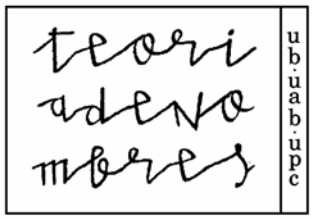
NOTES DEL SEMINARI



PROBLEMES D'IMMERSIÓ SOBRE COSSOS GRANS

Barcelona *1999*

4

Notes del Seminari de Teoria de Nombres (UB-UAB-UPC)

Comitè editorial
P. Bayer E. Nart J. Quer

PROBLEMES D'IMMERSIÓ SOBRE

COSSOS GRANS

Edició a cura de

M. Vela N. Vila

Amb contribucions de

C. Infante B. Plans M. Vela N. Vila X. Xarles

M. Vela N. Vila

Facultat de Matemàtiques, UB
Gran Via de les Corts Catalanes, 585
08007 Barcelona. Espanya

Comitè editorial

P. Bayer
Fac. de Matemàtiques
Univ. de Barcelona
Gran Via de les Corts
Catalanes, 585
08007 Barcelona
Espanya

E. Nart
Fac.de Ciències
Univ. Autònoma de
Barcelona
Dep. de Matemàtiques
08193 Bellaterra
Espanya

J. Quer
Fac. de Matemàtiques
i Informàtica
Univ. Politècnica de
Catalunya
Pau Gargallo, 5
08228 Barcelona
Espanya

Classificació AMS
Primària: 12F, 12J, 11R
Secundària: 20F, 26E

Barcelona, 1999
Amb suport parcial de DGE PB96-0970-C02-01

ISBN: 84-923250-3-8

Índex

1 Breu introducció a la geometria analítica rígida
Xavier Xarles **1**

1.1 Àlgebres afinoides 3
1.2 Varietats afinoides 6
1.3 G-espais topològics 8
1.4 Varietats analítiques rígides 11
Bibliografia 15

2 1/2 Teorema d'existència de Riemann amb acció de Galois
Bernat Plans **17**

2.1 Introducció 17
2.2 Enunciat del resultat 18
2.3 Construcció de recobriments cíclics 21
2.4 Enganxant recobriments cíclics convenientment 23
2.5 Conclusió 27
Bibliografia 31

3 Algunas consideraciones no-estándar
Carlos Infante **33**

3.1 Ultrafiltros y Ultrapotencias. 33

3.2 Cuerpos grandes y extensiones de cuerpos existencialmente cerradas 37
Bibliografia 43

4 Realitzacions galoisianes sobre cossos grans
MONTSERRAT VELA **45**
4.1 Cossos grans 47
4.2 Problemes d'immersió 48
4.2.1 Plantejament. Solucions pròpies i impròpies . . 48
4.2.2 Solucions regulars. Problema invers regular . . 50
4.2.3 Problemes d'immersió dominants 51
4.3 Teorema A 57
4.3.1 Primer Lema 58
4.3.2 Segon Lema 62
4.3.3 Conclusions. Final de la demostració del Teorema 63
4.4 Teorema B 63
4.4.1 Cossos hilbertians 64
4.4.2 Demostració del Teorema B 65
4.5 Un darrer resultat 66
Bibliografia 69

5 Conjectura de Šafarevič semi-local
NÚRIA VILA **71**
5.1 La conjectura de Šafarevič 71
5.2 Freiheitssatz de Iwasawa 74
5.3 Cossos satisfent un principi local-global universal . . 77
5.4 Topologies étale i estricta. Conjunts de tipus local . . 79
5.5 Grups relativament projectius 80
5.6 Cossos totalment $\mathfrak{S}$-àdics 81
Bibliografia 85

Introducció

Aquestes notes contenen les exposicions sobre el tema: *Problemes d'immersió sobre cossos grans*, del 98-99.SEMINARI DE TEORIA DE NOMBRES (UB-UAB-UPC), 13è. any, celebrat a Collbató, del 24 al 28 de Gener de 1999.

L'objectiu d'aquest tema va ser fer-se càrrec de l'article de Florian Pop, Annals of Math. 144 (1996), on es prova que tot grup finit es realitza com a grup de Galois sobre $k(T)$, on k és un cos gran. Núria Vila va programar i coordinar les cinc exposicions següents:

1. Geometria analítica rígida

   Expositor: X. Xarles

2. 1/2 teorema d'existència de Riemann

   Expositor: B. Plans

3. Algunes consideracions no-estàndard

   Expositor: C. Infante

4. Realitzacions galoisianes sobre cossos grans

   Expositor: M. Vela

5. Conjectura de Šafarevič semi-local

   Expositor: N. Vila

Cada autor ha redactat i completat els continguts de la seva exposició que recollim en aquest volum de les Notes del Seminari de Teoria de Nombres (UB-UAB-UPC).

Capítol 1

Breu introducció a la geometria analítica rígida

Xavier Xarles

Introducció

Objectiu

L'objectiu de la geometria rígida analítica és desenvolupar una "geometria" sobre un cos complet respecte un valor absolut no arquimedià de tal manera que:

1. Tota varietat algebraica V (o, més en general, tot esquema localment de tipus finit) tingui una única varietat analítica V^{an} associada. A més, si V és connexa (regular, reduïda, separada, etc.), la seva varietat analítica associada V^{an} també és connexa (regular, reduïda, separada, etc.).

2. Donada la varietat analítica $(\mathbb{A}^n)^{an}$, les funcions "regulars" siguin les sèries de potències amb n variables i coeficients a K, convergents a tot $\bar{K}^n$. A més, els "polidiscs" siguin oberts de $(\mathbb{A}^n)^{an}$.

3. Donada una varietat projectiva V, les subvarietats analítiques de V^{an} siguin algebraiques (teorema de Chow), o, més en general, tinguem un teorema GAGA (el mateix amb morfismes finits).

Motivació

La motivació inicial (de J. Tate a **4**) per a construir aquesta geometria era la de donar un sentit **geomètric** a l'afirmació: donat $q \in K^*$ amb $|q| < 1$, el grup $K^*/q^{\mathbb{Z}}$ és el grup de K-racionals d'una corba el·líptica (amb reducció multiplicativa split si el valor absolut de K és discret). El resultat què un arriba és que la corba analítica rígida $\mathbb{G}_m/q^{\mathbb{Z}}$ (que sols té sentit en la geometria analítica) és isomorfa (analíticament) a una corba el·líptica.

La nostra motivació serà: poder aplicar tècniques de la geometria analítica per a construir recobriments de Galois algebraics de $\mathbb{P}^1$.

Problema

Posem-nos per comoditat al cas en que $K = \bar{K}$. Aleshores $\mathbb{A}^1$ hauria de ser com a conjunt igual a K i podem considerar la topologia donada pel valor absolut. Aleshores:

Problema 1 K és totalment disconnex. De fet dues boles obertes $B(a,r) = \{x \in K \mid |x-a| < r\}$ o bé estan una dins de l'altra o bé són disjuntes.

Problema 2 Una funció f de K hauria de ser analítica si i només si ho és en cada obert d'un recobriment de K. Però tant les boles "obertes" $B(a,r)$ com les boles "tancades" $\bar{B}(a,r)$ són obertes a K! Podem per tant prendre el recobriment per oberts $K = B(0,1) \bigsqcup (K \setminus B(0,1))$ i considerar la funció

$$f(x) := \begin{cases} 0 & \text{si } |x| \leq 1 \\ 1 & \text{si } |x| > 1 \end{cases}$$

que és localment analítica però no globalment analítica (segons la nostra definició anterior).

Idea naïf

Seguim en el cas $K = \bar{K}$. Direm *obert admissible* tant sols a la unió disjunta de policilindres, o sigui d'oberts de la forma

$$\bar{B}(a,r) \setminus (\bigsqcup_{i=1}^{n} B(a_i, r_i))$$

(dits també oberts estàndard), observant que la unió (no necessàriament disjunta) d'oberts admissibles no és (en general) admissible, però la intersecció finita si que ho és. Definim ara *recobriment admissible* com un recobriment finit per oberts admissibles. Amb aquesta definició es pot provar que una funció de K a K és analítica (i.e. donada per una sèrie de potències) si i només si és analítica localment en cada obert d'un recobriment admissible.

Compte! Els oberts estàndard són base de la topologia de K. Així que el que volem és construir una mena de topologia on la unió d'oberts no sigui necessàriament un obert, però on haguem de dir què vol dir recobrir per oberts. Això és exactament el que fa el concepte de *topologia de Grothendieck*.

El mètode per a construir els espais analítics rígids és similar al de la teoria d'esquemes: primer estudiarem les àlgebres de funcions (anomenades afinoides), després els hi assignarem un conjunt (varietats afinoides), després definirem obert (admissible) en aquest conjunt i un feix d'anells estructural. Finalment els espais analítics rígids seran els *G-espais localment anellats* tals que localment siguin afinoides. Seguirem el mètode explicat en el llibre **1**.

1.1 Àlgebres afinoides

Comencem recordant la definició de cos complet per un valor absolut no arquimedià (o valor absolut ultramètric).

Definició 1.1.1. *Direm que un cos K té un valor absolut no arquimedià si existeix una aplicació $|\ |: K \to \mathbb{R}_{\geq 0}$ tal que*

(a) $|x| = 0 \iff x = 0$.

(b) $|xy| = |x|\,|y|$ *per a tot* $x, y \in K$.

(c) $|x+y| \leq \max\{|x|, |y|\}$ *per a tot* $x, y \in K$.

Direm que és complet respecte a $|\ |$ *si tota sèrie de Cauchy a* K *és convergent.*

Exemples 1.1.2. *Exemples de cossos complets respecte a un valor absolut són* $\mathbb{Q}_p$, $\mathbb{C}_p := \hat{\overline{\mathbb{Q}}}_p$ *(la completació de la clausura algebraica de* $\mathbb{Q}_p$*),*

$$k((t)) := \{\sum_{i \geq N}^{\infty} a_i t^i \ ;\ N \in \mathbb{Z}\ ,\ a_i \in k\}$$

(el cos de sèries de Laurent amb coeficients a un cos k *qualsevol), i en general qualsevol cos de fraccions d'un anell de valoració discreta complet, les seves extensions finites i la completació de la seva clausura algebraica.*

Per a la resta d'aquestes notes K sempre denotarà un cos complet respecte a un valor absolut no arquimedià.

Definició 1.1.3. *L'anell de sèries estrictament convergents sobre* K *amb* n *indeterminades (o àlgebra de Tate) és per definició*

$$\begin{aligned} \mathbb{T}_n = \mathbb{T}_n(K) \ &= K\langle X_1, \ldots, X_n\rangle := \\ &\{\textstyle\sum_{|\nu| \geq 0} a_\nu X^\nu \ ;\ a_\nu \in K \ i\ \lim_{|\nu|\to\infty} |a_\nu| = 0\}, \end{aligned}$$

on hem fet servir la notació $X = (X_1, \ldots, X_n)$, $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{Z}^n$, $|\nu| := \nu_1 + \cdots + \nu_n$ *i* $X^\nu := X_1^{\nu_1} \ldots X_n^{\nu_n}$.

Observem que $\mathbb{T}_n$ és el subanell de l'anell de sèries formals amb coeficients a K format per les sèries convergents a tota la bola unitat $B^n := \{x \in K^n \ ;\ \|x\| \leq 1\}$, on $\|(x_1, \ldots, x_n)\| := \max_i\{x_i\}$.

Definim, per a tot element $f = \sum a_\nu X^\nu \in \mathbb{T}_n$, la seva norma com a $\|f\| := \max_\nu\{a_\nu\}$. És una comprovació immediata que ens dóna una norma no arquimediana a $\mathbb{T}_n$ estenent el valor absolut de K.

Propietats 1.1.4. *(i)* $\mathbb{T}_n$ *és una àlgebra de Banach (i.e. és completa).*

(ii) $\mathbb{T}_n$ *és noetherià, factorial i Jacobson.*

(iii) Tots els ideals de $\mathbb{T}_n$ *són tancats i tot homomorfisme de* K*-àlgebres de* $\mathbb{T}_n$ *a* $\mathbb{T}_m$ *és continu.*

Definirem ara el que seran els anells de funcions de les varietats afinoides.

Definició 1.1.5. *Una* K*-àlgebra de Banach s'anomena afinoide si existeix un* $n \in \mathbb{N}$ *i un epimorfisme de* K*-àlgebres (continu)* $f : \mathbb{T}_n \longrightarrow A$*. En altres paraules, les* K*-àlgebres afinoides són els quocients de* $\mathbb{T}_n$ *respecte a un ideal (tancat).*

Propietats 1.1.6. *(i) Tota* K*-àlgebra afinoide és noetheriana i Jacobson.*

(ii) Tot ideal d'una K*-àlgebra afinoide és tancat i el seu quocient és una* K*-àlgebra afinoide.*

(iii) La suma directa de K*-àlgebres afinoides és una* K*-àlgebra afinoide.*

(iv) Si A *i* B *són* K*-àlgebres afinoides, aleshores el completat del producte tensorial,* $A\widehat{\otimes}_K B$*, també ho és.*

Exemples 1.1.7. *Sigui* A *una* K*-àlgebra afinoide.*

(1) $A\langle X\rangle$ *i* $A\langle X, X^{-1}\rangle$ *són* K*-àlgebres afinoides per a* X *una indeterminada.*

(2) Si denotem per $f = (f_1, \ldots, f_m)$ *i* $g = (g_1, \ldots, g_n)$ *on* f_i *i* g_j *són elements de* K*, aleshores*

$$A\langle f, g^{-1}\rangle := A\langle X, Y\rangle/(X - f, gY - 1)$$

és una K*-àlgebra afinoide.*

(3) Si tenim que $f_1, \ldots, f_m$ *i* g *generen l'ideal total de* A *(i.e. no tenen zeros en comú), aleshores*

$$A\langle \frac{f_1}{g}, \ldots, \frac{f_m}{g}\rangle := A\langle X_1, \ldots, X_n\rangle/(gX_1 - f_1, \ldots, gX_n - f_n)$$

és una K*-àlgebra afinoide.*

1.2 Varietats afinoides

De la mateixa manera que les varietats afins (clàssiques) són, com a conjunts, els espectres primers de les K-àlgebres de tipus finit, les varietats afinoides són com a conjunts els espectres maximals de les K-àlgebres afinoides.

Podem començar observant que si el cos K és algebraicament tancat aleshores l'espectre maximal de $\mathbb{T}_n$ està en correspondència bijectiva de manera natural amb els punts de la bola unitat B^n, i per tant podem considerar $\mathbb{T}_n$ com a funcions de B^n. Aquest resultat és degut a un "teorema dels zeros de Hilbert" que en el nostre context es dedueix del fet que $\mathbb{T}_n$ és Jacobson.

En general podem considerar $\mathbb{T}_n$ com a funcions sobre $\mathrm{Max}(\mathbb{T}_n)$ (que és isomorfa al quocient de $B^n(\bar{K})$ respecte a l'acció del grup de Galois absolut de K) amb valors a $\bar{K}$, definint, per a tot ideal maximal $\mathfrak{m}$ i tota $f \in \mathbb{T}_n$, $f(\mathfrak{m})$ com la imatge de f en $\mathbb{T}_n/\mathfrak{m}$, que és una extensió algebraica finita de K.

Donada una àlgebra afinoide A denotarem per $\mathrm{Sp}(A)$ el seu espectre maximal. Entendrem que un morfisme entre $\mathrm{Sp}(A)$ i $\mathrm{Sp}(A')$ és sempre el morfisme induït per un morfisme de K-àlgebres de A' a A (està ben definit doncs A i A' són Jacobson!).

El següent pas és definir què entendrem per obert a $\mathrm{Sp}(A)$. Una opció que podem prendre és definir obert com a *obert Zariski*; però és clar que aquesta opció no és la que ens interessa, doncs per a la bola unitat de dimensió 1 sols obtindríem els complementaris dels conjunts finits. La segona opció és definir-los via una certa propietat universal.

Definició 1.2.1. *Un* subdomini (o subconjunt) afinoide *de* $\mathrm{Sp}(A)$ *és el subconjunt imatge d'un morfisme injectiu* $\phi : \mathrm{Sp}(A') \hookrightarrow \mathrm{Sp}(A)$ *tal que verifica: per a tota àlgebra afinoide i tot morfisme* $\psi : \mathrm{Sp}(B) \to \mathrm{Sp}(A)$ *amb imatge dins de l'imatge de* ϕ*, existeix un únic morfisme* $\psi' : \mathrm{Sp}(B) \to \mathrm{Sp}(A')$ *tal que* $\psi = \phi \circ \psi'$,

$$\begin{array}{ccc} & \phi & \\ \mathrm{Sp}(A') & \hookrightarrow & \mathrm{Sp}(A) \\ & \nwarrow & \uparrow \psi \\ & \exists! & \mathrm{Sp}(B). \end{array}$$

Exercici 1.2.2. *Comproveu que l'anàleg en la teoria d'esquemes afins de la propietat universal de la definició anterior ens caracteritza els oberts afins d'un esquema afí.*

Exemple 1.2.3. *Sigui* $X = \mathrm{Sp}(A)$ *una varietat afinoide, i considerem funcions* $g, f_1, \ldots, f_n \in A$ *sense zeros comuns, i.e. generant l'ideal total. Anomenarem*

$$X(\frac{f}{g}) := X(\frac{f_1}{g}, \ldots, \frac{f_n}{g}) := \{x \in X \ ; \ |f_i(x)| \leq |g(x)| \ , \ i = 1, \ldots, n\}.$$

Els subconjunts de X *d'aquesta forma els anomenarem* dominis racionals. *Aleshores* $X(\frac{f}{g})$ *és la imatge del morfisme natural* $\mathrm{Sp}(A\langle\frac{f}{g}\rangle) \to \mathrm{Sp}(A)$.

Exercici 1.2.4. *Definiu els* dominis de Laurent $X(f, g^{-1})$ *d'una manera anàloga als dominis racionals i comproveu que són la imatge del morfisme natural de* $\mathrm{Sp}A\langle f, g^{-1}\rangle$ *a* $\mathrm{Sp}A$, *i que verifiquen la propietat universal. Finalment proveu que els dominis de Laurent són dominis racionals.*

Propietats 1.2.5. *(i) La intersecció de dos subdominis afinoides (racionals) és un subdomini afinoide (racional), donat per* $\mathrm{Sp}(B_1) \cap \mathrm{Sp}(B_2) = \mathrm{Sp}(B_1 \widehat{\otimes}_A B_2)$ *si*

$$\mathrm{Sp}(B_1) \hookrightarrow \mathrm{Sp}(A) \hookleftarrow \mathrm{Sp}(B_1).$$

(ii) La unió disjunta de dos subdominis afinoides (racionals) és un subdomini afinoide (racional), donat per $\mathrm{Sp}(B_1) \sqcup \mathrm{Sp}(B_2) = \mathrm{Sp}(B_1 \oplus B_2)$.

(iii) Si $\mathrm{Sp}(A'') \hookrightarrow \mathrm{Sp}(A')$ *i* $\mathrm{Sp}(A') \hookrightarrow \mathrm{Sp}(A)$ *són subdominis afinoides (racionals), aleshores* $\mathrm{Sp}(A'') \hookrightarrow \mathrm{Sp}(A)$ *donat per la composició també ho és.*

(iv) L'antiimatge d'un subdomini afinoide (racional) per un morfisme de varietats afinoides és un subdomini afinoide (racional).

De fet els subdominis racionals són a la pràctica els subconjunts afinoides que hem de considerar: tots els dominis afinoides són unió finita de dominis racionals (compte que no és cert que la unió finita de racionals sigui sempre afinoide!).

Per acabar podem veure com a exemple el cas de la bola unitat:

Exemple 1.2.6. *Tot subconjunt afinoide de* $\mathbb{B}^1$ *és unió disjunta de subconjunts de la forma*

$$\overline{B}(a,r)\setminus(\bigsqcup_{i=1}^{n} B(a_i,r_i))=\mathbb{B}^1\left(\frac{X-a}{r},\left(\frac{X-a_1}{r_1}\right)^{-1},\ldots,\left(\frac{X-a_n}{r_n}\right)^{-1}\right).$$

Com ja hem vist no és cert en general que la unió de subconjunts afinoides (ni tant sols si és finita) és afinoide. El nostre objectiu és definir una "topologia" on aquests siguin els oberts. Per això necessitem el concepte de topologia de Grothendieck.

1.3 G-espais topològics

Definició 1.3.1. *Una* topologia de Grothendieck *(o G-topologia) en un conjunt* X *consisteix a donar*

(a) Un família S *de subconjunts de* X*, anomenats oberts admissibles.*

(b) Per a cada $U \in S$*, un conjunt de recobriments* $Cov(U)$ *de* U *per elements de* S *anomenats recobriments admissibles (i.e.* $\mathcal{U} = (U_i) \in Cov(U)$ *ha de satisfer que tots els* U_i *són de* S *i que* $\bigcup U_i = U$*).*

Aquestes dades han de satisfer que

(i) $U,V \in S \Longrightarrow U \cap V \in S$.

(ii) $U \in S \Longrightarrow \{U\} \in Cov(U)$.

(iii) Si $\mathcal{U} \in Cov(U)$ *i* $U,V \in S$ *amb* $V \subset U$*, aleshores* $\mathcal{U} \cap V \in Cov(V)$.

(iv) Si $\mathcal{U}_i \in Cov(U_i)$ *i* $(U_i) \in Cov(U)$*, aleshores* $\bigcup \mathcal{U}_i \in Cov(U)$.

He posat aquí sols la definició de topologia de Grothendieck on els oberts són subconjunts de X. Existeix una definició molt més general que no usarem però que la majoria ja en coneixeu exemples (la topologia étale, la topologia fpqc, etc.. sobre un esquema).

El concepte de topologia de Grothendieck està perfectament ajustat a poder definir què és un feix $\mathcal{F}$; un functor que assigna a

cada obert admissible un grup (anell, etc...) i que verifica una certa propietat respecte els recobriments: Per a tot obert admissible U i tot recobriment admissible $\{U_i\}$ de U el diagrama

$$\mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \cap U_j)$$

és exacte, on les fletxes són les induïdes per les restriccions.

Direm ara que una parella $(X, \mathcal{O}_X)$, on X es un conjunt amb una topologia de Grothendieck i $\mathcal{O}_X$ és un feix d'anells sobre X, és un G-espai localment anellat si, per a tot $x \in X$, l'anell

$$\mathcal{O}_{X,x} := \varinjlim_{U} \mathcal{O}(X),$$

on U recorre els oberts admissibles que contenen a x, és un anell local. Definim la categoria de G-espais localment anellats com la categoria per a la qual els morfismes són parelles $(\phi, \psi) : (X, \mathcal{O}_X) \longrightarrow (Y, O_Y)$, on $\phi : X \to Y$ és un morfisme continu de G-espais topològics i $\psi : \mathcal{O}_Y \to \phi_* \mathcal{O}_X$ és un morfisme de feixos d'anells sobre Y tal que el morfisme induït

$$\psi_x : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$$

és un morfisme local (i.e. envia l'ideal maximal a l'ideal maximal) per a tot $x \in X$. Recordem que el feix $\phi_* \mathcal{O}_X$ és el que envia a tot V obert admissible de Y l'anell $\mathcal{O}_X(\phi^{-1}(V))$.

Donada una àlgebra afinoide A, definim ara la següent G-topologia a $X = \mathrm{Sp}(A)$: els oberts admissibles són els subconjunts afinoides; els recobriments admissibles són els recobriments **finits** formats per subconjunts afinoides. Aquesta topologia l'anomenarem topologia dèbil de X. Una altra opció, que és la seguida en el llibre **2**, és definir la topologia dèbil amb dominis racionals enlloc de dominis afinoides; les topologies obtingudes són però equivalents.

Finalment, definim el pre-feix $\mathcal{O}_X$ com el que assigna a cada obert afinoide $\mathrm{Sp}(A') \hookrightarrow \mathrm{Sp}(A)$ l'àlgebra A'.

Teorema 1.3.2. (d'aciclicitat de Tate) *$\mathcal{O}_X$ és un feix.*

Tenim aleshores

Proposició 1.3.3. *Donada una k-àlgebra afinoide A, la parella* $(X = \mathrm{Sp}(A), \mathcal{O}_X)$ *és un G-espai localment anellat. El functor que assigna a cada k-àlgebra afinoide aquest G-espai localment anellat és plenament fidel.*

De fet la topologia dèbil que hem introduït no és "prou bona" doncs no es comporta bé respecte recobriments: sabent la G-topologia de cada obert d'un recobriment admissible no determinem la G-topologia de l'espai total. Per a obtenir la G-topologia forta que és a la pràctica la que utilitzarem necessitem engrandir lleugerament la nostra G-topologia.

Direm que una G-topologia es comporta bé respecte els recobriments si verifica:

(G0) $\emptyset$ i X són oberts admissibles de X.

(G1) Si V és un subconjunt d'un obert admissible U tal que existeix un recobriment per oberts admissibles $\{U_i\}$ de U que verifiquen que $V \cap U_i$ és admissible per a tot i, aleshores V és admissible.

(G2) Si $\{U_i\}$ és un recobriment d'un obert admissible U tal que tots els U_i són admissibles i hi ha un refinament admissible de $\{U_i\}$, aleshores $\{U_i\}$ és admissible.

Aquestes condicions són necessàries per assegurar que la G-topologia en X ve determinada per la G-topologia d'un recobriment admissible de X. Per aconseguir que la G-topologia de les varietats afinoides verifiqui les condicions (G1) i (G2) utilitzem un procediment per "engrandir" G-topologies que ens dóna una G-topologia determinada per la dèbil i que anomenarem la G-topologia forta (o G-topologia) de les varietats afinoides. Aquesta G-topologia és més fina que la topologia dèbil, té com a base d'oberts els subdominis afinoides i tots els seus recobriments admeten un refinament per recobriments finits de subdominis afinoides. A més el feix $\mathcal{O}_X$ per a la topologia dèbil estén de manera única a un feix per a la topologia forta, que denotarem igualment per $\mathcal{O}_X$. A més verifica:

Lema 1.3.4. *(i) Sigui X una varietat afinoide. Aleshores tota unió finita de subdominis afinoides és un obert admissible (per a la G-topologia forta), i tot recobriment finit per a subdominis afinoides d'un subconjunt d'aquest tipus és admissible.*

(ii) Per a tot element $f \in A$, és admissible tota unió finita d'oberts del tipus $\{x \in X \ ; \ |f(x)| < 1\}$, $\{x \in X \ ; \ |f(x)| > 1\}$, $\{x \in X \ ; \ |f(x)| > 0\}$.

Com a conseqüència podem veure que tot obert Zariski és un obert admissible per a la G-topologia, i que tot recobriment per oberts Zariski és un recobriment admissible (recordem que les àlgebres afinoides són noetherianes).

Ara, amb aquesta G-topologia s'ha d'anar molt en compte: per exemple, si $X = \mathbb{B}^1$, les boles obertes i tancades i els seus complementaris són oberts admissibles, però no és cert que el recobriment format per una bola oberta i el seu complementari sigui admissible.

Observem que amb aquesta topologia ja hem solucionat els dos problemes mencionats al principi: els nostres espais ja no són totalment disconexos: de fet tenim que una varietat afinoide és connexa (respecte a la G-topologia) si ho és respecte a la topologia de Zariski. I el teorema d'aciclicitat de Tate ens resol el problema 2.

1.4 Varietats analítiques rígides

Podem ara imitar el que es fa amb la teoria d'esquemes definint una varietat analítica rígida com un espai topològic (de Grothendieck) localment anellat tal que localment és unió de varietats afinoides.

Definició 1.4.1. *Una* varietat analítica rígida *sobre K és un G-espai localment anellat $(X, \mathcal{O}_X)$ sobre K tal que:*

(i) La G-topologia de X verifica (G0), (G1) i (G2).

(ii) X admet un recobriment admissible $\{U_i\}$ tal que $(U_i, \mathcal{O}_{X|U_i})$ és una varietat afinoide per a tota i.

Usant aquesta definició tenim per exemple que podem construir K-varietats analítiques enganxant varietats afinoides mitjançant interseccions prescrites (com en el cas dels esquemes), i podem definir els morfismes analítics localment.

Proposició 1.4.2. *Donades X_i varietats analítiques juntament amb subvarietats obertes $X_{ij} \subseteq X_i$ i isomorfismes $\varphi_{ij} : X_{ij} \simeq X_{ji}$, verificant que*

(i) $\varphi_{ij} \circ \varphi_{ji} = id$, $X_{ii} = X_i$ *i* $\varphi_{ii} = id$.

(ii) El morfisme φ_{ij} *indueix morfismes* $\varphi_{ijl} : X_{ij} \cap X_{il} \to X_{ji} \cap X_{jl}$ *tal que* $\varphi_{ijl} = \varphi_{lji} \circ \varphi_{ilj}$.

existeix una única varietat analítica (fora d'isomorfisme) construïda enganxant les varietats X_i *via la identificació de* X_{ij} *amb* X_{ji}.

Observem que la unicitat és deguda al fet que les nostres varietats verifiquen (G0), (G1) i (G2) (aquest és el motiu principal pel qual hem hagut d'"engrandir" la nostra topologia dèbil).

També tenim productes fibrats, feixos coherents, immersions tancades, morfismes finits, morfismes separats, morfismes propis, etc.

Exemple 1.4.3. L'espai afí $\mathbb{A}^n$. *La idea per "construir" l'espai afí com a varietat afinoide és recobrir-lo per boles tancades centrades en el zero amb radi creixent. Prenem* $\pi \in K$ *amb valor absolut* $c := |\pi| > 1$ *i considerem* A_i *la* k*-àlgebra de les sèries convergents en la bola de radi* c^i *i centre* 0 *a* $\bar{K}^n$, *i.e.*

$$A_i := K\langle \pi^{-i} X_1, \ldots, \pi^{-i} X_n \rangle$$

Tenim una inclusió natural de A_{i+1} *dins* A_i *que ens identifica* $\mathrm{Sp}(A_i)$ *com a subdomini afinoide de* $\mathrm{Sp}(A_{i+1})$. *Fem servir aquestes inclusions per "enganxar" les varietats afinoides* $\mathrm{Sp}(A_i)$ *i l'espai analític obtingut l'anomenarem* $(\mathbb{A}^n)^{an}$, *o* $\mathbb{A}^n$ *quan quedi clar que ens estem referint a l'espai afí com a espai analític.*

Exemple 1.4.4. L'espai projectiu $\mathbb{P}^n$. *La idea és recobrir-lo per* $n+1$ *còpies de la bola unitat* $\mathbb{B}^n$. *Prenem*

$$X_i := \mathrm{Sp}\left(k\left\langle \frac{\zeta_0}{\zeta_i}, \ldots, \frac{\zeta_n}{\zeta_i} \right\rangle\right),$$

considerant ζ_j/ζ_i *com a indeterminades si* $j \neq i$ *i com a* 1 *si* $j = i$. *Ara, per a tota* i *i* j *definim* X_{ij} *com el subdomini racional de* X_i *que "inverteix"* ζ_j/ζ_i, *o sigui*

$$X_{ij} := X\left(\left(\frac{\zeta_j}{\zeta_i}\right)^{-1}\right).$$

Identifiquem X_{ij} *amb* X_{ji} *a través de l'isomorfisme natural, i enganxem les varietats* X_i *mitjançant aquestes identificacions.*

Exemple 1.4.5. Els tors analítics. *Sigui $q \in K^*$, $0 < |q| < 1$, i considerem el G-espai topològic quocient $\mathbb{G}_m^{an}/q^{\mathbb{Z}}$, on $\mathbb{G}_m^{an}$ el prenem com la subvarietat oberta Zariski de $\mathbb{A}^1$ obtinguda traient-ne l'origen, i on $q^{\mathbb{Z}}$ denota el subgrup de K^* generat per q i actuant a $\mathbb{G}_m$ per "multiplicació". Si considerem els subdominis racionals de $\mathbb{B}^1$ donats per*

$$X_1 := \left\{ x \in \mathbb{B}^1 \mid |q| \leq |x| \leq |q|^{\frac{1}{2}} \right\}, X_2 := \left\{ x \in \mathbb{B}^1 \mid |q|^{\frac{1}{2}} \leq |x| \leq 1 \right\},$$

podem veure fàcilment que el morfisme quocient ens els identifica amb un recobriment per oberts admissibles de $\mathbb{G}_m^{an}/q^{\mathbb{Z}}$ que són varietats afinoides, i per tant ens el doten d'una estructura de varietat analítica. Aquesta varietat és de fet l'analificació d'una corba el·líptica, la corba de Tate. Nota històrica: l'article original de Tate on es desenvolupà l'anàlisi rígida tenia com a objectiu donar un sentit "geomètric" a $\mathbb{G}_m/q^{\mathbb{Z}}$.

Utilitzant la mateixa idea que en el primer exemple podem definir una estructura de varietat analítica a qualsevol varietat afí (o en general tot K-esquema afí de tipus finit, i.e. l'espectre d'una K-àlgebra finitament generada). Utilitzant després que els oberts Zariski són oberts admissibles per la G-topologia analítica podem construir tota varietat algebraica (o en general tot K-esquema localment de tipus finit) com a varietat analítica recobrint-la per varietats afins. Es pot veure fàcilment reduint-nos al cas de l'espai afí que tot morfisme com a esquemes ens dóna un morfisme com a varietats analítiques. Així tenim que

Teorema 1.4.6. *La correspondència $X \rightsquigarrow X^{an}$ descrita a dalt ens dóna un functor*

$$\left\{ \begin{array}{l} K\text{-esquemes localment} \\ \text{de tipus finit} \end{array} \right\} \rightsquigarrow \{K\text{-varietats analítiques rígides}\}.$$

A més és verifica que si un esquema localment de tipus finit és connex (regular, reduït, separat, etc.), la seva analificació és també connexa (regular, reduïda, separada, etc.).

Finalment, tenim també un teorema GAGA com en el cas de la relació entre varietats analítiques sobre $\mathbb{C}$ i varietats algebraiques.

Teorema 1.4.7. *(i) Sigui X una varietat projectiva i sigui $f : Z \to X^{an}$ un morfisme* finit *entre dues varietats analítiques. Aleshores existeix una varietat projectiva Y i un morfisme finit $g : Y \to X$ de manera que $Y^{an} \cong Z$ i $g^{an} \cong f$.*

(ii) Siguin X i Y dues varietats projectives i sigui $f : X^{an} \to Y^{an}$ un morfisme com a varietats analítiques. Aleshores existeix un morfisme d'esquemes $g : X \to Y$ tal que $g^{an} = f$.

La demostració d'aquest teorema (vegeu **3**) és anàloga a la demostració del teorema GAGA donada per Serre. De fet també es certa la versió de Grothendieck utilitzant esquemes propis enlloc d'esquemes projectius.

Com a conseqüència tenim el teorema de Chow.

Corol.lari 1.4.8. *Sigui X una varietat projectiva i sigui V un subconjunt analític de X^{an}, i.e. el subconjunt format localment pels zeros d'un ideal. Aleshores V és l'analificació d'un subesquema tancat de X.*

Finalment mencionarem que hi ha una relació molt estreta (observada per primer cop per Raynaud) entre la geometria rígida analítica i la geometria formal sobre l'anell de valoració del cos K.

Bibliografia

1. S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean Analysis*, Springer-Verlag, 1984.

2. J. Fresnel, M. van der Put, *Géométrie Analytique Rigide et applications*, Prog. in Math. **18**, Birkhäuser, 1981.

3. U. Köpf, Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen, Schriftenreihe des Math. Inst. Univ. Münster, serie 2, Heft **7**, (1974).

4. J. Tate, Rigid analytic spaces, Invent. Math. **12**, (1971), pag 257–289.

Capítol 2

1/2 Teorema d'existència de Riemann amb acció de Galois

Bernat Plans

2.1 Introducció

Convenim que tots els cossos que considerarem estan continguts en un cos universal Ω algebraicament tancat.

Donat un cos κ i un conjunt tancat finit $S \subset \mathbb{P}^1_\kappa$, notem $U := \mathbb{P}^1_\kappa \backslash S$ i $\overline{U} := U \times_\kappa \overline{\kappa}$. Considerem una funció racional $t \in \kappa(\mathbb{P}^1_\kappa)$ tal que $\kappa(\mathbb{P}^1_\kappa) = \kappa(t)$ i S no talla el pol de t. Mitjançant t, identificarem $\mathbb{P}^1_\kappa(M)$ amb $M \cup \{\infty\}$, per a qualsevol $M \subset \Omega$.

Es té una successió exacta

$$1 \to \Pi_1(\overline{U}) \to \Pi_1(U) \xrightarrow{\rho_U} G_\kappa \to 1$$

on el grup fonamental $\Pi_1(U)$ es pot definir com $Gal(\kappa(U)^S|\kappa(U))$, amb $\kappa(U)^S$ la màxima extensió de $\kappa(U) = \kappa(t)$ no ramificada fora de S (anàlogament $\Pi_1(\overline{U})$). A més, es tracta d'una successió exacta

split, donat que $U(\kappa) \neq \emptyset$ (qualsevol $s_0 \in U(\kappa)$ defineix una inclusió $\kappa(U)^S \subset \overline{\kappa}((t-s_0))$, donant lloc a una secció $G_\kappa \to \Pi_1(U)$ de ρ_U).

Quan $\overline{\kappa} = \mathbb{C}$, el Teorema d'existència de Riemann ens diu que el grup fonamental algebraic $\Pi_1(\overline{U})$ és isomorf a la compleció profinita del grup fonamental topològic $\Pi_1^{top}(\overline{U})$. Concretament, es té:

Si $\overline{S} = \{s_1, \ldots, s_{n_S}\}$, aleshores $\Pi_1(\overline{U})$ és isomorf a

$$< g_1, \ldots, g_{n_S} \; ; \; g_1 \ldots g_{n_S} = 1 >,$$

grup profinit lliure en $n_S - 1$ generadors.

A més, podem triar aquest isomorfisme de manera que g_i sigui element d'inèrcia en s_i.

En canvi, l'estructura de $\Pi_1(U)$ és desconeguda. En general, no es coneix tampoc l'estructura de $\Pi_1(U)$ relativa a la de G_κ: sabem que $\Pi_1(U)$ és un producte semidirecte de $\Pi_1(\overline{U})$ i G_κ però no sabem construir una secció de ρ_U que ens permeti descriure l'acció.

Ens agradaria trobar quocients " interessants" $\Pi_1(\overline{U}) \to \overline{\Pi}$ que donessin lloc a quocients

$$\begin{array}{ccccccccc} 1 & \to & \Pi_1(\overline{U}) & \to & \Pi_1(U) & \to & G_\kappa & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & \overline{\Pi} & \to & G_\kappa \ltimes \overline{\Pi} & \to & G_\kappa & \to & 1 \end{array}$$

de manera que sabéssim descriure l'acció de G_κ en $\overline{\Pi}$ (i, per tant, coneguéssim l'estructura del quocient $G_\kappa \ltimes \overline{\Pi}$ de $\Pi_1(U)$ en termes de G_κ i $\overline{\Pi}$).

El nostre objectiu és demostrar un resultat de Pop ([Pop1]) en aquest sentit, sota certes hipòtesis sobre κ (i sobre S).

2.2 Enunciat del resultat

Conservem els convenis i notacions de la Introducció.

Sigui κ un cos complet respecte una valoració v de rang 1 (v també

denotarà la valoració de $\overline{\kappa}$) tal que $car(\kappa) = car(\kappa v)$, on κv és el cos residual de v.

Conservarem aquestes hipòtesis fins al final.

Comentari 2.2.1.

i) Per definició, que v sigui de rang 1 vol dir que el grup de valors $v(\kappa^*)$ satisfà el postulat d'Arquímedes; aquesta condició equival a que $v(\kappa^*)$ s'identifiqui amb un subgrup de $(\mathbb{R}, +)$. Així, podem pensar que κ és un cos complet respecte un valor absolut no arquimedià.

ii) El resultat que volem demostrar és cert també per a cossos més generals. Per exemple, del cas complet es pot deduir el resultat per a κ henselià respecte v, usant le teoria d'especialització de Grothendieck. Tampoc cal suposar que estem en el cas d'igual característica, però en aquesta situació el resultat es simplifica lleugerament. Les nostres hipòtesis inclouen la situació en la qual volem aplicar el resultat ([Pop2]).

Definició 2.2.2. *Direm que un conjunt tancat finit $S \subset \mathbb{P}^1_\kappa$ és* **v-ajustat en parells** *si els punts de $\overline{S}$ es poden distribuir en n parells $p_i := (x_i, y_i)$ tals que:*

$$\begin{cases} G_\kappa \text{ permuta els } p_i \text{ (conservant l'ordre dins de cada parell)} \\ v(x_i - y_i) > v(x_i - x_j),\ \forall j \neq i \end{cases}$$

En particular, $\overline{S}$ és un conjunt de cardinal parell $2n$.

El resultat que volem demostrar és:

Teorema 2.2.3. *(1/2 Teorema d'existència de Riemann amb acció de Galois)*

Si κ és un cos complet respecte una valoració v de rang 1 i $S \subset \mathbb{P}^1_\kappa$ és un conjunt tancat finit v-ajustat en parells, aleshores:

la successió exacta

$$1 \to \Pi_1(\overline{U}) \to \Pi_1(U_\kappa) \to G_\kappa \to 1$$

admet de forma canònica el quocient

$$1 \to \overline{\Pi} \to G_\kappa \ltimes \overline{\Pi} \to G_\kappa \to 1$$

on $\overline{\pi} :=< g_{p_1}, \ldots, g_{p_n} >$ *és el grup profinit lliure en* n *elements i el producte semidirecte correspon a l'acció de* G_κ *en* $\overline{\Pi}$ *definida per:*

$(g_{p_i})\sigma := (g_{\sigma^{-1}p_i})^{\chi(\sigma^{-1})}$, *amb* $\chi : G_\kappa \to \hat{\mathbb{Z}}^*$ *el caràcter ciclotòmic.*

A més, g_{p_i} *és un element d'inèrcia en* x_i *i* y_i, $\forall i$.

Per a demostrar el Teorema realitzarem els processos següents, controlant la ramificació i l'acció de G_κ en cadascun d'ells:

- construcció de recobriments cíclics convenients de $\mathbb{P}^1_\lambda$, per a $\lambda|\kappa$ normal finita prou gran (teories de Kummer i Artin-Schreier)
- per a cada $m \in \mathbb{Z}_{>0}$ i per a cada quocient finit (prou gran) C de $\Pi^{(m)} :=< g_{p_1}, \ldots, g_{p_n} \ ; \ {g_{p_i}}^m = 1 >$, construcció d'un C-recobriment de $\mathbb{P}^1_\lambda$, per a $\lambda|\kappa$ normal finita prou gran (enganxant recobriments cíclics rígids i usant GAGA rígid)
- passos al límit primer respecte C (amb m fixat) i després respecte m (functorialitat dels processos anteriors)

Comentari 2.2.4. Usant les mateixes eines que Pop i controlant els cossos de definició dels recobriments, Liu ja havia demostrat ([Liu]):

> si κ és cos complet respecte un valor absolut no arquimedià, aleshores tot grup finit G és quocient κ-racional de $\pi_1(\overline{U})$, per algun S convenient; és a dir, la successió exacta
>
> $$1 \to \Pi_1(\overline{U}) \to \Pi_1(U) \to G_\kappa \to 1$$
>
> admet un quocient
>
> $$1 \to G \to G \times G_\kappa \to G_\kappa \to 1$$
>
> Equivalentment, tot grup finit G és isomorf al grup de Galois d'una extensió regular de $\kappa(t)$.

Aquest resultat ja havia estat demostrat per Harbater ([Ha]) usant geometria formal; essencialment, Liu interpreta la demostració de Harbater en termes de geometria analítica rígida.

2.3 Construcció de recobriments cíclics

Conservem les hipòtesis i notacions de l'apartat anterior.

En tot l'apartat (i en el següent), suposarem $m \in \mathbb{Z}_{>0}$ fixat.

Per a simplificar, suposarem també $car(\kappa) = 0$.

Obs.: en el cas de característica positiva, a més de la teoria de Kummer, caldria usar la teoria d'Artin-Schreier.

Sigui $\lambda|\kappa$ una extensió de Galois finita per a la qual $\overline{S} \subset \mathbb{P}^1_\kappa(\lambda)$ i $\mu_m \subset \lambda$.

$$\text{Notem } \begin{cases} K := \kappa(t) \\ L := \lambda(t) \\ G := Gal(\lambda|\kappa) = Gal(L|K) \end{cases}$$

Comentari 2.3.1. *(Teoria de Kummer)*
Es té un isomorfisme canònic de G-mòduls:

$$\delta : L^*/m(-1) \overset{\cong}{\to} X_m(G_L) := Hom(G_L, \mathbb{Z}/m\mathbb{Z})$$

Recordem que, si A és un G_κ-mòdul de m-torsió, definim

$$A(r) := \begin{cases} A \otimes \mu_m^{\otimes r}, \text{ si } r \geq 0 \\ A \otimes Hom(\mu_m^{\otimes r}, \mathbb{Z}/m\mathbb{Z}), \text{ si } r < 0 \end{cases}$$

entenent que G_κ actua en μ_m pel caràcter ciclotòmic.
Com a grups abelians A i $A(r)$ són isomorfs però, fixat un isomorfisme, l'acció de G_κ en $A(r)$ correspon a l'acció en A multiplicada per la r-èssima potència del caràcter ciclotòmic.

Per a cada $i \in \{1, \ldots, n\}$, considerem l'extensió cíclica $L_i|L$ definida per $\chi_i := \delta(\frac{t-y_i}{t-x_i})$ i notem $G_i := Gal(L_i|L)$.

Per definició, $G_i \cong \mathbb{Z}/m\mathbb{Z}$.

Proposició 2.3.2.

a) *$\forall i$, l'extensió $L_i|L$ és regular sobre λ (i.e. $\overline{\lambda} \cap L_i = \lambda$), ramificada només en x_i i y_i i totalment ramificada.*

b) *Notant $L_0 := \prod_i L_i$, es té un isomorfisme canònic $Gal(L_0|L) \cong \prod_i G_i$. A més, $L_0|K$ és de Galois i, per tant, es té una successió exacta canònica*

$$1 \to Gal(L_0|L) \to Gal(L_0|K) \to G \to 1$$

c) *La successió exacta de b) defineix (per conjugació a $Gal(L_0|K)$) una única acció de G en $Gal(L_0|L) \cong \prod_i G_i$.*

A més, existeixen generadors g_{p_i} de G_i de manera que aquesta acció ve donada per:

$(g_{p_i})\sigma = (g_{\sigma^{-1}p_i})^{\chi(\sigma^{-1})}$, on $\chi : G \to (\mathbb{Z}/m\mathbb{Z})^*$ és el caràcter ciclotòmic.

DEMOSTRACIÓ.

a) L'afirmació sobre la ramificació és conseqència directa de les definicions. El fet que $L_i|L$ sigui totalment ramificada en x_i ens diu que $L_i|\lambda$ és regular.

b) Per a), les extensions $\{L_i|L\}_i$ tenen ramificació disjunta i $L_0|L$ no admet subextensions no ramificades (donat que $L_0|\lambda$ és regular). Per tant, $Gal(L_0|L) \cong \prod_i G_i$.

D'altra banda, S v-ajustat $\Rightarrow$ G_K permuta els cossos $\{L_i\}_i \Rightarrow$ $L_0|K$ de Galois.

c) La primera afirmació és clara, per ser $Gal(L_0|L)$ abelià.

De la teoria de Kummer deduïm un isomorfisme canònic de G-mòduls

$X_m(Gal(L_0|L)) =< \chi_1, \dots, \chi_n > \cong \bigoplus_i (p_i\mathbb{Z}/m(-1))$
on G actua en els $\{p_i\}_i$ per $\sigma p_i := (\sigma(x_i), \sigma(y_i))$.

Per tant, tenim un isomorfisme de G-mòduls

$Gal(L_0|L) \cong X_m(\bigoplus_i p_i\mathbb{Z}/m(-1))$.

Només cal agafar, per a cada i, g_{p_i} corresponent al caràcter tal que $p_j \mapsto \delta_{ij}$. □

2.4 Enganxant recobriments cíclics convenientment

Conservem les hipòtesis i notacions dels apartats anteriors; en particular, recordem que hem fixat $m \in \mathbb{Z}_{>0}$. Convenim, però, que el cos λ no està fixat; admetrem qualsevol cos satisfent les hipòtesis de l'apartat anterior. Analític sempre voldrà dir rígid analític.

Per a $i \in \{0, \dots, n\}$, sigui $\phi_i : X_i \to \mathbb{P}^1_\lambda$ la normalització de $\mathbb{P}^1_\lambda$ en $L_i|L$.

Comentari 2.4.1. Per la proposició anterior, X_i és geomètricament íntegre (equival a $L_i|\lambda$ regular) i tenim un isomorfisme canònic $Aut_{\mathbb{P}^1_\lambda}(X_i) \cong G_i^{op}$; així, via el functor d'analitificació, G_i^{op} és de manera canònica un grup de λ-automorfismes analítics de X_i^{an}. Per a simplificar les notacions, no distingirem entre un grup i el seu oposat; decidim si es tracta d'un o de l'altre segons el context (és a dir, segons els objectes sobre els quals actua).

Donat $\gamma := (\gamma_1, \dots, \gamma_n) \in (v(\lambda))^n$, considerem el recobriment admissible $\coprod_\gamma = \{U\} \cup \{U_i\}_i$ de $(\mathbb{P}^1_\lambda)^{an}$ definit per:

$$\begin{cases} U_i : \text{disc tancat de centre } x_i \text{ i radi } \gamma_i \\ U := (\mathbb{P}^1_\lambda)^{an} \backslash (\cup_i U_i^0), \text{ on } U_i^0 \text{ és el disc obert corresponent} \end{cases}$$

$$\text{Notem } \begin{cases} \partial U_i := U \cap U_i \\ V_i := \phi_i^{-1}(U_i) \\ \partial V_i := \phi_i^{-1}(\partial U_i). \end{cases}$$

Proposició 2.4.2. *(existència de recobriment admissible convenient)*

Per a λ prou gran, existeix γ tal que $\coprod_\gamma$ satisfà:

a) Els oberts U_i són disjunts dos a dos, U_i és l'únic obert del recobriment on ϕ_i^{an} ramifica i V_i és (obert admissible de X_i^{an}) connex i G_i-invariant.

b) $\phi_i^{-1}(\mathbb{P}^1_\lambda \backslash U_i^0)$ és obert admissible G_i-invariant de X_i^{an}. A més, és isomorf (com a λ-espai analític) a $G_i \times (\mathbb{P}^1_\lambda \backslash U_i^0)$, unió disjunta de $m = \sharp(G_i)$ còpies de $\mathbb{P}^1_\lambda \backslash U_i^0$, amb l'acció: $g_i(g_i', (.)) = (g_i g_i', (.))$.

c) El recobriment $\coprod_\gamma$ *és invariant per* G*, com a grup de* κ*-automorfismes analítics de* $(\mathbb{P}^1_\lambda)^{an}$*. De fet,* G *permuta els* $\{U_i\}_i$ *i deixa invariant* U*.*

d) Existeix una secció $\alpha_0 : G \to Gal(L_0|K)$ *de la projecció canònica* $Gal(L_0|K) \to G$ *tal que, per a cada* i*:*

$\exists\, \partial V_{i,e}$ *component connexa de* ∂V_i *invariant per* $Stab_{\alpha_0(G)}(L_i)$*.*

DEMOSTRACIÓ.

És clar que, per a λ prou gran, existeix $\gamma \in (v(\lambda))^n$ tal que:

$\forall i\,, \quad v(x_i - y_i) > \gamma_i > v(x_i - x_j)$, si $j \neq i$.

Redefinim γ de manera que $\gamma_i = \gamma_j$, sempre que p_i i p_j siguin G_κ-conjugats.

a) Que V_i sigui connex és conseqüència del fet que $x_i \in U_i$ és totalment ramificat per ϕ_i i de la G_i-invariància de V_i (per tant, $\phi_i^{-1}(x_i)$ pertany a totes les components connexes de V_i).

b) Sigui $c_i \in \lambda$ tal que $v(c_i) = \gamma_i$.

Com a sèrie en $(\frac{t-x_i}{c_i})^{-1}$, $(\frac{t-y_i}{t-x_i})^{1/m} = (1 + \frac{x_i-y_i}{c_i}(\frac{t-x_i}{c_i})^{-1})^{1/m}$ pertany a l'àlgebra de Tate de $\mathbb{P}^1_\lambda \backslash U_i^0$ (per hipòtesi sobre γ_i). Tenint en compte que λ conté les arrels m-èssimes de la unitat, obtenim l'isomorfisme desitjat.

c) Per ser S v-ajustat, G permuta els $\{x_i\}_i$. Tal com hem agafat γ, és clar que G permuta els $\{U_i\}_i$.

d) Sigui $\mathcal{P}$ la plaça κ-racional de K corresponent al divisor de pols de t i sigui $\overline{\mathcal{P}}$ una plaça de $\overline{K}$ sobre $\mathcal{P}$. Es té una successió exacta split

$$1 \to I(\overline{\mathcal{P}}|\mathcal{P}) \to D(\overline{\mathcal{P}}|\mathcal{P}) \xrightarrow{\Pi_\mathcal{P}} G_\kappa \to 1.$$

Si $\alpha_\mathcal{P}$ és una secció de $\Pi_\mathcal{P}$ i Π_0 és la projecció $G_K \to Gal(L_0|K)$, aleshores $\Pi_0 \circ \alpha_\mathcal{P}$ defineix una secció α_0 de $Gal(L_0|K) \to G$ (sempre que λ sigui prou gran).

Sigui $H_i := \alpha_0^{-1}(Stab_{\alpha_0(G)}(L_i))$ i $\lambda_i := \lambda^{H_i}$. Com a grup de λ_i-automorfismes analítics de X_i^{an}, H_i permuta les components connexes de $\phi_i^{-1}(\mathbb{P}^1_\lambda \backslash U_i^0)$.

Aquesta acció es pot llegir en l'acció de H_i en les solucions de $T^m = u_i$. Pel Lema de Hensel, aquesta equació té solucions a $\lambda_i[[1/t]]$ i, per tant, alguna de les components connexes ha de ser H_i-invariant. En particular, obtenim el resultat desitjat.

□

Comentari 2.4.3. Per l'apartat b) de la Proposició 2.4.2, ∂V_i és obert admissible de X_i^{an} (i de V_i) G_i-invariant i isomorf a $G_i \times \partial U_i$. A més, aquest isomorfisme defineix un recobriment admissible i G_i-invariant de ∂V_i, on els oberts són les components connexes de ∂V_i (totes elles isomorfes a ∂U_i).

Triant convenientment els $\{\partial V_{i,e}\}_i$ de l'apartat d) i notant $\partial V_{g_i} := g_i(\partial V_{i,e})$, l'acció de G (via α_0) en $\{\partial V_i\}_i$ satisfà:

$$\sigma(\partial V_{g_i}) = \partial V_{\sigma_{g_i}}, \forall \sigma \in G.$$

Teorema 2.4.4. *("enganxant")*

Sigui $\Pi^{(m)} :=< g_{p_1}, \ldots, g_{p_n};\ g_{p_i}^m = 1 >$ *el producte profinit lliure dels* $\{G_i\}_i$ *i suposem* λ *com a la Proposició 2.4.2. Si* $\Pi^{(m)} \xrightarrow{\varphi} C$ *és un quocient finit tal que la projecció canònica* $\Pi^{(m)} \to \prod_i G_i$ *factoritza per* φ*, aleshores:*

existeix $L_C|L$ *extensió de Galois tal que:*

a) $Gal(L_C|L) \cong C$ *i* $L_C|\lambda$ *és regular.*

b) $L_C|K$ *és de Galois i la successió exacta*

$$1 \to Gal(L_C|L) \to Gal(L_C|K) \to G \to 1$$

és canònicament isomorfa a

$$1 \to C \to G \ltimes C \to G \to 1$$

on el producte semidirecte correspon a l'acció de G *en* C *determinada per l'acció en* $\{G_i\}_i$ *de la proposició 2.3.2.*

DEMOSTRACIÓ.
La secció canònica de la projecció $\Pi^{(m)} \to G_i$ determina una secció $G_i \xrightarrow{\cong} \mathcal{C}_i \subset C$ de $1 \to C_i \to C \to G_i \to 1$.

Aquesta secció defineix una acció de $\mathcal{C}_i$ en qualsevol G_i-objecte.

Tenim una C-acció en els λ-espais analítics:

$$\begin{cases} \mathcal{U} := C \times U : & h(g,(.)) = (hg,(.)) \\ \mathcal{V} := \coprod_i (C_i \times V_i) : & h(h_i,(.)) = (h_i', g_i'(.)) \end{cases} \text{ amb } h_i' \in C_i,\ g_i' \in \mathcal{C}_i \text{ tals que } hh_i = h_i' g_i'.$$

Definim Y^{an} com el λ-espai analític resultant d'enganxar $\mathcal{U}$ i $\mathcal{V}$ per identificació (via ϕ_i) de $\{h_i\} \times \partial V_{g_i}$ amb $\{h_i g_i\} \times \partial U_i$.

Fet : Y^{an} és connex.

Enganxant de manera natural els morfismes analítics

$$\begin{cases} \mathcal{U} \xrightarrow{id_U} U \\ \mathcal{V} \xrightarrow{\coprod_i \phi_i} \coprod_i U_i \end{cases}$$

obtenim un recobriment analític connex $Y^{an} \xrightarrow{\phi^{an}} (\mathbb{P}^1_\lambda)^{an}$.

Com que l'enganxament és compatible amb l'acció de C, tenim un isomorfisme canònic $C \cong Aut_{(\mathbb{P}^1_\lambda)^{an}}(Y^{an})$.

Per GAGA, ϕ^{an} és l'analitificació d'un recobriment de Galois $Y \xrightarrow{\phi} \mathbb{P}^1_\lambda$ de grup C, amb Y geomètricament íntegre (per ser $Y^{an}(\lambda) \neq \emptyset$).

Sigui $L_C := \lambda(Y)|L$ l'extensió de cossos de funcions corresponent a ϕ.

L'apartat a) és clar.

Demostrem b).

Recordem que, com a grup de κ-automorfismes analítics, G permuta els $\{V_i\}_i$ i deixa invariant U; d'altra banda, l'acció de G en $\prod_i G_i$ via α_0 defineix accions en C i en $\{C_i\}_i$. Així, G actua

$$\begin{cases} \text{en } \mathcal{U} : & \sigma(g,(.)) = ({}^\sigma g, \sigma(.)) \\ \text{en } \mathcal{V} : & \sigma(h_i,(.)) = ({}^\sigma h_i, \sigma(.)). \end{cases}$$

Fet: Pensant C com a grup de κ-automorfismes analítics de $\mathcal{U}$, es tenen igualtats:
${}^{\sigma}g = \sigma g \sigma^{-1}$, $\quad \forall g \in C,\ \forall \sigma \in G$.
El mateix resultat també és cert a $\mathcal{V}$.

En particular, el grup de κ-automorfismes analítics d'$\mathcal{U}$ generat per C i G és canònicament isomorf a $G \ltimes C$ i el mateix val a $\mathcal{V}$. Pel Comentari 2.4.3, l'acció de G també és compatible amb l'enganxament fet; G actua canònicament a Y^{an} i la successió exacta

$$1 \to Aut_{(\mathbb{P}^1_\lambda)^{an}}(Y^{an}) \to Aut_{(\mathbb{P}^1_\kappa)^{an}}(Y^{an}) \to Aut_{(\mathbb{P}^1_\kappa)^{an}}((\mathbb{P}^1_\lambda)^{an}) \to 1$$

és canònicament isomorfa a

$$1 \to C \to G \ltimes C \to G \to 1\ .$$

Per GAGA, aquesta successió és canònicament isomorfa a

$$1 \to Aut_{\mathbb{P}^1_\lambda}(Y) \to Aut_{\mathbb{P}^1_\kappa}(Y) \to Aut_{\mathbb{P}^1_\kappa}(\mathbb{P}^1_\lambda) \to 1$$

i això demostra l'apartat b). □

2.5 Conclusió

Conservem les hipòtesis i notacions dels apartats anteriors, però ja no suposem m fixat; indiquem la dependència de m per als objectes de l'apartat anterior mitjançant superíndexs.

Teorema 2.5.1. *Sigui $m \in \mathbb{Z}_{>0}$. Si $\lambda^{(m)}$ és com en el teorema anteior, aleshores existeix $\widetilde{L}^{(m)}|L^{(m)}$ extensió de Galois tal que:*

a) $Gal(\widetilde{L}^{(m)}|L^{(m)}) \cong \Pi^{(m)}$, $\widetilde{L}^{(m)}|\lambda^{(m)}$ *és regular,* $L_0^{(m)} \subset \widetilde{L}^{(m)}$ *i* $\widetilde{L}^{(m)}|L_0^{(m)}$ *és no ramificada.*

b) $\widetilde{L}^{(m)}|K$ *és de Galois i la successió exacta*

$$1 \to Gal(\widetilde{L}^{(m)}|L^{(m)}) \to Gal(\widetilde{L}^{(m)}|K) \to G^{(m)} \to 1$$

és canònicament isomorfa a

$$1 \to \Pi^{(m)} \to G^{(m)} \ltimes \Pi^{(m)} \to G^{(m)} \to 1$$

on $G^{(m)}$ *actua en* $\Pi^{(m)}$ *per* $(g_{p_i}^{(m)})\sigma = (g_{\sigma^{-1}p_i}^{(m)})^{\chi(\sigma^{-1})}$,
amb $\chi : G^{(m)} \to (\mathbb{Z}/m\mathbb{Z})^*$ *el caràcter ciclotòmic.*

DEMOSTRACIÓ.

Siguin $\begin{cases} \Pi^{(m)} \xrightarrow{\varphi} C \\ \Pi^{(m)} \xrightarrow{\varphi'} C' \end{cases}$ com en el Teorema 2.4.4 i tals que $Ker(\varphi') \subset Ker(\varphi)$.

Notant $H := Ker(C' \xrightarrow{\varphi_{C'C}} C)$, tenim un isomorfisme canònic de λ-espais analítics $H\backslash(Y')^{an} \cong (Y)^{an}$. Per GAGA, tenim un λ-isomorfisme $H\backslash Y' \cong Y$.

Així, tenim un recobriment $Y' \xrightarrow{\phi_{C'C}} Y$ tal que $\phi' = \phi \circ \phi_{C'C}$.

Es satisfan:

- $L_C \subset L_{C'}$
- la projecció canònica $Gal(L_{C'}|L) \to Gal(L_C|L)$ correspon a $\varphi_{C'C}$ per l'isomorfisme del Teorema 2.4.4
- $\phi_{C'C}$ és recobriment étale, donat que $(\phi_{C'C})^{an}$ és λ-isomorfisme local

Definint $\widetilde{L}^{(m)} := \bigcup_C L_C$, el resultat és conseqüència del Teorema 2.4.4. □

Finalment, obtenim:

Corol.lari 2.5.2. *(límit respecte m)*

El Teorema 2.2.3 és cert.

DEMOSTRACIÓ.
Comencem observant que si $m \mid m'$ i $\lambda^{(m)} \subset \lambda^{(m')}$ aleshores el diagrama commutatiu

$$\begin{array}{ccccccccc} 1 & \to & Gal(\widetilde{L}^{(m')}|L^{(m')}) & \to & Gal(\widetilde{L}^{(m')}|K & \to & G^{(m')} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & Gal(\widetilde{L}^{(m)}|L^{(m)}) & \to & Gal(\widetilde{L}^{(m)}|K & \to & G^{(m)} & \to & 1 \end{array}$$

és canònicament isomorf a

$$\begin{array}{ccccccccc} 1 & \to & \Pi^{(m')} & \to & G^(m') \ltimes \Pi^{(m')} & \to & G^{(m')} & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \Pi^{(m)} & \to & G^(m) \ltimes \Pi^{(m)} & \to & G^{(m)} & \to & 1 \end{array}$$

Així, obtenim el resultat desitjat com a límit respecte els m del Teorema 2.5.1, observant que podem suposar $\bigcup_m \lambda^{(m)} = \overline{\kappa}$. □

mi casa

Bibliografia

[Ha] Harbater, D.: Galois coverings of the arithmetic line, in LNM **1240**, Springer-Verlag, Berlin-Heidelberg-NY, 1986.

[Liu] Liu, Q.: Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(t)$, in *Recent Developments in the Inverse Galois Problem*, ed. M. Fried et al., A.M.S. Contemp. Math., Providence, 1995.

[Pop1] Pop, F.: 1/2 Riemann existence theorem with Galois action, in *Algebra and Number Theory*, ed. G. Frey and J. Ritter, *de Gruyter Proceedings in Mathematics*, Berlin, New York, 1994.

[Pop2] Pop, F.: *Embedding problems over large fields*, Ann. of Math., **144** (1996), 1-34.

Capítol 3

Algunas consideraciones no-estándar

Carlos Infante

Estas notas tienen por objeto aclarar algunos de los conceptos sobre análisis no-estándar utilizados por Pop en el artículo "**Embedding Problems over Large Fields**" ([5]). De particular interés son los conceptos de **ultrapotencia** y **existencialmente cerrado** que estan estrechamente relacionados con el de **cuerpo grande**.

3.1 Ultrafiltros y Ultrapotencias.

Definición. *Sea I un conjunto. Una familia $\mathcal{D}$ no vacía de subconjuntos de I es un* **filtro** *en I si:*

(1) $\emptyset \notin \mathcal{D}$

(2) $A, B \in \mathcal{D} \Rightarrow A \cap B \in \mathcal{D}$

(3) $A \in \mathcal{D}$ *y* $A \subseteq B \subseteq I \Rightarrow B \in \mathcal{D}$.

$\mathcal{D}$ se llama **ultrafiltro** *si además,*

(4) $\forall A \subseteq I : A \in \mathcal{D}$ *ó* $I \backslash A \in \mathcal{D}$.

Observemos que en este último caso $\mathcal{D}$ satisface: $A \cup B \in \mathcal{D} \Rightarrow A \in \mathcal{D}$ o $B \in \mathcal{D}$

ya que si $A \notin \mathcal{D}$, entonces $I \backslash A \in \mathcal{D}$. Luego $(A \cup B) \cap (I \backslash A) \in \mathcal{D}$. Pero $(A \cup B) \cap (I \backslash A) = B \cap (I \backslash A) \subseteq B$ lo que implica que $B \in \mathcal{D}$.

Ejemplos.

a) La familia de subconjuntos de I con complemento finito es un filtro en I.

b) Para $a \in I$, $\mathcal{D}_a = \{A \subseteq I | a \in A\}$ es un ultrafiltro en I llamado principal.

Tenemos la siguiente caracterización para los ultrafiltros en I.

Proposición 1.*Sea $\mathcal{D}$ un filtro en I. $\mathcal{D}$ es un ultrafiltro $\Leftrightarrow$ $\mathcal{D}$ es un elemento maximal en la clase de filtros sobre I.*

Demostración: Sea $\mathcal{D}$ un ultrafiltro en I. Supongamos que existe $\mathcal{D}'$ un filtro en I tal que $\mathcal{D} \subset \mathcal{D}'$ (contención propia). Sea $A \in \mathcal{D}' \backslash \mathcal{D}$, como $\mathcal{D}$ es un ultrafiltro se tiene $I \backslash A \in \mathcal{D}$. Luego $\emptyset = A \cap I \backslash A \in \mathcal{D}'$!

Inversamente, sean $\mathcal{D}$ maximal y $A \subseteq I$. Asumamos que $I \backslash A \notin \mathcal{D}$. Sea $\mathcal{D}'$ la familia que resulta de unir a $\mathcal{D} \cup \{A\}$ todos los subconjuntos que contienen intersecciones finitas de elementos de $\mathcal{D} \cup \{A\}$. Aseguramos que $\mathcal{D}'$ es un filtro en I. Por la manera en que se ha definido, $\mathcal{D}'$ satisface las condiciones (2) y (3). Para verificar la condición (1) basta ver que $C \cap A \neq \emptyset$ con $C \in \mathcal{D}$. Si $C \cap A = \emptyset$, entonces $C \subseteq I \backslash A$. Pero por la propiedad (2) aplicada al filtro $\mathcal{D}$ se tiene $I \backslash A \in \mathcal{D}$! Finalmente, por la maximilidad de $\mathcal{D}$, tenemos $\mathcal{D} = \mathcal{D}'$ y por tanto $A \in \mathcal{D}$.□

Decimos que una familia $\mathcal{D}_0$ de subconjuntos de I satisface la **propiedad de intersección finita** si $A_1, ..., A_n \in \mathcal{D}_0$ implica $\bigcap_{i=1}^{n} A_i \neq \emptyset$.

Corolario 2. *Toda familia $\mathcal{D}_0$ de subconjuntos de I que satisface la propiedad de intersección finita está contenida en un ultrafiltro.*

Demostración: Añadiendo a $\mathcal{D}_0$ todos los conjuntos $B \subseteq I$ que contienen intersecciones finitas $\bigcap_{i=1}^{n} A_i$ de elementos de $\mathcal{D}_0$ obtenemos un filtro $\mathcal{D}_1$ sobre I. Por lema de Zorn, existe un filtro maximal $\mathcal{D}$ en I que contiene a $\mathcal{D}_1$ y por la proposición anterior $\mathcal{D}$ es un ul-

trafiltro. □

Antes de pasar al concepto de ultrapotencia debemos aclarar algunas cuestiones relativas al " lenguaje de primer orden" (ver [1]). Sea K un cuerpo en abstracto, es decir, un conjunto con dos operaciones "+" (adición) y "·" (multiplicación) que satisface los axiomas de la teoría de cuerpos. Construyamos un lenguaje sobre K, que denotaremos por $\mathcal{L}(K)$, a partir de los símbolos de las **variables** $X_1, X_2, X_3, ...$ (un número numerable), las **constantes** $c \in K$, el símbolo de **igualdad** $=$, las **funciones** $+, \cdot$ y los símbolos de **negación** $\neg$, **conjunción** $\wedge$, **existencial** $\exists$, paréntesis ( ) y corchetes [ ].

Sucesiones finitas de estos símbolos formarán las **palabras** de nuestro lenguaje $\mathcal{L}(K)$. Dentro de éstas sólo nos interesarán aquellas que tienen un cierto significado matemático y que llamaremos "fórmulas". Primero necesitamos definir lo que es un "término" y una "fórmula atómica".

La menor colección de palabras que contiene todas las variables X_i, todas las constantes $c \in K$ y todas las palabras $t_1 + t_2$, $t_1 \cdot t_2$ donde los t_i's son términos previamente definidos, forma la colección de **términos** de $\mathcal{L}(K)$. Así, un término no es más que un elemento de $K[X_1, ..., X_n]$ para algún $n \in \mathbf{N}$. Una **fórmula atómica** es una palabra del tipo: $t = t'$ para cada par de términos (t, t'). Finalmente, el conjunto de **fórmulas** en $\mathcal{L}(K)$ es la menor colección de palabras que contiene todas las fórmulas atómicas y satisface:

(1a)$\neg[\varphi]$ es una fórmula, si φ lo es;

(2a)$\varphi_1 \wedge \varphi_2$ es una fórmula, si φ_1 y φ_2 lo son; y

(3a)$(\exists X_l)[\varphi]$ es una fórmula, si φ lo es y $l \in \mathbf{N}$.

Por definición toda ocurrencia de una variable X en una fórmula atómica es **libre**. Si la ocurrencia de X en una fórmula φ es libre, y ψ es una fórmula arbitraria, entonces su ocurrencia es libre en $\neg[\varphi]$, $\varphi \wedge \psi$ y $(\exists Y)[\varphi]$ para Y distinta de X. Cualquier variable X que tenga una ocurrencia libre en una fórmula φ se dice que es una variable **libre** de φ. Escribiremos $\varphi(X_1, ..., X_n)$ para indicar que $X_1, ..., X_n$ incluye todas las variables libres de φ. Una fórmula sin variables libres es una **sentencia**.

Sean $a = \langle a_1, a_2, ... \rangle \in K^\omega$ una sucesión de elementos en K

y $\varphi(X_{i_1},...,X_{i_n})$ una fórmula. Decimos que a **satisface** φ en K, en símbolos $K \models \varphi(a)$, si la sucesión $a_{i_1},...,a_{i_n}$ satisface φ en K bajo la asignación $X_{i_j} \mapsto a_{i_j}, \forall j \in \{1,...,n\}$.

Sea I un conjunto y $\mathcal{D}$ un ultrafiltro sobre I. Sea $K^I := \prod_{i \in I} K$ el producto cartesiano de tantas copias de K como elementos en I.

Consideremos la relación de equivalencia en K^I definida por

$$a \sim b \quad \Leftrightarrow \quad \{i \in I | a(i) = b(i)\} \in \mathcal{D}$$

La reflexividad y simetría son claras. Para la transitividad observemos que

$$\{i \in I | a(i) = b(i)\} \cap \{i \in I | b(i) = c(i)\} \subseteq \{i \in I | a(i) = c(i)\}$$

Definición. *El conjunto de clases de equivalencia de K^I módulo esta relación se denomina la* **ultrapotencia** *de K módulo $\mathcal{D}$ y se denota por $K^I/\mathcal{D}$. La clase de $a \in K^I$ se denota por $a/\mathcal{D}$.*

Nuestro siguiente objetivo es interpretar las fórmulas del lenguaje $\mathcal{L}(K)$ en $K^I/\mathcal{D}$. Por la manera en que se han construído las fórmulas, basta con interpretar los términos y las fórmulas atómicas.

Para las constantes $c \in K$ el mapeo:

$$\jmath : K \to K^I/\mathcal{D}$$

$$c \mapsto \jmath(c) = a_c/\mathcal{D}$$

donde $a_c(i) = c, \forall i \in I$ nos da una inyección canónica de K en $K^I/\mathcal{D}$. Ya que $\jmath(c) \sim \jmath(c') \Leftrightarrow \{i \in I | a_c(i) = a_{c'}(i)\} \in \mathcal{D}$ que es distinto del vacío y por tanto $c = c'$.

Sea R_i una relación de rango n en $K, \forall i \in I$. Definimos una relación R del mismo rango en $K^I/\mathcal{D}$ por la condición:

$$\langle a_1/\mathcal{D},...,a_n/\mathcal{D}\rangle \in R \quad \Leftrightarrow \quad \{i \in I | \langle a_1(i),...,a_n(i)\rangle \in R_i\} \in \mathcal{D}$$

Similarmente, podemos definir las operaciones $a_1/\mathcal{D} + a_2/\mathcal{D}$, $a_1/\mathcal{D} \cdot a_2/\mathcal{D}$ como la clase de equivalencia de la función $i \mapsto a_1(i) + a_2(i)$, $a_1(i) \cdot a_2(i)$.

Sea φ una fórmula en el lenguaje $\mathcal{L}(K)$ y $a = \langle a_1, a_2, ...\rangle$ una sucesión de elementos en K^I. Denotemos $a/\mathcal{D} = \langle a_1/\mathcal{D}, a_2/\mathcal{D}, ...\rangle$ y $a(i) = \langle a_1(i), a_2(i), ...\rangle$.

Teorema 3.*Sea D un ultrafiltro sobre I. Entonces*

$$K^I/\mathcal{D} \models \varphi(a/\mathcal{D}) \quad \Leftrightarrow \quad \{i \in I | K \models \varphi(a(i))\} \in \mathcal{D}.$$

Demostración: Se prueba haciendo inducción sobre la longitud de la fórmula. Para fórmulas atómicas el teorema se sigue de la definición de ultrapotencia. Si el teorema es válido para φ, se procede por inducción sobre la estructura de las fórmulas (incisos (1a), (2a), (3a)) y las propiedades del ultrafiltro (ver [4]).

Observación. Dado que K satisface los axiomas de cuerpo, el teorema 3 nos dice que $K^I/\mathcal{D}$ es un cuerpo y que la $\jmath$-inyección canónica es una inyección a nivel de cuerpos. Más aún, el teorema 3 nos dice que $\jmath$ es una **inmersión elemental** de K en $K^I/\mathcal{D}$: si $a \in K^\omega, \jmath(a) := \langle \jmath(a_1), ..., \jmath(a_n), ... \rangle$ y φ es cualquier fórmula, entonces

$$K \models \varphi(a) \quad \Leftrightarrow \quad K^I/\mathcal{D} \models \varphi(\jmath(a)).$$

3.2 Cuerpos grandes y extensiones de cuerpos existencialmente cerradas

Definición. *Decimos que K es un* **cuerpo grande** *(large, ample) si tiene la siguiente propiedad:*

Toda curva lisa sobre K que tiene un punto K-racional, tiene una infinidad de puntos K-racionales.

Ejemplos.

(1)Cuerpos Pseudo Algebraicamente Cerrados (PAC): Toda variedad absolutamente irreducible sobre K tiene un punto K-racional (recordemos que una variedad X es absolutamente irreducible sobre K si permanece irreducible cuando es vista sobre cualquier extensión de K). Todo cuerpo algebraicamente cerrado es PAC.

(2) Cuerpos Pseudo Realmente Cerrados (PRC): Toda variedad absolutamente irreducible sobre K tiene un punto K-racional, siempre que tenga un $\bar{F}$-punto racional no singular en toda clausura real $\bar{F}$ de F.

(3) Cuerpos de números totalmente reales, totalmente p-ádicos, y más generalmente, extensiones algebraicas del cuerpo de

elementos totalmente $\mathfrak{S}$-ádicos $K^{\mathfrak{S}}$ de un cuerpo global K, donde $\mathfrak{S}$ es un conjunto finito de lugares de K y $K^{\mathfrak{S}}$ es la máxima extensión separable de K en la cual todo $\mathcal{P} \in \mathfrak{S}$ descompone completamente ([5]).

Definición. *Sea $\widehat{K}|K$ una extensión de cuerpos. Decimos que K es* **existencialmente cerrado** *en $\widehat{K}$, si para toda fórmula libre de cuantificadores $\varphi(X_1,...,X_n)$ del lenguaje $\mathcal{L}(K)$, la existencia de $b_1,...,b_n \in \widehat{K}$ tales que $\widehat{K} \models \varphi(b_1,...,b_n)$ implica la existencia de $a_1,...,a_n \in K$ tales que $K \models \varphi(a_1,...,a_n)$.*

Proposición 4. *Sea $\widehat{K}|K$ una extensión de cuerpos. Son equivalentes:*

(a) *K es existencialmente cerrado en $\widehat{K}$.*

(b) *Todo sistema de ecuaciones sobre K que tiene soluciones en $\widehat{K}$, tiene soluciones en K.*

(c) *Existe una K-inmersión de $\widehat{K}$ en una ultrapotencia de K.*

Demostración: $(a) \Rightarrow (b)$. Se sigue del hecho de que toda ecuación sobre K representa una fórmula libre de cuantificadores en $\mathcal{L}(K)$ y de que el ideal generado en $K[T]$ por el sistema de ecuaciones sobre K es finitamente generado. Usando el símbolo de conjunción obtenemos una fórmula libre de cuantificadores en $\mathcal{L}(K)$.

$(b) \Rightarrow (a)$. Se sigue de la estructura de los términos y de las fórmulas atómicas del lenguaje $\mathcal{L}(K)$. Observando que en una fórmula libre de cuantificadores solo intervienen los pasos (1a) y (2a) de la construcción de las fórmulas.

$(a) \Rightarrow (c)$. Bien ordenemos los elementos de $\widehat{K}$ en una sucesión $b = \{b_\alpha | \alpha < \gamma\}$ con γ un ordinal. Sea T el conjunto de todas las fórmulas libres de cuantificadores del lenguaje $\mathcal{L}(K)$ tales que el conjunto de variables que aparecen en ellas son escogidas a partir de la sucesión $\{\alpha | \alpha < \gamma\}$. Recordemos que $\widehat{K} \models \varphi(b)$ con $\varphi \in T$ significa que φ es satisfecha en $\widehat{K}$ por la sucesión $b_{\alpha_1},...,b_{\alpha_n}$ donde $X_{\alpha_1},...,X_{\alpha_n}$ es la sucesión de variables libres que aparecen en φ.

Sea $I = \{\varphi \in T | \widehat{K} \models \varphi(b)\}$. Para $\varphi \in I$, sean $X_{\beta_1},...,X_{\beta_s}$ las variables libres de φ para las cuales $b_{\beta_1},...,b_{\beta_s} \in K$ y sean $X_{\alpha_1},...,X_{\alpha_m}$ el resto de las variables libres en φ. Observemos que el elemento $\psi(X_{\alpha_1},...,X_{\alpha_m}) = \varphi(b_{\beta_1},...,b_{\beta_s},X_{\alpha_1},...,X_{\alpha_m})$ pertene a I y por tanto existe una sucesión $a'_\psi = \{a'_{\psi\alpha} | \alpha < \gamma\}$ de elementos en K tal que

$K \models \psi(a'_\psi)$. Luego, $a_\varphi := \{a_{\varphi\alpha} | \alpha < \gamma\}$ con $a_{\varphi\beta_j} = b_{\beta_j}, \forall j \in \{1, ..., s\}$ y $a_{\varphi\alpha} = a'_{\psi\alpha}$ para todas las demás α's nos define una sucesión de elementos en K tal que $K \models \varphi(a_\varphi)$.

Para $\varphi \in I$, sea $J_\varphi = \{\rho \in I | K \models \varphi(a_\rho)\}$. Sea $F = \{J_\varphi | \varphi \in I\}$. Aseguramos que F tiene la propiedad de intersección finita: si $J_{\varphi_1}, ..., J_{\varphi_n} \in F$, entonces $\varphi_1 \wedge \cdots \wedge \varphi_n \in \cap_i J_{\varphi_i}$. Aplicando el corolario 2, existe un ultrafiltro $\mathcal{D}$ que contiene a F.

Definamos el mapeo:

$$\lambda : \widehat{K} \to K^I/\mathcal{D}$$

$$b_\alpha \mapsto \lambda(b_\alpha) = a_\alpha/\mathcal{D}$$

donde $a_\alpha(\varphi) = a_{\varphi\alpha}, \forall \alpha < \gamma$. Además λ restringida a K coincide con la $\jmath$-inyección canónica de K en $K^I/\mathcal{D}$. Ya que si $b_\alpha = a \in K$ se tiene $\{\varphi \in I | a_\alpha(\varphi) = b_\alpha\} \in \mathcal{D}$, por tanto $a_\alpha/\mathcal{D} \sim a_a/\mathcal{D} = \jmath(a)$. Para ver que λ es inyectiva, recordemos que

$$a_\alpha/\mathcal{D} \sim a_\beta/\mathcal{D} \quad \Leftrightarrow \quad \{\varphi \in I | a_\alpha(\varphi) = a_\beta(\varphi)\} \in \mathcal{D}$$

y que $J_\varphi = \{\rho \in I | K \models \varphi(a_\rho)\} \in \mathcal{D}$; de donde λ es una K-inmersión de $\widehat{K}$ en $K^I/\mathcal{D}$ (ver [4]).

$(c) \Rightarrow (a)$. Si $\varphi(X_1, ..., X_n)$ es una fórmula libre de cuantificadores en $\mathcal{L}(K)$ con solución en $\widehat{K}$, entonces también es solución en $K^I/\mathcal{D}$. Por el teorema 3, esta fórmula es satisfecha en K.

Observación. K existencialmente cerrado en $\widehat{K}$ implica $\widehat{K}|K$ regular. Pues si $z \in \widehat{K} \cap \bar{K}$, sea $f(X) = \text{irred}(z, X, K) \in K[X]$. Luego, $f(X) = 0$ tiene una solución en K por ser una fórmula libre de cuantificadores en $\mathcal{L}(K)$. Dado que $f(X)$ es irreducible en $K[X]$ se tiene $f(X) = X - z \in K[X]$. Así, $\widehat{K} \cap \bar{K} = K$.

Por teoría de Galois: $\mathcal{G}_K \cong Gal(K^s \cdot \widehat{K} | \widehat{K})$, de donde la proyección canónica $\mathcal{G}_{\widehat{K}} \to \mathcal{G}_K$ es sobreyectiva.

Antes de pasar a la siguiente proposición recordemos algunos conceptos. Un cuerpo valuado K se llama **Henseliano** si toda extensión algebraica de K admite una única valoración que extiende la dada en K. Esto es equivalente al "**Lema de Hensel**": Sea $f(X) \in \mathcal{O}[X]$ y $a \in \mathcal{O}$ tal que su clase residual es un cero simple de la imágen de $f(X)$ en el cuerpo residual. Entonces existe $t \in K$ tal que $f(t) = 0$ y $v(t - a) > 0$.

Todo cuerpo valuado K admite una única extensión, llamada la **Henselianización** de K y denotada por K^h, tal que: K^h es Henseliano y dada cualquier extensión $L|K$ con L Henseliano existe un único K-isomorfismo como cuerpos valuados de K^h en L.

Proposición 5.*Sea K cuerpo y X/K una variedad. Denotemos por $X(K)$ el conjunto de todos los K-puntos racionales de X. Son equivalentes:*

(1) *K es grande.*

(2) *Para toda variedad X entera y lisa sobre K: $X(K) \neq \emptyset$ implica $X(K)$ es denso-Zariski.*

(3) *Para todo $\mathcal{K}|K$ cuerpo de funciones en una variable: $\mathcal{K}$ tiene una valoración K-racional implica $\mathcal{K}$ tiene una infinidad de valoraciones K-racionales.*

(4) *K es existencialmente cerrado en la Henselianización $K(u)^h$ de $K(u)$ con respecto a la u-valoración.*

(5) *K es existencialmente cerrado en el cuerpo de series de Laurent $\widehat{K} = K((u))$.*

Demostración: (1) $\Leftrightarrow$ (2) Se sigue del hecho de que el conjunto de curvas lisas sobre K a través de un K-punto liso dado en una variedad entera X/K es denso-Zariski en X. Luego, si K es grande, el conjunto de K-puntos racionales de cualquiera de tales curvas es denso-Zariski en la curva. Por tanto $X(K)$ es denso-Zariski en X ([5]).

(1) $\Leftrightarrow$ (3) Se sigue de la correspondencia entre $\mathcal{K}|K$ los cuerpos de funciones en una variable sobre K y las curvas lisas C sobre K. Recordando que si $\mathcal{P} \in C$, entonces $\mathcal{O}_{\mathcal{P}}$ es un anillo de valoración discreta y la valoración asociada $v_{\mathcal{P}}$ es una valoración sobre $\mathcal{K}$. Estamos considerando que $v_{\mathcal{P}}$ es K-racional $\Leftrightarrow \mathcal{P} \in C(K)$.

(3) $\Leftrightarrow$ (4) Es una reformulación.

(4) $\Leftrightarrow$ (5) Obsérvese que $K((u))$ es la completación de $K(u)$ y $K(u)^h$ respecto a la u-valoración sobre $K(u)$ dada por el ideal $\langle u \rangle$. Tenemos que $K((u))|K(u)^h$ es regular y que $K(u)^h$ es existencialmente cerrado en $K((u))$ (ver [2]). Así, utilizando el inciso (b) de la proposición 4, todo sistema de ecuaciones sobre K con solución en $K((u))$ tiene solución en $K(u)^h$ y por hipótesis en K. Por tanto K

es existencialmente cerrado en $K((u))$.

(5) $\Rightarrow$ (4) Dada la contención de $K(u)^h$ en $K((u))$, todo sistema de ecuaciones sobre K con soluciones en $K(u)^h$ tiene soluciones en $K((u))$. Por hipótesis tiene solución en K y por tanto K es existencialmente cerrado en $K(u)^h$. $\square$

Proposición 6.*Si K es un cuerpo grande y L es una extensión algebraica de K, entonces L es grande.*

Demostración: Si X es una curva lisa sobre L con $X(L) \neq \emptyset$, entonces existe una subextensión finita $L'|K$ de $L|K$ y una curva lisa X' sobre L' con $X'(L') \neq \emptyset$ y X obtenida a partir de X' por cambio de base $L' \hookrightarrow L$. Así, podemos suponer que $L|K$ es finita y, más aún, que X es afín. Sea V la restricción de Weil de X a K (ver [6], Apéndice 2). Entonces V es una K-variedad lisa con $V(K) \cong X(L)$ funtorialmente. Como $V(K) \neq \emptyset$, se tiene que es infinito. Por tanto $X(L)$ es infinito. $\square$

mi casa

Bibliografia

1. M. Fried and M. Jarden, Field Arithmetic, Springer-Verlag, 1986.

2. M. Jarden, Israel Journal of Math. 85 (1994) 263-275.

3. J.-L. Bell and A.-B. Slomson, Models and Ultraproducts: an Introduction, 1969.

4. S. Kochen, Ultraproducts in the theory of Models, Ann. of Math. 74 (1961) 221-261.

5. F. Pop, Embedding Problems over large fields, Ann. of Math. 144 (1996) 1-34.

6. J Oesterlé, Nombres de Tamagawa et groupes unipotents en caractéristique p, Invent. Math. 78 (1984) 13-88.

Capítol 4

Realitzacions galoisianes sobre cossos grans

MONTSERRAT VELA

Introducció

L'objectiu d'aquest capítol és estudiar la primera part de l'article [Po 96], especialment els teoremes: Main Theorem A i Main Theorem B.

L'enunciat d'aquests teoremes és el següent:

Teorema A: *Sigui κ un cos gran.*

Tot problema d'immersió finit i split sobre κ té solucions regulars i pròpies. En particular, tot grup finit és realitzable com a grup de Galois sobre $\kappa(t)$.

Els **preliminars** per entendre l'enunciat d'aquest teorema són:
- Cossos grans: definició i les seves propietats.
- Problemes d'immersió i solucions regulars.

Els **ingredients** que es fan servir per la demostració del teorema són:
- 1/2 Teorema d'existència de Riemann (Bernat Plans)
- Arguments de tipus no-estàndard: ultrapotències, existencialment tancat,... (Carlos Infante).

Amb el teorema anterior tenim solucions al problema d'immersió com a extensions del cos $\kappa(t)$. Per passar a una solució sobre κ fem servir el

Teorema B: *Sigui κ un cos gran hilbertià.*

Tot problema d'immersió finit i split sobre κ té solucions pròpies.

Els **preliminars** d'aquest teorema són els cossos hilbertians i les seves propietats.

En aquests teoremes resolem els problemes d'immersió que són split. El següent resultat, que també demostrarem, ens canvia aquesta hipòtesi per una altra sobre el cos.

Teorema: *Sigui κ un cos gran i hilbertià amb dimensió cohomològica 1. Tot problema d'immersió finit per G_κ té solucions pròpies.*

L'estructura de l'exposició serà la següent:

1. **Cossos grans i propietats**
2. **Problemes d'immersió:**
   - 2.1 Plantejament i solucions pròpies i impròpies
   - 2.2 Solucions regulars
   - 2.3 Problema invers regular
   - 2.4 Problemes d'immersió dominants
3. **Teorema A:**
   - 3.1 Lema 1
   - 3.2 Lema 2
   - 3.3 Conclusions. Final de la demostració

4. **Teorema B:**
   4.1 Cossos hilbertians i propietats
   4.2 Demostració del Teorema B
5. **Un darrer resultat**

4.1 Cossos grans

Definició 4.1.1. *Un cos κ és gran si tota corba llisa sobre κ que té un punt κ-racional en té infinits.*

Els cossos de nombres totalment reals i totalment p-àdics són cossos grans. Més exemples de cossos grans veurem al següent capítol. A més:

Proposició 4.1.2. *Tota extensió algebraica d'un cos gran és gran.*

Donarem ara propietats equivalents, per un cos, a ser gran. Començarem definint la noció d'existencialment tancat:

Definició 4.1.3. *Sigui $\hat{\kappa}/\kappa$ una extensió de cossos. Direm que κ és existencialment tancat en $\hat{\kappa}$ si cada sentència existencial amb paràmetres en κ que sigui certa per $\hat{\kappa}$ és certa per κ.*

Tenim, equivalentment, les següents caracteritzacions:

Proposició 4.1.4. *Sigui $\hat{\kappa}/\kappa$ una extensió de cossos. Són equivalents:*

- *κ és existencialment tancat en $\hat{\kappa}$.*
- *Tot sistema d'equacions a coeficients en κ que tingui solucions a $\hat{\kappa}$, té solucions a κ.*
- *Hi ha una κ-immersió de $\hat{\kappa}$ en alguna ultrapotència de κ.*

A més, en aquest cas, $\hat{\kappa}/\kappa$ és una extensió regular (i.e. $\hat{\kappa} \cap \overline{\kappa} = \kappa$) i, per tant, la projecció canònica $G_{\hat{\kappa}} \to G_{\kappa}$ és exhaustiva.

La següent proposició ens dóna condicions equivalents a que un cos sigui gran:

Proposició 4.1.5. *Sigui κ un cos i $X \to \kappa$ una varietat. Denotem per $X(\kappa)$ el conjunt de punts κ-racionals de X. Són equivalents:*

1. *κ és un cos gran.*
2. *Si X és una varietat íntegra i llisa sobre κ tal que $X(\kappa) \neq \emptyset$, llavors $X(\kappa)$ és infinit.*
3. *Tot cos de funcions en una variable K/κ que té una plaça κ-racional, en té infinites.*
4. *κ és existencialement tancat en la henselianització $\kappa(u)^h$ de $\kappa(u)$ respecte de la valoració u-àdica.*
5. *κ és existencialment tancat en el cos de sèries de Laurent $\hat{\kappa} = \kappa((u))$.*

4.2 Problemes d'immersió

Sigui κ un cos i G_κ el seu grup de Galois absolut.

4.2.1 Plantejament. Solucions pròpies i impròpies

El plantejament clàssic del problema d'immersió té per dades:

- El cos κ i una extensió de Galois L/κ amb grup $Gal(L/\kappa) \simeq A$.
- Una successió exacta de grups

$$1 \to ker(\alpha) = C \to B \xrightarrow{\alpha} A \to 1,$$

(o, equivalentment, un homomorfisme exhaustiu de grups $\alpha : B \to A$).

Amb aquestes dades, una solució al problema d'immersió és un cos M tal que:

M/L és una extensió de Galois amb grup $Gal(M/L) \simeq C$,

M/κ és una extensió de Galois amb grup $Gal(M/\kappa) \simeq B$,

$$\left.\begin{array}{c} M \\ |C \\ L \\ |A \\ K \end{array}\right\} B$$

i α és el morfisme de restricció, és a dir, el diagrama:

$$\begin{array}{ccc} B & \xrightarrow{\alpha} & A \\ \downarrow\wr & & \downarrow\wr \\ Gal(M/\kappa) & \longrightarrow & Gal(L/\kappa) \\ \sigma & \longrightarrow & \sigma_{|L} \end{array}$$

és commutatiu.

Höchsmann, en 1962, formula equivalentment el problema a partir de les dades

- El cos κ i un epimorfisme $\gamma : G_\kappa \to A$ en un cert grup A.
  El subcòs de la clausura separable κ^s fix pel $ker(\gamma)$ és el cos $L = (\kappa^s)^{ker(\gamma)}$, dada del problema clàssic.

- Una successió exacta de grups

$$1 \to ker(\alpha) = C \to B \xrightarrow{\alpha} A \to 1,$$

  (o, equivalentment, un homomorfisme exhaustiu de grups $\alpha : B \to A$).

En aquets cas, una solució és un morfisme $\beta : G_\kappa \to B$ tal que $\gamma = \alpha \circ \beta$, és a dir, tal que commuta el diagrama:

$$\begin{array}{ccccccccc} & & & & & & G_\kappa & & \\ & & & & & \swarrow & \downarrow\gamma & & \\ 1 & \to & C & \to & B & \xrightarrow{\alpha} & A & \to & 1. \end{array}$$

- Si β és exhaustiu, es diu que la solució és pròpia. El subcòs de κ fix pel $ker(\beta)$, $(\kappa^s)^{ker(\beta)} = M$ és un cos solució en el sentit anterior, és a dir $Gal(M/\kappa) \simeq B$.
- Si β no és exhaustiu, l'extensió $(\kappa^s)^{ker(\beta)}/\kappa$ té com a grup de Galois un subgrup de B. (Hasse, en 1948, a partir d'aquest cos, construeix unes àlgebres galoisianes, que tenen com a grup de Galois B).

Definició 4.2.1. *1. El problema d'immersió es diu finit si B és un grup finit.*

2. El problema d'immersió es diu split si l'epimorfisme α té una secció.

Notació: Per plantejar un problema d'immersió, essencialment hem de donar dos homomorfismes exhaustius de grups. Notarem

$$EP = (\gamma : G_\kappa \to A, \alpha : B \to A) = (\gamma, \alpha)$$

si els grups estan clars. A més, posarem $\kappa_{EP} = (\kappa^s)^{ker(\gamma)}$, el cos fix pel $ker(\gamma)$ (i.e. el cos dada del problema clàssic). Observem que, per definició, $Gal(\kappa_{EP}/\kappa) \simeq A$.

4.2.2 Solucions regulars. Problema invers regular

Sigui $K = \kappa(t)$ i $\Pi : G_K \to G_\kappa$ la projecció canònica. Cada problema d'immersió sobre κ, $EP = (\gamma, \alpha)$, dóna lloc (via Π) a un problema d'immersió sobre K, $EP_K = (\gamma\Pi, \alpha)$.

Si β és una solució de EP_K, denotem per $K_\beta = (K^s)^{ker(\beta)}$ el subcòs de la clausura separable de K fix pel $ker(\beta)$ (és a dir, una solució o el cos nucli de l'àlgebra solució al problema EP_K) i per $\kappa_\beta = K_\beta \cap \kappa^s$.

Definició 4.2.2. *Una solució regular (pròpia) de EP és una solució (pròpia) de EP_K, diguem-li β, tal que $\kappa_\beta = \kappa_{EP}$ (és a dir, per calcular la solució K_β només afegim " coses" que tenen t i no afegim elements algebraics sobre κ).*

Aquestes solucions són un cas particular de les solucions paramètriques definides per [Ma-Ma 94].

El **problema invers regular** de la teoria de Galois sobre κ consisteix en realitzar grups finits com a grups de Galois d'extensions de Galois $L/\kappa(t)$ tals que L/κ sigui una extensió regular (és a dir, $L \cap \overline{\kappa} = \kappa$).

En el llenguatge del problema d'immersió:

Sigui B un grup finit i considerem $A = \{1\}$ i el problema

$$\begin{array}{ccc} & & G_\kappa \\ & & \downarrow \gamma \\ B & \stackrel{\alpha}{\to} & A = \{1\}, \end{array}$$

on γ i α són els morfismes trivials.

El problema $EP = (\gamma, \alpha)$ és finit i split.

L'existència d'una solució regular i pròpia de EP és equivalent a una realització regular de B sobre κ.

4.2.3 Problemes d'immersió dominants

Sigui G un grup profinit qualsevol. En general, nosaltres pensarem en el grup de Galois absolut d'un cos κ.

Sigui $EP = (\gamma : G \to A, \alpha : B \to A)$ un problema d'immersió. La idea és que un problema d'immersió dominant és un altre problema que està "per sobre" i tal que, a partir d'una solució d'aquest podem trobar-ne una del problema inicial.

Sigui $EP' = (\gamma' : G \to A', \alpha' : B' \to A')$ un altre problema d'immersió per a G.

Definició 4.2.3. *Direm que EP' domina EP si existeixen morfismes exhaustius de grups $\gamma_0 : A' \to A$ i $\beta_0 : B' \to B$ tals que*

i) $\gamma = \gamma_0 \gamma'$.

ii) $\alpha\beta_0 = \gamma_0\alpha'$ *(és a dir, commuta el diagrama).*

iii) $\beta_0(ker(\alpha')) = ker(\alpha)$.

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \gamma'} & & \\ 1 & \longrightarrow & ker(\alpha') & \longrightarrow & B' & \xrightarrow{\alpha'} & A' & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \beta_0} & & \downarrow{\scriptstyle \beta_0} & & \downarrow{\scriptstyle \gamma_0} & & \\ 1 & \longrightarrow & ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1. \end{array}$$

Tenim:

1. Si $\beta' : G \to B'$ és una solució (pròpia) de EP', llavors $\beta = \beta_0\beta'$ és una solució (pròpia) de EP. Això és clar perquè si β' és exhaustiva, també ho és β.
2. Considerem $G = G_\kappa$. Si β' és una solució regular de EP', llavors $\beta = \beta_0\beta'$ és una solució regular de EP (perquè $(K^s)^{ker(\beta)} \subset (K^s)^{ker(\beta')}$).

Sigui $EP = (\gamma : G \to A, \alpha : B \to A)$ un problema d'immersió (split) per a G. Explicarem ara tres maneres de construir problemes d'immersió (split) EP' que dominen EP i que es fan servir després en les demostracions del teoremes.

A) Producte fibrat:

Sigui A' un grup amb $\gamma' : G \to A'$ un morfisme exhaustiu i tal que $ker(\gamma') \subseteq ker(\gamma)$. Considerem

$\gamma_0 : A' \to A$ la projecció canònica,

$B' = B \times_A A'$ el producte fibrat de B i A' sobre A i

$\beta_0 : B' \to B$, $\alpha' : B' \to A'$ els morfismes estructurals.

$$\begin{array}{ccc} B' = B \times_A A' & \xrightarrow{\alpha'} & A' \\ \downarrow{\scriptstyle \beta_0} & & \downarrow{\scriptstyle \gamma_0} \\ B & \xrightarrow{\alpha} & A. \end{array}$$

Recordem que aquest producte fibrat té la següent propietat universal: Si H és un altre grup i tenim morfismes $f_1 : H \to A'$ i $f_2 : H \to B$, existeix un únic morfisme $\theta : H \to B$ tal que $\alpha'\theta = f_1$ i $\beta_0\theta = f_2$.

Proposició 4.2.4. *El problema d'immersió*

$$EP' = (\gamma' : G \to A', \alpha' : B' \to A')$$

domina EP.

Proposició 4.2.5. *Cada secció* $\overline{\alpha}$ *de* α*, dóna lloc, functorialment, a una secció* $\overline{\alpha'}$ *de* α'.

Demostració. Tenim aquesta secció $\overline{\alpha'}$ per la propietat universal del producte fibrat. Considerem $f_1 = Id$, $f_2 = A' \xrightarrow{\gamma_0} A \xrightarrow{\overline{\alpha}} B$. Llavors, tenim un homomorfisme $\overline{\alpha'} : A' \to B'$ tal que $\alpha' \circ \overline{\alpha'} = Id_{A'}$. □

B) Producte fibrat a partir d'una solució:

Suposem ara que el problema EP té solució, diguem β a una de les solucions. Posem $A' = \beta(G)$. Considerem, com abans, $B' = B \times_A A'$ i

$$\begin{array}{ccc} B' = B \times_A A' & \xrightarrow{\alpha'} & A' \\ \downarrow{\scriptstyle \beta_0} & & \downarrow{\scriptstyle \gamma_0} \\ B & \xrightarrow{\alpha} & A. \end{array}$$

Proposició 4.2.6. *El problema*

$$EP' = (\gamma' = \beta : G \to A', \alpha' : B' \to A')$$

és un problema d'immersió split que domina EP.

Demostració. Clarament EP' domina EP. A més α' té una secció, de manera semblant a l'anterior, per la propietat universal del producte fibrat, considerant $H = A'$, $f_1 = Id$, f_2 la inclusió $A' = \beta(G) \subset B$, llavors $\overline{\alpha'} : A' \to B'$ és tal que $\alpha' \circ \overline{\alpha'} = Id_{A'}$. □

C) Producte semidirecte:

Sigui que EP és un problema d'immersió split i denotem per $\overline{\alpha} : A \to B$ una secció.

Volem trobar un problema d'immersió que domini EP. La idea del diagrama és:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & ker(\widetilde{\alpha}) & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \widetilde{\varphi}} & & \| & & \\ 1 & \longrightarrow & ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1. \end{array}$$

Hem de definir qui és el grup F i donar una acció de A en F per poder definir el producte semidirecte. Després hem de definir els morfismes $\widetilde{\alpha}$ i $\widetilde{\varphi}$.

1. Definició del grup F

Siguin $\Sigma = (\mathcal{C}_k)_k$ una família finita de subgrups cíclics de $C = Ker(\alpha)$ que generen C i m_Σ el mínim comú múltiple dels ordres dels $\mathcal{C}_k \quad \forall k$.

Per a cada $\sigma \in A$ i cada k, considerem un grup isomorf a $\mathcal{C}_k$, denotat per $\mathcal{C}_{k,\sigma}$ i l'isomorfisme $\iota_{k,\sigma} : \mathcal{C}_{k,\sigma} \xrightarrow{\simeq} \mathcal{C}_k$. Si $g_k \in \mathcal{C}_k$, denotem per $g_{k,\sigma} = \iota_{k,\sigma}^{-1}(g_k)$.

Posem $\widetilde{\Sigma} = (\mathcal{C}_{k,\sigma})_{k,\sigma}$ la família dels grups i definim F com el producte lliure profinit dels subgrups de $\widetilde{\Sigma}$.

Existeix una acció natural per la dreta de A en F definida per:

$$\begin{array}{rlll} ac_F : A & \to Aut(F) & & \\ \tau & \to ac_F(\tau) : \quad F & \to F & \forall \sigma, k \\ & \qquad\quad g_{k,\sigma} & \to (g_{k,\sigma})\tau = g_{k,\tau^{-1}\sigma} & \end{array}$$

Sigui $A \ltimes F$ el producte semidirecte de F per A. Identifiquem $A \ltimes 1$ i $1 \ltimes F$ com a A i F respectivament, dins de $A \ltimes F$.

(Recordem que el producte semidirecte de dos grups té com a elements els parells del producte directe però que el seu producte ve modificat, en la segona component, per l'acció definida.)

2. Definició de $\widetilde{\alpha}$

Definim com $\widetilde{\alpha} : A \ltimes F \to A$ com el morfisme estructural del producte semidirecte. Observem que $ker(\widetilde{\alpha}) \simeq F$.

3. Definició de $\widetilde{\varphi}$

Comencem definint una acció de A en C. Fixem una secció $\overline{\alpha} : A \to B$ de α. Via $\overline{\alpha}$ definim una acció de A en C a partir de la conjugació en B:

$$\begin{array}{rlll} ac_C : A & \to Aut(C) & & \\ \tau & \to ac_C(\tau) : & C & \to C \\ & & g & \to g\tau = g^{\overline{\alpha}(\tau)} = \overline{\alpha}(\tau)^{-1} i(g) \overline{\alpha}(\tau) \end{array}$$

on considerem l'element $i(g)$ com la imatge de g en B per la inclusió.

Afirmació 1: *L'acció ac_C està ben definida, és a dir, $g\tau \in C$ si $g \in C$ i $\tau \in A$.*

Demostració: Tenim que $g^{\overline{\alpha}(\tau)} \in C = ker(\alpha) \Leftrightarrow \alpha(g^{\overline{\alpha}(\tau)}) = 1_A$.

Per provar-ho, calculem

$$\alpha(g^{\overline{\alpha}(\tau)}) = \alpha(\overline{\alpha}(\tau)^{-1} i(g) \overline{\alpha}(\tau)) = \tau^{-1} \alpha(i(g))\tau = \tau^{-1}(1_A)\tau = 1_A. \square$$

Definim ara un morfisme canònic exhaustiu φ de F en C:

$$\begin{array}{rl} \varphi : F & \longrightarrow C \\ g_{k,\sigma} & \longrightarrow (g_k)\sigma^{-1} = \overline{\alpha}(\sigma) i(g_k) \overline{\alpha}(\sigma)^{-1}. \end{array}$$

Afirmació 2: *φ és compatible amb l'acció de A en F i C.*

Demostració: Hem de comprovar la commutativitat del següent diagrama:

$$\begin{array}{ccc} F & \xrightarrow{ac_F(\tau)} & F \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ C & \xrightarrow[ac_C(\tau)]{} & C \end{array}$$

Seguint la imatge d'un element qualsevol, tenim:

$$\begin{array}{ccc} g_{k,\sigma} & \xrightarrow{ac_F(\tau)} & (g_{k,\sigma})\tau = g_{k,\tau^{-1}\sigma} \\ \varphi\downarrow & & \downarrow\varphi \\ (g_k)\sigma^{-1} & \xrightarrow{ac_C(\tau)} & (g_k)\sigma^{-1}\tau = (g_k)(\tau^{-1}\sigma)^{-1}, \end{array}$$

i, per tant, el diagrama commuta. □

Així φ indueix canònicament, un homomorfisme de grups:

$$\begin{array}{rl} \widetilde{\varphi} : A \ltimes F & \longrightarrow B \\ (\tau, g) & \longrightarrow \overline{\alpha}(\tau)\varphi(g). \end{array}$$

Afirmació 3: *$\widetilde{\varphi}$ és un morfisme de grups.*

Demostració: Hem de provar que

$$\widetilde{\varphi}((\tau, g_{k,\sigma}), (\tau', g_{k',\sigma'})) = \widetilde{\varphi}(\tau, g_{k,\sigma})\widetilde{\varphi}(\tau', g_{k',\sigma'}).$$

Calculant els dos costats de la igualtat, tenim

$$\begin{array}{ll} \widetilde{\varphi} & ((\tau, g_{k,\sigma}), (\tau', g_{k',\sigma'})) = \widetilde{\varphi}(\tau\tau', ac_F(\tau')(g_{k,\sigma})g_{k',\sigma'}) = \\ & \overline{\alpha}(\tau\tau')\varphi(g_{k,(\tau')^{-1}\sigma})\varphi(g_{k',\sigma'}) \\ \text{i} & \widetilde{\varphi}(\tau, g_{k,\sigma})\widetilde{\varphi}(\tau', g_{k',\sigma'}) = \overline{\alpha}(\tau)\varphi(g_{k,\sigma})\overline{\alpha}(\tau')\varphi(g_{k',\sigma'}). \end{array}$$

Llavors:

$$\begin{array}{l} \overline{\alpha}(\tau\tau')\varphi(g_{k,(\tau')^{-1}\sigma})\varphi(g_{k',\sigma'}) = \overline{\alpha}(\tau)\varphi(g_{k,\sigma})\overline{\alpha}(\tau')\varphi(g_{k',\sigma'}) \\ \Leftrightarrow \overline{\alpha}(\tau')\varphi(g_{k,(\tau')^{-1}\sigma}) = \varphi(g_{k,\sigma})\overline{\alpha}(\tau') \\ \Leftrightarrow \overline{\alpha}(\tau')\overline{\alpha}(\tau')^{-1}\overline{\alpha}(\sigma)i(g_k)\overline{\alpha}((\tau')^{-1}\sigma)^{-1} = g_k\sigma^{-1}\overline{\alpha}(\tau') \\ \Leftrightarrow \overline{\alpha}(\sigma)i(g_k)\overline{\alpha}(\sigma)^{-1} = g_k\sigma^{-1}, \end{array}$$

que és certa per la definició de l'acció. □

Observem que $\forall\sigma \in A$ tenim que $\widetilde{\varphi}(\sigma, 1_F) = \overline{\alpha}(\sigma)$. A més $\widetilde{\varphi}$ aplica cada $\mathcal{C}_{k,\sigma}$ isomòrficament en $\overline{\alpha}(\sigma)\mathcal{C}_k\overline{\alpha}(\sigma)^{-1}$. Per tant, φ i $\widetilde{\varphi}$ són exhaustius.

Proposició 4.2.7. *El problema d'immersió $\widetilde{EP} = (\gamma, \widetilde{\alpha})$ és un problema d'immersió per G que, per construcció, domina EP.*

Demostració. Tenim la següent situació:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & ker(\widetilde{\alpha}) \simeq F & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \widetilde{\varphi}} & & \| & & \\ 1 & \longrightarrow & ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1. \end{array}$$

Per demostrar que el problema és dominant, hem de comprovar les tres propietats de la definició 4.2.3.

i) La primera és clara.

ii) Hem de veure que $\alpha \circ \widetilde{\varphi} = \widetilde{\alpha}$.

Per $(\tau, g_{k,\sigma}) \in A \ltimes F$, tenim que:

- $\widetilde{\alpha}(\tau, g_{k,\sigma}) = \tau$ i
- $\alpha(\widetilde{\varphi}(\tau, g_{k,\sigma}) = \alpha(\overline{\alpha}(\tau)\varphi(g_{k,\sigma})) = \alpha(\overline{\alpha}(\tau)\overline{\alpha}(\sigma)i(g_k)\overline{\alpha}(\sigma)^{-1} = \tau\sigma\alpha(g_k)\sigma^{-1} = \tau\sigma\sigma^{-1} = \tau$, perquè $g_k \in ker(\alpha)$.

iii) Hem de veure que $\widetilde{\varphi}(ker(\widetilde{\alpha})) = \widetilde{\varphi}(1_A \ltimes F) = ker(\alpha)$. Mirarem les dues inclusions:

$\subseteq$ $\widetilde{\varphi}(1, g_{k,\sigma}) = \overline{\alpha}(1_A)\varphi(g_{k,\sigma}) = 1_B\varphi(g_{k,\sigma}) \in ker(\alpha)$.

$\supseteq$ Si $g \in ker(\alpha)$, considerem $g_k \in \mathcal{C}_k$, llavors, $\widetilde{\varphi}(1_A, g_{k,1_A}) = \varphi(g_{k,1_A}) = i(g_k) = g_k$. $\square$

Proposició 4.2.8. *Si EP' és un problema d'immersió finit per a G obtingut pel producte fibrat (cas A) anterior), llavors, denotant per Σ' l'antiimatge de Σ per β_0, tenim que el problema d'immersió $\widetilde{EP'}$ domina canònicament $\widetilde{EP}$.*

4.3 Teorema A

Teorema A: *Sigui κ un cos gran. Tot problema d'immersió finit i split sobre κ té solucions regulars i pròpies.*

En particular, tot grup finit G és realitzable regularment com a grup de Galois sobre $\kappa(t)$.

Idea: La idea de la demostració és fer-la en dos passos:

1. Resoldre el problema en el cas de que el cos sigui el de les sèries de Laurent (Lema 1) fent servir el 1/2 teorema d'existència de Riemann. Recordem que el cos de les sèries de Laurent en una variable sobre un cos κ és:

$$\kappa((u)) := \{\sum_{i \geq N}^{\infty} a_i t^i; \quad N \in \mathbb{Z}, a_i \in \kappa\} = \hat{\kappa}.$$

2. Reduir després el cas general a aquest cas. Per això farem servir l'anàlisi no-estàndard.

4.3.1 Primer Lema

Lema 1: *Sigui $\hat{\kappa}$ el cos de sèries de Laurent en una variable sobre un cos donat κ. Tot problema d'immersió finit split per $\hat{\kappa}$ té solucions regulars i pròpies.*

De fet tenim:

Lema 1': *Amb les notacions de la secció anterior, sigui $EP = (\gamma, \alpha)$ un problema d'immersió finit i split sobre $\hat{\kappa}$ i $\widetilde{EP}$ el problema dominant construït mitjançant el producte semidirecte en C) de la secció anterior. El problema $\widetilde{EP}$ sobre $\hat{\kappa}$, té solucions regulars i pròpies.*

Tenim la següent situació:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & ker(\widetilde{\alpha}) \simeq F & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \widetilde{\varphi}} & & \| & & \\ 1 & \longrightarrow & ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1 \end{array}$$

Com $\widetilde{EP}$ domina EP, si el problema $\widetilde{EP}$ té solucions regulars i pròpies, EP té solucions regulars i pròpies. Per tant, Lema 1 $\Rightarrow$ Lema 1'. Demostrarem doncs, el Lema 1'.

Demostració del Lema 1': Farem servir les notacions de la secció anterior. Recordem que m_Σ és el mínim comú múltiple dels ordres del grups de Σ.

Afirmació 1: Podem suposar que les arrels de la unitat d'ordre m_Σ estan contingudes a $\hat{\kappa}_{EP} = (\hat{\kappa}^s)^{ker(\gamma)}$ que és el subcòs de la clausura separable de $\hat{\kappa}^s$ fix pel $ker(\gamma)$.

Demostració: Si no fos així, considerem $\hat{\kappa}_\Sigma/\hat{\kappa}$ una extensió de Galois que contingui $\hat{\kappa}_{EP}$ i les arrels de la unitat d'ordre m_Σ. Posem $A' = Gal(\hat{\kappa}_\Sigma/\hat{\kappa})$ i fent la construcció de A) de la secció anterior, considerem el corresponent producte fibrat $B' = B \times_A A' \to A'$ i el problema d'immersió associat $EP' = (\gamma' : G \to A', \alpha' : B' \to A')$.
Tenim $m_\Sigma = m_{\Sigma'}$ i $\hat{\kappa}_{EP'} = \hat{\kappa}_\Sigma$ perquè $A' = Gal(\hat{\kappa}_\Sigma/\hat{\kappa})$.
El problema $\widetilde{EP'} = (\gamma', \alpha')$ domina EP de manera canònica. I cada solució regular i pròpia de $\widetilde{EP'}$ dóna lloc a una solució regular i pròpia de $\widetilde{EP}$. Per tant, podem suposar que tenim les arrels de la unitat. □

Volem trobar una solució de $\widetilde{EP}$ a partir de les successions exactes de grups del 1/2 Teorema d'existència de Riemann. Per això construïm ara tots els ingredients que necessitem per aquest teorema:

Pel Teorema de la base normal [La 93, Teor. VI, 13.1] sabem que existeix un element $x \in \hat{\kappa}_{EP}$ de manera que el conjunt $\{x_\sigma\}_{\sigma \in A}$ (on $x_\sigma = \sigma(x)$) és una base de $\hat{\kappa}_{EP}/\hat{\kappa}$ ja que $Gal(\hat{\kappa}_{EP}/\hat{\kappa}) = A$.

• El conjunt S del 1/2 Teorema d'existència de Riemann és un conjunt de punts tancats de $\mathbb{P}^1_{\hat{\kappa}}$ que anem a definir:
Triem elements $a_k \in \hat{\kappa}$ tals que $x_{k,\sigma} = a_k x_\sigma \ \forall \sigma, k$ siguin diferents. Prenem també, per cada k, elements $b_k \neq a_k$ de $\hat{\kappa}$ (suficientment propers a a_k per la topologia de la valoració) i posem $y_{k,\sigma} = b_k x_\sigma$.
Sigui $S \subset \mathbb{P}^1_{\hat{\kappa}}$ el conjunt finit de punts tancats definit per $x_{k,\sigma}$ i $y_{k,\sigma}$ $(\forall k, \sigma)$. Llavors, el canvi de base de S a la clausura algebraica de $\hat{\kappa}$ és

$$\overline{S} = S \times_{\hat{\kappa}} \overline{\hat{\kappa}} = \{x_{k,\sigma}, y_{k,\sigma} \mid \forall k, \sigma\} \subset \mathbb{P}^1_{\overline{\hat{\kappa}}} .$$

A més, si els b_k són suficientment propers a a_k, tenim que S és ajustat en parells, és a dir, $\overline{S}$ es pot organitzar en parells $P_{k,\sigma} = (x_{k,\sigma}, y_{k,\sigma})$ $\forall k, \sigma$, amb unes certes propietats vistes al capítol 2.

• El conjunt $U = \mathbb{P}^1_{\hat{\kappa}} \setminus S$ i $\overline{U} = U \times_{\hat{\kappa}} \overline{\hat{\kappa}}$.

- El grup $\overline{\Pi}$ és el grup profinit generat per:

$$\overline{\Pi} :=< g_{x_k,\sigma}, h_{y_k,\sigma} \mid g_{x_k,\sigma} h_{y_k,\sigma} = 1,\ \forall k, \sigma >$$

i dotat amb la $G_{\hat{\kappa}}$-acció per la dreta definida per: $(g_{x_{k,\sigma}})\hat{\tau} = (g_{x_{k,\tau^{-1}\sigma}})^{\chi(\hat{\tau})}$, on $\hat{\tau} \in G_{\hat{\kappa}}$, τ és la seva imatge en el grup $Gal(\hat{\kappa}_{EP}/\hat{\kappa}) = A$ i χ és el caràcter ciclotòmic.

Llavors, amb aquest elements, tenim una successió exacta split de grups fonamentals:

$$1 \to \pi_1(\overline{U}) \to \pi_1(U) \to G_{\hat{\kappa}} \to 1.$$

Pel 1/2 teorema d'existència de Riemann, de manera canònica, tenim el quocient:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\overline{U}) & \longrightarrow & \pi_1(U) & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} \ltimes \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \end{array}$$

on les fletxes verticals són exhaustives i $G_{\hat{\kappa}} \ltimes \overline{\Pi}$ està considerat respecte de l'acció canònica per la dreta de $G_{\hat{\kappa}}$ en $\overline{\Pi}$.

A partir d'aquesta segona successió exacta, volem construir una solució al problema $\widetilde{EP}$. Tenim:

$$\begin{array}{ccccccccc} & & & & & & G_{\hat{\kappa}} & & \\ & & & & & & \| & & \\ 1 & \longrightarrow & \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} \ltimes \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \\ & & \downarrow j & & & & \downarrow \gamma & & \\ 1 & \longrightarrow & F = ker(\widetilde{\alpha}) & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1. \end{array}$$

Definirem ara un homomorfisme $j : \overline{\Pi} \to F$ i, a partir d'ell, el morfisme de la part central de la successió exacta.

Definim:

$$\begin{aligned} j : \overline{\Pi} &\longrightarrow F \\ g_{x_{k,\sigma}} &\longrightarrow (g_{k,\sigma})^{-\chi_{EP}(\sigma)} \end{aligned}$$

on χ_{EP} és el caràcter ciclotòmic de A.

Afirmació 2: *j és compatible amb l'acció de $G_{\hat{\kappa}}$ en $\overline{\Pi}$ i en F via γ*

(Això es prova fent servir que $\hat{\kappa}_{EP}$ conté les arrels m_Σ-èsimes de la unitat i, per tant, d'ordre m_k per a tot k.)

Tenim, per tant, un diagrama commutatiu de successions exactes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} \ltimes \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \gamma \ltimes j} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & F = ker(\widetilde{\alpha}) & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1, \end{array}$$

i el diagrama total:

$$\begin{array}{ccccccccc} & & & & & & G_{\hat{\kappa}} & & \\ & & & & & & \| & & \\ 1 & \longrightarrow & \pi_1(\overline{U}) & \longrightarrow & \pi_1(U) & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} \ltimes \overline{\Pi} & \longrightarrow & G_{\hat{\kappa}} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \gamma \ltimes j} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & F = ker(\widetilde{\alpha}) & \longrightarrow & A \ltimes F & \xrightarrow{\widetilde{\alpha}} & A & \longrightarrow & 1. \end{array}$$

Podem veure $\pi_1(U)$ com el grup de Galois de la màxima extensió de $\kappa(t)$ no ramificada fora de S. Per tant, tenim un homomorfisme exhaustiu $G_{\kappa(t)} \to \pi_1(U)$.

Afirmació 3: *El morfisme*

$$\widetilde{\beta} : G_{\kappa(t)} \to \Pi_1(U) \to G_{\hat{\kappa}} \ltimes \overline{\Pi} \overset{\gamma \ltimes j}{\to} A \ltimes F$$

és una solució regular i pròpia de $\widetilde{EP}$.

Demostració: La solució és clarament pròpia perquè, per construcció tots els morfismes són exhaustius.

És regular perquè el nucli de la successió exacta dels grups fonamentals és $\pi_1(\overline{U})$.

□

4.3.2 Segon Lema

Lema 2: *Sigui $\hat{\kappa}/\kappa$ una extensió de cossos amb κ existencialment tancat en $\hat{\kappa}$ i $\hat{\Pi} : G_{\hat{\kappa}} \to G_\kappa$ la projecció canònica.*

Siguin $EP = (\gamma, \alpha)$ un problema d'immersió finit sobre κ i $\hat{EP} = (\gamma\hat{\Pi}, \alpha)$ el corresponent problema d'immersió per $\hat{\kappa}$.

Llavors, si $\hat{EP}$ té solucions regulars i pròpies, EP té solucions regulars i pròpies.

Demostració del Lema 2:

Per a la demostració d'aquest lema es fan servir arguments de tipus no-estàndard.

Com κ és existencialment tancat en $\hat{\kappa}$, per 4.1.4 existeix una ultrapotència de κ, ${}^*\kappa = \kappa^I/\mathcal{D}$ i una κ-immersió $\hat{\kappa} \hookrightarrow {}^*\kappa$.
Tenim, per tant, la projecció canònica ${}^*\Pi : G_{{}^*\kappa} \to G_\kappa$, i, a partir del problema d'immersió $EP = (\gamma, \alpha)$, podem considerar el problema ${}^*EP = ({}^*\gamma{}^*\Pi, \alpha)$.

Afirmació 4: *Si $\hat{\beta} : G_{\hat{\kappa}(t)\to B} \to B$ és una solució regular i pròpia de $\hat{EP}$, llavors ${}^*\beta : G_{{}^*\kappa(t)} \overset{can}{\to} G_{\hat{\kappa}(t)} \overset{\hat{\beta}}{\to} B$ és solució regular pròpia de ${}^*EP$.*

Per tant, si $\hat{EP}$ té solucions regulars i pròpies, llavors ${}^*EP$ té solucions regulars i pròpies.

Demostració:

- La solució és regular perquè, amb les notacions anteriors,

$$ {}^*\kappa_{{}^*\beta} = {}^*\kappa\hat{\kappa}_\beta = {}^*\kappa\hat{\kappa}_{\hat{EP}} = {}^*\kappa\kappa_{EP} = {}^*\kappa_{{}^*EP}. $$

- Per veure que la solució és pròpia, només cal veure que l'homomorfisme *can* és exhaustiu. Notem que la clausura algebraica de ${}^*\kappa$ és linealment disjunta amb la clausura algebraica de $\hat{\kappa}(t)$ sobre la clausura algebraica de $\hat{\kappa}$. □

Com estem suposant que $\hat{EP}$ té solucions regulars i pròpies, llavors ${}^*EP$ té solucions regulars i pròpies. Sigui ${}^*\beta$ una d'aquestes solucions i posem $L = ([{}^*\kappa(t)]^s)^{ker({}^*\beta)}$, és a dir, un cos solució de ${}^*EP$. Podem veure el cos $L =^* \kappa(t)(X_1,\ldots,X_n)$. Considerem $L^i =^* \kappa(t)(X_1(i),\ldots,X_n(i))$, $i \in I$ els representants locals de L. Aquests representants locals els tenim definits en [Po 88] (i, de fet, a partir del teorema d'il.lusió sobre l'estructura de les fórmules -exposició de C. Infante-).

Afirmació 5: *Els cossos $L^i/\kappa(t)$ són extensions de Galois que donen lloc a solucions regulars i pròpies de EP.*

La demostració està, de fet, en [Po 88].

4.3.3 Conclusions. Final de la demostració del Teorema

Sigui $EP = (\gamma,\alpha)$ un problema d'immersió sobre κ finit i split. Sigui $\hat{\kappa}$ el cos de sèries de Laurent sobre κ. El cos κ és existencialment tancat en $\hat{\kappa}$ perquè κ és gran (proposició 4.1.5). Sigui $\hat{EP} = (\gamma\hat{\Pi},\alpha)$ el corresponent problema d'immersió.

Pel Lema 1, el problema $\hat{EP} = (\gamma\hat{\Pi},\alpha)$ té solucions regulars i pròpies.

Pel Lema 2, el problema $EP = (\gamma,\alpha)$ té solucions regulars i pròpies. □

4.4 Teorema B

Teorema B: *Sigui κ un cos gran hilbertià.*

Tot problema d'immersió finit i split sobre κ té solucions regulars i pròpies.

Observem que a l'afegir al cos la hipòtesi de hilbertià, podem passar de solucions regulars a solucions pròpies.

4.4.1 Cossos hilbertians

En poques paraules, podem dir que un cos és hilbertià si compleix el teorema d'irreductibilitat de Hilbert. Recordem què diu aquest teorema:

Teorema d'irreductibilitat de Hilbert: *Sigui κ un cos de nombres i sigui $F \in \kappa[T_1, \dots T_r; X_1, \dots X_s]_{r,s,\geq 1}$ un polinomi irreductible. Aleshores existeixen infinites r-tuples $(t_1, \dots t_r) \in \mathbb{Z}^r$ de tal manera que el polinomi $F(t_1, \dots, t_r; X_1, \dots X_s) \in \kappa[X_1, \dots, X_s]$ és també irreductible.*

De manera més precisa, donem la definició de cos hilbertià que es troba a [La 83, Ch. 9].

Siguin κ un cos i $T = (T_1, \dots, T_r), X = (X_1, \dots, X_n)$ dos conjunts de variables. Siguin $f_1(T, X), \dots, f_m(T, X) \in \kappa(T)[X]$ polinomis irreductibles. Sigui $g \in \kappa[T]$ amb $g \neq 0$.

Definició 4.4.1. *El conjunt*

$$\mathcal{H}_\kappa(f_1, \dots f_m; g) := \{a \in \kappa^r \mid g(a) \neq 0, f_i(a, X) \in \kappa[X] \text{ estan definits i són irreductibles } \}$$

és un conjunt hilbertià.

Definició 4.4.2. *El cos κ es diu hilbertià si tots els conjunts hilbertians són no buits.*

En un cos hilbertià tots els conjunts hilbertians són no buits i infinits. En particular tot cos hilbertià és infinit.

Exemples de cossos hilbertians són: $\mathbb{Q}$, tots els cossos de nombres, $\mathbb{Q}^{ab}$.

Propietats dels cossos hilbertians:

1. *Si κ és un cos hilbertià, qualsevol extensió separable finitament generada L de κ és hilbertià.*

2. *En el cas anterior, tot conjunt hilbertià de L conté elements de κ.*

3. *Siguin κ un cos hilbertià i $K = \kappa(t)$ on t és una variable. Observem que l'anell d'enters de K és $\kappa[t]$. Sigui L/K una extensió de Galois finita.*
   Si $a \in \kappa$ considerem l'ideal $\mathfrak{p} = (t-a)$. El cos residual de K és $\kappa[t]/\mathfrak{p} \simeq \kappa$.
   Sigui B l'anell d'enters de L i denotem $\overline{L_\mathfrak{p}} = B/\mathfrak{p}$ el seu cos residual.

   Llavors, existeixen infinits valors $a \in \kappa$ pels quals

$$Gal(L/K) \simeq Gal(\overline{L_\mathfrak{p}}, \kappa[t]/\mathfrak{p}) = Gal(\overline{L_\mathfrak{p}}, \kappa).$$

   Observem que, com $\mathfrak{p}$ és inert,

$$Gal(L/K) \simeq Gal(\overline{L_\mathfrak{p}}, \kappa[t]/\mathfrak{p}) = D_\mathfrak{p}/I_\mathfrak{p} \simeq D_\mathfrak{p}.$$

4.4.2 Demostració del Teorema B

Sigui $EP = (\gamma : G_\kappa \to A, \alpha : B \to A)$ un problema d'immersió finit i split sobre κ. Denotem $K = \kappa(t)$, $\kappa_{EP} = (\kappa^s)^{ker(\gamma)}$ i $K_{EP} = \kappa_{EP}(t)$. Tenim el diagrama:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \Pi & & \\ & & & & & & G_\kappa & & \\ & & & & & & \downarrow \gamma & & \\ (E) & 1 & \longrightarrow & C = ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow 1. \end{array}$$

Sigui $\beta : G_K \to B$ una solució regular i pròpia, que existeix pel Teorema A i denotem per $L = (K^s)^{ker(\beta)}$ amb $L \cap \kappa^s = \kappa_{EP}$, un cos solució.

A nivell de grups de Galois, la successió exacta (E) queda:

$$1 \to Gal(L/K_{EP}) \to Gal(L/K) \to Gal(K_{EP}/K) \to 1.$$

Com κ és hilbertià, per les propietats anteriors, el cos extensió κ_{EP} és hilbertià i tot conjunt hilbertià de κ_{EP} conté elements de κ. Sigui $a \in \kappa$ i considerem l'ideal $\mathfrak{p} = (t-a)$ de manera que

$$\begin{aligned} Gal(L/K_{EP}) &\simeq Gal(\overline{L_\mathfrak{p}}/\kappa_{EP}), \\ Gal(L/K) &\simeq Gal(\overline{L_\mathfrak{p}}/\kappa), \\ Gal(K_{EP}/K) &\simeq Gal(\kappa_{EP}/\kappa). \end{aligned}$$

Sabem que existeixen infinits valors de $a \in \kappa$ pels quals tenim els isomorfismes anteriors, per les propietats dels cossos hilbertians. Així, per una d'aquestes especialitzacions en a la successió exacta (E) queda

$$1 \to Gal(\overline{L_\mathfrak{p}}/\kappa_{EP}) \to Gal(\overline{L_\mathfrak{p}}/\kappa) \to Gal(\kappa_{EP}/\kappa) \to 1.$$

Per tant, el cos $\overline{L_\mathfrak{p}}$ extensió de κ és una solució pròpia de EP.
□

4.5 Un darrer resultat

En aquesta secció demostrarem el següent resultat:

Teorema 4.5.1. *Sigui κ un cos gran i hilbertià. Si κ té dimensió cohomològica 1, llavors, tot problema d'immersió finit per G_κ té solucions pròpies.*

Observem que, en aquest cas en que el cos té dimensió cohomològica 1, es resolen tots els problemes d'immersió finits. De fet, que la dimensió cohomològica sigui 1 ens assegura l'existència de solucions que poden ser impròpies. Aplicant els resultats anteriors, en trobarem una de pròpia.

Demostració. El cos κ té dimensió cohomològica 1 si el grup G_κ té dimensió cohomològica 1. En aquest cas, el grup G_κ és projectiu, és

a dir, per a qualssevol successió exacta (E) i morfisme $\gamma : G_\kappa \to A$,

$$\begin{array}{cccccccccc} & & & & & & & & G_\kappa & \\ & & & & & & & & \downarrow \gamma & \\ (E) & 1 & \longrightarrow & C = ker(\alpha) & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1 \end{array}$$

existeix un morfisme $\beta : G_\kappa \to B$. Les propietats dels grups amb dimensió cohomològica 1, estan, per exemple en [Se 94].

Sigui $EP = (\gamma, \alpha)$ un problema d'immersió per G_κ. Com G_κ té dimensió cohomològica 1, existeix un morfisme β com l'anterior, que és una solució al problema d'immersió (que pot ser no pròpia). Anem a construir un problema d'immersió a partir d'aquest que ens en doni una de pròpia.

Sigui EP' el problema d'immersió que domina EP pel procés B), és a dir, considerem $A' = \beta(G_\kappa)$ i el problema

$$\begin{array}{ccc} & & G_\kappa \\ & & \downarrow \beta \\ B' = B \times_K A' & \xrightarrow{\alpha'} & A' \\ \downarrow \beta_0 & & \downarrow \gamma_0 \\ B & \xrightarrow{\alpha} & A. \end{array}$$

El problema $EP' = (\beta, \alpha')$ domina EP i és split (per la propietat universal del producte fibrat).

Pel Teorema B, el problema EP' té solucions pròpies i, per tant, EP té solucions pròpies. □

Podríem aplicar un argument similar sobre un cos gran hilbertià sempre que poguem assegurar l'existència d'una solució encara que no sigui pròpia, per passar a una de pròpia. Aquest resultat és una "generalització" del teorema de Ikeda que assegura que, si el nucli C és abelià, a partir d'una solució impròpia, podem construir una de pròpia.

Bibliografia

[La 93] S. Lang, *Algebra 3rd. ed.*, Addison-Wesley P. Comp., 1993.

[La 83] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[Ma-Ma 94] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Preprint 94-48, Heidelberg, 1994.

[Po 96] F. Pop, *Embedding problems over large fields*, Annals of Mathematics, **144** (1996), 1-34.

[Po 88] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. reine angew. Math., **392** (1988), 145-175.

[Se 94] J.P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, 5 (5è. édition, révisée et complétée), Berlin, 1994.

Capítol 5

Conjectura de Šafarevič semi-local

Núria Vila

L'objectiu d'aquesta part és presentar els resultats que, a més dels estudiats fins ara en els capítols anteriors, obté F. Pop en l'article [Po 96]. Aquests volen contribuir al coneixement de l'estructura del grup de Galois absolut d'un cos. Més concretament, els resultats s'emmarquen en el context de l'anomenada conjectura de Šafarevič. Voldria, doncs, donar una visió de com els resultats estudiats en els capítols anteriors incideixen en el coneixement de l'estructura del grup de Galois absolut d'una àmplia família de cossos, els que satisfan un principi local-global universal per l'existència de punts racionals sobre varietats. Aquests cossos constitueixen, a més, exemples interessants de cossos grans.

5.1 La conjectura de Šafarevič

La qüestió plantejada originalment per Šafarevič és que el grup de Galois absolut de $\mathbb{Q}^{\mathrm{ab}}$, la màxima extensió abeliana de $\mathbb{Q}$, ha de ser un grup profinit lliure. Del fet que, $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cycl}}$, la conjectura de

Šafarevič es formula:

Conjectura de Šafarevič (SC). El grup de Galois absolut $G_{K^{\mathrm{cycl}}}$ de K^{cycl}, la màxima extensió ciclotòmica d'un cos global K, és profinit lliure.

Resultats que en donen evidència:

1. Un teorema d'Iwasawa [Iw 53] que afirma que el grup de Galois de la màxima extensió resoluble de K^{cycl} sobre K^{cycl}, $\mathrm{Gal}(K^{\mathrm{sol}}/K^{\mathrm{cycl}})$, és proresoluble lliure, amb un nombre numerable de generadors lliures.
2. Un resultat de Tate (cf. [Se 94]) que ens diu que el grup de Galois absolut de K^{cycl} té dimensió cohomològica 1, i per tant $G_{K^{\mathrm{cycl}}}$ és un grup projectiu.

Si K és un cos global de característica positiva, es té que

$$K = \mathbb{F}_q(t) \qquad K^{\mathrm{cycl}} = \overline{\mathbb{F}_p}(t),$$

es parla de la conjectura de Šafarevič geomètrica:

Geometric (SC). Sigui K/k un cos de funcions en una variable sobre un cos algebraicament tancat k. Aleshores el grup de Galois absolut de K és profinit lliure.

La conjectura de Šafarevič geomètrica és certa. És un resultat clàssic, conseqüència del teorema d'existència de Riemann, per $k = \mathbb{C}$; via el principi de Lefschetz s'obté per k de característica zero (cf. [Do 64]). Per característica positiva, està relacionada amb la conjectura de Abhyankar i, fou provada per D. Harbater [Hb 95] utilitzant patching formal i per F. Pop [Po 95] utilitzant geometria rígida.

Presentació dels resultats

En l'article [Po 96] es proven els teoremes següents:

Teorema 1. *Sigui κ un cos numerable, PAC, hilbertià. Aleshores G_κ és profinit lliure.*

Cal tenir en compte que

1. Per característica zero va ser provat per Fried i Völklein [Fr-Vo 92], utilitzant el teorema d'existència de Riemann clàssic.

2. Frey [Fre 73] provà que $\mathbb{Q}^{\mathrm{ab}}$ no és PAC.

El segon teorema dóna una resposta afirmativa al que anomena conjectura de Šafarevič semi-local:

Sigui K un cos global i $\mathfrak{S}$ un conjunt finit de valoracions de K. Denotem per $K_{\mathfrak{p}}$ el completat de K en $\mathfrak{p} \in \mathfrak{S}$, i per $\mathbb{C}_{\mathfrak{p}}$ el completat de $\overline{K_{\mathfrak{p}}}$. Un element $a \in \overline{K}$ s'anomena totalment $\mathfrak{p}$-àdic si per a tota K-immersió $\iota : \overline{K} \hookrightarrow \mathbb{C}_{\mathfrak{p}}$ és $\iota(a) \in K_{\mathfrak{p}}$.

Considerem $K^{\mathfrak{S}}$ el màxim subcos de $\overline{K}$ totalment $\mathfrak{S}$-àdic, és a dir, format per elements totalment $\mathfrak{p}$-àdics, per a tot $\mathfrak{p} \in \mathfrak{S}$. Remarquem que aquesta és la generalització natural de cos totalment real i de cos totalment p-àdic.

Denotem per $K^{\mathfrak{S},\mathrm{cycl}}$ l'extensió ciclotòmica maximal de $K^{\mathfrak{S}}$.

Teorema 2 (conjectura de Šafarevič semi-local). *El grup de Galois absolut de $K^{\mathfrak{S},\mathrm{cycl}}$ és profinit lliure.*

Val a dir que podem pensar que els cossos $K^{\mathfrak{S},\mathrm{cycl}}$ aproximen, per sobre, K^{cycl}, quan el conjunt finit de primers $\mathfrak{S}$ es va engrandint. Dit amb una mica més de precisió, és clar que

$$K \subseteq K^{\mathfrak{S}} \subset \overline{K}$$

i que $K^{\mathfrak{S}} = \overline{K}$ si $\mathfrak{S} = \emptyset$. Si engrandim el conjunt finit de primes $\mathfrak{S}$, fem més petit el cos $K^{\mathfrak{S}}$, relativament a $\overline{K}$. D'altra banda,

$$K^{\mathrm{cycl}} \subseteq K^{\mathfrak{S},\mathrm{cycl}} \subset \overline{K}.$$

La conjectura de Šafarevič (SC) prediu que el grup de Galois absolut $G_{K^{\mathrm{cycl}}}$ és profinit lliure, el teorema 2 diu que $G_{K^{\mathfrak{S},\mathrm{cycl}}}$ és profinit lliure. Ara, $G_{K^{\mathfrak{S},\mathrm{cycl}}} \subset G_{K^{\mathrm{cycl}}}$. En conseqüència, la conjectura de Šafarevič semi-local dóna evidencia de la conjectura de Šafarevič.

En el treball es prova un tercer teorema que és un teorema d'estructura del grup $G_{K^{\mathfrak{S}}}$ i que nosaltres, aquí, només enunciarem.

Si $\mathfrak{p} \in \mathfrak{S}$, sigui $X_\mathfrak{p}$ el conjunt d'extensions de $\mathfrak{p}$ a $K^\mathfrak{S}$. $X_\mathfrak{p}$ és un espai compacte, totalment disconnex, en el que $\mathrm{Gal}(K^\mathfrak{S}/K)$ hi actua contínuament, transitivament i fidelment. Per tant, $X_\mathfrak{p}$ és homeomorf a l'espai topològic subjacent de $\mathrm{Gal}(K^\mathfrak{S}/K)$. Sigui $G_\mathfrak{p} = \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$, on $K_\mathfrak{p}$ és el completat de K a $\mathfrak{p}$. Es defineix $F_{G_\mathfrak{p},X_\mathfrak{p}}$, producte lliure profinit generalitzat de $G_\mathfrak{p}$ en l'espai $X_\mathfrak{p}$ i es prova

Teorema 3.

$$G_{K^\mathfrak{S}} \simeq \star_{\mathfrak{p}\in\mathfrak{S}} F_{G_\mathfrak{p},X_\mathfrak{p}}.$$

Remarquem que:

1. En el cas en què $\mathfrak{S}$ conté només valoracions reals el resultat fou provat per Fried-Haran-Völklein [Fr-Ha-Vo 93], utilitzant d'altres mètodes.
2. A [Po 96] es proven els teoremes 2 i 3 en un context una mica més general. El cos global K és substituït per κ cos numerable, hilbertià i $\mathfrak{S}$ per un conjunt finit de valoracions de κ de tipus local, això és, $\kappa_\mathfrak{p}$ és un cos localment compacte, separablement generat sobre κ.

A continuació intentarem donar una visió i analitzar els ingredients fonamentals per obtenir una prova dels teoremes 1 i 2.

5.2 Freiheitssatz de Iwasawa

Abans de res donem un teorema vital per comprendre els lligams entre els resultats obtinguts fins ara, en particular els del Capítol 4, i els que volem obtenir. El teorema de la llibertat de Iwasawa [Iw 53], th. 4.

Teorema 5.2.1. *(Freiheitssatz) Sigui G un grup profinit de rang numerable (infinit). La condició necessària i suficient perquè el grup G sigui profinit lliure és que tot problema d'immersió finit per G tingui solucions pròpies.*

De fet aquest teorema és cert per una classe $\underline{C}$ de subgrups, és a dir una classe de subgrups finits tancada per subgrups, quocients per

subgrups normals i per producte directe de subgrups. Com exemples de classes $\underline{C}$ de subgrups interessants destaquem: els grups finits; els p-grups; els grups resolubles; els grups abelians; els grups nilpotents; els grups cíclics. Així, el Freiheitssatz de Iwasawa diu que la condició necessària i suficient per que el grup profinit G de rang numerable sigui pro-$\underline{C}$-grup lliure és que tot $\underline{C}$-problema d'immersió per G tingui solucions pròpies.

Una demostració clara d'aquest resultat i del background que involucra es troba en les notes de L. Ribes [Ri 70].

Es prova primer un lema tècnic:

Lema 5.2.2. *Sigui G un grup profinit, és equivalent*

(i) *G satisfà l'axioma de la numerabilitat*

(ii) *G es pot generar per un conjunt numerable A convergent a 1, és a dir, un entorn obert de 1 conté quasi tot element de A.* □

En particular, un grup profinit G de rang numerable admet una base numerable de subgrups oberts normals de G tals que $U_1 \supseteq U_2 \supseteq \cdots \supseteq U_i \supseteq \cdots$.

Demostració. (Freiheitssatz) Si G és un grup lliure sobre el conjunt $\{\sigma_1, \sigma_2, \sigma_3, \ldots\}$, considerem el problema d'immersió:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle \phi} & & \\ 1 & \longrightarrow & C & \longrightarrow & B & \xrightarrow{j} & A & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array}$$

El grup A està generat pels $\phi(\sigma_i)$. A més, existeix un k tal que $\phi(\sigma_i) = 1$ per a tot $i > k$. Escollim elements $h_i \in B$ tals que: (1) generen B; (2) $h_i = 1$, per quasi tot i; (3) $j(h_i) = \phi(\sigma_i)$. Definim $\psi : G \longrightarrow B$ com $\psi(\sigma_i) = h_i$, per a tot i. És clar que ψ és epijectiu, per construcció, i que $j \circ \psi = \phi$.

Recíprocament, sigui F un grup profinit lliure amb una base numerable. Sigui

$$F \supseteq F_1 \supseteq \cdots \supseteq F_n \supseteq \cdots$$

base de subgrups oberts i normals de F. Sigui

$$G \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq \cdots$$

base de subgrups oberts i normals de G.

Volem construir noves bases de subgrups oberts i normals de F i de G, a partir de les anteriors: $F \supseteq F'_1 \supseteq \cdots \supseteq F'_n \supseteq \cdots$; $G \supseteq G'_1 \supseteq \cdots \supseteq G'_n \supseteq \cdots$, de manera que els sistemes projectius

$$\{F/F'_i\}_i \qquad \text{i} \qquad \{G/G'_i\}_i$$

siguin isomorfs. Això ens donarà isomorfismes en els límits projectius i en conseqüència l'isomorfisme $G \simeq F$.

Construirem els nous subgrups per inducció sobre i:

Siguin $F'_1 = F_1 = F$, $G'_1 = G_1 = G$; suposem que tenim construïts F'_i i G'_i per $i = 1, 2, \ldots, n$, tals que:

i) $F'_i \subseteq F_i$, $G'_i \subseteq G_i$

ii) $F \supseteq F'_1 \supseteq F'_2 \supseteq \cdots \supseteq F'_n$
$G \supseteq G'_1 \supseteq G'_2 \supseteq \cdots \supseteq G'_n$

iii) Els diagrames

$$\begin{array}{ccc} F/F'_i & \xrightarrow{\simeq} & G/G'_i \\ \downarrow & & \downarrow \\ F/F'_{i-1} & \xrightarrow{\simeq} & G/G'_{i-1} \end{array}$$

commuten.

Anem a construir F'_{n+1} i G'_{n+1}. Siguin

$\Phi = F'_n \cap F_{n+1}$,

$\Gamma = G'_n \cap G_{n+1}$,

i $\phi : G \longrightarrow F/\Phi$ una solució al problema d'immersió:

$$\begin{array}{ccccc} & & G & & \\ & & \downarrow & & \\ F/\Phi & \longrightarrow & F/F'_n \simeq G/G'_n & \longrightarrow & 1. \end{array}$$

Siguin $\Delta = \ker(\phi) \cap \Gamma$ i $\delta : F \longrightarrow G/\Delta$ una solució al problema d'immersió:

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow & & \\ G/\Delta & \longrightarrow & F/\Phi & \longrightarrow & 1 \end{array}$$

Sigui $\Lambda = \ker(\delta) \subset \Phi$, δ indueix un isomorfisme $F/\Lambda \simeq G/\Delta$. Prenem $F'_{n+1} = \Lambda$ i $G'_{n+1} = \Delta$, que clarament satisfan les condicions volgudes. □

Com a conseqüència d'aquest teorema i del Teorema 4.5.1 obtingut al Capítol 4 es té:

Corol.lari 5.2.3. *Sigui κ un cos hilbertià, numerable, gran amb dimensió cohomològica 1. Aleshores G_κ és un grup profinit lliure de rang numerable.*

5.3 Cossos satisfent un principi local-global universal

Anem ara a definir el que entendrem per cossos satisfent un principi local-global universal i a provar que són cossos grans. A més veurem que els cossos PAC, PRC i PpC en són, de fet, casos particulars.

Sigui κ un cos qualsevol i κ^s una clausura separable de κ.

Definició 5.3.1. *Una* **localitat** *de κ és una extensió Λ/κ algebraica i separable tal que és o bé real tancada o bé henseliana respecte de una valoració de κ no trivial.*

Per exemple $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$ és una localitat de $\mathbb{Q}$.

Definició 5.3.2. *Sigui $\mathcal{L}$ un conjunt de localitats de κ. Es diu que el cos κ satisfà un* **principi local-global universal respecte el conjunt** *$\mathcal{L}$, si per a tota varietat X sobre κ llisa, geomètricament íntegra es té:*

$$Si \quad X(\Lambda) \neq \emptyset, \quad per\ a\ tot \quad \Lambda \in \mathcal{L} \quad és \quad X(\kappa) \neq \emptyset.$$

Casos particulars:

• Si $\mathcal{L} = \emptyset$, un cos κ satisfà un principi local-global universal respecte el conjunt $\mathcal{L}$ si $X(\kappa) \neq \emptyset$, per a tota varietat X/κ llisa i geomètricament íntegra. Els cossos satisfent aquesta propietat s'anomenen PAC (pseudo-algebraicament tancats)

• Si $\mathcal{L} =\{$ totes les clausures reals de $\kappa\}$, un cos κ que satisfà un principi local-global universal respecte el conjunt $\mathcal{L}$ s'anomena PRC (pseudo-realment tancat)

• Si $\mathcal{L} =\{$ totes les clausures p-àdiques de $\kappa\}$, un cos κ que satisfà un principi local-global universal respecte el conjunt $\mathcal{L}$ s'anomena PpC (pseudo-p-àdicament tancat)

• Més generalment, si $\mathcal{L} =\{$ totes les $\mathbb{K}$ clausures de $\kappa\}$, on $\mathbb{K}$ és un conjunt finit de cossos clàssics, és a dir, cossos localment compactes de característica zero. Un cos κ s'anomena pseudo-clàssicament tancat si satisfà un principi local-global universal respecte el conjunt $\mathcal{L}$.

Teorema 5.3.3. *Sigui κ un cos satisfent un principi local-global universal respecte un conjunt de localitats $\mathcal{L}$ aleshores κ és un cos gran.*

Demostració. Sigui X una corba llisa sobre κ tal que $X(\kappa) \neq \emptyset$. Podem suposar que X és geomètricament íntegra, prenent la component connexa amb punts κ-racionals. Volem provar que $X(\kappa)$ és infinit. Això és equivalent a dir que per a tot obert afí U de X és $U(\kappa) \neq \emptyset$. Si $\mathcal{L} = \emptyset$, aleshores κ és PAC, per tant $U(\kappa) \neq \emptyset$, per definició. Si $\mathcal{L} \neq \emptyset$, sigui $\Lambda \in \mathcal{L}$, aleshores $X(\Lambda)$ és Zariski dens, per tant $U(\kappa) \neq \emptyset$, per a tot U obert afí. Donat que κ satisfà un principi local-global universal respecte el conjunt $\mathcal{L}$ es té $U(\kappa) \neq \emptyset$. □

Ara podem provar el teorema 1

Teorema 5.3.4. *Sigui κ numerable, PAC i hilbertià, aleshores G_κ és profinit lliure de rang numerable.*

Demostració. Un teorema de Ax [Ax 68] (cf. [Se 94]) ens diu que si κ és PAC, aleshores la dimensió cohomològica de G_κ és ≤ 1. D'altra banda, pel teorema anterior tot cos κ PAC és un cos gran. Aplicant el Corol·lari 5.2.3 s'obté el teorema. □

5.4 Topologies étale i estricta. Conjunts de tipus local

Sigui κ un cos qualsevol i κ^s una clausura separable de κ. En el conjunt de tots els κ-subcossos Λ' de κ^s podem considerar la topologia étale i la topologia estricta. Aquestes són, per definició, les que tenen com a base d'entorns conjunts de la forma:

étale: $\mathcal{U}^{et}_{\Lambda,\lambda} = \{\Lambda' : \Lambda \cap \lambda \subseteq \Lambda' \cap \lambda\}$, on $\kappa \subset \Lambda$, $\lambda \subset \kappa^s$ recorren el conjunt de totes les subextensions.

estricte: $\mathcal{U}^{st}_{\Lambda,\lambda} = \{\Lambda' : \Lambda \cap \lambda = \Lambda' \cap \lambda\}$, on $\kappa \subset \Lambda$, $\lambda \subset \kappa^s$ recorren el conjunt de totes les subextensions Galois finites.

Sigui G un grup profinit, en el conjunt de tots els subgrups tancats Γ' de G (per la topologia profinita) podem considerar la topologia étale i la topologia estricta. Aquestes són, per definició, les que tenen com a base d'entorns conjunts de la forma:

étale: $\mathcal{U}^{et}_{\Gamma,N} = \{\Gamma' : N\Gamma' \subset N\Gamma\}$, on Γ, N recorren el conjunt de subgrups tancats de G.

estricte: $\mathcal{U}^{st}_{\Gamma,N} = \{\Gamma' : N\Gamma' = N\Gamma\}$, on Γ, N recorren el conjunt de subgrups oberts i normals de G.

Sigui $G_\kappa = \mathrm{Gal}(\kappa^s/\kappa)$ el grup de Galois absolut de κ. És clar, per construcció, que la correspondència del teorema fonamental de la teoria de Galois entre els subgrups tancats $\Gamma \subset G_\kappa$ i els subcossos $\Lambda \subset \kappa^s$ és un homomorfisme per les topologies étale i estricta.

Definició 5.4.1. *Un conjunt de localitats $\mathcal{L}$ de κ (cf. 5.3.1) es diu de* **tipus local** *si és tancat per l'acció del grup G_κ, i es pot escriure com $\mathcal{L} = \mathcal{L}_\infty \cup \mathcal{L}_*$, on $\mathcal{L}_\infty$ i $\mathcal{L}_*$ són tancats per la topologia estricta i satisfan:*

1. *Tot $\Lambda \in \mathcal{L}_\infty$ té grup de Galois absolut $G_\Lambda \simeq G_{\mathbb{R}}$.*
2. *Tot $\Lambda \in \mathcal{L}_*$ té grup de Galois absolut G_Λ isomorf al grup de Galois absolut d'algun cos no-arquimedià localment compacte.*

La definició corresponent per a subgrups tancats d'un grup profinit G és:

Definició 5.4.2. *Un conjunt de subgrups tancats $\mathcal{G}$ de G es diu de* **tipus local** *si és tancat per la conjugació interna, i es pot escriure com $\mathcal{G} = \mathcal{G}_\infty \cup \mathcal{G}_*$, on $\mathcal{G}_\infty$ i $\mathcal{G}_*$ són tancats per la topologia estricta i satisfan:*

1. *Tot $\Gamma \in \mathcal{G}_\infty$ és isomorf al grup de Galois absolut dels reals $G_{\mathbb{R}}$.*
2. *Tot $\Gamma \in \mathcal{G}_*$ és isomorf al grup de Galois absolut d'algun cos no-arquimedià localment compacte.*

5.5 Grups relativament projectius

Sigui G un grup profinit i $\mathcal{G}$ un conjunt de subgrups tancats, quasi-compacte per la topologia étale.

Un problema d'immersió finit per G relatiu a $\mathcal{G}$ és:

$$\mathrm{EP}_{\mathcal{G}} = (\gamma,\ \alpha,\ \mathcal{B}),$$

on EP=$(\gamma,\ \alpha)$ és un problema d'immersió per G i $\mathcal{B}$ és un conjunt de subgrups tancats tals que per a tot $\Gamma \in \mathcal{G}$ el problema d'immersió local $\mathrm{EP}_\Gamma = (\gamma_\Gamma, \alpha_\Gamma)$, on $\gamma_\Gamma = \gamma|\Gamma$ i

$$\alpha_\Gamma : \alpha^{-1}(\gamma(\Gamma)) \xrightarrow{\alpha} \gamma(\Gamma),$$

té solucions β_Γ tals que $\beta_\Gamma(\Gamma) \in \mathrm{con}(\mathcal{B})$. Denotem per $\mathrm{con}(\mathcal{B})$ el més petit conjunt de subgrups tancats de G contenint $\mathcal{G}$, G-invariant i tancat per subgrups.

Una solució de $\mathrm{EP}_{\mathcal{G}}$ és un morfisme $\beta : G \to B$ tal que $\gamma = \alpha\,\beta$, és a dir una solució de EP.

Una solució forta de $\mathrm{EP}_{\mathcal{G}}$ és un morfisme $\beta : G \to B$ tal que $\gamma = \alpha\ \beta$ i $\beta(\mathcal{G}) \subseteq \mathrm{con}(\mathcal{B})$

Definició 5.5.1. *Un grup G es diu que és $\mathcal{G}$-projectiu (resp. fortament) si tot $\mathcal{G}$-problema d'immersió per G té solucions (resp. fortes).*

Cal tenir en compte que es pot provar

Teorema 5.5.2. *Sigui G un grup profinit i $\mathcal{G}$ un conjunt de tipus local de subgrups tancats de G. Si tot $\mathcal{G}$-problema d'immersió per G té solucions (pròpies), aleshores tot $\mathcal{G}$-problema d'immersió per G té solucions fortes (pròpies).*

Un resultat important pels nostres propòsits és

Teorema 5.5.3. *Sigui κ un cos satisfent un principi local-global universal respecte d'un conjunt $\mathcal{L}$ de localitats, G_κ-invariant i quasi-compacte per la topologia étale. Considerem G_κ amb el conjunt de subgrups tancats $\mathcal{G}_\mathcal{L} = \{\mathcal{G}_\Lambda : \Lambda \in \mathcal{L}\}$. Aleshores G_κ és $\mathcal{G}_\mathcal{L}$-projectiu.*

En particular, G_κ té dimensió cohomològica ≤ 1 si i només si totes les localitats $\Lambda \in \mathcal{L}$ tenen dimensió cohomològica ≤ 1.

Una idea de la demostració és a [Po 96]. Nosaltres, de fet, utilitzarem la darrera part que permet provar que G_κ té dimensió cohomològica ≤ 1 si la dimensió cohomològica de totes les localitats $\Lambda \in \mathcal{L}$ és ≤ 1, sempre que κ satisfaci un principi local-global universal respecte d'un conjunt $\mathcal{L}$ de localitats G_κ-invariant i quasi-compacte per la topologia étale.

5.6 Cossos totalment $\mathfrak{S}$-àdics

Sigui κ un cos i κ^s una clausura separable de κ.

Definició 5.6.1. *Una valoració $\mathfrak{p}$ de κ es diu de* **tipus local** *si el completat $\kappa_\mathfrak{p}$ de κ en $\mathfrak{p}$ és un cos localment compacte i separablement generat sobre κ.*

Definició 5.6.2. *Sigui $\mathfrak{p}$ una valoració de tipus local de κ, i $\mathbb{C}_\mathfrak{p}$ el completat d'una clausura algebraica de $\kappa_\mathfrak{p}$. Diem que un element $a \in \overline{\kappa}$ és* **totalment $\mathfrak{p}$-àdic** *si per a tota κ-immersió $\iota : \overline{\kappa} \hookrightarrow \mathbb{C}_\mathfrak{p}$ es té $\iota(a) \in \kappa_\mathfrak{p}$.*

Notem que la noció d'element totalment $\mathfrak{p}$-àdic generalitza, de manera natural, la noció de nombre algebraic totalment real o totalment p-àdic.

Definició 5.6.3. *Sigui $\mathfrak{S}$ un conjunt finit de valoracions de κ de tipus local. Un element algebraic a sobre κ és* **totalment $\mathfrak{S}$-àdic** *si a és* **totalment $\mathfrak{p}$-àdic** *per a tot $\mathfrak{p} \in \mathfrak{S}$.*

Denotem per $\kappa^\mathfrak{S}$ el conjunt de tots els elements de $\overline{\kappa}$ totalment $\mathfrak{S}$-àdics, és a dir, format per elements totalment $\mathfrak{p}$-àdics, per a tot $\mathfrak{p} \in \mathfrak{S}$, on $\mathfrak{S}$ és un conjunt finit de valoracions de κ de tipus local.

Observem que l'extensió $\kappa^{\mathfrak{S}}/\kappa$ és de Galois. Denotem per $\mathcal{L}^{\mathfrak{p}}$ el conjunt de cossos de descomposició de totes les extensions de $\mathfrak{p}$ a κ^s i per $\mathcal{L}^{\mathfrak{S}}$ la reunió dels $\mathcal{L}^{\mathfrak{p}}$, per a tot $\mathfrak{p} \in \mathfrak{S}$.

Són fàcils de provar els fets següents:

- L'extensió $\kappa^{\mathfrak{S}}/\kappa$ és de Galois.
- $\kappa^{\mathfrak{S}}$ és la intersecció de totes les localitats $\Lambda \in \mathcal{L}^{\mathfrak{p}}$.
- El grup de Galois absolut $G_{\kappa^{\mathfrak{S}}}$ de $\kappa^{\mathfrak{S}}$ és el subgrup tancat de G_κ generat pels grups de descomposició de totes les extensions de $\mathfrak{p} \in \mathfrak{S}$ a κ^s.
- $\mathcal{L}^{\mathfrak{p}}$ amb la topologia étale és homeomorf a l'espai quocient $G_\kappa/D_{\mathfrak{p}}$, on $D_{\mathfrak{p}}$ és el grup de descomposició d'alguna extensió de $\mathfrak{p}$ a κ^s.
- $\mathcal{L}^{\mathfrak{p}}$ és compacte amb la topologia étale.
- $\mathcal{L}^{\mathfrak{S}}$ és compacte amb la topologia étale.
- $\mathcal{L}^{\mathfrak{S}}$ és un conjunt de localitats de κ de tipus local.

Teorema 5.6.4. *($\mathfrak{S}$) Sigui λ una extensió algebraica de $\kappa^{\mathfrak{S}}$. Sigui $\mathcal{L} = \{\Lambda\lambda | \Lambda \in \mathcal{L}^{\mathfrak{S}}\}$ el conjunt de les extensions de $\mathcal{L}^{\mathfrak{S}}$ a λ. Aleshores λ satisfà un principi local-global universal respecte de $\mathcal{L}$.*

Aquest resultat és una generalització del principi local-global de Rumely. La seva prova és difícil. Una idea d'aquesta prova es troba en un apèndix de l'article de Pop [Po 96], la prova està en [Gr-Ma-Po 95]. Involucra la restricció de Weil i arguments tipus Bertini, entre d'altres.

En particular i en conseqüència, els cossos d'elements algebraics totalment reals o els totalment p-àdics són cossos PRC o PpC. A més, si tot $\Lambda\lambda \in \mathcal{L}$ és separablement tancat, λ és PAC. En particular, $\kappa^{\mathfrak{S},\mathrm{sol}}$ és un cos PAC.

Finalment, estem en condicions de provar el teorema 2. De fet donarem la prova d'un teorema en les condicions més generals d'aquest paràgraf, per obtenir, així, una prova del teorema 2.

Teorema 5.6.5. *Sigui κ un cos numerable i hilbertià. Sigui $\mathfrak{S}$ un conjunt finit de valoracions de κ de tipus local. Aleshores $G_{\kappa^{\mathfrak{S},cycl}}$ és profinit lliure.*

Demostració. Sigui $\lambda = \kappa^{\mathfrak{S},\mathrm{cycl}}$, es té que:

1. λ és un cos gran: λ és una extensió algebraica de $\kappa^{\mathfrak{S}}$, pel Teorema $\mathfrak{S}$ satisfà un principi local-global universal, en conseqüència, pel Teorema 5.3.3, λ és un cos gran.

2. λ és un cos hilbertià: Sigui $S \neq \emptyset$ un conjunt de nombres primers i $\kappa^{\mathfrak{S}}(\mu_S)$ el cos obtingut al adjuntar a $\kappa^{\mathfrak{S}}$ totes les arrels de la unitat amb ordre divisible només pels primers de S. Els cossos $\kappa^{\mathfrak{S}}(\mu_S)$ són una extensió de $\kappa^{\mathfrak{S}}$ i si S i T són dos conjunts de nombres primers no comparables per la relació de inclusió, els cossos $\kappa^{\mathfrak{S}}(\mu_S)$ i $\kappa^{\mathfrak{S}}(\mu_T)$ tampoc ho són. Escollim conjunts S i T de nombres primes no comparables per la inclusió tals que la seva reunió és el conjunt de tots els nombres primes. El cossos $\kappa^{\mathfrak{S}}(\mu_S)$ i $\kappa^{\mathfrak{S}}(\mu_T)$ són extensions de Galois del cos κ, que per hipòtesi és hilbertià, i el seu compositum és λ, aleshores λ és hilbertià (cf. [Ha-Ja 91]).

3. λ té dimensió cohomològica 1: $\mathcal{L} = \{\Lambda\lambda | \Lambda \in \mathcal{L}^{\mathfrak{S}}\}$ és el conjunt de les extensions de $\mathcal{L}^{\mathfrak{S}}$ a λ. Pel Teorema $\mathfrak{S}$, λ satisfà un principi local-global respecte de $\mathcal{L}$. Pel Teorema 5.5.3 n'hi ha prou en veure que $\Lambda\lambda \in \mathcal{L}$ té dimensió cohomològica 1. Ara $\Lambda^{\mathrm{cycl}} = \Lambda\lambda$, té dimensió cohomològica 1.

D'altra banda, λ és numerable, i aplicant el Corol·lari 5.2.3 obtenim el resultat. □

Bibliografia

[Ax 68] Ax, J.: *The elementary theory of finite fields*, Annals of Mathematics **88** (1968), 239-271.

[Do 64] Douady, A.: *Détermination d'un groupe de Galois*, C. R. Acad. Sci. Paris **258** (1964), 5305-5308.

[Fre 79] Frey, G.: *Pseudo algebraically closed fields with non-archimedian real valuations*, Journal of Algebra **26** (1973), 202-207.

[Fr-Ha-Vo 93] Fried, M.: Haran, D.; Völklein, H.: *Absolute Galois group of the totally real numbers*, C. R. Acad. Sci. Paris **317** (1993), 995-999.

[Fr-Ja 86] Fried, M.; Jarden, M.: *Field arithmetic,* Springer, 1986.

[Fr-Vo 92] Fried, M.; Völklein, H.: *The embedding problem over a Hilbertian PAC-field*, Annals of Mathematics **135** (1992), 469-480.

[Gr-Ma-Po 95] Green, B.-W.; Matignon, M.; Pop, F.: *On the local Skolem property*, J. reine angew. Math. **458** (1995), 183-199.

[Ha-Ja 91] Haran, D.; Jarden, M.: *Compositum of Galois extensions of hilbertian fields*, Ann. Scient. Éc. Normal Sup., 4è série **24** (1991), 739-748.

[Hb 95] Harbater, D.: Fundamental groups and embedding problems in characteristic p, in *Recent Developments*

in the Inverse Galois Problem, ed. M. Fried; et al., A.M.S. Contemporary Mathematics **186**(1995), 353-369.

[Iw 53] Iwasawa, K. *On solvable extensions of number fields*, Annals of Mathematics **58** (1953), 548-572.

[Po 94] Pop, F.: $\frac{1}{2}$ Riemann existence theorem with Galois action, in *Algebra and Number Theory*, ed. G. Frey; J. Ritter, de Gruyter Proceedings in Mathematics, 1994.

[Po 95] Pop, F.: *Étale Galois covers of affine smooth curves*, Inventiones Math. **120** (1995), 555-578.

[Po 96] Pop, F.: *Embedding problems over large fields*, Annals of Mathematics **144** (1996), 1-34.

[Ri 70] Ribes, L.: *Introduction to profinite groups and Galois cohomologie*, Queen's papers in Pure and Applied Mathematics **24**, Ontario, 1970.

[Se 94] Serre, J-P.: *Cohomologie Galoisienne*, Lecture Notes in Mathematics, 5 (5è. édition, révisée et complétée), Berlin, 1994.