UNIVERSITAT DE BARCELONA
Departament d'Àlgebra i Geometria

Grups de Galois sobre $\mathbb{Q}$ amb condicions de ramificació prefixades

Bernat Plans i Berenguer

Grups de Galois sobre $\mathbb{Q}$ amb condicions de ramificació prefixades

Memòria presentada per a optar al grau
de doctor en Matemàtiques per

Bernat Plans i Berenguer

Universitat de Barcelona, 2003

Departament d'Àlgebra i Geometria
Programa de Doctorat d'Àlgebra i Geometria, Bienni 1994-1996
Doctorand: Bernat Plans i Berenguer
Directora de Tesi: Dra. Núria Vila i Oliva

Núria Vila i Oliva, Professora Titular d'Àlgebra
de la Facultat de Matemàtiques de la Universitat de Barcelona,
FAIG CONSTAR
que el senyor Bernat Plans i Berenguer ha realitzat aquesta memòria
per a optar al grau de doctor en Matemàtiques sota la meva direcció.

Barcelona, febrer de 2003

Firmat: Núria Vila i Oliva

A l'Helena, el Pol, la Mireia i els pares

Índex

Introducció

El context general en el qual s'inscriu aquesta memòria el proporciona el problema invers de la teoria de Galois sobre el cos $\mathbb{Q}$ dels racionals. Aquest problema clàssic, encara obert, pregunta si tot grup finit es pot realitzar com a grup de Galois d'alguna extensió de $\mathbb{Q}$. El nostre objectiu principal és estudiar versions refinades d'aquest problema que s'obtenen quan prefixem determinades condicions de ramificació, com ara el nombre de primers que ramifiquen o el tipus de ramificació en l'extensió de cossos. Més concretament, les nostres contribucions estan centrades en els problemes següents:

Problema 1: Donat un grup finit G, quin és el mínim natural $ram(G)$ per al qual existeix alguna extensió de Galois de $\mathbb{Q}$ ramificada només en $ram(G)$ primers i amb grup de Galois isomorf a G?

Problema 2: Donats un grup finit G i un conjunt finit de primers racionals S, existeix alguna realització de G com a grup de Galois d'una extensió de $\mathbb{Q}$ no ramificada en S?

Una de les nostres motivacions a l'hora d'estudiar el problema 2 prové de la següent qüestió plantejada per Birch [Bir94], també coneguda com el problema invers moderat de la teoria de Galois.

Problema 3: Donat un grup finit G, existeix alguna extensió de Galois $F/\mathbb{Q}$ moderadament ramificada i amb grup de Galois $\mathrm{Gal}(F/\mathbb{Q}) \cong G$?

Si S és el conjunt de primers que divideixen l'ordre d'un grup finit G, aleshores una resposta afirmativa al problema 2 per a G i S implica, trivialment, una

resposta afirmativa al problema 3 per a G. Sovint, el mateix tipus d'arguments que ens permeten respondre afirmativament al problema 3 per a un grup finit G donat, proporcionen també una resposta afirmativa al problema 2 per a G i per a qualsevol conjunt finit S. De vegades, fins i tot, podem abordar versions més fortes del problema 2 dels tipus següents:

Problema 2.1: Donats un grup finit G i un conjunt finit de primers racionals S, existeix alguna realització de G com a grup de Galois d'una extensió de $\mathbb{Q}$ en la qual tots els primers de S descomponen completament?

Problema 2.2: Donats un grup finit G i un conjunt finit de primers racionals S, existeix alguna realització de G com a grup de Galois sobre $\mathbb{Q}$ d'un polinomi irreductible i mònic de $\mathbb{Z}[X]$ amb discriminant no divisible per cap primer de S?

Alguns resultats coneguts

Si G és un grup abelià finit qualsevol, el Teorema de Kronecker-Weber permet respondre les qüestions dels problemes 1, 2 i 3. El nombre mínim de primers ramificats en el problema 1 és, genèricament, el nombre mínim de generadors de G. El problema 2 admet una resposta afirmativa per a qualsevol conjunt finit S. A més, si G és un grup abelià finit sense elements d'ordre 8, aleshores es té la següent conseqüència de l'anomenat Teorema de Grunwald-Wang:

($*$) Sigui G un grup abelià finit sense elements d'ordre 8. Per a cada primer p d'un conjunt finit qualsevol S, suposem donada una extensió de Galois $K_p/\mathbb{Q}_p$ amb grup de Galois $\mathrm{Gal}(K_p/\mathbb{Q}_p) \subseteq G$. Aleshores, existeix alguna extensió de Galois $K/\mathbb{Q}$ amb grup de Galois $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ i tal que, per a cada $p \in S$, l'extensió $K_p/\mathbb{Q}_p$ s'obté per compleció de $K/\mathbb{Q}$ en p.

La mateix conclusió és vàlida per a un grup abelià finit qualsevol G quan el primer $p = 2$ no pertany a S. Si admetem $2 \in S$ (i G té algun element d'ordre

8), el resultat sempre falla tal com demostra el següent fet observat per Wang [Wan48]: no existeix cap extensió de $\mathbb{Q}$ amb grup de Galois cíclic d'ordre 8 que, localment en $p = 2$, sigui precisament l'única extensió no ramificada de $\mathbb{Q}_2$ amb grup de Galois cíclic d'ordre 8. En qualsevol cas, altres comportaments locals en $p = 2$ sí són admissibles. Per exemple, tot grup abelià finit es realitza com a grup de Galois d'una extensió de $\mathbb{Q}$ en la qual tots els primers d'un conjunt finit prefixat S qualsevol descomponen completament.

El resultat $(*)$ és, a la seva vegada, un cas particular d'un resultat de Saltman [Sal82] que estableix la mateixa conclusió per a tot grup finit G que admet una extensió genèrica sobre $\mathbb{Q}$. Per als grups que satisfan aquesta hipòtesi es té, doncs, una resposta afirmativa al problema 2.1 (i, per tant, també als problemes 2 i 3) per a qualsevol conjunt finit S. Això s'aplica, en particular, sempre que es té una resposta afirmativa al problema de Noether per a G (cf. [Kuy64, Thm. 1]) com, per exemple, quan $G = S_n$ és un grup simètric.

En un resultat famós, Shafarevich estableix una resposta afirmativa al problema invers de la teoria de Galois per a tot grup resoluble finit (cf. [Sha54] i [Sha89]). El Teorema de Shafarevich s'obté com a conseqüència del fet que tot problema d'immersió galoisiana sobre $\mathbb{Q}$, finit, split i amb nucli nilpotent admet alguna solució pròpia. A [NSW00] es demostra una versió més forta d'aquest resultat que, en particular, permet conservar el caràcter moderat de la ramificació en la resolució d'aquests problemes d'immersió. Així es pot obtenir una resposta afirmativa al problema 3 per a tot grup resoluble finit. De fet, els arguments de [NSW00] també permeten conservar la no ramificació dels primers d'un conjunt finit fixat S qualsevol i, d'aquesta manera, donar una resposta afirmativa al problema 2, per a tot grup resoluble finit i tot conjunt finit S (cf. [KM02, Thm. 6.2]). Quan l'ordre de G és senar, això és un cas particular d'un resultat de tipus Grunwald-Wang establert per Neukirch [Neu79, Cor. 2] que permet respondre afirmativament també al problema 2.1.

Un dels casos particulars més estudiats del problema 2 correspon a plantejar-se l'existència d'extensions totalment reals de $\mathbb{Q}$ amb grup de Galois prefixat. El primer de l'infinit $p = \infty$ es caracteritza per ser l'únic primer de $\mathbb{Q}$ amb subgrups de descomposició (i d'inèrcia) en $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ finits que, de fet, són d'ordre 2. Utilitzant aquesta propietat característica, Serre [Ser92a] obté que, si tot grup finit es realitza com a grup de Galois sobre $\mathbb{Q}$, aleshores tot grup finit es realitza com a grup de Galois d'alguna extensió totalment real de $\mathbb{Q}$. És a dir, una resposta afirmativa al problema invers de la teoria de Galois per a tot grup finit equival a una resposta afirmativa al problema 2 per a $S = \{\infty\}$ i per a tot grup finit G.

Contingut de la memòria

En aquesta memòria estudiem els problemes plantejats més amunt per a certs grups finits, per als quals es coneix una resposta afirmativa al problema invers de la teoria de Galois.

A l'hora d'abordar els problemes 1, 2 i 3, els tipus de grups que considerem en cada cas són essencialment diferents. En cert sentit, els prototipus són els grups abelians, per al primer, i els grups simètrics, per al segon i tercer.

Ens plantejem el problema 1 per a algunes famílies de grups resolubles finits que, com ja hem comentat, sempre admeten resposta afirmativa als problemes 2 i 3. En algun punt dels nostres arguments, recorrem a resultats explícits de la teoria de cossos de classes.

Per als problemes 2 i 3, en canvi, considerem famílies de grups finits no resolubles. L'eina bàsica desenvolupada per tractar aquests problemes és l'especialització d'extensions de $\mathbb{Q}(T)$. Més concretament, consisteix en la recerca d'especialitzacions racionals que donin lloc a extensions de $\mathbb{Q}$ amb les condicions de ramificació i el grup de Galois desitjats. Quan, a més, aquestes extensions de $\mathbb{Q}(T)$ són regulars, obtenim una resposta afirmativa als problemes 2 i (o) 3 per a infinites realitzacions galoisianes linealment disjuntes sobre $\mathbb{Q}$

d'un mateix grup finit G.

A continuació resumim els resultats principals d'aquesta memòria, que es compon de sis capítols diferents. Fem notar que cadascun d'ells conté la seva pròpia introducció amb una descripció més detallada del seu contingut, amb l'excepció del Capítol 1, de caràcter preliminar.

En el Capítol 1 recordem alguns fets, essencialment coneguts, relatius als temes següents: problemes d'immersió galoisiana, cossos de classes d'anell de cossos quadràtics, especialització d'extensions de $\mathbb{Q}(T)$ i polígons de Newton. L'objectiu principal és fixar notacions i enunciar resultats per a futura referència, en la forma específica en la qual s'usaran en la resta de la memòria.

El Capítol 2 és l'únic dedicat al problema 1. Considerem aquesta qüestió per a grups nilpotents finits d'ordre senar i per a grups diedrals generalitzats.

El Teorema de Scholz-Reichardt estableix una resposta afirmativa al problema invers de la teoria de Galois sobre $\mathbb{Q}$ per a tot l-grup finit G, quan l és un primer senar qualsevol. La demostració de [Ser92b, Chap. 2] d'aquest resultat fa evident que, si G té ordre l^N, aleshores G es realitza com a grup de Galois d'una extensió de $\mathbb{Q}$ ramificada en, com a màxim, N primers. Demostrem que és suficient admetre r primers ramificats, on r és una constant explícita menor o igual que la suma dels nombres de generadors dels factors de la sèrie central inferior de G. A més, obtenim la corresponent generalització d'aquest resultat per a grups nilpotents finits d'ordre senar.

Per a un grup diedral generalitzat G qualsevol, la teoria de cossos de classes d'anell de cossos quadràtics ens permet demostrar que G es realitza com a grup de Galois d'una extensió de $\mathbb{Q}$ ramificada en $d(G)$ primers finits, on $d(G)$ és el nombre mínim de generadors de G. Caracteritzem, a més, quins d'aquests grups admeten alguna realització galoisiana sobre $\mathbb{Q}$ amb un únic primer ramificat, tant en el cas moderat com en el salvatge.

Assumint la validesa de la Hipòtesi (H) de Schinzel obtenim, per a un grup diedral D_{2n} qualsevol, el nombre mínim de primers ramificats en una extensió de Galois de $\mathbb{Q}$ amb grup de Galois D_{2n}.

En la darrera secció del Capítol 2 considerem el problema d'afitar el nombre de generadors d'un grup finit G en termes dels primers ramificats en una realització qualsevol de G com a grup de Galois d'una extensió moderadament ramificada de $\mathbb{Q}$. Per a certs grups finits, demostrem la validesa d'una fita conjecturada per Harbater [Har94].

En el Capítol 3 caracteritzem, per a un natural n, l'existència de realitzacions galoisianes del grup alternat A_n sobre $\mathbb{Q}$ obtingudes com a cossos de descomposició de trinomis i amb certs comportaments prefixats en els primers d'un conjunt finit S. Això comporta un estudi de la ramificació en extensions trinomials de $\mathbb{Q}$. Més concretament, obtenim les caracteritzacions corresponents a demanar, respectivament, que els primers de S no divideixin el discriminant del trinomi, que els primers de S no divideixin el discriminant de l'extensió i que els primers de S siguin moderadament ramificats. En particular, veiem que, per a tot natural $n \equiv 4 \pmod 8$, el cos de descomposició sobre $\mathbb{Q}$ de qualsevol trinomi de grau n amb grup de Galois A_n defineix sempre una extensió salvatgement ramificada de $\mathbb{Q}$.

Restringir-se a les realitzacions trinomials de A_n sobre $\mathbb{Q}$ correspon a admetre només extensions obtingudes per especialització de certes realitzacions trinomials de A_n sobre $\mathbb{Q}(T)$. En aquest sentit, es pot pensar que el que fem en aquest capítol és estudiar l'existència d'especialitzacions racionals amb un comportament de ramificació prefixat en els primers d'un conjunt finit. En particular, obtenim exemples de realitzacions regulars de A_n ($n \equiv 4 \pmod 8$) sobre $\mathbb{Q}(T)$ que no admeten cap especialització racional moderadament ramificada.

En el Capítol 4 demostrem que, per a tot natural n i tot conjunt finit de primers S, existeixen polinomis mònics de grau n en $\mathbb{Z}[X]$, totalment reals, amb grup de Galois A_n i discriminant no divisible per cap primer de S. D'aquesta manera, obtenim una resposta afirmativa als problemes 2, 3 i 2.2, per a tot grup alternat i tot conjunt finit S. Per fer-ho, considerem especialitzacions de realitzacions regulars de A_n sobre $\mathbb{Q}(T)$ que obtenim mitjançant una construcció coneguda de Mestre [Mes90]. El mateix tipus d'arguments ens permet provar, també, que tot grup alternat es realitza com a grup de Galois d'alguna extensió de $\mathbb{Q}$ en la qual tots els primers d'un conjunt finit prefixat qualsevol descomponen completament (problema 2.1).

Els resultats principals d'aquest capítol apareixeran publicats a *Journal of Algebra* en el treball, conjunt amb N. Vila, "Tame A_n-extensions of $\mathbb{Q}$".

El Capítol 5 consta de dues parts ben diferenciades. En la primera, l'objectiu és obtenir resultats condicionals per als problemes 2 i 3. Com ja hem comentat, si un grup finit G admet una extensió genèrica sobre $\mathbb{Q}$, aleshores es té una resposta afirmativa al problema 2.1 per a G i per a qualsevol conjunt finit S. Veiem com es pot relaxar aquesta hipòtesi (que, en general, no es satisfà), conservant la validesa de la conclusió anterior.

A la segona part del capítol estudiem l'existència d'especialitzacions moderadament ramificades d'algunes realitzacions galoisianes regulars conegudes sobre $\mathbb{Q}(T)$. Els exemples triats provenen de construccions obtingudes per l'anomenat mètode de la rigidesa. Birch suggereix que, per especialització d'aquest tipus de realitzacions sobre $\mathbb{Q}(T)$, en general s'obtenen extensions salvatgement ramificades de $\mathbb{Q}$. Nosaltres provem que els grups de Mathieu M_{11} i M_{12} i el grup $\mathrm{Aut}(M_{22})$ es realitzen com a grups de Galois d'extensions moderadament ramificades de $\mathbb{Q}$, obtingudes per especialització d'extensions "rígides"de $\mathbb{Q}(T)$. En contraposició, provem que l'extensió de $\mathbb{Q}(T)$ amb grup de Galois M_{22}, deduïda de la realització "rígida"de $\mathrm{Aut}(M_{22})$, no admet cap especialització moderadament ramificada. Aquest fet té un cert paral.lelisme

amb alguns resultats del Capítol 3, quan interpretem les realitzacions trinomials sobre $\mathbb{Q}$ del grup alternat A_n com a especialitzacions de realitzacions regulars de A_n sobre $\mathbb{Q}(T)$ deduïdes de realitzacions "rígides" del grup simètric S_n. Com a conclusió, observem que, en els exemples tractats, les dificultats per respondre afirmativament al problema 3 no semblen provenir del caràcter rígid de les realitzacions.

En el Capítol 6 estudiem l'existència de solucions de problemes d'immersió galoisiana centrals finits sobre $\mathbb{Q}(T)$ amb certs comportaments prefixats per especialització. Primer considerem la possibilitat de tenir alguna especialització amb un cert comportament local i, després, prefixem un comportament global, és a dir, una solució del problema sobre $\mathbb{Q}$.

Demostrem que sempre es pot conservar l'existència d'especialitzacions moderadament ramificades en resoldre (pròpiament) problemes d'immersió centrals finits sobre $\mathbb{Q}(T)$. Apliquem aquest resultat a realitzacions galoisianes conegudes sobre $\mathbb{Q}(T)$ i, utilitzant resultats obtinguts en capítols anteriors, demostrem que el problema 3 admet una resposta afirmativa per a tot grup extensió central finita d'algun dels grups següents: grups alternats, grups simètrics i els grups de Mathieu M_{11} i M_{12}.

Acabem el capítol contribuint al problema de l'aixecament aritmètic que consisteix, bàsicament, en provar que tota realització d'un grup finit com a grup de Galois sobre $\mathbb{Q}$ es pot obtenir per especialització d'una realització del mateix grup com a grup de Galois d'una extensió regular de $\mathbb{Q}(T)$. Concretament, demostrem que, si K és un cos de característica 0 i G és un grup extensió central finita de A_n ($n \neq 4, 6, 7$), aleshores tota extensió de K amb grup de Galois G s'obté per especialització d'alguna realització galoisiana regular de G sobre $K(T)$. És a dir, G satisfà la propietat d'aixecament aritmètic sobre K. Obtenim, també, una generalització d'aquest resultat que ens permet resoldre positivament el problema 2.1 per a G i per a qualsevol conjunt finit S.

Els resultats del Capítol 6 apareixeran publicats a *International Mathematics Research Notices* (2003) en el treball "Central embedding problems, the arithmetic lifting property and tame extensions of $\mathbb{Q}$".

Agraïments

No vull acabar aquesta introducció sense expressar el meu agraïment a la Dra. Núria Vila i Oliva per la seva guia i estímul constants durant tot aquest temps. La seva dedicació al projecte ha estat determinant en la realització d'aquest treball.

Agraeixo també a tots els membres del Seminari de Teoria de Nombres de Barcelona els moments compartits en aquests darrers anys i, en particular, als habituals del Seminari Bars: Francesc, Jaume, Carlos, Daniel, Luis, Xavi, Enric, Enrique, Julio, Víctor, Jordi, ...

Finalment, també voldria donar les gràcies als companys del Departament de Matemàtica Aplicada I de la Universitat Politècnica de Catalunya.

Capítol 1

Preliminars

En aquest capítol recordem breument algunes notacions, conceptes i resultats coneguts. Es tracta d'incidir especialment en aquells resultats que usarem més endavant.

1.1 Problemes d'immersió galoisiana

Sigui K un cos. Sempre suposarem fixada una clausura separable $\overline{K}$ de K i denotarem per G_K el **grup de Galois absolut de** K, és a dir,

$$G_K = \mathrm{Gal}(\overline{K}/K).$$

Definició 1.1.1. *Fixat un cos base K, les dades d'un* ***problema d'immersió galoisiana*** *(π, φ) sobre K són:*

(i) una successió exacta de grups finits $1 \to C \to \widetilde{G} \xrightarrow{\pi} G \to 1$,

(ii) un epimorfisme $\varphi : G_K \to G$.

Una ***solució*** *del problema d'immersió galoisiana (π, φ) és un morfisme*

$$\widetilde{\varphi} : G_K \to \widetilde{G}$$

tal que $\pi \circ \widetilde{\varphi} = \varphi$. *Quan* $\widetilde{\varphi}$ *és un epimorfisme, direm que es tracta d'una solució* ***pròpia***.

En la definició anterior, en principi, no cal suposar la finitud dels grups de la successió exacta (i); de fet, la definició donada correspon als problemes d'immersió anomenats **finits**. A nosaltres, però, només ens interessa aquesta situació i, sovint, usarem indistintament els termes "problema d'immersió" i "problema d'immersió finit".

Les dades del problema d'immersió (π, φ) es sintetitzen en el diagrama següent:

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1. \end{array}$$

Observem que una solució pròpia $\widetilde{\varphi}$ del problema (π, φ) determina una realització de $\widetilde{G}$ com a grup de Galois sobre K. De fet, si L i $\widetilde{L}$ són, respectivament, el cos fix pel nucli de φ i $\widetilde{\varphi}$, aleshores es tenen inclusions $K \subseteq L \subseteq \widetilde{L}$ i isomorfismes

$$\mathrm{Gal}(L/K) \cong G\ , \quad \mathrm{Gal}(\widetilde{L}/K) \cong \widetilde{G},$$

de manera que π correspon precisament a l'epimorfisme de restricció

$$\mathrm{Gal}(\widetilde{L}/K) \to \mathrm{Gal}(L/K).$$

Quan la solució $\widetilde{\varphi}$ no és pròpia, aleshores només es té una inclusió

$$\mathrm{Gal}(\widetilde{L}/K) \cong \widetilde{\varphi}(G_K) \subseteq \widetilde{G}.$$

En qualsevol cas, tota solució $\widetilde{\varphi}$ del problema d'immersió (π, φ) correspon a una àlgebra de Galois sobre K amb grup $\widetilde{G}$. Es tracta d'un cos exactament quan la solució és pròpia.

Ocasionalment, també considerarem problemes d'immersió per a certs quocients de G_K i demanarem que les solucions factoritzin a través seu. És a dir,

donada una extensió de Galois M/K, ens plantejarem el problema corresponent a un diagrama del tipus

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(M/K) & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1. \end{array}$$

Obsevem que, amb les notacions anteriors, ara tindrem $L \subseteq M$ i les solucions d'aquest problema correspondran a subcossos $\widetilde{L} \subseteq M$.

Definició 1.1.2. *Direm que un problema d'immersió (π, φ) és* ***split*** *si la successió exacta $1 \to C \to \widetilde{G} \stackrel{\pi}{\to} G \to 1$ és escindida, és a dir, si π admet una secció. Direm que el problema (π, φ) és* ***central*** *(resp.* ***Frattini****) si el nucli C de l'epimorfisme π està contingut en el centre (resp. el subgrup de Frattini) de $\widetilde{G}$.*

Recordem que el subgrup de Frattini d'un grup G es defineix com la intersecció de tots els subgrups maximals de G.

El següent resultat és conseqüència directa de les definicions i es troba, per exemple, a [ILF97, Chap.1] o [MM99, Chap.IV].

Proposició 1.1.3.

(i) Tot problema d'immersió split admet solució.

(ii) Tota solució (si n'hi ha) d'un problema d'immersió Frattini és pròpia.

1.1.1 Problemes d'immersió amb nucli abelià finit

A partir d'ara, suposarem que el nucli C del problema d'immersió (π, φ) és abelià i finit. Que el problema (π, φ) tingui solució equival a que l'aixecament de π per φ (pull-back)

$$1 \to C \to \widetilde{G_K} \stackrel{\pi^*}{\to} G_K \to 1$$

admeti una secció.

Dit d'una altra manera, si $\varepsilon \in H^2(G, C)$ denota la classe de cohomologia corresponent a l'extensió de grups

$$1 \to C \to \widetilde{G} \xrightarrow{\pi} G \to 1$$

i $\varphi^* : H^2(G, C) \to H^2(G_K, C)$ és el morfisme d'inflació induït per φ, aleshores:

(π, φ) admet solució si i només si $\varphi^*(\varepsilon) = 0$.

Definició 1.1.4. *Amb les notacions anteriors, direm que $\varphi^*(\varepsilon)$ és l'**obstrucció** del problema d'immersió (π, φ).*

Si $\widetilde{\varphi} : G_K \longrightarrow \widetilde{G}$ és una solució qualsevol d'un problema d'immersió (π, φ) amb nucli abelià finit C i $x : G_K \to C$ és un 1-cocicle, aleshores l'aplicació ${}^x\widetilde{\varphi} : G_K \longrightarrow \widetilde{G}$ definida per ${}^x\widetilde{\varphi}(g) = x(g).\widetilde{\varphi}(g)$ també és (morfisme) solució del mateix problema. Això defineix una acció simplement transitiva de $H^1(G_K, C)$ en el conjunt de classes d'equivalència de solucions de (π, φ), convenint que dues solucions $\widetilde{\varphi}$ i $\widetilde{\varphi}'$ són **equivalents** si existeix algun $c \in C$ tal que $\widetilde{\varphi}'(\sigma) = c^{-1}\widetilde{\varphi}(\sigma)c$, per a tot $\sigma \in G_K$ (cf., per exemple, [NSW00, Prop. 9.4.4]).

En particular, si C està contingut en el centre de $\widetilde{G}$, aleshores $H^1(G_K, C) = \mathrm{Hom}(G_K, C)$ i es té:

Proposició 1.1.5. *Sigui $\widetilde{\varphi}$ una solució qualsevol d'un problema d'immersió central finit (π, φ). Aleshores el conjunt de totes les solucions de (π, φ) és $\{\chi.\widetilde{\varphi}\}_\chi$, on χ recorre els elements de* $\mathrm{Hom}(G_K, C)$.

1.1.2 Problemes d'immersió centrals sobre $\mathbb{Q}$ i sobre $\mathbb{Q}_p$

Per a cada primer racional p, suposarem fixat un primer $\overline{p}$ de (la clausura entera de $\mathbb{Z}$ en) $\overline{\mathbb{Q}}$ sobre p i denotarem per D_p (resp. I_p) el corresponent subgrup de descomposició (resp. inèrcia) en $G_{\mathbb{Q}}$.

Si $\varphi : G_{\mathbb{Q}} \longrightarrow G$ és un morfisme qualsevol, $\varphi_p : G_{\mathbb{Q}_p} \longrightarrow G$ denotarà la restricció de φ a D_p, identificat amb el grup de Galois absolut del cos dels nombres p-àdics, $G_{\mathbb{Q}_p}$.

Qualsevol problema d'immersió global (π, φ) (sobre $\mathbb{Q}$)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

dóna lloc a problemes d'immersió locals (sobre $\mathbb{Q}_p$)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C & \to & \pi^{-1}(\varphi_p(G_{\mathbb{Q}_p})) & \stackrel{\pi}{\to} & \varphi_p(G_{\mathbb{Q}_p}) & \to & 1, \end{array}$$

que denotarem per (π, φ_p). Per comoditat, sovint descriurem el problema (π, φ_p) pel diagrama

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1, \end{array}$$

encara que φ_p no sigui un epimorfisme en G.

En la resta d'aquesta secció, només considerarem problemes d'immersió centrals finits sobre $\mathbb{Q}$.

La Proposició 1.1.5 ens diu que, donada una solució $\widetilde{\varphi}$ d'un problema d'immersió central finit (π, φ) amb nucli C, la possibilitat d'obtenir alguna solució $\widetilde{\varphi}'$ "prou bona" depèn de (φ i de) l'existència d'algun morfisme $\chi \in \mathrm{Hom}(G_{\mathbb{Q}}, C)$ "prou bo".

Quan C és abelià, donats morfismes (locals) $\{\gamma_p \in \mathrm{Hom}(G_{\mathbb{Q}_p}, C)\}_{p \in S}$ per als primers d'un conjunt finit S qualsevol, sempre existeix algun morfisme (global) $\chi \in \mathrm{Hom}(G_{\mathbb{Q}}, C)$ no ramificat fora de S i tal que $\chi_{p|I_p} = \gamma_{p|I_p}$, per a tot $p \in S$ (cf. [Ser92b, Lemma 2.1.6]). Això permet concloure:

Proposició 1.1.6. *[Ser92b, Prop. 2.1.7]*
Considerem un problema d'immersió central finit (π, φ)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

que admet alguna solució. Per a cada primer p *d'un conjunt finit qualsevol* S*, suposem donada una solució* $\widetilde{\phi}_p : G_{\mathbb{Q}_p} \longrightarrow \widetilde{G}$ *del problema local* (π, φ_p)*. Aleshores existeix alguna solució* $\widetilde{\varphi} : G_{\mathbb{Q}} \longrightarrow \widetilde{G}$ *del problema global* (π, φ) *tal que:*

(i) per a tot $p \in S$*,* $\widetilde{\varphi}_{|I_p} = \widetilde{\phi}_{p|I_p}$*,*

(ii) per a tot $p \notin S$*,* $\widetilde{\varphi}_p$ *és no ramificat si* φ_p *ho és.*

Observació 1.1.7. *Sovint, si eliminem la condició (ii) en la conclusió de la Proposició 1.1.6, el resultat també és cert demanant coincidència en tot el grup de descomposició* D_p *en (i). Concretament, del Teorema de Grunwald-Wang (cf., per exemple, [NSW00, Chap.IX, §2.]) es dedueix que això és així sempre que* C *no conté elements d'ordre* 8*. És a dir, en aquest cas, la resolubilitat del problema global garanteix l'existència d'una solució que, localment, coincideix amb solucions arbitràries dels problemes locals en un nombre finit de primers qualssevol. A més, això sempre es pot aconseguir amb una solució pròpia del problema global (veure demostració de la Proposició 1.1.8).*

Com a conseqüència de la Proposició anterior s'obté el següent resultat.

Proposició 1.1.8. *Considerem un problema d'immersió central finit* (π, φ)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

que admet alguna solució. Aleshores:

(i) Existeix alguna solució $\widetilde{\varphi}$ del problema (π, φ) ramificada exactament en els mateixos primers que φ.

(ii) Si φ és no ramificat en els primers d'un conjunt finit qualsevol S, aleshores existeix alguna solució pròpia de (π, φ) no ramificada en S.

Demostració. (i) Veure [Ser92b, Cor. 2.1.8]. Només cal usar la Proposició 1.1.6, tenint en compte que, si l'epimorfisme φ és no ramificat en un primer p, aleshores el problema local (π, φ_p) sempre admet una solució no ramificada. De fet, $\varphi_p : G_{\mathbb{Q}_p} \to G$ factoritza pel grup procíclic $\mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}}$, on $\mathbb{Q}_p^{nr}/\mathbb{Q}_p$ denota la màxima subextensió no ramificada de $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$. El problema d'immersió

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

clarament admet solució: només cal aixecar el generador del grup cíclic $\varphi_p(G_{\mathbb{Q}_p})$.

(ii) Tal com veurem, la Proposició 1.1.6 també ens permet garantir que la solució obtinguda sigui pròpia; en general, però, caldrà acceptar nous primers ramificats.

Si $\{c_1, \ldots, c_m\}$ és un conjunt de generadors de C, triem $\{p_1, \ldots, p_m\}$ primers fora de S que no divideixen l'ordre de C i que descomponen completament a $K/\mathbb{Q}$ (l'extensió definida per φ).

Per a cadascun dels primers p_i, existeix una extensió $K_i/\mathbb{Q}_{p_i}$ totalment ramificada de grau l'ordre de c_i (cíclica, per ser moderada) i podem considerar "el" corresponent morfisme

$$\widetilde{\phi_{p_i}} : G_{\mathbb{Q}_{p_i}} \longrightarrow \mathrm{Gal}(K_i/\mathbb{Q}_{p_i}) \cong < c_i > \subset C \subset \widetilde{G}.$$

Per hipòtesi, $\varphi(G_{\mathbb{Q}_{p_i}}) = \{1\}$ i, per tant, $\widetilde{\phi_{p_i}}$ és una solució del problema local (π, φ_{p_i}).

La Proposició 1.1.6 garanteix l'existència d'una solució $\widetilde{\varphi}$ del problema global (π, φ) tal que $\widetilde{\varphi}_{|I_p} = \widetilde{\phi}_{p|I_p}$, per a tot $p \in \{p_1, \ldots, p_m\}$. La imatge de $\widetilde{\varphi}$ contindrà C i, per tant, es tractarà d'una solució pròpia.

Com que, per hipòtesi, S no conté cap dels primers p_i, el resultat enunciat s'obté de la Proposició 1.1.6 raonant com a l'apartat (i). □

1.1.3 Grups perfectes: extensió central universal

Els següents conceptes i resultats bàsics de la teoria d'extensions centrals es troben, per exemple, a [Suz82, Chap. II, §9.]. Tots els grups i extensions que apareguin són *finits*, encara que no insistim en aquesta hipòtesi cada vegada. $D(G)$ denotarà el subgrup derivat d'un grup G.

(i) Si $1 \to C \to \widetilde{G} \to G \to 1$ és una extensió central i $\widetilde{G_1}$ és un subgrup de $\widetilde{G}$ tal que $\widetilde{G} = C.\widetilde{G_1}$, aleshores $1 \to C \cap \widetilde{G_1} \to \widetilde{G_1} \to G \to 1$ és una extensió central i $\widetilde{G}$ és (isomorf a) un quocient de $C \times \widetilde{G_1}$.

Es diu que l'extensió és **irreductible** si no existeix cap subgrup propi $\widetilde{G_1} \subset \widetilde{G}$ amb la propietat $\widetilde{G} = C.\widetilde{G_1}$.

Així, tot grup extensió central de G és quocient del producte directe d'un grup abelià i un grup extensió central irreductible de G.

(ii) S'anomena **grup dels multiplicadors de Schur de** G a $M(G) := H^2(G, \mathbb{C}^*)$ (G actuant trivialment en $\mathbb{C}^*$).

Es tracta d'un grup finit amb la propietat que, per a tota extensió central $1 \to C \to \widetilde{G} \to G \to 1$, el grup $D(\widetilde{G}) \cap C$ és (isomorf a) un subgrup de $M(G)$.

Es diu que l'extensió és **primitiva** si és irreductible i es té un isomorfisme $D(\widetilde{G}) \cap C \cong M(G)$.

Tota extensió central irreductible de G és quocient d'alguna extensió central primitiva de G.

(iii) Es diu que una extensió central $1 \to C \to \widetilde{G} \to G \to 1$ és un **grup de representació de** G si és primitiva i el seu nucli està contingut en el subgrup derivat $D(\widetilde{G})$, és a dir, si és primitiva i es té un isomorfisme $C \cong M(G)$. Tot grup finit té algun grup de representació.

Direm que G és un grup **perfecte** si es té $D(G) = G$. En aquest cas, G admet una única (classe d'isomorfisme d') extensió central primitiva

$$1 \to M \to U \to G \to 1,$$

que s'anomena **extensió central universal de** G. Es tracta d'un (únic) grup de representació de G (per tant, amb nucli $M \cong M(G)$) tal que, per a qualsevol extensió central $1 \to C \to \widetilde{G} \to G \to 1$, existeix un únic morfisme $U \to \widetilde{G}$ fent commutatiu el diagrama

$$\begin{array}{ccccccccc} 1 & \to & M & \to & U & \to & G & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow id & & \\ 1 & \to & C & \to & \widetilde{G} & \to & G & \to & 1 \end{array}$$

De fet, l'existència d'una extensió central de G amb aquesta propietat universal equival a que G sigui perfecte.

Des del punt de vista dels problemes d'immersió galoisiana, les propietats anteriors (i el fet que els problemes split sempre admeten solució) impliquen, per a un epimorfisme $\varphi : G_K \longrightarrow G$ (K un cos qualsevol):

- la resolubilitat de tots els problemes d'immersió centrals finits primitius per a φ garanteix la resolubilitat de tots els problemes d'immersió centrals finits per a φ,
- si G és perfecte, la resolubilitat del problema universal per a φ garanteix la resolubilitat de tots els problemes d'immersió centrals finits per a φ.

1.2 Cossos de classes d'anell

En aquesta secció recordem alguns resultats de la teoria dels anomenats cossos de classes d'anell ("ring class fields") que usarem a la Secció 2.3 i que, essencialment, es troben a [Coh78] (veure també [Cox89]).

1.2.1 Grups diedrals generalitzats

Les extensions diedrals generalitzades de $\mathbb{Q}$ corresponen exactament als cossos de classes d'anell de cossos quadràtics. Comencem recordant la definició de grup diedral generalitzat i remarcant algunes propietats bàsiques.

Definició 1.2.1. *Donat un grup abelià finit A, definim el* ***grup diedral generalitzat*** $D_{2.A}$ *per una extensió de grups*

$$1 \to A \to D_{2.A} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 1$$

tal que existeix $\tau \in D_{2.A}$ satisfent:

(i) $\pi(\tau)$ *és el generador de* $\mathbb{Z}/2\mathbb{Z}$,

(ii) $\tau^2 = 1$,

(iii) $\tau\sigma\tau = \sigma^{-1}$, *per a tot* $\sigma \in A$.

Equivalentment, $D_{2.A}$ és isomorf al producte semidirecte $A \rtimes_\theta \mathbb{Z}/2\mathbb{Z}$ respecte l'acció $\theta : \mathbb{Z}/2\mathbb{Z} \to Aut(A)$ definida per $\theta(\overline{1}) = \{\sigma \mapsto \sigma^{-1}\}$.

Denotarem per $d(G)$ el nombre mínim de generadors d'un grup G.

Lema 1.2.2.

(i) Si A és un grup cíclic de n elements, aleshores $D_{2.A}$ és isomorf al grup diedral de $2n$ elements $D_{2.n}$.

(ii) *El subgrup derivat de* $D_{2.A}$ *és* $D'_{2.A} = A^2$.

L'abelianitzat de $D_{2.A}$ *és* $D^{ab}_{2.A} \cong D_{2.A}/D'_{2.A} \cong \mathbb{Z}/2\mathbb{Z} \times \overset{r+1}{\cdots} \times \mathbb{Z}/2\mathbb{Z}$, *on* $r = r_2(A)$ *és el 2-rang de* A.

(iii) $d(D_{2.A}) = d(A) + 1$.

(iv) *Tot subgrup* H *de* A *és normal en* $D_{2.A}$ *i es té* $D_{2.A}/H \cong D_{2.A/H}$.

1.2.2 Extensions diedrals generalitzades de $\mathbb{Q}$

El nostre següent objectiu és definir el concepte de cos de classes d'anell d'un cos quadràtic K. Recordem, primer, algunes notacions i fets generals de la teoria de cossos de classes.

Denotem per $\mathcal{O}_K$ l'anell d'enters d'un cos de nombres K. Donat un ideal $\mathfrak{m}_0 \subseteq \mathcal{O}_K$ i un producte formal $\mathfrak{m}_\infty$ de primers infinits reals de K, diferents dos a dos, podem considerar el **cicle** (o **divisor** o **mòdul de raig**) $\mathfrak{m} = \mathfrak{m}_0.\mathfrak{m}_\infty$ de K. Associats a un cicle $\mathfrak{m}$, tenim els grups:

$I^{\mathfrak{m}}$: grup d'ideals fraccionaris de K coprimers amb $\mathfrak{m}_0$,

$P^{\mathfrak{m}}$: **raig mòdul** $\mathfrak{m}$; és el subgrup de $I^{\mathfrak{m}}$ format pels ideals fraccionaris principals que es poden generar per algun $\alpha \in K$ tal que $\alpha \equiv 1 \pmod{{}^*\mathfrak{m}}$, és a dir, $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ i $\sigma(\alpha) > 0$ per a tot σ dividint $\mathfrak{m}_\infty$.

Anomenem **grup de classes de raig mòdul** $\mathfrak{m}$ al grup quocient $I^{\mathfrak{m}}/P^{\mathfrak{m}}$. Denotarem per $K^{\mathfrak{m}}$ el **cos de classes de raig mòdul** $\mathfrak{m}$. Recordem que $K^{\mathfrak{m}}/K$ és una extensió abeliana, no ramificada fora de $\mathfrak{m}$ i amb grup de Galois

$$\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong I^{\mathfrak{m}}/P^{\mathfrak{m}}.$$

Per a qualsevol extensió abeliana finita L/K existeix algun cicle $\mathfrak{m}$ de K tal que $L \subseteq K^{\mathfrak{m}}$. En aquest cas, direm que $\mathfrak{m}$ és un **cicle de declaració** per a

l'extensió L/K. El **conductor** de L/K es defineix com el màxim comú divisor de tots els cicles de declaració per a L/K.

A qualsevol subgrup $H \subseteq I^{\mathfrak{m}}$ que conté $P^{\mathfrak{m}}$ li correspon una única subextensió L/K de $K^{\mathfrak{m}}/K$ amb grup de Galois

$$\mathrm{Gal}(L/K) \cong I^{\mathfrak{m}}/H.$$

En aquest cas, notarem $K(H) = L$ i direm que $K(H)$ és el **cos de classes de** H.

Siguin $\mathfrak{m}_1$ i $\mathfrak{m}_2$ dos cicles de K i suposem donats subgrups $H_1 \subseteq I^{\mathfrak{m}_1}$, $H_2 \subseteq I^{\mathfrak{m}_2}$ tals que

$$P^{\mathfrak{m}_i} \subseteq H_i \subseteq I^{\mathfrak{m}_i}\ , \quad \text{per a } i \in \{1,2\}.$$

Recordem que les condicions següents són equivalents:

(a) $K(H_1) \subseteq K(H_2)$,

(b) $H_1 \cap I^{\mathfrak{m}} \supseteq H_2 \cap I^{\mathfrak{m}}$, on $\mathfrak{m}$ és el mínim comú múltiple de $\mathfrak{m}_1$ i $\mathfrak{m}_2$.

En particular, si $\mathfrak{m}_1$ divideix $\mathfrak{m}_2$, aleshores la inclusió de cossos $K(H_1) \subseteq K(H_2)$ equival a la inclusió de grups $H_1 \supseteq H_2$.

En la resta d'aquesta secció, K sempre denotarà un cos extensió quadràtica de $\mathbb{Q}$ de discriminant d_K. Denotarem per ∞_K el producte dels primers infinits reals de K.

Associat a un natural qualsevol f, considerem el cicle $\widetilde{f}$ de K definit per

$$\widetilde{f} := (f)\mathcal{O}_K.\infty_K.$$

Definició 1.2.3. *Sigui $f \geq 2$ un nombre natural i considerem un sistema de representants positius $\{z_1, \ldots, z_{\varphi(f)}\}$ de $(\mathbb{Z}/f\mathbb{Z})^*$. Definim el subgrup $P(\widetilde{f})$ de $I^{\widetilde{f}}$ com:*

$$P(\widetilde{f}) := \{(z_1) \cup \ldots \cup (z_{\varphi(f)})\}.P^{\widetilde{f}}.$$

La inclusió de grups $P^{\widetilde{f}} \subseteq P(\widetilde{f}) \subseteq I^{\widetilde{f}}$ *correspon a una inclusió de cossos* $K \subseteq K(P(\widetilde{f})) \subseteq K^{\widetilde{f}}$. *Al cos* $K(P(\widetilde{f}))$ *se l'anomena* ***cos de classes d'anell de*** K ***per al conductor*** $\widetilde{f}$.

Notem que $K(P(\widetilde{f}))/K$ és una subextensió de $K^{\widetilde{f}}/K$ amb grup de Galois

$$\mathrm{Gal}(K(P(\widetilde{f}))/K) \cong I^{\widetilde{f}}/P(\widetilde{f}).$$

Definició 1.2.4. *Direm que un cos* L *és un* ***cos de classes d'anell de*** K *si existeix algun natural* $f \geq 2$ *tal que* $K \subseteq L \subseteq K(P(\widetilde{f}))$.

És a dir, L/K *és una extensió abeliana finita que admet* $\widetilde{f}$ *com a cicle de declaració i* $L = K(H)$ *per algun subgrup* $H \subseteq I^{\widetilde{f}}$ *tal que* $P(\widetilde{f}) \subseteq H \subseteq I^{\widetilde{f}}$.

Observació 1.2.5. *Generalment, també es consideren les definicions anàlogues a les donades per al cicle* $\widetilde{f} := (f)\mathcal{O}_K$ *(cf. [Coh78]). Per als nostres propòsits no caldrà contemplar aquesta possibilitat: només ens interessarem per la no ramificació dels primers finits.*

En el Lema següent destaquem algunes propietats bàsiques dels cossos de classes d'anell, que s'obtenen com a conseqüència de les pròpies definicions.

Lema 1.2.6. *Amb les notacions anteriors es té:*

(i) Donat $f \geq 2$, *l'extensió* $K(P(\widetilde{f}))/K$ *és no ramificada en els ideals primers de* K *que no divideixen* $(f)\mathcal{O}_K$. *A més,* $K(P(\widetilde{f}))$ *sempre conté* H_+, *el cos de classes de Hilbert (estricte) de* K.

(ii) Si f_1 *divideix* f_2, *aleshores* $K(P(\widetilde{f}_1)) \subseteq K(P(\widetilde{f}_2))$.

(iii) Si L *és un cos de classes d'anell de* K *i el conductor de* L/K *divideix* $\widetilde{f}$, *aleshores* $L \subseteq K(P(\widetilde{f}))$.

El següent resultat es pot interpretar com un anàleg al Teorema de Kronecker-Weber; els grups diedrals generalitzats i els cossos de classes d'anell $K(P(\widetilde{f}))$ substitueixen, respectivament, els grups abelians finits i els cossos ciclotòmics.

Proposició 1.2.7. *[Bru66, Satz 8]*
Per a un cos de nombres L són equivalents:

(a) *$L/\mathbb{Q}$ és una extensió diedral generalitzada, és a dir, $L/\mathbb{Q}$ és una extensió de Galois amb grup de Galois isomorf a un grup diedral generalitzat.*

(b) *L és un cos de classes d'anell d'algun cos quadràtic K.*

Acabem aquesta secció recordant que, donat un cos quadràtic K i un natural $f \geq 2$, existeixen fórmules per al grau de l'extensió $K(P(\widetilde{f}))/K$; aquest grau no és res més que el nombre de classes estricte de l'ordre de conductor f, $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$.

Usarem les següents notacions habituals:

- $h_+(d_K f^2) := (I^{\widetilde{f}} : P(\widetilde{f})) = [K(P(\widetilde{f})) : K]$,
- H_+ denotarà el cos de classes de Hilbert estricte de K, és a dir, el cos de classes de raig mòdul ∞_K,
- $h_+(d_K) := (I^{\infty_K} : P^{\infty_K}) = [H_+ : K]$ (nombre de classes estricte de K),
- per a K real ($d_K > 0$), ϵ_+ denotarà el generador de les unitats totalment positives de $\mathcal{O}_K$ i $E_+ \in \mathbb{Z}_{>0}$ el mínim natural tal que ${\epsilon_+}^{E_+} \in \mathcal{O}_f$,
- per a K imaginari, es defineix $E_+ := 2$ si $d_K = -4$, $E_+ := 3$ si $d_K = -3$ i $E_+ := 1$ si $d_K < -4$.

Proposició 1.2.8. *[Coh78, Cor. 15.40]*
Amb les notacions anteriors es té:

$$h_+(d_K f^2) = h_+(d_K).f.\prod_{p|f}\left(1 - \frac{\left(\frac{d_K}{p}\right)}{p}\right).\frac{1}{E_+}\ .$$

1.3 Especialització d'extensions de $\mathbb{Q}(T)$

1.3.1 El Teorema d'Irreductibilitat de Hilbert

Considerem indeterminades $T_1, \dots, T_d$.

Definició 1.3.1. *Donat un cos K, un* ***subconjunt de Hilbert bàsic de*** K^d *és qualsevol conjunt de la forma*

$$\{t \in K^d \text{ tal que } f(t, X_1, \dots, X_s) \text{ és irreductible a } K[X_1, \dots, X_s]\},$$

per algun polinomi $f(T_1, \dots, T_d, X_1, \dots, X_s) \in K(T_1, \dots, T_d)[X_1, \dots, X_s]$ irreductible.

La intersecció d'un nombre finit de subconjunts de Hilbert bàsics amb un obert Zariski no buit de K^d s'anomena ***subconjunt de Hilbert de*** K^d.

En la definició de subconjunt de Hilbert bàsic cal demanar, evidentment, que el polinomi especialitzat $f(t, X_1, \dots, X_s)$ sigui un polinomi ben definit de $K[X_1, \dots, X_s]$. Convenim que aquesta condició està implícita sempre que calgui.

El Teorema d'Irreductibilitat de Hilbert estableix que tot subconjunt de Hilbert de $\mathbb{Q}^d$ és no buit. Més generalment, es té (cf. [Sch00, 4.4, Thm. 46]):

Proposició 1.3.2. *Per a qualsevol cos de nombres K, tot subconjunt de Hilbert de K^d conté infinits $t \in \mathbb{Z}^d$.*

Donats $t_0 \in \mathbb{Q}^d$ i $M, N \in \mathbb{Z}$, la irreductibilitat en $X_1, \dots, X_s$ d'un polinomi $f(T, X_1, \dots, X_s) \in K(T)[X_1, \dots, X_s]$ equival a la irreductibilitat del polinomi $f(t_0 + \frac{M}{1+NT}, X_1, \dots, X_s)$, on $T = (T_1, \dots, T_d)$. Així, el resultat anterior admet la següent conseqüència, que és el que sovint citarem com a Teorema d'Irreductibilitat de Hilbert.

Proposició 1.3.3. *Sigui K un cos de nombres i suposem fixat un conjunt finit S de primers racionals qualsevol. Sigui H un subconjunt de Hilbert qualsevol de*

K^d. Aleshores $H \cap \mathbb{Q}^d$ és dens a $(\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p)^d$ respecte la topologia producte (via la inclusió diagonal).

En aquesta memòria ens interessarà especialitzar polinomis irreductibles de $K(T)[X]$ de manera que es conservi, no només el caràcter irreductible, sinó també el grup de Galois. És a dir, els subconjunts de K^d (K cos de nombres) que apareixeran són, essencialment, del tipus

$$\{t \in K^d \text{ tal que } \mathrm{Gal}_K(f(t,X)) \cong \mathrm{Gal}_{K(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X))\},$$

per algun polinomi $f(T_1,\dots,T_d,X) \in K(T_1,\dots,T_d)[X]$ irreductible en X. Aquests conjunts sempre contenen algun subconjunt de Hilbert de K^d (cf., per exemple, [JLY02, Thm. 2.3.5]) i, per tant, satisfan el resultat de densitat de la Proposició anterior.

Definició 1.3.4. *Sigui K un cos. Una extensió finita $L_T/K(T_1,\dots,T_d)$ es diu que és K-**regular** quan K és algebraicament tancat en L_T.*

Observem que, si L_T és el cos de descomposició sobre $K(T_1,\dots,T_d)$ d'un polinomi $f(T_1,\dots,T_d,X)$, aleshores l'extensió $L_T/K(T_1,\dots,T_d)$ és K-regular si i només si

$$\mathrm{Gal}_{K(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X)) \cong \mathrm{Gal}_{\overline{K}(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X)).$$

Proposició 1.3.5. *Sigui $f(T_1,\dots,T_d,X) \in \mathbb{Q}(T_1,\dots,T_d)[X]$ un polinomi irreductible en X tal que el seu cos de descomposició sobre $\mathbb{Q}(T_1,\dots,T_d)$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T_1,\dots,T_d)$. Notem*

$$H_f := \{t \in \mathbb{Q}^d \text{ tal que } \mathrm{Gal}_{\mathbb{Q}}(f(t,X)) \cong \mathrm{Gal}_{\mathbb{Q}(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X))\}.$$

Sigui U un entorn qualsevol a $(\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p)^d$ d'un punt arbitrari $t_0 \in (\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p)^d$. Aleshores, existeixen infinits punts $t \in U \cap H_f$ tals que els cossos de descomposició sobre $\mathbb{Q}$ dels corresponents polinomis $f(t,X)$ defineixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos.

En les hipòtesis d'aquest resultat, els cossos de descomposició K_1, K_2 corresponents a dos punts $t_1, t_2 \in H_f$ defineixen extensions de $\mathbb{Q}$ linealment disjuntes exactament quan es tenen isomorfismes

$$\mathrm{Gal}_{K_1}(f(t_2, X)) \cong \mathrm{Gal}_{\mathbb{Q}}(f(t_2, X)) \cong \mathrm{Gal}_{\mathbb{Q}(T)}(f(T, X)) \cong \mathrm{Gal}_{K_1(T)}(f(T, X)),$$

on $T = (T_1, \ldots, T_d)$. Així, el resultat enunciat és conseqüència directa de la Proposició 1.3.3. De fet, la hipòtesi de regularitat equival a la infinitud en la conclusió de la Proposició anterior.

En aquesta memòria, el concepte d'*especialització* apareixerà, bàsicament, aplicat a polinomis; consisteix, simplement, en fer substitució de paràmetres com fins ara. Al Capítol 6 ens caldrà usar, però, especialització d'extensions galoisianes de $K(T)$, on K és un cos de característica 0; habitualment tindrem $K = \mathbb{Q}$.

1.3.2 Especialització d'extensions

En la resta d'aquesta secció, K denotarà sempre un cos de característica 0 i T una (única) indeterminada.

Definició 1.3.6. *Sigui $L_T/K(T)$ una extensió de Galois finita i suposem donat $t_0 \in K$ tal que el primer $(T - t_0)$ de $K(T)$ no ramifica a $L_T/K(T)$. Denotem per L_{t_0} el cos obtingut per composició de tots els cossos residuals dels primers sobre $(T - t_0)$ en $L_T/K(T)$. Direm que l'extensió L_{t_0}/K és l'**especialització de** $L_T/K(T)$ **en** $T = t_0$.*

Notem que, per definició, l'especialització de $L_T/K(T)$ en $T = t_0$ només té sentit quan $(T - t_0)$ no ramifica a $L_T/K(T)$. Aquesta condició estarà implícita sempre que parlem d'especialització.

L'especialització d'una extensió de Galois finita de $K(T)$ sempre es pot interpretar via l'especialització de polinomis (és a dir, avaluant T en t_0), gràcies al següent fet (veure també demostració de [Sal82, Lemma 5.6]).

Proposició 1.3.7. *Sigui K un cos de característica 0 i suposem donat un element $t_0 \in K$. Sigui $L_T/K(T)$ una extensió de Galois finita no ramificada en $(T - t_0)$. Aleshores, L_T és el cos de descomposició sobre $K(T)$ d'algun polinomi irreductible i mònic $f(T, X) \in K[T, X]$ tal que $D(f(t_0, X)) \neq 0$. En aquest cas, el cos L_{t_0} obtingut per especialització en $T = t_0$ és precisament el cos de descomposició sobre K del polinomi (separable) $f(t_0, X) \in K[X]$.*

Demostració. Sigui $\mathcal{O}$ la clausura entera de $K[T]$ en L_T. La hipòtesi de no ramificació sobre $(T - t_0)$ garanteix que es té un isomorfisme

$$\mathcal{O}/(T - t_0)\mathcal{O} \cong L_1 \times \cdots \times L_m,$$

on $L_1, \ldots, L_m$ són els cossos residuals en els primers sobre $(T-t_0)$ a $L_T/K(T)$. A més, la suma dels graus de les extensions finites L_i/K és precisament el grau de $L_T/K(T)$.

Per a cada i, podem considerar un element primitiu $x_i \in L_i$ per a l'extensió L_i/K. Per hipòtesi, K és infinit i, per tant, podem suposar que el producte de polinomis mínims $f_i(X) \in K[X]$ dels x_i té discriminant no nul. Notem $f(X) = \prod_i f_i(X)$.

Si $x \in \mathcal{O}$ és una antimatge de $(x_1, ..., x_m)$ per l'epimorfisme (reducció) $\mathcal{O} \to \prod_i L_i$ i $f(T, X) \in K[T][X]$ és el polinomi mínim de x sobre $K(T)$, aleshores $f(X)$ ha de dividir $f(t_0, X)$. Per comparació de graus, ha de ser $f(X) = f(t_0, X)$ i $L_T = K(T)[x]$. □

Observació 1.3.8. *Potser és més habitual definir l'especialització de $L_T/K(T)$ en $T = t_0$ com l'extensió*

$$K \subset \mathcal{O}/(T - t_0)\mathcal{O} \cong L_1 \times \cdots \times L_m.$$

A nosaltres, però, només ens interessa especialitzar per a obtenir extensions galoisianes de ***cossos****. Això sempre és així amb la definició donada.*

En qualsevol cas, les extensions L_i/K són totes K-isomorfes entre elles i coincideixen amb L_{t_0}/K, un cop fixada una clausura algebraica $\overline{K}$ de K.

Al Capítol 6 estudiarem problemes d'immersió sobre $K(T)$. En aquesta situació, serà convenient parlar també d'especialització de morfismes del grup de Galois absolut $G_{K(T)}$ de $K(T)$.

Definició 1.3.9. *Sigui G un grup finit. Una G-**extensió de** K és un epimorfisme $G_K \to G$.*

Donar una G-extensió de K equival a donar una extensió de Galois L/K i un isomorfisme $\mathrm{Gal}(L/K) \cong G$. Per comoditat, sovint farem l'abús de llenguatge de dir que L/K és una G-extensió de K.

Sigui G un grup finit i $\varphi_T : G_{K(T)} \to G$ una G-extensió de $K(T)$. Volem definir l'especialització de φ_T en un punt (no ramificat) $T = t_0 \in K$.

Denotem per $L_T/K(T)$ l'extensió de Galois corresponent a φ_T. L'especialització L_{t_0}/K de $L_T/K(T)$ en un punt no ramificat $T = t_0$ és, en general, una extensió de Galois amb grup de Galois isomorf a un subgrup de G, ben definit només a menys de conjugació en G. Remarquem que, si $(T - t_0)$ és inert en $L_T/K(T)$, aleshores l'extensió L_{t_0}/K defineix, de manera natural, una G-extensió de K.

Sigui S un conjunt finit de places de $K(T)$ (trivials a K) tal que:

(a) $(T - t_0) \notin S$,

(b) S conté totes les places ramificades a $L_T/K(T)$.

Es té una inclusió de cossos $L_T \subset \overline{K(T)}^S$, on $\overline{K(T)}^S/K(T)$ denota la màxima subextensió de $\overline{K(T)}/K(T)$ no ramificada fora de S.

Cada plaça $\mathcal{P}_0$ de $\overline{K(T)}^S$ sobre $(T - t_0)$ dóna lloc a un monomorfisme $s_0 : G_K \to \mathrm{Gal}(\overline{K(T)}^S/K(T))$ (subgrup de descomposició) que ens permet fer la següent definició.

Definició 1.3.10. *Amb les notacions anteriors, anomenarem **especialització** de φ_T en $T = t_0$ al morfisme*

$$\varphi_{t_0} = \varphi_T \circ s_0 : G_K \to G.$$

Notem que aquesta definició depèn del primer $\mathcal{P}_0$ triat. Implícitament, sempre suposarem fixat $\mathcal{P}_0$ com més amunt i, per tant, no hi haurà ambigüitat en dir que un morfisme $\varphi : G_K \to G$ és l'especialització de φ_T en $T = t_0$.

D'aquesta manera, la imatge $H = \varphi_{t_0}(G_K)$ és un subgrup ben definit de G i l'especialització L_{t_0}/K defineix, de forma natural, una H-extensió de K.

Observem, finalment, que el conjunt S es pot ampliar per tal que contingui, per exemple, tots els primers ramificats en alguna altra extensió de $K(T)$ (sempre que també sigui no ramificada en $(T - t_0)$).

1.4 Polígons de Newton

Per a cada primer p, suposem fixada una clausura algebraica $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ i una valoració v_p a $\overline{\mathbb{Q}_p}$, extensió de la valoració p-àdica de $\mathbb{Q}_p$.

Definició 1.4.1. *Donat un primer p i un polinomi $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \overline{\mathbb{Q}_p}[X]$, anomenem **polígon de Newton de f(X)** a l'envolvent convexa inferior del conjunt de punts del pla $\{(i, v_p(a_i))\}_i$ (ignorant els coeficients nuls) i el denotem per $N(f(X))$.*

Comencem recordant el següent resultat bàsic de la teoria clàssica dels polígons de Newton (cf., per exemple, [Mil96] o [Neu99, Chap. II, §6.]).

Proposició 1.4.2. *Si el polígon de Newton $N(f(X))$ d'un polinomi mònic $f(X) \in \overline{\mathbb{Q}_p}[X]$ té un segment d'amplada m i pendent $-s$, aleshores $f(X)$ té exactament m arrels α_i amb $v_p(\alpha_i) = s$.*

A més, el polinomi $f_s(X) = \prod_{v_p(\alpha_i)=s}(X - \alpha_i)$ té coeficients a $\mathbb{Q}_p(\{a_i\}_i)$.

Tenint en compte que l'índex de ramificació $e(K/\mathbb{Q}_p)$ d'una extensió finita $K/\mathbb{Q}_p$ es caracteritza per la propietat $v_p(K^*) = \dfrac{1}{e(K/\mathbb{Q}_p)}\mathbb{Z}$, es té:

Corol.lari 1.4.3. *Sigui $(\mathbb{Q}_p)_f$ el cos obtingut adjuntant a $\mathbb{Q}_p$ les arrels d'un polinomi mònic i separable $f(X) \in \overline{\mathbb{Q}_p}[X]$. Si el polígon de Newton $N(f(X))$ té un segment d'amplada m i pendent $-s = -\frac{h}{e}$ amb $(h, e) = 1$, aleshores e divideix l'índex de ramificació $e((\mathbb{Q}_p)_f/\mathbb{Q}_p)$.*

En aquesta memòria, usarem la Teoria dels polígons de Newton només per a obtenir conclusions del tipus "p no ramifica"o "p és moderadament ramificat"enlloc de "l'índex de ramificació i el grau residual de p són ...". Per aquest motiu, els resultats anteriors seran essencialment suficients per als nostres propòsits. Tot i així, per comoditat, usarem també alguns resultats més precisos de Ore [Ore28] (Teorema del polígon i Teorema del polinomi associat) que es poden trobar, per exemple, a [Mon99]. Ens limitem a recordar les definicions i enunciats en la situació particular en la qual després els aplicarem.

Definició 1.4.4. *Donat un polinomi $f(X) \in \mathbb{Z}_p[X]$ i un polinomi mònic $\phi(X) \in \mathbb{Z}_p[X]$, considerem el desenvolupament $\phi(X)$-àdic de $f(X)$*

$$f(X) = \sum_i A_i(X)(\phi(X))^i.$$

*Anomenem **polígon de Newton de** $f(X)$ **respecte** $\phi(X)$ a $N_\phi(f(X))$, l'envolvent convexa inferior del conjunt de punts del pla $\{(i, v_p(A_i(X)))\}_i$, on $v_p(A_i(X))$ és el mínim de les valoracions p-àdiques dels coeficients de $A_i(X)$.*

Per a un polinomi $f(X) \in \mathbb{Z}_p[X]$, denotarem per $\overline{f}(X) \in \mathbb{F}_p[X]$ la reducció mòdul p de $f(X)$.

Definició 1.4.5. *Amb les notacions i hipòtesis de la definició anterior, suposem que $\overline{\phi}(X) \in \mathbb{F}_p[X]$ és un factor irreductible de grau m de $\overline{f}(X) \in \mathbb{F}_p[X]$ i que $\xi \in \overline{\mathbb{F}_p}$ és una arrel de $\overline{\phi}(X)$. Si S és un segment de pendent negativa $-\frac{h}{e}$ de $N_\phi(f(X))$ amb $(h, e) = 1$ i α és el mínim de les abscisses dels punts de*

S, anomenem ***polinomi associat a*** $f(X)$ ***i al segment*** S *a:*

$$P_S(X) = \sum_i \overline{B_i}(\xi) X^{\frac{i-\alpha}{e}} \in \mathbb{F}_{p^m}[X],$$

on el sumatori recorre els punts $(i, v_p(A_i(X))) \in S$ *i* $B_i(X)$ *es defineix per* $B_i(X) = p^{-v_p(A_i(X))} A_i(X) \in \mathbb{Z}_p[X]$.

La Proposició següent resumeix els resultats que volem recordar en termes de descomposició d'ideals.

Proposició 1.4.6. *Sigui* p *un primer qualsevol. Considerem un cos de nombres* $K = \mathbb{Q}(\theta)$ *amb anell d'enters* $\mathcal{O}$*, on* $\theta \in \overline{\mathbb{Q}}$ *és una arrel d'un polinomi irreductible i mònic* $f(X) \in \mathbb{Q}[X]$ *amb tots els coeficients de valoració* p*-àdica positiva.*

(i) (Lema de Hensel) Si $\overline{f}(X) = \psi_1(X)^{a_1} \cdots \psi_k(X)^{a_k}$ *és la descomposició de* $\overline{f}(X)$ *en producte d'irreductibles mònics a* $\mathbb{F}_p[X]$*, aleshores l'ideal* $p\mathcal{O}$ *admet una descomposició del tipus* $p\mathcal{O} = \mathfrak{a}_1 \cdots \mathfrak{a}_k$*, on els* $\mathfrak{a}_i$ *són ideals de* $\mathcal{O}$ *coprimers dos a dos.*
Per a cada ideal primer $\mathfrak{p}$ *que divideix* $\mathfrak{a}_i$*, el grau residual* $f(\mathfrak{p}|p)$ *és divisible per* $gr(\psi_i)$ *i* $\sum_{\mathfrak{p}|\mathfrak{a}_i} f(\mathfrak{p}|p).e(\mathfrak{p}|p) = a_i.gr(\psi_i)$*. En particular, si* $a_i = 1$*, aleshores* $\mathfrak{a}_i$ *és un ideal primer (no ramificat).*

(ii) (Teorema del polígon) Amb les notacions de (i), fixem un $\psi_i(X)$ *i notem* $\psi(X) = \psi_i(X)$*,* $a = a_i$ *i* $\mathfrak{a} = \mathfrak{a}_i$*; considerem un polinomi mònic* $\phi(X) \in \mathbb{Z}[X]$ *de grau* $m = gr(\psi(X))$ *tal que* $\overline{\phi}(X) = \psi(X)$*. Si el polígon de Newton* $N_\phi(f(X))$ *té* r *costats* $S_1, \ldots, S_r$ *de pendents negatives* $\{-\frac{h_i}{e_i}\}_i$ *amb* $(h_i, e_i) = 1$*, aleshores l'ideal* $\mathfrak{a}$ *admet una descomposició del tipus* $\mathfrak{a} = {\mathfrak{b}_1}^{e_1} \cdots {\mathfrak{b}_r}^{e_r}$*, on els* $\mathfrak{b}_i$ *són ideals de* $\mathcal{O}$ *coprimers dos a dos.*
Si l'amplada del costat S_i *és* $e_i.d_i$*, aleshores* $\sum_{\mathfrak{p}|\mathfrak{b}_i} f(\mathfrak{p}|p).e(\mathfrak{p}|p) = m.e_i.d_i$*. En particular, si* $d_i = 1$*, aleshores* $\mathfrak{b}_i$ *és un ideal primer (amb índex de ramificació* $e(\mathfrak{b}_i|p) = e_i$ *i grau residual* $f(\mathfrak{b}_i|p) = m$*).*

(iii) *(Teorema del polinomi associat) Amb les notacions de (ii), fixem un costat S_i i notem $S = S_i$, $e = e_i$, $h = h_i$ i $\mathfrak{b} = \mathfrak{b}_i$. Si $P_S(X) = c.\chi_1(X)^{b_1} \cdots \chi_s(X)^{b_s}$ és la descomposició en producte d'irreductibles mònics a $\mathbb{F}_{p^m}[X]$ del polinomi associat a $f(X)$ i al costat S, aleshores l'ideal $\mathfrak{b}$ admet una descomposició del tipus $\mathfrak{b} = \mathfrak{c}_1 \cdots \mathfrak{c}_s$, on els $\mathfrak{c}_i$ són ideals de $\mathcal{O}$ coprimers dos a dos.*

Per a cada ideal primer $\mathfrak{p}$ que divideix $\mathfrak{c}_i$, el grau residual $f(\mathfrak{p}/p)$ és divisible per $m.gr(\chi_i)$ i $\sum_{\mathfrak{p}|\mathfrak{c}_i} f(\mathfrak{p}|p).e(\mathfrak{p}|p) = m.e.b_i.gr(\chi_i)$. En particular, si $b_i = 1$, aleshores $\mathfrak{c}_i$ és un ideal primer (amb índex de ramificació $e(\mathfrak{c}_i/p) = e$ i grau resiual $f(\mathfrak{c}_i/p) = m.gr(\chi_i)$).

Montes [Mon99] generalitza les definicions i resultats anteriors amb la introducció dels polígons de Newton d'ordre superior. Tot i que no usarem explícitament els seus resultats, cal remarcar que els polígons de Newton d'ordre superior apareixeran implícitament (de fet, els de segon ordre) en el Capítol 3.

Capítol 2

Nombre de primers ramificats i nombre de generadors

2.1 Introducció

Donat un grup finit G, $ram(G)$ denotarà el mínim natural tal que G es realitza com a grup de Galois d'alguna extensió de $\mathbb{Q}$ ramificada exactament en $ram(G)$ primers finits. Definim $ram^t(G)$ de manera anàloga quan, a més, ens restringim a extensions moderadament ramificades.

L'objectiu principal d'aquest capítol és estudiar $ram(G)$ i $ram^t(G)$ per a certes famílies de grups resolubles G.

La Secció 2.2 està dedicada als grups nilpotents finits d'ordre senar.

El Teorema de Scholz-Reichardt (cf. [Rei37]) estableix que, donat un primer senar l, tot l-grup és grup de Galois d'una extensió de $\mathbb{Q}$. Per a realitzar un l-grup G d'ordre l^N és suficient resoldre (pròpiament) una successió de N problemes d'immersió centrals amb nucli $\mathbb{Z}/l\mathbb{Z}$, partint del morfisme trivial $G_{\mathbb{Q}} \to \{1\}$. A [Ser92b, Chap. 2] es veu que aquest procés es pot fer afegint un únic primer ramificat en cada pas, obtenint $ram^t(G) \leq N$. Aquesta fita

es pot millorar fàcilment per a obtenir el valor $N - n + d$, on l^n és l'ordre de l'abelianitzat G^{ab} i $d = d(G)$ és el nombre mínim de generadors de G (i de G^{ab}). A diferència de la primera, aquesta nova fita coincideix amb el valor exacte en el cas de l-grups abelians, per als quals es té $ram(G) = ram^t(G) = d$ gràcies al Teorema de Kronecker-Weber.

Basant-nos en la demostració del Teorema de Scholz-Reichardt de [Ser92b], millorem la fita anterior. La millora consisteix, essencialment, en admetre problemes d'immersió centrals amb nucli cíclic qualsevol (no necessàriament d'ordre l) i veure que encara és suficient afegir un únic primer ramificat en cada pas. D'aquesta manera, afitem $ram^t(G)$ en termes dels nombres mínims de generadors dels factors de la sèrie central inferior de G. Generalitzem aquesta millora al cas en el qual G és un grup nilpotent finit d'ordre senar. Per alguns d'aquests grups G com, per exemple, tots els de classe de nilpotència ≤ 2, la fita obtinguda proporciona el valor exacte $ram(G) = ram^t(G) = d(G)$. En un resultat recent [CHVS00] s'afirma la validesa de la igualtat anterior per a tot grup nilpotent finit G d'ordre senar. En la demostració d'aquest resultat, però, hem trobat un error.

A la Secció 2.3 ens ocupem dels grups diedrals generalitzats. Aquests són precisament els grups de Galois dels anomenats cossos de classes d'anell d'algun cos quadràtic, que hem recordat al Capítol 1.

El resultat principal que obtenim és que $ram^t(G) \leq d(G)$, per a qualsevol grup diedral generalitzat G. Per a demostrar aquesta desigualtat usem les fórmules, recordades al Capítol 1, per al grau del cos de classes d'anell per al conductor f d'un cos quadràtic. L'existència de grups de classes no trivials per a cossos quadràtics fa que, en general, aquesta fita no sigui òptima (és a dir, sovint passa $ram^t(G) < d(G)$). Caracteritzem, a més, els grups diedrals G amb la propietat $ram^t(G) = 1$ (resp. $ram(G) = 1$).

A la Secció 2.4 obtenim resultats condicionals sota la hipòtesi (H) de Schin-

zel. Concretament, assumint la validesa d'aquesta conjectura, obtenim el valor exacte de $ram^t(G)$ i $ram(G)$, per a tot grup diedral $G = D_{2n}$.

També veiem que, suposant certa la hipòtesi (H) de Schinzel, s'obté la igualtat $ram(S_n) = ram^t(S_n) = 1$, per a tot grup simètric S_n.

La Secció 2.5 està dedicada a una conjectura de Harbater relativa a les realitzacions galoisianes sobre $\mathbb{Q}$ moderadament ramificades. Així com l'objectiu en les seccions anteriors era afitar $ram^t(G)$ en termes de $d(G)$, ara es tracta d'afitar $d(G)$ en termes dels primers ramificats en una realització qualsevol de G com a grup de Galois d'una extensió moderadament ramificada de $\mathbb{Q}$. Establim la validesa de la fita proposada en la conjectura de Harbater, per a tot grup G extensió de $\mathbb{Z}/2\mathbb{Z}$ per un grup nilpotent finit d'ordre senar qualsevol.

2.2 Grups nilpotents finits d'ordre senar

En aquesta secció usarem notacions i resultats recordats a la Secció 1.1.

Donat un grup finit G, $D(G)$ denota el subgrup derivat de G i $G^{ab} := G/D(G)$ l'abelianitzat de G. Com en tota la memòria, $d(G)$ és el nombre mínim de generadors de G.

Pel Teorema de la base de Burnside, si G és un grup nilpotent finit, aleshores $d(G) = d(G^{ab})$.

Com en el capítol anterior, sobre cada primer racional p suposarem fixat un primer $\overline{p}$ de $\overline{\mathbb{Q}}$ i denotarem per D_p (resp. I_p) el corresponent subgrup de descomposició (resp. inèrcia) en $G_{\mathbb{Q}}$.

Suposem fixat un primer senar l.

Definició 2.2.1. *Siguin G un l-grup i $K/\mathbb{Q}$ la G-extensió de $\mathbb{Q}$ corresponent a un epimorfisme $\varphi : G_{\mathbb{Q}} \to G$. Sigui N un natural. Direm que l'extensió $K/\mathbb{Q}$ és* ***de tipus*** *(S_N) quan, per a tot primer p ramificat a $K/\mathbb{Q}$, es satisfà:*

- $p \equiv 1 \pmod{l^N}$,
- $\varphi(I_p) = \varphi(D_p)$.

En aquest cas, també direm que l'epimorfisme φ és ***de tipus*** (S_N).

Un fet essencial en l'estratègia del Teorema de Scholz-Reichardt és la validesa d'un principi local-global per a problemes d'immersió centrals finits amb nucli $\mathbb{Z}/l\mathbb{Z}$. La condició "tipus (S_N)"s'introdueix precisament per a garantir (N prou gran) la resolubilitat dels problemes locals en tots els primers ramificats. Tenint en compte que els problemes locals en els primers no ramificats sempre admeten solució, s'obté el resultat següent (cf. [Ser92b, Chap. 2]).

Teorema 2.2.2. *Sigui $1 \to C \to G \xrightarrow{\pi} H \to 1$ una extensió central de l-grups i $\varphi : G_{\mathbb{Q}} \to H$ l'epimorfisme corresponent a una H-extensió de $\mathbb{Q}$ de tipus (S_N). Si l^N és múltiple de l'exponent de G, aleshores el problema d'immersió (π, φ) és resoluble.*

Tenint en compte la Proposició 1.1.5, es pot modificar convenientment una solució de (π, φ) per a obtenir una solució pròpia de tipus (S_N). D'aquí es dedueix el Teorema de Scholz-Reichardt, donat que tot l-grup s'obté per successives extensions centrals partint del grup trivial (cf. [Ser92b, Chap. 2]).

Ens interessa fer aquest procés augmentant poc la ramificació i de manera que els resultats siguin generalitzables a grups nilpotents finits d'ordre senar. Amb aquest objectiu, aplicarem la Proposició 1.1.5 amb elements ben triats de $\mathrm{Hom}(G_{\mathbb{Q}}, C)$, l'existència dels quals cal provar primer. Es tracta de generalitzar convenientment [Ser92b, Lemma 2.1.9].

Denotarem per $\mathrm{Ram}(K/\mathbb{Q})$ el conjunt dels nombres primers ramificats en una extensió $K/\mathbb{Q}$. Si $K/\mathbb{Q}$ és una G-extensió corresponent a un epimorfisme $\varphi : G_{\mathbb{Q}} \to G$, també notarem $\mathrm{Ram}(\varphi) = \mathrm{Ram}(K/\mathbb{Q})$.

Proposició 2.2.3. *Sigui l un primer senar. Considerem una l-extensió $K/\mathbb{Q}$ de tipus (S_N) i un grup cíclic $C =< c >$ d'ordre l^r amb $r \leq N$. Suposem fixat un primer p_0 ramificat a $K/\mathbb{Q}$ i notem $S = \mathrm{Ram}(K/\mathbb{Q}) \backslash \{p_0\}$.*

Donats enters qualssevol $\{\nu_p\}_{p\in S}$*, aleshores:*

(i) Per a tot natural $k<r$*, existeix algun (infinits) primer* q *tal que:*

- q *descompon completament a* $K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l^k]{p_0}\right)$,
- q *no descompon completament a* $\mathbb{Q}\left(\zeta_{l^N}, \sqrt[l^{k+1}]{p_0}\right)$.

(ii) Per a qualsevol enter ν_0 *amb* $v_l(\nu_0)<r$ *i qualsevol primer* q *com a (i) amb* $k=v_l(\nu_0)$*, existeix un epimorfisme* $\chi:(\mathbb{Z}/q\mathbb{Z})^*\to C$ *de manera que:*

- $\chi(p_0)=c^{\nu_0}$,
- $\chi(p)=c^{\nu_0\cdot\nu_p}$*, per a tot* $p\in S$.

Demostració. (i) Pel Teorema de densitat de Txebotarev (cf., per exemple, [Jan96, Chap.V, 10.4]), és suficient veure:

$$\sqrt[l^{k+1}]{p_0}\notin K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l^k]{p_0}\right).$$

Si això no fos cert, la teoria de Kummer (amb cos base $K\mathbb{Q}(\zeta_{l^N})$) proporcionaria una expressió del tipus:

$${p_0}^{l^{r-k-1}}=a^{l^r}\cdot\prod_{p\in S}\left(\frac{p}{{p_0}^{\nu_p}}\right)^{r_p}\cdot\left({p_0}^{l^{r-k}}\right)^{r_0},$$

per a certs $a\in K\mathbb{Q}(\zeta_{l^N})$ i $r_0,r_p\in\mathbb{Z}$, per a tot $p\in S$. Per tant,

$${p_0}^{l^{r-k-1}}=b^{l^{r-k}}\cdot\prod_{p\in S}\left(\frac{p}{{p_0}^{\nu_p}}\right)^{r_p},$$

per a cert $b\in K\mathbb{Q}(\zeta_{l^N})$. Això voldria dir que:

$$\sqrt[l]{p_0}\in K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right).$$

En particular, tindríem la inclusió de cossos:

$$K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l]{p_0}\right) \subseteq K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right).$$

D'altra banda, com a [Ser92b, Lemma 2.1.9], tenint en compte que l'extensió $\mathbb{Q}\left(\zeta_l, \left\{\sqrt[l]{p}\right\}_{p\in S}, \sqrt[l]{p_0}\right)/\mathbb{Q}$ no admet cap subextensió galoisiana de grau l, es dedueix la igualtat

$$\mathbb{Q}\left(\zeta_l, \{\sqrt[l]{p}\}_{p\in S}, \sqrt[l]{p_0}\right) \cap K\mathbb{Q}(\zeta_{l^N}) = \mathbb{Q}(\zeta_l).$$

Per tant, si s denota el cardinal de S, es té un isomorfisme

$$\mathrm{Gal}\left(K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}, \sqrt[l]{p_0}\right)/K\mathbb{Q}\left(\zeta_{l^N}\right)\right) \cong \mathbb{Z}/l\mathbb{Z}\times \overset{s+1}{\cdots} \times\mathbb{Z}/l\mathbb{Z}.$$

Per la inclusió de cossos obtinguda, aquest grup hauria de ser un quocient de

$$\mathrm{Gal}\left(K\mathbb{Q}\left(\zeta_{l^N}, \left\{\sqrt[l^{r-k}]{\frac{p}{{p_0}^{\nu_p}}}\right\}_{p\in S}\right)/K\mathbb{Q}\left(\zeta_{l^N}\right)\right).$$

Aquest darrer grup de Galois, però, es pot generar amb només s elements, donat que correspon a la composició de s extensions cícliques. Hem arribat a una contradicció, tal com volíem.

(ii) Per hipòtesi, $q \equiv 1 \pmod{l^N}$ i C és isomorf al subgrup C' de $(\mathbb{Z}/q\mathbb{Z})^*$ format pels elements d'ordre dividint l^r.

Considerem l'epimorfisme natural "elevar a $\frac{q-1}{l^r}$":

$$\chi' : (\mathbb{Z}/q\mathbb{Z})^* \to C'.$$

Les condicions de (i) sobre q garanteixen que:

- p_0 és una l^k-èsima potència mòdul q,
- $\frac{p}{{p_0}^{\nu_p}}$ és una l^r-èsima potència mòdul q, per a tot $p \in S$,

- p_0 no és una l^{k+1}-èsima potència mòdul q.

Equivalentment,

- $\chi'(p_0)$ té ordre l^{r-k},
- $\chi'(p) = \chi'(p_0)^{\nu_p}$, per a tot $p \in S$.

Això és el que calia veure donat que, per hipòtesi, $v_l(\nu_0) = k$ i, per tant, existeix algun generador c' de C' tal que $\chi'(p_0) = (c')^{\nu_0}$ i $\chi'(p) = (c')^{\nu_0 \cdot \nu_p}$, per a tot $p \in S$. □

La Proposició anterior ens permet obtenir la següent generalització de [Ser92b, Thm. 2.1.3].

Proposició 2.2.4. *Sigui l un primer senar. Considerem una extensió central de l-grups $1 \to C \to G \xrightarrow{\pi} H \to 1$ amb nucli cíclic i un epimorfisme $\varphi : G_{\mathbb{Q}} \to H$. Sigui N tal que l^N és múltiple de l'exponent de G. Si l'epimorfisme φ és de tipus (S_N) i el problema d'immersió (π, φ) és Frattini o split, aleshores (π, φ) admet una solució pròpia $\widetilde{\varphi}$ de tipus (S_N) tal que:*

$$\sharp \operatorname{Ram}(\widetilde{\varphi}) \leq 1 + \sharp \operatorname{Ram}(\varphi).$$

Demostració. Suposem primer que el problema d'immersió és Frattini.

Pel Teorema 2.2.2 i per l'apartat (i) de la Proposició 1.1.8, existeix alguna solució ψ del problema d'immersió (π, φ) tal que $\operatorname{Ram}(\psi) = \operatorname{Ram}(\varphi)$. Per la Proposició 1.1.3, s'ha de tractar d'una solució pròpia.

Per a cada primer p, triem una antimatge $\sigma_p \in D_p$ de l'automorfisme de Frobenius $Frob_p \in G_{\mathbb{F}_p} \cong \widehat{\mathbb{Z}}$ per l'epimorfisme $D_p \to D_p/I_p \cong G_{\mathbb{F}_p}$.

La hipòtesi (S_N) sobre φ garanteix que, per a tot $p \in \operatorname{Ram}(\varphi)$, $\varphi(\sigma_p) \in \varphi(I_p)$. Canviant els representants σ_p triats, podem suposar que $\varphi(\sigma_p) = 1$ i, per tant, $\psi(\sigma_p) \in C$, per a tot $p \in \operatorname{Ram}(\varphi)$. Triem $p_0 \in \operatorname{Ram}(\varphi)$ de manera que tots els elements $\{\psi(\sigma_p)\}_{p \in \operatorname{Ram}(\varphi)}$ pertanyin al subgrup $< \psi(\sigma_{p_0}) > \subseteq C$.

Suposem $\psi(\sigma_{p_0}) \neq 1$; altrament, $\widetilde{\varphi} := \psi$ ja satisfà les conclusions desitjades.

Definim $S = \mathrm{Ram}(\varphi)\backslash\{p_0\}$. Fixat un generador c de C, existeixen naturals $\{\nu_p\}_{p\in\mathrm{Ram}(\varphi)}$ tals que, notant $\nu_0 = \nu_{p_0}$ es té:

- $\psi(\sigma_{p_0}) = c^{\nu_0}$,
- $\psi(\sigma_p) = (c^{\nu_0})^{\nu_p}$, per a tot $p \in S$.

Per la Proposició anterior, existeix un epimorfisme $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to C$ tal que:

- q és un primer satisfent $\varphi(D_q) = \{1\}$,
- $q \equiv 1 \pmod{l^N}$,
- $\chi(p) = \psi(\sigma_p)$, per a tot $p \in \mathrm{Ram}(\varphi)$.

També denotarem per χ l'epimorfisme $G_{\mathbb{Q}} \to C$ deduït de l'isomorfisme natural $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^*$ que, per a tot $p \neq q$, identifica $\sigma_{p_{|\mathbb{Q}(\zeta_q)}}$ amb $p \pmod{q}$.

És clar que $\widetilde{\varphi} := \psi.\chi^{-1} : G_{\mathbb{Q}} \to G$ és una solució del problema d'immersió (π, φ) tal que $\mathrm{Ram}(\widetilde{\varphi}) = \mathrm{Ram}(\varphi) \cup \{q\}$. A més, es tracta d'una solució pròpia, donat que estem suposant que el problema (π, φ) és Frattini. Finalment, observem que $\widetilde{\varphi}$ és de tipus (S_N), per ser:

- $\widetilde{\varphi}(D_p) =< \widetilde{\varphi}(\sigma_p), \widetilde{\varphi}(I_p) >= \widetilde{\varphi}(I_p)$, per a tot $p \in \mathrm{Ram}(\varphi)$,
- $\widetilde{\varphi}(D_q) \subseteq C = \chi^{-1}(I_q) = \widetilde{\varphi}(I_q)$.

Suposem, ara, que el problema (π, φ) és split, és a dir, $G \cong H \times C$.

En aquest cas, és suficient raonar com a [Ser92b, pàg. 11]. Concretament, si $K/\mathbb{Q}$ és la H-extensió corresponent a φ i q és un primer que descompon completament en

$$K\mathbb{Q}\left(\zeta_{l^N}, \{\sqrt[l^r]{p}\}_{p\in\mathrm{Ram}(\varphi)}\right),$$

aleshores, qualsevol epimorfisme

$$\chi : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^* \to C$$

satisfà:

- $\chi(\sigma_p) = 1$, per a tot $p \in \mathrm{Ram}(\varphi)$,
- $\mathrm{Ram}(\chi) = \{q\}$.

En particular, χ correspon a una C-extensió de $\mathbb{Q}$, linealment disjunta de $K/\mathbb{Q}$. Tenint en compte que els primers que ramifiquen en una d'aquestes dues extensions descomponen completament en l'altra, l'epimorfisme

$$\widetilde{\varphi} : G_{\mathbb{Q}} \xrightarrow{(\varphi,\chi)} H \times C \cong G$$

satisfà les conclusions enunciades. □

Per a un l-grup G, el resultat anterior permet obtenir una fita per al nombre mínim de primers ramificats en una G-extensió de $\mathbb{Q}$. Recordem primer algunes definicions.

Els **subgrups commutadors superiors** $C_i(G)$ d'un grup G es defineixen inductivament per:

$$\begin{cases} C_1(G) := G \\ C_{i+1}(G) := [C_i(G), G], \text{ si } i > 1. \end{cases}$$

Un grup G és **nilpotent** si existeix un enter r tal que

$$C_r(G) = \{1\}$$

i, per tant, el mateix val per a tot $i > r$. La **classe de nilpòtencia** d'un grup nilpotent G és el mínim natural n tal que

$$C_{n+1}(G) = \{1\}.$$

Recordem també que, per a un grup finit G, $ram(G)$ (resp. $ram^t(G)$) denota el nombre mínim de primers finits ramificats en alguna G-extensió (resp. G-extensió moderadament ramificada) de $\mathbb{Q}$.

Proposició 2.2.5. *Si l és un primer senar i G és un l-grup de classe de nilpotència n, aleshores:*

$$d(G) \leq ram(G) \leq ram^t(G) \leq d(G) + \sum_{2 \leq i \leq n-1} d(C_i(G)/C_{i+1}(G)),$$

entenent que el sumatori és nul quan $n \leq 2$.

Demostració. La primera desigualtat és evident si tenim en compte que, pel Teorema de la base de Burnside i pel Teorema de Kronecker-Weber,

$$d(G) = d(G^{ab}) = ram(G^{ab}).$$

Centrem-nos, doncs, en la darrera desigualtat.

Si $n = 1$, aleshores $G = G^{ab}$ i hem acabat.

Suposem $n \geq 2$. Per hipòtesi, tenim una cadena d'extensions centrals:

$$\begin{cases} 1 \to C_n(G) \to G \stackrel{\pi_n}{\to} G/C_n(G) \to 1 \\ 1 \to C_{n-1}(G)/C_n(G) \to G/C_n(G) \stackrel{\pi_{n-1}}{\to} G/C_{n-1}(G) \to 1 \\ \quad \vdots \\ 1 \to C_2(G)/C_3(G) \to G/C_3(G) \stackrel{\pi_2}{\to} G/C_2(G) \to 1 \\ 1 \to G/C_2(G) \to G/C_2(G) \stackrel{\pi_1}{\to} \{1\} \to 1 \end{cases}$$

Per definició, $C_2(G)$ és el grup derivat de G i, per tant, $G/C_2(G) = G^{ab}$ és l'abelianitzat de G. Així, la successió exacta definida per π_1 descompon en $d(G) = d(G^{ab})$ successives extensions centrals cícliques split. Per a $i > 1$, la successió exacta definida per π_i descompon en $d(C_i(G)/C_{i+1}(G))$ successives extensions centrals cícliques que, per força, han de ser Frattini.

Partint de l'epimorfisme trivial $\varphi_1 : G_{\mathbb{Q}} \to \{1\}$ i aplicant successivament la Proposició anterior, obtenim un epimorfisme $\varphi_n : G_{\mathbb{Q}} \to G/C_n(G)$ de tipus

(S_N) ramificat en, com a màxim,

$$\sum_{1\leq i\leq n-1} d(C_i(G)/C_{i+1}(G) \;=\; d(G) + \sum_{2\leq i\leq n-1} d(C_i(G)/C_{i+1}(G)$$

primers. En particular, $l \notin \mathrm{Ram}(\varphi_n)$.

Només falta observar que, pel Teorema 2.2.2 i la Proposició 1.1.8, el problema (π_n, φ_n) admet una solució $\varphi : G_{\mathbb{Q}} \to G$ satisfent $\mathrm{Ram}(\varphi) = \mathrm{Ram}(\varphi_n)$. Tractant-se d'un problema Frattini, aquesta solució haurà de ser pròpia. □

El resultat anterior admet la següent generalització.

Teorema 2.2.6. *Si G és un grup nilpotent d'ordre senar i $\{G_1, \ldots, G_s\}$ són els seus subgrups de Sylow, aleshores:*

$$d(G) \;\leq\; ram(G) \;\leq\; ram^t(G) \;\leq\; \max_{1\leq j\leq s}\left\{ d(G_j) + \sum_{2\leq i\leq n_j-1} d(C_i(G_j)/C_{i+1}(G_j)) \right\},$$

entenent que el sumatori és nul quan la classe de nilpotència de G_j satisfà $n_j \leq 2$.

Demostració. La primera desigualtat és clara, com abans.

Per hipòtesi, es té un isomorfisme $G \cong G_1 \times \cdots \times G_s$, on cada G_j és un l_j-grup per a cert primer senar l_j. Així, la darrera desigualtat equival a l'existència de G_j-extensions $K_j/\mathbb{Q}$ moderadament ramificades i tals que:

$$\sharp\left(\bigcup_j \mathrm{Ram}(K_j/\mathbb{Q})\right) \leq \max_{1\leq j\leq s}\left\{ d(G_j) + \sum_{2\leq i\leq n_j-1} d(C_i(G_j)/C_{i+1}(G_j)) \right\}.$$

Això s'obté amb un raonament anàleg al fet a la demostració de la Proposició anterior, usant la generalització de la Proposició 2.2.4 que demostrem a continuació. □

Proposició 2.2.7. *Sigui $\mathcal{L} = \{l_1, \dots, l_s\}$ un conjunt finit de primers senars. Per a cada $l_j \in \mathcal{L}$, considerem una extensió central de l_j-grups*

$$1 \to C_j \to G_j \xrightarrow{\pi_j} H_j \to 1$$

amb nucli cíclic C_j i un epimorfisme $\varphi_j : G_{\mathbb{Q}} \to H_j$. Sigui N un natural tal que ${l_j}^N$ és múltiple de l'exponent de G_j, per a tot $1 \leq j \leq s$. Suposem que, per a cada $l_j \in \mathcal{L}$, l'epimorfisme φ_j és de tipus (S_N), el conjunt $\mathrm{Ram}(\varphi_j)$ no conté cap dels primers de $\mathcal{L}$ i el problema d'immersió (π_j, φ_j) és Frattini o split. Aleshores, cadascun dels problemes (π_j, φ_j) admet una solució pròpia $\widetilde{\varphi_j}$ de tipus (S_N) de manera que

$$\sharp\left(\bigcup_j \mathrm{Ram}(\widetilde{\varphi_j})\right) \leq 1 + \sharp\left(\bigcup_j \mathrm{Ram}(\varphi_j)\right).$$

Demostració. Quan $s = 1$, el resultat enunciat no és res més que la Proposició 2.2.4.

Tenint en compte com hem demostrat la cadena d'implicacions

$$\text{Prop. 2.2.3 (i)} \Rightarrow \text{Prop. 2.2.3 (ii)} \Rightarrow \text{Prop. 2.2.4},$$

només cal generalitzar convenientment l'apartat (i) de la Proposició 2.2.3.

Per a cada $j \in \{1, \dots, s\}$, assumim les hipòtesis i notacions de la Proposició 2.2.3, convenint que un subíndex j denota dependència respecte el primer l_j i que prenem:

$$\begin{cases} N_j = N, \\ K_j/\mathbb{Q} \text{ la } H_j\text{-extensió corresponent a } \varphi_j\ . \end{cases}$$

Per a simplificar, si $K = K_j$, $l = l_j$, $S = S_j$, $p_0 = p_{0,j}$ i $k = k_j$, notarem:

$$\begin{cases} L_j = K\mathbb{Q}\left(\zeta_{l^N}, \left\{ \sqrt[l^r]{\frac{p}{{p_0}^{\nu_p}}} \right\}_{p \in S}, \sqrt[l^k]{p_0}\right), \\ M_j = \mathbb{Q}\left(\zeta_{l^N}, \sqrt[l^{k+1}]{p_0}\right). \end{cases}$$

D'aquesta manera, el que cal veure és que existeix un primer q tal que, per a tot $j \in \{1, \dots, s\}$, q descompon completament a L_j i q no descompon completament a M_j.

Comencem observant que l'apartat (i) de la Proposició 2.2.3 estableix la igualtat $[L_j.M_j : L_j] = l_j$, per a cada j.

Notem $a = (l_1 \cdot \ldots \cdot l_s)^N$ i $a(j) = \frac{a}{l_j{}^N}$.

Per hipòtesi, les extensions $L_j.M_j/\mathbb{Q}$ i $\mathbb{Q}(\zeta_{a(j)})/\mathbb{Q}$ tenen ramificació disjunta i, per tant, $[L_j.M_j(\zeta_a) : L_j(\zeta_a)] = l_j$. Com que l_j no divideix el grau de l'extensió $L_1 \ldots L_s.M_1 \ldots M_{j-1}/L_j(\zeta_a)$, obtenim que:

$$M_j \nsubseteq L_1 \ldots L_s.M_1 \ldots M_{j-1}\,, \quad \text{per a tot } j \in \{1, \ldots, s\}.$$

En particular, existeix algun $\sigma \in \mathrm{Gal}(L_1 \ldots L_s.M_1 \ldots M_s/L_1 \ldots L_s)$ tal que:

$$\sigma_{|M_j} \neq id\,, \quad \text{per a tot } j \in \{1, \ldots, s\}.$$

Pel Teorema de densitat de Txebotarev, existeixen infinits primers q amb les propietats desitjades. □

Observació 2.2.8. *El Teorema 2.2.6, a més de ser una generalització de la Proposició 2.2.5, la millora en el següent sentit.*

La Proposició 2.2.5 proporciona el valor exacte $ram(G) = ram^t(G) = d(G)$, només quan l és un primer senar i G és un l-grup de classe de nilpotència $n \leq 2$ (abelià o metabelià). Aquest resultat, de fet, s'obté directament del cas abelià, usant el Teorema 2.2.2 i la Proposició 1.1.3.

Del Teorema 2.2.6, en canvi, s'obté $ram(G) = ram^t(G) = d(G)$, per a tot grup nilpotent finit d'ordre senar tal que

$$d(G) \;=\; \max_{1\leq j\leq s} \left\{ d(G_j) + \sum_{2\leq i\leq n_j-1} d(C_i(G_j)/C_{i+1}(G_j)) \right\}.$$

Aquesta condició es satisfà per a altres grups, a més dels de classe de nilpotència $n = \max_j\{n_j\} \leq 2$.

Observació 2.2.9. *En un resultat recent [CHVS00, Thm. 5], s'enuncia la validesa de la igualtat*

$$ram(G) = ram^t(G) = d(G),$$

per a qualsevol grup nilpotent finit G d'ordre senar. En la demostració d'aquest resultat, però, hem trobat un error (pàg. 308, "Therefore, $q_1, \ldots, q_{h+1}$ are fleissig in $K_1''/\mathbb{Q}$ ...").

La prova de la igualtat passa, en algun moment, per considerar la situació següent (l primer senar):

- *l^N és múltiple de l'exponent d'un l-grup G,*
- *$1 \to \mathbb{Z}/l\mathbb{Z} \to G \xrightarrow{\pi} H \to 1$ és una extensió central Frattini,*
- *$\varphi : G_{\mathbb{Q}} \to H$ és un epimorfisme de tipus (S_N),*
- *$\sharp \operatorname{Ram}(\varphi) = d(H)$.*

Els autors obtenen, per "torçament"d'una solució $\widetilde{\varphi}_1$ del problema d'immersió (π, φ) tal que $\operatorname{Ram}(\widetilde{\varphi}_1) = \operatorname{Ram}(\varphi)$, una solució (pròpia) $\widetilde{\varphi}_2$ del mateix problema, de tipus (S_N) i tal que $\operatorname{Ram}(\widetilde{\varphi}_2) = \operatorname{Ram}(\varphi)$.

El següent resultat fa evident que aquest procés no és possible, a menys que $\widetilde{\varphi}_1$ ja sigui de tipus (S_N). Si no admetem nous primers ramificats, la solució al problema (π, φ) és essencialment única. Això també ens permet pensar que, en cert sentit, la fita obtinguda a la Proposició 2.2.5 (i al Teorema 2.2.6) no és millorable en general (sense modificar l'argument inductiu usat).

Proposició 2.2.10. *Sigui l un primer senar i G un l-grup d'exponent menor o igual que l^N. Considerem una extensió central Frattini $1 \to C \to G \xrightarrow{\pi} H \to 1$ amb nucli cíclic d'ordre l i un epimorfisme $\varphi : G_{\mathbb{Q}} \to H$ de tipus (S_N) tal que $\sharp \operatorname{Ram}(\varphi) = d(H)$. Aleshores, són equivalents:*

(i) El problema d'immersió (π, φ) admet una solució de tipus (S_N) ramificada només en $d(H)$ primers finits.

(ii) Tota solució del problema (π, φ) ramificada només en $d(H)$ primers finits és de tipus (S_N).

Demostració. Suposem que $\widetilde{\varphi}_1$, $\widetilde{\varphi}_2$ són dues solucions diferents del problema d'immersió (π, φ), necessàriament pròpies, tals que

$$\mathrm{Ram}(\widetilde{\varphi}_1) = \mathrm{Ram}(\widetilde{\varphi}_2) = \mathrm{Ram}(\varphi).$$

Així, existeix un epimorfisme $\chi \in \mathrm{Hom}(G_{\mathbb{Q}}, C)$ tal que

$$\widetilde{\varphi}_1 = \widetilde{\varphi}_2.\chi.$$

Per força, $\mathrm{Ram}(\chi) \subseteq \mathrm{Ram}(\varphi)$. És a dir,

$$\overline{\mathbb{Q}}^{Ker\chi}/\mathbb{Q}$$

és una extensió de grau l ramificada només en primers de $\mathrm{Ram}(\varphi)$. D'altra banda, la hipòtesi $\sharp\,\mathrm{Ram}(\varphi) = d(H) = d(H^{ab})$ garanteix que tota extensió abeliana de $\mathbb{Q}$ d'exponent l ramificada només en primers de $\mathrm{Ram}(\varphi)$ està continguda en la màxima subextensió abeliana de

$$\overline{\mathbb{Q}}^{Ker\varphi}/\mathbb{Q}.$$

Per tant, $\overline{\mathbb{Q}}^{Ker\chi} \subseteq \overline{\mathbb{Q}}^{Ker\varphi}$ i es té

$$\overline{\mathbb{Q}}^{Ker\widetilde{\varphi}_1} = \overline{\mathbb{Q}}^{Ker\widetilde{\varphi}_2}.$$

Dit d'una altra manera, totes les solucions del problema (π, φ) ramificades només en primers de $\mathrm{Ram}(\varphi)$ defineixen la mateixa extensió galoisiana de $\mathbb{Q}$. □

2.3 Grups diedrals generalitzats

En aquesta secció usarem resultats per als cossos de classes d'anell de cossos quadràtics, recordats a la Secció 1.2. Mantenim les notacions següents:

$d(G)$: nombre mínim de generadors d'un grup G,

G^{ab} : abelianitzat d'un grup G,

$r_2(A)$: 2-rang d'un grup abelià A,

$ram(G)$ (resp. $ram^t(G)$) : nombe mínim de primers finits ramificats en alguna G-extensió (resp. G-extensió moderadament ramificada) de $\mathbb{Q}$.

Per comoditat, en aquesta Secció denotarem per $K(\widetilde{f})$ el cos de classes d'anell per al conductor f d'un cos quadràtic K (a la Secció 1.2, era $K(P(\widetilde{f}))$).

Teorema 2.3.1. *Si A és un grup abelià finit, aleshores:*

$$d(D_{2A}^{ab}) \leq ram^t(D_{2.A}) \leq d(D_{2.A}).$$

Demostració. Del Teorema de Kronecker-Weber es dedueix la igualtat

$$ram^t(D_{2.A}^{ab}) = d(D_{2.A}^{ab}).$$

Així, la primera desigualtat enunciada és clara tenint en compte que, trivialment, $ram^t(D_{2.A}) \geq ram^t(D_{2.A}^{ab})$.

Només cal veure, doncs, $ram^t(D_{2.A}) \leq d(D_{2.A})$.

Sigui $r = d(A)$ el nombre mínim de generadors de A. Considerem naturals $m_1, \ldots, m_r$ tals que:

$$A \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.$$

Es té la igualtat $d(D_{2.A}) = r + 1$.

Fixem un primer senar qualsevol q i definim $K := \mathbb{Q}(\sqrt{q^*})$, on $q^* := (-1)^{\frac{q-1}{2}}q$. D'aquesta manera, el discriminant de K és $d_K = q^*$ i q és l'únic primer ramificat a l'extensió quadràtica $K/\mathbb{Q}$.

Per a un natural qualsevol $f \geq 2$, $E_{+,f}$ denotarà la constant considerada a la Proposició 1.2.8 (respecte $K = \mathbb{Q}(\sqrt{q^*})$). Recordem que, si $d_K < 0$, aleshores $E_{+,f}$ és independent de f; en canvi, quan $d_K > 0$, $E_{+,f}$ és el mínim natural tal que ${\epsilon_+}^{E_{+,f}} \in \mathcal{O}_f$, on ϵ_+ és el generador de les unitats totalment positives de l'anell d'enters $\mathcal{O}_K$ i $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ és l'ordre de conductor f.

Podem triar primers diferents $p_1, \ldots, p_r$ tals que:

$$(*) \qquad p_i \equiv 1 \pmod{m_i.E_{+,p_i}.q}, \text{ per a tot } i \in \{1, \ldots, r\}.$$

Això no suposa cap problema si K és imaginari. Per a K real, és suficient triar p_i que descompongui completament a $K(\zeta_{m_i.q}, \sqrt[m_i.q]{\epsilon_+})$ i raonar, per exemple, com a la demostració de [JY82, Thm. I.2.1]. Concretament, $m_i.q$ haurà de dividir $p_i - 1$ i, per a qualsevol ideal primer $\mathfrak{p}_i$ de $\mathcal{O}_K$ sobre p_i, $\epsilon_+ \pmod{\mathfrak{p}_i}$ haurà de ser una $(m_i.q)-$èsima potència a $\mathbb{F}_{p_i}$. Així,

$${\epsilon_+}^{\frac{p_i-1}{m_i.q}} \equiv 1 \pmod{p_i}$$

i, per tant, $\frac{p_i-1}{m_i.q}$ haurà de ser un múltiple de E_{+,p_i}, tal com volíem.

Fixem primers $p_1, \ldots, p_r$ satisfent la congruència $(*)$ i, per a cadascun d'ells, considerem el corresponent cos de classes d'anell de K per al conductor $\widetilde{f}$, $K(\widetilde{p_i})$. Recordem que el cicle $\widetilde{f}$ s'obté afegint a $f\mathcal{O}_K$ tots els primers infinits reals de K.

Si H_+ denota el cos de classes de Hilbert estricte de K, tenim una inclusió $H_+ \subseteq K(\widetilde{p_i})$.

D'altra banda, la fórmula recordada a la Proposició 1.2.8, estableix:

$$[K(\widetilde{p_i}) : K] = [H_+ : K].p_i.\left(1 - \frac{\left(\frac{q^*}{p_i}\right)}{p_i}\right).\frac{1}{E_{+,p_i}}.$$

Observem que la Llei de reciprocitat quadràtica i la congruència $(*)$ garanteixen:

$$\left(\frac{q^*}{p_i}\right) = \left(\frac{p_i}{q}\right) = 1 \ , \text{ per a tot } i \in \{1, \dots, r\}.$$

D'aquesta manera, notant $h_+ := [H_+ : K]$ i $n_i := \frac{p_i - 1}{E_{+,p_i}}$, obtenim:

$$[K(\widetilde{p_i}) : K] = h_+.n_i \ , \quad [K(\widetilde{p_i}) : H_+] = n_i.$$

Cadascun dels primers p_i descompon completament a K,

$$p_i \mathcal{O}_K = \mathfrak{p}_i.\mathfrak{p}_i'.$$

Els subgrups d'inèrcia de $\mathrm{Gal}(K(\widetilde{p_i})/K)$ en els ideals primers $\mathfrak{p}_i$ i $\mathfrak{p}_i'$ de $\mathcal{O}_K$ són conjugats a $\mathrm{Gal}(K(\widetilde{p_i})/\mathbb{Q})$. Com que l'extensió $K(\widetilde{p_i})/\mathbb{Q}$ és diedral generalitzada, aquests subgrups d'inèrcia són iguals i coincideixen amb el subgrup d'inèrcia de $\mathrm{Gal}(K(\widetilde{p_i})/\mathbb{Q})$ en p_i, que denotarem per I_i.

Tenint en compte que $\mathfrak{p}_i$ i $\mathfrak{p}_i'$ són els únics ideals primers de K que ramifiquen a $K(\widetilde{p_i})/K$ i que H_+/K és la màxima subextensió no ramificada en cap ideal primer, obtenim $I_i = \mathrm{Gal}(K(\widetilde{p_i})/H_+)$.

Per a cada $i \in \{1, \dots, r\}$, l'ordre del grup d'inèrcia I_i és $n_i = \frac{p_i - 1}{E_{+,p_i}}$. En particular, aquest ordre és coprimer amb p_i i, per tant, l'extensió $K(\widetilde{p_i})/\mathbb{Q}$ és moderadament ramificada en p_i. Així, I_i és un grup cíclic i es té:

$$\mathrm{Gal}(K(\widetilde{p_i})/H_+) = I_i \cong \mathbb{Z}/n_i\mathbb{Z}.$$

Cadascuna de les extensions $\{K(\widetilde{p_i})/H_+\}_i$ és totalment ramificada en els ideals primers de H_+ que divideixen p_i i no ramificada en cap altre primer. Per tant,

$$\mathrm{Gal}(K(\widetilde{p_1}) \dots K(\widetilde{p_r})/H_+) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Com que $p_1 \cdot \ldots \cdot p_r$ és obviament divisible per cadascun dels primers p_i, es tenen inclusions

$$K \subseteq K(\widetilde{p_1}) \dots K(\widetilde{p_r}) \subseteq K(\widetilde{p_1 \cdot \ldots \cdot p_r}).$$

D'altra banda, de la congruència $(*)$ s'obté que m_i divideix n_i, per a tot $i \in \{1, \ldots, r\}$. Per tant, A és isomorf a un quocient de $\mathrm{Gal}(K(\widetilde{p_1 \cdot \ldots \cdot p_r})/K)$ i, pel Lema 1.2.2 (iv), $\mathrm{Gal}(K(\widetilde{p_1 \cdot \ldots \cdot p_r})/\mathbb{Q})$ admet un quocient isomorf a $D_{2.A}$.

Per a concloure només falta observar que els únics primers finits que ramifiquen a $K(\widetilde{p_1 \cdot \ldots \cdot p_r})/\mathbb{Q}$ són $q, p_1, \ldots, p_r$ i tots ells ho fan moderadament, donat que l'ordre d'un grup d'inèrcia en q (resp. p_i) és 2 (resp. n_i, que és un divisor de $p_i - 1$). □

La demostració de la segona desigualtat del Teorema 2.3.1 es simplifica lleugerament triant els primers $q, p_1, \ldots, p_r$ de manera que:

(i) $q \neq 3$ i $q \equiv 3 \pmod 4$,

(ii) $p_i \equiv -1 \pmod{q.m_i}$, per a tot $i \in \{1, \ldots, r\}$.

Convé notar, però, que la demostració donada estableix el següent resultat, més fort que l'enunciat, que generalitza [JY82, Thm. I.2.1].

Teorema 2.3.2. *Per a qualsevol grup diedral generalitzat $D_{2.A}$ i qualsevol primer senar q, existeixen infinits cossos de classes d'anell L de $\mathbb{Q}(\sqrt{q^*})$ tals que:*

(a) $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2.A}$,

(b) en l'extensió $L/\mathbb{Q}$ ramifiquen, com a màxim, $d(D_{2.A})$ primers finits i tots ells ho fan moderadament.

Recordant que $d(D_{2A}) = 1 + d(A)$ i $d(D_{2A}^{ab}) = 1 + r_2(A)$ (Lema 1.2.2), obtenim:

Corol.lari 2.3.3. *Sigui A un grup abelià finit tal que $d(A) = r_2(A)$. Aleshores:*

$$ram^t(D_{2.A}) = d(D_{2.A}) = 1 + r_2(A).$$

Ja hem observat anteriorment que, pel Teorema de Kronecker-Weber, tot grup abelià finit G satisfà la igualtat $ram^t(G) = d(G)$. Per a grups diedrals generalitzats, en canvi, aquesta igualtat no és certa en general. Per exemple, existeixen extensions diedrals generalitzades de $\mathbb{Q}$ ramificades en un únic primer finit i moderadament ramificades. La següent proposició caracteritza aquestes extensions.

Proposició 2.3.4. *Sigui A un grup abelià finit. Aleshores, les condicions següents són equivalents:*

(i) $ram^t(D_{2.A}) = 1$.

(ii) Existeix algun primer $p \neq 2$ tal que A és isomorf a un subgrup de $Cl_+(\mathbb{Q}(\sqrt{p^*}))$, grup de classes estricte de $\mathbb{Q}(\sqrt{p^*})$.

Demostració. La implicació (ii) $\Rightarrow$ (i) és clara donat que, si H_+ denota el cos de classes de Hilbert estricte de $\mathbb{Q}(\sqrt{p^*})$, aleshores l'extensió $H_+/\mathbb{Q}$ és diedral generalitzada, ramificada només en el primer (finit) p i el seu grup de Galois $\mathrm{Gal}(H_+/\mathbb{Q})$ admet un quocient isomorf a $D_{2.A}$.

Per a demostrar (i) $\Rightarrow$ (ii), assumim $ram^t(D_{2.A}) = 1$, és a dir, suposem que existeix una extensió de Galois $L/\mathbb{Q}$ tal que $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2.A}$, p és l'únic primer finit que ramifica a $L/\mathbb{Q}$ i ho fa moderadament.

Per força, L ha de ser un cos de classes d'anell del subcos quadràtic de L fix per A, $K = L^A$ (Proposició 1.2.7). Com que p és l'únic primer finit que ramifica a $L/\mathbb{Q}$ i ho fa moderadament, necessàriament haurà de ser $p \neq 2$, $K = \mathbb{Q}(\sqrt{p^*})$ i $L \subset K(\widetilde{p^m})$, per algun $m \geq 1$.

La Proposició 1.2.8 estableix la igualtat:

$$[K(\widetilde{p^m}) : K] = [H_+ : K].p^n,$$

per a cert natural convenient $n \leq m$. En particular, es té:

$$[K(\widetilde{p^m}) : H_+] = p^n.$$

Sigui $\mathfrak{p}$ l'únic ideal primer de $\mathcal{O}_K$ que divideix p, és a dir, $p\mathcal{O}_K = \mathfrak{p}^2$. El grup d'inèrcia de $K(\widetilde{p^m})/K$ en $\mathfrak{p}$ és precisament $\mathrm{Gal}(K(\widetilde{p^m})/H_+)$ i, per tant, coincideix amb el subgrup de ramificació salvatge (té ordre p^n).

Concloem, doncs, que H_+/K és la màxima subextensió moderadament ramificada de $K(\widetilde{p^m})/K$. Així, $L \subset H_+$ i, tal com volíem, $A \subset Cl_+(K)$. □

Observació 2.3.5. *Del Corol.lari 2.3.3 es dedueix que, si $K/\mathbb{Q}$ és una extensió quadràtica ramificada exactament en s primers finits senars, aleshores el grup de classes estricte de K té 2-rang $r_2(Cl_+(K)) \leq s-1$; en particular, per a qualsevol primer senar p, el grup $Cl_+(\mathbb{Q}(\sqrt{p^*}))$ té ordre senar. Un resultat clàssic de la Teoria dels gèneres de Gauss estableix que, de fet, es té la igualtat $r_2(Cl_+(K)) = s-1$ (cf., per exemple, [Nar90, Thm. 8.8]).*

Si A és un grup abelià finit d'ordre parell, aleshores el Teorema 2.3.1 estableix la desigualtat $ram^t(D_{2.A}) > 1$. Pot passar, però, que $ram(D_{2.A}) = 1$.

Proposició 2.3.6. *Sigui A un grup abelià finit d'ordre parell. Aleshores, les condicions següents són equivalents:*

(i) $ram(D_{2.A}) = 1$,

(ii) *A és un 2-grup cíclic.*

Demostració. Comencem suposant que $ram(D_{2.A}) = 1$. Així, existeix una extensió de Galois $L/\mathbb{Q}$ ramificada en un únic primer p amb grup de Galois

$$\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2.A}.$$

Per la Proposició 1.2.7, L és un cos de classes d'anell del cos quadràtic $K = L^A$.

Pel Teorema de Kronecker-Weber, $D_{2.A}^{ab}$ és un quocient de $(\mathbb{Z}/p^n\mathbb{Z})^*$, per algun natural n. D'altra banda, si r denota el 2-rang de A, aleshores:

$$D_{2.A}^{ab} \cong \mathbb{Z}/2\mathbb{Z} \times \overset{r+1}{\cdots} \times \mathbb{Z}/2\mathbb{Z}.$$

Per hipòtesi, $r \geq 1$ i, per tant, només pot ser $p = 2$ i $r = 1$. Només falta veure, doncs, que A és un 2-grup.

Com que $p = 2$ és l'únic primer finit que ramifica a l'extensió quadràtica $K/\mathbb{Q}$, les úniques possibilitats per a K són $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ i $\mathbb{Q}(i)$. Tots aquests cossos tenen nombre de classes estricte 1 i, per tant, el grau de l'extensió $K(\widetilde{2^m})/K$ és una potència de 2, per a qualsevol m (Proposició 1.2.8). Com que $L \subset K(\widetilde{2^m})$ per algun m, concloem que A és un 2-grup.

Finalment, la implicació (ii) $\Rightarrow$ (i) és conseqüència del fet conegut que els 2-grups que es realitzen com a grups de Galois d'extensions de $\mathbb{Q}$ ramificades només en $p = 2$ (i potser a l'infinit) són exactament aquells que es poden generar per dos elements, amb un d'ells d'ordre 2 (cf. [Mar63] o [Har94, pàg. 59]). Quan A és un 2-grup cíclic, $D_{2.A}$ satisfà obviament aquesta condició. □

Notem que, a la demostració anterior, hem obtingut la implicació (i) $\Rightarrow$ (ii) com a conseqüència del següent resultat.

Proposició 2.3.7. *Sigui A un grup abelià finit d'ordre parell. Sigui $L/\mathbb{Q}$ una extensió de Galois ramificada en un únic primer finit p i amb grup de Galois* $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2.A}$. *Aleshores $p = 2$ i A és un 2-grup cíclic.*

Del Corol.lari 2.3.3 i de la Proposició 2.3.6 obtenim el valor exacte de $ram(D_{2n})$ i $ram^t(D_{2n})$, per a tot natural parell n.

Corol.lari 2.3.8. *Sigui n un natural parell. Aleshores:*

$ram(D_{2n}) = 1$ *i* $ram^t(D_{2n}) = 2$, *si n és una potència de* 2,

$ram(D_{2n}) = ram^t(D_{2n}) = 2$, *altrament.*

2.4 Nombre de primers ramificats i la Hipòtesi (H) de Schinzel

Comencem recordant l'enunciat de l'anomenada Hipòtesi (H) de Schinzel (cf. [SS58] o [Ser94]).

> **Hipòtesi (H) de Schinzel:**
> Siguin $p_1(T), \ldots, p_r(T) \in \mathbb{Z}[T]$ polinomis irreductibles a $\mathbb{Q}[T]$, tots ells amb coeficient principal positiu. Suposem també que, per a cada nombre primer p, existeix algun enter $n_p \in \mathbb{Z}$ tal que p no divideix $p_1(n_p) \cdot \ldots \cdot p_r(n_p)$. Aleshores, existeixen infinits naturals $n \in \mathbb{N}$ tals que $p_1(n), \ldots, p_r(n)$ són tots nombres primers.

Aquesta hipòtesi generalitza el Teorema de Dirichlet dels primers en progressió aritmètica. La seva validesa implicaria, per exemple, una resposta afirmativa a la "conjectura dels primers bessons".

La Hipòtesi (H) de Schinzel ha estat usada per a obtenir resultats (condicionals) relatius a l'obstrucció per a la validesa de principis locals-globals i d'aproximació feble (veure, per exemple, [CT98]).

Els polinomis als quals nosaltres aplicarem aquesta conjectura apareixeran precisament com a discriminants de polinomis i, per tant, obtindrem extensions ramificades en un únic primer. En els següents resultats, només aplicarem la Hipòtesi (H) de Schinzel a un polinomi cada vegada, és a dir, sempre tindrem $r = 1$ amb la notació anterior.

Proposició 2.4.1. *Assumim la validesa de la Hipòtesi (H) de Schinzel. Aleshores, per a tot grup diedral D_{2n} es satisfà la igualtat:*

$$ram^t(D_{2n}) = d(D_{2n}^{ab}).$$

Demostració. Per a n parell, ja hem provat a la secció anterior que es té la igualtat incondicional $ram^t(D_{2n}) = 2$. Per a n senar, cal veure $ram^t(D_{2n}) = 1$.

Sigui $n = {p_1}^{e_1} \cdot \ldots \cdot {p_m}^{e_m}$ un natural senar qualsevol. Veurem que la Hipòtesi (H) de Schinzel implica que, per alguna extensió quadràtica $K/\mathbb{Q}$ ramificada en un únic primer finit, el grup de classes d'ideals de K conté un subgrup isomorf a $\mathbb{Z}/n\mathbb{Z}$. Així, si H_+ denota el cos de classes de Hilbert de K, l'extensió $H_+/\mathbb{Q}$ ramifica en un únic primer finit i el grup de Galois $\mathrm{Gal}(H_+/\mathbb{Q})$ admet un quocient isomorf a D_{2n}. Per tant, $ram^t(D_{2n}) = 1$.

Considerem un primer senar $l \equiv 1 \pmod{n}$ i sigui $x \in \mathbb{Z}$ un enter senar tal que $x \pmod{l}$ és un generador de $(\mathbb{Z}/l\mathbb{Z})^*$. En particular, per a tot $i \in \{1, \ldots, m\}$, x no és una p_i-èsima potència mòdul l. En aquesta situació, un resultat de Yamamoto [Yam70, Prop.1] estableix que, per a qualsevol enter $t \in \mathbb{Z}$ coprimer amb x tal que $x^2 - 4t^n l^n < 0$, el grup de classes d'ideals del cos quadràtic $\mathbb{Q}(\sqrt{x^2 - 4t^n l^n})$ conté algun element d'ordre n.

Considerem el polinomi $p(T) := 4l^n T^n - x^2 \in \mathbb{Z}[T]$.

Com que $(n, n-2) = 1$, el polinomi

$$2^{n-2} p\left(\frac{T}{2l}\right) = T^n - 2^{n-2} x^2$$

és irreductible a $\mathbb{Q}[T]$ i, per tant, $p(T)$ també ho és.

D'altra banda, tenint en compte que $(2l, x) = 1$, és clar que $(p(0), p(1)) = 1$. En particular, donat un nombre primer p qualsevol, p no divideix $p(0)$ o bé p no divideix $p(1)$.

Aplicant la Hipòtesi (H) de Schinzel al polinomi $p(T)$, obtenim l'existència de (infinits) $t \in \mathbb{N}$ tal que $q = p(t)$ és un nombre primer, necessàriament $q \equiv 3 \pmod{4}$. En aquest cas, q és l'únic primer finit que ramifica a l'extensió quadràtica $\mathbb{Q}(\sqrt{-q})/\mathbb{Q}$ i el grup de classes d'ideals de $\mathbb{Q}(\sqrt{-q})$ conté un subgrup isomorf a $\mathbb{Z}/n\mathbb{Z}$, tal com volíem veure. □

Observació 2.4.2. *Tenint en compte el Corol.lari 2.3.8, obtenim el valor exacte de $ram(D_{2n})$ i $ram^t(D_{2n})$, per a tot natural n (sota la hipòtesi (H) de Schinzel):*

$ram(D_{2n}) = 1$ i $ram^t(D_{2n}) = 2$, si n és una potència de 2,

$ram(D_{2n}) = ram^t(D_{2n}) = d(D_{2n}^{ab})$, altrament.

El resultat següent proporciona un altre exemple, sota la Hipòtesi (H) de Schinzel, de realitzacions de grups finits com a grups de Galois d'extensions poc ramificades de $\mathbb{Q}$. Concretament, es tracta de realitzacions trinomials del grup simètric S_n. Aquest tipus de realitzacions es tornaran a considerar en el Capítol 3.

Proposició 2.4.3. *Assumim la validesa de la Hipòtesi (H) de Schinzel. Aleshores, per a tot grup simètric S_n es satisfà la igualtat:*

$$ram(S_n) = ram^t(S_n) = 1.$$

Demostració. Suposem fixat un natural n qualsevol.

Sigui $f(X) \in \mathbb{Z}[X]$ un polinomi mònic de grau n. Tal com recordarem a la Secció 3.2, és conegut que la condició

$$\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$$

es pot garantir imposant la congruència $f(X) \equiv X^n - X - 1 \pmod{N}$, per algun natural N convenient. A més, sempre podem suposar que N és coprimer amb un natural prefixat qualsevol.

En particular, donats enters $t, a, b \in \mathbb{Z}$ qualssevol, el polinomi

$$F(t, X) := X^n - (1 + Nat)X - (1 + Nb) \in \mathbb{Z}[X]$$

té grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(F(t, X)) \cong S_n$.

Sigui T una indeterminada. El discriminant en X del polinomi $F(T, X) \in \mathbb{Z}[T, X]$ és, llevat del signe, el polinomi:

$$p(T) := (-1)^n n^n (1 + Nb)^{n-1} + (n - 1)^{n-1}(1 + NaT)^n \in \mathbb{Z}[T].$$

El Teorema de Dirichlet dels primers en progressió aritmètica ens permet triar b de manera que $q := 1+Nb$ sigui un nombre primer més gran que n. D'aquesta manera, tindrem

$$v_q\left(\frac{n^n(1+Nb)^{n-1}}{(n-1)^{n-1}}\right) = n-1.$$

Per tant,

$$\frac{n^n(1+Nb)^{n-1}}{(n-1)^{n-1}}$$

no és la $p-$èsima potència d'un nombre racional, per a cap primer p que divideixi n. Així, $p(T)$ haurà de ser un polinomi irreductible a $\mathbb{Q}[T]$.

D'altra banda, canviant N (i b) si cal, podem suposar que

$$(N, (-1)^n n^n + (n-1)^{n-1}) = 1$$

i, per tant, $(N, p(0)) = 1$. Això és suficient per a garantir l'existència d'algun enter $a \in \mathbb{Z}$ de manera que $p(T)$ tingui coeficient principal positiu i

$$(p(1), p(0)) = 1.$$

En aquesta situació, la Hipòtesi (H) de Schinzel afirma que, per a infinits naturals t, $p(t)$ és un nombre primer. En conclusió, S_n es realitza com a grup de Galois d'una extensió de $\mathbb{Q}$ ramificada en un únic primer i moderadament ramificada. □

Observació 2.4.4. *En principi, l'argument anterior es pot adaptar per a d'altres grups finits $G \neq S_n$. Convé notar, però, que el fet que un trinomi de $\mathbb{Q}[X]$ tingui grup de Galois isomorf a G pot ser incompatible, per alguns G, amb que l'extensió que defineix sigui poc ramificada. Al Capítol 3 veurem que aquest és el cas per alguns grups alternats A_n, fins i tot quan admetem ramificació salvatge. Per exemple, donat un natural $n \equiv 2, 6 \pmod 8$ i un primer $p \equiv 3 \pmod 4$ que divideix n, tota realització de A_n com a grup de Galois sobre $\mathbb{Q}$ d'un trinomi de grau n ramifica en p (Teorema 3.3.5). Així, considerant només extensions trinomials, és impossible establir una fita (constant) per a $ram(A_n)$ vàlida per a tot n.*

2.5 Sobre una conjectura de Harbater

Motivat per raons geomètriques i per l'analogia entre cossos de nombres i cossos de funcions, David Harbater proposa la següent conjectura.

> **Conjectura** [Har94]:
> Existeix una constant C tal que, per a qualsevol natural n lliure de quadrats, si G és un grup finit que es realitza com a grup de Galois d'alguna extensió de $\mathbb{Q}$ ramificada només en primers que divideixen n i moderadament ramificada, aleshores $d(G) \leq \ln(n) + C$.

Si G és un grup abelià finit, la "validesa de la conjectura per a G"(amb $C = 1$) és conseqüència directa del Teorema de Kronecker-Weber. D'altra banda, la desigualtat conjecturada és trivialment certa (amb $C = 3$ i, de fet, també amb $C = 2$) quan G és un grup finit quasi-simple (per exemple, simple no abelià) donat que, per a aquests grups, sempre es té $d(G) \leq 3$ (cf. [VL95]). Remarquem també que, pel Teorema de la base de Burnside, la validesa de la desigualtat per a tot grup nilpotent finit G (també amb $C = 1$) es dedueix del cas abelià. Aquest darrer fet admet la següent generalització.

Proposició 2.5.1. *Existeix una constant C que satisfà la conclusió de la conjectura anterior per a qualsevol grup G extensió de $\mathbb{Z}/2\mathbb{Z}$ per un grup nilpotent finit N, és a dir, tal que existeix una successió exacta*

$$1 \to N \to G \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Demostració. Suposem que $L/\mathbb{Q}$ és una extensió de Galois ramificada només en els primers $\{p_1, \ldots, p_m\}$, moderadament ramificada i amb grup de Galois

$$G \cong \mathrm{Gal}(L/\mathbb{Q}).$$

Cal provar la desigualtat

$$d(G) \leq ln(p_1 \cdot \ldots \cdot p_m) + C,$$

amb C constant (independent de G i de $p_1, \ldots, p_m$).

Per hipòtesi sobre G, tenim una cadena de cossos

$$\mathbb{Q} \subset K \subset K_1 \subset L,$$

on $K/\mathbb{Q}$, L/K i K_1/K són extensions de Galois amb grups de Galois

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\,, \quad \mathrm{Gal}(L/K) \cong N \quad \text{i} \quad \mathrm{Gal}(K_1/K) \cong N^{ab}.$$

Pel Teorema de la base de Burnside, $d(N) = d(N^{ab})$ i, per tant,

$$d(G) \leq d(N) + 1 = d(\mathrm{Gal}(K_1/K)) + 1.$$

Sigui H_+/K la màxima subextensió de K_1/K no ramificada en cap ideal primer. Així, els subgrups d'inèrcia de $\mathrm{Gal}(K_1/K)$ generen $\mathrm{Gal}(K_1/H_+)$. Com que $[K : \mathbb{Q}] = 2$ i a $L/\mathbb{Q}$ només ramifiquen m primers, com a màxim hi ha $s := 2m - 1$ ideals primers $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ de $\mathcal{O}_K$ que ramifiquen a K_1/K (com a mínim un dels p_i ha de ramificar a K). Per hipòtesi, l'extensió K_1/K és abeliana i, per tant, hi ha un únic subgrup d'inèrcia de $\mathrm{Gal}(K_1/K)$ en cadascun dels primers $\mathfrak{p}_i$. A més, aquests grups d'inèrcia han de ser cíclics, donat que estem suposant que no hi ha ramificació salvatge. En resum,

$$d(\mathrm{Gal}(K_1/H_+)) \leq 2m - 1.$$

Tenint en compte que $\mathrm{Gal}(H_+/K)$ és un quocient del grup de classes d'ideals estricte $Cl_+(K)$, obtenim:

$$d(G) \leq d(\mathrm{Gal}(K_1/H_+)) + d(\mathrm{Gal}(H_+/K)) + 1 \leq d(Cl_+(K)) + 2m.$$

D'altra banda, la Teoria dels gèneres de Gauss estableix que el 2-rang de $Cl_+(K)$ és $m - 1$ (cf., per exemple, [Nar90, Thm. 8.8]). També és conegut que (cf., per exemple, [Nar90, Thm. 4.4, Prop. 8.7])

$$h_+(K) \leq p_1 \cdot \ldots \cdot p_m.$$

Donat un primer p, denotem per $r_p(Cl_+(K))$ el $p-$rang de $Cl_+(K)$. Notem que, per a $p \geq 3$, es té

$$r_p \leq \log_p(h_+(K)) \leq \log_3(h_+(K)).$$

Com que $d(Cl_+(K)) = \max_p\{r_p(Cl_+(K))\}$, obtenim:

$$d(Cl_+(K)) \leq \log_3(p_1 \cdot \ldots \cdot p_m).$$

D'aquesta manera, es té:

$$d(G) \leq \sum_{1 \leq i \leq m} (2 + \log_3(p_i)).$$

Per a concloure només cal definir, per exemple:

$$C := \sum_p (2 + \log_3(p) - \ln(p)),$$

on el sumatori recorre els primers p tals que $2 + \log_3(p) - \ln(p) \geq 0$. □

Capítol 3

Realitzacions trinomials de grups alternats sobre $\mathbb{Q}$ amb condicions de ramificació en els primers d'un conjunt finit S

3.1 Introducció

L'objectiu d'aquest capítol és estudiar l'existència d'extensions trinomials de $\mathbb{Q}$ amb condicions de ramificació prefixades en un conjunt finit de primers. Essencialment, ens interessem per les extensions amb grup de Galois alternat i prioritzem l'obtenció d'extensions moderadament ramificades.

És conegut que el discriminant d'un trinomi $f(X) = X^n + aX^k + b$ amb $(k, n) = 1$ és (cf. [Swa62, Thm.2]):

$$D(f(X)) = (-1)^{\frac{n(n-1)}{2}} b^{k-1} \left(n^n b^{n-k} + (-1)^{n-1}(n-k)^{n-k} k^k a^n\right).$$

A partir d'aquesta expressió, i tenint en compte la hipòtesi $(k, n) = 1$, és clar que sempre podem trobar coeficients a, $b \in \mathbb{Z}$ de manera que el discriminant

$D(f(X))$ no sigui divisible per cap primer d'un conjunt finit S prefixat. Triant $f(X)$ d'aquesta manera, els primers de S no ramifiquen a l'extensió de Galois $\mathbb{Q}_f/\mathbb{Q}$, on $\mathbb{Q}_f$ denota el cos de descomposició sobre $\mathbb{Q}$ de $f(X)$.

Per a $n \geq 5$, un trinomi $f(X) = X^n + aX^k + b$ sense arrels múltiples sempre té alguna no real i, per tant, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és ramificada en el primer de l'infinit. Aquest és el motiu pel qual, a diferència del capítol següent, en aquest capítol mai demanarem que $p = \infty$ no ramifiqui.

Comencem la Secció 3.2 observant que, per a tot n, existeixen trinomis $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$ i discriminant no divisible pels primers d'un conjunt finit fixat qualsevol. Això deixa de ser cert quan demanem $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \subseteq A_n$. El resultat principal de la Secció 3.2 és la caracterització de les ternes n, k, S, on S és un conjunt finit de primers, tals que existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no divisible per cap primer de S. De fet, la condició que obtenim només depèn de n, k i del conjunt de primers $p \in S$ tals que $p \leq n$.

A la Secció 3.3 ens interessem per l'obtenció d'extensions trinomials de $\mathbb{Q}$, amb grup de Galois A_n, no ramificades en els primers d'un conjunt finit prefixat. Si θ és una arrel d'un polinomi irreductible i mònic $f(X) \in \mathbb{Z}[X]$, aleshores es pot recórrer a resultats clàssics de Kummer, Dedekind, Hensel, Bauer, Öre, ... per a estudiar la ramificació en l'extensió $\mathbb{Q}(\theta)/\mathbb{Q}$ dels primers que divideixen el discriminant de $f(X)$. En aquest sentit, a [LNV84] s'obtenen resultats quan $f(X)$ és un trinomi. Nosaltres utilitzem la tècnica dels polígons de Newton per a caracteritzar, per a un natural n qualsevol, l'existència d'algun trinomi $X^n + aX^k + b \in \mathbb{Z}[X]$ amb grup de Galois A_n sobre $\mathbb{Q}$ i cos de descomposició no ramificat en els primers d'un conjunt finit prefixat.

La Secció 3.4 està dedicada a la ramificació moderada. Aprofitant els resultats de les seccions anteriors, caracteritzem els n per als quals existeix algun

trinomi mònic $f(X) \in \mathbb{Z}[X]$ de grau n tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és moderadament ramificada i té grup de Galois isomorf a A_n. En particular, obtenim una resposta afirmativa, per a infinits A_n, al problema de Birch sobre la possibilitat de realitzar tot grup finit com a grup de Galois d'alguna extensió moderadament ramificada de $\mathbb{Q}$. Més concretament, demostrem que aquest és el cas per a tot n senar.

La caracterització obtinguda també fa evident que, per a infinits A_n, no es pot respondre al problema 3 de la Introducció considerant només extensions trinomials. Provem, per exemple, que $p = 2$ ramifica salvatgement sempre que $n \equiv 4 \pmod 8$. Aquest resultat proporciona exemples d'extensions regulars de $\mathbb{Q}(T)$, amb grup de Galois A_n, que no admeten cap especialització racional moderadament ramificada. Al Capítol 5 trobarem altres exemples d'aquest mateix fenomen.

3.2 Trinomis amb discriminant coprimer amb els primers de S

3.2.1 Trinomis amb grup de Galois S_n

Proposició 3.2.1. *Sigui S un conjunt finit de primers qualsevol. Per a tot natural n existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ tal que:*

(a) $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$.

(b) El discriminant $D(f(X))$ no és divisible per cap $p \in S$. En particular, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en els primers de S.

Demostració. És conegut (cf., per exemple, [Ser92b, 4.4]) que, per a tot n, el grup de Galois sobre $\mathbb{Q}$ del polinomi $X^n - X - 1$ és

$$\mathrm{Gal}_{\mathbb{Q}}(X^n - X - 1) \cong S_n.$$

Per tant, si T_1, T_2 denoten indeterminades, necessàriament es té:

$$\mathrm{Gal}_{\mathbb{Q}(T_1,T_2)}(X^n + T_1X + T_2) \cong S_n.$$

Pel Teorema d'Irreductibilitat de Hilbert (veure Proposició 1.3.3), donats racionals $a_0, b_0 \in \mathbb{Q}$ qualssevol, sempre existeixen coeficients $a, b \in \mathbb{Q}$ de manera que el trinomi

$$f(X) = X^n + aX + b$$

té grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$ i, per a tot $p \in S$, satisfà la congruència

$$f(X) \equiv X^n + a_0X + b_0 \pmod{p}.$$

Agafant, per exemple, $a_0 = 1$ i

$$b_0 \equiv \begin{cases} 0 \pmod{p}, & \text{si } p \nmid n-1 \\ 1 \pmod{p}, & \text{si } p \mid n-1, \end{cases}$$

garantim que p no divideixi el discriminant $D(f(X))$, per a tot $p \in S$.

Canviant $f(X)$ per $M^n f(X/M)$, amb $M \in \mathbb{Z}$ convenient, podem suposar $f(X) \in \mathbb{Z}[X]$. □

Corol.lari 3.2.2. *Per a tot natural n, el grup simètric S_n es realitza com a grup de Galois d'una extensió moderadament ramificada de $\mathbb{Q}$ obtinguda com a cos de descomposició d'un trinomi de grau n.*

Observació 3.2.3. *La Proposició 3.2.1 també es pot demostrar observant que les condicions (a), (b) per a un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ queden garantides a partir d'un nombre finit de condicions locals en els coeficients a, b:*

- *mòdul els primers de S, per a la condició (b),*
- *mòdul els primers d'un conjunt finit convenient que podem suposar disjunt amb S, per a la condició (a).*

De fet, pel Teorema de Densitat de Txebotarev, la classe de conjugació de qualsevol permutació σ de S_n apareix com a element de Frobenius en el grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(X^n-X-1) \cong S_n$*, en infinits primers. A més, si* $p \nmid D(X^n-X-1)$ *és un d'aquests primers, aleshores el tipus de descomposició de σ en cicles disjunts coincideix amb el tipus de factorització de $X^n - X - 1$ mòdul p. Així, podem triar un natural N no divisible per cap primer de S de manera que, per a tot polinomi mònic $f(X) \in \mathbb{Z}[X]$ tal que $f(X) \equiv X^n - X - 1 \pmod{N}$, el grup de Galois* $\mathrm{Gal}_{\mathbb{Q}}(f(X))$ *és isomorf a un subgrup de S_n que talla totes les classes de conjugació de S_n. Per un resultat de Jordan, això només és possible si* $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$ *(cf., per exemple, [Ser92b, Lemma 4.6.1]).*

Notem que, en l'observació anterior, no cal suposar que $f(X)$ sigui un trinomi. De fet, l'única condició global sobre $f(X)$ que hem usat és que el seu grau sigui n i, per tant, $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \subseteq S_n$.

Si volem obtenir $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong G \subsetneq S_n$, caldrà imposar també alguna condició global sobre els coeficients a, b que garanteixi $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \subseteq G$. Això es pot fer, per exemple, demanant que $f(X)$ s'obtingui per especialització d'un polinomi $f(T, X) \in \mathbb{Q}(T)[X]$ amb grup de Galois $\mathrm{Gal}_{\mathbb{Q}(T)}(f(T, X)) \cong G$.

Quan $G = A_n$, caldrà exigir que el discriminant de $f(X)$ sigui un quadrat a $\mathbb{Q}$; el fet de treballar amb trinomis simplifica l'estudi d'aquesta condició.

3.2.2 Trinomis amb discriminant quadrat

Que el discriminant d'un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ sigui un quadrat a $\mathbb{Z}$ pot ser incompatible amb condicions locals del tipus $p \nmid D(f(X))$, per a certs primers p. En el resultat següent, caracteritzem aquestes ternes n, k, p.

Denotarem per $\left(\frac{u}{v}\right)$ el símbol de Jacobi de dos enters $u, v \in \mathbb{Z}$, amb v senar.

Proposició 3.2.4. *Siguin $k < n$ dos naturals tals que $(n, k) = 1$. Per a un primer p, són equivalents:*

(i) *Existeix un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no divisible per p.*

(ii) *Si n és parell i p és senar, aleshores $v_p(n) = 0$ o bé $\left(\frac{-1}{p}\right)^{n/2} = 1$.*

Si n és parell i $p = 2$, aleshores $(-1)^{n/2}(1 - kn) \equiv 1 \pmod 8$.

Si n és senar i p és senar, aleshores $v_p(k(n-k)) = 0$ o bé $\left(\frac{p}{n}\right) = 1$.

Si n és senar i $p = 2$, aleshores $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 8$ o bé $(-1)^{\frac{n-1}{2}} n \equiv 5 \pmod 8$ i $k(n-k) = 2(n-2)$.

Demostració.

Assumim, primer, que es satisfà la condició (i). Si p és senar, haurà de ser $\left(\frac{D(f(X))}{p}\right) = 1$. Quan $p = 2$, tindrem $D(f(X)) \equiv 1 \pmod 8$.

Sabem que el discriminant d'un trinomi $f(X) = X^n + aX^k + b$ amb $(k, n) = 1$ és

$$D(f(X)) = (-1)^{\frac{n(n-1)}{2}} b^{k-1} \left(n^n b^{n-k} + (-1)^{n-1}(n-k)^{n-k} k^k a^n\right).$$

Suposem primer que n és parell. Si p és un primer senar que divideix n i que no divideix $D(f(X))$, aleshores:

$$\left(\frac{D(f(X))}{p}\right) = \left(\frac{(-1)^{\frac{n}{2}} k^n a^n b^{k-1}}{p}\right) = \left(\frac{-1}{p}\right)^{n/2}.$$

Si $p = 2$, a i k hauran de ser senars i obtenim $(n > 2)$:

$$D(f(X)) \equiv (-1)^{n/2}(1 - kn) \pmod 8.$$

Si n és senar i p és un primer que divideix $k(n-k)$ i que no divideix $D(f(X))$, de la llei de reciprocitat quadràtica obtenim:

$$\left(\frac{D(f(X))}{p}\right) = \left(\frac{(-1)^{\frac{n-1}{2}} n^n b^{n-1}}{p}\right) = \left(\frac{(-1)^{\frac{n-1}{2}} n}{p}\right) = \left(\frac{p}{n}\right).$$

Finalment, quan n és senar i $p = 2$, b ha de ser senar i, com que $v_2(k^k(n-k)^{n-k}) \geq 2$, obtenim:

$$D(f(X)) \equiv (-1)^{\frac{n-1}{2}} n \pmod 4.$$

A més, la congruència $k^k(n-k)^{n-k} \equiv 4 \pmod 8$ només es dóna si $k=2$ o bé $n-k=2$.

Assumim, ara, que es satisfà la condició (ii).

Suposem primer que n és parell i considerem naturals r, $s \in \mathbb{N}$ tals que

$$s(n-k) - rn = 1\,, \quad 0 < s < n \quad \text{i} \quad 0 \leq r < n-k.$$

Expressem $n = m.p^h$, amb $h = v_p(n)$. En particular, $(m,p) = 1$.

El discriminant d'un trinomi de la forma $f(X) = X^n + aX^k + b$ amb $a = mt^r$ i $b = t^s$ és:

$$D(f(X)) = t^{s(k-1)+rn} m^n \left((-1)^{n/2}(k-n)^{n-k}k^k + (-1)^{n/2}p^{hn}t\right).$$

Per als primers p que divideixen n, la hipòtesi (ii) garanteix precisament que l'equació

$$Y^2 - \left((-1)^{n/2}(k-n)^{n-k}k^k\right) \equiv 0 \pmod{p^{hn}}$$

admet alguna solució entera.

Com que p no divideix $(k-n)^{n-k}k^k$ (i $n > 2$), existeix algun $t \in \mathbb{Z}$ tal que $D(f(X))$ és un quadrat a $\mathbb{Z}$ no divisible per p.

El resultat anàleg quan p no divideix n és clar donat que, en aquest cas, $h = 0$ i $p^{hn} = 1$.

En el cas n senar, considerem naturals r, $s \in \mathbb{N}$ tals que

$$rn - s(n-k) = 1\,, \quad 0 < s < n \quad \text{i} \quad 0 < r \leq n-k.$$

Expressem $(n-k)^{n-k}k^k = mp^h$, on $h = v_p((n-k)^{n-k}k^k)$. Per tant, $(m,p) = 1$.

Prenent $a = mp^h t^r$ i $b = m^{n+1}t^s$, el discriminant d'un trinomi de la forma $f(X) = X^n + aX^k + b$ és

$$D(f(X)) = t^{s(n-1)} m^{(n+1)k} \left((-1)^{\frac{n-1}{2}} n^n m^{(n+1)(n-k-1)} + (-1)^{\frac{n-1}{2}} p^{h(n+1)} t\right).$$

De la hipòtesi (ii) s'obté que, si p és un primer que divideix $k(n-k)$, aleshores l'equació

$$Y^2 - \left((-1)^{\frac{n-1}{2}} n^n m^{(n+1)(n-k-1)}\right) \equiv 0 \pmod{p^n}$$

té alguna solució entera.

Com que p no divideix $n^n m^{(n+1)(n-k-1)}$ (i $n+1>2$), existeix algun $t \in \mathbb{Z}$ tal que $D(f(X))$ és un quadrat a $\mathbb{Z}$ no divisible per p.

La mateixa conclusió és obviament certa quan p no divideix $k(n-k)$. □

És conegut que els trinomis del tipus $f(X) = X^n + aX^k + b$ es poden classificar mitjançant el paràmetre $\frac{b^{n-k}}{a^n}$. Concretament, quan $(n,k)=1$ existeixen naturals s, r satisfent $s(n-k) - rn = 1$ i es té:

$$\left(\frac{b^r}{a^s}\right)^n f\left(\frac{a^s}{b^r}X\right) = X^n + \left(\frac{b^{n-k}}{a^n}\right)^r X^k + \left(\frac{b^{n-k}}{a^n}\right)^s.$$

Així, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ es pot obtenir per especialització (en $T = \frac{b^{n-k}}{a^n}$) de l'extensió $L_T/\mathbb{Q}(T)$, on L_T és el cos de descomposició sobre $\mathbb{Q}(T)$ del trinomi

$$f(T,X) := X^n + T^r X^k + T^s \in \mathbb{Q}(T)[X].$$

Denotem per $D_X(f(T,X))$ el discriminant de $f(T,X)$ com a polinomi en X.

Com que $D_X(f(T,X))$ és, a menys de quadrats de $\mathbb{Q}(T)$, un polinomi de grau 1 de $\mathbb{Q}[T]$ o $\mathbb{Q}[1/T]$, l'extensió $\mathbb{Q}(T)(\sqrt{D_X(f(T,X))})/\mathbb{Q}$ és racional. És a dir, el cos $\mathbb{Q}(T)(\sqrt{D_X(f(T,X))})$ és purament transcendent sobre $\mathbb{Q}$. Es té, doncs, una parametrització de les extensions de $\mathbb{Q}$ que s'obtenen com a cossos de descomposició d'algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Q}[X]$ amb discriminant quadrat a $\mathbb{Q}$. Tenint en compte que el trinomi $f(T,X)$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ amb grup de Galois S_n, s'obté (cf., per exemple, [HS01, Prop.1, Prop.2]):

Proposició 3.2.5. *Siguin $k < n$ dos naturals amb $(k,n) = 1$. Considerem naturals r, $s \in \mathbb{N}$ tals que $s(n-k) - rn = 1$, $0 < s < n$ i $0 \leq r < n-k$. Aleshores, existeix $a(T) \in \mathbb{Q}(T)$ tal que:*

(a) Els coeficients de qualsevol trinomi $X^n+aX^k+b \in \mathbb{Q}[X]$ amb discriminant quadrat a $\mathbb{Q}$ es poden expressar com $a = a(t)^r\mu^{n-k}$ i $b = a(t)^s\mu^n$, per a certs t, $\mu \in \mathbb{Q}$.

(b) El trinomi $X^n + a(T)^r X^k + a(T)^s \in \mathbb{Q}(T)[X]$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ amb grup de Galois isomorf a A_n.

D'aquesta manera, per a estudiar l'existència d'algun trinomi de $\mathbb{Q}[X]$ amb grup de Galois alternat sobre $\mathbb{Q}$ i amb un comportament prefixat en els primers d'un conjunt finit, serà suficient demanar que el discriminant del trinomi sigui un quadrat a $\mathbb{Q}$.

Proposició 3.2.6. *Siguin $k < n$ dos naturals amb $(k, n) = 1$. Per a qualsevol conjunt finit de primers S, són equivalents:*

(i) Existeix un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong A_n$ i discriminant $D(f(X))$ no divisible per cap primer de S.

(ii) Per a cada primer $p \in S$, existeix un trinomi $X^n + a_pX^k + b_p \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no divisible per p.

Demostració. La implicació (i) $\Rightarrow$ (ii) és obvia.

Suposem que es satisfà la condició (ii). Per la Proposició anterior, per a cada $p \in S$ existeixen racionals $t_p, \mu_p \in \mathbb{Q}$ tals que:

$$a_p = a(t_p)^r {\mu_p}^{n-k} \quad \text{i} \quad b_p = a(t_p)^s {\mu_p}^n,$$

amb $r, s \in \mathbb{N}$ i $a(T) \in \mathbb{Q}(T)$ com a la Proposició 3.2.5.

Suposem que T_1, T_2 són indeterminades i considerem el polinomi

$$f(T_1, T_2, X) := X^n + a(T_1)^r T_2^{n-k} X^k + a(T_1)^s {T_2}^n \in \mathbb{Q}(T_1, T_2)[X].$$

Notem que la Proposició 3.2.5 estableix que:

$$\mathrm{Gal}_{\mathbb{Q}(T_1,T_2)}(f(T_1, T_2, X)) = \mathrm{Gal}_{\mathbb{Q}(T_1,T_2)}(f(T_1, 1, X)) \cong A_n.$$

Si $t_1, t_2 \in \mathbb{Q}$ són racionals prou propers p-àdicament a t_p, μ_p, per a tot $p \in S$, aleshores es satisfà la congruència

$$f(t_1, t_2, X) \equiv X^n + a_p X^k + b_p \pmod{p},$$

per a tot primer $p \in S$. Per força, els coeficients de $f(t_1, t_2, X) \in \mathbb{Q}[X]$ tenen tots valoració p-àdica positiva.

Pel Teorema d'Irreductibilitat de Hilbert (veure Proposició 1.3.3), existeixen $t_1, t_2 \in \mathbb{Q}$ d'aquesta manera tals que, a més, el trinomi $f(t_1, t_2, X)$ té grup de Galois

$$\mathrm{Gal}_{\mathbb{Q}}(f(t_1, t_2, X)) \cong A_n.$$

Triant un enter $M \equiv 1 \pmod{\prod_{p \in S} p}$ de manera que el trinomi $f(X) := M^n f(t_1, t_2, X/M)$ tingui coeficients enters, aleshores $f(X)$ satisfà totes les condicions desitjades. □

De la Proposició 3.2.4 es dedueix que, per alguns n, existeix un conjunt finit S_0 de primers "dolents"en el sentit que, si el discriminant d'un trinomi $f(X) \in \mathbb{Q}[X]$ de grau n és un quadrat a $\mathbb{Z}$, aleshores $D(f(X))$ és divisible per tots els primers de S_0. En el següent resultat caracteritzem els n amb aquesta propietat.

Teorema 3.2.7. *Per a un natural n, són equivalents:*

(i) *Per a qualsevol conjunt finit de primers S, existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ tal que $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong A_n$ i $D(f(X))$ no és divisible per cap primer de S.*

(ii) *Per a qualsevol conjunt finit de primers S, existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ tal que $D(f(X))$ és un quadrat a $\mathbb{Z}$ no divisible per cap primer de S.*

(iii) *n satisfà alguna de les condicions següents:*

$$n \equiv 0,\ 1 \pmod{8}$$

$$n \equiv 2 \pmod 8 \text{ } i \text{ } p \equiv 1 \pmod 4, \textit{ per a tot primer senar } p \mid n,$$

$$n \equiv 3 \pmod 8 \text{ } i \text{ } p \equiv 1, 3 \pmod 8, \textit{ per a tot primer } p \mid n-2.$$

Demostració. La implicació (i) $\Rightarrow$ (ii) és clara.

Demostrem (ii) $\Rightarrow$ (iii). Podem suposar $n \geq 3$. Considerem un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ satisfent la hipòtesi (ii), respecte el conjunt S de primers menors o iguals que n. Per força haurà de ser $(k, n) = 1$, donat que qualsevol primer que divideixi (k, n) divideix també $D(f(X))$.

Cas n parell. Per la Proposició 3.2.4, haurà de ser:

(a) $\left(\frac{-1}{p}\right)^{\frac{n}{2}} = 1$, per a qualsevol primer senar p dividint n,

(b) $(-1)^{\frac{n}{2}}(1 - nk) \equiv 1 \pmod 8$.

La condició (a) només és possible si:

$$\begin{cases} n \equiv 0, 4 \pmod 8 \\ n \equiv 2, 6 \pmod 8 \text{ i } p \equiv 1 \pmod 4 \end{cases}$$

Per a $n \equiv 6 \pmod 8$, necessàriament algun primer $p \mid n$ ha de satisfer $p \equiv 3 \pmod 4$. Quan $n \equiv 4 \pmod 8$, la condició (b) no es satisfà.

En conclusió, les úniques possibilitats per a n són les considerades a (iii).

Cas n senar. Per la Proposició 3.2.4, haurà de ser:

(a) $\left(\frac{p}{n}\right) = 1$, per a qualsevol primer senar p dividint $k(n-k)$,

(b) si $n \equiv 3 \pmod 8$ o $n \equiv 5 \pmod 8$, aleshores $k(n-k) = 2(n-2)$.

Si notem $r = v_2(k(n-k))$, de la condició (a) obtenim:

$$1 = \left(\frac{k(n-k)}{n}\right)\left(\frac{2^r}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right)^r = (-1)^{\frac{n-1}{2} + r\frac{n^2-1}{8}}.$$

Aquesta igualtat es satisfà exactament en els casos:

$$\begin{cases} n \equiv 1 \pmod 8 \\ n \equiv 3 \pmod 8 \text{ i } r \text{ és senar} \\ n \equiv 5 \pmod 8 \text{ i } r \text{ és parell} \end{cases}$$

Per la condició (b), el cas $n \equiv 5 \pmod 8$ no es pot donar ($r = 1$); el cas $n \equiv 3 \pmod 8$ només és possible quan, per a tot primer $p \mid n-2$, es té $1 = \left(\frac{p}{n}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{2}{p}\right)$, és a dir, $p \equiv 1, 3 \pmod 8$.

En conclusió, les úniques possibilitats per a n són les considerades a (iii).

Per acabar, demostrem (iii) $\Rightarrow$ (i).

Suposem que n és un natural satisfent alguna de les condicions de la hipòtesi (iii). Fixem $k = n-2$ si $n \equiv 3 \pmod 8$ i $k = n-1$ en la resta de casos. Així, per a qualsevol primer p, la condició (ii) de la Proposició 3.2.4 es satisfà i, per tant, existeixen enters a_p, b_p de manera que el trinomi $X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ té discriminant quadrat a $\mathbb{Z}$ no divisible per p. Això acaba la demostració, gràcies a la Proposició 3.2.6. □

Per aplicacions successives del resultat anterior a conjunts S ben triats o, alternativament, de la regularitat enunciada a la Proposició 3.2.5, s'obté:

Corol.lari 3.2.8. *Sigui n un natural satisfent alguna de les hipòtesis de la condició (iii) de la Proposició 3.2.7. Sigui S un conjunt finit de primers qualsevol. Aleshores, existeixen infinits trinomis mònics a $\mathbb{Z}[X]$ amb grup de Galois A_n sobre $\mathbb{Q}$, discriminant no divisible per cap primer de S i de manera que els seus cossos de descomposició sobre $\mathbb{Q}$ defineixen infinites extensions linealment disjuntes dos a dos.*

Observació 3.2.9. *De la demostració de la Proposició 3.2.7 s'obté també que les afirmacions (i), (ii) i (iii) són equivalents a:*

(ii)' per al conjunt S dels primers menors o iguals que n, existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ tal que $D(f(X))$ és un quadrat a $\mathbb{Z}$ no divisible per cap primer de S.

Observació 3.2.10. *La implicació (iii) ⇒ (i) de la Proposició 3.2.7 també es pot demostrar raonant com a l'Observació 3.2.3. Només cal obtenir condicions locals addicionals sobre $X^n + aX^k + b$, compatibles amb tenir discriminant quadrat, que garanteixin $A_n \subseteq \mathrm{Gal}_{\mathbb{Q}}(X^n + aX^k + b)$. Si usem el fet que $\mathrm{Gal}_{\mathbb{Q}}(X^n - X - 1) \cong S_n$, les condicions locals seran del tipus $a \equiv b \equiv -1 \pmod{N}$, on N és un enter convenient coprimer amb $\prod_{p\in S} p$.*

Notem que la condició $A_n \subseteq G_{\mathbb{Q}}(X^n + aX^k + b)$ es pot imposar amb poques condicions locals, és a dir, amb N producte de pocs primers. Per exemple (cf. [Col87]), si q és un primer tal que $\frac{n}{2} < q < n-2$ (per a $n \geq 8$ sempre existeix; cf. [Tsc52]) i $G \subseteq S_n$ és un subgrup transitiu que conté un q-cicle, aleshores G és primitiu i $A_n \subseteq G$ per un Teorema de Jordan (cf. [Hal59, 5.6.2, 5.7.2]).

3.3 Extensions trinomials no ramificades en S

L'objectiu principal d'aquesta secció és caracteritzar, per a un conjunt finit de primers S qualsevol, l'existència de trinomis mònics $f(X) \in \mathbb{Z}[X]$ amb grup de Galois alternat sobre $\mathbb{Q}$ i cos de descomposició no ramificat en S. És a dir, voldrem que els primers de S no divideixin el discriminant de l'extensió $\mathbb{Q}_f/\mathbb{Q}$ però, a diferència de la secció anterior, admetrem que puguin dividir el discriminant de $f(X)$.

3.3.1 Primers ramificats en extensions trinomials

Els dos resultats següents garanteixen la ramificació de certs primers en extensions trinomials de $\mathbb{Q}$.

Proposició 3.3.1. *Sigui $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ un trinomi separable amb $b \neq 0$ i $(k, n) = 1$.*

(a) *Si p és un primer senar que divideix n i $v_p(a^n) \geq v_p(n^n b^{n-k})$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és ramificada en p.*

Si, a més, $v_p(n) > 1$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada en p.

(b) *Si $v_2(n) > 1$ i $v_2(a^n) \geq v_2(n^n b^{n-k}) - 2$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada en $p = 2$.*

Demostració. Sigui p un primer que divideix n. Si p satisfà les hipòtesis de l'enunciat, aleshores en qualsevol cas (p senar o $p = 2$) es té $v_p(a^n) \geq v_p(b^{n-k})$. Canviant, si cal, $f(X)$ per $\frac{1}{M^n} f(MX)$ amb M convenient, podem suposar i suposem:

$$v_p(b) < n.$$

Notem $d = (n, v_p(b))$ i expressem $v_p(b) = dh$, $n = de$. Si $v_p(e) > 0$, aleshores el polígon de Newton de $f(X)$ té un costat de pendent $-\frac{h}{e}$. Pel Corol.lari 1.4.3, p ramifica salvatgement a $\mathbb{Q}_f/\mathbb{Q}$. Suposem, doncs, que $v_p(e) = 0$, és a dir, $v_p(v_p(b)) \geq v_p(n)$ (admetem $v_p(b) = 0$).

Notem $r = v_p(n)$ i considerem enters n' i b' (no divisibles per p) tals que $n = n'p^r$ i $b = b'p^{dh}$.

Siguin $\theta, \eta \in \overline{\mathbb{Q}_p}$ arrels de $X^e - p$ i $X^{n'} + b'$, respectivament. Observem que l'extensió $\mathbb{Q}_p(\eta)/\mathbb{Q}_p$ és no ramificada i l'extensió $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$ és moderadament ramificada, donat que és totalment ramificada de grau e (per ser $X^e - p$ un polinomi p-Eisenstein).

Considerem el polinomi de $\mathbb{Q}_p(\theta, \eta)[X]$ següent:

$$g(X) := \frac{1}{\theta^{hn}} f(\theta^h(X + \eta)) = (X + \eta)^n + \frac{a}{\theta^{h(n-k)}}(X + \eta)^k + b' = \sum_{0 \leq i \leq n} c_i X^i.$$

Els coeficients c_i de $g(X)$ són:

$$c_0 = \eta^n + \tfrac{a}{\theta^{h(n-k)}}\eta^k + b' = \tfrac{a}{\theta^{h(n-k)}}\eta^k + b' - (b')^{p^r},$$

$$c_i = \begin{pmatrix} n \\ i \end{pmatrix} \eta^{n-i} + \tfrac{a}{\theta^{h(n-k)}} \begin{pmatrix} k \\ i \end{pmatrix} \eta^{k-i}, \text{ per a } 1 \leq i \leq k,$$

$$c_i = \left(\begin{array}{c} n \\ i \end{array} \right) \eta^{n-i}, \text{ per a } i > k.$$

Cas $r = v_p(n) > 1$.

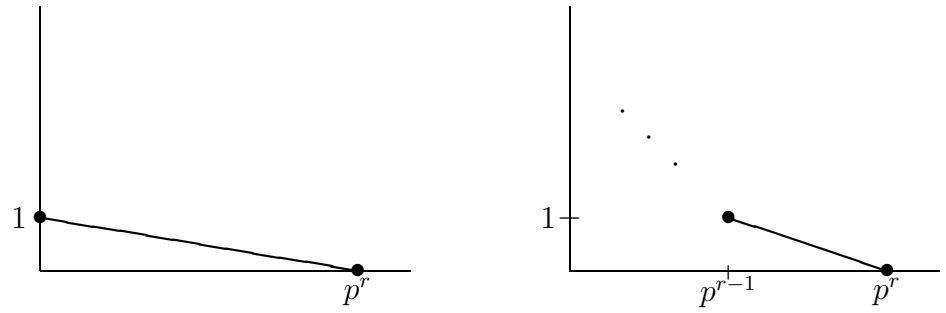
Com que haurà de ser $v_p(a^n) \equiv v_p(n^n b^{n-k}) \pmod{p^2}$, també en el cas $p = 2$ tindrem $v_p(a^n) \geq v_p(n^n b^{n-k})$. Així, obtenim:

$$v_p\left(\frac{a}{\theta^{h(n-k)}}\right) = v_p(a) - \frac{n-k}{n} v_p(b) \geq r.$$

Aquesta desigualtat força els coeficients c_i de $g(X)$ a satisfer:

1. $v_p(c_0) = 1$ o bé $v_p(c_0) \geq 2$ i, per tant, $\dfrac{v_p(c_0)}{p^r} \geq \dfrac{1}{p^r - p^{r-1}}$,
2. per a tot natural $j < r$, si $p^j < i < p^{j+1}$ aleshores $v_p(c_i) \geq r - j$,
3. per a tot natural $j < r$, $v_p(c_{p^{j+1}}) = r - j - 1$.

Així, el polígon de Newton de $g(X)$ ha de ser d'un dels dos tipus següents (depenent de $v_p(c_0)$):



En qualsevol cas, el Corol.lari 1.4.3 garanteix que p és salvatgement ramificat a $(\mathbb{Q}_p)_g/\mathbb{Q}_p$. Així, p haurà de ramificar salvatgement a $\mathbb{Q}_f/\mathbb{Q}$ donat que $(\mathbb{Q}_p(\theta,\eta))_g = (\mathbb{Q}_p(\theta,\eta))_f = \mathbb{Q}_p(\theta)\mathbb{Q}_p(\eta)(\mathbb{Q}_p)_f$ i la composició d'extensions moderadament ramificades és moderadament ramificada.

Cas $r = v_p(n) = 1$.

A partir d'ara, $p \neq 2$. Cal veure que p ramifica a $\mathbb{Q}_f/\mathbb{Q}$.

Podem suposar $v_p(b) = 0$ donat que, altrament, el polígon de Newton de $f(X)$ té un únic costat de pendent no entera $-\frac{v_p(b)}{n} > -1$. Així, $b = b'$, $h = 0$ i $g(X)$ és el polinomi de $\mathbb{Q}_p(\eta)[X]$:

$$g(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^k + b = \sum_{0 \leq i \leq n} c_i X^i.$$

Canviant, si cal, $f(X)$ per

$$\frac{X^n}{b} f\left(\frac{b}{X}\right) = X^n + ab^{k-1}X^{n-k} + b^{n-1}$$

(i, per tant, k per $n-k$), es comprova que podem assumir l'existència d'algun $j < p-1$ tal que $v_p\begin{pmatrix} k \\ j \end{pmatrix} > 0$ (o bé $k < j$) i, per tant, $v_p(c_j) = 1$.

Així, el polígon de Newton de $g(X)$ té algun costat de pendent no entera $-\frac{1}{p-j} > -1$ i, per tant, l'extensió $(\mathbb{Q}_p)_g/\mathbb{Q}_p$ és ramificada. Com que l'extensió $\mathbb{Q}_p(\eta)/\mathbb{Q}_p$ és no ramificada i $(\mathbb{Q}_p(\eta))_g = \mathbb{Q}_p(\eta)(\mathbb{Q}_p)_f$, la conclusió és que p ramifica a $\mathbb{Q}_f/\mathbb{Q}$. □

Proposició 3.3.2. *Sigui $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ un trinomi separable amb $b \neq 0$ i $(k,n) = 1$.*

(a) Sigui p un primer senar que divideix $k(n-k)$ i tal que

$$v_p(b^{n-k}) \geq v_p(k^k(n-k)^{n-k}a^n).$$

Si no estem en el cas

$$p = 3,\ n \text{ parell},\ k(n-k) = n-1,\ v_3(n-1) = 1,$$

aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és ramificada en p.

Si, a més, $v_p(k(n-k)) > 1$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada en p.

(b) *Si* $v_2(k(n-k)) > 1$ *i* $v_2(b^{n-k}) \geq v_2(k^k(n-k)^{n-k}a^n)-2$, *aleshores l'extensió* $\mathbb{Q}_f/\mathbb{Q}$ *és salvatgement ramificada en* $p = 2$.

Demostració. Sigui p un primer que satisfà les hipòtesis de l'enunciat.

Canviant $f(X)$ per $\frac{X^n}{b} f\left(\frac{b}{X}\right) = X^n + ab^{k-1}X^{n-k} + b^{n-1}$, si cal, podem suposar que p divideix k.

Anàlogament a 3.3.1, podem suposar i suposem:

$$v_p(a) < n - k.$$

Notem $d = (k, v_p(b) - v_p(a))$, $v_p(b) - v_p(a) = dh$ i $k = de$. El polígon de Newton $N(f(X))$ té un costat de pendent $-\frac{h}{e}$. L'extensió $\mathbb{Q}_f/\mathbb{Q}$ només pot ser moderadament ramificada en p quan $v_p(e) = 0$ (Corol.lari 1.4.3).

Notem $r = v_p(k)$ i expressem $k = k'p^r$, $a = a'p^{v_p(a)}$ i $b = b'p^{v_p(b)}$.

Com a la Proposició 3.3.1, si $\theta, \eta \in \overline{\mathbb{Q}_p}$ són arrels de $X^e - p$ i $a'X^{k'} + b'$, respectivament, aleshores l'extensió $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$ és moderadament ramificada i l'extensió $\mathbb{Q}_p(\eta)/\mathbb{Q}_p$ és no ramificada.

Considerem el polinomi de $\mathbb{Q}_p(\theta, \eta)[X]$ següent:

$$g(X) := f(X + \eta\theta^h) = (X + \eta\theta^h)^n + a(X + \eta\theta^h)^k + b = \sum_{0 \leq i \leq n} c_i X^i.$$

Els coeficients c_i de $g(X)$ són:

$$c_0 = (\eta\theta^h)^n + a(\eta\theta^h)^k + b = \eta^n\theta^{hn} + p^{v_p(b)}\left(a'\eta^k + b'\right),$$

$$c_i = (\eta\theta^h)^{k-i}\left(\binom{n}{i}(\eta\theta^h)^{n-k} + a\binom{k}{i}\right), \text{ per a } 1 \leq i \leq k,$$

$$c_i = \binom{n}{i}(\eta\theta^h)^{n-i}, \text{ per a } i > k.$$

Cas $r = v_p(k) > 1$.

Donat que $v_p(d) = v_p(k) > 1$, tindrem $v_p(b) \equiv v_p(a) \pmod{p^2}$ i, per força,

$$v_p(k^k(n-k)^{n-k}a^n) \equiv v_p(b^{n-k}) \pmod{p^2}.$$

Així, també en el cas $p = 2$ haurà de ser

$$v_p(b^{n-k}) \geq v_p(k^k(n-k)^{n-k}a^n).$$

Per tant,

$$v_p\left(\theta^{h(n-k)}\right) \geq v_p(a) + r.$$

Aquesta desigualtat força els coeficients c_i de $g(X)$ a satisfer:

1. per a tot natural $j < r$, si $p^j < i < p^{j+1}$ aleshores $v_p(c_i) \geq v_p(a) + r - j + (k-i)\frac{h}{e}$,

2. per a tot natural $j < r$, si $i = p^{j+1}$ aleshores $v_p(c_i) = v_p(a) + r - j - 1 + (k-i)\frac{h}{e}$,

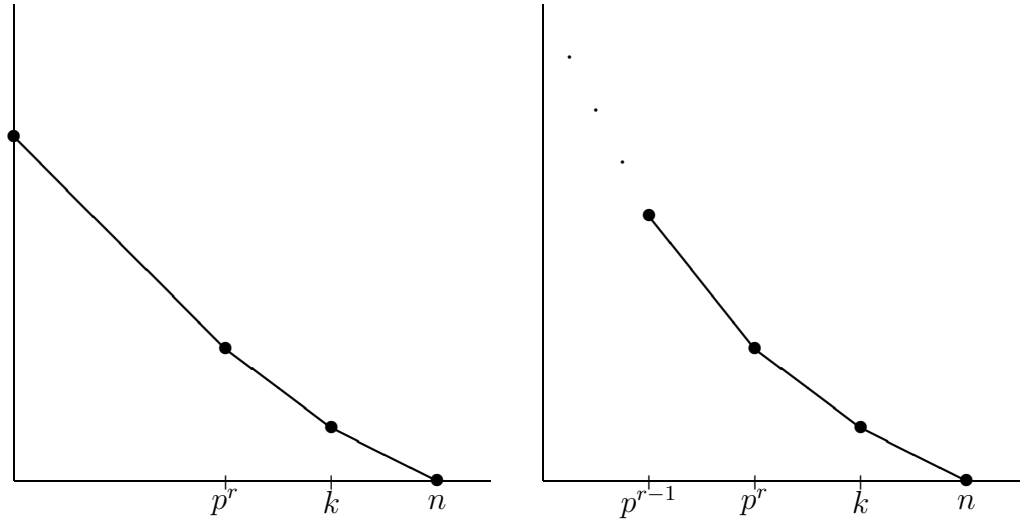
3. $v_p(c_0) = v_p(b) + 1$ o bé $\dfrac{v_p(c_0) - v_p(c_{p^r})}{p^r} \geq \dfrac{v_p(c_{p^{r-1}}) - v_p(c_{p^r})}{p^r - p^{r-1}}$,

4. si $p^r < i < k$, aleshores $v_p(c_i) \geq v_p(a) + (k-i)\frac{h}{e}$,

5. $v_p(c_k) = v_p(a)$,

6. si $k < i < n$, aleshores $v_p(c_i) \geq (n-i)\frac{h}{e}$.

El polígon de Newton de $g(X)$ només pot ser d'un dels dos tipus següents:



En el primer cas ($v_p(c_0) = v_p(b) + 1$), el polígon de Newton $N(g(X))$ té un costat de pendent $-\left(\frac{h}{e} + \frac{1}{p^r}\right)$. En el segon cas, en té un de pendent

$$-\left(\frac{v_p(c_{p^{r-1}}) - v_p(c_{p^r})}{p^r - p^{r-1}}\right) = -\left(\frac{1}{p^{r-1}(p-1)} + \frac{h}{e}\right).$$

Pel Corol.lari 1.4.3, p és salvatgement ramificat a $(\mathbb{Q}_p)_g/\mathbb{Q}_p$ i, per tant, també a $\mathbb{Q}_f/\mathbb{Q}$.

Cas $r = v_p(k) = 1$. $(p \neq 2)$

Volem veure que p ramifica a $\mathbb{Q}_f/\mathbb{Q}$; és suficient, doncs, considerar el cas en el qual tots els costats del polígon de Newton de $f(X)$ tenen pendent entera, és a dir, $v_p(a) = 0$ i k divideix $v_p(b)$. Així, $e = 1$ i $g(X)$ és el polinomi de $\mathbb{Q}_p(\eta)[X]$:

$$g(X) = f(X + \eta p^h) = (X + \eta p^h)^n + a(X + \eta p^h)^k + b = \sum_{0 \leq i \leq n} c_i X^i.$$

Ara tenim que $v_p(b) = kh$ i els coeficients c_i de $g(X)$ satisfan:

1. si $0 \leq i < p$, aleshores $v_p(c_i) \geq 1 + h(k - i)$,

2. $v_p(c_p) = h(k-p)$,

3. si $p < i < k$, aleshores $v_p(c_i) \geq h(k-i)$,

4. $v_p(c_k) = 0$.

Si $v_p(c_1) = 1 + h(k-1)$, aleshores el polígon $N(g(X))$ té un costat de pendent $-s$, amb s tal que:

$$h + \frac{1}{p} \leq s \leq h + \frac{1}{p-1}.$$

Si $v_p(c_2) = 1 + h(k-2)$, aleshores el polígon $N(g(X))$ té un costat de pendent $-s$, amb s tal que:

$$h + \frac{1}{p} \leq s \leq h + \frac{1}{p-2}.$$

Per a concloure que, en les nostres hipòtesis, $N(g(X))$ sempre té un costat de pendent no entera i, per tant, p ramifica a $\mathbb{Q}_f/\mathbb{Q}$, només cal notar que:

1. si $h(n-k) \neq 1$, aleshores $v_p(c_1) = 1 + h(k-1)$,

2. si $h(n-k) = 1$, aleshores $v_p(c_2) = 1 + h(k-2)$,

3. si k és parell, aleshores (k' és parell, n és senar i) podem suposar $v_p(c_1) = 1 + h(k-1)$ canviant, si cal, η per $-\eta$.

□

Observació 3.3.3. *En el cas "excepcional"*

$$p = 3,\ n \text{ parell},\ k(n-k) = n-1,\ v_3(n-1) = 1,$$

el resultat anterior realment és fals. Per exemple, $p = 3$ no ramifica a $\mathbb{Q}_f/\mathbb{Q}$ quan $f(X) = X^4 + aX^3 + 3^3 b \in \mathbb{Z}[X]$ amb

$$2 \leq v_3(4+a) < \frac{1 + v_3(3+a+b)}{2} - 1.$$

3.3.2 Primers no ramificats en extensions trinomials amb grup de Galois alternat

Observem que, en els apartats (a) de les dues proposicions anteriors, només hem admès p primer senar. El següent resultat estableix que, en general, els anàlegs per a $p = 2$ fallen. De fet, els "contraexemples"que obtenim han estat triats pensant en la demostració de la caracterització que donarem en el Teorema 3.3.5.

Proposició 3.3.4. *(i) Sigui $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ un trinomi separable amb $(n,k) = 1$, $v_2(n) = 1$ i $(-1)^{n/2}(1-kn) \not\equiv 1 \pmod 8$. Si $v_2(b+1) \geq 3$ i $v_2(a) \geq 3$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $p = 2$.*

(ii) Sigui $f(X) = X^n + aX^{n-k} + b \in \mathbb{Z}[X]$ un trinomi separable amb $(n,k) = 1$, $v_2(k) = 1$ i $(-1)^{\frac{n-1}{2}} n \not\equiv 1 \pmod 8$. Si $v_2(a+1) \geq 2$ i $v_2(b) = \lambda(n-k) \geq 2$ per algun $\lambda \in \mathbb{N}$, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $p = 2$.

Demostració. Suposem, primer, que es satisfan les hipòtesis de (i). En particular, $n' := \frac{n}{2}$ és senar. Sigui $\eta \in \overline{\mathbb{Q}_2}$ una arrel de $\psi(X) := X^{n'} - 1$ i considerem el polinomi de $\mathbb{Q}_2(\eta)[X]$ següent:

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^k + b = \sum_i c_i X^i.$$

Els coeficients c_i de $h(X)$ satisfan:

1. $c_0 = 1 + a\eta^k + b$ i, per hipòtesi, $v_2(c_0) \geq 3$,
2. $c_1 = n\eta^{n-1} + ak\eta^{k-1}$ i, per hipòtesi, $v_2(c_1) = 1$;
3. $c_2 = \frac{n(n-1)}{2}\eta^{n-2} + a\frac{k(k-1)}{2}\eta^{k-2}$ si $k > 1$ i $c_2 = \frac{n(n-1)}{2}\eta^{n-2}$ si $k = 1$; en tots dos casos, les hipòtesis sobre a i n garanteixen $v_2(c_2) = 0$.

Examinant el polígon de Newton $N(h(X))$ veiem que $h(X)$ té dues arrels a $\mathbb{Q}_2(\eta)$ (de valoracions positives diferents), que corresponen precisament a les dues arrels de $f(X)$ congruents a η mòdul 2. Així, $f(X)$ descompon completament a $(\mathbb{Q}_2)_\psi[X]$, és a dir, $(\mathbb{Q}_2)_f \subseteq (\mathbb{Q}_2)_\psi$. Per tant, l'extensió $(\mathbb{Q}_2)_f/\mathbb{Q}_2$ és no ramificada. Tal com volíem veure, $p = 2$ no ramifica a $\mathbb{Q}_f/\mathbb{Q}$.

Assumim, ara, les hipòtesis i notacions de (ii). En particular, $k' = \frac{k}{2}$ és senar i $n \equiv 3, 5 \pmod 8$. El Lema de Hensel proporciona una factorització $f(X) = f_1(X).f_2(X)$ a $\mathbb{Z}_2[X]$ amb $f_1(X) \equiv X^{n-k} \pmod 2$ i $f_2(X) \equiv (X^{k'}-1)^2 \pmod 2$.

Les $n-k$ arrels $\{\alpha_i\}_i$ de $f_1(X)$ són exactament les arrels de $f(X)$ a $\overline{\mathbb{Q}_2}$ amb valoració 2-àdica λ. Notant $b' = \frac{b}{2^{v_2(b)}}$, es té que els elements

$$\left\{\frac{2^\lambda b'}{\alpha_i}\right\}_i$$

són precisament les $n-k$ arrels a $\overline{\mathbb{Q}_p}$ de valoració 0 del polinomi:

$$g(X) := \frac{X^n}{b} f\left(\frac{2^\lambda b}{X}\right) = X^n + a(b')^{n-k-1}X^k + (b')^{n-1}2^{\lambda k}.$$

A més, aquestes són les arrels del factor $g_1(X) \equiv X^{n-k}-1 \pmod 2$ de $g(X)$ que proporciona el Lema de Hensel. Així, $(\mathbb{Q}_2)_{f_1} = (\mathbb{Q}_2)_{g_1}$ i l'extensió $(\mathbb{Q}_2)_{f_1}/\mathbb{Q}_2$ és no ramificada.

Falta veure, doncs, que $(\mathbb{Q}_2)_{f_2}/\mathbb{Q}_2$ també és no ramificada.

Sigui $\eta \in \overline{\mathbb{Q}_2}$ una arrel de $\psi(X) := X^{k'} - 1$ i considerem el polinomi de $\mathbb{Q}_2(\eta)[X]$ següent:

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^{n-k} + b = \sum_i c_i X^i.$$

Els coeficients c_i de $h(X)$ satisfan:

1. $c_0 = \eta^{n-k}(1+a) + b$ i, per hipòtesi, $v_2(c_0) \geq 2$,
2. $c_1 = \eta^{n-k-1}(n(1+a) - ak)$ i, per hipòtesi, $v_2(c_1) = 1$;

3. si $n-k>1$, aleshores $c_2=\eta^{n-k-2}\left(\frac{n(n-1)}{2}+\frac{(n-k)(n-k-1)}{2}a\right)$; tenint en compte que $v_2(k)=1$, obtenim $v_2(c_2)=0$,

4. si $n-k=1$, aleshores $c_2=\frac{n(n-1)}{2}\eta^{n-2}$; com que $v_2(k)=1$, aquest cas només és possible quan $n\equiv 3 \pmod 8$ i, per tant, $v_2(c_2)=0$.

A $\mathbb{Q}_2(\eta)[X]$, $h(X)$ té un factor $h_2(X)=(X-\beta_1)(X-\beta_2)$ de grau 2 que correspon precisament a les dues arrels de $f_2(X)$ congruents a η mòdul 2. Si $v_2(c_0)>2$, aleshores $(\mathbb{Q}_2(\eta))_{h_2}=\mathbb{Q}_2(\eta)$. Si $v_2(c_0)=2$, aleshores $\frac{2}{\beta_1},\frac{2}{\beta_2}$ són exactament les dues arrels de valoració 0 del polinomi de $\mathbb{Q}_2(\eta)[X]$

$$\frac{X^n}{c_0}h\left(\frac{2}{X}\right)\equiv X^{n-2}\left(X^2+\frac{2c_1}{c_0}X+\frac{4c_2}{c_0}\right) \pmod 2.$$

Com que $X^2+\frac{2c_1}{c_0}X+\frac{4c_2}{c_0}$ és un polinomi separable mòdul 2, $(\mathbb{Q}_2(\eta))_{h_2}/\mathbb{Q}_2(\eta)$ és una extensió no ramificada.

En conclusió, $((\mathbb{Q}_2)_\psi)_{f_2}/(\mathbb{Q}_2)_\psi$ és una extensió no ramificada i, per tant, $p=2$ no ramifica a $\mathbb{Q}_f/\mathbb{Q}$. □

Els resultats obtinguts fins ara ens permeten caracteritzar, per a un conjunt finit de primers fixat S qualsevol, els naturals n tals que el grup alternat A_n es realitza com a grup de Galois d'alguna extensió trinomial de $\mathbb{Q}$ no ramificada en S.

Teorema 3.3.5. *Siguin $k<n$ dos naturals tals que $(n,k)=1$. Per a qualsevol conjunt finit de primers S, són equivalents:*

(i) Existeix un trinomi $f(X)=X^n+aX^k+b\in\mathbb{Z}[X]$ amb cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ té grup de Galois A_n i és no ramificada en els primers de S.

(ii) Per a cada primer $p\in S$, existeix un trinomi $f(X)=X^n+a_pX^k+b_p\in\mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no nul i cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en p.

(iii) *Per a cada primer $p \in S$, es satisfà alguna de les condicions següents:*

Si n és parell i p és senar, aleshores $v_p(n) = 0$ o bé $\left(\frac{-1}{p}\right)^{n/2} = 1$.

Si n és parell i $p = 2$, aleshores $(-1)^{n/2}(1 - kn) \equiv 1 \pmod 8$ o bé $v_2(n) = 1$.

Si n és senar i p és senar, aleshores $v_p(k(n-k)) = 0$ o bé $\left(\frac{p}{n}\right) = 1$.

Si n és senar i $p = 2$, aleshores $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 8$ o bé $v_2(k(n - k)) = 1$.

Demostració.
(i) $\Rightarrow$ (iii)

Suposem que el trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ té grup de Galois A_n sobre $\mathbb{Q}$. Si $p \in S$ és un primer que no ramifica a $\mathbb{Q}_f/\mathbb{Q}$, aleshores les Proposicions 3.3.1 i 3.3.2 garanteixen, en particular:

1. si n és parell i p és un primer senar que divideix n, aleshores $v_p(a^n) < v_p(n^n b^{n-k})$,

2. si $p = 2$ divideix n, aleshores $v_2(a^n) < v_2(n^n b^{n-k}) - 2$ o bé $v_2(n) = 1$,

3. si n és senar i p és un primer senar que divideix $k(n - k)$, aleshores $v_p(b^{n-k}) < v_p(k^k(n-k)^{n-k}a^n)$,

4. si $p = 2$ divideix $k(n - k)$, aleshores $v_2(b^{n-k}) < v_2(k^k(n-k)^{n-k}a^n) - 2$ o bé $v_2(k(n - k)) = 1$.

De l'expressió per al discriminant d'un trinomi $f(X)$, obtenim que $D(f(X))$ coincideix, a menys de quadrats a $\mathbb{Z}$, amb un enter N tal que:

1. $N \equiv (-1)^{n/2} \pmod p$, si n és parell i p és un primer senar que divideix n,

2. $N \equiv (-1)^{n/2}(1 - kn) \pmod 8$, si n és parell i $p = 2$ satisfà $v_2(n) > 1$,

3. $N \equiv (-1)^{\frac{n-1}{2}} n \pmod{p}$, si n és senar i p és un primer senar que divideix $k(n-k)$,

4. $N \equiv (-1)^{\frac{n-1}{2}} n \pmod{8}$, si n és senar i $p = 2$ satisfà $v_2(k(n-k)) > 1$.

Quan imposem que $D(f(X))$ sigui un quadrat a $\mathbb{Z}$, obtenim precisament les condicions enunciades a (iii).

(iii) $\Rightarrow$ (ii)

Només cal demostrar (ii) quan $p = 2$ i estem en un dels dos casos següents:

- n parell, $v_2(n) = 1$ i $(-1)^{n/2}(1 - kn) \not\equiv 1 \pmod{8}$,

- n senar, $v_2(k(n-k)) = 1$ i $(-1)^{\frac{n-1}{2}} n \not\equiv 1 \pmod{8}$.

La resta de casos ja s'han obtingut a la Proposició 3.2.4.

Cas n parell.

Per la Proposició 3.3.4 (i), és suficient veure que existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no nul i tal que:

$$(*) \qquad v_2(b+1) \geq 3 \ \text{ i } \ v_2(a) \geq 3.$$

Si r, s són dos naturals tals que $s(n-k) - rn = 1$ i $A, t \in \mathbb{Z}$, aleshores el discriminant $D(f(X))$ del trinomi $f(X) = X^n + nAt^r X^k + t^s$ és, a menys de quadrats a $\mathbb{Z}$,

$$-t + (n-k)^{n-k} k^k A^n.$$

Per a qualsevol $A \in \mathbb{Z}$ tal que $v_2(A^n) \geq 3$, existeix algun enter senar t de manera que $D(f(X))$ és un quadrat a $\mathbb{Z}$ no nul. Per força $t \equiv -1 \pmod{8}$ i, com que s és senar, els coeficients $a = nAt^r$ i $b = t^s$ de $f(X)$ satisfan la condició (*).

Cas n senar.

Podem suposar k parell i $v_2(k) = 1$. Per la Proposició 3.3.4 (ii), és suficient veure que existeix algun trinomi $f(X) = X^n + aX^{n-k} + b \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no nul i tal que:

$$(*) \qquad v_2(a+1) \geq 2 \text{ i } v_2(b) = \lambda(n-k) \geq 2, \text{ amb } \lambda \in \mathbb{N}.$$

Si r, s són dos naturals tals que $rn - sk = 1$ i $B, t \in \mathbb{Z}$, aleshores el discriminant del trinomi $f(X) = X^n + (n-k)^{k-1}t^r X^{n-k} + k(n-k)^{n-1}Bt^s$ és, a menys de quadrats a $\mathbb{Z}$,

$$(-1)^{\frac{n-1}{2}} n^n B^k + (-1)^{\frac{n-1}{2}} t.$$

Per a qualsevol $B \in \mathbb{Z}$ tal que $v_2(B^k)$ és (un múltiple de $n-k$) més gran o igual que 3, podem triar un senar t de manera que $D(f(X))$ sigui un quadrat a $\mathbb{Z}$ no nul. En aquest cas, haurà de ser $(-1)^{\frac{n-1}{2}} t \equiv 1 \pmod 8$. Tenint en compte que, per hipòtesi, $n \equiv 3, 5 \pmod 8$ i $v_2(k) = 1$, s'obté que els coeficients $a = (n-k)^{k-1}t^r$ i $b = k(n-k)^{n-1}Bt^s$ de $f(X)$ satisfan la condició $(*)$.

(ii) $\Rightarrow$ (i).

Per hipòtesi, per a cada primer $p \in S$, el trinomi $X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ té discriminant quadrat a $\mathbb{Z}$. Per la Proposició 3.2.5, existeixen $r, s \in \mathbb{N}$ i $a(T) \in \mathbb{Q}(T)$ de manera que el trinomi

$$f(T, X) := X^n + a(T)^r X^k + a(T)^s \in \mathbb{Q}(T)[X]$$

satisfà:

- $\mathrm{Gal}_{\mathbb{Q}(T)}(f(T, X)) \cong A_n$,
- per a cada $p \in S$, existeix $t_p \in \mathbb{Q}$ tal que els trinomis $X^n + a_p X^k + b_p$ i $f(t_p, X)$ tenen el mateix cos de descomposició sobre $\mathbb{Q}$.

Pel Teorema d'Irreductibilitat de Hilbert (veure Proposició 5.2.2), existeix algun $t \in \mathbb{Q}$ tal que:

- $\mathrm{Gal}_{\mathbb{Q}}(f(t, X)) \cong A_n$,

- t i t_p són arbitràriament propers p-àdicament, per a cada $p \in S$.

D'altra banda, si dos polinomis separables de $\mathbb{Q}[X]$ són prou propers p-àdicament, aleshores el Lema de Krasner garanteix que els seus cossos de descomposició sobre $\mathbb{Q}_p$ coincideixen (veure Proposició 5.2.1). Podem suposar, doncs, que els trinomis $f(t, X)$ i $X^n + a_p X^k + b_p$ tenen el mateix cos de descomposició sobre $\mathbb{Q}_p$, per a tot $p \in S$. Així, per hipòtesi, els primers de S no ramifiquen en el cos de decomposició sobre $\mathbb{Q}$ de $f(t, X)$.

Triant un enter M de manera que $f(X) := M^n f(t, X/M)$ tingui coeficients enters, el trinomi $f(X)$ satisfà totes les condicions desitjades. □

Teorema 3.3.6. *Per a un natural n, són equivalents:*

(i) *Per a qualsevol conjunt finit de primers S, existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ té grup de Galois A_n i és no ramificada en els primers de S.*

(ii) *n satisfà alguna de les condicions següents:*

$n \equiv 0, 1 \pmod 8$,

$n \equiv 2, \pmod 8$ *i* $p \equiv 1 \pmod 4$, *per a tot primer senar* $p \mid n$,

$n \equiv 3 \pmod 8$ *i existeix algun natural* $k < n$ *tal que* $(k, n) = 1$, $v_2(k(n-k)) = 1$ *i* $\left(\frac{p}{n}\right) = 1$, *per a tot primer senar* $p \mid k(n-k)$.

Demostració. Només cal comprovar que, per a un natural n, la condició (ii) equival a l'existència d'algun k de manera que la condició (iii) del Teorema 3.3.5 es satisfà per a tot primer.

És suficient remarcar que:

1. si $n \equiv 1 \pmod 8$, podem agafar $k = n - 1$,

2. si $n \equiv 4 \pmod 8$, aleshores k és senar i $(-1)^{n/2}(1 - kn) \equiv 5 \pmod 8$,

3. si $n \equiv 6 \pmod 8$, aleshores existeix algun primer senar $p \mid n$ tal que $\left(\frac{-1}{p}\right)^{n/2} = -1$,

4. si $n \equiv 5, 7 \pmod 8$ i $v_2(k(n-k)) = 1$, aleshores sempre existeix algun primer senar $p \mid k(n-k)$ tal que $\left(\frac{p}{n}\right) = -1$.

Per a veure 3. i 4., es pot raonar com en el Teorema 3.2.7. □

Observació 3.3.7. *Els casos que apareixen en el Teorema 3.3.6 són pràcticament els mateixos que els del Teorema 3.2.7. Les úniques diferències es produeixen quan* $n \equiv 3 \pmod 8$. *Per alguns* $n \equiv 3 \pmod 8$ *podem aconseguir que* $p = 2$ *no ramifiqui però no que no divideixi* $D(f(X))$.

3.4 Extensions trinomials moderadament ramificades en S

En les caracteritzacions obtingudes a la secció anterior, demanàvem que determinats primers no ramifiquessin. Ara acceptem que ramifiquin, sempre que ho fassin moderadament. Apareixeran casos nous corresponents a primers moderadament ramificats que mai podem aconseguir que no ramifiquin.

Teorema 3.4.1. *Siguin* $k < n$ *dos naturals tals que* $(n, k) = 1$. *Per a qualsevol conjunt finit de primers* S, *són equivalents:*

(i) Existeix un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ *amb cos de descomposició* $\mathbb{Q}_f$ *tal que l'extensió* $\mathbb{Q}_f/\mathbb{Q}$ *té grup de Galois* A_n *i és moderadament ramificada en els primers de* S.

(ii) *Per a cada primer $p \in S$, existeix un trinomi $f(X) = X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no nul i cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és moderadament ramificada en p.*

(iii) *Per a cada primer $p \in S$, es satisfà alguna de les condicions següents:*

Si n és parell i p és senar, aleshores $v_p(n) \leq 1$ o bé $\left(\frac{-1}{p}\right)^{n/2} = 1$.

Si n és parell i $p = 2$, aleshores $(-1)^{n/2}(1 - kn) \equiv 1 \pmod 8$ o bé $v_2(n) = 1$.

Si n és senar i p és senar, aleshores $v_p(k(n-k)) \leq 1$ o bé $\left(\frac{p}{n}\right) = 1$.

Si n és senar i $p = 2$, aleshores $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 8$ o bé $v_2(k(n-k)) = 1$.

Demostració. El resultat enunciat s'obté amb un raonament anàleg al que hem usat per a demostrar el Teorema 3.3.5 (tenint en compte les Proposicions 3.3.1, 3.3.2 i 3.3.4). L'únic fet que cal justificar és que es pot aconseguir moderació també en els casos nous (que no apareixien a 3.3.5). És a dir, cal veure que la propietat (ii) es satisfà en els dos casos següents:

(a) n parell, p senar tal que $v_p(n) = 1$ i $\left(\frac{-1}{p}\right)^{n/2} = -1$,

(b) n senar, p senar tal que $v_p(k(n-k)) = 1$ i $\left(\frac{p}{n}\right) = -1$.

Cas n parell.

Considerem un trinomi separable $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ tal que:

$$(*) \qquad v_p(b+1) \geq 2 \ \text{ i } \ v_p(a) \geq 2.$$

Volem veure que $\mathbb{Q}_f/\mathbb{Q}$ és moderadament ramificada en p.

Notem $n' := \frac{n}{p}$ i considerem el polinomi de $\mathbb{Q}_p(\eta)[X]$:

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^k + b = \sum_i c_i X^i,$$

on $\eta \in \overline{\mathbb{Q}_p}$ és una arrel de $\psi(X) := X^{n'} - 1$.

Raonant com a la demostració de la Proposició 3.3.4 (allà era $p = 2$), s'obté que el polígon de Newton de $h(X)$ consta d'un costat d'amplada 1 i un altre d'amplada $p-1$ i alçada 1. Així, les p arrels de $f(X)$ congruents a η mòdul p pertanyen a un cos extensió de $\mathbb{Q}_p(\eta)$ de grau $p-1$. Per tant, les extensions $((\mathbb{Q}_p)_\psi)_f/(\mathbb{Q}_p)_\psi$ i $(\mathbb{Q}_p)_f/\mathbb{Q}_p$ són moderadament ramificades (i $p-1$ divideix l'índex de ramificació). En conclusió, p és moderadament ramificat a $\mathbb{Q}_f/\mathbb{Q}$.

Es comprova, com a la demostració de (iii) $\Rightarrow$ (ii) del Teorema 3.3.5, que existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb discriminant quadrat a $\mathbb{Z}$ no nul i que satisfà $(*)$.

Cas n senar.

Suposem $v_p(k) = 1$ i notem $k' = \frac{k}{p}$, $m = (-1)^{\frac{n-1}{2}}(n-k)$. Considerem un trinomi $f(X) = X^n + aX^{n-k} + b \in \mathbb{Z}[X]$ (separable) tal que:

$$(*) \qquad v_p(a - m^p) \geq 2 \ \text{ i } \ v_p(b) = \lambda(n-k) \geq p, \ \text{ amb } \lambda \in \mathbb{N}.$$

Veurem que $\mathbb{Q}_f/\mathbb{Q}$ és moderadament ramificada.

Del Lema de Hensel s'obté una factorització $f(X) = f_1(X).f_2(X)$ a $\mathbb{Z}_p[X]$ amb $f_1(X) \equiv X^{n-k} \pmod{p}$ i $f_2(X) \equiv (X^{k'} - 1)^p \pmod{p}$. Com a la Proposició 3.3.4, s'obté que l'extensió $(\mathbb{Q}_p)_{f_1}/\mathbb{Q}_p$ és no ramificada.

Sigui $\eta \in \overline{\mathbb{Q}_p}$ una arrel de $\psi(X) := X^{k'} + m$ i considerem el següent polinomi de $\mathbb{Q}_p(\eta)[X]$:

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^{n-k} + b = \sum_i c_i X^i.$$

Amb un raonament anàleg al de la demostració de la Proposició 3.3.4, es comprova que el polígon de Newton de $h(X)$ consta d'un costat d'amplada 1 i un altre d'amplada $p-1$ i alçada 1 (tenint en compte que $v_p(k) = 1$ i $a \equiv -1 \pmod{p}$). Igual que en el cas parell, això és suficient per a concloure que p és moderadament ramificat a $\mathbb{Q}_f/\mathbb{Q}$.

Comprovem, finalment, l'existència d'algun trinomi $f(X) = X^n + aX^{n-k} + b$ satisfent la condició $(*)$ i amb discriminant quadrat a $\mathbb{Z}$ no nul.

Considerem dos naturals r, s tals que $rn - sk = 1$. Donats $B, t \in \mathbb{Z}$, el discriminant de $f(X) = X^n + m^p t^r X^{n-k} + k(n-k)^{2n-1} B^2 t^s$ és, a menys de quadrats a $\mathbb{Z}$,

$$(-1)^{\frac{n-1}{2}} n^n (n-k)^{n(2k-p-1)} B^{2k} + t.$$

És clar que existeixen B, t tals que $f(X)$ té discriminant quadrat no nul a $\mathbb{Z}$ i satisfà (*); només cal observar que sempre podem agafar $t \equiv 1 \pmod{p^2}$. □

Com a conseqüència del resultat anterior, obtenim la caracterització que buscàvem en aquesta secció.

Teorema 3.4.2. *Per a un natural n, són equivalents:*

(i) Existeix algun trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ té grup de Galois A_n i és moderadament ramificada.

(ii) Si n és parell, aleshores existeix algun natural $k < n$ amb $(k, n) = 1$ de manera que $v_p(n) = 1$, per a tot primer $p \mid n$ tal que $\left(\frac{p}{k(n-k)}\right) = -1$.

Si n és senar, aleshores existeix algun natural $k < n$ amb $(k, n) = 1$ de manera que $v_p(k(n-k)) = 1$, per a tot primer $p \mid k(n-k)$ tal que $\left(\frac{p}{n}\right) = -1$.

És clar que tots els naturals que satisfan alguna de les condicions següents superen el criteri establert en el resultat anterior:

- $n \equiv 0, 1 \pmod{8}$; és suficient agafar $k = 1$.
- n parell, lliure de quadrats.

A continuació obtindrem que, de fet, això també és cert per a *tot* natural senar n, com a conseqüència directa del resultat següent. Agraïm a Carl Pomerance haver-nos suggerit que un argument de garbell ("sieve") hauria de ser suficient per a demostrar-lo (per a n prou gran).

Proposició 3.4.3. *Tot natural $n > 1$ es pot expressar com a suma de dos naturals lliures de quadrats coprimers amb n.*

Demostració. Associat a un natural fixat $n > 1$ i a un primer q qualsevol, considerem el conjunt $R_q(n)$ format per tots els naturals a que satisfan les condicions següents:

- $1 \leq a \leq n-1$,
- $(a, n) = 1$,
- $v_q(a) > 1$.

Definim el conjunt $R(n)$ com la reunió dels $R_q(n)$, on q recorre tots els nombres primers. Denotem per $r(n)$ (resp. $r_q(n)$) el cardinal de $R(n)$ (resp. $R_q(n)$).

El nombre de parells de naturals $\{k, n-k\}$ coprimers amb n és $\frac{\phi(n)}{2}$, on ϕ denota la funció indicatriu d'Euler. Cal veure que, per algun d'aquests parells, ni k ni $n-k$ pertanyen a $R(n)$. Així, és suficient provar la desigualtat

$$r(n) < \frac{\phi(n)}{2}.$$

Comencem observant que, si $p_1, \ldots, p_s$ són els factors primers de n i q és un primer que no divideix n, aleshores

$$\begin{aligned} r_q(n) &= \left[\frac{n}{q^2}\right] - \sum_{1\leq i\leq s}\left[\frac{n}{q^2 p_i}\right] + \sum_{1\leq i<j\leq s}\left[\frac{n}{q^2 p_i p_j}\right] - \cdots \\ &< \frac{n}{q^2} - \sum_{1\leq i\leq s}\left(\frac{n}{q^2 p_i} - 1\right) + \sum_{1\leq i<j\leq s}\frac{n}{q^2 p_i p_j} - \cdots \\ &= \frac{n}{q^2}\prod_{1\leq i\leq s}\left(1 - \frac{1}{p_i}\right) + 2^{s-1} = \frac{\phi(n)}{q^2} + 2^{s-1}. \end{aligned}$$

D'aquesta manera, obtenim

$$r(n) \leq \sum_{q \nmid n} r_q(n) < \phi(n) \left(\sum_{q \nmid n} \frac{1}{q^2} \right) + 2^{s-1}\pi(\sqrt{n}),$$

on $\pi(x)$ denota el nombre de primers $\leq x$.

Per tant, és suficient provar la desigualtat

$$\frac{2^{s-1}\pi(\sqrt{n})}{\phi(n)} < \frac{1}{2} - \sum_{q \nmid n} \frac{1}{q^2}.$$

És conegut que, per a qualsevol enter $m \geq 2$, es té (cf. [Apo80, Thm. 4.6]):

$$\pi(m) < \frac{6m}{\ln(m)}.$$

D'altra banda, de la igualtat

$$\sum_{i \geq 1} \frac{1}{i^2} = \zeta(2) = \frac{\pi^2}{6},$$

es dedueix immediatament la fita:

$$\sum_{q} \frac{1}{q^2} < 0,4523.$$

En resum, si definim

$$f(n) := \frac{2^s n}{\phi(n)} \frac{6}{\sqrt{n}\ln(n)},$$

aleshores la conclusió del resultat enunciat és certa per a tot natural n que satisfà la desigualtat

$$(*) \qquad f(n) < 0,0477 + \sum_{1 \leq i \leq s} \frac{1}{(p_i)^2}.$$

Observem que

$$f(n) = \left(\prod_{1 \leq i \leq s} \frac{2p_i}{p_i - 1} \right) \frac{6}{\sqrt{n}\ln(n)}.$$

Per tant, si $q_1, \ldots, q_s$ són els s nombres primers més petits, aleshores:

$$f(n) \leq f(p_1.\cdots.p_s) \leq f(q_1.\cdots.q_s).$$

Tenint en compte que $\frac{2\sqrt{q}}{q-1} < 1$ si $q \geq 7$ i que

$$f(2.3.5.7.11.13.17.19.23.29) = 0,0214 < 0,0477,$$

concloem que la desigualtat (*) és certa sempre que n té $s \geq 10$ divisors primers diferents.

D'altra banda, si el nombre de factors primers de n és $s \leq 9$, aleshores

$$\frac{n}{\phi(n)} \leq \frac{2.3.5.7.11.13.17.19.23}{\phi(2.3.5.7.11.13.17.19.23)} < 6,113$$

i, per tant, es té

$$f(n) < 2^9.(6,113).\frac{6}{\sqrt{n}\ln(n)}.$$

Això permet comprovar que es té $f(n) < 0,0477$ i, en particular, la desigualtat (*), per a tot $n \geq 10^9$.

Quan en l'argument anterior, a més, tenim en compte (als dos costats de la desigualtat (*)) quins dels primers $2, 3, 5$ divideixen n, la conclusió que s'obté és que tot $n \geq 150000$ satisfà la desigualtat (*). De fet, aquesta desigualtat falla exactament per a 3064 naturals $n > 1$, el més gran dels quals és $n = 120120 = 2^3.3.5.7.11.13$.

Finalment, per a tots els naturals $1 < n < 150000$ (o per als 3064 esmentats), es comprova directament la validesa del resultat enunciat. □

Corol.lari 3.4.4. *Tot natural senar $n > 1$ supera el criteri establert en el Teorema 3.4.2, és a dir, existeix un trinomi $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ amb cos de descomposició $\mathbb{Q}_f$ tal que l'extensió $\mathbb{Q}_f/\mathbb{Q}$ té grup de Galois A_n i és moderadament ramificada.*

Un dels objectius que perseguim, i que resoldrem en el capítol següent, és la realització de *tot* grup alternat A_n com a grup de Galois d'alguna extensió

moderadament ramificada de $\mathbb{Q}$. El Teorema 3.4.2 ens diu que, per a infinits n, això no es pot aconseguir només amb extensions definides per trinomis de grau n. Per exemple, aquest és el cas sempre que $n \equiv 4 \pmod 8$ donat que, per a qualsevol senar k, es té $\left(\frac{2}{k(n-k)}\right) = -1$. De fet, els arguments donats per a demostrar el Teorema 3.4.2 també estableixen el resultat següent.

Teorema 3.4.5. *Sigui $f(X) = X^n + aX^k + b \in \mathbb{Q}[X]$ un trinomi de grau $n \equiv 4 \pmod 8$ amb k senar i discriminant quadrat no nul a $\mathbb{Q}$. Aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada (en $p = 2$).*

Demostració. És suficient raonar com en el Teorema 3.4.2, tenint en compte les següents observacions.

- De la hipòtesi $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong A_n$, l'únic que realment hem usat és que $f(X)$ no tingui arrels múltiples i que el seu discriminant $D(f(X))$ sigui un quadrat a $\mathbb{Q}$. No hem usat enlloc, per exemple, el caràcter irreductible de $f(X)$.

- En principi, sí hem usat fortament la hipòtesi $(n, k) = 1$. Quan només suposem k senar i notem $n_1 = \frac{n}{(n,k)}$ i $k_1 = \frac{k}{(n,k)}$, aleshores el trinomi $g(X) = X^{n_1} + aX^{k_1} + b$ té grau $n_1 \equiv 4 \pmod 8$ i clarament $\mathbb{Q}_g \subseteq \mathbb{Q}_f$.

□

Per a un natural n, considerem un trinomi

$$f(T, X) := X^n + a(T)^r X^k + a(T)^s \in \mathbb{Q}(T)[X]$$

com a la Proposició 3.2.5. Sigui L_T el cos de descomposició de $f(T, X)$ sobre $\mathbb{Q}(T)$. Recordem que $L_T/\mathbb{Q}(T)$ és una extensió $\mathbb{Q}$-regular amb grup de Galois

$$\mathrm{Gal}_{\mathbb{Q}(T)}(f(T, X)) \cong A_n.$$

Es pot interpretar que el que hem fet en aquest capítol és buscar "bones"especialitzacions dels trinomis $f(T, X)$, on el significat del terme "bones"ha anat

canviant en cada apartat. Des d'aquest punt de vista, el Teorema anterior ens diu que, quan $n \equiv 4 \pmod 8$, les extensions $L_T/\mathbb{Q}(T)$ són exemples d'extensions regulars de $\mathbb{Q}(T)$ amb grup de Galois A_n que no admeten cap especialització racional moderadament ramificada.

Capítol 4

Realització de grups alternats com a grups de Galois sobre $\mathbb{Q}$ amb condicions de ramificació

4.1 Introducció

En aquest capítol veurem que, donat un conjunt finit de primers qualsevol S, tot grup alternat A_n es realitza com a grup de Galois d'alguna extensió de $\mathbb{Q}$ no ramificada en $S \cup \{\infty\}$. En particular, veiem que la qüestió plantejada per Birch sobre la possibilitat de realitzar tot grup finit com a grup de Galois d'alguna extensió moderadament ramificada de $\mathbb{Q}$ admet una resposta afirmativa per als grups alternats.

Més concretament, el resultat principal estableix que, per a qualsevol n i qualsevol conjunt finit de primers S, existeix algun polinomi mònic $f(X) \in \mathbb{Z}[X]$ de grau n amb grup de Galois A_n, discriminant no divisible per cap primer finit de S i amb totes les arrels reals. D'aquesta manera, $\mathbb{Q}_f/\mathbb{Q}$ és una A_n-extensió no ramificada en $S \cup \{\infty\}$ i, si α és una arrel de $f(X)$ i $\mathcal{O}$ denota l'anell d'enters de $\mathbb{Q}(\alpha)$, aleshores els primers de S no divideixen l'índex

$(\mathcal{O} : \mathbb{Z}[\alpha])$.

Al Capítol 3 ja hem vist com, per a infinits valors de n, aquest objectiu es pot aconseguir considerant cossos de descomposició de trinomis de grau n (excepte la condició en $p = \infty$). També hem vist que, per a infinits valors de n, això no es pot aconseguir considerant només aquest tipus d'extensions (per algun S, encara que ignorem la condició en $p = \infty$).

Les realitzacions buscades de A_n sobre $\mathbb{Q}$ s'obtenen, com en el Capítol 3, per especialització de realitzacions regulars de A_n sobre $\mathbb{Q}(T)$. Un resultat de Mestre [Mes90] ens proporciona les extensions de $\mathbb{Q}(T)$ que usarem en aquest capítol. Aquestes corresponen (per a n senar) a recobriments de grau n de $\mathbb{P}^1$ per $\mathbb{P}^1$, definits sobre $\mathbb{Q}$, ramificats en exactament $n-1$ punts i tals que la seva clausura galoisiana té grup de Galois A_n.

A la Secció 4.2 recordem la construcció de Mestre que, a partir d'un polinomi mònic $P(X) \in \mathbb{Q}[X]$ de grau senar n satisfent certes hipòtesis, dona lloc a una realització regular d'A_n sobre $\mathbb{Q}(T)$ definida per un polinomi del tipus $P(X) - TQ(X)$, per a cert $Q(X) \in \mathbb{Q}[X]$ de grau menor o igual que $n-1$. Al Capítol 6, on considerarem problemes d'immersió centrals per a grups alternats, recordarem altres resultats de [Mes90]. De fet, el resultat principal de [Mes90] és que, per a tot $n \geq 4$, existeixen realitzacions regulars de $\widetilde{A_n}$ sobre $\mathbb{Q}(T)$, on $\widetilde{A_n}$ denota l'única extensió central no trivial de A_n amb nucli $\mathbb{Z}/2\mathbb{Z}$.

Una virtud de la construcció de Mestre és que les hipòtesis exigides a $P(X)$ són poc restrictives. Aquest fet ens permet demostrar l'existència de polinomis mònics $P(X) \in \mathbb{Z}[X]$ amb totes les arrels reals i discriminant no divisible per cap primer finit de S per als quals el resultat de Mestre és aplicable. La Secció 4.3 està dedicada a la construcció de $P(X)$ amb aquestes propietats.

A la Secció 4.4 obtenim les extensions buscades de $\mathbb{Q}$ per especialització de $P(X) - TQ(X)$, en principi, només per a n senar. Podrem raonar com

a [Mes90] per a deduir el cas n parell del cas n senar, gràcies al fet que els polinomis $P(X)$ construïts a la Secció 4.3 sempre tenen una arrel racional ($n \geq 5$).

Acabem el capítol observant que els arguments donats també permeten resoldre, per a tot A_n, el Problema 2.1 plantejat a la Introducció de la memòria. Concretament, obtenim l'existència de realitzacions de A_n com a grup de Galois d'alguna extensió de $\mathbb{Q}$ en la qual tots els primers d'un conjunt finit prefixat qualsevol descomponen completament.

4.2 Les realitzacions de Mestre de grups alternats sobre $\mathbb{Q}(T)$

Considerem indeterminades $T_1, \ldots, T_n$.

Donat un polinomi A en diverses indeterminades, sovint usarem la notació $D_X(A)$ per a remarcar que considerem el discriminant respecte la indeterminada X. Anàlogament, $Res_X(\cdot,\cdot)$ denotarà la resultant respecte X.

Proposició 4.2.1. *[Mes90, Prop. 1, Prop.2]*
Sigui $n \geq 3$ un natural senar i K un cos de característica 0. Aleshores, existeix un polinomi $H = H(T_1, \ldots, T_n) \in \mathbb{Z}[T_1, \ldots, T_n]$ de manera que, per a tot polinomi $P(X) = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ de grau n tal que $H(a_1, \ldots, a_n) \neq 0$, existeix un polinomi $Q(X) \in K[X]$ de grau menor o igual que $n-1$ amb les propietats següents:

(a) $D_X(P(X) - TQ(X)) = D(P(X))(S(T))^2$, *per a cert polinomi* $S(T) \in K[T]$ *de grau* $n-1$.

(b) El grup de Galois de $P(X) - TQ(X)$ *sobre* $\overline{K}(T)$ *és*

$$\mathrm{Gal}_{\overline{K}(T)}(P(X) - TQ(X)) \cong A_n.$$

En particular, si el discriminant $D(P(X))$ *és un quadrat a* K *(resp. un no quadrat a* K*), aleshores el cos de descomposició sobre* $K(T)$ *del polinomi* $P(X) - TQ(X)$ *defineix una extensió* K*-regular (resp. no* K*-regular) de* $K(T)$ *amb grup de Galois* A_n *(resp.* S_n*).*

Amb les hipòtesis i notacions d'aquest resultat, es diu que un polinomi mònic $X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ és H**-general** quan $H(a_1, \ldots, a_n) \neq 0$. Observem que el discriminant d'un polinomi H-general $P(X)$ és necessàriament no nul.

A [Mes90, Prop. 4] s'obté, per al polinomi $X^n - X$ de grau senar $n \geq 3$, la igualtat:

$$H(0, \ldots, 0, -1, 0) = (-1)^{\frac{n-1}{2}} 2^{n-1} n^{n(n-1)} (n-1)^{2(n-1)} (n-2)^{(n-2)(n-1)+1}.$$

En particular, si $P(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ és un polinomi mònic de grau n tal que $P(X) \equiv X^n - X \pmod{l}$ per algun primer l que no divideix $n(n-1)(n-2)$, aleshores l no divideix $H(a_1, \ldots, a_n) \in \mathbb{Z}$ i, per tant, $P(X)$ és H-general. D'aquí s'obté el següent resultat que, essencialment, és el que usarem en aquest capítol.

Corol.lari 4.2.2. *Sigui* $P(X) \in \mathbb{Z}[X]$ *un polinomi mònic de grau senar* $n \geq 3$ *tal que:*

(i) $P(X)$ *té discriminant quadrat a* $\mathbb{Z}$*,*

(ii) $P(X) \equiv X^n - X \pmod{l}$*, amb* l *primer no dividint* $n(n-1)(n-2)$*.*

Aleshores, existeix un polinomi $Q(X) \in \mathbb{Z}[X]$ *de grau més petit o igual que* $n-1$ *tal que el cos de descomposició de* $P(X) - TQ(X)$ *defineix una extensió* $\mathbb{Q}$*-regular de* $\mathbb{Q}(T)$ *amb grup de Galois isomorf a* A_n*.*

4.3 Construcció del polinomi $P(X)$

En tota aquesta secció suposarem fixat un conjunt finit de primers (finits) racionals S qualsevol.

L'objectiu és construir, per a cada natural senar n, un polinomi mònic $P(X) \in \mathbb{Z}[X]$ de grau n amb bones propietats locals en un nombre finit de primers (en particular, els de $S \cup \{\infty\}$), discriminant quadrat a $\mathbb{Z}$ i amb una arrel racional (quan $n \geq 5$). Per a $n \geq 7$, $P(X)$ serà del tipus $Xg(X)h(X)$; en els dos lemes següents construïm els polinomis $g(X)$ i $h(X)$.

Lema 4.3.1. *Sigui $n \geq 7$ un natural senar i sigui $l \notin S$ un primer tal que $l \equiv 1 \pmod{n-1}$. Aleshores, existeix algun polinomi mònic $h(X) \in \mathbb{Z}[X]$ de grau $n-3$ satisfent les condicions següents:*

(i) $h(X)$ *divideix* $X^{n-1}-1$ *a* $\mathbb{F}_l[X]$,

(ii) $h(X)$ *és irreductible a* $\mathbb{F}_p[X]$, *per a tot* $p \in S$, $p \neq 2$,

(iii) $h(X)$ *no té factors irreductibles de grau més petit que* 3 *a* $\mathbb{F}_2[X]$ *i té discriminant* $D(h(X)) \equiv 5 \pmod{8}$,

(iv) totes les arrels de $h(X)$ *són reals.*

Demostració. Pel Teorema Xinès del residu, l'existència de $h(X) \in \mathbb{Z}[X]$ satisfent les condicions (i), (ii), (iii) alhora equival a l'existència de tres polinomis satisfent-les per separat. Com que $X^{n-1}-1$ descompon a $\mathbb{F}_l[X]$ en producte de factors de grau 1, la condició (i) no suposa cap problema. Clarament, la condició (ii) tampoc. A continuació explicitem polinomis satisfent la condició (iii).

De l'expressió per al discriminant d'un trinomi s'obté, per a $m \geq 4$ parell i $k < m$ senar tal que $m \neq 2k$,

$$D(X^m + X^k + 1) \equiv (-1)^{m/2}(1 - km) \pmod{8}.$$

D'altra banda, $X^m + X^k + 1$ no té arrels a $\mathbb{F}_2$ i, per tant, $X^2 + X + 1$ és el seu únic possible factor irreductible a $\mathbb{F}_2[X]$ de grau més petit que 3. Prenem $m = n - 3$.

1. Si $m \equiv 2, 4 \pmod 8$, $h(X) = X^m + X^3 + 1$ satisfà (iii).

2. Si $m \equiv 6 \pmod 8$, els polinomis $X^m + X + 1$ i $X^m + X^5 + 1$ no tenen factors comuns a $\mathbb{F}_2[X]$, donat que la seva diferència és $X(X+1)^4$; com a mínim un d'ells satisfà (iii).

3. Si $m \equiv 0 \pmod 8$ i $m - 6 > 9$, els polinomis $h_1(X) = X^{m-6} + X + 1$, $h_2(X) = X^{m-6} + X^5 + 1$ i $h_3(X) = X^{m-6} + X^9 + 1$ són dos a dos coprimers a $\mathbb{F}_2[X]$, donat que les seves diferències només tenen factors X i $X + 1$. Com a mínim un dels polinomis $(X^6 + X + 1)h_i(X)$, $i \in \{1, 2, 3\}$, satisfà (iii). Notem que, en els casos $m = 16, 24$, un d'aquests tres polinomis no té discriminant $\equiv 5 \pmod 8$ (per ser $m - 6 = 2k$); en aquests casos, però, un dels dos polinomis restants satisfà (iii).
   Si $m = 8$, $h(X) = X^8 + X^4 + X^3 + X + 1$ satisfà (iii).

Hem vist, doncs, l'existència d'algun polinomi $h_0(X)$ satisfent les condicions (i), (ii) i (iii).

Per a obtenir la condició (iv), considerem el polinomi

$$h_M(X) := h_\infty(X) + \frac{1}{M}(h_0(X) - h_\infty(X)),$$

on $h_\infty(X)$ és qualsevol polinomi separable i mònic de $\mathbb{Z}[X]$ de grau $n - 3$ i amb totes les arrels reals. Quan $M \in \mathbb{Z}$ és prou gran, totes les arrels de $h_M(X)$ també hauran de ser reals, donat que les arrels d'un polinomi depenen contínuament dels seus coeficients (cf. [Nar90, Lemma 2.1]). Així, prenent $M \equiv 1 \pmod{8\,l \prod_{p \in S} p}$ prou gran, el polinomi

$$h(X) = M^{n-3} h_M(\frac{X}{M}) \in \mathbb{Z}[X]$$

satisfà totes les condicions desitjades, donat que totes les seves arrels són reals, $h(X) \equiv h_0(X) \pmod 8$ i $h(X) \equiv h_0(X) \pmod p$ per a tot $p \in S \cup \{l\}$. □

Lema 4.3.2. *Sigui $n \geq 7$ un natural senar i sigui $l \notin S$ un primer tal que $l \equiv 1 \pmod{n-1}$. Sigui $h(X) \in \mathbb{Z}[X]$ un polinomi com en el Lema 4.3.1. Aleshores, existeix algun polinomi mònic $g(X)$ a $\mathbb{Z}[X]$ de grau 2 satisfent les condicions següents:*

(i) $g(X)h(X) \equiv X^{n-1} - 1 \pmod{l}$,

(ii) $g(X)$ *és irreductible a* $\mathbb{F}_p[X]$, *per a tot* $p \in S \cup \{2\}$,

(iii) $g(X)h(X)$ *té discriminant quadrat a* $\mathbb{Z}$.

Demostració. Com que, per hipòtesi, $h(X)$ divideix $X^{n-1}-1$ a $\mathbb{F}_l[X]$, existeix algun polinomi

$$g_0(X) = X^2 + a_0X + b_0 \in \mathbb{Z}[X]$$

satisfent la condició (i). És clar que podem suposar que $g_0(X)$ també satisfà (ii), per ser $l \notin S \cup \{2\}$.

Els coeficients a_0, b_0 del polinomi $g_0(X)$ hauran de ser enters senars (per (ii)) i, per tant, el discriminant de $g_0(X)$ és $D(g_0(X)) \equiv 5 \pmod{8}$. De la condició (iii) del Lema 4.3.1 obtenim

$$D(g_0(X)) \equiv D(h(X)) \pmod{8}.$$

D'altra banda, com que el polinomi $X^{n-1} - 1$ té $n-1$ arrels diferents a $\mathbb{F}_l$, el seu discriminant és un residu quadràtic mòdul l. Per la condició (i) sobre $g_0(X)$, tenim

$$\left(\frac{D(g_0(X))}{l}\right) = \left(\frac{D(h(X))}{l}\right) \neq 0.$$

Tenint en compte que, per a tot $p \in S$ senar, $g_0(X)$ i $h(X)$ són polinomis irreductibles a $\mathbb{F}_p[X]$ de grau parell, s'obté

$$\left(\frac{D(g_0(X))}{p}\right) = \left(\frac{D(h(X))}{p}\right) = 1.$$

En resum, per a tot $p \in S \cup \{l\}$ senar, es té

$$\left(\frac{D(g_0(X))}{p}\right) = \left(\frac{D(h(X))}{p}\right) \neq 0\ .$$

D'aquesta manera, haurà de ser

$$D(g_0(X)) \equiv q^2 D(h(X)) \pmod{8\,l \prod_{p\in S} p},$$

per algun primer $q \notin S \cup \{2, l\}$. Per tant, $q^2 D(h(X)) = {a_0}^2 - 4b$, per algun enter $b \equiv b_0 \pmod{2\,l \prod_{p\in S} p}$.

El polinomi $g(X) = X^2 + a_0 X + b \in \mathbb{Z}[X]$ satisfà les condicions (i), (ii) i (iii), donat que

$$D(g(X)h(X)) = (q\, D(h(X))R(g,h))^2$$

i, per a tot $p \in S \cup \{2, l\}$,

$$g(X) \equiv g_0(X) \pmod{p}.$$

□

Proposició 4.3.3. *Sigui $n \geq 3$ un natural senar i sigui $l \notin S \cup \{n\}$ un primer tal que $l \equiv 1 \pmod{n-1}$. Aleshores, existeix algun polinomi mònic $P(X) \in \mathbb{Z}[X]$ de grau n satisfent les condicions següents:*

(i) *$P(X)$ té discriminant quadrat a $\mathbb{Z}$ i satisfà $P(X) \equiv X^n - X \pmod{l}$,*

(ii) *el discriminant de $P(X)$ no és divisible per cap primer de S,*

(iii) *totes les arrels de $P(X)$ són reals,*

(iv) *quan $n \geq 5$, $P(X)$ té alguna arrel racional.*

Demostració. Si $n \geq 7$ i $h(X)$, $g(X)$ són polinomis obtinguts dels Lemes 4.3.1 i 4.3.2, el polinomi $P(X) = Xh(X)g(X)$ satisfà les condicions enunciades, donat que:

- $P(X) \equiv X^n - X \pmod{l}$, per (i) del Lema 4.3.2,
- $D(P(X))$ és un quadrat a $\mathbb{Z}$, per (iii) del Lema 4.3.2,

- $D(P(X))$ no és divisible per cap $p \in S$, donat que $P(X)$ no té factors múltiples mòdul p, per (ii), (iii) del Lema 4.3.1 i per (ii) del Lema 4.3.2,
- les arrels de $P(X)$ són totes reals, per (iv) del Lema 4.3.1 i per ser $D(g(X)) > 0$ (donat que $D(g(X)h(X))$, $D(h(X)) > 0$).

Només falta considerar, doncs, els casos $n = 3, 5$.

Cas $n = 5$

Recordem que $D(X^3 + AX + AB) = A^2(-27B^2 - 4A)$.

Triem un polinomi $g_0(X) = X^3 + a_0X + a_0b_0$ in $\mathbb{Z}[X]$ tal que:

$$g_0(X) \equiv \begin{cases} X^3 - X + 1 \pmod 6 \\ X^3 - X \pmod p, \text{ per a tot } p \in S \cup \{l\},\ p \neq 2, 3 \end{cases}$$

Notem que $D(g_0(X)) \equiv 1 \pmod 8$ i, per a tot primer senar $p \in S \cup \{3, l\}$, es té $\left(\frac{D(g_0(X))}{p}\right) = 1$. Així, del Teorema de Dirichlet dels primers en progressió aritmètica, s'obté que existeix algun primer $q \notin S \cup \{2, 3, l\}$ tal que

$$q^2 \equiv -27{b_0}^2 - 4a_0 \pmod 8$$

i, per a tot $p \in S \cup \{3, l\}$,

$$q^2 \equiv -27{b_0}^2 - 4a_0 \pmod p.$$

Per tant, per algun enter $a \equiv a_0 \pmod p$, per a tot $p \in S \cup \{2, 3, l\}$, es té

$$q^2 = -27{b_0}^2 - 4a.$$

El polinomi $g(X) := X^3 + aX + ab_0$ té discriminant $D(g(X)) = (qa)^2$, que és un quadrat a $\mathbb{Z}$, i totes les seves arrels són reals. A més, $g(X) \equiv g_0(X) \pmod p$ per a tot $p \in S \cup \{2, 3, l\}$.

Com que $l \equiv 1 \pmod 4$, -1 és un quadrat mòdul l i, per tant, existeixen enters $c, d \in \mathbb{Z}$ tals que:

$$(X - c)(X - d) \equiv \begin{cases} X(X + 1) \pmod 6 \\ X^2 + 1 \pmod l \\ (X - 2)(X + 2) \pmod p, \text{ per a tot } p \in S,\ p \neq 2, 3 \end{cases}$$

El polinomi $P(X) = (X-c)(X-d)g(X)$ satisfà les condicions enunciades.

Cas $n = 3$

En aquest cas, no considerem la condició (iv). Amb les notacions del cas $n = 5$, el polinomi $P(X) = g(X)$ satisfà les condicions (i), (ii) i (iii). □

4.4 Polinomis totalment reals amb discriminant no divisible pels primers de S i grup de Galois alternat

Ara ja podem demostrar el resultat principal d'aquest capítol.

Teorema 4.4.1. *Sigui n un natural i sigui S un conjunt finit de primers racionals qualsevol. Aleshores, existeixen infinits polinomis mònics a $\mathbb{Z}[X]$ de grau n amb grup de Galois A_n sobre $\mathbb{Q}$, discriminant no divisible per cap primer de S i amb totes les arrels reals. A més, com a cossos de descomposició d'aquests polinomis s'obtenen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, amb grup de Galois A_n i no ramificades en els primers de $S \cup \{\infty\}$.*

Demostració. Sense pèrdua de generalitat podem suposar $2 \in S$.

Demostrarem l'existència d'un polinomi $f(T, X)$ a $\mathbb{Q}(T)[X]$ tal que:

(i) $f(T, X)$ és un polinomi mònic de grau n en X,

(ii) $f(T, X)$ defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois A_n,

(iii) per algun $t_0 \in \mathbb{Q}$, $f(t_0, X)$ és un polinomi ben definit de $\mathbb{Z}[X]$ amb totes les arrels reals i amb discriminant no divisible per cap primer $p \in S$.

D'aquí s'obté el Teorema 4.4.1 de la forma següent.

Considerem el conjunt

$$H = \{\, t \in \mathbb{Q} \text{ tal que } f(t,X) \in \mathbb{Q}[X] \text{ i } \mathrm{Gal}_{\mathbb{Q}}(f(t,X)) \cong A_n\}.$$

Per la condició (iii), si $t_1 \in H$ és prou proper a t_0 en $\mathbb{R} \times \prod_{p\in S} \mathbb{Q}_p$, aleshores el polinomi $f(t_1,X) \in \mathbb{Q}[X]$ té totes les arrels reals i $v_p(D(f(t_1,X))) = 0$, per a tot $p \in S$. Per a $M \in \mathbb{Z}$ convenient, $M^n f(t_1, \frac{X}{M})$ és un polinomi de $\mathbb{Z}[X]$, amb discriminant no divisible per cap primer de S i amb totes les arrels reals. Evidentment, el seu cos de descomposició sobre $\mathbb{Q}$ coincideix amb el de $f(t_1,X)$.

La condició (ii) i el Teorema d'Irreductibilitat de Hilbert (veure Proposició 1.3.5) garanteixen l'existència d'infinits $t \in H$, tan propers a t_0 com volguem, de manera que els cossos de descomposició sobre $\mathbb{Q}$ dels polinomis $f(t,X)$ defineixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos.

És suficient veure, doncs, l'existència d'un polinomi $f(T,X)$ de $\mathbb{Q}(T)[X]$ satisfent les condicions (i), (ii) i (iii). Per a cada natural senar $n \geq 3$, triem un nombre primer $l \notin S \cup \{n\}$ tal que $l \equiv 1 \pmod{n-1}$.

Cas $n \geq 3$ senar

Considerem un polinomi $P(X) \in \mathbb{Z}[X]$ de grau n com a la Proposició 4.3.3. En particular, $P(X)$ satisfà les hipòtesis del Corol.lari 4.2.2 i, per tant, existeix un polinomi $Q(X) \in \mathbb{Z}[X]$ de grau més petit o igual que $n-1$ tal que $F(T,X) = P(X) - TQ(X)$ defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois A_n. Així, $F(T,X)$ és un polinomi de $\mathbb{Q}(T)[X]$ satisfent les condicions (i), (ii) i (iii) (amb $t_0 = 0$).

Cas $n \geq 4$ parell

El raonament anterior aplicat al natural senar $n+1$ ens proporciona polinomis $P(X)$, $Q(X)$ de $\mathbb{Z}[X]$ tals que $F(T,X) = P(X) - TQ(X)$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ amb grup de Galois A_{n+1}.

Si $U \in \overline{\mathbb{Q}(T)}$ és una arrel de $F(T,X) \in \mathbb{Q}(T)[X]$ com a polinomi en X, aleshores $T = \frac{P(U)}{Q(U)}$. Per tant, $\mathbb{Q}(T,U) = \mathbb{Q}(U)$ és el cos fix per algun subgrup $A_n \subset A_{n+1}$, en el cos de descomposició de $F(T,X)$ sobre $\mathbb{Q}(T)$. D'aquesta manera, el cos de descomposició sobre $\mathbb{Q}(U)$ del polinomi

$$G(U,X) = \frac{F\left(\frac{P(U)}{Q(U)}, X\right)}{X-U} = \frac{P(X) - \frac{P(U)}{Q(U)}Q(X)}{X-U}$$

defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(U)$ amb grup de Galois A_n.

Com que $P(X)$ és un polinomi de grau $n+1 \geq 5$ obtingut de la Proposició 4.3.3, $(X-u_0)$ divideix $P(X)$, per algun $u_0 \in \mathbb{Z}$. Concretament, $u_0 = 0$ si $n+1 \geq 7$, i $u_0 = c$ si $n+1 = 5$ (amb les notacions de la Proposició 4.3.3). Com que els polinomis $P(X)$ i $Q(X)$ són coprimers (a $\mathbb{Q}[X]$), haurà de ser $P(u_0) = 0$, $Q(u_0) \neq 0$ i, per tant, $G(u_0, X) = \frac{P(X)}{X-u_0}$.

En conclusió, el polinomi $G(T,X)$ de $\mathbb{Q}(T)[X]$ satisfià les condicions (i), (ii) i (iii) (amb $t_0 = u_0$). □

Corol.lari 4.4.2. *Per a tot natural $n \geq 3$ existeixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, amb grup de Galois isomorf a A_n i moderadament ramificades.*

La construcció del polinomi $P(X)$ de la secció 4.3 ha estat essencial, en la conclusió del Teorema 4.4.1, per a realitzar A_n com a grup de Galois d'alguna extensió $K/\mathbb{Q}$ que s'obté com a cos de descomposició d'un polinomi mònic de $\mathbb{Z}[X]$ amb discriminant no divisible per cap primer de S. El Corol.lari anterior, però, només fa referència al comportament dels primers de $S \cup \{\infty\}$ en l'extensió $K/\mathbb{Q}$. També es pot obtenir com a conseqüència, per exemple, del resultat següent.

Teorema 4.4.3. *Sigui n un natural i sigui S un conjunt finit de primers racionals qualsevol. Aleshores, existeixen infinites A_n-extensions de $\mathbb{Q}$ en les quals tots els primers de $S \cup \{\infty\}$ descomponen completament.*

Demostració. És suficient raonar com a la demostració del Teorema 4.4.1, tenint en compte que:

(a) Per a qualsevol senar n, sempre existeixen $x_1, \dots, x_n \in \mathbb{Q}$ tals que el polinomi $P(X) = \prod_i (X - x_i)$ és H-general. Això és evident si pensem en $H(T_1, \dots, T_n)$ com a polinomi (no nul) en les arrels del polinomi genèric de grau n, $X^n + T_1 X^{n-1} + \cdots + T_n$. Alternativament, es pot usar el Corol.lari 4.2.2 (cf. [Mes90, Rem. 1]).

(b) Per la Proposició 5.2.2, si $P(X)$ és com a (a) i $t \in \mathbb{Q}$ és prou proper a 0 en $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$, aleshores els primers de $S \cup \{\infty\}$ descomponen completament en el cos de descomposició sobre $\mathbb{Q}$ de $P(X) - tQ(X)$.

□

A la Secció 6.3 obtindrem una generalització d'aquest resultat.

Observació 4.4.4. *Convé esmentar que els casos $n = 3, 4, 5$ admeten un argument específic. Precisament A_3, A_4 i A_5 són els únics grups alternats per als quals es coneix una resposta afirmativa al Problema de Noether. És a dir, si $X_1, \dots, X_n$ denoten indeterminades, aquests són els únics casos per als quals és conegut que el cos fix $\mathbb{Q}(X_1, \dots, X_n)^{A_n}$ definieix una extensió transcendent pura de $\mathbb{Q}$. Això implica, per a aquests grups, l'existència de polinomis genèrics sobre $\mathbb{Q}$ (veure Secció 5.2). Així, per a $n = 3, 4, 5$, el Teorema anterior no és res més que un cas particular d'un resultat de tipus Grunwald-Wang que Saltman [Sal82] dedueix de l'existència de polinomis genèrics (veure Teorema 5.2.9).*

Capítol 5

Especialització i ramificació moderada

5.1 Introducció

En aquest capítol ens interessem per la possibilitat d'obtenir, per especialització d'alguna realització d'un grup finit G com a grup de Galois sobre $\mathbb{Q}(T)$, realitzacions de G com a grup de Galois d'extensions de $\mathbb{Q}$ no ramificades en els primers d'un conjunt finit prefixat S. A diferència dels dos capítols anteriors, no ens preocuparem de que aquestes extensions es puguin obtenir com a cossos de descomposició de polinomis mònics de $\mathbb{Z}[X]$ amb discriminant no divisible per cap primer de S. Com en gran part de la memòria, ens interessarà especialment l'obtenció d'extensions moderadament ramificades de $\mathbb{Q}$ amb grup de Galois prefixat.

Per a certs grups finits, l'anomenat mètode de la rigidesa proporciona realitzacions galoisianes regulars sobre $\mathbb{Q}(T)$ (cf. [MM99]). Birch suggereix que, en general, les especialitzacions d'aquestes extensions seran salvatgement ramificades (cf. [Bir94, pàg. 35]). Un dels objectius d'aquest capítol és considerar aquesta qüestió per alguns exemples concrets. La conclusió és que, en els ex-

emples tractats, la no existència d'especialitzacions moderadament ramificades no sembla provenir del fet que les realitzacions considerades s'hagin construït pel mètode de la rigidesa.

Comencem la Secció 5.2 observant que, donada una realització galoisiana d'un grup finit G sobre $\mathbb{Q}(T_1, \ldots, T_d)$, l'existència d'alguna especialització racional de $(T_1, \ldots, T_d)$ amb condicions de ramificació prefixades en els primers d'un conjunt finit S és essencialment suficient per a garantir l'existència d'altres especialitzacions amb el mateix comportament en S i amb grup de Galois G. Aquest fet ens permet demostrar que, si per a prous cossos de nombres K existeix un polinomi irreductible a $\mathbb{Q}(T_1, \ldots, T_d)[X]$ que parametritza totes les G-extensions de K, aleshores G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$ en les quals els primers d'un conjunt finit prefixat qualsevol descomponen completament. En particular, els grups que satisfan la hipòtesi anterior sempre es realitzen com a grups de Galois d'extensions moderadament ramificades de $\mathbb{Q}$. Quan existeix un polinomi genèric per a G-extensions sobre $\mathbb{Q}$, aquest fet és un cas particular d'un resultat de tipus Grunwald-Wang establert per Saltman [Sal82].

A la Secció 5.3 utilitzem la teoria dels polígons de Newton per a estudiar l'existència de "bones"especialitzacions d'alguns exemples d'extensions de $\mathbb{Q}(T)$, obtingudes pel mètode de la rigidesa. En primer lloc considerem realitzacions regulars conegudes sobre $\mathbb{Q}(T)$ dels dos grups esporàdics simples més petits: els grups de Mathieu M_{11} i M_{12}. La realització de M_{12} correspon a (la clausura galoisiana d') un recobriment de grau 12 de $\mathbb{P}^1$ per $\mathbb{P}^1$, definit sobre $\mathbb{Q}$. La realització d'M_{11} s'obté de l'anterior, amb un raonament anàleg al fet a la secció 4.4 per a A_n i A_{n+1} en el cas n parell. En tots dos casos obtenim, per a qualsevol conjunt finit de primers S, l'existència d'especialitzacions no ramificades en $S\backslash\{5\}$ i moderadament ramificades en $p = 5$. En particular, M_{11} i M_{12} admeten realitzacions moderadament ramificades sobre $\mathbb{Q}$. El prob-

lema 3 plantejat a la Introducció de la memòria admet, doncs, una resposta afirmativa per a aquests grups.

També considerem una realització regular coneguda del grup $\mathrm{Aut}(M_{22})$ sobre $\mathbb{Q}(T)$ i veiem que admet especialitzacions moderadament ramificades sobre $\mathbb{Q}$ amb grup de Galois $\mathrm{Aut}(M_{22})$. Del fet que es tracti d'una extensió de $\mathbb{Q}(T)$ ramificada en només tres primers de grau 1, se'n dedueix una realització regular de M_{22} (subgrup d'índex 2 de $\mathrm{Aut}(M_{22})$) sobre $\mathbb{Q}(T)$, que provem que no admet cap especialització moderadament ramificada sobre $\mathbb{Q}$ amb grup de Galois M_{22}. Tal com observem a la Secció 5.3.3, aquesta situació és paral.lela al fet que, per a $n \equiv 4 \pmod 8$, existeixen extensions trinomials de $\mathbb{Q}$ moderadament ramificades amb grup de Galois S_n i, en canvi, no n'hi ha amb grup de Galois A_n (Capítol 3).

5.2 Especialitzacions amb condicions de ramificació prefixades

Per a cada primer p suposem fixada $\overline{\mathbb{Q}_p}$, una clausura algebraica de $\mathbb{Q}_p$.

Una conseqüència típica del Lema de Krasner és que dos polinomis irreductibles a $\mathbb{Q}_p[X]$ del mateix grau tenen el mateix cos de descomposició sobre $\mathbb{Q}_p$, sempre que siguin prou propers p-àdicament. D'altra banda, com més propers són dos polinomis separables (discriminant no nul) de $\mathbb{Q}_p[X]$ del mateix grau, més properes són les seves descomposicions en producte d'irreductibles. Així s'obté (cf., per exemple, [NSW00, Lemma 12.1.1] o [Sal82, Lemma 5.5]):

Proposició 5.2.1. *Sigui $f(X) \in \mathbb{Q}_p[X]$ un polinomi amb discriminant no nul. Suposem que $g(X) \in \mathbb{Q}_p[X]$ és un polinomi del mateix grau que $f(X)$ i tal que,*

per algun natural s, es té:

$$g(X) \equiv f(X) \pmod{p^s}.$$

Si s és prou gran, aleshores els cossos de descomposició de $g(X)$ i $f(X)$ sobre $\mathbb{Q}_p$ coincideixen. De fet, si $\{\alpha_i\}$ són les arrels de $f(X)$, aleshores les arrels $\{\beta_i\}$ de $g(X)$ es poden ordenar de manera que $\mathbb{Q}_p(\alpha_i) = \mathbb{Q}_p(\beta_i)$, per a tot i.

Del Teorema d'Irreductibilitat de Hilbert (Proposicions 1.3.3 i 1.3.5) i del resultat anterior, l'anàleg real del qual és clar (cf., per exemple, [Nar90, Lemma 2.1]), obtenim:

Proposició 5.2.2. *Sigui $f(T_1, \dots, T_d, X) \in \mathbb{Q}(T)[X]$ un polinomi mònic irreductible en X, on $T_1, \dots, T_d$ són indeterminades. Sigui S un conjunt finit de primers qualsevol i, per a cada $p \in S$ (resp. $p = \infty$), suposem donat $t_p \in {\mathbb{Q}_p}^d$ (resp. $t_\infty \in \mathbb{R}^d$) tal que $f_p(X) := f(t_p, X)$ és un polinomi ben definit a $\mathbb{Q}_p[X]$ (resp. a $\mathbb{R}[X]$). Si el discriminant de $f_p(X)$ és no nul, per a tot $p \in S \cup \{\infty\}$, aleshores:*

(i) Existeixen infinits $t \in \mathbb{Q}^d$ tals que $f(X) := f(t, X)$ és un polinomi ben definit a $\mathbb{Q}[X]$ que satisfà:

- $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong \mathrm{Gal}_{\mathbb{Q}(T_1,\dots,T_d)}(f(T_1, \dots, T_d, X))$,
- $(\mathbb{Q}_p)_f = (\mathbb{Q}_p)_{f_p}$, *per a tot $p \in S$,*
- $\mathbb{R}_f = \mathbb{R}_{f_\infty}$.

En particular, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $S \cup \{\infty\}$ (respectivament, moderadament ramificada) si ho són les extensions $(\mathbb{R})_{f_\infty}/\mathbb{R}$ i $(\mathbb{Q}_p)_{f_p}/\mathbb{Q}_p$, per a tot $p \in S$.

(ii) Si, a més, el cos de descomposició de $f(T_1, \dots, T_d, X)$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T_1, \dots, T_d)$, aleshores existeixen infinits $t \in \mathbb{Q}^d$ com a (i) definint infinites extensions de $\mathbb{Q}$ linealment disjuntes.

Observació 5.2.3. *Aquesta Proposició s'aplica, en particular, quan* $t_p = t_0 \in \mathbb{Q}^d$*, per a tot* $p \in S \cup \{\infty\}$*. En aquest cas, el resultat estableix que tot comportament local dels primers de* $S \cup \{\infty\}$ *en alguna especialització* $t_0 \in \mathbb{Q}^d$ *tal que* $D(f(t_0, X)) \neq 0$*, també es dóna en alguna especialització amb grup de Galois* $\mathrm{Gal}_{\mathbb{Q}}(f(t_0, X)) \cong \mathrm{Gal}_{\mathbb{Q}(T)}(f(T, X))$*.*

El resultat anterior jugarà un paper clau a l'hora d'obtenir realitzacions sobre $\mathbb{Q}$ de certs grups finits amb condicions de ramificació prefixades en un nombre finit de primers.

5.2.1 Polinomis paramètrics i polinomis genèrics

Les següents definicions es troben, per exemple, a [Led00a] (veure també [JLY02]).

Definició 5.2.4. *Siguin* K *un cos i* G *un grup finit. Direm que un polinomi mònic* $P(T_1, \ldots, T_d, X) \in K(T_1, \ldots, T_d)[X]$ *és* ***paramètric per a*** G***-extensions sobre*** K *quan satisfà les dues condicions següents:*

(i) $\mathrm{Gal}_{K(T_1,\ldots,T_d)}(P(T_1, \ldots, T_d, X)) \cong G$*,*

(ii) tota G*-extensió de* K *es pot obtenir com a cos de descomposició sobre* K *de* $P(a, X)$ *per algun* $a \in K^d$*.*

Definició 5.2.5. *Direm que un polinomi* $P(T_1, \ldots, T_d, X) \in K(T_1, \ldots, T_d)[X]$ *és* ***genèric per a*** G***-extensions sobre*** K *si és paramètric per a* G*-extensions sobre qualsevol cos que conté* K*.*

L'existència d'un polinomi genèric per a G-extensions sobre $\mathbb{Q}$ és una hipòtesi força restrictiva. Per a un grup abelià finit G, equival a que G no tingui cap element d'ordre 8 (cf. [Sal82]).

Aquesta condició és certa, per exemple, sempre que es té una resposta afirmativa al problema de Noether per a $G \subseteq S_n$; és a dir, quan el cos $\mathbb{Q}(X_1, \ldots, X_n)^G$ és racional sobre $\mathbb{Q}$ (cf. [Kuy64, Thm. 1]).

També es coneix l'existència de polinomis genèrics sobre $\mathbb{Q}$ per a alguns grups diedrals (cf. [Sal82] i [Bla99a]).

Observació 5.2.6.

1. *Quan K és un cos infinit, les condicions següents són equivalents (cf. [DeM83] i [Led00b]):*

   (a) *Existeix un polinomi genèric per a G-extensions sobre K.*

   (b) *Existeix una G-extensió genèrica sobre K (per a la definició, veure [Sal82]).*

   (c) *Existeix un polinomi irreductible a $K(T_1, \ldots, T_d)[X]$ que és genèric per a G-extensions sobre K.*

   (d) *Existeix un polinomi $P(T_1, \ldots, T_d, X)$ **G-descent-genèric sobre** K; és a dir, si $H \subseteq G$ és un subgrup qualsevol i L és un cos que conté K, aleshores tota H-extensió de L s'obté per especialització de $P(T_1, \ldots, T_d, X)$ en algun $a \in L^d$.*

   De fet, a [Kem01] es prova que tot polinomi genèric per a G-extensions sobre un cos infinit K és G-descent-genèric sobre K.

2. *El cos de descomposició d'un polinomi $P(T_1, \ldots, T_d, X)$, genèric sobre K, sempre defineix una extensió K-regular de $K(T_1, \ldots, T_d)$. Això és clar quan K és infinit donat que la propietat descent-genèric garanteix l'existència d'algun $t \in K^d$ tal que $P(t, X)$ té totes les arrels a K.*

Teorema 5.2.7. *Sigui $n \geq 5$ un natural, G un subgrup del grup alternat A_n i S un conjunt finit de primers racionals qualsevol. Suposem que G es realitza com a grup de Galois d'alguna extensió de $\mathbb{Q}$. Suposem també que, per a cada cos de nombres L de grau $[L : \mathbb{Q}] = (A_n : G)$, existeix un polinomi irreductible $f(T_1, \ldots, T_d, X) \in \mathbb{Q}(T_1, \ldots, T_d)[X]$ que és paramètric per a G-extensions sobre L. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$ linealment disjuntes en les quals els primers de $S \cup \{\infty\}$ descomponen completament. En particular, G es realitza com a grup de Galois d'infinites extensions moderadament ramificades de $\mathbb{Q}$.*

Demostració. Pel Teorema 4.4.3, existeix alguna extensió de Galois $K/\mathbb{Q}$ tal que:

- $\mathrm{Gal}(K/\mathbb{Q}) \cong A_n$,
- els primers de $S \cup \{\infty\}$ descomponen completament a $K/\mathbb{Q}$.

A partir d'ara, suposem $\{1\} \subsetneq G \subsetneq A_n$. Per hipòtesi, existeix un polinomi $f(T_1, \ldots, T_d, X) \in \mathbb{Q}(T_1, \ldots, T_d)[X]$ que és paramètric per a G-extensions sobre el cos fix K^G. L'extensió K/K^G té grup de Galois

$$\mathrm{Gal}(K/K^G) \cong G$$

i, per tant, existeix algun $\alpha_0 \in (K^G)^d$ tal que K és el cos de descomposició de $f(\alpha_0, X)$ sobre K^G.

També per hipòtesi, existeix alguna extensió $M/\mathbb{Q}$ amb grup de Galois G. Com que el grup A_n és simple ($n \geq 5$), l'extensió $K/\mathbb{Q}$ no admet subextensions galoisianes no trivials i, en particular, les extensions $K/\mathbb{Q}$ i $M/\mathbb{Q}$ són linealment disjuntes. Així, les extensions MK^G/K^G i K/K^G són linealment disjuntes i totes dues tenen grup de Galois isomorf a G. Tenint en compte que el polinomi $f(T_1, \ldots, T_d, X)$ és paramètric per a G-extensions de K^G, obtenim que el cos de descomposició sobre $K^G(T_1, \ldots, T_d)$ de $f(T_1, \ldots, T_d, X)$ defineix una extensió K^G-regular de $K^G(T_1, \ldots, T_d)$. En particular,

$$\mathbb{Q}(T_1, \ldots, T_d)_{f(T_1, \ldots, T_d, X)} \cap K \subseteq K^G.$$

Tornant a usar el fet que A_n és un grup simple, ara és clar que es té:

$$\mathbb{Q}(T_1,\dots,T_d)_{f(T_1,\dots,T_d,X)}\cap K=\mathbb{Q}=\mathbb{Q}(T_1,\dots,T_d)_{f(T_1,\dots,T_d,X)}\cap K^G.$$

Per tant, es tenen isomorfismes

$$\mathrm{Gal}_{K^G(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X))\cong G\cong \mathrm{Gal}_{\mathbb{Q}(T_1,\dots,T_d)}(f(T_1,\dots,T_d,X)).$$

Per força, l'extensió $\mathbb{Q}(T_1,\dots,T_d)_{f(T_1,\dots,T_d,X)}/\mathbb{Q}(T_1,\dots,T_d)$ és $\mathbb{Q}$-regular. Observem també que $f(\alpha_0,X)$ és un polinomi irreductible a $K^G[X]$, donat que $\mathrm{Gal}_{K^G}(f(\alpha_0,X))\cong G$ i, per hipòtesi, $f(T_1,\dots,T_d,X)$ és un polinomi irreductible a $\mathbb{Q}(T_1,\dots,T_d)[X]$. En particular, $D(f(\alpha_0,X))\neq 0$.

Sigui $p\in S$. Per elecció de K, p descompon completament a $K/\mathbb{Q}$ i, en particular, a $K^G/\mathbb{Q}$. Així, si $\mathfrak{p}$ és un primer de (l'anell d'enters de) K^G que divideix p, aleshores podem pensar

$$\alpha_0\in (K^G)^d\subseteq ((K^G)_{\mathfrak{p}})^d=(\mathbb{Q}_p)^d$$

i, per força, $(\mathbb{Q}_p)_{f(\alpha_0,X)}=\mathbb{Q}_p$. D'aquesta manera, si $t_0\in\mathbb{Q}^d$ satisfà $t_0\equiv\alpha_0 \pmod{p^m}$ amb m prou gran, aleshores $(\mathbb{Q}_p)_{f(t_0,X)}=\mathbb{Q}_p$ (Proposició 5.2.1).

D'altra banda, si $t_0\in\mathbb{Q}^d$ és prou proper a $\alpha_0\in(K^G)^d\subseteq\mathbb{R}^d$ respecte la topologia real, aleshores $f(t_0,X)$ tindrà totes les arrels reals i diferents (les de $f(\alpha_0,X)$ ho són, donat que $K\subseteq\mathbb{R}$ i $D(f(\alpha_0,x))\neq 0$).

En resum, existeix algun $t_0\in\mathbb{Q}^d$ tal que $D(f(t_0,X))\neq 0$ i el cos de descomposició de $f(t_0,X)$ sobre $\mathbb{Q}$ és un cos totalment real en el qual descomponen completament tots els primers de S. L'apartat (i) de la Proposició 5.2.2 (i l'Observació 5.2.3) ens permet concloure que existeix algun $t_1\in\mathbb{Q}^d$ amb aquestes mateixes propietats i que, a més, satisfà

$$\mathrm{Gal}_{\mathbb{Q}}(f(t_1,X))\cong G.$$

És clar que, aplicant successivament l'argument anterior a diferents conjunts S ben triats, s'obté la infinitud enunciada. Per la Proposició 5.2.2 (ii), això també s'obté del fet que el cos de descomposició de $f(T_1,\dots,T_d,X)$ defineix una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T_1,\dots,T_d)$. □

Observació 5.2.8. *Sobre les hipòtesis en el resultat anterior convé remarcar:*

- *Que G sigui un subgrup de A_n, per algun n, no suposa cap restricció.*
- *Assumir, d'una manera o d'una altra, una resposta afirmativa al problema invers de la teoria de Galois sobre $\mathbb{Q}$ per a G és imprescindible si volem una conclusió com l'enunciada.*
- *No han estat realment essencials ni el caràcter irreductible ni el caràcter paramètric de $f(T_1, \ldots, T_d, X)$. Hagués estat suficient suposar que l'extensió $L(T_1, \ldots, T_d)_{f(T_1,\ldots,T_d,X)}/L(T_1, \ldots, T_d)$ no era constant i, amb les notacions de la demostració, $D(f(\alpha_0, X)) \neq 0$.*
- *Enlloc de A_n, podíem haver considerat algun altre grup no necessàriament simple com, per exemple, el grup simètric S_n. En aquest cas, haguéssim hagut d'afegir alguna hipòtesi per a garantir que el grup de Galois de $f(T_1, \ldots, T_d, X)$ sobre $\mathbb{Q}(T_1, \ldots, T_d)$ fos isomorf a G.*
- *Hagués estat desitjable que l'única hipòtesi en el resultat anterior fos l'existència d'un polinomi $f(T_1, \ldots, T_d, X) \in \mathbb{Q}(T_1, \ldots, T_d)[X]$ paramètric per a G-extensions sobre $\mathbb{Q}$. Observem, però, que el resultat implica la regularitat de l'extensió $\mathbb{Q}(T_1, \ldots, T_d)_{f(T_1,\ldots,T_d,X)}/\mathbb{Q}(T_1, \ldots, T_d)$. En canvi, el caràcter paramètric sobre $\mathbb{Q}$ (a diferència del genèric) no és suficient, en principi, per a garantir aquesta propietat. Tot i així, cal esperar que aquesta regularitat sempre sigui certa; equival, per exemple, a que el grup $G \times G$ es realitzi com a grup de Galois sobre $\mathbb{Q}$.*

Si $n \leq 4$ i G és un subgrup qualsevol de A_n, aleshores existeix un polinomi genèric per a G-extensions sobre $\mathbb{Q}$ (cf. [JLY02]). En aquest cas, el Teorema anterior (per a tot S) és un cas particular del següent resultat de tipus Grunwald-Wang, que només enunciem sobre $\mathbb{Q}$.

Teorema 5.2.9. *[Sal82, Thm. 5.9] Sigui G un grup finit. Per a cada primer d'un conjunt finit qualsevol $S = \{p_i\}_i$ suposem donada una extensió de Galois $K_i/\mathbb{Q}_{p_i}$ amb $\mathrm{Gal}(K_i/\mathbb{Q}_{p_i}) \subseteq G$ i, per a $p = \infty$, suposem donada $K_\infty/\mathbb{R}$ amb $\mathrm{Gal}(K_\infty/\mathbb{R}) \subseteq G$. Si existeix un polinomi genèric per a G-extensions sobre $\mathbb{Q}$, aleshores les extensions $K_i/\mathbb{Q}_{p_i}$ (resp. $K_\infty/\mathbb{R}$) s'obtenen per compleció en p_i (resp. $p = \infty$) d'alguna extensió de Galois $K/\mathbb{Q}$ amb grup de Galois $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.*

Aquest resultat, establert per Saltman en termes d'extensions genèriques, es pot obtenir de la Proposició 5.2.2 com a conseqüència directa del fet següent, implícit a la demostració de Kemper [Kem01] de que tot polinomi genèric sobre un cos infinit és descent-genèric.

Sigui K un cos infinit i $P(T_1, \ldots, T_d, X)$ un polinomi genèric per a G-extensions sobre K, que podem suposar separable. Sigui $h(T_1, \ldots, T_d) \in K(T_1, \ldots, T_d)$ un element no nul qualsevol. Considerem un cos $L \supseteq K$ i un subgrup $H \subseteq G$. Aleshores, tota H-extensió de L s'obté com a cos de descomposició sobre L de $P(a, X)$, per algun $a \in L^d$ tal que $h(a) \neq 0$. En particular, sempre podem suposar $D(P(a, X)) \neq 0$.

5.3 Exemples: grups de Mathieu

5.3.1 Els grups M_{11} i M_{12}

Les realitzacions regulars sobre $\mathbb{Q}(T)$ dels grups de Mathieu M_{11} i M_{12} que volem especialitzar es troben a [MZM86] (també a [MM99, Chap.I,Thm.9.10 i Cor.9.11]):

Proposició 5.3.1.

(i) El següent polinomi defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois M_{12}:

$$\begin{aligned} f(T,X) \;:=\; & X^{12}+20X^{11}+162X^{10}+\frac{3348}{5}X^9+\frac{35559}{5^2}X^8+\frac{5832}{5}X^7 \\ & -\frac{84564}{5^3}X^6-\frac{857304}{5^4}X^5+\frac{807003}{5^5}X^4+\frac{1810836}{5^5}X^3 \\ & -\frac{511758}{5^6}X^2+\frac{2125764}{5^7}X+\frac{531441}{5^8}-TX^2 \end{aligned}$$

(ii) Expressant el polinomi de l'apartat (i) com $f(T,X)=h(X)-TX^2$, el següent polinomi defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois M_{11}:

$$g(T,X) \;:=\; \frac{T^2h(X)-h(T)X^2}{X-T}$$

Proposició 5.3.2. *Siguin $f(T,X)$, $g(T,X)$ els polinomis de la Proposició 5.3.1 i considerem un conjunt finit de primers qualsevol S. Aleshores:*

(i) Existeixen infinits $t\in\mathbb{Q}$ tals que els cossos de descomposició dels corresponents polinomis $f(t,X)$ defineixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, no ramificades en $S\backslash\{5\}$, moderadament ramificades en $p=5$ i amb grup de Galois M_{12}.

(ii) Existeixen infinits $t\in\mathbb{Q}$ tals que els cossos de descomposició dels corresponents polinomis $g(t,X)$ defineixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, no ramificades en $S\backslash\{5\}$, moderadament ramificades en $p=5$ i amb grup de Galois M_{11}.

Demostració. Gràcies a l'apartat (ii) de la Proposició 5.2.2, només cal veure que, per a cada $p\in S\backslash\{5\}$ (resp. $p=5$), existeix alguna especialització $t\in\mathbb{Q}$

tal que el discriminant $D(f(t,X))$ és no nul i l'extensió $\mathbb{Q}_{f(t,X)}/\mathbb{Q}$ és no ramificada en p (resp. moderadament ramificada en $p=5$). El mateix val per a $g(T,X)$.

(i) Notem $f_1(T,X) = 5^{12} f\left(T, \frac{X}{5}\right) \in \mathbb{Z}[T][X]$, és a dir,

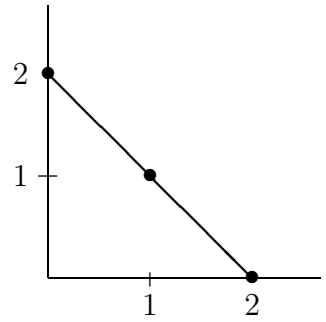
$$\begin{aligned} f_1(T,X) = {} & X^{12} + 2^2.5^2X^{11} + 2.3^4.5^2X^{10} + 2^2.3^3.31.5^2X^9 + 3^4.439.5^2X^8 \\ & +2^3.3^6.5^4X^7 - 2^2.3^6.29.5^3X^6 - 2^3.3^7.7^2.5^3X^5 + 3^9.41.5^3X^4 \\ & +2^2.3^9.23.5^4X^3 - 5^4(2.3^9.13 + 5^6T)X^2 + 2^2.3^{12}.5^4X + 3^{12}.5^4. \end{aligned}$$

Com que $D(f_1(0,X)) = 2^{144}3^{120}5^{44}$, només cal estudiar els primers 2, 3 i 5. Per a qualsevol altre primer $p \in S$, podem agafar $t \equiv 0 \pmod{p}$.

Cas $p=2$. Si $v_2(t) = 0$, la reducció mòdul 2 de $f(X) := f_1(t,X) \in \mathbb{Z}_{(2)}[X]$ és $\overline{f}(X) = (X^6+X^4+X^2+X+1)^2$. Si definim $\phi(X) = X^6+X^4+X^2+X+1$, es té la congruència

$$f(X) \equiv \phi(X)^2 + (2X + 4X^2 + 4X^5)\phi(X) + ((1-t)X^2 + 4X^3) \pmod{8}.$$

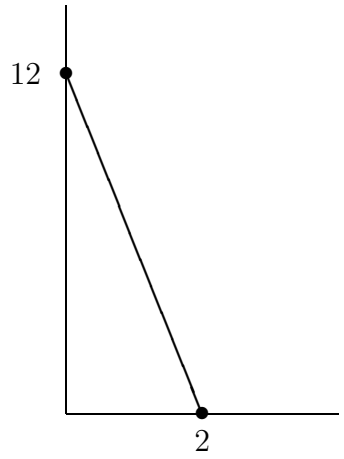
Si, a més, $t \equiv 1 \pmod{4}$, el polígon de Newton de $f(X)$ respecte $\phi(X)$ és



Així, el coeficient de grau 1 de $P_S(X)$, polinomi associat a l'únic segment de $N_\phi(f(X))$, és $\xi \in \overline{\mathbb{F}_2}$, arrel de $\overline{\phi}(X) \in \mathbb{F}_2[X]$. Per tant, el polinomi $P_S(X)$ no té arrels múltiples.

En conclusió, si $t \equiv 1 \pmod 4$ i el polinomi $f_1(t, X) \in \mathbb{Q}[X]$ és irreductible, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $p = 2$ (Proposició 1.4.6).

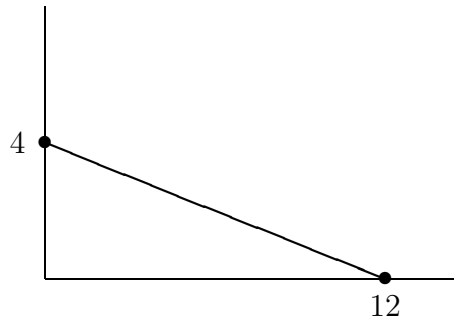
Cas $p = 3$**.** Si $v_3(t) = 0$, la reducció mòdul 3 de $f(X) = f_1(t, X) \in \mathbb{Z}_{(3)}[X]$ és $\overline{f}(X) = X^2(X^{10} + X^9 - t)$. El polinomi $X^{10} + X^9 - t \in \mathbb{F}_3[X]$ no té arrels múltiples i, per tant, el polígon de Newton de $f(X)$ respecte $\phi(X) = X$ és



El polinomi associat a l'únic segment de $N_\phi(f(X))$ és $P_S(X) = -X^2 + t \in \mathbb{F}_3[X]$ que, per ser $t \neq 0$, no té arrels múltiples.

En conclusió, si $t \equiv 1, 2 \pmod 3$ i el polinomi $f_1(t, X) \in \mathbb{Q}[X]$ és irreductible, aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $p = 3$.

Cas $p = 5$**.** Si $v_5(t) \geq -6$, la reducció mòdul 5 de $f(X) = f_1(t, X) \in \mathbb{Z}_{(5)}[X]$ és $\overline{f}(X) = X^{12}$. El polígon de Newton de $f(X)$ respecte $\phi(X) = X$ és



Si ($f(X)$ és irreductible i) $\theta \in \overline{\mathbb{Q}}$ és una arrel de $f(X)$, la Proposició 1.4.6 garanteix que els índexs de ramificació a $\mathbb{Q}(\theta)/\mathbb{Q}$ dels primers que divideixen $p = 5$ són tots múltiples de 3. Com que es tracta d'una extensió de grau 12, cap d'aquests índexs pot ser divisible per 5. Per tant, $p = 5$ ramifica moderadament a l'extensió $\mathbb{Q}(\theta)/\mathbb{Q}$.

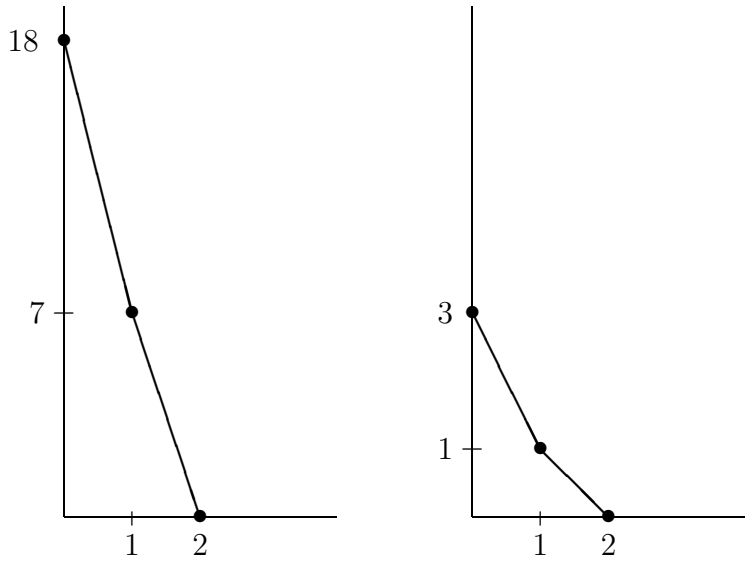
En conclusió, si $v_5(t) \geq -6$ i el polinomi $f_1(t, X) \in \mathbb{Q}[X]$ és irreductible, aleshores $p = 5$ ramifica moderadament a $\mathbb{Q}_f/\mathbb{Q}$.

(ii) És suficient estudiar les especialitzacions del polinomi mònic

$$g_1(T, X) = 5^{13}T^9 g\left(\frac{T}{5}, \frac{X}{5T}\right) \in \mathbb{Z}[T][X].$$

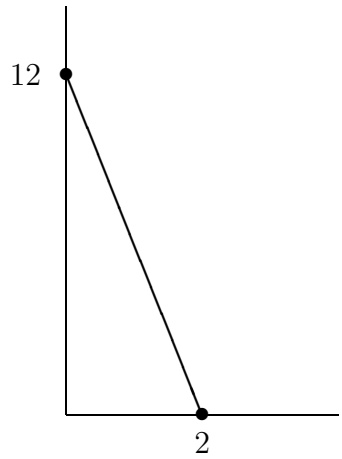
Com que $(D(g_1(1, X)), D(g_1(2, X))) = 2^{98}3^{12}5^{12}$, només cal estudiar els primers 2, 3 i 5. Per a qualsevol altre primer $p \in S$, triem $t = 1$ o $t = 2$ de manera que p no divideixi $D(g_1(t, X))$.

Cas $p = 2$. Agafem $t = \frac{1}{2}$. El polinomi mònic $g(X) = 4^{11}g_1(\frac{1}{2}, \frac{X}{4}) \in \mathbb{Z}[X]$ és irreductible i la seva reducció mòdul 2 és $\overline{g}(X) = (1 + X)X^2(1 + X + X^2 + X^3 + X^4)^2$. Els polígons de Newton de $g(X)$ respecte $\phi_1(X) = X + 2^6$ i $\phi_2(X) = X^4 + X^3 + X^2 + X + 1$ són, respectivament:



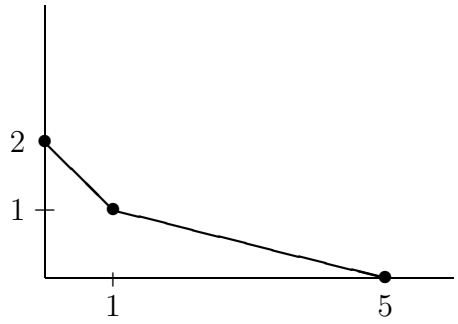
Per la Proposició 1.4.6, l'extensió $\mathbb{Q}_g/\mathbb{Q}$ és no ramificada en $p = 2$.

Cas $p = 3$**.** Agafem $t = 1$. El polinomi $g(X) = g_1(1, X) \in \mathbb{Z}[X]$ és irreductible i la seva reducció mòdul 3 és $\overline{g}(X) = X^2(X^3 + X^2 + X + 2)(X^6 + X^5 + 2X^3 + X^2 + 2X + 1)$. El polígon de Newton de $g(X)$ respecte $\phi(X) = X + 3^6$ és



El polinomi associat a l'únic segment de $N_\phi(g(X))$ és $P_S(X) = -(X^2+X+2) \in \mathbb{F}_3[X]$. Com que $P_S(X)$ no té arrels múltiples, l'extensió $\mathbb{Q}_g/\mathbb{Q}$ és no ramificada en $p = 3$.

Cas $p = 5$. Com en el cas $p = 3$, considerem $t = 1$. La reducció mòdul 5 de $g(X) = g_1(1, X)$ és $\overline{g}(X) = X^2(X + 1)^5(X + 4)^4$. El polígon de Newton de $g(X)$ respecte $\phi(X) = X + 1$ és



Si $\theta \in \overline{\mathbb{Q}}$ és una arrel de $g(X)$, cap dels índexs de ramificació a $\mathbb{Q}(\theta)/\mathbb{Q}$ dels primers que divideixen $p = 5$ és divisible per 5. Per tant, $p = 5$ ramifica moderadament a $\mathbb{Q}_g/\mathbb{Q}$. □

Corol.lari 5.3.3. *Per especialització racional de l'extensió de $\mathbb{Q}(T)$ definida pel polinomi $f(T, X)$ (resp. $g(T, X)$) de la Proposició 5.3.1 s'obtenen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, moderadament ramificades i amb grup de Galois M_{12} (resp. M_{11}).*

Observació 5.3.4. *Es pot comprovar que $p = 5$ ramifica en totes les realitzacions de M_{11} i M_{12} com a grups de Galois sobre $\mathbb{Q}$ obtingudes per especialització dels polinomis $f(T, X)$ i $g(T, X)$ de la Proposició 5.3.1.*

5.3.2 Els grups M_{22} i $\mathrm{Aut}(M_{22})$

Les realitzacions regulars de $\mathrm{Aut}(M_{22})$ i M_{22} sobre $\mathbb{Q}(T)$ que volem especialitzar es poden definir pels polinomis següents (cf. [MM99, pàg. 411]):

Proposició 5.3.5.

(i) El següent polinomi defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois $\mathrm{Aut}(M_{22})$:

$$\begin{aligned} f(T,X) &:= (5X^4+34X^3-119X^2+212X-164)^4 \\ &\quad (19X^3-12X^2+28X+32)^2-(X^2-X+3)^{11}T. \end{aligned}$$

(ii) Amb les notacions de l'apartat (i), el següent polinomi defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois M_{22}:

$$g(T,X) := f\left(\frac{2^{22}}{11T^2+1}, X\right).$$

Proposició 5.3.6. *Si $f(T,X)$ i $g(T,X)$ són els polinomis de la Proposició 5.3.5, aleshores:*

(i) Existeixen infinits $t \in \mathbb{Q}$ tals que els cossos de descomposició dels corresponents polinomis $f(t,X)$ defineixen infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, moderadament ramificades i amb grup de Galois $\mathrm{Aut}(M_{22})$.

(ii) No existeix cap especialització $t \in \mathbb{Q}$ de manera que $g(t,X)$ defineixi una extensió de $\mathbb{Q}$ moderadament ramificada i amb grup de Galois M_{22}.

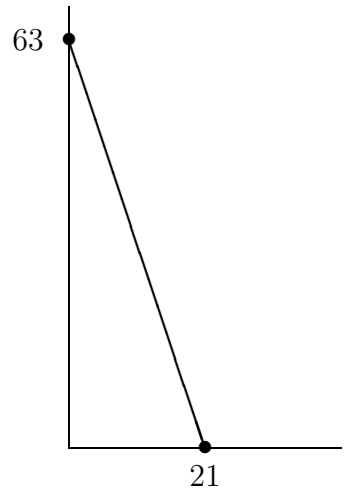
Demostració. (i) Per la Proposició 5.2.2 (ii), és suficient veure que, per a cada primer p que divideix l'ordre $\sharp\,\mathrm{Aut}(M_{22})$, existeix alguna especialització $t \in \mathbb{Q}$

tal que $D(f(t,X)) \neq 0$ i l'extensió $\mathbb{Q}_{f(t,X)}/\mathbb{Q}$ és moderadament ramificada en p. És suficient estudiar les especialitzacions del polinomi mònic

$$f_1(T,X) = (5^4 19^2 - T)^{21} f\left(T, \frac{X}{5^4 19^2 - T}\right) \in \mathbb{Z}[T][X].$$

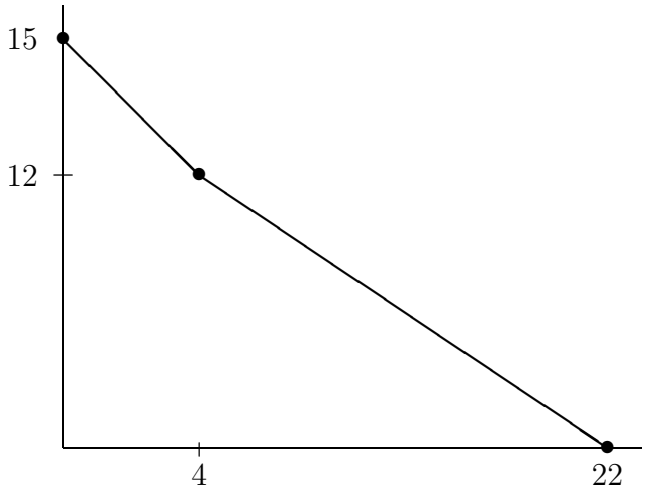
Com que $(D(f_1(2,X)), D(f_1(3,X))) = 2^{22}11^{253}$, només cal considerar els primers 2 i 11. Per a qualsevol altre primer p dividint $\sharp\,\mathrm{Aut}(M_{22})$, triem $t = 2$ o $t = 3$ de manera que p no divideixi $D(f_1(t,X))$.

Cas $p = 2$. Agafem $t = 1$. El polinomi mònic $f(X) = f_1(1,X) \in \mathbb{Z}[X]$ és irreductible, la seva reducció mòdul 2 és $\overline{f}(X) = X^{21}(1+X)$ i el seu polígon de Newton respecte $\phi(X) = X$ és



El polinomi associat a l'únic segment de $N_\phi(f(X))$ és $P_S(X) = (X^7 + X^6 + X^5 + X^2 + 1)(X^{14} + X^{13} + X^{12} + X^8 + X^7 + X^4 + X^2 + X + 1) \in \mathbb{F}_2[X]$. Com que $P_S(X)$ no té arrels múltiples, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és no ramificada en $p = 2$.

Cas $p = 11$. Prenem $t = 11^4$. El polinomi mònic $f(X) = f_1(11^4, X) \in \mathbb{Z}[X]$ és irreductible, la seva reducció mòdul 11 és $\overline{f}(X) = (X+9)^{22}$ i el seu polígon de Newton respecte $\phi(X) = X + 9$ és



Si $\theta \in \overline{\mathbb{Q}}$ és una arrel de $f(X)$, la Proposició 1.4.6 garanteix que els índexs de ramificació a $\mathbb{Q}(\theta)/\mathbb{Q}$ dels primers que divideixen $p = 11$ són tots múltiples de 3 o bé múltiples de 4. Tractant-se d'una extensió de grau 22, cap d'aquests índexs pot ser divisible per 11. Així, $p = 11$ ramifica moderadament a $\mathbb{Q}(\theta)/\mathbb{Q}$ i, per tant, a $\mathbb{Q}_f/\mathbb{Q}$.

(ii) És suficient estudiar les especialitzacions del polinomi mònic

$$g_1(T, X) = f_1\left(\frac{2^{22}}{11T^2+1}, X\right) \in \mathbb{Q}(T)[X],$$

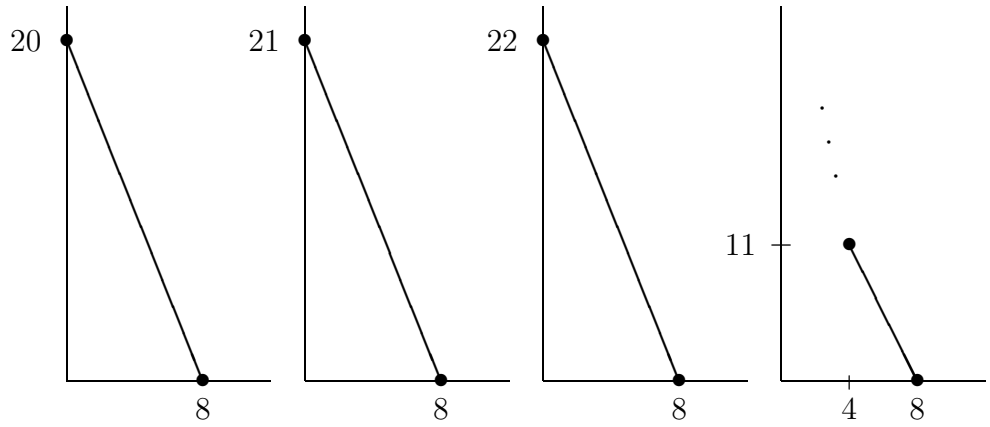
on $f_1(T, X)$ és el polinomi introduït a la demostració de (i). Veurem que l'extensió $\mathbb{Q}_{g_1(t,X)}/\mathbb{Q}$ és salvatgement ramificada, per a qualsevol especialització $t \in \mathbb{Q}$ tal que $\mathrm{Gal}_{\mathbb{Q}}(g_1(t, X)) \cong M_{22}$.

Per a tot $t \in \mathbb{Q}$, $v_2(11t^2 + 1) \leq 2$ i, per tant, $v_2\left(\frac{2^{22}}{11t^2+1}\right) \geq 20$. Així, serà suficient veure que, si $s \in \mathbb{Q}$ satisfà $v_2(s) \geq 20$ i el polinomi mònic $f(X) = f_1(s, X) \in \mathbb{Z}_{(2)}[X]$ és irreductible, aleshores $p = 2$ ramifica salvatgement a l'extensió $\mathbb{Q}_f/\mathbb{Q}$. Veiem-ho.

Com que $v_2(s) > 0$, la reducció mòdul 2 de $f(X)$ és $\overline{f}(X) = X^{14}(X-1)^8$. Si $f_1(T, X) = \sum_i c_i(T)(X-1)^i$ és el desenvolupament $(X-1)$-àdic de $f_1(T, X)$, es

comprova que les valoracions 2-àdiques dels termes independents dels polinomis $c_0(T), \cdots, c_8(T)$ són, respectivament, 20, 22, 17, 16, 11, 11, 7, 6 i 0.

Evidentment, $\sum_i c_i(s)(X-1)^i$ és el desenvolupament $(X-1)$-àdic de $f(X) = f_1(s, X)$. Tenint en compte que $v_2(s) \geq 20$, les úniques possibilitats per al polígon de Newton de $f(X)$ respecte $\phi(X) = X - 1$ (en $p = 2$) són:



En els quatre casos, $N_\phi(f(X))$ té algun costat de pendent $-\frac{h}{e}$ amb $v_2(e) > v_2(h)$. Per la Proposició 1.4.6, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada en $p = 2$. □

Observació 5.3.7. *Es pot veure que $p = 2$ és l'únic primer problemàtic en la Proposició anterior. És a dir, sí existeixen especialitzacions de $g(T, X)$ amb grup de Galois M_{22} sobre $\mathbb{Q}$ i moderadament ramificades en tots els primers $p \neq 2$.*

5.3.3 Comentaris sobre les Seccions 3.4, 5.3.1 i 5.3.2

La Proposició 5.3.6 proporciona un exemple de realització regular del grup M_{22} sobre $\mathbb{Q}(T)$ que no admet cap especialització racional moderadament ramifi-

cada. A la Secció 3.4 hem obtingut exemples de realitzacions de grups alternats amb aquesta mateixa propietat.

Adaptant els arguments emprats per a trinomis, es poden obtenir resultats anàlegs als del Capítol 3 per a polinomis del tipus

$$f(X) = X^k(X-a)^{n-k} + b.$$

El discriminant de $f(X)$ és

$$D(f(X)) = (-1)^{\frac{n(n-1)}{2}} b^{n-2} \left(n^n b + (k-n)^{n-k} k^k a^n\right)$$

i es comprova, per exemple, la validesa del següent resultat (corresponent al Teorema 3.4.5).

Teorema 5.3.8. *Sigui $f(X) = X^k(X-a)^{n-k}+b \in \mathbb{Q}[X]$ un polinomi de grau $n \equiv 4 \pmod 8$ amb k senar i discriminant quadrat no nul a $\mathbb{Q}$. Aleshores l'extensió $\mathbb{Q}_f/\mathbb{Q}$ és salvatgement ramificada (en $p = 2$).*

Anàlogament al que passa amb trinomis, donats naturals $k < n$, la família de polinomis del tipus

$$f(X) = X^k(X-a)^{n-k} + b$$

admet una parametrització que permet interpretar-la com un recobriment de $\mathbb{P}^1{}_{\mathbb{Q}}$. Concretament, es té

$$\frac{1}{a^n} f(aX) = X^k(X-1)^{n-k} + \frac{b}{a^n}$$

i, per tant, l'extensió $\mathbb{Q}_f/\mathbb{Q}$ s'obté per especialització en $T = \frac{b}{a^n}$ de l'extensió $M_T/\mathbb{Q}(T)$, on M_T és el cos de descomposició sobre $\mathbb{Q}(T)$ del polinomi

$$f_{n,k}(T, X) := X^k(X-1)^{n-k} + T \in \mathbb{Q}(T)[X].$$

És conegut que, quan $(k, n) = 1$, l'extensió $M_T/\mathbb{Q}(T)$ és regular i té grup de Galois

$$\mathrm{Gal}(M_T/\mathbb{Q}(T)) \cong \mathrm{Gal}_{\mathbb{Q}(T)}(f_{n,k}(T, X)) \cong S_n.$$

De fet, aquestes són les realitzacions galoisianes del grup simètric S_n que s'obtenen típicament quan s'aplica el mètode de la rigidesa (cf. [Vil85] o [Ser92b]). Raonant com a la Proposició 3.2.1, obtenim:

Proposició 5.3.9. *Sigui S un conjunt finit de primers qualsevol. Donats dos naturals coprimers $k < n$, existeix algun polinomi del tipus $f(X) = X^k(X-a)^{n-k}+b \in \mathbb{Z}[X]$, amb grup de Galois $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong S_n$ i discriminant $D(f(X))$ no divisible per cap $p \in S$.*

Les extensions regulars $M_T/\mathbb{Q}(T)$ considerades més amunt ramifiquen en només tres primers de $\mathbb{Q}(T)$, tots tres de grau 1 (com passava amb els trinomis). Sota aquesta hipòtesi, de la fórmula del gènere de Riemann-Hurwitz s'obté (cf., per exemple, [Ser92b, Lemma 4.5.1]):

Proposició 5.3.10. *Sigui H un subgrup d'índex 2 d'un grup finit G. Sigui $K/\mathbb{Q}(T)$ una extensió regular amb grup de Galois $\mathrm{Gal}(K/\mathbb{Q}(T)) \cong G$, ramificada com a màxim en tres primers, tots tres racionals sobre $\mathbb{Q}$. Aleshores, el subcos de K fix per H és racional, és a dir, l'extensió $K^H/\mathbb{Q}$ és transcendent pura (de grau de transcendència 1).*

En la nostra situació, aquest resultat estableix una igualtat del tipus ${M_T}^{A_n} = \mathbb{Q}(T')$, per a cert $T' \in M_T$ (transcendent). Dit d'una altra manera, (redefinint $T' = T$) existeix algun $a(T) \in \mathbb{Q}(T)$ de manera que el cos de descomposició sobre $\mathbb{Q}(T)$ del polinomi

$$f_{n,k}(a(T), X) = X^k(X-1)^{n-k} + a(T) \in \mathbb{Q}(T)[X]$$

defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois

$$\mathrm{Gal}_{\mathbb{Q}(T)}(f_{n,k}(a(T), X)) \cong A_n.$$

Denotem per $f_{11}(T, X)$, $f_{12}(T, X)$, $f_{22}(T, X)$ i $f_{a22}(T, X)$ els polinomis de $\mathbb{Q}(T)[X]$ considerats a les seccions 5.3.1 i 5.3.2 amb grups de Galois M_{11}, M_{12}, M_{22} i $\mathrm{Aut}(M_{22})$, respectivament. Hem vist:

(i) els cossos de descomposició sobre $\mathbb{Q}(T)$ dels polinomis

$$f_{11}(T,X), \quad f_{12}(T,X), \quad f_{a22}(T,X) \quad \text{i} \quad f_{n,k}(T,X), \text{ amb } (k,n)=1,$$

defineixen extensions regulars de $\mathbb{Q}(T)$ que admeten especialitzacions racionals moderadament ramificades (Proposició 5.3.2, Proposició 5.3.6 (i) i Proposició 5.3.9),

(ii) els cossos de descomposició sobre $\mathbb{Q}(T)$ dels polinomis

$$f_{22}(T,X) \quad \text{i} \quad f_{n,k}(a(T),X), \text{ amb } (k,n)=1,$$

defineixen extensions regulars de $\mathbb{Q}(T)$ que **no** admeten cap especialització racional moderadament ramificada (Proposició 5.3.6 (ii) i Teorema 5.3.8).

Tots aquests exemples tenen en comú el fet que s'obtenen, directament o indirectament, pel mètode de la rigidesa. Aquest mètode permet construir, quan es té un sistema de generadors amb bones propietats per a un grup finit G de centre trivial, una G-extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ (cf., per exemple, [MM99]). El fet que les realitzacions de (ii) no admetin cap especialització moderadament ramificada és consistent amb el suggeriment fet per Birch que, en general, les especialitzacions d'una "G-extensió rígida"de $\mathbb{Q}(T)$ són salvatgement ramificades (cf. [Bir94, pàg. 35]). Dels exemples considerats, però, precisament els de (ii) són els únics que no són pròpiament "rígids". Tots dos s'obtenen en considerar subcossos fixos en "realitzacions rígides"dels exemples de (i) per a $\mathrm{Aut}(M_{22})$ i S_n, respectivament (i aplicar la Proposició 5.3.10). Podem pensar, doncs, que la no existència d'especialitzacions moderadament ramificades en els exemples de (ii) no prové estrictament del fet que es tracti d'extensions construïdes pel mètode de la rigidesa. Finalment, convé esmentar que els exemples de (i) no han estat preseleccionats amb la finalitat que admetessin especialitzacions moderadament ramificades.

Capítol 6

Problemes d'immersió centrals sobre $\mathbb{Q}$ i sobre $\mathbb{Q}(T)$

6.1 Introducció

Una estratègia habitual per a obtenir realitzacions d'alguns grups finits com a grups de Galois sobre $\mathbb{Q}$ consisteix en trobar realitzacions d'algun quocient per a les quals el corresponent problema d'immersió galoisiana sigui pròpiament resoluble. Un dels objectius d'aquest capítol és estudiar alguns d'aquests problemes per tal d'obtenir, quan el problema és resoluble, solucions amb un bon comportament de ramificació. Ens interessa, especialment, la possibilitat de realitzar un grup finit G com a grup de Galois d'una extensió moderadament ramificada de $\mathbb{Q}$ a partir de realitzacions moderades d'algun quocient de G.

Per a problemes d'immersió (sobre $\mathbb{Q}$) amb nucli d'ordre senar, Neukirch demostra que, sota certes hipòtesis, es satisfà un principi local-global i que, quan el problema és resoluble, solucions arbitràries dels problemes locals en un nombre finit de primers qualssevol sempre es poden obtenir per compleció d'alguna solució pròpia del problema global (cf. [Neu79, Main Thm.]). En particular, sempre es pot trobar una solució pròpia conservant el caràcter no

ramificat dels primers d'un conjunt finit prefixat. Quan el nucli no és d'ordre senar, però, el resultat anàleg ja falla, per exemple, en el cas abelià.

Comencem la Secció 6.2 veient que, si un problema d'immersió (sobre $\mathbb{Q}$) central finit admet solució, aleshores sempre existeix alguna solució pròpia conservant el caràcter moderat de la ramificació (respectivament la no ramificació en un conjunt finit qualsevol S). Demostrem, també, que aquest resultat admet (per especialització) una "versió regular"sobre $\mathbb{Q}(T)$, assumint la resolubilitat del problema sobre $\mathbb{Q}(T)$. Això, i resultats de capítols anteriors, ens permet demostrar que tot grup extensió central finita dels grups A_n, S_n, M_{11} o M_{12} es realitza com a grup de Galois d'infinites extensions moderadament ramificades de $\mathbb{Q}$, dos a dos linealment disjuntes. En particular, el problema 3 de la Introducció de la memòria admet una resposta afirmativa per a tots aquests grups.

A la Secció 6.3 tornem a considerar problemes d'immersió centrals finits per a les realitzacions regulars de A_n obtingudes per Mestre ([Mes90]). Enlloc de perseguir condicions de ramificació prefixada com a la Secció 6.2, ara es tracta de contribuir al problema proposat per S.Beckmann (cf. [Bec94]) sobre l'existència de realitzacions regulars d'un grup finit G sobre $\mathbb{Q}(T)$ que especialitzin a una G-extensió de $\mathbb{Q}$ prefixada. Quan això és així per a tota G-extensió de $\mathbb{Q}$, es diu que G satisfà la propietat d'aixecament aritmètic sobre $\mathbb{Q}$.

El resultat principal de la Secció 6.3 és que, si G és un grup extensió central finita de A_n amb $n \neq 4, 6, 7$, aleshores G satisfà la propietat d'aixecament aritmètic sobre qualsevol cos de característica 0. Demostrem també una generalització d'aquest resultat que, en particular, proporciona G-extensions regulars de $\mathbb{Q}(T)$ amb un primer de grau 1 que descompon completament. Això ens permet garantir l'existència d'infinites G-extensions de $\mathbb{Q}$ en les quals tots els primers d'un conjunt finit prefixat qualsevol descomponen completament (problema 2.1 de la Introducció).

6.2 Problemes d'immersió centrals i ramificació moderada

En aquest capítol usarem notacions i resultats introduïts a la Secció 1.1.

6.2.1 Existència de solucions pròpies moderadament ramificades

Per tal que un problema d'immersió galoisiana (π, φ) sobre $\mathbb{Q}$ admeti una solució pròpia moderadament ramificada és evidentment necessari que:

- el problema (π, φ) admeti solució,
- l'epimorfisme φ sigui moderadament ramificat.

El resultat següent estableix que, per a problemes centrals finits, les condicions anteriors també són suficients.

Teorema 6.2.1. *Sigui G un grup finit i sigui $\varphi : G_{\mathbb{Q}} \to G$ un epimorfisme. Suposem donat un problema d'immersió central finit (π, φ)*

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & & \downarrow \varphi & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

que admet solució. Si l'epimorfisme φ és moderadament ramificat, aleshores existeix alguna solució pròpia del problema (π, φ), moderadament ramificada.

Demostració. Raonant com a la demostració de la Proposició 1.1.8, és suficient veure que els problemes locals (π, φ_p) en els primers p que divideixen l'ordre de C admeten sempre alguna solució moderadament ramificada. Aquests són els únics primers que poden ramificar salvatgement, per la hipòtesi de moderació sobre φ.

Com que el nucli C és producte directe de l-grups cíclics, qualsevol solució del problema local (π, φ_p)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C & \to & \widetilde{G} & \to & G & \to & 1 \end{array}$$

s'obté com la composició (producte fibrat) de solucions de problemes del tipus

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C_l & \to & \widetilde{G_l} & \to & G & \to & 1, \end{array}$$

on C_l és un l-grup cíclic i $\widetilde{G_l}$ és el quocient de $\widetilde{G}$ per un complement de C_l en C (cf. [ILF97, Chap.1,§12.]).

Tenint en compte que el caràcter moderat es conserva per composició, només cal considerar problemes d'aquest darrer tipus amb $l = p$.

En resum, donat un p-grup cíclic C_p i un epimorfisme $\varphi_p : G_{\mathbb{Q}_p} \to G_p$ moderadament ramificat, cal provar que, si un problema d'immersió central finit (π, φ_p)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow \varphi_p & & \\ 1 & \to & C_p & \to & \widetilde{G_p} & \stackrel{\pi}{\to} & G_p & \to & 1 \end{array}$$

admet solució, aleshores n'admet alguna de moderadament ramificada.

Definim $H_p = \varphi_p(I_p)$, on I_p denota el subgrup d'inèrcia de $G_{\mathbb{Q}_p}$. Per hipòtesi, φ_p és moderadament ramificat i, per tant, $H_p \subset G_p$ és un subgrup normal cíclic d'ordre coprimer amb p. Així, $\widetilde{H_p} := \pi^{-1}(H_p)$ és un subgrup normal abelià (l'extensió és central) de $\widetilde{G_p}$ isomorf a $C_p \times H_p$ (C_p és un p-grup).

Si H'_p denota un complement de C_p en $\widetilde{H_p}$, es té el diagrama commutatiu següent:

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H'_p & \overset{\cong}{\to} & H_p & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \to & C_p & \to & \widetilde{G_p} & \overset{\pi}{\to} & G_p & \to & 1 \\
 & & \downarrow \cong & & \downarrow & & \downarrow & & \\
1 & \to & C_p & \to & \widetilde{G_p}/H'_p & \to & G_p/H_p & \to & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

D'aquesta manera, es té un isomorfisme

$$\widetilde{G_p} \cong G_p \times_{G_p/H_p} \widetilde{G_p}/H'_p$$

i tota solució del problema (π, φ_p) és l'aixecament (per $G_p \to G_p/H_p$) d'una solució del problema

$$\begin{array}{ccccccccc}
 & & & & & & G_{\mathbb{Q}_p} & & \\
 & & & & & & \downarrow \varphi_p & & \\
 & & & & & & G_p & & \\
 & & & & & & \downarrow & & \\
1 & \to & C_p & \to & \widetilde{G_p}/H'_p & \overset{\pi}{\to} & G_p/H_p & \to & 1
\end{array}$$

(cf., per exemple, [ILF97, Prop. 1.13.3]).

Aquest darrer problema d'immersió sempre admet alguna solució no ramificada, per ser $G_{\mathbb{Q}_p} \overset{\varphi_p}{\to} G_p \to G_p/H_p$ no ramificat (veure Proposició 1.1.8). Per tant, el problema (π, φ_p) sempre admet alguna solució moderadament ramificada, donat que φ_p ho és per hipòtesi i p no divideix l'ordre de H'_p. □

Les hipòtesis del Teorema 6.2.1 es satisfan, per exemple, quan l'epimorfisme $\varphi : G_{\mathbb{Q}} \to G$ s'obté per especialització (en algun $T = t_0 \in \mathbb{Q}$) d'un epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to G$ tal que el problema d'immersió (π, φ_T) admet solució. En aquesta situació, obtenim el resultat següent.

Teorema 6.2.2. *Sigui G un grup finit i sigui $\varphi_T : G_{\mathbb{Q}(T)} \to G$ un epimorfisme. Suposem donat un problema d'immersió central finit (π, φ_T)*

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_T} & & \\ & & & & & & \downarrow \varphi_T & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

que admet solució.

(i) Si l'especialització de φ_T en algun $T = t_0 \in \mathbb{Q}$ és moderadament ramificada (resp. no ramificada en un conjunt finit S), aleshores existeix alguna solució pròpia del problema (π, φ_T) tal que la seva especialització en algun $T = t_1 \in \mathbb{Q}$ és moderadament ramificada (resp. no ramificada en S).

(ii) Si, a més de les hipòtesis de (i), l'epimorfisme φ_T és $\mathbb{Q}$-regular, aleshores existeix alguna solució $\mathbb{Q}$-regular de (π, φ_T) com a (i). En particular, en aquest cas, existeixen infinites realitzacions de $\widetilde{G}$ com a grup de Galois d'extensions moderadament ramificades de $\mathbb{Q}$ (resp. no ramificades en S), linealment disjuntes dos a dos.

Demostració. (i) Recordem que, per a $t \in \mathbb{Q}$, $\varphi_t : G_{\mathbb{Q}} \longrightarrow G$ denota l'especialització de φ_T en $T = t$.

Considerem una solució qualsevol $\widetilde{\varphi_T}$ del problema (π, φ_T). Per la Proposició 5.2.2, existeix algun $t_1 \in \mathbb{Q}$ tal que $\widetilde{\varphi_T}$ és no ramificada en $T = t_1$, $\varphi_{t_1}(G_{\mathbb{Q}}) = G$ i φ_{t_1} és moderadament ramificat (resp. no ramificat en S).

L'especialització $\widetilde{\varphi_{t_1}}$ de $\widetilde{\varphi_T}$ en $T = t_1$ és una solució del problema (π, φ_{t_1}):

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & & \downarrow \varphi_{t_1} & & \\ 1 & \to & C & \to & \widetilde{G} & \stackrel{\pi}{\to} & G & \to & 1 \end{array}$$

El Teorema anterior (resp. la Proposició 1.1.8) garanteix que aquest problema admet alguna solució pròpia moderadament ramificada (resp. no ramificada en S), que haurà de ser del tipus $\chi.\widetilde{\varphi_{t_1}}$, per algun $\chi \in H^1(G_{\mathbb{Q}}, C) = \mathrm{Hom}(G_{\mathbb{Q}}, C)$.

Sempre existeix algun $\chi_T \in \mathrm{Hom}(G_{\mathbb{Q}(T)}, C)$ tal que la seva especialització en $T = t_1$ és precisament χ. Per exemple, podem considerar el morfisme constant

$$\chi_T : G_{\mathbb{Q}(T)} \to \mathrm{Gal}(\overline{\mathbb{Q}}(T)/\mathbb{Q}(T)) \cong G_{\mathbb{Q}} \xrightarrow{\chi} G.$$

D'aquesta manera, $\chi_T.\widetilde{\varphi_T}$ és una solució del problema d'immersió (π, φ_T) tal que la seva especialització en $T = t_1$ és moderadament ramificada (resp. no ramificada en S). A més, es tracta d'una solució pròpia de (π, φ_T) donat que especialitza a la solució pròpia $\chi.\widetilde{\varphi_{t_1}}$ de (π, φ_{t_1}).

(ii) Podem raonar com a (i). Cal garantir, però, que $\chi_T.\widetilde{\varphi_T}$ sigui $\mathbb{Q}$-regular (a més de pròpia). Això equival a que $(\chi_T.\widetilde{\varphi_T})(G_{\overline{\mathbb{Q}}(T)}) = \widetilde{G}$.

És conegut que, si C és un grup abelià finit i $\chi : G_{\mathbb{Q}} \to C$ és un epimorfisme qualsevol, aleshores existeixen infinits $\chi_T \in \mathrm{Hom}(G_{\mathbb{Q}(T)}, C)$ $\mathbb{Q}$-regulars tals que $\chi_{t_1} = \chi$ i amb conjunts de ramificació disjunts dos a dos (veure Proposició 6.3.3).

En particular, sempre podem triar χ_T de manera que les extensions de $\overline{\mathbb{Q}}(T)$ definides per χ_T i $\widetilde{\varphi_T}$ no tinguin primers ramificats en comú i, per tant, siguin linealment disjuntes.

En aquest cas,

$$(\chi_T, \widetilde{\varphi_T}) : G_{\overline{\mathbb{Q}}(T)} \longrightarrow \chi_T(G_{\overline{\mathbb{Q}}(T)}) \times \widetilde{\varphi_T}(G_{\overline{\mathbb{Q}}(T)}) = C \times \widetilde{\varphi_T}(G_{\overline{\mathbb{Q}}(T)})$$

és un epimorfisme i, per tant, $\chi_T.\widetilde{\varphi_T} : G_{\overline{\mathbb{Q}}(T)} \longrightarrow \widetilde{G}$ també ho és, tal com volíem. □

Observació 6.2.3. *L'argument donat a la demostració anterior fa evident, en particular, que si $\varphi_T : G_{\mathbb{Q}(T)} \to G$ és l'epimorfisme corresponent a una extensió de Galois finita $\mathbb{Q}$-regular de $\mathbb{Q}(T)$, aleshores tot problema d'immersió central*

finit per a φ_T que admet una solució, també n'admet alguna de pròpia i $\mathbb{Q}$-regular.

En la resta d'aquesta secció, aplicarem el Teorema anterior a realitzacions galoisianes conegudes dels grups $G = A_n,\ S_n,\ M_{11}$ i M_{12}. Provarem que tot grup extensió central finita de qualsevol d'aquests grups admet infinites realitzacions com a grup de Galois d'extensions moderadament ramificades de $\mathbb{Q}$, dos a dos linealment disjuntes.

Per a futura referència, convé recordar la següent conseqüència del Teorema de Shafarevich ([Sha54] i [Sha89]) sobre l'existència d'extensions de $\mathbb{Q}$ amb grup de Galois resoluble finit qualsevol.

Proposició 6.2.4. *[KM02, Thm. 6.2] Tot grup resoluble finit es realitza com a grup de Galois d'una extensió de $\mathbb{Q}$ no ramificada en els primers d'un conjunt finit prefixat qualsevol S. En particular, tot grup resoluble finit es realitza com a grup de Galois d'alguna extensió moderadament ramificada de $\mathbb{Q}$.*

6.2.2 Extensions centrals finites de grups alternats

A la Secció 4.2 hem recordat una construcció de Mestre [Mes90] que proporciona, per a qualsevol cos K de característica 0, realitzacions K-regulars del grup alternat A_n sobre $K(T)$. El resultat principal de [Mes90] és la realització regular sobre $\mathbb{Q}(T)$ de $\widetilde{A_n}$ ($n \geq 4$), l'única extensió central no trivial de A_n per $\mathbb{Z}/2\mathbb{Z}$. Això es dedueix del fet que els grups d'inèrcia en les A_n-extensions de $K(T)$ obtingudes són tots d'ordre 3. Tenint en compte, per exemple, [Ser94], també s'obté:

Proposició 6.2.5. *Sigui K un cos de característica 0, $P(X) \in K[X]$ un polinomi H-general de grau senar $n \geq 3$ i $Q(X) \in K[X]$ el polinomi de la*

Proposició 4.2.1. Considerem un epimorfisme

$$\varphi_T : G_{K(T)} \to \mathrm{Gal}_{K(T)}(P(X) - TQ(X)) \cong G$$

corresponent al cos de descomposició sobre $K(T)$ de $P(X)-TQ(X)$. Suposem donada una extensió central finita

$$1 \to C \to \widetilde{G} \xrightarrow{\pi} G \to 1,$$

amb nucli C d'ordre coprimer amb 3. Aleshores, l'obstrucció al problema d'immersió (π, φ_T) és constant, és a dir, pertany a $H^2(G_K, C)$ via la inclusió natural $H^2(G_K, C) \hookrightarrow H^2(G_{K(T)}, C)$.

En les hipòtesis d'aquest resultat, G és isomorf a A_n (resp. S_n) si el discriminant de $P(X)$ és un quadrat (resp. no quadrat) a K. A més, si φ_T no ramifica en $T = t \in K$, aleshores l'obstrucció de (π, φ_T) coincideix amb l'obstrucció del problema d'immersió (π, φ_t) sobre K.

Teorema 6.2.6. *Sigui n un natural qualsevol i G un grup extensió central finita del grup alternat A_n. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$ moderadament ramificades, linealment disjuntes dos a dos.*

Demostració. Per a $n < 5$, qualsevol grup extensió central de A_n és resoluble i, per tant, només cal aplicar la Proposició 6.2.4.

Suposem, doncs, $n \geq 5$. El grup dels multiplicadors de Schur de A_n és (cf. [Suz82, Chap.3,§2.]):

$$M(A_n) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}\ , \text{ si } n \neq 6, 7 \\ \mathbb{Z}/6\mathbb{Z}\ , \text{ si } n = 6, 7 \end{cases}$$

Com que $n \geq 5$, el grup A_n és simple i, en particular, perfecte.

Considerem l'extensió central universal de A_n

$$1 \to M(A_n) \to U \xrightarrow{\pi} A_n \to 1.$$

Per a qualsevol epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to A_n$, la resolubilitat del problema d'immersió central universal (π, φ_T)

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}(T)} & & \\ & & & & & & \downarrow \varphi_T & & \\ 1 & \to & M(A_n) & \to & U & \stackrel{\pi}{\to} & A_n & \to & 1 \end{array}$$

implica la resolubilitat de tots els problema d'immersió centrals finits per a φ_T.

Així, pel Teorema 6.2.2, és suficient veure l'existència d'un epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to A_n$ $\mathbb{Q}$-regular tal que:

(a) el problema d'immersió central universal (π, φ_T) és resoluble,

(b) l'especialització de φ_T en algun $T = t_0 \in \mathbb{Q}$ és moderadament ramificada.

Tractarem per separat els casos $n = 6, 7$.

Cas $n \neq 6, 7$ (i $n \geq 5$)

En aquest cas, el nucli de l'extensió central universal és $M(A_n) \cong \mathbb{Z}/2\mathbb{Z}$ i $U \cong \widetilde{A_n}$, on $\widetilde{A_n}$ denota l'única extensió central no trivial de A_n amb nucli $\mathbb{Z}/2\mathbb{Z}$.

Sigui $P(X) \in \mathbb{Q}[X]$ un polinomi H-general de grau senar n o $n+1$ amb totes les arrels racionals i diferents; l'existència de $P(X)$ és evident per ser $\mathbb{Q}$ infinit (i $H \neq 0$).

Considerem un epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to A_n$ corresponent al cos de descomposició sobre $\mathbb{Q}(T)$ de $P(X) - TQ(X)$ (veure Secció 4.2).

Com que el nucli $M(A_n)$ de π és d'ordre 2, la Proposició anterior garanteix que l'obstrucció al problema (π, φ_T) és constant. Aquesta obstrucció ha de ser trivial donat que s'anul.la en el punt no ramificat $T = 0$, per ser $\varphi_0(G_{\mathbb{Q}}) = \{1\}$.

Tal com volíem, φ_T satisfà (a) i (b) donat que φ_0 és moderadament ramificat.

Finalment, el cas parell s'obté del cas senar. Per a n senar, el polinomi

$$G(s,X) = \frac{P(X) - \frac{P(s)}{Q(s)}Q(X)}{X-s}$$

defineix una A_{n-1}-extensió regular de $\mathbb{Q}(s)$ per a la qual l'obstrucció al problema d'immersió corresponent és constant (els grups d'inèrcia són d'ordre 3). Només falta notar que, si $a \in \mathbb{Q}$ és una de les arrels de $P(X)$, aleshores el polinomi $G(a,X)$ (està ben definit i) té $n-1$ arrels racionals diferents.

Cas $n = 6$

En aquest cas, el nucli de l'extensió central universal és $M(A_6) \cong \mathbb{Z}/6\mathbb{Z}$ i, en particular, d'ordre divisible per 3; l'argument anterior, doncs, no és aplicable.

A [Mes98] es demostra que el polinomi

$$625X^6+15750X^4-51300X^2+6696-\frac{2454(T^2+186)}{5T}X(X^2-8X+6)(X^2+8X+6)$$

defineix una A_6-extensió regular de $\mathbb{Q}(T)$ per a la qual el problema d'immersió central universal és resoluble. Malhauradament, es comprova que totes les especialitzacions racionals d'aquest polinomi defineixen extensions de $\mathbb{Q}$ salvatgement ramificades (en $p = 2$).

La construcció de Mestre, però, proporciona una família de polinomis del tipus $F_u(T,X) = Q(X) - f(T)P(X)$, depenent d'un paràmetre u, tals que $F_u(T,X)$ defineix una A_6-extensió regular de $\mathbb{Q}(T)$ per a la qual el problema d'immersió central universal és resoluble (el polinomi anterior correspon al cas $u = 5$). Per a $u = 2$, després d'"arreglar"els coeficients de $F_2(T,X)$ per canvis lineals en X i T, s'obté el polinomi:

$$X^6 - 11655X^4 + 2402595X^2 - 25984989 - f(T)(X^5 - 925X^3 + 49284X)$$

amb

$$f(T) = \frac{37T^2 - 63903343473}{15392T}.$$

Usant polígons de Newton com a la Secció 5.3, es comprova que l'especialització en $T = 7$ és moderadament ramificada (de fet, no ramificada en $p = 2, 3, 5$).

Notem que, en $p = 2$, per a obtenir aquest resultat cal considerar els desenvolupaments X-àdic i $(X + 2^3)$-àdic.

Cas $n = 7$

Com en el cas anterior, el nucli de l'extensió central universal és $M(A_7) \cong \mathbb{Z}/6\mathbb{Z}$.

A [Mes98] es demostra que, prenent

$$f(T) = \frac{120636000T}{11626727T^2 + 31255},$$

el polinomi

$$X(49X^6 - 882X^4 + 1365X^2 - 100) - f(T)(32585X^4 - 9702X^2 + 141)$$

defineix una A_7-extensió regular de $\mathbb{Q}(T)$ per a la qual el problema d'immersió central universal admet solució.

Es comprova que l'especialització en $T = 0$ (i, per tant, $f(T) = 0$) és moderadament ramificada. □

Observació 6.2.7. *Per a $n \geq 5$ hem demostrat, de fet, que tot grup extensió central finita de A_n es realitza com a grup de Galois d'una extensió regular de $\mathbb{Q}(T)$ que admet especialitzacions moderadament ramificades sobre $\mathbb{Q}$.*

L'argument donat en la demostració anterior també permet establir el resultat següent.

Teorema 6.2.8. *Sigui $n \neq 6, 7$ un natural i G un grup extensió central finita del grup alternat A_n. Sigui S un conjunt finit de primers qualsevol. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$ no ramificades en S, linealment disjuntes dos a dos.*

Observació 6.2.9. *De fet, per a $n \neq 4, 6, 7$, obtindrem també el resultat anàleg demanant "tots els primers de S descomponen completament"(veure Corol.lari 6.3.7).*

6.2.3 Extensions centrals finites de grups simètrics

Per a grups extensió central finita del grup simètric S_n, provem el resultat anàleg al Teorema 6.2.6. Ho veurem seguint l'estratègia de Sonn per a demostrar que tot grup extensió central finita de S_n es realitza com a grup de Galois d'una extensió regular de $\mathbb{Q}(T)$ (cf. [Son91]).

Teorema 6.2.10. *Sigui n un natural qualsevol i G un grup extensió central finita del grup simètric S_n. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, moderadament ramificades.*

Demostració. Per a $n < 5$, qualsevol grup extensió central de S_n és resoluble i, per tant, el resultat és conseqüència de la Proposició 6.2.4.

Suposem, doncs, $n \geq 5$. En aquest cas, S_n és un grup no perfecte amb grup de multiplicadors de Schur (cf. [Suz82, Chap.3,§2.])

$$M(S_n) \cong \mathbb{Z}/2\mathbb{Z}.$$

Usant també que el subgrup derivat de S_n (és a dir, A_n) té índex 2, es pot veure que el nucli de qualsevol extensió central primitiva de S_n és un 2-grup (cf. [KSS89, Thm. 6]).

Així, pel Teorema 6.2.2 és suficient veure que, donada una extensió central finita

$$1 \to C \to G \xrightarrow{\pi} S_n \to 1$$

amb nucli un 2-grup, aleshores existeix un epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to S_n$ $\mathbb{Q}$-regular tal que:

(a) el problema d'immersió (π, φ_T) és resoluble,

(b) l'especialització de φ_T en algun $T = t_0 \in \mathbb{Q}$ és moderadament ramificada.

Sigui $C_2 \subseteq S_n$ el subgrup generat per un 2-cicle i considerem l'extensió central corresponent

$$1 \to C \to A \xrightarrow{\pi} C_2 \to 1.$$

Com que el grup $A = \pi^{-1}(C_2)$ és un grup abelià finit, és conegut que existeix una A-extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ tal que la seva especialització en algun $T = t_0 \in \mathbb{Q}$ és moderadament ramificada (veure Secció 6.3). Sigui $\widetilde{\varphi_T} : G_{\mathbb{Q}(T)} \to A$ l'epimorfisme corresponent.

L'extensió quadràtica $K_T/\mathbb{Q}(T)$ corresponent a $\varphi_T := \pi \circ \widetilde{\varphi_T}$ s'obté com a cos de descomposició sobre $\mathbb{Q}(T)$ d'un polinomi mònic $f(T, X) \in \mathbb{Q}[T, X]$ de grau 2. A més, podem suposar que $P(T, X) = f(T, X) \prod (X - a_i)$ és un polinomi H-general de grau senar n o $n + 1$, amb $a_i \in \mathbb{Q}$ convenients (veure Proposició 6.3.4).

De la Proposició 4.2.1 obtenim un epimorfisme

$$\varphi_{T,U} : G_{\mathbb{Q}(T,U)} \to \mathrm{Gal}_{\mathbb{Q}(T,U)}(P(T, X) - U.Q(T, X)) \cong S_n,$$

on U denota una nova indeterminada.

Com que estem suposant que C és un 2-grup, la Proposició 6.2.5 garanteix que l'obstrucció al problema d'immersió $(\pi, \varphi_{T,U})$ no depèn de U. D'altra banda, $\widetilde{\varphi_T}$ és una solució de $(\pi, \varphi_{T,0})$ i, per tant, aquest problema té obstrucció nul.la. En conclusió, l'obstrucció de $(\pi, \varphi_{T,U})$ és trivial i el mateix val per a (π, φ_{T,u_0}), per a qualsevol $u_0 \in \mathbb{Q}$ (no ramificat).

Gràcies a la Proposició 5.2.2, podem triar $u_0 \in \mathbb{Q}$ tal que $\varphi_{T,u_0}(G_{\mathbb{Q}(T)}) = S_n$ i φ_{T,u_0} admet especializacions racionals (de T) moderadament ramificades (donat que això es satisfà per a $K_T/\mathbb{Q}(T)$, és a dir, per a $\varphi_{T,0}$); només cal imposar $u_0 \equiv 0 \pmod{(n!)^k}$, amb k prou gran.

Notem, finalment, que la S_n-extensió de $\mathbb{Q}(T)$ definida per φ_{T,u_0} és necessàriament $\mathbb{Q}$-regular, per ser-ho la seva única subextensió galoisiana no trivial $K_T/\mathbb{Q}(T)$.

□

Observació 6.2.11. *Aquest resultat també es pot obtenir sense recórrer als arguments de [Son91]. De fet, si $P(X) \in \mathbb{Q}[X]$ és un polinomi H-general*

amb discriminant no quadrat, aleshores el polinomi $P(X) - TQ(X)$ defineix una S_n-extensió de $\mathbb{Q}(T)$; no es tracta, però, d'una extensió $\mathbb{Q}$-regular (veure Proposició 4.2.1).

L'avantatge de la demostració donada és que estableix, per a $n \geq 5$, que tot grup extensió central finita de S_n es realitza com a grup de Galois d'una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ que admet especialitzacions moderadament ramificades sobre $\mathbb{Q}$.

Raonant com a la demostració del Teorema anterior, també obtenim el resultat següent.

Teorema 6.2.12. *Sigui n un natural qualsevol i G un grup extensió central finita del grup simètric S_n. Sigui S un conjunt finit de primers qualsevol. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$ no ramificades en S, linealment disjuntes dos a dos.*

6.2.4 Extensions centrals finites dels grups de Mathieu M_{11} i M_{12}

Les realitzacions regulars sobre $\mathbb{Q}(T)$ dels grups de Mathieu M_{11} i M_{12} que considerarem són, essencialment, les ja recordades a la Secció 5.3. Allà hem provat que totes dues admeten especialitzacions racionals moderadament ramificades.

Teorema 6.2.13. *Sigui G un grup extensió central finita d'un dels grups de Mathieu M_{11} o M_{12}. Aleshores, G es realitza com a grup de Galois d'infinites extensions moderadament ramificades de $\mathbb{Q}$, linealment disjuntes dos a dos.*

Demostració. M_{11} és un grup simple amb grup de multiplicadors de Schur trivial. Així, tota extensió central de M_{11} és split i, per tant, sempre dóna lloc a problemes d'immersió resolubles. En aquest cas només cal aplicar la Proposició 5.3.2 i el Teorema 6.2.2.

M_{12} és un grup simple d'ordre $2^6.3^3.5.11$ amb grup de multiplicadors de Schur $H_2(M_{12},\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Pel Teorema 6.2.2, és suficient veure l'existència d'un epimorfisme $\varphi_T : G_{\mathbb{Q}(T)} \to M_{12}$ (regular) admetent alguna especialització moderadament ramificada i tal que el problema d'immersió central universal $(\widetilde{M_{12}}, \varphi_T)$

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}(T)} & & \\ & & & & & & \downarrow \varphi_T & & \\ 1 & \to & \mathbb{Z}/2\mathbb{Z} & \to & \widetilde{M_{12}} & \to & M_{12} & \to & 1 \end{array}$$

sigui resoluble.

A la Secció 5.3 hem recordat que el polinomi (de [MZM86])

$$\begin{aligned} f(T,X) \;:=\; & X^{12} + 20X^{11} + 162X^{10} + \frac{3348}{5}X^9 + \frac{35559}{5^2}X^8 + \frac{5832}{5}X^7 \\ & - \frac{84564}{5^3}X^6 - \frac{857304}{5^4}X^5 + \frac{807003}{5^5}X^4 + \frac{1810836}{5^5}X^3 \\ & - \frac{511758}{5^6}X^2 + \frac{2125764}{5^7}X + \frac{531441}{5^8} - TX^2 \end{aligned}$$

defineix una extensió regular de $\mathbb{Q}(T)$ amb grup de Galois M_{12}. Si $\varphi_T : G_{\mathbb{Q}(T)} \to M_{12}$ denota l'epimorfisme corresponent, l'obstrucció al problema $(\widetilde{M_{12}}, \varphi_T)$ és no nul.la. A [BLV86] es demostra, però, que existeixen especialitzacions $t \in \mathbb{Q}$ per a les quals el problema d'immersió (sobre $\mathbb{Q}$) $(\widetilde{M_{12}}, \varphi_t)$ admet solució; aquest és el cas, per exemple, per a $t = 133$.

El tipus de ramificació de φ_T i el fet que l'obstrucció de $(\widetilde{M_{12}}, \varphi_T)$ s'anul.li per especialització en algun punt no ramificat $T = t_0 \in \mathbb{Q}$ permeten a Mestre deduir (per canvi de variable) una realització regular de $\widetilde{M_{12}}$ sobre $\mathbb{Q}(T)$ (cf. [Mes94b] i [Mes94a]). Concretament, es demostra que existeix una funció racional $h(T) \in \mathbb{Q}(T)$ tal que $h(0) = t_0$ i $f(h(T), X)$ defineix una M_{12}-extensió regular de $\mathbb{Q}(T)$ per a la qual el problema d'immersió corresponent $(\widetilde{M_{12}}, \psi_T)$ és resoluble.

D'altra banda, a la Proposició 5.3.2 hem vist que l'extensió de $\mathbb{Q}$ definida per $f(t,X) \in \mathbb{Q}[X]$ ($t \in \mathbb{Q}$ amb $f(t,X)$ irreductible) és

- no ramificada en $p = 2$ i $p = 3$, si $t \equiv 1 \pmod{12}$,

- moderadament ramificada en $p = 5$, si $v_5(t) \geq -6$,
- no ramificada en $p \neq 2, 3, 5$, si $t \equiv 0 \pmod{p}$.

En particular, φ_{133} no ramifica en $p = 2, 3$ i és moderadament ramificat en $p = 5$. Com que $v_{11}(D(f(133, X))) = 0$, concloem que φ_{133} és moderadament ramificat.

Així, el resultat enunciat és conseqüència del Teorema 6.2.2. □

Observació 6.2.14.

1. *Hem demostrat, de fet, que tot grup extensió central finita de M_{11} o M_{12} es realitza com a grup de Galois d'una extensió $\mathbb{Q}$-regular de $\mathbb{Q}(T)$ que admet especialitzacions moderadament ramificades sobre $\mathbb{Q}$.*

2. *A [Mes94b] es remarca que l'obstrucció al problema $(\widetilde{M_{12}}, \varphi_T)$ és l'element de la 2-component del grup de Brauer $Br_2(\mathbb{Q}(T)) \cong H^2(G_{\mathbb{Q}(T)}, \mathbb{Z}/2\mathbb{Z})$ corresponent a la $\mathbb{Q}(T)$-àlgebra de quaternions $(2^{22}3^{18} - 5^{15}T^2, 6T)$. Per tant, fent el canvi de base $T = 6U^2$ s'obté una realització regular de M_{12} sobre $\mathbb{Q}(U)$ per a la qual el problema d'immersió central universal és resoluble. Hem comprovat, però, que aquesta extensió de $\mathbb{Q}(U)$ no admet especialitzacions moderadament ramificades.*

6.3 La propietat d'aixecament aritmètic per a extensions centrals finites de grups alternats

L'objectiu d'aquesta secció és contribuir al següent problema proposat per S.Beckmann (cf. [Bec94]):

> Tota realització d'un grup finit G com a grup de Galois sobre $\mathbb{Q}$ es pot obtenir per especialització d'una realització regular de G com a grup de Galois sobre $\mathbb{Q}(T)$?

Notem que una resposta afirmativa a la qüestió anterior per a tot grup finit G implicaria, en particular, que el problema invers de la teoria de Galois sobre $\mathbb{Q}$ és equivalent al problema invers regular sobre $\mathbb{Q}(T)$.

6.3.1 La propietat d'aixecament aritmètic

E. Black proposa la següent definició (cf. [Bla99a] i [Bla99b]).

Definició 6.3.1. *Direm que un grup finit G té la* ***propietat d'aixecament aritmètic*** *sobre un cos K si tota G-extensió de K s'obté per especialització d'alguna G-extensió K-regular de $K(T)$ en algun $T = t_0 \in K$.*

Beckmann i Black parlen de "G-recobriments ramificats de $\mathbb{P}^1$ definits sobre K" enlloc de "G-extensions K-regulars de $K(T)$" ; es tracta de terminologies equivalents, via el functor *cossos de funcions*.

Generalitzant el problema de Beckmann, Black conjectura que la propietat d'aixecament aritmètic es satisfà per a tot grup finit sobre *qualsevol cos* (cf. [Bla99b]). La validesa de la conjectura de Black implicaria (una resposta afirmativa a) el problema invers regular de la teoria de Galois sobre qualsevol cos (cf. [Dèb99a, Prop. 1.2]).

Resultats recents de Colliot-Thélène [CT00] (característica 0) i Moret-Bailly [MB01] (característica qualsevol) estableixen que, sobre un *cos gran* (large field) K, sempre es té la següent generalització de la propietat d'aixecament aritmètic:

> Si H és un subgrup d'un grup finit G, aleshores tota H-extensió de K s'obté per especialització d'alguna G-extensió K-regular de $K(T)$ en algun $T = t_0 \in K$.

En particular, tot grup finit satisfà la propietat d'aixecament aritmètic sobre un cos gran K. Aquest resultat generalitza el fet conegut que el problema invers regular admet una resposta afirmativa sobre $K(T)$, quan K és un cos gran qualsevol (cf. [Har87], [Pop96]).

Convé remarcar que els cossos base que més ens interessen són els cossos de nombres (especialment $K = \mathbb{Q}$), i aquests estan molt lluny de ser cossos grans.

A partir d'ara, (gairebé) sempre suposarem que K és un cos de característica 0 i, en particular, infinit.

Si existeix un polinomi $P(T_1, \ldots, T_m, X) \in K(T_1, \ldots, T_m)[X]$ genèric per a G-extensions sobre K, aleshores G satisfà la propietat d'aixecament aritmètic sobre K (cf. [Bla99a, Prop. 1.2]). Això és clar si tenim en compte que:

1. si L/K és una G-extensió de K, aleshores L és el cos de descomposició de $P(t, X)$ per algun $t \in K^m$,

2. existeix algun $s \in K^m$ tal que totes les arrels de $P(s, X)$ són simples i pertanyen a K (cf. [Kem01]),

3. $P(t + T(s - t), X)$ defineix una G-extensió de $K(T)$ que especialitza a L/K (en $T = 0$); per 2., es tracta d'una extensió K-regular.

Si suposem, a més, que K és hilbertià, aleshores en l'argument anterior podem triar s de manera que el cos de descomposició sobre K de $P(s, X)$ defineixi una G-extensió de K linealment disjunta amb L/K. En aquest cas, doncs, podem admetre que l'extensió prefixada tingui grup de Galois $\mathrm{Gal}(L/K)$ isomorf a un subgrup qualsevol de G (usant [Kem01]). És a dir, val la versió generalitzada de la propietat d'aixecament aritmètic.

A la Secció 5.2 ja hem recordat alguns grups per als quals es coneix l'existència de polinomis genèrics sobre $\mathbb{Q}$ (i, per tant, sobre qualsevol cos de característica 0) com, per exemple, tots els grups simètrics i alguns grups abelians

i diedrals. Tots aquests grups satisfan, doncs, la propietat d'aixecament aritmètic sobre qualsevol cos de característica 0.

Altres resultats relatius a la propietat d'aixecament aritmètic es poden trobar, per exemple, a [Bla98], [Bla99b] i [Dèb99a].

Per als nostres propòsits, convé destacar:

Proposició 6.3.2. *[Bec94]*
La propietat d'aixecament aritmètic es satisfà per a tot grup abelià finit, sobre qualsevol cos de nombres.

Més generalment, Dèbes [Dèb99b] obté que tot grup abelià finit satisfà la propietat d'aixecament aritmètic sobre *qualsevol* cos. Per completitud, demostrem la següent generalització d'aquest resultat, esmentada a [Dèb99b] i que ja hem utilitzat en seccions anteriors.

Proposició 6.3.3. *Sigui H un subgrup d'un grup abelià finit G i sigui K un cos qualsevol. Suposem donats $t_0 \in K$ i un conjunt finit $D \subset \mathbb{P}^1(K)$. Aleshores, tota H-extensió de K es pot obtenir per especialització en $T = t_0$ d'alguna G-extensió K-regular de $K(T)$ no ramificada sobre D.*

Demostració. Sigui $\chi : G_K \to H$ l'epimorfisme corresponent a la H-extensió donada L/K i considerem l'epimorfisme constant

$$\chi_T : G_{K(T)} \to \mathrm{Gal}(L(T)/K(T)) \cong H.$$

Com que G es abelià finit, és conegut que existeix alguna G-extensió K-regular de $K(T)$ no ramificada en un conjunt finit prefixat $S \subset \mathbb{P}^1(K)$ qualsevol (cf. [Dèb99b]). En particular, existeix alguna G-extensió K-regular $M_T/K(T)$ no ramificada en $T = t_0$. Sigui $\varphi_T : G_{K(T)} \to G$ l'epimorfisme corresponent.

Sigui M/K l'especialització de $M_T/K(T)$ en $T = t_0$. M/K és una A-extensió de K, per algun subgrup $A \subseteq G$.

Considerem ara el morfisme constant

$$\psi_T : G_{K(T)} \to \mathrm{Gal}(M(T)/K(T)) \cong A \subseteq G,$$

obtingut de $\mathrm{Gal}(M(T)/K(T)) = \mathrm{Gal}(M/K)$.

Definim el morfisme $\phi_T : G_{K(T)} \to G$ com $\phi_T := \chi_T.\varphi_T.\psi_T^{-1}$. Clarament, χ és precisament l'especialització de ϕ_T en $T = t_0$. A més,

$$\phi_T(G_{\overline{K}(T)}) = \varphi_T(G_{\overline{K}(T)}) = G$$

i, per tant, ϕ_T correspon a una G-extensió K-regular de $K(T)$.

Això acaba la demostració, donat que podem suposar també $D \subseteq S$; és a dir, podem triar φ_T que no ramifiqui sobre D (i, per tant, tampoc ho farà ϕ_T). □

6.3.2 Extensions centrals finites de grups alternats

Tal com Black esmenta a [Bla99b], de la construció de Mestre [Mes90] es pot obtenir la propietat d'aixecament aritmètic per a tot grup alternat sobre qualsevol cos de característica 0. Això és clar a partir del Teorema d'Irreductibilitat de Hilbert i del següent resultat conegut que ja hem usat a la Secció 6.2.

Proposició 6.3.4. *(cf., per exemple, [Kem01, Lemma 2])*
Sigui $G \subseteq S_n$ un grup de permutacions i N/L una G-extensió de cossos infinits. Si $s(X_1, \ldots, X_n) \in N[X_1, \ldots, X_n]$ és un polinomi no nul qualsevol, aleshores existeixen $\alpha_1, \ldots, \alpha_n \in N$ tals que:

(a) $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, *per a tot* $\sigma \in G$

(b) $s(\alpha_1, \ldots, \alpha_n) \neq 0$

Convé notar:

1. Si $\prod_{i \neq j}(X_i - X_j)$ és un factor de $s(X_1, \ldots, X_n)$, aleshores els elements α_i són diferents dos a dos i N és el cos de descomposició sobre L del polinomi $\prod_i (X - \alpha_i) \in L[X]$.

2. La Proposició 6.3.4 s'acostuma a demostrar en el cas $G \subseteq S_n$ transitiu (com a [Kem01]). El cas general es pot obtenir d'aquest, per exemple, per un argument inductiu sobre el nombre d'òrbites.

El resultat principal d'aquesta secció és el següent.

Teorema 6.3.5. *Sigui $n \neq 4, 6, 7$ un natural i sigui G un grup extensió central finita de A_n.*

(a) G satisfà la propietat d'aixecament aritmètic sobre qualsevol cos K de característica 0.

(b) Si L/K és una extensió de Galois de cossos hilbertians de característica 0 amb grup de Galois isomorf a un subgrup $I \subseteq G$, aleshores L/K s'obté per especialització d'alguna G-extensió K-regular de $K(T)$ en algun $T = t_0 \in K$.

Demostració. Les demostracions dels apartats (a) i (b) són completament anàlogues. Demostrarem els dos enunciats alhora, remarcant en quin punt cal usar el caràcter hilbertià de K (per a obtenir (b)).

Per a $n \leq 3$, el grup A_n és cíclic i, per tant, tot grup G extensió central finita de A_n és abelià. Així, per la Proposició 6.3.3, només cal considerar els casos $n = 5$ i $n > 7$.

Suposem donada una extensió central finita

$$1 \to C \to G \xrightarrow{\pi} A_n \to 1$$

i una I-extensió M/K de cossos de característica 0, on I és un subgrup de G ($I = G$ en (a) i I qualsevol en (b)). Denotem per

$$\widetilde{\varphi} : G_K \longrightarrow \mathrm{Gal}(M/K) \cong I \subseteq G$$

l'epimorfisme corresponent.

Cal provar l'existència d'un epimorfisme K-regular $G_{K(T)} \to G$ que especialitzi a $\widetilde{\varphi}$ en algun $T = t_0 \in K$.

Sigui L/K la $\pi(I)$-subextensió de M/K corresponent a

$$\varphi := \pi \circ \widetilde{\varphi} : G_K \longrightarrow \pi(I) \subseteq A_n.$$

Gràcies a la Proposició 6.3.4, podem suposar que L és el cos de descomposició sobre K d'un polinomi mònic $f(X) \in K[X]$ de grau n tal que:

- si n és senar, $P(X) := f(X)$ és H-general,
- si n és parell, $P(X) := (X - a)f(X)$ és H-general per algun $a \in K$.

Podem aplicar, doncs, els resultats de [Mes90] (veure Proposició 4.2.1) per a obtenir una A_n-extensió K-regular $L_T/K(T)$ que especialitzi a L/K en algun $T = t_0 \in K$. Més concretament, amb les notacions de la Secció 4.2, és suficient agafar L_T com el cos de descomposició sobre $K(T)$ de:

- $P(X) - TQ(X)$, per a n senar,
- $\frac{P(X) - \frac{P(T)}{Q(T)}Q(X)}{X - T}$, per a n parell.

Així, prendrem $t_0 = 0$ si n és senar i $t_0 = a$ si n és parell.

Sigui $\varphi_T : G_{K(T)} \longrightarrow A_n$ l'epimorfisme corresponent a aquesta G-extensió $L_T/K(T)$. Per hipòtesi, $\varphi_{t_0} = \varphi$.

Fem la següent hipòtesi que demostrarem més endavant.

(∗) El problema d'immersió (π, φ_T) admet una solució $\widetilde{\varphi_T} : G_{K(T)} \longrightarrow G$ no ramificada en $T = t_0$.

Considerem la següent extensió central de $\pi(I)$ obtinguda de π

$$1 \to C \to I.C \xrightarrow{\pi_I} \pi(I) \to 1.$$

Com que tant $\widetilde{\varphi_{t_0}}$ com $\widetilde{\varphi}$ són solucions del problema (π_I, φ), haurà de ser $\chi.\widetilde{\varphi_{t_0}} = \widetilde{\varphi}$, per algun $\chi \in \mathrm{Hom}(G_K, C)$. A més, per la Proposició 6.3.3, χ

es pot obtenir per especialització en $T = t_0$ d'algun epimorfisme K-regular $\chi_T \in \mathrm{Hom}(G_{K(T)}, C)$ no ramificat on $\widetilde{\varphi_T}$ ramifica.

Del fet que $\widetilde{\varphi_T}$ i χ_T defineixin extensions linealment disjuntes sobre $\overline{K}(T)$ s'obté que el morfisme

$$(\chi_T, \widetilde{\varphi_T}) : G_{\overline{K}(T)} \to \chi_T(G_{\overline{K}(T)}) \times \widetilde{\varphi_T}(G_{\overline{K}(T)})$$

és un epimorfisme. D'altra banda, $\chi_T(G_{\overline{K}(T)}) = C$ i $\widetilde{\varphi_T}(G_{\overline{K}(T)}) = A_n$ donat que φ_T i χ_T són K-regulars.

En conclusió, $\chi_T.\widetilde{\varphi_T}(G_{\overline{K}(T)}) = G$ i, per tant, $\chi_T.\widetilde{\varphi_T}$ és una solució pròpia K-regular del problema d'immersió (π, φ_T) que especialitza a $\widetilde{\varphi}$ en $T = t_0$.

Haurem acabat la demostració del Teorema si provem l'afirmació $(*)$.

Notem que l'afirmació $(*)$ és independent de la solució prefixada $\widetilde{\varphi}$ del problema (π_I, φ); el fet realment essencial és que aquest problema d'immersió sigui resoluble. A partir d'ara podem suposar, doncs, que $\widetilde{\varphi}$ és una solució *pròpia* de (π_I, φ). Això és clar per a l'enunciat (a) donat que, per hipòtesi, $\widetilde{\varphi}(G_K) = I = G$. En la situació de (b), l'existència d'una solució pròpia de (π_I, φ) s'obté de la resolubilitat del problema, gràcies a la hipòtesi addicional K hilbertià (cf. [MM99, Chap. IV, Cor. 6.2]).

No hi ha res a demostrar quan la successió exacta

$$1 \to C \to G \xrightarrow{\pi} A_n \to 1$$

és split. En aquest cas, si $s : A_n \to G$ és una secció de π, aleshores $s \circ \varphi_T : G_{K(T)} \to G$ és una solució de (π, φ_T) no ramificada en $T = t_0$.

Suposem, doncs, que la successió exacta anterior no escindeix. Com que estem considerant els casos $n = 5$ o $n > 7$, A_n és un grup perfecte amb grup de multiplicadors de Schur isomorf a $\mathbb{Z}/2\mathbb{Z}$. Si $H \subseteq G$ és un subgrup minimal amb la propietat $\pi(H) = A_n$, aleshores H és una extensió central de A_n per $< \tau >$, per algun $\tau \in C$ d'ordre 2 ($H \cong \widetilde{A_n}$).

Sigui $\overline{C}$ el 2-subgrup de Sylow de C i notem $\overline{G} = \overline{C}.H$. Un complement $\widehat{C}$ de $\overline{C}$ en C haurà de ser també un complement (central) de $\overline{G}$ en G.

Considerem l'extensió central natural (restricció de π)

$$1 \to \overline{C} \to \overline{G} \stackrel{\overline{\pi}}{\to} A_n \to 1.$$

Tota solució del problema d'immersió $(\overline{\pi}, \varphi_T)$ defineix també una solució de (π, φ_T) via la inclusió $\overline{G} \subseteq G$. A més, és clar que l'obstrucció del problema d'immersió $(\overline{\pi}, \varphi_T)$ s'anul.la en $T = t_0$, donat que $G = \overline{G} \times \widehat{C}$ (producte directe intern) i (π_I, φ) és resoluble per hipòtesi. De fet, aquesta és la raó per la qual considerem $\overline{G}$ i no ens conformem amb H: l'existència de $\widetilde{\varphi}$ no és suficient (ni en (a) ni en (b)) per a garantir la resolubilitat del problema universal per a φ i, per tant, tampoc per a φ_T.

De tot l'anterior concloem que, per a provar $(*)$, podem suposar que C és un 2-grup, conservant la hipòtesi de resolubilitat sobre el problema (π_I, φ). Seguim denotant per $\widetilde{\varphi}$ una solució pròpia de (π_I, φ) corresponent a una I-extensió M/K.

Considerem, ara, les extensions centrals naturals

$$1 \to < \tau > \to C \stackrel{\gamma_1}{\to} G_1 \to 1$$

$$1 \to < \tau > \to H \stackrel{\gamma_2}{\to} G_2 = A_n \to 1$$

$$1 \to < \tau > \to G \stackrel{\gamma_3}{\to} G_3 \to 1$$

i denotem per $\varepsilon_1, \varepsilon_2, \varepsilon_3$ les corresponents classes de cohomologia en $H^2(G_i, < \tau >)$.

Notem que $G_3 = G_1 \times G_2$ (producte directe intern) i que γ_2 és precisament la restricció de π a H. Per a $i = 1, 2$, $p_i : G_3 \to G_i$ denotarà la projecció natural.

Considerem els epimorfismes naturals:

$$\varphi_3 := \gamma_3 \circ \widetilde{\varphi} : G_K \to \gamma_3(I) \subseteq G_3,$$

$$\varphi_2 := p_2 \circ \varphi_3 : G_K \to \pi(I) \subseteq G_2,$$

$$\varphi_1 := p_1 \circ \varphi_3 : G_K \to G_1.$$

Per a cada $i = 1, 2, 3$, denotem per L_i/K la subextensió de M/K corresponent a φ_i. Clarament, $\varphi_2 = \varphi$, $L_3 = L_1.L_2$ i $\varphi_3 = \varphi_1.\varphi_2$.

Com que $< \tau >$ no té elements d'ordre 3, la Proposició 6.2.5 garanteix que l'obstrucció al problema d'immersió (γ_2, φ_T) és constant (però no necessàriament trivial).

Sigui $\phi_T : G_{K(T)} \to \mathrm{Gal}(L_1(T)/K(T)) \cong G_1$ l'epimorfisme constant que especialitza en $T = t_0$ (i en qualsevol $T = t \in K$) a φ_1. L'obstrucció del problema (γ_1, ϕ_T) és constant i coincideix amb l'obstrucció de (γ_1, φ_1).

Per a $i = 1, 2$, denotem per $\inf_i : H^2(G_i, < \tau >) \to H^2(G_3, < \tau >)$ el corresponent morfisme d'inflació.

En $H^2(G_3, < \tau >)$, es té la igualtat $\varepsilon_3 = \inf_1(\varepsilon_1) + \inf_2(\varepsilon_2)$. Així, l'obstrucció al problema d'immersió $(\gamma_3, \varphi_T.\phi_T)$ és precisament la suma de les obstruccions als problemes (γ_2, φ_T) i (γ_1, ϕ_T).

En particular, l'obstrucció a $(\gamma_3, \varphi_T.\phi_T)$ és constant. Per força ha de ser trivial, donat que s'anul.la en el punt no ramificat $T = t_0$, donat que $\widetilde{\varphi}$ és una solució de $(\gamma_{3|I}, \varphi_3) = (\gamma_{3|I}, \varphi_{t_0}.\phi_{t_0})$.

Sigui, doncs, $\widetilde{\varphi_T} : G_{K(T)} \longrightarrow G$ una solució de $(\gamma_3, \varphi_T.\phi_T)$ (necessàriament pròpia). Clarament, $\widetilde{\varphi_T}$ és també una solució de (π, φ_T).

Suposem que l'epimorfisme $\widetilde{\varphi_T}$ ramifica en $T = t_0$. Tant φ_T com ϕ_T no ramifiquen en $T = t_0$ i, per tant, tampoc ho fa $\varphi_T.\phi_T$. Així, la imatge de qualsevol grup d'inèrcia (en $T = t_0$) en $G = \widetilde{\varphi_T}(G_{K(T)})$ ha d'estar continguda en el nucli $< \tau >$ de γ_3. Sigui $\omega_T \in \mathrm{Hom}(G_{K(T)}, < \tau >)$ l'epimorfisme corresponent a una $< \tau >$-extensió de $K(T)$ totalment ramificada en $T = t_0$ com, per exemple, el cos de descomposició sobre $K(T)$ de $X^2 - (T - t_0)$. D'aquesta manera, $\widetilde{\varphi_T}.\omega_T$ és una solució als problemes d'immersió $(\gamma_3, \varphi_T.\phi_T)$ i (π, φ_T), no ramificada en $T = t_0$ donat que el generador de la inèrcia és $\tau.\tau = 1$.

En conclusió, la hipòtesi $(*)$ queda provada i, per tant, també el Teorema.

□

Observació 6.3.6. *Quan $n = 4, 6, 7$, la demostració anterior no és vàlida perquè A_n no és perfecte ($n = 4$) o el seu grup de multiplicadors de Schur*

conté elements d'ordre 3 *($n = 6, 7$). Tot i així, l'argument donat sí s'aplica a alguns problemes d'immersió i s'obté, per exemple, que A_n i $\widetilde{A_n}$ satisfan la conclusió del Teorema anterior i, per tant, la propietat d'aixecament aritmètic sobre qualsevol cos de característica* 0*, per a tot n. Només cal notar que la demostració donada funciona sempre que existeixi algun subgrup $H \subseteq G$ isomorf a A_n o $\widetilde{A_n}$ tal que $\pi(H) = A_n$.*

L'apartat (b) del Teorema anterior ens permet recuperar directament el Teorema 6.2.6 per a $n \neq 4, 6, 7$. De fet, prenent $H = \{1\}$ i aplicant la Proposició 5.2.2 obtenim el següent resultat.

Corol.lari 6.3.7. *Sigui $n \neq 4, 6, 7$ un natural i sigui G un grup extensió central finita de A_n. Aleshores, G es realitza com a grup de Galois d'infinites extensions de $\mathbb{Q}$, linealment disjuntes dos a dos, en les quals els primers d'un conjunt finit prefixat qualsevol S descomponen completament.*

Més generalment, l'argument anterior permet demostrar en alguns casos l'existència d'infinites G-extensions de $\mathbb{Q}$ que, per compleció, donen lloc a extensions locals (de $\mathbb{Q}_p$) prefixades, una per a cada primer p d'un conjunt finit S. Això és clar, per exemple, sempre que tots els grups de Galois de les extensions locals donades siguin isomorfs a algun subgrup d'un únic $H \subseteq G$ per al qual es té un resultat de tipus Grunwald-Wang (per exemple, si existeix un polinomi genèric per a H-extensions sobre $\mathbb{Q}$).

Bibliografia

[Apo80] T.M. Apostol, *Introducción a la Teoría de Números*, Reverté, 1980.

[Bec94] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering ?*, J. Algebra **164** (1994), 430–451.

[Bir94] B. Birch, *Noncongruence subgroups, Covers and Drawings*, In "The Grothendieck theory of dessins d'enfants", edited by L. Schneps, pp. 25–46, Cambridge Univ. Press, Cambridge, 1994.

[Bla98] E. V. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra **203** (1998), 12–29.

[Bla99a] E. Black, *Deformations of dihedral 2-group extensions of fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241.

[Bla99b] E. Black, *On semidirect products and the arithmetic lifting property*, J. London Math. Soc. (2) **60** (1999), 677–688.

[BLV86] P. Bayer, P. Llorente, and N. Vila, $\widetilde{M_{12}}$ *comme groupe de Galois sur* $\mathbb{Q}$, C. R. Acad. Sci. Paris **303** (1986), 277–280.

[Bru66] G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32** (1966), 317–326.

[CHVS00] A. Cueto-Hernández and G.D. Villa-Salvador, *Nilpotent extensions of number fields with bounded ramification*, Pacific J. of Math. **196** (2000), 297–316.

[Coh78] H. Cohn, *A classical invitation to Algebraic Numbers and Class Fields*, Springer, 1978.

[Col87] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, L'Ens. Math. **33** (1987), 183–189.

[Cox89] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Pure and Applied Mathematics, Wiley and Sons, 1989.

[CT98] J.-L. Colliot-Thélène, *The Hasse principle in a pencil of algebraic varieties*, In "Number Theory, Proc. Of a Conference Held at Tiruchirapalli, 1996", Contemp. Math. 210, pp. 19–39, AMS, 1998.

[CT00] J.-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*, Ann. of Math. **151** (2000), 359–373.

[Dèb99a] P. Dèbes, *Galois covers with prescribed fibers: The Beckmann-Black Problem*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), 273–286.

[Dèb99b] P. Dèbes, *Some arithmetic properties of algebraic covers*, In "Aspects of Galois Theory", London Math. Soc. LNS 256 (2), pp. 66–84, Cambridge Univ. Press, 1999.

[DeM83] F. R. DeMeyer, *Generic Polynomials*, J. Algebra **84** (1983), 441–448.

[Hal59] M. Hall, *Theory of Groups*, Macmillan, 1959.

[Har87] D. Harbater, *Galois coverings of the arithmetic line*, In "Number Theory Seminar, (New York 1984/85)", LNM 1240, pp. 165–195, Springer-Verlag, New York, 1987.

[Har94] D. Harbater, *Galois groups with prescribed ramification*, In "Arithmetic Geometry"(Tempe, A.Z., 1993), Contemp. Math. 174, pp. 35–60, AMS, Providence, 1994.

[HS01] A. Hermez and A. Salinier, *Rational trinomials with the alternating group as Galois group*, J. Number Theory **90** (2001), 113–129.

[ILF97] V. V. Ishkhanov, B. B. Lur'e, and D. K. Faddeev, *The Embedding Problem in Galois Theory*, Translations of Mathematical Monographs, vol. 165, AMS, Providence, 1997.

[Jan96] G.J. Janusz, *Algebraic Number Fields*, Graduate Studies in Math., AMS, 1996.

[JLY02] C.U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Cambridge Univ. Press, Cambridge, 2002.

[JY82] C. U. Jensen and N. Yui, *Polynomials with D_p as Galois Group*, J. Number Theory **15** (1982), 347–375.

[Kem01] G. Kemper, *Generic polynomials are Descent-Generic*, Manuscripta Math. **105** (2001), 139–141.

[KM02] J. Klüners and G. Malle, *Counting nilpotent Galois extensions*, preprint, 2002.

[KSS89] D. Kotlar, M. Schacher, and J. Sonn, *Central extensions of symmetric groups as Galois groups*, J. Algebra **124** (1989), 183–198.

[Kuy64] W. Kuyk, *On a theorem of E. Noether*, Nederl. Akad. Wetensch Proc. Ser. A **67** (1964), 32–39.

[Led00a] A. Ledet, *Generic and explicit realization of small p-Groups*, J. Symbolic Comput. **30** (2000), 859–865.

[Led00b] A. Ledet, *Generic Extensions and Generic Polynomials*, J. Symbolic Comput. **30** (2000), 867–872.

[LNV84] P. Llorente, E. Nart, and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arithm. **XLIII** (1984), 367–373.

[Mar63] H. Markscheitis, *On p-extensions with one critical prime (en rus)*, Izv. Akad. Nauk. SSSR, Ser. Mat. **27** (1963), 463–466.

[MB01] L. Moret-Bailly, *Construction de revêtements de courbes pointées*, J. Algebra **240** (2001), 505–534.

[Mes90] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$*, J. Algebra **131** (1990), 483–495.

[Mes94a] J.-F. Mestre, *Annulation, par changement de variable, d'éléments de $Br_2(k(x))$ ayant quatre pôles*, C. R. Acad. Sci. Paris **319** (1994), 529–532.

[Mes94b] J.-F. Mestre, *Construction d'extensions régulières de $\mathbb{Q}(t)$ à groupes de Galois $SL_2(\mathbb{F}_7)$ et $\widetilde{M}_{12}$*, C. R. Acad. Sci. Paris **319** (1994), 781–782.

[Mes98] J.-F. Mestre, *Extensions $\mathbb{Q}$-régulières de $\mathbb{Q}(T)$ de groupe de Galois $6A_6$ et $6A_7$*, Israel Journal of Mathematics **107** (1998), 333–341.

[Mil96] J.S. Milne, *Algebraic number theory (Math 676)*, http://www.jmilne.org/math/, 1996.

[MM99] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer-Verlag, 1999.

[Mon99] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, Ph.D. thesis, Universitat de Barcelona, 1999.

[MZM86] B.H. Matzat and A. Zeh-Marschke, *Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$*, J. Number Theory **23** (1986), 195–202.

[Nar90] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer, Berlin, 1990.

[Neu79] J. Neukirch, *On solvable number fields*, Invent. Math. **53** (1979), 135–164.

[Neu99] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Springer, 2000.

[Ore28] Ö Ore, *Newtonsche polygone in der theorie der algebraischen körper*, Math. Ann. **99** (1928), 84–117.

[Pop96] F. Pop, *Embedding problems over large fields*, Ann. of Math. **144** (1996), 1–34.

[Rei37] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. Crelle **177** (1937), 1–5.

[Sal82] D. Saltman, *Generic Galois extensions and problems in Field Theory*, Adv. Math. **43** (1982), 250–283.

[Sch00] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge Univ. Press, Cambridge, 2000.

[Ser92a] J.-P. Serre, *Carta a B. H. Matzat*, 20 juliol, 1992.

[Ser92b] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett, Boston, 1992.

[Ser94] J.-P. Serre, *Cohomologie galoisienne des extensions transcendantes pures*, In " Cohomologie Galoisienne", 5-ième édition, révisée et complétée, LNM 5, Springer-Verlag, Berlin, 1994.

[Sha54] I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk. SSSR **18** (1954), 525–578, traducció a: Amer. Math. Soc. Transl. 4 (1956), 185-237.

[Sha89] I.R. Shafarevich, *On the factors of a descending central series*, Mat. Zam. **45** (1989), 114–117, trad. a: Math. Notes 45 (1989), 262-264.

[Son91] J. Sonn, *Central extensions of S_n as Galois groups of regular extensions of $\mathbb{Q}(T)$*, J. Algebra **140** (1991), 355–359.

[SS58] A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208, Errata, ibid. 5 (1959), 259.

[Suz82] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[Swa62] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[Tsc52] P. I. Tschebyshev, *Sur la totalité des nombres premiers inférieurs á une limite donnée*, J. de Math. **17** (1852), 341–365.

[Vil85] N. Vila, *On central extensions of A_n as Galois group over $\mathbb{Q}$*, Arch. Math. **44** (1985), 424–437.

[VL95] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), 194–223.

[Wan48] S. Wang, *A counterexample to Grunwald's theorem*, Ann. of Math. **49** (1948), no. 4, 1008–1009.

[Yam70] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.