb{F}_{p^{p^{j+1}}} : \mathbb{F}_p] = p^{j+1}$, i com que aquest j el podem fer tant gran com vulguem,
quan $j \to \infty$ $[\mathbb{F}_{p^{p^j}} : \mathbb{F}_p] = p^j \to \infty$. □

Proposició 3.1.6. *El grup de Galois $Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)$ és un grup abelià isomorf a $\varprojlim Gal(F_{p^{p^j}}/\mathbb{F}_p)$ i en particular a $(\mathbb{Z}_p, +)$ on $\mathbb{Z}_p$ és l'anell dels nombres p-àdics.*[1]

Demostració. Observem que per a cada j, $[\mathbb{F}_{p^{p^j}} : \mathbb{F}_p] = p^j$, veiem que $Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) \cong (\mathbb{Z}/(p^j), +)$.
Efectivament per a cada j, $Frob_{p,p^j}$ té ordre p^ji definim
ψ_j de $Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) =< Frob_{p,p^j} >$ a $(\mathbb{Z}/(p^j), +)$ que envia $Frob_{p,p^j}$ al 1, que clarament és un isomorfisme.
Tenim el següent diagrama commutatiu per a cada j,

$$\begin{array}{ccc} Gal(\mathbb{F}_{p^{p^{j+1}}}/\mathbb{F}_p) =< Frob_{p,p^j} > & \xrightarrow{\psi_{j+1}} & (\mathbb{Z}/(p^{j+1}), +) \\ \downarrow & & \downarrow \\ Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) =< Frob_{p,p^j} > & \xrightarrow{\psi_j} & (\mathbb{Z}/(p^j), +) \end{array} \tag{3.1}$$

on la aplicació que va de $Gal(\mathbb{F}_{p^{p^{j+1}}}/\mathbb{F}_p)$ a $Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p)$ és la restricció de cossos a $\mathbb{F}_{p^{p^j}}$ i la que va de $\mathbb{Z}/(p^{j+1})$ a $\mathbb{Z}/(p^j)$ la projecció natural.
De les propietats de límits projectius, veiem la secció A.1. del apèndix,

[1] consultar apèndix A.1 per definició de límits projectius i A.1.7. i A.1.8. per deficinició i propietats de $\mathbb{Z}_p$

$\varprojlim Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) \cong \varprojlim(\mathbb{Z}/(p^j),+) \cong (\mathbb{Z}_p,+)$.

Explicitem finalment que
$Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p) \cong \varprojlim Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p)$ on recordem de A.1 que
$\varprojlim Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) = \{(a_i)_i \in \prod Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) \mid a_i \restriction_{\mathbb{F}_{p^{p^i}}} = a_j \text{ per } j < i\}$.

Amb les restriccions naturals tenim que el següent sistema commuta:

$$\begin{array}{ccc} Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p) & \xrightarrow{\varphi_i} & Gal(\mathbb{F}_{p^{p^i}}/\mathbb{F}_p) \\ & {\scriptstyle\varphi_j}\searrow \quad \swarrow{\scriptstyle\varphi_{ij}} & \\ & Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) & \end{array}$$

Llavors, $\exists!\varphi : Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p) \longrightarrow \varprojlim Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p)$ morfisme de grups, per la propietat universal de límit projectiu.
I ara cal veure que φ és bijecctiva.
El morfisme φ és injectiu:
Siguin $\sigma,\tau \in Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)$ essent $\sigma \neq \tau$, tenim, $\exists x \in \bigcup_{j\in\mathbb{N}} \mathbb{F}_{p^{p^j}}$ on $\sigma(x) \neq \tau(x)$.
$x \in \mathbb{F}_{p^{p^l}}$ per cert $l \in \mathbb{N}$. Llavors, per aquest l, com que $\mathbb{F}_{p^{p^l}}$ és normal sobre $\mathbb{F}_p$, $\sigma(x),\tau(x) \in \mathbb{F}_{p^{p^l}}$, i aleshores, $\sigma \restriction_{\mathbb{F}_{p^{p^l}}} \neq \tau \restriction_{\mathbb{F}_{p^{p^l}}}$
Per tant, $\varphi(\sigma) \in \prod_{j\in\mathbb{N}} Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p)$ i $\varphi(\tau) \in \prod_{j\in\mathbb{N}} Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p)$ són diferents (perquè ho són en una component). I aleshores φ és injectiva.
El morfisme φ és exhaustiu:
Sigui $(\sigma_n)_n \in \varprojlim Gal(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p)$, i definim
$\widetilde{\sigma} : \mathbb{F}_{p^{p^\infty}} \longrightarrow \mathbb{F}_{p^{p^\infty}}$ de la manera següent.
Com que $\mathbb{F}_{p^{p^\infty}} = \bigcup_{j\in\mathbb{N}} \mathbb{F}_{p^{p^j}}$, si $x \in \mathbb{F}_{p^{p^j}}$, $\widetilde{\sigma}(x) := \sigma_j(x)$ on sabem que $\sigma_j(x) = \sigma_l(x), \forall l \geq j$.
És fàcil comprovar que $\widetilde{\sigma} \in Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)$.

□

Proposició 3.1.7. *Per $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$, l'aplicació Θ no és bijectiva.*

Demostració. Definim $\mathcal{F}rob_p = \prod(Frob_{p,p^n}) \in \varprojlim Gal(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p) \subseteq \prod Gal(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p)$.
Aquest $\mathcal{F}rob_p \in \varprojlim Gal(\mathbb{F}_{p^{p^n}}/\mathbb{F}_p)$, pel diagrama (3.1) que hem vist abans.
Via l'isomorfisme
$\phi : \varprojlim Gal(\mathbb{F}_{p^{p^j}}/\mathbb{F}_p) \longrightarrow \mathbb{Z}_p$, on

$$\phi(\prod(Frob_p)) = \prod 1 \in \prod(\mathbb{Z}/(p^n),+)$$

L'element $\prod 1$ és de $\mathbb{Z}_p$, i correspon a $1 + 0p + 0p^2 + ...$ (en la definició de $\mathbb{Z}_p$ en A.1.7), que és l'element que genera $\mathbb{Z}$ dins de $\mathbb{Z}_p$. Per tant, $\phi(< \mathcal{F}rob_p >) =< 1 >= \mathbb{Z}$.
Ara, tornem a la correspondencia bijectiva, observem:
$\Theta(< \mathcal{F}rob_p >) = \mathbb{F}_{p^{p^\infty}}^{<\mathcal{F}rob_p>} = \{\alpha \in \mathbb{F}_{p^{p^\infty}} |\ \mathcal{F}rob_p(\alpha) = (\alpha)\} = \mathbb{F}_p$, ja que donat $\alpha \in \mathbb{F}_{p^{p^\infty}}$, $\alpha \in \mathbb{F}_{p^{p^i}}$ per cert i, i $\mathcal{F}rob_p(\alpha) = Frob_{p,p^i}(\alpha) = \alpha^p = \alpha$ on $\alpha \in \mathbb{F}_p$.
Per altra banda, si agafem $Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)$ i mirem quin és el cos fixat per tots els $\mathbb{F}_p$-automorfismes de $\mathbb{F}_{p^{p^\infty}}$, com que Θ conserva les inclusions, obtenim: $\mathbb{F}_p = \mathbb{F}_p^{<\mathcal{F}rob_p>} \supseteq \mathbb{F}_p^{Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)} \supseteq \mathbb{F}_p$. És a dir, que $\mathbb{F}_p^{Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)} = \mathbb{F}_p$.
Observem que $\mathbb{Z} \lneq \mathbb{Z}_p$, ja que l'element $1 + p + p^2 + ... \in \mathbb{Z}_p$ i no pertany a $\mathbb{Z}$ (veiem els elements de $\mathbb{Z}_p$ en A.1.7). Observem que $< \mathcal{F}rob_p > \cong \mathbb{Z}$ i $Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p) \cong \mathbb{Z}_p$, són dos sugbrups diferents, donen el mateix cos fix via l'aplicació Θ. Per tant, Θ no és injectiva. □

3.2 Posem topologia en Gal(F/K), grups profinits.

Siguin F i K cossos tals que F és una extensió de Galois de K. En aquesta secció:
$G = Gal(F/K) = \{\sigma \in AutF : \sigma \restriction_K = id_K\}$
$\mathcal{I}$=$\{$E | $K \subseteq E \subseteq F$ amb [E:K] $\leq \infty$ i E/K de Galois$\}$
$\mathcal{E} = \{N \leq G \mid N = Gal(F/E)$ per algun $E \in \mathcal{I}\}$

Lema 3.2.1. *Sigui F/K és normal, i $K \subseteq L \subseteq F \subseteq E$ inclusió cossos amb $\tau : L \longrightarrow E$ un K-homomorfisme, és a dir $\tau \restriction_K = id$. Llavors $\tau(L) \subseteq F$ i existeix un $\sigma \in Aut_K F$ tal que $\sigma \restriction_L = \tau$.*

Demostració. Veiem que $\tau(L) \subseteq F$.
Sigui $\alpha \in L$, α és algebraic i com F/K és normal $Irr(\alpha, K)[x]$ té totes les arrels en F.
Com $\tau(Irr(\alpha, K)[x]) = Irr(\alpha, K)[x]$, perque $\tau \restriction_K = id$, obtenim que $\tau(\alpha)$ és arrel de $Irr(\alpha, K)[x]$, per tant $\tau(\alpha) \in F$ provant $\tau(L) \subseteq F$.
Veiem que existeix un $\sigma \in Aut_K F$ tal que $\sigma \restriction_L = \tau$.
Sigui $\beta \in F$, com F/K és normal, F/L també ho és. Per tant existeix $Irr(\beta, L)[x] \in L[x]$. Com que τ és homomorfisme, $\tau(Irr(\beta, L)[x])$ tindrà els coeficients en $\tau(L)$.
Definim $\widetilde{\tau} : L(\beta) \longrightarrow F$ com
$\widetilde{\tau} \restriction_L = \tau$ i $\widetilde{\tau}(\beta) :=$ una arrel de $\tau(Irr(\beta, L)[x])$; que sabem que existeix perque $F/\tau(L)$ és normal.

Podem repetir aquest procés per $\beta_i \in F/L(\beta_1, ..., \beta_{i-1})$ fins aconseguir tot F, obtenint així $\sigma : F \longrightarrow F$ injectiva, morfisme de cossos i per construcció $\sigma \restriction_L = \tau$.
Veiem que és exhaustiva.
Sigui $\gamma \in F$ i considerem el conjunt finit $R_\gamma = \{$ arrels en F del polinomi $Irr(\gamma, K)[x]\}$. Aleshores, per $\delta \in R_\gamma$ tenim:

$$Irr(\gamma, K)[\sigma(\delta)] = \sigma(Irr(\gamma, K)[\delta]) = \sigma(0) = 0$$

Per tant, σ envia R_γ a ell mateix, i com σ injectiva i R_γ finit, tenim que τ restringida a $R\gamma$ és bijectiva, d'on per $\delta \in R_\gamma$ sempre existeix $\beta \in R_\gamma$ tal que $\sigma(\beta) = \gamma$. Per tant, donat $\mu \in F$ $\mu \in R_\mu$ i $\exists \beta \in F$ on $\sigma(\beta) = \mu$, per tant σ exhaustiva. □

Anem ara a obtenir algunes propietats de G, $\mathcal{I}$ i $\mathcal{E}$.

Lema 3.2.2. *Donats $\alpha_1, ..., \alpha_n \in F$, existeix $E \in \mathcal{I}$ amb $\alpha_i \in E$ $\forall i = 1, ..., n$.*

Demostració. Sigui E el cos de descomposició sobre K de $\prod_{i=1}^{n} Irr(\alpha_i, K)$, per tant E normal sobre K.
Com que els α_i són separables sobre K, ja que F/K és Galois, el cos E és normal i separable sobre K; és a dir, que E és de Galois sobre K.
Com $E = K(\alpha_1, ..., \alpha_n)$ i α_i K-algebraics, tenim $[E : K] < \infty$, per tant $E \in \mathcal{I}$. □

Lema 3.2.3. *Sigui $N \in \mathcal{E}$, $N = Gal(F/E)$ amb $E \in \mathcal{I}$. Llavors, $E = F^N$ i N és normal en G.*
A més, $G/N \cong Gal(E/K)$ i $|G/N| = |Gal(E/K)| = [E : K] < \infty$.

Demostració. Com que F és normal i separable sobre K, també ho és sobre E. Llavors, F/E és de Galois, pel corol·lari 2.1.7.
Veiem que $E = F^N$.
Que $E \subseteq F^N$ és evident, perquè si $\alpha \in E \subseteq F$, $\sigma(\alpha) = \alpha$ $\forall \sigma \in Gal(F/E) = N$ i d'on $\alpha \in \{\beta \in F \mid \sigma(\beta) = \beta \ \forall \sigma \in N\} = F^N$.
Per veure $F^N \subseteq E$, suposem que existeix $\alpha \in F^N$ tal que $\alpha \notin E$.
Aleshores, $E \subsetneq E(\alpha)$. A més l'extensió $E(\alpha)/E$ és finita. Per tant, de la demostració del lema 3.2.1, com F/E i $F/E(\alpha)$ són de Galois, $\exists \sigma \in Gal(F/E) = N$ on
$\sigma : E(\alpha) \longrightarrow F$ envia α a una altre arrel de $Irr(\alpha, E)[x]$ diferent de α (per ser separable) i σ es pot extendre fins a F.

Per tant, $\sigma \notin Gal(F/E(\alpha))$, és a dir, $Gal(F/E) \gneq Gal(F/E(\alpha))$.
Per tant $\sigma \in N - Gal(F/E(\alpha))$, $\sigma(\alpha) \neq \alpha$ i per tant $\alpha \notin F^N$, contradicció.
Per tant, $E = F^N$.
Per veure que $N \trianglelefteq G$, recordem que el nucli d'un morfisme de grups sempre és un subgrup normal.
Considerem l'aplicació $\phi : Gal(F/K) \longrightarrow Gal(E/K)$ tal que $\sigma \longmapsto \sigma \restriction_E$.
Clarament ϕ és morfisme de grups. Si mirem

$$ker\phi = \{\sigma \in Gal(F/K) \mid \sigma \restriction_E = id\} = Gal(F/E) = N$$

A més, pel lema 3.2.1 ϕ és exhaustiva (perquè hem vist que si $K \subseteq E \subseteq F$ una inclusió de cossos on F/K normal, per a cada $\tau \in Aut_K E$ $\exists \sigma : F \longrightarrow F$ tal que $\phi(\tau) = \tau \restriction E = \tau$).
Aleshores, pel primer teorema d'isomorfia de grups,
$Gal(E/K) \cong G/N$.
D'on fàcilment, $|G/N| = |Gal(E/K)| = [E : K] < \infty$.

□

Lema 3.2.4. *Es té* $\bigcap_{N\in\mathcal{E}} N = \{id\}$. *A més,* $\bigcap_{N\in\mathcal{E}} \sigma N = \{\sigma\}$ $\forall \sigma \in G$

Demostració. Sigui $\tau \in \bigcap_{N\in\mathcal{E}} N$ i $a \in F$ arbitrari. Pel lema 3.2.2, existeix $E \in \mathcal{I}$ amb $a \in E$.
Agafem $N = Gal(F/E) \in \mathcal{E}$; com $\tau \restriction_E = id$ si $\tau \in N$, tenim $\tau(a) = a$. Per tant $\forall a \in F$ $\exists \tau_a \in N_a \in \mathcal{E}$ on $\tau_a(a) = a$. D'aquí $\bigcap_{N\in\mathcal{E}} N = id$.
Pel segon apartat, si $\omega \in \bigcap_{N\in\mathcal{E}} \sigma N$, llavors $\sigma^{-1}\omega \in N$ per tot $N \in \mathcal{E}$. Això implica que $\sigma^{-1}\omega = id$, per tant $\bigcap_{N\in\mathcal{E}} \sigma N = \sigma$

□

Lema 3.2.5. *Siguin* $N_1, N_2 \in \mathcal{E}$, *llavors* $N_1 \cap N_2 \in \mathcal{E}$

Demostració. Sigui $N_i = Gal(F/E_i)$ amb $E_i \in \mathcal{I}$ per $i = 1, 2$. Cada E_i és una extensió finita de Galois sobre K, pel que E_1E_2 també ho és, i fàcilment, $E_1E_2 \in \mathcal{I}$ (on E_1E_2 és el cos més petit que conté a tots dos).
Per finalitzar és suficient demostrar que $Gal(F/E_1E_2) = N_1 \cap N_2$.
Definim $\phi : G \longrightarrow Gal(E_1E_2/K)$ tal que $\sigma \restriction_{E_1E_2}$.
Veiem $N_1 \cap N_2 \subseteq \ker\phi$.
Com E_i/K són extensions normals i finites, $E_1 = K(\alpha_1, ..., \alpha_n)$ i $E_2 = K(\delta_1, ..., \delta_l)$ on $E_1E_2 = K(\alpha_1, ..., \alpha_n, \delta_1, ..., \delta_l)$. Si $\tau \in N_1 \cap N_2$ $\tau(\alpha_i) = \alpha_i$ i $\tau(\delta_j) = \delta_j$, d'on $\tau \restriction_{N_1\cap N_2} = id$, per tant $\tau \in ker\phi$.
Per veure l'altre inclusió, si $\omega \in ker\phi$, $\omega(\alpha_i) = \alpha_i$ $\forall i = 1, ..., n$ d'on $\omega \in N_1$, i $\omega(\delta_j) = \delta_j$ $\forall j = 1, ..., l$ d'on $\omega \in N_2$. Per tant $ker\phi = N_1 \cap N_2$. Ara pel

lema 3.2.3, $\frac{Gal(F/K)}{N_1 \cap N_2} \cong Gal(E_1E_2/K)$, i obtenim $Gal(F/E_1E_2) = N_1 \cap N_2$.

□

Definició 3.2.6. *La topologia de Krull en G es defineix de la següent manera:*
Un subconjunt X és obert si $X = \emptyset$ o bé $X = \bigcup_{i \in I} \sigma_i N_i$ per $\sigma_i \in G$ amb $N_i \in \mathcal{E}$

Observació 3.2.7. *La topologia de Krull defineix una topologia en G:*
És clar que G i $\emptyset$ són oberts, i també que la unió d'oberts ho és.
Per veure que és una topologia veiem que l'intersecció de dos oberts és obert.
És suficient veure que $\tau_1 N_1 \cap \tau_2 N_2$ és obert per qualsevol $N_1, N_2 \in \mathcal{E}$.
Si $\sigma \in \tau_1 N_1 \cap \tau_2 N_2$, llavors
$\tau_1 N_1 \cap \tau_2 N_2 = \sigma N_1 \cap \sigma N_2 = \sigma(N_1 \cap N_2)$ i $\sigma(N_1 \cap N_2)$ és obert perquè $N_1 \cap N_2 \in \mathcal{E}$ (del lema 3.2.5).

Observació 3.2.8. *Si $G = Gal(F/K)$ és finit, llavors la topologia de Krull de G és la topologia discreta.*

Demostració. [Observació 3.2.8] Si $Gal(F/K)$ és finit es té F/K finit, ja que si F/K de Galois fos no finita, tendriem una cadena extrictament creixent i no finita $K(\alpha_1) \subsetneq K(\alpha_1, \alpha_2) \subsetneq \cdots F$ i del lema 3.2.1 deduïm una cadena infinita de subgrups

$$Gal(F/K) \gneq Gal(F/K(\alpha_1)) \gneq Gal(F/K(\alpha_1, \alpha_2)) \gneq \cdots$$

d'on $Gal(F/K)$ no pot tenir ordre finit.
Com $\{id\} = idN_F$ amb $N_F = Gal(F/F)$ és obert i qualsevol $\sigma \in G$ es pot escriure $\{\sigma\} = \sigma\{id\}$ amb $\{id\} \in \mathcal{E}$, tenim que $\{\sigma\}$ obert.
Escrivim, $Gal(F/K) = \{id, \sigma_1, \sigma_2, ..., \sigma_n\}$ on cada σ_i és obert, d'on $\{\sigma\} = Gal(F/K) - \{\bigcup_{\sigma_i \neq \sigma} \sigma_i\}$ també tancat. □

Observació 3.2.9. *Com que qualsevol obert no buit de G és unió de cosets de subgrups de $\mathcal{E}$, el conjunt $\Delta = \{\sigma N \mid \sigma \in G, N \in \mathcal{E}\}$ és una base de la topologia de Krull de G.*

Lema 3.2.10. *Si $N \in \mathcal{E}$ i $\sigma \in G$ es té σN és obert i tancat.*

Demostració. Si $N \in \mathcal{E}$, per definició, $|G : N| < \infty$, G s'escriu com una unió finita $G = \bigcup_{i=1}^{n} \sigma_i N$, llavors $G - \sigma N = \bigcup_{i=1, \sigma_i \neq \sigma}^{n} \sigma_i N$ és una unió finita d'elements de Δ.

□

Definició 3.2.11. *Un grup Gr amb una topologia s'anomena grup topològic si Gr és un grup amb operació $\circ$ i les aplicacions $op : Gr \times Gr \to Gr$ donat pel producte $(g_1, g_2) \mapsto g_1 \circ g_2$ i $inv : Gr \to Gr$ definit per $inv(g) = g^{-1}$ són continues.*

Proposició 3.2.12. *El grup $G = Gal(F/K)$ amb la topología de Krull és un grup topològic.*

Demostració. Veiem primer $inv : G \to G$ és continua. Sigui U un obert de G, escrivim del fet de ser U obert $U = \cup\sigma = \cup\sigma N_\sigma$ on $N_\sigma \in \mathcal{E}$ on σ els elements de U. Obtenim

$$inv^{-1}(U) = \cup inv^{-1}(\sigma N_\sigma) = \cup N_\sigma\sigma^{-1} = \cup\sigma^{-1}(\sigma N_\sigma\sigma^{-1}) = \cup\sigma^{-1}N_\sigma$$

obert en G on en l'última igualtat hem usat N_σ normal en G pel lema 3.2.3.

Calculem ara $op^{-1}(U) = \cup_{\sigma\in U}\{(g_1, g_2)|g_1 \cdot g_2 = \sigma\}$. També obtenim:

$$op^{-1}(U) = \cup_{\sigma\in U} op^{-1}(\sigma N_\sigma) \supseteq \cup_{\sigma\in U}\{g_1N_\sigma \times g_2N_\sigma | g_1g_2 = \sigma\} = *$$

on l'última inclusió ve de
$op(g_1N_\sigma \times g_2N_\sigma) = g_1N_\sigma \cdot g_2N_\sigma = g_1g_2(g_2^{-1}N_\sigma \cdot g_2)N_\sigma = g_1g_2N_\sigma$ pel lema 3.2.3.
Clarament $* \supseteq op^{-1}(U)$ d'on $op^{-1}(U) = \cup_{\sigma\in U}\{g_1N_\sigma \times g_2N_\sigma | g_1g_2 = \sigma\}$ és obert de $G \times G$.

□

Definició 3.2.13. *Un espai topològic és totalment disconnex si i només si, els únics subconjunts connexes són els punts aïllats.*

Teorema 3.2.14. *Amb la topologia de Krull a G, G és Hausforff, compacte i totalment disconnex.*

Demostració. Sigui X un subconjunt de G (amb més d'un element), $\sigma, \tau \in X$ i $\sigma N \in \sigma\mathcal{E}$ un entorn obert de σ tal que $\tau \notin \sigma N$.Com,

$$X = (\sigma N \cap X) \cup ((G - \sigma N) \cap X)$$

on $(\sigma N \cap X)$ i $((G - \sigma N) \cap X)$ són oberts de X amb la topologia induïda, ja que σN i $G - \sigma N$ ho són a G. Per tant X és unió de dos oberts no buits i disjunts; per això X és no connex. I llavors, com qualsevol subconjunt de G és no connex, G és totalemnt disconnex.

Per veure que és Hausdorff, agafem $\sigma \in G$.

Del lema 3.2.4 tenim $\{\sigma\} = \bigcap_{N\in\mathcal{E}} \sigma N$. Si $\tau \neq \sigma$ existeix $N \in \mathcal{E}$ tal que $\tau \notin \sigma N$. Cada σN és un entorn obert de σ, però també tancat. Llavors, σN i $G - \sigma N$ són conjunts oberts disjunts tals que $\sigma \in \sigma N$ i $\tau \in G - \sigma N$; és a dir, G és Hausdorff.

Falta veure que G és compacte. (Per demostrar-ho veurem com es contrueix G a través de productes de grups finits de Galois d'extensions finites).
Sigui $P = \prod_{N\in\mathcal{E}} G/N$. Considerem P amb la topologia del producte, i els grups finits G/N amb la topologia discreta.
Notem que cada G/N és Hausdorff i compacte, llavors P és Hausdorff i pel teorema de Thychonoff P és compacte.
Hi ha un morfisme natural $f : G \longrightarrow P$, que envia σ a $f(\sigma) = (\sigma N)_{N\in\mathcal{E}}$.
Veurem que f és un homeomorfisme de G a l'imatge de f i que aquest imf és tancat en P.
Com que P és compacte i Hausdorff, això demostrarà que imf és compacte, i llavors G també ho serà, per ser homeomorf a imf.
• f és injectiva:
$Kerf = \{\sigma \in G \mid \sigma N = N \ \forall N \in \mathcal{E}\}$. D'on $\sigma \in Kerf \Leftrightarrow \sigma N = N$ $\forall N \in \mathcal{E} \Leftrightarrow \sigma \in \bigcap_{N\in\mathcal{E}} N \Leftrightarrow \sigma = id$, i $Kerf = id$, provant que f es injectiva.
• f és contínua:
Sigui ara $\pi_N : P \longrightarrow G/N$ la projecció exhaustiva per a cada N. Llavors, $\pi_N(f(\sigma)) = \sigma N$ per cada $\sigma \in G$. Els conjunts τN forman una base de la topologia discreta en G/N. Llavors, per la definició de la topologia del producte, qualsevol conjunt obert de P és unió d'interseccions finites de conjunts de la forma $\pi_N^{-1}(\tau N)$ per $\tau \in G$ i $N \in \mathcal{E}$.
$\bigcup_{\tau\in G, N\in\mathcal{E}} \bigcap_{i=1}^{k} \pi_N^{-1}(\tau_i N_i)$
Per veure que f és continua és suficient veure que $f^{-1}(\pi_N^{-1}(\{\tau N\}))$ és obert en G per a qualsevol $\tau N \in G$. Però $f^{-1}(\pi_N^{-1}(\{\tau N\})) = \tau N$és obert, i llavors f és continua. Per tant, com que hem vist que és injectiva, és un homeomorfisme de G a imf.
• imf és tancada:
Per definició de G i $N \in \mathcal{E}$ tenim que G/N és isomorf a $Gal(E_N/K)$ on $E_N = F^N$. (Aquest isomorfisme és cert pel lema 3.2.3).
I identifiquem τN amb $\tau \restriction_{E_N}$ en G/N.
Amb aquesta identificació per $\rho \in P$, $\pi_N(\rho)$ és un automorfisme en E_N. Notem que per a $\tau \in G$ tenim que $\pi_N(f(\tau)) = \tau \restriction_{E_N}$.
$G \xrightarrow{f} P \xrightarrow{\pi_N} G/N \cong Gal(E_N/K)$ via
$\sigma \longmapsto \sigma N \longmapsto \sigma \restriction_{E_N}$
Escrivim:

$C = \{\gamma \in P : \forall N, M \in \mathcal{E}\ \pi_N(\gamma) \restriction_{E_N \cap E_M} = \pi_M(\gamma) \restriction_{E_N \cap E_M}\}$.
Veiem que $C = imf$
Clarament, $C \supseteq imf$, perquè $\pi_N(f(\tau)) \restriction_{E_N} = \tau_{E_N}$ per $\tau \in G$.
Veiem, $C \subseteq imf$. Sigui $\gamma \in C$. Definim $\tau : F \longrightarrow F$ de la manera següent: per $a \in F$, agafem $E_N \in \mathcal{I}$ tal que $a \in E_N$ (es pot fer pel lema 3.2.2) i definim $\tau(a) := \pi_N(\gamma)(a)$.
La condició $\gamma \in C$, demostra que τ està ben definida (independent del E_N que agafem i τ_N).
Fàcilment τ és homorfisme d'anells, si $a, b \in F$ sigui $E_N \in \mathcal{I}$ amb $a, b \in E_N$. Llavors $\tau \restriction_{E_N} = \tau_N(\gamma)$ és un homomorfisme d'anells.
Aleshores $\tau(a+b) = \tau(a) + \tau(b)$ i $\tau(ab) = \tau(a)\tau(b)$. d'aquí, τ és morfisme de cossos.
A més, τ és una bijecció perquè F/K normal i pel lema 3.2.1, i és clar que τ fixa K. Llavors, $\tau \in G$. Ara, com que $\tau_{E_N} = \pi_N(\gamma)$, veiem que $f(\tau) = \gamma$, i llavors $C \subseteq imf$.
Per veure que C és tancat en P, agafem qualsevol $\gamma \in P$ amb $\gamma \notin C$. Llavors hi han $N, M \in \mathcal{E}$ amb $\pi_N(\gamma) \restriction_{E_N \cap E_M} \neq \pi_M(\gamma) \restriction_{E_N \cap E_M}$.
Ara, $\pi_N^{-1}(\pi_N(\gamma)) \cap \pi_M^{-1}(\pi_M(\gamma))$ és un obert de P que conté a γ i disjunt amb C, llavors $P - C$ és obert d'on $C = imf$ tancat. □

Definició 3.2.15. *Un grup $\mathcal{G}$ s'anomena profinit si és un grup topològic isomorf al límit projectiu de grups finits G_i amb la topologia discreta que formen un sistema projectiu $\{G_i, \varphi_{ij}\}$ amb φ_{ij} morfismes continus de grups. $\mathcal{G} = (\varprojlim G_i, \varphi_i)$ té estructura de grup on φ_i són morfismes de grups i també d'espai topològic donat per la topologia del límit projectiu.*[2]

Teorema 3.2.16 (Grups de Galois són grups profinits)**.** *Sigui F/K una extensió de cossos Galois. Aleshores, $G = Gal(F/K)$ és un grup profinit i la topologia de Krull és equivalent a la topologia de grup profinit del límit projectiu.*

Demostració. Seguint la prova del teorema 3.2.14 demostrem que
$f : G \longrightarrow \varprojlim_{N \in \mathcal{E}} G/N \subseteq \prod_{N \in \mathcal{E}} G/N$ on f es definida per $f(\sigma) = (\sigma N)_{N \in \mathcal{E}}$
és un homomorfisme i per tant la topologia de Krull és equivalent a la del límit projectiu, ja que és la induïda de la topologia producte $\prod G/N$ amb $/N$ dotats de la topologia discreta.
Clarament, f és morfisme de grups, per tant, dóna un isomorfisme de grups topològics entre $G = Gal(F/K)$ i $\varprojlim_{N \in \mathcal{E}} G/N$ que recordem, és per definició, $\varprojlim Gal(E/K)$ on E/K és una extensió de Galois finita amb $E \subseteq F$. □

[2]Consultar apèndix A.3. per definició i propietats dels espais profinits i A.1. per a límit projectiu.

Teorema 3.2.17. *Sigui H un subgrup de G, i escrivim $H' = Gal(F/F^H)$. Llavors, $H' = \overline{H}$, on $\overline{H}$ és la clausura de H amb la topologia de Krull de G.*

Demostració. És clar que $H \subseteq H'$, veurem que H' és tancat i $H' \subseteq \overline{H}$.
Veiem primer que H' és tancat.
Agafem qualsevol $\sigma \in G - H'$. Llavors, $\exists \alpha \in F^H$ amb $\sigma(\alpha) \neq \alpha$. Agafem $E \in \mathcal{I}$ tal que $\alpha \in E$ i $N = Gal(F/E) \in \mathcal{E}$. Aleshores per a qualsevol $\tau \in N$ $\tau(\alpha) = \alpha$, i $\sigma(\tau(\alpha)) = \sigma(\alpha) \neq \alpha$.
Ara σN és un entorn de σ disjunt amb H'. Això implica que $G - H'$ és obert, i per tant, H' tancat.
Veiem ara $H' \subseteq \overline{H}$. Escrivim $L = F^H$. Sigui $\sigma \in H'$ i $N \in \mathcal{E}$, $E = F^N \in \mathcal{I}$ i $H_0 = \{\omega \restriction_E : \omega \in H\}$ un subgrup del grup finit $Gal(E/K)$.
Com que $F^{H_0} = F^H \cap E = L \cap E$, pel teorema fonamental de Galois per extensions finites, tenim que $H_0 = Gal(E/E \cap L)$.
Com que $\sigma \in H'$ tenim que $\sigma \restriction_L = id$, d'on $\sigma \restriction_E \in H_0$. Aleshores hi ha $\omega \in H$ amb $\omega \restriction_E = \sigma \restriction_E \Rightarrow \sigma^{-1}\omega \in Gal(F/E) = N \Rightarrow \omega \in \sigma N \cap H$.
Això demostra que qualsevol entorn obert σN de $\sigma \in H'$ talla H. Per tant, $\sigma \in \overline{H}$. I així hem demostrat l'inclusió $H' \subseteq \overline{H}$. □

Observació 3.2.18. Una manera per descriure $H' = Gal(F/F^H)$ és $H' = \bigcap_{N \in \mathcal{E}} HN$

Demostració. $\overline{H} = \{\sigma \in G \mid \forall N \in \mathcal{E}\ \sigma N \cap H \neq \emptyset\}$. Sigui $\sigma \in G$, aleshores $\sigma \in \bigcap_{N \in \mathcal{E}} HN \Leftrightarrow \forall N \in \mathcal{E}\ \sigma \in HN \Leftrightarrow \sigma N \cap H \neq \emptyset$ □

3.3 Correspondencia bijectiva de Galois per a F/K de Galois arbitrària

Teorema 3.3.1. *[Teorema fonamental de la teoria Galois] Sigui F una extensió de Galois sobre K i $G = Gal(F/K)$, amb la topologia de Krull.*
Les aplicacions entre $\mathcal{A}$=\{ L cos $\mid$ $K \subseteq L \subseteq F$\} i
$\widetilde{\mathcal{B}}$=\{H $\mid$ $H \leq G$ on H tancat en G \} donades per:

$$\Psi : \mathcal{A} \longrightarrow \widetilde{\mathcal{B}} \text{ on } \Psi(L) = Gal(F/L)$$
$$\Theta : \widetilde{\mathcal{B}} \longrightarrow \mathcal{A} \text{ via } \Theta(H) = F^H = \{\alpha \in F \mid h(\alpha) = \alpha,\ \forall h \in H\}$$

són bijeccions i si $L_1 \subseteq L_2$, $Gal(F/L_1) = \Psi(L_1) \geq \Psi(L_2) = Gal(F/L_2)$.
A més, en la bijecció anterior $L \longleftrightarrow H$, tenim:
(1) $|G : H| < \infty \Leftrightarrow [L : K] < \infty \Leftrightarrow H$ és obert, i a més $|G : H| = [L : K]$.
(2) H normal en $G \Leftrightarrow L$ és de Galois sobre K.

Quan això succeeix, tenim $Gal(L/K) \cong G/H$, i si agafem G/H amb la topologia quocient, aquest isomorfisme és també homeomorfisme.

Demostració. Sigui L un subcos de F que conté K; llavors F és normal i separable sobre L, i per tant F és de Galois sobre L i tot seguit demostrarem que $L = F^{Gal(F/L)}$.
És clar que $L \subseteq F^{Gal(F/L)}$. Veiem que $L \supseteq F^{Gal(F/L)}$.
Com en la demostració del lema 3.2.2 triem $\alpha \in F^{Gal(F/L)} - L$ i podem contruir $\sigma : L(\alpha) \longrightarrow F$ tal que envia α a una arrel de $Irr(\alpha, L)[x]$ diferent de α, amb $\sigma \restriction_L = id$. Pel lema 3.2.1 podem extendre σ a un automorfisme de F, τ, de manera que $\tau \restriction_{L(\alpha)} = \sigma$. Aleshores, $\tau \in Gal(F/L)$ però $\tau(\alpha) \neq \alpha$, això no pot ser, ja que $\alpha \in F^{Gal(F/L)}$ i $\tau \in Gal(F/L)$ en contradicció.
Si H és un subgrup de G, pel teorema 3.2.17 tenim:

$$H = Gal(F/F^H) \Leftrightarrow Htancat$$

.
Per tant, les dues aplicacions $L \longrightarrow Gal(F/L)$ i $H \longrightarrow F^H$ donen la correspondència bijectiva entre cossos intermedis entre F i K i els subgrups tancats de G.
Anem ara a demostrar (1).
Demostrarem primer que $|G : H| < \infty \Rightarrow H$ obert. Sigui L un cos entre F i K i $H = Gal(F/L)$. Supossem que $|G : H| < \infty$. Aleshores, $G - H$ és unió finita de cosets de H (certs σH), cadascun d'ells tancats, ja que H és tancat. Per rant, $G - H$ és tancat i per tant H és obert.
Veiem ara H obert $\Rightarrow |G : H| < \infty$.
Si H és obert, conté algun entorn bàsic de l'identitat, és a dir, $N \subseteq H$ per algun $N \in \mathcal{E}$. Tenim $E = F^N$ on $L \subseteq E$, és a dir, $[L : K] < \infty$.
Per acabar, si $[L : K] < \infty$, escollim $E \in \mathcal{I}$ amb $L \subseteq E$ (això es pot fer pel 3.2.2). Agafem $N = Gal(F/E)$. Ara, $N \trianglelefteq H$ perquè $L \subseteq E$ i és clar, $|G : H| < |G : N| < \infty$.

Veiem $|G : H| = [L : K]$. Pel lema 3.2.3, tenim $G/N \cong Gal(E/K)$ via $\sigma N \longrightarrow \sigma \restriction_E$ (que envia H/N a $\{\omega \restriction_E : \omega \in H\}$ un subgrup de $Gal(E/K)$ amb cos fix $L \cap E = L$). Pel teorema 2.2.2, l'ordre del grup és $[E : L]$. Aleshores,
$|G : H| = |G/N : H/N| = \frac{|G/N|}{|H/N|} = \frac{[E:K]}{[E:L]} = [L : K]$

Anem ara a demostrar (2) i la part final del teorema.
Per veure l'afirmació sobre normalitat, agafem $H = Gal(F/L)$ en la correspondència bijectiva. Supossem que H és normal, sigui $a \in L$, i denotem

$f(x) = Irr(a, K)[x]$.
Si $b \in F$ és arrel de f, pel 3.2.1, existeix $\sigma \in G$ amb $\sigma(a) = b$. Per veure que $b \in L$, agafem $\tau \in H$. Llavors $\tau(b) = \sigma^{-1}(\sigma\tau\sigma^{-1}(a)) = \sigma^{-1}(a) = b$, perquè $\sigma\tau\sigma^{-1} \in H$, per ser H normal en G. Així, $b \in F^H = L$. Llavors f descomposa sobre L i això demostra que L és normal sobre K, i separable pel fet de que F/K ho és. I per tant, tenim que L és de Galois sobre K.
En l'altre sentit, si L és de Galois sobre K, pel lema 3.2.2,
$\theta : G \longrightarrow Gal(L/K)$ que envia σ a $\sigma\,{}_{|L}$, està ben definit i és homomorfisme de grups.
El nucli de θ és $Gal(F/L) = H$, llavors H és normal en G i θ exhaustiva. Pel primer teorema d'isomorfia, $G/H = Gal(L/K)$.

Per completar la prova falta demostrar que l'aplicació natural
$\nu : G/H \longrightarrow Gal(L/K)$ induïda per θ és homeomorfisme quan H és normal en G.
Notem que un obert bàsic de $Gal(L/K)$ és de la forma $\omega Gal(L/E)$ per algun E de Galois sobre K contingut en L tal que E/K és finit i Galois amb $\omega \in Gal(L/K)$. Possem $N = Gal(F/E) \in \mathcal{E}$. Llavors, $\theta^{-1}(Gal(L/E)) = N$. Així $\theta^{-1}(\omega Gal(L/E)) = \tau N$ per algun $\tau \in G$ amb $\tau\,{}_{|L} = \omega$. I aquesta preimatge és oberta en G. D'on θ és continua.
A més, l'imatge d'un compacte per una aplicació continua segueix essent compacte, i qualsevol subconjunt d'un espai Hausdorff és tancat.
Com que G és compacte i $Gal(L/K)$ Hausdorff, θ envia tancats a tancats; és a dir, és una aplicació tancada.
Per acabar, l'aplicació $\nu : G/H \longrightarrow Gal(L/K)$ induïda per θ és també continua i tancada amb la topologia quocient, i per tant homeomorfisme.
□

3.4 Grups profinits com a grups de Galois

Veiem que tot grup profinit és grup de Galois per a certa extensió de cossos.

Teorema 3.4.1 (Waterhouse)**.** *Sigui* $(\mathcal{G} = \varprojlim G_i, \varphi_i)$ *un grup profinit amb* G_i *grups finits i* $\varphi_i : \mathcal{G} \longrightarrow G_i$ *morfismes de grups. Aleshores, existeix una extensió de cossos* F/K *de Galois, tal que* $(\mathcal{G} = \varprojlim G_i, \varphi_i) \cong Gal(F/K) \cong (\varprojlim_{N \in \mathcal{E}} Gal(F/K)/N, proj : Gal(F/K) \longrightarrow N$ *amb* $N = Gal(F/E)$ *on* E/K *finita* $E \subseteq F$.

Demostració. Sigui k un cos qualsevol. Denotem per T a la unió disjunta de tots els $\mathcal{G}/M$ on els M recorre tots els subgrups normals i oberts de $\mathcal{G}$,

$T = \bigcup_{M \trianglelefteq \mathcal{G}, Mobert} \mathcal{G}/M$ on la unió és disjunta. Recordem que M és obert en $\mathcal{G}$ i com $\mathcal{G}$ és compacte $|\mathcal{G} : M|$ té index finit i $\mathcal{G}/M$ és un grup finit i en particular, M és tancat.
Pensem els elements de T com a indeterminades i considerem $F = k(T)$ el cos de fraccions de l'anell de polinomis en les indeterminades donades pels elements del conjunt T.
El grup $\mathcal{G}$ actua sobre aquestes indeterminades de forma natural:
si $\gamma \in \mathcal{G}$ i $\overline{\gamma'} \in \mathcal{G}/M$ per cert M,
tenim $\overline{\gamma\gamma'} \in \mathcal{G}/M$ on $\overline{\gamma\gamma'} \neq \overline{\gamma'}$ si $\gamma \notin M$.
Així $\gamma \in Aut_K F$ i tenim $\mathcal{G} \leq Aut_k F$.
Escrivim $K := F^{\mathcal{G}}$ i afirmem F/K és Galois amb $Gal(F/K) \cong \mathcal{G}$.
Anem-ho a demostrar: Per $a \in F$, considerem

$$G_a = \{\gamma \in \mathcal{G} | \gamma(a) = a\} \leq \mathcal{G}.$$

Com els $a \in F$ s'escriu com $a = \frac{l(T)}{m(T)}$ on $l(T) = l(t_{\alpha_1}, ..., t_{\alpha_n})$ i $m(T) = m(t_{\beta_1}, ..., t_{\beta_s})$ per certes indetermiades del conjunt T, tenim que a té una expressió involucrant un número finit d'indeterminades

$$\{t_{\gamma_1}, ..., t_{\gamma_r}\} = \{t_{\alpha_1}, ..., t_{\alpha_n}, t_{\beta_1}, ..., t_{\beta_s}\},$$

que corresponen a r elements de $T = \bigcup_{M \trianglelefteq \mathcal{G}, Mobert} \mathcal{G}/M$.
Pensem t_{γ_i} element de $\mathcal{G}/M_{\gamma_i}$, $i = 1, ..., r$ on M_{γ_i} no són necessariament diferents. Llavors, és clar que M_{γ_i} fixa t_{γ_i} per aquest i concret.
D'aquí, $\widetilde{M} = \cap_{i=1}^{k} M_{\gamma_i}$ fixa t_{γ_i} $\forall i = 1, ..., r$, Sper tant, $G_a \supseteq \widetilde{M}$.
Fixem-nos que G_a és obert en $\mathcal{G}$ i té index finit:
index finit és clar, perquè M_{γ_i} són oberts i tancats, pel fet què $\cap M_{\gamma_i}$ és obert i tancat (per ser intersecció finita). Per tant $\cap M_{\gamma_i}$ té index finit en $\mathcal{G}$, i d'aqui G_a té index finit en $\mathcal{G}$.
Per demostrar G_a obert, $\widetilde{M} \leq G_a$, on $\widetilde{M}$ obert.
Per a cada $\sigma \in G_a$ $\sigma\widetilde{M}$ és un entorn obert de σ ja que $\mathcal{G}$ és un grup topològic, i per tant G_a és obert.
D'aquí, $\Omega = \{g(a) \mid g \in \mathcal{G}\}$, l'orbita de a per l'acció de $\mathcal{G}$ és un conjunt finit $\Omega = \{a, a_2, ..., a_l\}$.
Considerem el polinomi

$$f(x) = \prod_{i=1}^{l} (x - a_i)$$

on $\mathcal{G}$ actua sobre els coeficients del polinomi via $(\sigma f(x)) = \prod_{i=1}^{l}(x - \sigma(a_i)) = f(x)$, $\forall \sigma \in \mathcal{G}$, d'on $f(x) \in K[x]$, demostrant que a és algebraic sobre K.
És clar que a és separable sobre K, ja que $Irr(a, K)[x]|f(x)$ i totes les arrels de f són diferents.
També F/K és normal ja que si $a \in F$ amb l'argument d'abans,
$Irr(a, K)[x]|f(x)$, i totes les arrels de f són a F.
Per tant, F/K Galois. Demostrem finalment que $Gal(F/K) \cong \mathcal{G}$.
Sigui H el grup de Galois de F/K; llavors per construcció, $\mathcal{G}$ ha de ser un subgrup de H. Per veure que són el mateix, considerem l'inclusió $\mathcal{G} \hookrightarrow H$ i veiem primer que és continua i per la correspondència bijectiba de Galois podem concloure.
Sabem que a $H = Gal(F/K) \cap \sigma U$ on U obert és una base d'entorns, on $U = Gal(F/E)$ amb E/K de Galois i finit. Com estem en grups topològics, és suficient demostrar-ho per U.
Si $U \leq H$, sigui F^U el subcos dels elements fixats per U; llavors pel teorema fonamental de Galois 3.3.1 F^U/K és una extensió finita de Galois.
Possem $F^N = K(a'_1, ..., a'_r)$ per alguns $a'_1, ..., a'_r \in F$.
Llavors, $\mathcal{G} \cap U \supseteq \bigcap_{i=1}^{s} G_{a'_i}$. Aleshores $\mathcal{G} \cap U$ i com $\bigcap_{i=1}^{s} G_{a'_i}$ és obert, d'aquí per $\tau \in \mathcal{G} \cap U$, $\tau(\bigcap_{i=1}^{s} G_{a'_i}) \subseteq \mathcal{G} \cap U$ provant que $\mathcal{G} \cap U$ és un obert de $\mathcal{G}$.
Aleshores, l'inclusió $\varphi : \mathcal{G} \hookrightarrow H$ continua. Per tant, $\varphi^{-1}(H) = \mathcal{G}$ d'on $\mathcal{G}$ és obert i tancat, en particular $\mathcal{G}$ i H són tancats de $Gal(F/K)$ amb el mateix cos fix K, i per la correspondencia bijectiva de Galois 3.3.1 $\mathcal{G} = H$. □

3.5 Exemples. Extensions no finites, topologia del grup profinit i correspondencia de Galois.

Primer de tot enunciem i provem alguns lemes que usem en els exemples:

Definició 3.5.1. *Sigui $\mathbb{Z}_p$, l'anell dels nombres p-àdics, i escrivim $h \in \mathbb{Z}_p$ en base p $h = a_0 + a_1 p + a_2 p^2 + ...$ amb $0 \leq a_i \leq p-1$. La valoració p-àdica de h es defineix com $v_p(h) = n$ on $n = min\{k \in \mathbb{N} \mid a_k \neq 0\}$.*
Aquesta valoració indueïx una norma i per tant una topologia anaítica definida per $|h|_p = p^{-v_p(h)}$. A més la topologia induïda per aquesta norma, i la donada pel límit projectiu (en A.1) són equivalents, i els entorns oberts són de la forma $p^n\mathbb{Z}_p$. A més, l'anell $\mathbb{Z}_p$ és la completació per $|\ |_p$ de $\mathbb{Z}$.

Lema 3.5.2. *Si $h \neq 0$ amb $h \in \mathbb{Z}_p$, llavors $\overline{< h >} = p^n\mathbb{Z}_p$ on $v_p(h) = n$.*

Demostració. Fixat $h = p^n(b_0 + b_1p + ...) \in \mathbb{Z}_p$ amb $b_0 \neq 0$, $0 \leq b_i \leq p-1$, tenim $< h >= \{mh \mid m \in \mathbb{Z}\}$.
Per construcció, $\overline{< h >}$ seràan successions de Cauchy $\{m_ih\}_{i\in\mathbb{N}}$ amb $m_i \in \mathbb{Z}$ i $\mid m_ih - m_jh \mid = \mid m_i - m_j \mid \mid h \mid \longrightarrow 0$, tenim $m_i \longrightarrow y \in \mathbb{Z}_p$, i per tant

$$\overline{< h >} \subseteq \{hy \mid y \in \mathbb{Z}_p\}.$$

Inversament, donat $hy = h(y_0 + y_1p + ...)$, $0 \leq y_i \leq p-1$ considerem la succession de Cauchy $n_jh := (y_0 + y_1p + ... + y_jp^j)h$ i obtenim

$$yh = \{n_jh\}_j \in \overline{< h >}.$$

És fàcil veure que per $\alpha = b_0 + b_1p + ...$ amb $b_0 \neq 0$ $\exists w \in \mathbb{Z}_p$ on $w\alpha = 1$ i per tant, $\overline{< h >} = p^n\mathbb{Z}_p$. □

Corol·lari 3.5.3. *Tot subgrup H de $\mathbb{Z}_p$ amb $H \neq \{0\}$, si H és tancat, llavors $|\mathbb{Z}_p : H| < \infty$.*

Definició 3.5.4. *Fixat $n \in N$ el polinomi ciclotòmic d'ordre n és:*
$\Phi_n(x) = \prod_{i=1,(i,n)=1}^{n-1} (x - \xi^i)$ *on $\xi = \mathrm{e}^{2\pi i/n} \in \mathbb{C}$ és una arrel n-èssima de la unitat.*
Es demostra que $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
I també que $Irr(\mathrm{e}^{2\pi i/n}, \mathbb{Q})[x] = \Phi_n(x)$.
A més el grau del polinomi $\Phi_n(x)$ és $\varphi(n) = (p_1 - 1)p_1^{k_1-1} \cdots (p_s - 1)p_s^{k_s-1}$ si $n = p_1^{k_1} \cdots p_s^{k_s}$ és la factorització de n com a producte de primers diferents entre ells.

Lema 3.5.5. *Sigui K un cos i S un conjunt on $\beta \in S$, es té β é algebraic sobre K. Aleshores l'extensió $K(S)/K$ és algebraica.*

Demostració. Sigui $\delta \in K[S]$, aleshores,
$\delta = \sum_{j=1}^{m} a_j\beta_j$ on $a_j \in K$ i $\beta_j \in S$.
$\delta \in K(\beta_1, ..., \beta_m)$ i $K(\beta_1, ..., \beta_m)/K$ és finit i algebraic (perquè cada β_i ho és).
Pensem ara $\delta \in K(S)$.
$\delta = \frac{\sum_{j=1}^{m} a_j\beta_j}{\sum_{k=1}^{r} b_ks'_k}$ on $\alpha = \sum_{j=1}^{m} a_j\beta_j$ i $\beta = \sum_{k=1}^{r} b_ks'_k \neq 0$ amb $\alpha \in K(\beta_1, ..., \beta_m)$
i $\beta \in K(s'_1, ..., s'_r)$.
Aleshores, $\frac{\alpha}{\beta} \in K(\beta_1, ..., \beta_m, \beta'_1, ..., \beta'_r)$ que és una extensió finita i algebraica sobre K i per tant $\delta = \frac{\alpha}{\beta}$ algebraic. □

3.5.1 Exemple 1: $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$ amb p primer fixat

Ja hem vist en la secció 3.1. $Gal(\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p)$ isomorf a $\mathbb{Z}_p$. Recordem
$\varphi_i : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$ les projeccions naturals, pel apartat (b) del corol·lari A.2.9 del apèndix, $\overline{\mathbb{Z}} = \varprojlim \varphi_i(\mathbb{Z}) = \varprojlim Z/p^i\mathbb{Z} = \mathbb{Z}_p$, tenim que $\mathbb{Z}$ és dens a $\mathbb{Z}_p$, i per tant no hi ha cap subgrup tancat entre $\mathbb{Z}$ i $\mathbb{Z}_p$.
A més pel corol·lari 3.5.3 no hi ha subgrups tancats d'index no finit a $\mathbb{Z}_p$, i llavors l'única extensió de cossos de Galois no finita és la de $\mathbb{F}_{p^{p^\infty}}/\mathbb{F}_p$. Totes les altres, són finites sobre $\mathbb{F}_p$, justament les que corresponen als subgrups $\mathbb{Z}/(p^j)$, que són $\mathbb{F}_{p^{p^j}}/\mathbb{F}_p$ corresponents a cossos finits.

3.5.2 Exemple 2: $\mathbb{Q}(e^{2\pi i/p^\infty})/\mathbb{Q}$ amb p primer fix

Considerem $F = \mathbb{Q}(\{e^{2\pi i/p^n} \mid n \in \mathbb{N}\})$ el cos generat sobre $\mathbb{Q}$ per les arrels p-èssimes de l'unitat en $\mathbb{C}$. Evident que això F/K no finita.
A més, com que F és el cos de descomposició sobre $\mathbb{Q}$ de la familia de polinomis $\{x^{p^n} - 1 \mid n \in \mathbb{N}\}$, és normal i com estem a característica zero tenim que $F/\mathbb{Q}$ és de Galois.

Teorema 3.5.6. *El grup de Galois de l'extensió de cossos $F/\mathbb{Q}$ és isomorf a $\mathbb{Z}_p^*$, els elements invertibles de $\mathbb{Z}_p$ amb el producte i es veu $\mathbb{Z}_p^* = (Z/(p))^* \times (\mathbb{Z}_p, +)$, on la topologia a la primera component és la discreta i a la segona la del anell dels p-àdics.*

Demostració. Només demostrarem que $Gal(F/\mathbb{Q}) \cong \mathbb{Z}_p^*$. Per a $j \in \mathbb{N}$, tenim $\varphi : Gal(\mathbb{Q}(e^{2\pi i/p^j})/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p^j)^*$ tal que, si $\sigma(e^{2\pi i/p^j}) = e^{2\pi ia/p^j}$ on $(a, p^j) = 1$, ja que σ envia arrels primitives p^j-èssimes a una altre que també ho sigui. Per tant definim φ via $\sigma \mapsto a$, que es pot demostrar que és un isomorfisme de grups.
Veiem que el següent diagrama commuta:

$$\begin{array}{ccc} Gal(\mathbb{Q}(e^{2\pi i/p^j})/\mathbb{Q}) & \xrightarrow{\varphi_j} & \mathbb{Z}/(p^j)^* \\ {\scriptstyle \text{restricció}}\downarrow & & \downarrow{\scriptstyle \text{projecció}} \\ Gal(\mathbb{Q}(e^{2\pi i/p^{j-1}})/\mathbb{Q}) & \xrightarrow{\varphi_{j-1}} & \mathbb{Z}/(p^{j-1})^* \end{array}$$

Si $\sigma \in Gal(\mathbb{Q}(e^{2\pi i/p^j})/\mathbb{Q})$ $\sigma(e^{2\pi i/p^j}) = e^{2\pi ia/p^j}$,
$\sigma\,{}_{|_{\mathbb{Q}(e^{2\pi i/p^{j-1}})}}(e^{2\pi ip/p^j}) = e^{2\pi ipa/p^j} = e^{2\pi ia/p^{j-1}}$ on a el podem pensar com la classe de a en $(\mathbb{Z}/p^{j-1})^*$. Per tant commuta.
D'aquí, $Gal(\mathbb{Q}(e^{2\pi i/p^\infty})/\mathbb{Q}) = \varprojlim Gal(\mathbb{Q}(e^{2\pi i/p^j})/\mathbb{Q}) \cong \varprojlim(\mathbb{Z}/p^n)^* = \mathbb{Z}_p^*$. □

En aquet cas, com que l'únic subgrup d'index no finit de $\mathbb{Z}_p$ és el (0), els sugbrups d'index no finit seràn els de la forma $H \times (0)$ amb $H \leq (\mathbb{Z}/(p))^*$, ja que en $(\mathbb{Z}/(p))^*$ tenim la topologia discreta i per tant tot subgrup serà tancat.
Sigui, per exemple, $H = \{1, -1\}$ amb $p \geq 3$. El sugbrup d'automorfismes que li correspon a H és el de la identitat i la conjugació complexa, que envia $e^{2\pi i/p^j}$ a $e^{-2\pi i/p^j}$. Aleshores $\mathbb{Q}(e^{2\pi i/p^j})^H = \mathbb{Q}(e^{2\pi i/p^j} + e^{-2\pi i/p^j}) = \mathbb{Q}(cos(2\pi i/p^j))$. Per tant obtenim l'extensió de cossos no finita:
$\mathbb{Q} \subseteq \cdots \mathbb{Q}(cos(2\pi i/p^j)) \subseteq \mathbb{Q}(cos(2\pi i/p^{j+1})) \subseteq \cdots \mathbb{Q}(cos(2\pi i/p^\infty))$.

Si triem $H = (\mathbb{Z}/p)^*$, $\mathbb{Q}(e^{2\pi i/p^\infty})^H$ es denota per $\mathbb{Q}_{p,cyc}$ i s'anomena l'extensió p-ciclotòmica de $\mathbb{Q}$, és una extensio de Galois sobre $\mathbb{Q}$ amb grup de Galois isomorf a $\mathbb{Z}_p$.

3.5.3 Exemple 3: $\mathbb{Q}(\{\sqrt{p} \mid p \in \mathbb{N} \textbf{ i } p \textbf{ primer}\})/\mathbb{Q}$

Lema 3.5.7. *Siguin $p_1, ..., p_n$ un número finit de nombres primers diferents. Llavors $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})/\mathbb{Q}$ és de Galois amb $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$ i amb grup de Galois isomorf a $\prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$.*

Demostració. Farem la demostració per inducció sobre n.
Per a $n = 1$ és clar. Supossem cert per a n i veiem-ho per a $n + 1$.
Per hipòtesi d'inducció tenim que $L = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})/\mathbb{Q}$ de Galois amb $[L : \mathbb{Q}] = 2^n$. Sigui p_{n+1} un primer diferent de $p_1, ..., p_n$ i considerem l'extensió $L(\sqrt{p_{n+1}})/L$. Sabem que $[L(\sqrt{p_{n+1}}) : L]$ ha de ser 1 o 2.
Si fos 1, $\mathbb{Q}(\sqrt{p_{n+1}})$ és cos intermedi de $L/\mathbb{Q}$.
Tenim que $Gal(L/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$, via $\sigma \mapsto (\sigma_1, ..., \sigma_n)$ on
$\sigma_i = 0$ si $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ i $\sigma_i = 1$ si $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$.
Per altre banda, tenim, $\mathbb{Q}(\sqrt{p_1}), \mathbb{Q}(\sqrt{p_1 p_2}), ..., \mathbb{Q}(\sqrt{p_1 p_2 ... p_n})$,
$\mathbb{Q}(\sqrt{p_2}), ..., \mathbb{Q}(\sqrt{p_2 ... p_n}), ..., \mathbb{Q}(\sqrt{p_n})$ són $2^n - 1$ cossos diferents d'index dos sobre $\mathbb{Q}$ que corresponen a
$(1, 0, ..., 0) \in \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Q}(\sqrt{p_1})$
$(1, 1, 0, ..., 0) \longrightarrow \mathbb{Q}(\sqrt{p_1 p_2})$
...
Com que $|\prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} - \{id\}| = 2^n - 1$, si $\mathbb{Q}(\sqrt{p_{n+1}}) \subseteq L$ aleshores $\mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{p_{i_1} ... p_{i_s}})$ per certs $p_{i_j} \in \{p_1, ..., p_n\}$.
Com que p_{n+1} és primer i diferent de tots els demés, $mcd(p_{i_1} ... p_{i_s}, p_{n+1}) = 1$.

Si $\mathbb{Q}(\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{p_{i_1}...p_{i_s}})$, $\sqrt{p_{n+1}} = a + b\sqrt{p_{i_1}...p_{i_s}}$ on $a, b \in \mathbb{Q}$.
Per tant, $p_{n+1} = a^2 + b^2 p_{i_1}...p_{i_s} + 2ab\sqrt{p_{i_1}...p_{i_s}}$ on $p_{n+1} \in \mathbb{Z}$, $a^2 + b^2 p_{i_1}...p_{i_s} \in \mathbb{Q}$ i $2ab\sqrt{p_{i_1}...p_{i_s}} \notin \mathbb{Q}$. Per tant $ab = 0$.
Si $b = 0$, $a = \sqrt{p_{n+1}}$, contradicció.
Si $a = 0$, $\sqrt{p_{n+1}} = b\sqrt{p_{i_1}...p_{i_s}} \Rightarrow \sqrt{\frac{p_{n+1}}{p_{i_1}...p_{i_s}}} = b \in \mathbb{Q}$ no pot ser.
Per tant $[L(\sqrt{p_{n+1}}) : L] = 2$. I definim $\sigma \in Gal(L(\sqrt{p_{n+1}}/\mathbb{Q})$ via $\sigma(\sqrt{p_{n+1}}) = \pm\sqrt{p_{n+1}}$ i $\sigma \restriction_L = \tau$ on $\tau \in Gal(L/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$.

Es pot demostrar fàcilment que $Gal(L(\sqrt{p_{n+1}})/\mathbb{Q}) \cong \prod_{i=1}^{n+1} \mathbb{Z}/2\mathbb{Z}$. □

Lema 3.5.8. *$F = \mathbb{Q}(\{\sqrt{p} \mid p \in \mathbb{N}\})$, $F/\mathbb{Q}$ és una extensió de Galois no finita.*

Demostració. • $F/\mathbb{Q}$ algebraica:
Com que $S = \{\sqrt{p} \mid p \in \mathbb{N}\}$ és un conjunt de elements algebraics sobre $\mathbb{Q}$ pel lema 3.5.5 $F = \mathbb{Q}(S)/\mathbb{Q}$ és algebraica.
• $F/\mathbb{Q}$ normal i separable:
Si $\alpha \in F$, tenim que $\alpha \in \mathbb{Q}(\sqrt{p_{i_1}}, ..., \sqrt{p_{i_s}})$ per certs $p_{i_j} \in S$.
Aleshores, $Irr(\alpha, \mathbb{Q})[x]$ desconpon en $\mathbb{Q}(\sqrt{p_{i_1}}, ..., \sqrt{p_{i_s}})$ del fet $\mathbb{Q}(\sqrt{p_{i_1}}, ..., \sqrt{p_{i_s}})/\mathbb{Q}$ és de Galois (lema 3.5.7).
En particular, $Irr(\alpha, \mathbb{Q})[x]$ trenca en producte de polinomis de grau 1 en F sense arrels repetides.
És clar que l'extensió és no finita perquè $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$ i aquesta n la podem fer tant gran com volguem, per tant això tendeix a infinit. □

Calculem $Gal(F/\mathbb{Q})$ i la seva topologia de Krull.
Primer de tot ordenem els elements $\sqrt{p_1}, \sqrt{p_2}, ...$ de manera que $p_1 < p_2 < p_3 < ....$ Aleshores,
$Gal(F/\mathbb{Q}) \supseteq Gal(F/\mathbb{Q}(\sqrt{p_1})) \supseteq Gal(F/\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})) \supseteq ....$
Denotem per $L_i = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_i})$.
Sabem que $Gal(F/\mathbb{Q}) = \varprojlim_{[K_i:\mathbb{Q}]} Gal(K_i/\mathbb{Q}) = \varprojlim Gal(L_i/\mathbb{Q})$[3], ja que $Gal(L_i/\mathbb{Q})$ són els entorns base de la topologia (considerant cada $Gal(K_i/\mathbb{Q})$ amb la topologia discreta); on els morfismes del sistema projectiu són:

$$\begin{aligned} \varphi_{i,i-1} : Gal(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_i})/\mathbb{Q}) &\longrightarrow Gal(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{i-1}})/\mathbb{Q}) \\ \sigma &\longmapsto \sigma \restriction_{\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_{i-1}})} \end{aligned}$$

[3]hi ha igualtat ja que els $Gal(F/L_i)$ formen un sistema cofinal pels $\mathcal{E}$ i aplicant el lema A.2.12 del apèndix obtenim la igualtat

Notem que l'isomorfisme definit a la demostració del lema 3.5.7:
$Gal(L_i/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$, via $\sigma \mapsto (\sigma_1, ..., \sigma_n)$ on
$\sigma_i = 0$ si $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ i $\sigma_i = 1$ si $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$,
és compatible amb els morfismes $\varphi_{i,i-1}$ que acabem de definir.

Per tant, tenim que $\varprojlim Gal(L_i/\mathbb{Q}) \cong \varprojlim_i \prod_{j=1}^{i} \mathbb{Z}/2\mathbb{Z}$ com a grups topològics, on considerem la topologia discreta en cada $\prod_{j=1}^{i} \mathbb{Z}/2\mathbb{Z}$ i els morfismes de projecció naturals
$\widetilde{\varphi}_{i,i-1} : \prod_{j=1}^{i} \mathbb{Z}/2\mathbb{Z} \longrightarrow \prod_{j=1}^{i-1} \mathbb{Z}/2\mathbb{Z}$ via $(a_1, ..., a_{i-1}, a_i) \mapsto (a_1, ..., a_{i-1})$.

Lema 3.5.9. *Tenim que* $\varprojlim_n \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ *amb la topologia producte on* $\mathbb{Z}/2\mathbb{Z}$ *dotats de la topologia discreta.*

Demostració. Veiem que $(\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}, +)$ compleix la propietat universal del límit projectiu.
Sigui $\{G, \varphi_n\}$ un sistema compatible, és a dir, que el següent diagrama commuta:

$$\begin{array}{ccc} G & \xrightarrow{\varphi_n} & \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} \\ & {\scriptstyle \varphi_{n-1}} \searrow \quad \swarrow {\scriptstyle \pi_{n,n-1}} & \\ & \prod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z} & \end{array}$$

on $\pi_{n,n-1}$ són les projeccions naturals.
Si $\varphi_n(g) = (\beta_1, ..., \beta_n)$ per $g \in G$, definim
$\psi : G \longrightarrow \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ via

$\psi(g) = (\psi_l(g))_{l \in I}$ on $\psi_l(g)$ és la component l-éssima de $\varphi_l(g)$ en $\prod_{i=1}^{l} \mathbb{Z}/2\mathbb{Z}$.
Per construcció,

$$\begin{array}{ccc} G & \xrightarrow{\varphi_n} & \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} \\ & {\scriptstyle \psi} \searrow \quad \nearrow {\scriptstyle \pi_{\infty,n}} & \\ & \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} & \end{array}$$

commuta, és a dir, $\pi_{\infty,n} \circ \psi = \varphi_n$ i a més ψ és morfisme de grups.
Veiem ara que ψ és continua:
Tenim $\pi_l : \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ la projecció en lacomponent l. Els entorns oberts en la topologia del producte de $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ són de la forma $\pi_i^{-1}(U)$ on U és un obert de $\mathbb{Z}/2\mathbb{Z}$.
Per tant és suficient veure que $\psi^{-1}(\pi_l^{-1}(U))$ és obert amb U obert.
Per definició, $\psi^{-1}(\pi_l^{-1}(U)) = \bigcup_{n \geq l} \varphi_n^{-1}(\{(\alpha_1, ..., \alpha_n) \in \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} | \alpha_l \in U\})$.
Com que $\{(\alpha_1, ..., \alpha_n) \in \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z} | \alpha_l \in U\}$ és obert a $\prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$ i φ_n continua, obtenint el resultat.

□

Veiem ara alguns cossos intermedis de $F/\mathbb{Q}$ tals que l'extensió sobre $\mathbb{Q}$ sigui no finita.
$G = \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ amb la topologia del producte on $\mathbb{Z}/2\mathbb{Z}$ amb la topologia discreta.

• Si H és d'index finit i tancat en G, per la correspondencia bijectiva obtenim una extensió $L/\mathbb{Q}$ finita, i aquestes les tenim molt estudiades, per exemple,

$$H = \{0\} \times \{0\} \times \{0\} \times \{0\} \times \prod_{i=5}^{\infty} \mathbb{Z}/2\mathbb{Z} \leq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

amb l'ordre que hem fixat pels primers, $H \leq Gal(F/\mathbb{Q}\{\sqrt{p_i}\} \mid i \geq 5)$ i per tant,
$F^H = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$.

• Pensem $H \leq G$ d'index no finit i tancat amb H finit, tenim molts exemples:

$$H = \prod_{i=1}^{3} \mathbb{Z}/2\mathbb{Z} \times \prod_{i \geq 4} \{0\} \leq G$$

$H = (\bigcap_{j=4}^{\infty} \pi_j^{-1}(0))$ tancat de G i
$F^H = \mathbb{Q}(\{\sqrt{p_i}\}, i \geq 4)$.

• Pensem $H \leq G$ d'index no finit, però H no finit, també tenim molts exemples:

$$H = \mathbb{Z}/2\mathbb{Z} \times \{0\} \times \mathbb{Z}/2\mathbb{Z} \times \{0\} \times ...$$

H és tancat perquè, $H = \bigcap_{j=1}^{\infty} \pi_{2j}^{-1}(0)$ i H no finit. Tenim que, $F^H = \mathbb{Q}(\sqrt{p_i} \mid i \text{ parell})$.

3.6 Problema invers de Galois per a grups profinits?

Seguint el cas de grups finits, podem preguntar-nos

Qüestió 3.6.1. *Sigui $\mathcal{G}$ un grup profinit i K un cos, existeix una extensió F/K amb grup de Galois $\mathcal{G}$?*

Pensem-ho tan sols per K amb $[K : \mathbb{Q}] < \infty$. Intentem com al problema invers de Galois preguntarnos primer per a a grups profinits abelians. Tenim el següent resultats de classificació de grups profinits commutatius [11, Theorem 4.3.3, 4.3.5]:

Teorema 3.6.2. *Sigui G un grup abelià profinit i lliure de torsió. Llavors*

$$G \cong \prod_{p} (\prod_{\mathfrak{m}(p)} \mathbb{Z}_p)$$

on p recorre tots els primers i cada $\mathfrak{m}(p)$ és un nombre cardinal.

Per la teoria de classes [10] sobre K obtenim que tan sols grups topològics finit generats poden sortir com a extensions abelianes de K, per tant restringim la pregunta 3.6.1 a grups profinits finit generats.

Teorema 3.6.3. *Sigui G un grup abelià profinit, finit generat i lliure de torsió. Llavors tenim*

$$G \cong (\oplus_p (\oplus_{m(p)} \mathbb{Z}_p))$$

on p varia tots els primers i $m(p)$ és un natural que val zero per gairebé tot p.

Hem vist que donat p primer podem construir l'extensió $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ amb $Gal(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = Gal(\mathbb{Q}_{cyc,p}/\mathbb{Q}) \times \Delta$ on $\Delta \cong (\mathbb{Z}/p)^*$ i $Gal(\mathbb{Q}_{cyc,p}/\mathbb{Q}) \cong \mathbb{Z}_p$, on $\mathbb{Q}_{cyc,p}$ s'anomena l'extensió p- ciclotòmica de $\mathbb{Q}$.

Qüestió 3.6.4. *Donat $G = \mathbb{Z}_p^n$ amb $n \geq 1$ podem construir una extensió de Galois sobre $\mathbb{Q}$ amb grup de Galois $\mathbb{Z}_p^n$?*

La resposta ja sabem que és NO per $n \geq 2$ del teorema de Weber 2.4.4, per tant la pregunta anàloga del problema invers de Galois per a grups profinits finit generats és negativa pels grups abelians.

En aquest camp hi ha la següent conjectura que tan sols escrivim en un cas molt particular:

Conjectura 3.6.5 (Leopoldt)**.** *Fix p un primer i sigui $[K : \mathbb{Q}] < \infty$ amb $K \subseteq \mathbb{R}$. Llavors no existeix cap extensió de cossos Galois L/K on $Gal(L/K) \cong \mathbb{Z}_p^\ell$ amb $\ell \geq 2$*

Observació 3.6.6. *Evidentment podem construir l'extensió per $\ell = 1$ introduint les arrels ζ_{p^n} de la unitat.*
Ferrero i Washington demostren la conjectura quan $K/\mathbb{Q}$ és de Galois amb grup de Galois $Gal(K/\mathbb{Q})$ un grup abelià.

Apèndix A

Límits projectius

A la primer secció d'aquest appendix, es dóna la definició de límit projectiu, tant com a conjunts com a espais topològics. S'observa que si els objectes en el límit projectiu són grups, anells o R-mòduls, llavors el límit es dota d'aquesta estructura (impossant que els morfismes mantenen l'estructura). A més, com a exemple introduïm l'anell dels nombres p-àdics.
A la segona part, passem a estudiar propietats topològiques dels espais projectius en general, que en serviràn després a la tercera part per a donar una caracterització dels espais profinits.

A.1 Definició i exemples

Definició A.1.1. *Sigui I un conjunt. Es diu que I és un conjunt dirigit parcialment ordenat si existeix una relació $\leq$ en I tal que:*
(i) $i \leq i, \forall i \in I$
(ii) $i \leq j, j \leq i \Rightarrow i = j$
(iii) $i \leq j, j \leq k \Rightarrow i \leq k$
(iv) $i, j \in I \Rightarrow \exists k \in I$ *tal que* $i, j \leq k$

Definició A.1.2. *Un sistema projectiu de conjunts (espais topològics) indexada per I, és una col·lecció de conjunts (espais topològics) X_i, $i \in I$, i de aplicacions $\varphi_{ij} : X_i \longrightarrow X_j$ (aplicacions continues) que existeixen sempre que $i \leq j$, complint que $\varphi_{kj} \circ \varphi_{ij} = \varphi_{ik}$ per a tot $k \leq j \leq i$; és a dir, que el diagrama*

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{ij}} & X_j \\ & {\scriptstyle \varphi_{ik}}\searrow \quad \swarrow{\scriptstyle \varphi_{jk}} & \\ & X_k & \end{array}$$

sigui commutatiu. Aquest sistema el denotem per $\{X_i, \varphi_{ij}\}$.

Definició A.1.3. *Sigui un conjunt (espai topològic) Y i $\{X_i, \varphi_{ij}\}$ un sistema projectiu de conjunts (espais topològics), i siguin $\psi_i : Y \longrightarrow X_i$ aplicacions (aplicacions continues) per a cada $i \in I$. Es diu que aquestes aplicacions són compatibles si $\varphi_{ij}\psi_i = \psi_j$, sempre que $j \leq i$ i direm que (Y, ψ_i) forma un sistema compatible amb $\{X_i, \varphi_{ij}\}$.*

Definició A.1.4. *Donat un sistema projectiu $\{X_i, \varphi_{ij}\}$ es diu que X amb les aplicacions compatibles $\varphi_i : X \longrightarrow X_i$ és un límit projectiu del sistema, si compleix la següent propietat universal:*
donat Y un conjunt (espai topològic) i $\psi_i : Y \longrightarrow X_i$ aplicacions compatibles, llavors
$\exists!$ $\psi : Y \longrightarrow X$ (continua) tal que $\varphi_i\psi = \psi_i, \forall i \in I$. És a dir, tenim un diagrama commutatiu per tot i:

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & X \\ & {\scriptstyle \psi_i}\searrow \quad \swarrow{\scriptstyle \varphi_i} & \\ & X_i & \end{array}$$

i denotem $X = \varprojlim X_i$ o, si volem especificar les aplicacions: $(X = \varphi_i)$.

Teorema A.1.5. *Si $\{X_i, \varphi_{ij}\}$ és un sistema projectiu, existeix $X = \varprojlim X_i$ i a més, si (X, φ_i) i (X', φ_i') són límits del sistema, tenim que $\exists!$ $\psi : X \longrightarrow X'$ bijectiu complint $\varphi_i'\psi = \varphi_i, \forall i \in I$ (i si X_i, X_i' espais topològics amb φ_i i φ_i' continues α continua amb ψ^{-1} continua).*

Demostració. Primer de tot demostrem la unicitat del límit.
Siguin (X, φ_i) i (X', φ_i') dos límits projectius del mateix sistema $\{X_i, \varphi_{ij}\}$. Com que X és límit, i (X', φ_i') un sistema compatible, $\exists!$ $\psi : X' \longrightarrow X$ continu tal que $\psi\varphi_i = \varphi_i'$. Ara, com que X' és límit, i (X, φ_i) un sistema

compatible, $\exists!\ \widetilde{\psi} : X \longrightarrow X'$ continu tal que $\widetilde{\psi}\varphi'_i = \varphi_i$.
Llavors, tenim que $\psi\widetilde{\psi} : X' \longrightarrow X'$ és $id_{X'}$, del fet de que X' és límit i $\widetilde{\psi}\psi : X \longrightarrow X$ és id_X del fet de que X és límit. És a dir, $X \cong X'$.

Demostrem ara l'existència del límit. Sigui X un subconjunt del producte directe $\prod_{i\in I} X_i$ tal que $(x_i)_{i\in I} \in X$, si compleix $\varphi_{ij}x_i = x_j$ sempre i quan $i \leq j$. Definim per $\varphi_i : X \longrightarrow X_i$ la projecció canònica en la component i. Demostrem que X és el límit del sistema $\{X_i, \varphi_i\}$.
Siguin Y i $\psi_i : Y \longrightarrow X_i$ compatibles, és a dir, $\varphi_{ij}\psi_i = \psi_j\ \forall i, j \in I$. Construïm tot seguit $\psi : Y \longrightarrow X$ fent el següent diagrama commutatiu:

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & X \\ {\scriptstyle\psi_i}\searrow & \swarrow & {\scriptstyle\varphi_i} \\ & X_i & \end{array}$$

Observem que, per a cada $\alpha \in Y$ tenim que $\psi_i(\alpha) = \beta_{i,\alpha} \in X_i, \forall i$, és clar $\prod_{i\in I} \beta_{i,\alpha} \in \prod_{i\in I} X_i$.
Veiem, $\prod_{i\in I} \beta_{i,\alpha} \in X$. Per a qualsevol $j \leq i$ tenim $\psi_i(\alpha) = \beta_{i,\alpha}$ i $\psi_j(\alpha) = \beta_{j,\alpha}$ i com $\varphi_{ij}(\beta_{i,\alpha}) = \varphi_{ij}(\psi_i(\alpha)) = \psi_j(\alpha) = \beta_{j,\alpha}$ obtenim $\prod_{i\in I} \beta_{i,\alpha} \in X$.
efinimD $\psi : Y \longrightarrow X$ via $\psi(\alpha) := \prod_{i\in I} \beta_{i,\alpha}$ on $\beta_{i,\alpha} = \psi_i(\alpha), \forall i \in I$. (És fàcil comprovar la continuitat en cas d'espais topològics).

□

Observació A.1.6. *(1) Siguin X_i R-mòduls i $\varphi_{ij} : X_i \longrightarrow X_j$ morfismes compatibles que són morfismes de R-mòduls. Observem llavors X, el límit, també és un R-mòdul i φ_i morfismes de R-mòduls.*
Com que acabem de veure a la demostració que el límit és $X = \{(x_i)_{i\in I} : \varphi_{ij}(x_i) = x_j\} \subset \Pi X_i$, és fàcil demostrar que aquest conjunt compleix les propietats de R-mòdul si ψ_j és morfisme de R-mòdul.

(2) Si els X_i del sistema projectiu són anells i els φ_{ij} són morfismes d'anells, aleshores el límit projectiu, X és també un anell amb els ψ_i morfismes d'anells.
(3) Si X_i grups i φ_{ij} morfismes de grups es té que X és grup i ψ_i morfismes de grups. També es fa amb un argument semblant, tan sols remarcar que si $x = (x_i)_{i\in I} \in X$ $x^{-1} \in X$ ja que per a cada $i \geq j$ $\varphi_{ij}(x_i^{-1}) = \varphi_{ij}(x_i)^{-1} = x_j^{-1}$, per tant $x^{-1} = (x_i^{-1})_{i\in I} \in X$.

(4) En els casos (2) i (3) si $(X_i, \varphi_{i,j})$ és un sistema projectiu amb X_i anells o grups dotats amb la topología, i els morfisme $\varphi_{i,j}$ són morfismes d'anells o de grups continus, el límit projectiu tindrà estructura natural d'espai topològic pensant la topología com la induïda per ser un subconjunt de la topología producte en $\prod X_i$ i també com a anell o grup. A més, si X_i són grups topològics es trasllada a que el límit projectiu dels X_i és també un grup topològic.

Definició A.1.7. *Sigui p un primer fix. Els nombres p-àdics són el conjunt d'expressions $\{\sum_{i=0}^{\infty} a_i p^i$ on $a_i \in (0, p-1)\}$ i es denota per $\mathbb{Z}_p$.*

Proposició A.1.8. *$\mathbb{Z}_p$ és isomorf al límit projectiu del sistema $(\mathbb{Z}/(p^i), \varphi_{ij})$ on $\varphi_{ij} : \mathbb{Z}/(p^i) \longrightarrow \mathbb{Z}/(p^j)$ són els morfismes d'anells $\alpha + (p^i) \mapsto \alpha + (p^j)$ $\forall j \leq i$; i per tant $\mathbb{Z}_p$ té estructura d'anell i $\mathbb{Z}_p$ s'anomena l'anell dels nombres p-àdics.*
A més, $\mathbb{Z}_p$ té estructura d'anell topològic, on cada $\mathbb{Z}/(p^n)$ el considerem amb la topologia discreta, ja que així els morfismes d'anells són φ_{ij} continus.

Demostració. Veiem primer que $(\mathbb{Z}/(p^i), \varphi_{ij})$ és un sistema projectiu.
Si $k \leq j \leq i$ $\alpha + (p^i) \in \mathbb{Z}/(p^i)$
$\varphi_{kj}(\varphi_{ij}(\alpha + (p^i))) = \varphi_{kj}(\alpha + (p^j)) = \alpha + (p^k) = \varphi_{ik}(\alpha + (p^i))$ I a més, els φ_{ij} estàn ben definits, ja que si,
$\overline{\alpha} \neq \overline{\alpha'} \in \mathbb{Z}/(p^i) \Rightarrow p^i \nmid (\alpha - \alpha') \Rightarrow$ com $k \geq i$ $p^k \nmid (\alpha - \alpha')$ on $\alpha + (p^k) \neq \alpha' + (p^k)$, on φ_{ij} són morfismes d'anells.
Sabem que $\varprojlim(\mathbb{Z}/(p^i), \varphi_{ij})$ existeix i que és únic llevat d'isomorfisme i té estructura d'anell topològic amb la topologia discreta en $\mathbb{Z}/(p^i)$. Sigui (Y, β_i) un sistema tal que faci que el següent diagrama commuti:

$$\begin{array}{ccc} Y & \xrightarrow{\beta_i} & \mathbb{Z}/(p^i) \\ & {\scriptstyle\psi_j}\searrow \quad \swarrow{\scriptstyle\varphi_{ij}} & \\ & \mathbb{Z}/(p^j) & \end{array}$$

on Y anell i β_i morfismes d'anells.

Si demostrem que existeix un únic morfisme de Y a $\mathbb{Z}_p$ tal que sigui compatible amb els $\varphi_i : \mathbb{Z}_p \longrightarrow \mathbb{Z}/(p^i)$ on $\varphi_i(\sum_{k=0}^{\infty} a_k p^k) = \sum_{k=0}^{i-1} a_k p^k + (p^i)$ (que són les projeccions naturals) hem acabat, ja que $(\mathbb{Z}_p, \varphi_i)$ complirà la propietat universal.

Com que el diagrama commmuta, tenim que per a cada $y \in Y$, $\beta_i(y) \in \mathbb{Z}/(p^i)$, $\varphi_{i,i-1}(\beta_i(y)) = \beta_{i-1}(y) \in \mathbb{Z}/(p^{i-1})$.
Definim, $\beta : Y \longrightarrow \mathbb{Z}_p$ per $\beta(y) := \sum_{l=0}^{m} b_{y,l}p^l$ on $b_{y,l} \in \{0, ..., p-1\}$ complint $\sum_{l=0}^{\infty} b_{y,l}p^l \equiv \beta_{m+1}(y)$ en $\mathbb{Z}/(p^{m+1})$ per a cada m.
Veiem que aquest β que hem definit està ben definit i que el següent diagrama commuta:

$$\begin{array}{ccc} Y & \xrightarrow{\beta} & \mathbb{Z}_p \\ & {\scriptstyle\beta_j}\searrow \quad \swarrow{\scriptstyle\varphi_j} & \\ & \mathbb{Z}/(p^j) & \end{array}$$

Sigui $y \in Y$, hem dit que $\beta(y) = \sum_{l=0}^{\infty} b_{l,y}p^l$ tal que $\sum_{l=0}^{m} b_{l,y}p^l \equiv \beta_{m+1}(y)$ en $\mathbb{Z}/(p^{m+1})$.
Ara, $\varphi_j(\beta(y)) = \sum_{l=0}^{j-1} b_{y,l}p^l$ en $\mathbb{Z}/(p^j)$.
Però $\beta(y)$ per $m = j-1$, $\sum_{l=0}^{j-1} b_{y,l}p^l \equiv \beta_j(y)(mod\ p^j)$
Per tant, $\beta_j(y) = \varphi_j(\beta(y))$ en $\mathbb{Z}/(p^j)$, fent el diagrama commutatiu on $b_{y,l}$ és sempre el mateix independentment del $m \geq l$.
D'aquí $\mathbb{Z}_p$ és el límit projectiu dels $(\mathbb{Z}/(p^i), \varphi_{ij})$. □

A.2 Propietats topològiques dels límits projectius

Lema A.2.1. *Sigui $\{X_i, \varphi_{ij}\}$ un sistema projectiu d'espais topològics amb X_i Hausdorff $\forall i$. Llavors $\varprojlim X_i$ és tancat en $\prod_{i\in I} X_i$.*

Demostració. Sigui $(x_i)_{i\in I} \in \prod_{i\in I} X_i - (\varprojlim X_i)$. Aleshores, existeixen $r, s \in I$ amb $s \leq r$ tals que $\varphi_{rs}(x_r) \neq x_s$. Agafem dos entorns disjunts U i V de $\varphi_{rs}(x_r)$ i x_s respectivament en X_s.
Sigui U' un entorn obert de x_r en X_r tal que $\varphi_{rs}(U') \subseteq U$.
Ara considerem un obert $W = \prod_{i\in I} V_i$ de $\prod_{i\in I} X_i$ tal que $V_r = U'$, $V_s = V$ i $V_i = X_i$ per $i \neq r, s$. Llavors W és un entorn obert de $(x_i)_i$ en $\prod_{i\in I} X_i$ disjunt amb $\varprojlim X_i$. D'on $\varprojlim X_i$ és tancat. □

Proposició A.2.2. *Sigui $\{X_i, \varphi_{ij}\}$ un sistema projectiu amb X_i compactes, Hausdorff i totalment disconnexes. Llavors, $\varprojlim X_i$ és també un espai compacte, Hausdorff i totalment disconnex.*

Demostració. Pel teorema de Tychonoff, si cada X_i és compacte, aleshores el producte directe $\prod_{i\in I} X_i$ també ho és. I un subespai tancat d'un compacte és compacte, aleshores, pel lema que acabem de demostrar, com que $\varprojlim X_i$ és tancat, és compacte. Veiem que és Hausdorff i totalment disconnex.
Com que les propietats de ser Hausdorff i ser totalment disconnex es mantenen pel producte, $\prod X_i$ és Hausdorff i totalment disconnex.
Siguin $x = (x_i) \neq y = (y_i) \in \varprojlim X_i \subseteq \prod X_i$. Aleshores $\exists j$ tal que $x_j \neq y_j$, i com X_j Hausdorff, existeixen dos oberts disjunts en X_j amb $x_j \in Uj$ i $y_j \in V_j$. Els oberts de $\varprojlim X_i$ són els $U' \in \varprojlim X_i$ tal que $U' = U \cap \varprojlim X_i$ on U és un obert de $\prod X_i$. Per tant, si agafem $U = \prod_{i\neq j} X_i \times U_j$ i $V = \prod_{i\neq j} X_i \times V_j$, on clarament U i V són oberts en $\prod X_i$. Per tant, prenent $U' = U \cap \varprojlim X_i$ i $V' = V \cap \varprojlim X_i$, tenim dos oberts tals que $x \in U'$ i $y \in V'$ amb intersecció buida, provant que $\varprojlim X_i$ Hausdorff.
Per veure que és totalment disconnex, sigui $Y = (Y_i) \in \varprojlim X_i \subseteq \prod_{i\in I} X_i$. Com que per a cada i $Y_i \subseteq X_i$, existeixen dos oberts U_i i V_i oberts tals que $Y_i = U_i \cup V_i$ i $U_i \cap V_i = \emptyset$. Pel mateix motiu d'abans $U' = \prod U_i \cup \varprojlim X_i$ i $V' = \prod V_i \cup \varprojlim X_i$ sóon dos oberts i és clar que $U' \cup V' = Y$ i $U' \cap V' = \emptyset$. □

Proposició A.2.3. *Sigui $\{X_i, \varphi_{ij}\}$ un sistema projectiu on cada X_i és un espai no buit, compacte i Hausdorff. Aleshores, $\varprojlim X_i$ és no buit. En particular, el límit projectiu d'un sistema de conjunts finits no buits és no buit.*

Demostració. Per cada $j \in I$ definim
$Y_j = \{(x_i)_{i\in I} | \varphi_{jk}(x_j) = x_k, \forall k \leq j\} \subseteq \prod_{i\in I} X_i$.
Utilitzant l'axioma de l'elecció cada Y_j és no buit i amb un argument semblant al A.2.1 s'obté que cada Y_j tancat a $\prod_{i\in I} X_i$. Observem que si $j \leq j'$, aleshores $Y_j \supseteq Y_{j'}$. Llavors, per ser $\prod_{i\in I} X_i$ compacte es dedueix que $\bigcap Y_j$ és no buida, ja que si $\bigcap Y_j = \emptyset$ $\prod_{i\in I} X_i = \bigcup Y_i^c = Y_{i_1}^c \cup \cdots \cup Y_{i_n}^c$, però $Y_{i_1} \cap \cdots \cap Y_{i_n} = \emptyset$, escollim $j \geq i_1, \cdots, i_n$, aleshores $Y_{i_1} \supseteq Y_j$ i $Y_j \neq \emptyset$, $\emptyset = Y_{i_1} \cap \cdots \cap Y_{i_n} \supseteq Y_j \neq \emptyset$ i això és imposible. Com que $\varprojlim X_i = \bigcap_{j\in I} Y_j$ hem acabat. □

Definició A.2.4. *Siguin $\{X_i, \varphi_{ij}\}$ i $\{X'_i, \varphi'_{ij}\}$ són dos sistemes projectius d'espais topològics sobre el mateix conjunt I.Llavors un morfisme entre aquestes sistemes és*
$\Gamma : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\}$
on Γ és una col·lecció de aplicacions continues $\theta_i : X_i \longrightarrow X'_i$ tals que si $i \geq j$ el següent diagrama commuta:

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{ij}} & X_j \\ \theta_i \downarrow & & \downarrow \theta_j \\ X'_i & \xrightarrow{\varphi'_{ij}} & X'_j \end{array}$$

Observació A.2.5.
(1) Tenim $\Gamma : \{X_i, \varphi_{ij}\} \longrightarrow \{X_i, \varphi_{ij}\}$ on $\theta_i = id\,{}_{\restriction X_i}$, escrivim $\Gamma \equiv id$
(2) La composició està definida de manera natural. Si tenim $\Gamma : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\}$ i $\Psi : \{X'_i, \varphi'_{ij}\} \longrightarrow \{X''_i, \varphi''_{ij}\}$ on $\Psi\Gamma$ ve donat per la col·lecció d'aplicacions $\psi_i\theta_i$.
(3)Siguin, $\{X_i, \varphi_{ij}\}$ i $\{X'_i, \varphi'_{ij}\}$ dos sistemes projectius d'espais topològics, Γ un morfisme de sistemes projectius i $X = \varprojlim X_i$ i $X' = \varprojlim X'_i$. Llavors la col·lecció de morfismes $\theta_i\varphi_i : X \longrightarrow X'_i$ indueixen una aplicació continua: $\varprojlim \Gamma = \varprojlim \theta_i : \varprojlim X_i \longrightarrow \varprojlim X'_i$
(4) Que θ_i sigui exhaustiva per tot i no implica que $\varprojlim \theta_i$ ho sigui.
Per exemple, si agafem els sistemes projectius $\{\mathbb{Z}, id\}$ i $\{\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij}\}$ on φ_{ij}-s són les projeccions naturals per $j \leq I$. Per a cada $i \in N$ $\theta_i : \mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z}$ és exhaustiva, però $\Gamma : \varprojlim \theta_i : \varprojlim\{\mathbb{Z}, id\} = \mathbb{Z} \longrightarrow \varprojlim\{\mathbb{Z}/p^i\mathbb{Z}, \varphi_{ij}\} = \mathbb{Z}_p$ no ho és. Ja que, l'imatge de $\mathbb{Z}$ per Γ és $\{(a_n) \mid a_n = t, t \in \mathbb{Z}\}$ les tuples constants, i $1 + p + p^2 + \cdots \notin \mathbb{Z}$.

Lema A.2.6. *Sigui $\Gamma : \{X_i, \varphi_{ij}\} \longrightarrow \{X'_i, \varphi'_{ij}\}$ una aplicació de sistemes projectius Hausdorff i compactes. Si cada $\theta_i : X_i \longrightarrow X'_i$ és exhaustiu, es te que $\varprojlim \Gamma = \varprojlim \theta_i : \varprojlim X_i \longrightarrow \varprojlim X'_i$ és exhaustiu.*

Demostració. Sigui $(x'_i)_{i\in I} \in \varprojlim X'_i$. Posem $\widetilde{X_i} = \theta_i^{-1}(x'_i)$, $\forall i \in I$. $\widetilde{X_i}$ és tancat en X_i perque $\prod X'_i - x'_i$ és obert, i com que θ_i és continua i exhaustiva $\theta^{-1}(\prod X'_i - x'_i) = \prod X_i - \theta_i^{-1}(x'_i)$ obert. Com que l'espai X_i és compacte, $\widetilde{X_i}$ també ho és. Observem que $\varphi_{ij}(\widetilde{X_i}) \subseteq \widetilde{X_j}$ per $i \geq j$.
Aleshores $\{\widetilde{X_i}, \varphi_{ij}\}$ és un sistema projectiu de compactes no buits, i per la propocició A.2.3, $\varprojlim \widetilde{X_i} \neq \emptyset$.
Sigui $(x_i) \in \varprojlim \widetilde{X_i} \subseteq \varprojlim X_i$, llavors per constucció $\varprojlim(\Gamma)(x_i) = (x'_i)$. □

Corol·lari A.2.7. *Sigui $\{X_i, \varphi_{ij}, I\}$ un sistema projectiu de espais compactes i Hausdorff. I sigui X un espai compacte i Hausdorff. Suposem que $\{\varphi_i : X \longrightarrow X_i\}_{i\in I}$ és un sistema de aplicacions continues compatibles exhaustives. Llavors l'aplicació induïda $\varprojlim \varphi_i : X \longrightarrow \varprojlim X_i$ és exhaustiva.*

Demostració. Considerem el sistema projectiu constant $\{X, id\}$ sobre I. Llavors, clarament la col·lecció de funcions $\{\varphi_i\}_{i\in I}$ de $\{X, id\}$ a $\{X_i, \varphi_{ij}\}$ indueix una aplicació $\varprojlim \varphi_i : X \longrightarrow \varprojlim X_i$ que és exhaustiva pel lema A.2.6. □

Lema A.2.8. *Sigui $\{X_i, \varphi_{ij}\}$ un sistema projectiu d'espais topològics i $\varphi_i : X \longrightarrow X_i$ compatibles i exhaustius per a cada $i \in I$. llavors ó $\varprojlim X_i = \emptyset$ ó $\varprojlim \varphi_i : X \longrightarrow \varprojlim X_i$ envia X a un subconjunt dens de $\varprojlim X_i$.*

Demostració. Suposem que $\varprojlim X_i \neq \emptyset$. Un obert generic V de $\varprojlim X_i$ es pot descriure de la manera següent: siguin $\{i_1, ..., i_n\} \subseteq I$ i U_{i_j} un obert de X_{i_j} $j = 1, ..., n$;
$V = (\varprojlim X_i) \cap (\prod_{i\in I} V_i)$
on $V_{i_j} = U_{i_j}, j = 1, ..., n$ i $V_i = X_i$ si $i \neq i_1, ..., i_n$.
Suposem que V és no buit. Hem de veure que $\varprojlim \varphi_i(X) \cap V \neq \emptyset$. Sigui $i_0 \geq i_1, ..., i_n$ i $y = (y_i) \in V$. Escollim $x \in X$ tal que $\varprojlim \varphi_{i_0}(x) = y_{i_0}$ (això ho podem fer perque cada φ_i és exhaustiva). Llavors $\varprojlim \varphi_i(x) \in V$. □

Corol·lari A.2.9. *Sigui $\{X_i, \varphi_{ij}\}$ un sistema projectiu de espais compactes i Hausdorff; $X = \varprojlim X_i$ i $\varphi_i : X \longrightarrow X_i$ les projeccions. Aleshores,*
(a) Si $Y \subseteq X$,$Y \subseteq \varprojlim \varphi_i(Y)$, i si Y tancat $Y = \varprojlim \varphi_i(Y)$
(b) Si $Y \subseteq X$, llavors $\overline{Y} = \varprojlim \varphi_i(Y)$
(c) Si $Y, Y' \subseteq X$ i $\varphi_i(Y) = \varphi_i(Y')$ per a cada $i \in I$, llavors $\overline{Y} = \overline{Y'}$.

Demostració. (a) Observem que tenim les inclusions obvies $Y \hookrightarrow \varprojlim \varphi_i(Y) \hookrightarrow \varprojlim X_i = X$. Pel corol·lari A.2.7 la primera inclussió és exhaustiva i per tant $\overline{Y} \subseteq \varprojlim \varphi_i(Y)$. Ara pel lema A.2.8, l'imatge de Y és densa, i com que Y tancat, obtenim la igualtat.
(b) Pel lema A.2.8, la inclusió envia Y a un subespai dens dins de $\varprojlim \varphi_i(Y)$. Argumentant com al lema A.2.1 es veu que $\varprojlim \varphi_i(Y)$ és tancat en X, i finalitzem. (c) Conclusió obvia per (a) i (b). □

Definició A.2.10. *Sigui $(I, \leq)$ un conjunt dirigit, i I' un sucbonjunt de I. De manera natural $(I', \leq)$ es converteix en un conjunt dirigit. Diem que I' és cofinal en I si per tot $i \in I$ existeix algun $\imath' \in I'$ tal que $i \leq i'$.*

Observació A.2.11. *Observem que $\{X_i, \varphi_{ij}\}_{i,j\in I'}$ es converteix en un sistema projectiu. Direm que $\{X_i, \varphi_{ij}, I'\}$ és un sistema cofinal de $\{X_i, \varphi_{ij}, I\}$. Si $\{X_i, \varphi_{ij}, I'\}$ és un sistema cofinal de $\{X_i, \varphi_{ij}, I\}$ i $(\varprojlim X_{i'}, \varphi_{i'})$ i $(\varprojlim X_i, \varphi_i)$ els límits projectius de cadascun d'ells; per cada $j \in I$, agafem $j' \in I'$ tal que $j' \geq j$ i definim $\overline{\varphi_j} : \varprojlim_{I'} X_{i'} \longrightarrow X_j$ com la composició de les aplicacions canòniques $\varphi_{j'j}\varphi_{j'}$. Observem que els $\overline{\varphi_j}$ estàn ben definits (perque són independents de la j' que escollim) i són compatibles. Aleshores, indueixen un $\overline{\varphi} : \varprojlim_{I'} X_{i'} \longrightarrow \varprojlim_I X_i$ tal que $\varphi_j\overline{\varphi} = \overline{\varphi_j}$.*

Lema A.2.12. *Sigui $\{X_i, \varphi_{ij}, I\}$ un sistema projectiu de espais compactes sobre I, i I' un subconjunt cofinal de I. Llavors, $\varprojlim_I X_i \cong \varprojlim_{I'} X_{i'}$.*

Demostració. Veiem primer de tot que $\overline{\varphi} : \varprojlim_{I'} X_{i'} \longrightarrow \varprojlim_I X_i$ és una bijecció continua.
$\overline{\varphi}$ és injectiva perque si $(x_{i'}) \in \varprojlim_{I'} X_{i'}$ i $\varphi(x'_i) = y_i$, $x_{i'} = y_{i'}$ per tot $i' \in I'$. Per veure l'exhaustivitat, si $(y_i) \in \varprojlim_I X_i$, considerem $(x_{i'})$ on $x_{i'} = y_{i'}$ per tot $i' \in I$. Llavors $(x_{i'}) \in \varprojlim_{I'} X_{i'}$ i $\varphi(x_{i'}) = (y_i)$. I com que $\overline{\varphi}$ és una bijecció continua i $\varprojlim_{I'} X_{i'}$ i $\varprojlim_I X_i$ són compactes, tenim que $\overline{\varphi}$ és homeomorfisme. □

Observació A.2.13. *Diem que un sistema projectiu és exhaustiu si cada $\varphi_{ij}(i \geq j)$ és exhaustiu. Pel corol·lari A.2.7, per a cada sistema projectiu existeix un sistema exhaustiu $\{\varphi_i(X), \varphi'_{ij}, I\}$ on els φ'_{ij} són les restriccions de φ_{ij} a $\varphi_i(X)$ amb el mateix límit projectiu X.*
Si $\{X_i, \varphi_{ij}, I\}$ és un sistema projectiu de espais topológics X_i sobre I. Possem $X = \varprojlim X_i$ i siguin $\varphi_j : X \longrightarrow X_j$ les projeccions naturals. Supossem $X \neq \emptyset$. Si φ_j és exhaustiu per a cada $j \in I$, llavors $\varphi_{rs} : X_r \longrightarrow X_s$ també ho és per a tot $r, s \in I$ amb $r \geq s$. (El recíproc no té per que ser cert però ho és si demanem que els X_i siguin compactes).

Proposició A.2.14. *Sigui $\{X_i, \varphi_{ij}, I\}$ un sistema projectiu exhaustiu d'espais compactes, Hausdorff i no buits. Llavors per a cada $j \in I$ la projecció $\varphi_j : \varprojlim X_i \longrightarrow X_j$ és exhaustiva.*

Demostració. Fixem $j \in I$. El conjunt $I_j = \{i \in I : i \geq j\}$ és cofinal en I. Llavors pel lema A.2.12 $\varprojlim_{I_j} X_i \cong \varprojlim_I X_i$. Per tant podem suposar que $j \leq i$ per a tot $i \in I$.
Sigui $x_j \in X_j$ i possem $Y_r = \varphi_{rj}^{-1}(x_j)$ per a $r \in I$. Com que φ_{rj} és exhaustiu i continu, $Y_r \neq \emptyset$ i compacte en X_r. A més, si $r \geq s$ en I, $\varphi_{rs}(Y_r) \subseteq Y_s$, i $\{Y_r, \varphi_{rs}, I\}$ és un sistema projectiu. Per la proposició A.2.3 $\varprojlim Y_r \neq \emptyset$. Sigui $(y_r) \in \varprojlim Y_i \subseteq \varprojlim X_i$. Llavors, $\varphi_j(y_r) = x_j$. □

A.3 Propietats topològiques dels espais profinits

Definició A.3.1. *X s'anomena espai profinit si és un espai topològic isomorf $\varprojlim X_i$ on X_i són conjunts finits dotats amb la topologia discreta.*

Lema A.3.2. *Sigui X un espai compacte i Hausdorff, i $x \in X$. Llavors la component connexa C_x de x és la intersecció de tots els entorns "clopens" (i.e. oberts i tancats a la vegada) de x.*

Demostració. Sigui $\{U_t : t \in T\}$ la familia dels entorns "clopens" de x i $A = \bigcap_{t\in T} U_t$. Que $C_x \subseteq A$ és evident. Per tant només cal veure que A és connex.
Si $A = U \cup V$ on $U \cap V \neq \emptyset$ amb U i V tancats en A. Hem de veure que o U o V és buit.
Com que X és Hausdorff i U i V compactes disjunts, existeixen U' i V' oberts en X tals que $U \subseteq U'$ i $V \subseteq V'$ amb $U' \cap V' = \emptyset$. Aleshores, $[X - U' \cap V'] \cap A = \emptyset$. Ara, $X - (U' \cap V')$ és tancat, i com que X és compacte existeix T' finit, una familia de T tal que $[X - (U' \cap V')] \cap [\bigcap_{t'\in T'} U_{t'}] = \emptyset$. Observem que $B = \bigcap_{t'\in T'} U_{t'}$ és un clopen de X, perquè T' és finit. Per altra banda, $x \in (B \cap U') \cup (B \cap V') = B$.
Sigui $x \in B \cap U'$ (amb V' es faria igual). $B \cap U'$ és obert i tancat a la vegada, perquè $B \cap V'$ és obert i $(X\ B \cap V') \cap = B \cap U'$. Aleshores $A \subseteq B \cap U' \subseteq U'$. I per tant $A \cap V \subseteq A \cap V' = \emptyset \Rightarrow V' = \emptyset$. □

Teorema A.3.3. *Sigui X un espai topologic. Les següents condicions són equivalents:*
(a) X és profinit.
(b) X és compacte, Hausdorff i totalment disconnex.
(c) X és compacte, Hausdorff i admet una base de clopens en la topologia de X.

Demostració. (a)⇒ (b)
Sigui X profinit, és a dir, $X \cong \varprojlim X_i$ amb X_i finit. Per la proposició A.2.2, X és Hausdorff i totalment disconnex. (Perquè cada X_i amb la topologia discreta és Hausdorff i totalment disconnexa). I compacte per la mateixa proposició.
(b)⇒ (c)
Sigui W un entorn obert de x en X. Hem de veure que W conté un clopen de x. Sigui $\{U_t | t \in T\}$ la familia de tots els clopens de x. Pel lema A.3.2, $\{x\} = \bigcap_{t\in T} U_t$ (perquè X totalment disconnex i aleshores $C_x = \{x\}, \forall x \in X$). Com que $X - W$ és tancat i disjunt $\bigcap_{t\in T} U_t$, per la compacticitat de

X, existeix $T' \subseteq T$ finit tal que $(X\ W) \cap (\bigcap_{t\in T} U_t) = \emptyset$. Per tant, aquest $\bigcap_{t\in T} U_t$ és un clopen de x contingut en W.
(c)$\Rightarrow$ (a)
Suposem que X és Hausdorff i que admet una base de clopens amb la seva topologia. Denotem $\boldsymbol{R}$ la col·leccio de totes les relacions d'equivalencia de X, tal que la classe d'equivalencia de x, xR és un clopen. Per a cada R, X/R és finit i discret, perquè $X = \bigcup_{j\in I} x_j R$ essent aquesta unió disjunta. Cada $x_j R$ és obert, però també tancat, i com que X és compacte, aquesta unió és finita, i per tant X/R discret. El conjunt $\boldsymbol{R}$ està naturalment ordenat de la següent manera: si $R, R' \in \boldsymbol{R}$, $R \geq R' \Leftrightarrow xR \subseteq xR', \forall x \in X$. Llavors $\boldsymbol{R}$ és un conjunt dirigit, perquè si $R_1, R_2 \in \boldsymbol{R}$ definim $R_1 \cap R_2$ com la relació d'equivalencia corresponent a la partició de X obtinguda per totes les interseccions de les classes d'equivalencia de R_1 i R_2. Clarament $R_1 \cap R_2 \geq R_1, R_2$. Ara, si $R, R' \in \boldsymbol{R}$, definim $\varphi_{R,R'} : X/R \longrightarrow X/R'$ de manera que $\varphi_{RR'}(xR) = (xR')$. Llavors $\{X/R, \varphi_{RR'}\}$ és un sistema projectiu sobre $\boldsymbol{R}$. Demostrem ara que $X \cong \varprojlim_{R\in\boldsymbol{R}} X/R$.
Sigui $\psi : Y \longrightarrow \varprojlim_{R\in\boldsymbol{R}} X/R$ l'aplicació continua induïda per les projeccions canóniques $\psi_R : X \longrightarrow X/R$, pel corol·lari A.2.7, ψ és continua i exhaustiva. Per veure que ψ és homeomorfisme, és suficient veure que és injectiva, perquè X és compacte.
Siguin, $x, y \in X$. Per hipótesi, existeix un entorn U de x obert i tancat a la vegada que no conté a y. Considerem la relació d'equivalencia R' en X que té dos classes d'equivalencia: U i $X - U$. Clarament, $R' \in \boldsymbol{R}$ i $\psi_{R'}(x) \neq \psi_{R'}(y)$. Llavors $\psi(x) \neq \psi(y) \Rightarrow \psi$ injectiva. $\square$

Bibliografia

[1] J. Bosman, *A polynomial with Galois group $SL_2(\mathbb{F}_{16})$*, Journal of Computation and Mathematics, vol.10 (2007), pp 378-388.

[2] F.Michael Bulter, *Infinite Galois Theory, A Thesis in Matematics*, Pensilvania, 2001.

[3] Daniel Gorenstein, Richard Lyons, Ronald Solomon *The Classification of the Finite Simple Groups* (volume 1), AMS, 1994 (volume 2), AMS.

[4] Philipe H.Gharmoy *Galois Theory*, Escola politècnica Federal de Lousiana, 2008

[5] L.Dieulefait, Modular Galois Realizations of Linear Groups, Thesis UB, 2001.

[6] G.Karpilovsky, *Field Theory, Classical Foundation and Multiplicative Groups*, Editorial Board, 1988

[7] G.Karpilovsky, *Topics in Field Theory*, Elsevier Science Publishers B.V., 1989

[8] J.Klüners and G.Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J.Symbolic Comput. 30(2000), no6, 675-716.

[9] P.Morandi, *Field and Galois Theory*, Springer, 1996

[10] Jürgen Neukirch, *Algebraic Number Theory*, Springer Verlag 1992.

[11] L.Ribes i Plzakesski, *Profinits Groups, Volume 40*, Sprimger, 2000

[12] Joshep J.Rotman, *An Introduction to the Theory of Groups*, Quarta edició, Springer-Verlag, 1994

[13] Jean Pierre Serre, *Topics in Galois Theory*, Jones and Barlett Publishers, 1992

[14] Alexander Schmith i Kay Winberg *Shafarevic's Theorem on Solvable Groups as Galois Groups*, http://www.math.uiuc.edu/Algebraic-Number-Theory/0136/

[15] Nuria Vila *On the inverse problem of Galois theory*, Publicacions matemàtiques Vol. 36, pp.1053-1073, (1992).

[16] Andrew Johans Wills *Topics in Invers Galois Theory*, Blacksburg, Virginia, 2011